ENCYKLOPEDIA BEZPIECZEŃSTWA

TOM 9

ENCYKLOPEDIA
BEZPIECZEŃSTWA

TOM 9

A–Z

REDAKCJA NAUKOWA
OLGA WASIUTA, SERGIUSZ WASIUTA

ENCYKLOPEDIA
BEZPIECZEŃSTWA

TOM 9
A–Z

REDAKCJA NAUKOWA
OLGA WASIUTA, SERGIUSZ WASIUTA

© Copyright by Authors & Wydawnictwo Libron
Kraków 2026

ISBN: 978-83-68637-15-1

Recenzenci:
Prof. dr hab. Wojciech Jakubowski (Uniwersytet Warszawski)
Prof. dr hab. Bogusław Pacek (Muzeum Wojska Polskiego w Warszawie)

Redakcja:
Sylwia Mosińska

Korekta wydawnicza:
Marta Masłowska

Projekt okładki i skład:
LIBRON

Publikacja sfinansowana przez Uniwersytet Komisji Edukacji Narodowej w Krakowie

Wydawnictwo LIBRON – Filip Lohner
al. Daszyńskiego 21/13
31-537 Kraków
tel. 12 628 05 12
e-mail: office@libron.pl
www.libron.pl

SPIS TREŚCI

7 WYKAZ HASEŁ
13 HASŁA

Agencja Projektów Społecznych 13
Agencja Unii Europejskiej ds. Narkotyków 20
AI literacy 29
Akademia Wojskowa Stanów Zjednoczonych w West Point 35
Akulturacja 35
Amerykański system obrony przeciwlotniczej i przeciwrakietowej 48
Anarchosyndykalizm 53
Apartheid 60
Architektura bezpieczeństwa 66
Autodestrukcja 71

Bałtycka Akademia Obrony 79
Bezpieczeństwo akustyczne 85
Bezpieczeństwo elektryczne 87
Bezpieczeństwo rynków kapitałowych 100
Bezpieczeństwo w sensie pozytywnym i negatywnym 112
Bezpieczeństwo żywnościowe 117
Biała księga w sprawie przyszłości Europy 122
Blokada ekonomiczna/blokada gospodarcza 126
Bractwa kurkowe 131

Centra Doskonałości NATO – COE 143
Centrum Stimsona 150
ChatGPT 156
Cyberodporność 162
Cyberpopulizm 171
Cyberutopizm 177
Cyfrowa osoba 186
Cyfrowy autorytaryzm 194
Czwarta władza 201

Degradacja attention span w środowiskach AI 207
Deklaracja weimarska w kontekście zagrożeń rosyjską dezinformacją 213

Demarkacja 219
Dron FPV 223

Etatyzm 231
Etnopopulizm 241
Europejskie sojusze przemysłowe na rzecz małych reaktorów modułowych 245
Europejski Korpus Solidarności (EKS) 253
Europejski Sojusz Nuklearny 262

Fałszywy clickbait 271
Finansowanie terroryzmu 277
FOMO 290
Formacje policyjne w Polsce do czasów Księstwa Warszawskiego 296
Fregaty 304
Fronda 308
Fundacja na rzecz Międzynarodowego Pokoju Carnegie 313

Gabinet Cieni 319
Generative overproduction i AI slop 324

Himars M142 331
Hinduski nacjonalizm (hindutwa) 335

Incydent cybernetyczny 345
Inżynieria podpowiedzi 351
Irańskie pociski balistyczne 361

Karelski Batalion Narodowy 367
Katastrofa nuklearna 375
Komitet Bezpieczeństwa Morskiego 383
Korweta 389
Krążownik 394
Kryptografia kwantowa 398
Kwantowe zabezpieczenia 405

Legion "Wolność Rosji" 415
Lingua franca 424
LLM Grooming 429
Los Zetas 433
Lotniskowiec 438

Manipulacja algorytmiczna 445
Międzynarodowa Organizacja Pracy, MOP 455
Międzynarodowe wielostronne partnerstwo przeciwko cyberterroryzmowi (IMPACT) 464
Miękka siła 471
Militaryzacja narodu 481
Mimikra społeczna przestępców 486

Narodowa Strategia Wojskowa Węgier z 2021 r. 495
Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni 500
Niszczyciel 505

Ochrona najważniejszych organów państwa polskiego w okresie międzywojennym 511
Odporność ekologiczna 519
Odporność energetyczna 530
Odporność finansowa 541
Odstraszanie przez karę 551
Odstraszanie przez uniemożliwienie/odmowę 559
Okręt podwodny 568
Oligarchia 573
Operacja „Pajęczyna" 587
Operacja sił połączonych 595
Oprogramowanie antyszpiegowskie 601
Osobowość przestępcza 605

Pancernik 613
Paternalizm 618
Polacy a sztuczna inteligencja 625

Polskie formacje policyjne w okresie II Wojny Światowej 632
Pomoc humanitarna 639
Populizm antyimigrancki 647
Populizm prawicowy 653
Praktyki operacyjne darczyńców humanitarnych 661
Pranie brudnych pieniędzy lub pranie pieniędzy 668
Projekt na rzecz elektrowni jądrowej w Polsce 676
Przestępczość nieletnich 683
Przestępstwo 697

Quasipaństwo 707

Restytucja 717
Rewanżyzm 721
Rezerwa strategiczna 726
Rosyjska Agencja Projektowania Społecznego, APS 731
Rosyjska fundacja Pravfond 740
Rosyjska operacja dezinformacyjna „Doppelgänger" 749
Rosyjska operacja dezinformacyjna „Kylo" 759
Rosyjska operacja dezinformacyjna „Matrioszka" 769
Rosyjska operacja „Przeciążenie" 786
Rosyjska operacja dezinformacyjna „Undercut" 797
Rosyjska Powstańcza Armia 805
Rosyjskie operacje FIMI 810
Rosyjska sieć dezinformacyjna Storm-1516 820
Rosyjskie fortyfikacje w wojnie w Ukrainie 831
Rosyjski Korpus Ochotniczy 837

Sekta 853
Sharenting 862
Socjalizm demokratyczny 868
Siły zbrojne Republiki Chińskiej 877
Służba kontrwywiadu wojskowego RP 882
Służba wojskowa kobiet 886
Stała współpraca strukturalna w dziedzinie obronności 892

Stowarzyszenie Cywilnych Zespołów Ratowniczych z Psami 897
Strefa zdemilitaryzowana 902
Szowinizm opiekuńczy 912
Środkowoeuropejska Współpraca Obronna 917

Technooptymizm 925
Technosolucjonizm 930
Traktaty o ograniczeniu zbrojeń strategicznych 935
Traktaty o redukcji zbrojeń strategicznych 943
Tripwire 950
Turning Point USA (TPUSA) 959

Ustawa CXL z 2021 r. o Obronie Narodowej oraz Węgierskich Siłach Zbrojnych 965
Ustawa LXIX z 2024 r. o węgierskim cyberbezpieczeństwie 970

Viginum 977

Werbunek 985
Węgierska strategia cyberbezpieczeństwa 2025–2030 993
Węgierski Program Rozwoju Obrony Narodowej i Sił Zbrojnych Zrínyi 1000
Wiedeńskie Centrum ds. Rozbrojenia i Nieproliferacji 1005
Wojna cybernetyczna 1010
Wojna kognitywna 1018
Wojna kulturowa 1030
Wojska aeromobilne 1031
Wojskowe systemy ratownicze 1037
Wsparcie przez państwo gospodarza 1048
Wychowanie narodowe 1053
Wytłumaczalność 1059
Wzmocniona Wysunięta Obecność 1064

Zasady świadczenia pomocy humanitarnej 1071
Zatrzymanie nieletniego 1077

A

AGENCJA PROJEKTÓW SPOŁECZNYCH (ros. Агентство Социального Проектирования, ang. Social Design Agency, SDA) to rosyjskie przedsiębiorstwo informatyczne **i** komunikacyjne prowadzące – według oficjalnych dokumentów oraz międzynarodowych sankcji – działania związane z cyfrowymi kampaniami informacyjnymi i dezinformacyjnymi na zlecenie Kremla, których celem są mieszkańcy krajów Zachodu.

Organizacja jest zarejestrowana w Rosji, została założona w 2001 r. i oficjalnie zajmuje się projektowaniem i realizacją tzw. projektów społeczno-politycznych oraz usługami specjalistycznymi w sferze komunikacji. Natomiast w kontekście wojny z Ukrainą i rosyjskiej machiny propagandowej stała się jednym z kluczowych podmiotów dezinformacyjnych o znaczeniu międzynarodowym. Jej rola w praktyce znacznie się rozszerzyła, a działania są ściśle powiązane z rosyjskimi służbami państwowymi i polityką Kremla, zwłaszcza w obszarze informacji, propagandy i dezinformacji poza granicami Federacji Rosyjskiej.

Od 2022 r. Agencja Projektów Społecznych została zidentyfikowana jako kluczowy element rosyjskiej kampanii dezinformacyjnej prowadzonej w kontekście pełnoskalowej agresji przeciwko Ukrainie.

Agencja Projektów Społecznych w latach 2022–2025 stała się jednym z kluczowych wykonawców zleceń Kremla w obszarze operacji informacyjnych i psychologicznych (PSYOPS). Założona przez Ilję Gambaszydzego SDA wyewoluowała z klasycznej agencji marketingowej w zaawansowane centrum operacyjne prowadzące kampanie dezinformacyjne na skalę globalną, ze szczególnym uwzględnieniem Unii Europejskiej, Stanów Zjednoczonych i Izraela.

Z naukowego punktu widzenia SDA stanowi przykład „outsourcingu agresji informacyjnej", gdzie państwo autorytarne wykorzystuje prywatne podmioty komercyjne do realizacji celów strategicznych, co pozwala na zachowanie pewnego stopnia „wiarygodnego zaprzeczenia" (*plausible deniability*).

Niemieckie redakcje „Sueddeutsche Zeitung", „Westdeutscher Rundfunk (WDR)" i „Norddeutscher Rundfunk (NDR)" są znane ze współpracy w ramach sieci dziennikarstwa śledczego. WDR i NDR, a także estoński portal Delfi uzyskały od anonimowego informatora wewnętrzne dokumenty agencji, które pokazują mechanizm działania „machiny kłamstw" Putina. Zachodnie służby oceniają, że dokumenty są autentyczne. Z analizy przejętych plików wynika, że SDA zajmuje się projektowaniem i przygotowywaniem kampanii rozsiewających fałszywe rosyjskie narracje – m.in. dla Ukraińców i Niemców. Jednym z celów realizowanych przez SDA jest sprawienie, żeby Niemcy „bali się przyszłości tak bardzo, jak to możliwe" – pisze dziennik „Tageschau".

Jej działania obejmują m.in.:

- **tworzenie i koordynowanie fałszywych stron internetowych**. SDA prowadziła ogromną sieć stron podszywających się pod autentyczne media lub organizacje rządowe w krajach takich jak Niemcy, Francja, Włochy, Ukraina czy Wielka Brytania. Ich celem było rozpowszechnianie zmanipulowanych narracji i ataków informacyjnych sprzyjających Moskwie oraz podważanie wiarygodności realnych mediów;
- **wspieranie kampanii „RRN" (Russian Narrative Network/Rosyjska Sieć Narracji)**. Agencja była wskazywana jako kluczowy podmiot kampanii RRN – systematycznych działań mających na celu:

- manipulowanie opinią publiczną;
- szerzenie prorosyjskich przekazów politycznych;
- obniżenie poparcia dla państw wspierających Ukrainę;
- podważanie suwerenności i integralności terytorialnej Ukrainy oraz państw europejskich.

Media analizujące wewnętrzne dokumenty Agencji wskazują, że organizacja ta odgrywała rolę „aktora operacyjnego wojny mentalnej", działając na rzecz dyskredytacji Ukrainy, jej instytucji i społeczeństwa. Wśród materiałów jest firmowy film SDA, w którym występuje szef agencji Ilja Gambaszydze – na jego kurtce w barwach munduru widnieje napis: „Rosyjskie ideologiczne siły zbrojne". W tym filmie otwarcie mówi on o tym, czym zajmuje się SDA: chodzi o „zbieranie i analizowanie informacji z zachodniego sektora medialnego, opracowywanie własnych narracji i opakowanie ich w treści".

Z dokumentów datowanych na połowę 2024 r. wynika, że działania SDA opierają się na „fałszerstwach i kłamstwach". Materiały te obejmują m.in. listy zawierające około 100 nazwisk i obszarów działalności stałych i wolnych współpracowników opracowujących jednocześnie kilka kampanii dezinformacyjnych w różnych krajach. Wiele razy pojawia się także nazwisko kobiety pracującej w rosyjskiej administracji prezydenckiej, która regularnie brała udział w spotkaniach z SDA.

Z dokumentów, które wyciekły i zostały zaprezentowane konsorcjum dziennikarzy europejskich mediów, wynika, że w 2024 r. SDA miała zatrudniać ponad 100 osób, w tym 18 pracowników administracyjnych w głównym biurze, 8 redaktorów, 12 osób w dziale monitoringu prasy tradycyjnej, a 20 – w dziale monitoringu mediów społecznościowych. SDA zatrudnia również 7 tłumaczy, 3 twórców memów i rysunków, 4 osoby odpowiedzialne za produkcje wideo i wielu pracowników wykonujących swoje obowiązki zdalnie. Ujawnione dziennikarzom dokumenty pokazują, że SDA rozpoczyna przygotowanie do swoich operacji poprzez badanie sytuacji politycznej, społecznej i ekonomicznej w danym kraju, starając się identyfikować potencjalne napięcia oraz frustracje w społeczeństwie.

SDA stworzyła sieć co najmniej 120 stron podszywających się pod istniejące serwisy informacyjne i rządowe, do których przekierowuje użytkowników mediów społecznościowych. Stosowane taktyki obejmowały

unikanie popularnych słów kluczowych, aby ominąć narzędzia moderacji treści i uniknąć usunięcia konta.

Wyciek wewnętrznych materiałów Agencji Projektowania Społecznego ujawnił, że:

- tworzyła kampanie dezinformacyjne adresowane zarówno do społeczeństw europejskich, jak i ukraińskich;
- jej strategia obejmowała m.in. kampanie wywoływania strachu, polaryzowania opinii i legalizowania narracji prorosyjskich;
- podważała zaufanie do instytucji demokratycznych;
- wzmacniała prorosyjskie narracje w Europie;
- dezorientowała odbiorców co do faktów związanych z wojną i polityką międzynarodową;
- postrzegała swoje działania przez pryzmat „rosyjskich oddziałów ideologicznych", a jej szef Ilja Gambaszydze był identyfikowany przez amerykańskie służby jako kluczowa osobistość w „wojnie informacyjnej" Kremla.

Przecieki materiałów wewnętrznych uwidaczniają koordynację zespołu, który codziennie analizował zachodnie media w wielu językach, zarówno aby oceniać narracje prorosyjskie, jak i generować nowe treści propagandowe. To wskazuje, że jego projekty były częścią szerszego systemu rosyjskich operacji informacyjnych, w których narzędzia technologiczne łączono z celami geopolitycznymi.

Choć dokładna struktura Agencji nie jest w pełni jawna, śledztwa medialne ujawniają, że na kluczowych stanowiskach znajdują się osoby mające bliskie kontakty z administracją prezydenta Rosji, a także z instytucjami państwowymi odpowiedzialnymi za propagandę i komunikację strategiczną. Szef tej organizacji, często wymieniany w mediach dochodzeniowych, jest określany jako osoba odgrywająca znaczącą rolę w koordynowaniu działań propagandowych Rosji w warunkach wojny informacyjnej z Zachodem.

Agencja Projektów Społecznych funkcjonuje w obszarze, który dzisiaj określa się jako FIMI (Foreign Information Manipulation & Interference) – jej działania nastawione są na manipulowanie informacją w państwach obcych mające wpływ na ich debatę publiczną, politykę i społeczeństwo. Działalność tej organizacji pokazuje, jak rosyjskie podmioty – formalne

i półformalnie powiązane z państwem – realizują kampanie propagandowe, które:

- wykorzystują narzędzia cyfrowe i media społecznościowe;
- tworzą sztuczne konta, portale oraz narracje;
- starają się wpływać na postawy społeczne w państwach europejskich.

Agencja nie jest „neutralnym" podmiotem społecznym ani organizacją pozarządową, lecz częścią infrastruktury rosyjskich operacji informacyjnych, które realizują cele strategiczne państwa w sferze dezinformacji i ingerencji informacyjnej.

Agencja Projektów Społecznych nie działa w izolacji – według analiz OSW i materiałów zachodnich wywiadów stanowi część większej sieci podmiotów wspierających rosyjską operację wpływu znaną jako „Doppelgänger", współpracując z innymi podmiotami, takimi jak Struktura (ros. Grupa Kompanii Struktura; ang. Company Group Structura) czy ANO Dialog (autonomiczna organizacja, również zaangażowana w propagandę), odpowiedzialnymi za bezpośrednie kontakty z przedstawicielami Kremla, wykonywanie zadań i raportowanie o postępach poszczególnych kampanii.

Agencja Projektów Społecznych działa nie na klasycznym polu walki, lecz na „frontach narracyjnych" i medialnych, zaś manipulacje informacjami mają:

- wpływać na postawy społeczne i polityczne w Europie;
- osłabiać zaufanie do instytucji demokratycznych;
- wzmacniać antyukraińskie i prorosyjskie narracje w krajach zachodnich;
- osłabiać poparcie dla sankcji i wsparcia wojskowego wobec Ukrainy.

To sprawia, że Agencja Projektów Społecznych jest uznawana dziś za narzędzie wojny hybrydowej i informacyjnej Federacji Rosyjskiej – część systemu oddziaływania, który uzupełnia operacje militarne.

Agencja Projektów Społecznych działa na granicy technologii, komunikacji i propagandy, wykorzystuje nowoczesne narzędzia internetowe (fałszywe portale, social media), operuje w wielu językach i targetuje różne grupy społeczne. Jej działalność pokazuje, że walkę o narrację społeczną

i polityczną prowadzi się dziś równolegle do działań militarnych i jest to część szerszej konfrontacji o wpływy polityczne, społeczne i kulturowe.

Najbardziej rozpoznawalną i najlepiej udokumentowaną operacją realizowaną przez SDA jest kampania „Doppelgänger" (Sobowtór). Mechanizm ten opiera się na tworzeniu precyzyjnych kopii (klonów) witryn internetowych renomowanych mediów oraz instytucji państwowych.

Działalność SDA nie jest chaotyczna, opiera się na głębokiej analizie nastrojów społecznych w państwach docelowych. Główne wektory narracyjne obejmują:

- podsycanie sporów między USA a Europą w kwestiach bezpieczeństwa;
- wzmacnianie polaryzacji wewnętrznej, wykorzystywanie tematów wrażliwych (migracja, inflacja, prawa mniejszości) do skłócania grup społecznych w Niemczech, Francji i Polsce;
- delegitymizację pomocy dla Ukrainy: przedstawianie wsparcia militarnego jako czynnika przedłużającego konflikt i zagrażającego bezpieczeństwu obywateli Zachodu;
- zasypywanie zachodnich redakcji i organizacji factcheckingowych prośbami o zweryfikowanie fałszywych informacji, co w rzeczywistości służy marnowaniu ich zasobów i testowaniu sprawności systemów weryfikacji (operacja „Matrioszka").

SDA wyróżnia się na tle tradycyjnych struktur dezinformacyjnych (jak np. petersburska „farma trolli" Prigożyna) wysokim stopniem technicyzacji. Wycieki wewnętrznych dokumentów agencji ujawniły:

1. Systemy monitoringu w czasie rzeczywistym: wykorzystanie narzędzi do analizy sentymentu w mediach społecznościowych w celu identyfikacji „punktów zapalnych", które można wykorzystać w kampanii informacyjnej.
2. Generowanie treści multimedialnych: tworzenie profesjonalnie wyglądających memów, infografik oraz deepfake'ów, które mają wyższy potencjał wiralowy niż suchy tekst.
3. Personalizacja przekazu: tworzenie różnych wariantów tej samej dezinformacji dostosowanych do konkretnych grup demograficznych (np. inne argumenty dla rolników, studentów itp.).

Skuteczność SDA doprowadziła do bezprecedensowej mobilizacji służb wywiadowczych i organizacji zajmujących się cyberbezpieczeństwem. 28 lipca 2023 r. Agencja Projektów Społecznych została oficjalnie wpisana na listę sankcyjną Rady UE jako podmiot prowadzący działania podważające integralność terytorialną Ukrainy i wspierające narracje Kremla. Decyzja ta podkreśliła, że organizacja aktywnie wspiera rosyjską wojnę informacyjną oraz jest powiązana z władzami Federacji Rosyjskiej. Podstawami prawnymi sankcji są rozporządzenie wykonawcze Rady UE 2023/1563 i decyzje 2023–1566 dotyczące działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy, wpisujące agencję jako podmiot przyczyniający się do destabilizacji debaty politycznej w państwach UE w związku z wojną oraz działający w sposób wspierający rosyjską strategię propagandową. Włączenie jej na listy sankcyjne oznacza, że europejskie instytucje uznały jej działania za zagrożenie dla bezpieczeństwa informacyjnego i politycznego regionu.

Podobne działania sankcyjne wobec Agencji Projektów Społecznych podjęły także we wrześniu 2024 r. władze USA, uznając jej rolę w wojnie informacyjnej za część większego rosyjskiego aparatu propagandowego. Departament Sprawiedliwości USA opublikował również obszerne akta (tzw. SDA Leaks), ujawniając tysiące stron wewnętrznej korespondencji, budżety oraz listy płac agencji, co stanowi najdokładniejszy w historii wgląd w funkcjonowanie rosyjskich struktur dezinformacyjnych.

Agencja znajduje się również na brytyjskich listach sankcyjnych jako involved person (osoba zaangażowana), co oznacza, że uznano ją za organizację wspierającą strategicznie działania Rosji, zwłaszcza w sektorze technologii informacyjnych i komunikacji. Kanada i Australia przyłączyły się do potępienia nieuczciwych działań SDA na całym świecie.

Działalność SDA stanowi paradygmatyczny przykład ewoluującego zagrożenia hybrydowego. Wyciągnięte wnioski wskazują na konieczność:

1. Zwiększenia odporności cyfrowej (*resilience*): edukacja medialna społeczeństwa pozostaje jedyną długofalową obroną przed technikami „Doppelgängera".
2. Współpracy publiczno-prywatnej: rządy muszą ściślej współpracować z gigantami technologicznymi w celu szybszego wykrywania i usuwania infrastruktur dezinformacyjnych.

3. Aktywnej komunikacji strategicznej: państwa demokratyczne nie mogą ograniczać się do reaktywnego fact-checkingu, lecz muszą tworzyć własne atrakcyjne narracje oparte na prawdzie.

SDA to agencja dysponująca znacznym budżetem, z profesjonalną kadrą podzieloną na zespoły z konkretnymi zadaniami. Wyłaniający się obraz przypomina nowoczesną agencję PR. Jest zaangażowana praktycznie w większość operacji informacyjnych prowadzonych przez Kreml i stanowi element ekosystemu, w skład którego wchodzą inne grupy i organizacje.

Olga Wasiuta

A. Kozłowski, *#CyberMagazyn: Social Design Agency – rosyjska fabryka trolli na sterydach*, 15.11.2025, https://cyberdefence24.pl/armia-i-sluzby/cybermagazyn-social-design-agency-rosyjska-fabryka-trolli-na-sterydach (dostęp 14.01.2026); M. Laine, A. Morozova, *Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections*, 16.09.2024, https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/ (dostęp 12.01.2026); *Media o wycieku wewnętrznych dokumentów. Pokazują, jak działa machina propagandowa Kremla*, 18.09.2024, https://tvn24.pl/swiat/rosja-wyciekly-dokumenty-agencji-projektowania-spolecznego-odpowiada-za-kampanie-dezinformacyjne-kremla-st8095662?utm_source=chatgpt.com (dostęp 12.01.2026); *Sanctions List Search*, https://sanctionssearch.ofac.treas.gov/Details.aspx?id=45230 (dostęp 13.01.2026); M. Sieradzka, *Rosyjskie fake newsy mają osłabić spójność Zachodu*, 12.02.2024, https://www.dw.com/pl/niemieckie-media-wyciek%C5%82y-dokumenty-putinowskiej-fabryki-k%C5%82amstw/a-70237252 (dostęp 13.01.2026); Social Design Agency, https://socialdesignagency.com/ (dostęp 12.01.2026); *UK sanctions Putin's interference actors*, 28.10.2024, https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors (dostęp 14.01.2026); A. Windyk, *Niemieckie media: wyciek z putinowskiej „fabryki kłamstw", 17.09.2024,* https://www.dw.com/pl/niemieckie-media-wyciek%C5%82y-dokumenty-putinowskiej-fabryki-k%C5%82amstw/a-70237252 (dostęp 12.01.2026).

AGENCJA UNII EUROPEJSKIEJ DS. NARKOTYKÓW (ang. The European Union Drugs Agency, EUDA). Podczas posiedzenia Rady Europejskiej w Luksemburgu w dniach 28–29 czerwca 1991 r. podjęto decyzję o utworzeniu Europejskiego Centrum Monitorowania Narkotyków. Instytucja ta, funkcjonująca pod nazwą Europejskie Centrum Monitorowania Narkotyków i Narkomanii (ang. European Monitoring Centre for Drugs

and Drug Addiction, EMCDDA), została formalnie powołana na mocy rozporządzenia Rady (EWG) nr 302/93 z dnia 8 lutego 1993 r., które następnie przekształcono Rozporządzeniem (WE) nr 1920/2006 Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. w sprawie Europejskiego Centrum Monitorowania Narkotyków i Narkomanii. EMCDDA utworzono w celu gromadzenia, analizowania i przekazywania Unii Europejskiej, państwom członkowskim oraz uczestniczącym krajom trzecim rzetelnych, obiektywnych, wiarygodnych i porównywalnych informacji dotyczących narkotyków, uzależnień od nich oraz ich konsekwencji w skali europejskiej. Działalność EMCDDA koncentrowała się na zapewnieniu całościowego rozeznania w tym obszarze, wspierającego świadome kształtowanie polityk publicznych oraz ukierunkowywanie inicjatyw służących przeciwdziałaniu temu zjawisku. Mimo że zasadniczy cel rozporządzenia (WE) nr 1920/2006 pozostawał aktualny, z czasem przestał zapewniać adekwatne ramy do skutecznego reagowania na wyzwania związane z problemem narkotyków. W związku z tym konieczne było dokonanie przeglądu mandatu EMCDDA, w tym jego zastąpienie nowymi rozwiązaniami oraz wzmocnienie zakresu działań. Na mocy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1322 z dnia 27 czerwca 2023 r. w sprawie Agencji Unii Europejskiej ds. Narkotyków (EUDA) i uchylenia rozporządzenia (UE) nr 1920/2006 ustanowiono Agencję Unii Europejskiej ds. Narkotyków (ang. European Union Drugs Agency, EUDA), która zastąpiła EMCDDA i stała jego następcą prawnym.

EUDA z siedzibą w Lizbonie stanowi jednostkę organizacyjną UE i posiada osobowość prawną. Na terytorium każdego państwa członkowskiego dysponuje pełną zdolnością prawną oraz zdolnością do czynności prawnych w zakresie najszerszym przewidzianym przez prawo krajowe dla osób prawnych. W szczególności jest uprawniona do nabywania i zbywania mienia ruchomego i nieruchomego, a także występowania jako strona w postępowaniach sądowych. Agencja ma za zadanie:

- zapewnianie UE i państwom członkowskim rzetelnych, obiektywnych i porównywalnych informacji, wczesnego ostrzegania oraz ocen zagrożeń dotyczących narkotyków, ich używania i uzależnień, obejmujących profilaktykę, leczenie, opiekę,

redukcję szkód, rehabilitację, reintegrację społeczną oraz rynki i podaż narkotyków, w tym nielegalną produkcję i handel;
- opracowywanie opartych na dowodach konkretnych zaleceń dotyczących skutecznego i terminowego reagowania na wyzwania związane z narkotykami, ich używaniem i uzależnieniami we wskazanych obszarach;
- wykonywanie zadań z poszanowaniem praw podstawowych i przepisów o ochronie danych, przy zastosowaniu zintegrowanego, zrównoważonego i multidyscyplinarnego podejścia, uwzględniającego prawa człowieka, równość, zdrowie oraz aspekty społeczne.

EUDA ustanawia i koordynuje Europejską Sieć Informacji o Narkotykach i Narkomanii, tj. sieć REITOX, tworzy i zarządza europejskim systemem szybkiego powiadamiania dotyczącego narkotyków, a także ustanawia sieć laboratoriów kryminalistycznych i toksykologicznych zajmujących się badaniami nt. narkotyków oraz szkód wywołanych ich używaniem.

Sieć REITOX składa się z ośrodków krajowych, które pełnią funkcję łączników między państwami uczestniczącymi a EUDA oraz wspierają interakcje w kontaktach z Agencją, przyczyniając się do skoordynowanego działania Unii. Na poziomie krajowym ośrodki koordynują gromadzenie, monitorowanie, analizowanie i przekazywanie EUDA danych oraz informacji dotyczących narkotyków i ich używania, w tym nowych tendencji, określonych substancji psychoaktywnych i systemu wczesnego ostrzegania, a także wspierają rozwój źródeł danych epidemiologicznych i działania *ad hoc* w związku z nowymi zagrożeniami. Współpracują z właściwymi organami, ekspertami i zainteresowanymi stronami, stosują uzgodnione protokoły i standardy, zapewniają jakość i porównywalność danych, sporządzają roczne sprawozdania ze swojej działalności oraz uwzględniają aspekt płci w obszarze polityki narkotykowej przy jednoczesnym nieprzekazywaniu danych umożliwiających identyfikację osób.

Europejski system szybkiego powiadamiania dotyczący narkotyków uzupełnia krajowe systemy powiadamiania oraz wczesnego ostrzegania w odniesieniu do nowych substancji psychoaktywnych. Służy natychmiastowemu przekazywaniu EUDA – przez ośrodki krajowe we współpracy

z właściwymi organami krajowymi – informacji o poważnych bezpośrednich lub pośrednich zagrożeniach związanych z narkotykami dla zdrowia, wymiaru społecznego lub bezpieczeństwa. EUDA analizuje i ocenia otrzymane informacje, uzupełnia je danymi naukowymi i technicznymi pochodzącymi m.in. z systemu wczesnego ostrzegania, innych ocen zagrożeń, źródeł otwartych oraz pozyskanymi od właściwych organów i organizacji międzynarodowych, a następnie przekazuje ukierunkowane, szybkie powiadomienia o zagrożeniu odpowiednim organom krajowym. System obejmuje dalszą wymianę informacji o podjętych działaniach, ścisłą współpracę Agencji z Komisją i państwami członkowskimi, możliwość udziału państw trzecich lub organizacji międzynarodowych na zasadzie wzajemności oraz, w razie potrzeby, przekazywanie informacji o szczególnych zagrożeniach osobom używającym lub potencjalnie używającym narkotyków, przy jednoczesnej aktualizacji powiadomień.

Sieć laboratoriów kryminalistycznych i toksykologicznych działa jako forum generowania danych oraz wymiany informacji nt. zmian i tendencji. Organizuje również szkolenia w celu podnoszenia kompetencji ekspertów w dziedzinie narkotyków i toksykologii. Wspiera wdrażanie programów zapewniania jakości oraz dalszą harmonizację metod gromadzenia danych i analitycznych, zapewniając jednocześnie EUDA dostęp do danych kryminalistycznych i toksykologicznych wytwarzanych lub gromadzonych przez laboratoria, w tym do celów analizy nowych substancji psychoaktywnych. Sieć współpracuje z innymi podmiotami i organizacjami, unika powielania działań, przekazuje informacje o swojej pracy ośrodkom krajowym i sieci REITOX. Jej działalność jest koordynowana przez EUDA, która zwołuje posiedzenia, wskazuje i finansuje konkretne projekty oraz tworzy bazę danych do przechowywania i udostępniania informacji.

W skład struktury administracyjno-kierowniczej EUDA wchodzą:

– zarząd, który m.in. wyznacza strategiczne kierunki działania Agencji oraz przyjmuje kluczowe dokumenty planistyczne, budżetowe i sprawozdawcze, w tym jednolity dokument programowy, roczny budżet oraz skonsolidowane roczne sprawozdanie z działalności. Pełni funkcje nadzorcze i regulacyjne, przyjmując m.in. zasady finansowe, strategie dotyczące zwalczania nadużyć finansowych, wydajności, komunikacji, współpracy

międzynarodowej, zapobiegania konfliktom interesów oraz zapewniając działania następcze po audytach i ocenach. Wykonuje także kluczowe kompetencje organizacyjne i kadrowe, w tym powołuje dyrektora wykonawczego, księgowego i członków komitetu naukowego, decyduje o strukturze wewnętrznej Agencji oraz sprawuje lub deleguje uprawnienia organu powołującego wobec personelu;

– rada wykonawcza podejmująca decyzje w sprawach finansowych przewidzianych w zasadach finansowych, które nie zostały zastrzeżone dla zarządu, oraz zapewniająca działania następcze w odniesieniu do ustaleń i zaleceń wynikających z audytów, ocen oraz dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych i Prokuraturę Europejską. Monitoruje i nadzoruje wykonywanie decyzji zarządu w celu wzmocnienia kontroli nad zarządzaniem administracyjnym i budżetowym, bez uszczerbku dla obowiązków dyrektora wykonawczego. W sytuacjach pilnych może podejmować decyzje tymczasowe w imieniu zarządu, w szczególności w zakresie zarządzania administracyjnego oraz kwestii budżetowych, na warunkach określonych w regulaminie wewnętrznym zarządu;
– dyrektor wykonawczy odpowiedzialny za zarządzanie EUDA, bieżące kierowanie jej pracami oraz realizację zadań szczególnych, działający niezależnie w wykonywaniu swoich obowiązków i ponoszący odpowiedzialność przed zarządem. Dyrektor przygotowuje i wykonuje decyzje zarządu, opracowuje oraz wdraża jednolity dokument programowy, sporządza skonsolidowane roczne sprawozdanie z działalności, a także przygotowuje projekty dokumentów finansowych i wykonuje budżet Agencji. Reprezentuje EUDA na zewnątrz, chroni interesy finansowe Unii poprzez zapobieganie nadużyciom oraz realizuje działania następcze po audytach i dochodzeniach, a na wezwanie Parlamentu Europejskiego lub Rady przedstawia sprawozdania i uczestniczy w ich posiedzeniach;
– komitet naukowy, który wydaje opinie w przypadkach przewidzianych w rozporządzeniu 2023/1322 oraz w sprawach

wszelkich kwestii naukowych dotyczących działalności Agencji, które mogą zostać mu przedłożone przez zarząd lub dyrektora wykonawczego. Do celów oceny zagrożeń stwarzanych przez nowe substancje psychoaktywne lub ich grupy komitet może zostać rozszerzony o dodatkowych ekspertów z odpowiednich dziedzin nauki, powoływanych przez dyrektora wykonawczego spośród listy zatwierdzonej przez zarząd;

– sieć REITOX, za pośrednictwem której państwa członkowskie przyczyniają się do realizacji zadania Agencji dotyczącego gromadzenia i przedkładania spójnych i ujednoliconych informacji dotyczących zjawiska narkotyków w całej Unii.

Założenia programowe EUDA na lata 2025–2027 opierają się 4 głównych wymiarach strategicznych, tj. przewidywanie, alarmowanie, reagowanie, uczenie się.

W obszarze współpracy międzynarodowej EUDA realizuje następujące cele strategiczne:

– śledzenie i analizowanie globalnych tendencji w obszarze narkotyków, które mogą stwarzać zagrożenia lub wywoływać skutki dla UE;
– zacieśnianie współpracy z partnerami międzynarodowymi, unijnymi oraz innymi interesariuszami w odniesieniu do zagrożeń narkotykowych pojawiających się poza UE, a oddziałujących na systemy ochrony zdrowia, sferę społeczną i bezpieczeństwo w Unii;
– wspomaganie wymiany doświadczeń, najlepszych praktyk oraz możliwych do zastosowania rezultatów badań na arenie międzynarodowej;
– rozwijanie współpracy technicznej z partnerami i interesariuszami międzynarodowymi oraz wspieranie włączania kluczowych danych unijnych do międzynarodowych mechanizmów monitorowania i zwalczania zjawiska narkotyków.

EUDA współpracuje m.in. z Europolem, Agencją UE ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust), Agencją Praw Podstawowych UE, Agencją UE ds. Szkolenia w Dziedzinie Ścigania, Europejską Agencją Leków, Europejską Służbą Działań Zewnętrznych

i delegaturami UE, Europejskim Centrum ds. Zapobiegania i Kontroli Chorób, Europejską Fundacją na rzecz Poprawy Warunków Życia i Pracy (Eurofound), Grupą Pompidou (szczególnie w dziedzinie epidemiologii), Biurem Narodów Zjednoczonych ds. Narkotyków i Przestępczości, Światową Organizacją Celną, Światową Organizacją Zdrowia, Wspólnym Programem Narodów Zjednoczonych ds. HIV i AIDS, Radą Gospodarczą i Społeczną ONZ oraz Międzynarodowym Organem Kontroli Środków Odurzających, a także ze środowiskiem naukowym i organizacjami społeczeństwa obywatelskiego. EUDA współpracuje również z krajami kandydującymi i potencjalne kandydującymi do Unii Europejskiej, objętymi Europejską Polityką Sąsiedztwa (EPS) oraz innymi państwami trzecimi na podstawie umów bilateralnych lub projektów międzynarodowych.

Współpraca z państwami w ramach rozszerzenia UE (kraje kandydujące: Albania, Bośnia i Hercegowina, Gruzja, Kosowo, Mołdawia, Czarnogóra, Macedonia Północna, Serbia, Turcja, Ukraina – stan na styczeń 2026) ukierunkowana jest na wsparcie procesu akcesyjnego oraz rozwijanie zdolności krajowych do dostosowania się do standardów UE oraz przygotowanie do udziału w pracach EUDA. Odbywa się w ramach IPA (ang. Instrument for Pre-accession Assistance), tj. projektu współpracy technicznej finansowanego z Instrumentu Pomocy Przedakcesyjnej Komisji Europejskiej. Obecna edycja IPA8 realizowana jest w latach 2023–2026, a beneficjentami są Albania, Bośnia i Hercegowina, Macedonia Północna, Kosowo, Czarnogóra i Serbia. Projekt wspomaga państwa Bałkanów Zachodnich w adaptacji najlepszych unijnych praktyk i rozwiązań w obszarze zdrowia i bezpieczeństwa, a także umacnianiu strategicznej i operacyjnej współpracy zarówno w regionie, jak i z UE w zakresie monitorowania narkotyków i obiegu informacji o nich, z wykorzystaniem unijnych norm i narzędzi. Jego celem jest przede wszystkim podniesienie jakości i dostępności informacji nt. zagrożeń związanych z narkotykami, wsparcie partnerów w opracowywaniu adekwatnych mechanizmów reagowania, w tym tworzenia krajowych obserwatoriów narkotykowych i systemów wczesnego ostrzegania, sprzyjanie wdrażaniu dorobku prawnego UE w obszarze informacji o narkotykach, przy budżecie projektu wynoszącym 1,5 mln euro.

Wsparcie w monitorowaniu problemu narkotykowego i wzmocnienie współpracy oraz pogłębienie wymiany wiedzy eksperckiej z państwami obszaru EPS odbywa się w ramach projektu EU4MD (ang. EU4Monitoring Drugs), realizowanego w latach 2019–2022 (EU4MD I) i 2023–2027 (EU4MD II). Beneficjentami są Algieria, Armenia, Azerbejdżan, Izrael, Jordania, Liban, Libia, Mołdawia, Maroko, Tunezja, Ukraina, Palestyna, współpraca z Białorusią i Gruzją została natomiast zawieszona. Obecny EU4MD II zakłada wzmocnienie wiedzy technicznej i potencjału partnerów poprzez rozwój nowoczesnych systemów monitorowania i reagowania na zjawisko narkotyków, a także zwiększenie zdolności gromadzenia i wymiany danych do wspólnych analiz strategicznych dotyczących nowych trendów i zagrożeń. Istotnym elementem programu jest konsolidacja krajowych systemów monitorowania narkotyków, realizowana poprzez strukturalne wsparcie krajowych obserwatoriów narkotykowych lub wsparcie decydentów krajowych w pracach nad tymi systemami, przy jednoczesnym nacisku na *networking*, partnerstwo i wymianę wiedzy między partnerami EPS a państwami członkowskimi UE. Obejmuje szeroki zakres działań, takich jak integracja partnerów w sieciach UE, rozwój badań ankietowych i monitoringu zdrowotnego oraz bezpieczeństwa, wymiana informacji o nowych substancjach psychoaktywnych, szkolenia i stypendia, przy całkowitym budżecie projektu wynoszącym 4 mln euro.

Od 2011 r. EUDA jest zaangażowana w Program współpracy między Ameryką Łacińską, Karaibami a Unią Europejską w zakresie polityki narkotykowej (ang. Cooperation Programme between Latin America, the Caribbean and the European Union on Drug Policies, COPOLAD), realizując zadania na rzecz wsparcia krajowych obserwatoriów narkotykowych oraz dialogów między UE a partnerami programu. W ramach COPOLAD III EUDA kontynuuje to zaangażowanie, opierając się na doświadczeniach zdobytych podczas realizacji wcześniejszych edycji projektu, tj. COPOLAD I (2011–2015) i COPOLAD II (2016–2020), jako partner współpracujący z Międzynarodową Fundacją Iberoamerykańską na rzecz Polityk Publicznych i Administracji (ang. International Ibero-American Foundation for Public Policies and Administrations, FIIAPP), Międzynarodową Organizacją Włosko-Latynoamerykańską (wł. Organizzazione Internazionale Italo-Latino Americana, IILA) oraz Niemieckim

Towarzystwem Współpracy Międzynarodowej (niem. Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH, GIZ). Trzecia edycja COPOLAD ukierunkowana jest na wzmocnienie zdolności technicznych i znaczenia instytucjonalnego krajowych obserwatoriów narkotykowych, podniesienie spójności, jakości i oparcia na dowodach polityk ograniczania popytu na narkotyki, zwiększenie liczby państw z tego obszaru wdrażających oparte na dowodach strategie ograniczania podaży narkotyków, uwzględniających prawa człowieka, perspektywę płci, włączenie społeczne, zrównoważony rozwój i bezpieczeństwo publiczne. W lipcu 2022 r. EUDA zawarła umowę grantową z IILA mającą na celu wsparcie działań państw Ameryki Łacińskiej i Karaibów poprzez wzmocnienie gromadzenia danych, rozwój polityk opartych na dowodach oraz badań naukowych.

Agencja współpracuje również z Morskim Centrum Analiz i Operacji w celu zwalczania nielegalnego handlu narkotykami drogą morską i powietrzną (ang. Maritime Analysis and Operations Centre (Narcotics), MAOC (N)). Jest to inicjatywa 8 państw członkowskich UE (Belgii, Francji, Niemiec, Irlandii, Włoch, Hiszpanii, Holandii i Portugalii) oraz Wielkiej Brytanii, współfinansowana ze środków Funduszu Bezpieczeństwa Wewnętrznego UE, służąca usprawnianiu wymiany informacji wywiadowczych oraz koordynacji działań służb egzekwowania prawa na pełnym morzu w celu przechwytywania statków przewożących kokainę i marihuanę, z udziałem marynarki wojennej i organów ścigania, przy wiodącej roli tych ostatnich w realizacji operacji. Współpraca EUDA i MAOC (N) koncentruje się na planach ograniczania podaży narkotyków, w tym opracowania kluczowych jej wskaźników. Od września 2010 r. EUDA uczestniczy w posiedzeniach zarządu wykonawczego MAOC (N) w charakterze obserwatora.

W 1995 r. EUDA rozpoczęła współdziałanie z Europejskim programem badań ankietowych w szkołach nt. alkoholu i innych narkotyków (ang. European School Survey Project on Alcohol and Other Drugs, ESPAD), sformalizowanym w 2007 r. poprzez uzgodnione ramy współpracy. W 2011 r. przyjęto wspólne oświadczenie, w którym strony zobowiązały się do opracowania usprawnionej, w tym wielojęzycznej, strategii upowszechniania wyników ESPAD, współpracy na rzecz harmonizacji

i rozwoju metodologicznego, przygotowania wspólnego programu prac sprzyjającego długoterminowej stabilności sieci ESPAD oraz regularnych spotkań poświęconych wspólnym inicjatywom. W 2015 r. rząd Szwecji zakończył międzynarodową koordynację ESPAD, uznając EUDA za naturalne centrum tej działalności. W 2016 r. EUDA sporządziła raport ESPAD za rok 2015, opracowując jednocześnie część strony internetowej ESPAD.

EUDA współpracuje również m.in. z Kirgistanem w ramach Programu działań antynarkotykowych w Azji Środkowej (ang. Central Asian Drug Action Programme, CADAP). W latach 2021–2023 realizowała projekt EMCDDA4GE będący częścią szerszego programu UE4 „Bezpieczeństwo, rozliczalność i walka z przestępczością w Gruzji", który ukierunkowano na pomoc państwu w udoskonaleniu reakcji na zagrożenia dla zdrowia i bezpieczeństwa związane z narkotykami. Ponadto w 2026 r. EUDA przewodniczy Sieci Agencji UE ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (ang. Justice and Home Affairs Agencies' Network, JHAAN), utworzonej w 2010 r. w celu połączenia agencji wdrażających politykę UE w obszarze wolności, bezpieczeństwa i sprawiedliwości. W skład JHAAN wchodzą CEPOL, EIGE, EUAA, EUDA, eu-LISA, Eurojust, Europol, FRA, Frontex.

Klaudia Cenda-Miedzińska

European Monitoring Centre for Drugs and Drug Addiction, *Single Programming Document 2024–2026*, EMCDDA; European Union Drugs Agency, *EUDA International Operation Framework. Acting today, anticipating tommorow*, EUDA 2024; European Union Drugs Agency, https://www.euda.europa.eu/index_en (dostęp 24.01.2026); European Union Drugs Agency, *Single Programming Document 2025–2027*, EUDA; Rozporządzenie (WE) nr 1920/2006 Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. w sprawie Europejskiego Centrum Monitorowania Narkotyków i Narkomanii (wersja przekształcona), Dz.U. L 376, s. 1–13; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1322 z dnia 27 czerwca 2023 r. w sprawie Agencji Unii Europejskiej ds. Narkotyków (EUDA) i uchylenia rozporządzenia (UE) nr 1920/2006, Dz.U. L 166 z, s. 6–47.

AI LITERACY (kompetencje AI, kompetencje w zakresie AI, kompetencje w zakresie sztucznej inteligencji/SI) – zestaw kompetencji umożliwiających korzystanie z narzędzi AI oraz rozumienie ich działania, ocenę jakości

wygenerowanych wyników i krytyczne podejście do ich zastosowania. Termin ten obejmuje umiejętności pozwalające na świadome, odpowiedzialne i bezpieczne używanie systemów opartych na sztucznej inteligencji – zarówno w życiu zawodowym, jak i prywatnym.

AI literacy to pojęcie obejmujące wiedzę o tym, czym jest sztuczna inteligencja, jak działają algorytmy i modele generatywne oraz jak analizować i oceniać rezultaty ich działania. Według literatury przedmiotu rozwój tych umiejętności można rozłożyć na cztery główne obszary:

1. Znajomość i rozumienie podstawowych pojęć – co to jest AI, jak uczy się model, jaka jest różnica między AI a zwykłym algorytmem.
2. Umiejętność wykorzystywania narzędzi AI, czyli praktyczne korzystanie z różnych narzędzi.
3. Ocena jakości i interpretacja wyników – jak rozpoznać błędy, błędne wnioski i halucynacje AI.
4. Świadomość etyczna i społeczna – zrozumienie konsekwencji używania AI w różnych obszarach życia człowieka (np. wpływ na prywatność użytkowników, aspekty prawa autorskiego, zmiany na rynku pracy).

Badania wskazują, że zrozumienie działania i wykorzystanie narzędzi AI jest na bardzo różnym poziomie: wiele osób korzysta z nich bez pełnej świadomości, jak one działają, co może tworzyć m.in. ryzyko związane z brakiem analizy jakości treści generowanych przez AI.

W raporcie *2025 AI in Education* podkreślono, że AI już teraz coraz częściej jest wykorzystywana w szkołach na całym świecie, a tematy związane ze sztuczną inteligencją zaczynają pojawiać się w programach nauczania. Coraz więcej nauczycieli korzysta z systemów AI, aby usprawniać przygotowanie lekcji, upraszczać materiały dla uczniów czy oceniać prace i zadania, a jednocześnie część z nich zgłasza brak odpowiednich kompetencji albo obawę przed negatywnymi konsekwencjami tej technologii (np. plagiatami lub oszustwami).

W kontekście szkolnictwa wyższego sytuacja wygląda podobnie: badania przeprowadzone przez różne instytucje pokazują, że większość studentów aktywnie używa narzędzi AI w pracy akademickiej, mimo że często czują się nieprzygotowani do ich właściwego i krytycznego wykorzystania. W raporcie HEPI *Student Generative AI Survey 2025* wskazano,

że ponad 90% respondentów – studentów w Wielkiej Brytanii – deklaruje korzystanie z narzędzi AI, ale tylko nieco ponad połowa uważa, że ma wystarczającą wiedzę o AI, aby używać jej w sposób odpowiedzialny. Podobne wnioski można znaleźć w analizach dotyczących studentów w USA i Europie – aż 86–90% respondentów deklaruje używanie AI w procesie nauki, jednak znacząca część z nich zgłasza trudności z rozumieniem, jak systemy generatywne działają i jakie są ich ograniczenia. Co więcej, nawet jeśli studenci intensywnie używają narzędzi AI, wielu z nich zgłasza luki w kompetencjach, które można przypisać właśnie brakowi *AI literacy* – na przykład nieumiejętność oceny wiarygodności generowanych treści, rozpoznawania błędów logicznych czy świadomego i etycznego stosowania tych narzędzi w pracy akademickiej.

W literaturze przedmiotu podkreśla się, że pomimo coraz powszechniejszego wykorzystywania narzędzi AI w szkołach, placówki edukacyjne i uczelnie nie nadążają za dynamicznym rozwojem tych technologii. Chodzi nie tylko o to, by uczyć, jak korzystać z narzędzi AI, ale jak rozumieć ich działanie i konsekwencje ich użycia. Wydaje się, że wcześniejsze wprowadzenie *AI literacy* już w szkołach podstawowych może mieć korzystny wpływ na długoterminowe kompetencje informacyjno-cyfrowe uczniów. Pojawiają się propozycje włączenia do edukacji w klasach szkoły podstawowej tematów związanych z AI, które łączyłyby naukę matematyki, logiki z podstawowymi mechanizmami działania sztucznej inteligencji. Również w szkolnictwie wyższym pojawiają się inicjatywy badawcze i dydaktyczne związane z kształceniem kompetencji w tym zakresie.

Kompetencje AI mają również kluczowe znaczenie na rynku pracy. Raporty europejskie podkreślają, że obecnie stawia się na rozwój kompetencji i umiejętności w obszarze sztucznej inteligencji jako jednego z priorytetów polityki cyfrowej. Celem jest zarówno przygotowanie przyszłych ekspertów AI, jak i szerokiego grona pracowników, którzy będą potrafili efektywnie, etycznie i krytycznie wykorzystywać narzędzia oparte na AI. W praktyce oznacza to, że *AI literacy* staje się częścią kompetencji potrzebnych nie tylko programistom, ale również specjalistom z zakresu marketingu, zarządzania czy edukacji – wszędzie tam, gdzie AI zaczyna mieć realne zastosowanie. Inwestowanie w rozwój takich kompetencji wewnątrz organizacji robi się wręcz koniecznością biznesową.

AI literacy to także umiejętność rozumienia konsekwencji społecznych i etycznych użycia sztucznej inteligencji. Obejmuje świadomość potencjalnych uprzedzeń algorytmicznych (wynikających m.in. ze stronniczości danych treningowych), ryzyka związanego z dezinformacją, prywatnością danych i odpowiedzialnym podejściem do automatyzacji. Przy braku takich kompetencji użytkownicy mogą łatwo stać się ofiarami wykorzystania błędnych wyników czy dezinformacji, a decyzje oparte na AI mogą prowadzić do niezamierzonych negatywnych skutków społecznych.

W literaturze przedmiotu podkreśla się, że samo techniczne opanowanie narzędzi nie wystarcza, konieczne jest także zrozumienie etycznych dylematów, które pojawiają się w kontekście AI. Wiedza ta powinna towarzyszyć nauce praktycznego użycia AI i być elementem każdego programu rozwijającego *AI literacy*.

Szczególnie istotnym elementem *AI literacy* jest umiejętność rozpoznawania treści wygenerowanych przez AI i stworzonych przez człowieka. Wraz z rosnącą popularnością generatywnej sztucznej inteligencji, która w znaczący sposób przyspiesza tworzenie różnego rodzaju treści, użytkownicy informacji stają przed coraz większym wyzwaniem związanym z ekspozycją na ogromną liczbę fałszywych tekstów, obrazów i filmów. Biorąc pod uwagę fakt, że wiarygodność takich materiałów jest niepewna, zagrożenia wynikające z napotkania i udostępniania treści generowanych przez AI (AIGC – *AI generated content*), takich jak fałszywe reklamy, kradzież tożsamości, pornografia, propaganda polityczna, dezinformacja czy syntetyczne prace akademickie, są głęboko niepokojące i słusznie rodzą poważne pytania etyczne, zarówno na poziomie indywidualnym, jak i społecznym. Zdolność do skutecznego wykrywania treści AIGC jest zatem nie tylko przydatna, ale wręcz konieczna do poruszania się po coraz bardziej złożonym i zawodnym świecie informacji. W tym kontekście wykrywanie treści generowanych przez AI staje się kluczowym elementem zarówno kompetencji *AI literacy*, jak i ogólnie *information literacy* – dwóch obszarów, które coraz silniej się przenikają, ponieważ sztuczna inteligencja przekształca sposoby dostępu, oceny i tworzenia informacji.

Biorąc pod uwagę znaczące nakładanie się *AI literacy* oraz *media and information literacy* (MIL) – zwłaszcza w obszarach takich jak strategie wyszukiwania, krytyczna ocena oraz odpowiedzialne korzystanie z informacji

– traktowanie *AI literacy* jako części lub naturalnego rozszerzenia *information literacy* jest nie tylko logiczne, ale i konieczne. Związek ten staje się szczególnie widoczny w praktycznych zastosowaniach, takich jak inżynieria promptów, etyczne korzystanie z narzędzi AI oraz ocena treści generowanych przez sztuczną inteligencję. Wszystkie te aspekty mogą być efektywnie rozwijane dzięki dobrze ugruntowanym modelom i standardom *information literacy*. Najnowsze badania wykazały, że kompetencje *AI literacy* można zintegrować zarówno z ACRL Framework for Information Literacy for Higher Education, jak i z innymi modelami, takimi jak Big6 Skills oraz SCONUL Seven Pillars of Information Literacy. W tym świetle wykrywanie treści AIGC nie jest jedynie zadaniem technicznym, lecz krytycznym zaangażowaniem w proces tworzenia autorstwa i znaczenia, czyli fundamentalnych kwestii dla wielu rodzajów kompetencji. Pomimo rosnącego uznania wśród badaczy znaczenia rozwijania kompetencji człowieka w relacji do AI większość obecnych prac dotyczących wykrywania treści AIGC nadal przyjmuje perspektywę technologiczną, czyli koncentruje się bardziej na skuteczności detektorów AI niż zdolnościach oceny samych użytkowników.

Rosnące wykorzystanie AI w edukacji, pracy i codziennym życiu pokazuje, że inwestowanie w kompetencje *AI literacy* jest konieczne i może przynieść wymierne pozytywne efekty. Kluczowe działania obejmują:

- wprowadzanie treści AI do programów nauczania – od szkoły podstawowej po studia, tak aby uczniowie stopniowo rozwijali umiejętności dotyczące mechanizmów AI i ich konsekwencji;
- szkolenia oraz kursy dla nauczycieli i pracowników – aby ci, którzy mają nauczać lub wspierać innych, sami posiadali solidne podstawy wiedzy o AI;
- edukację społeczną i programy pozaformalnej nauki – np. warsztaty, bootcampy czy kursy online, które pomagają dorosłym użytkownikom lepiej zrozumieć technologie AI;
- integrację komponentów etycznych i krytycznych – rozwijanie umiejętności oceniania AI w kontekście uprzedzeń, prywatności czy konsekwencji społecznych.

AI literacy to kluczowa kompetencja XXI w., ponieważ umożliwia nie tylko efektywne korzystanie z narzędzi sztucznej inteligencji, ale również

świadome rozumienie ich działania i odpowiedzialne użycie. W miarę jak AI staje się integralną częścią edukacji, pracy i życia codziennego, rozwijanie takich kompetencji staje się priorytetem zarówno dla systemów edukacyjnych, jak i instytucji publicznych oraz prywatnych. Statystyki pokazują, że choć narzędzia AI są powszechnie używane, znaczna część użytkowników nadal nie posiada pełnej wiedzy o ich ograniczeniach ani potencjalnych zagrożeniach, co zdecydowanie podkreśla pilną potrzebę edukacji w zakresie *AI literacy*.

Paulina Motylińska, Anna Pieczka-Węgorkiewicz

2025 AI in Education Report, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/education/2025-Microsoft-AI-in-Education-Report.pdf (dostęp 15.12.2025); *AI Talent, Skills and Literacy*, https://digital-strategy.ec.europa.eu/pl/policies/ai-talent-skills-and-literacy (dostęp 14.02.2025); M.C. Carrisi, M. Marras, S. Vergallo, *A Structured Unplugged Approach for Foundational AI Literacy in Primary Education*, https://arxiv.org/abs/2505.21398 (dostęp 15.12.2025); M. Kaput, *AI Literacy Education & Training*, https://www.marketingaiinstitute.com/blog/ai-literacy-education-training (dostęp 15.12.2025); R. Kelly, *Survey: 86% of Students Already Use AI in Their Studies*, https://campustechnology.com/articles/2024/08/28/survey-86-of-students-already-use-ai-in-their-studies.aspx (dostęp 14.12.2025); A. Legatt, *90% of College Students Use AI – Higher Ed Needs AI Fluency Support Now*, https://www.forbes.com/sites/avivalegatt/2025/09/18/90-of-college-students-use-ai-higher-ed-needs-ai-fluency-support-now/ (dostęp 15.12.2025); D. Long, B. Magerko, *What is AI Literacy? Competencies and Design Considerations*, „International Journal of Artificial Intelligence in Education" 2020, vol. 30(2), s. 303–314; J. Scott-Branch, R. Laws, P. Terzi, *The intersection of AI, information and digital literacy: Harnessing ChatGPT and other generative tools to enhance teaching and learning*, 2023, https://repository.ifla.org/handle/20.500.14598/2788 (dostęp 10.11.2025); *Student Generative AI Survey 2025*, https://www.hepi.ac.uk/reports/student-generative-ai-survey-2025/ (dostęp 14.02.2025); *Two-Thirds of Higher Education Institutions Have or Are Developing Guidance on AI Use*, https://www.unesco.org/en/articles/unesco-survey-two-thirds-higher-education-institutions-have-or-are-developing-guidance-ai-use (dostęp 14.12.2025); A.M. Warrier, *AI Literacy for Community Colleges: Instructors' Perspectives on Scenario-Based and Interactive Approaches to Teaching AI*, https://arxiv.org/abs/2511.05363 (dostęp 15.12.2025).

AKADEMIA WOJSKOWA STANÓW ZJEDNOCZONYCH W WEST POINT (ang. United States Military Academy at West Point, USMA) – została założona w 1802 r. w West Point, w stanie Nowy Jork, jednakże plan jej utworzenia sięga jeszcze czasów okresu rewolucji amerykańskiej, kiedy to generał George Washington, późniejszy pierwszy prezydent Stanów Zjednoczonych Ameryki, zdecydował w 1778 r., by generał brygady Armii Kontynentalnej w czasie wojny o niepodległość Stanów Zjednoczonych i równocześnie inżynier wojskowy Tadeusz Kościuszko zaprojektował fortyfikacje w West Point. Miejsce to miało się stać jednym z ważniejszych punktów obrony rzeki Hudson i równocześnie wschodniego wybrzeża Stanów Zjednoczonych.

W 1779 r. do West Point została przeniesiona siedziba Washingtona. Już w czasach jego prezydentury (1789–1797) rozważano możliwość ustanowienia tam instytucji, której celem byłoby zarówno kształcenie, jak i prowadzenie badań w zakresie sztuki wojennej, a która przyczyniłaby się do zwiększenia kompetencji żołnierzy i inżynierów wojskowych, niezbędnych dla prawidłowego funkcjonowania armii Stanów Zjednoczonych. Koncepcja ta w tym czasie spotkała się z dezaprobatą ówczesnego sekretarza stanu Thomasa Jeffersona, który jednak, już jako prezydent Stanów Zjednoczonych (1801–1809), uznał, że profesjonalizacja armii jest niezbędna, by młode amerykańskie państwo mogło w przyszłości uniknąć groźby inwazji zewnętrznej na jego terytorium.

Z tego też względu 16 marca 1802 r. prezydent Jefferson podpisał dokument ustanawiający Akademię Wojskową Stanów Zjednoczonych; znalazła się ona pod patronatem Korpusu Inżynierów Armii Stanów Zjednoczonych (U.S. Army Corps of Engineers). Instytucja ta stała się także pierwszą uczelnią inżynieryjną w Stanach Zjednoczonych, a wszyscy jej dowódcy do 1866 r. byli oficerami inżynierii. Oprócz inżynierów wojskowych kształciła również oficerów w piechocie, kawalerii, artylerii i innych rodzajach wojsk armii granicznej. W XIX w. jej absolwenci byli głównie odpowiedzialni za budowę większości nowoczesnych dróg wodnych, infrastruktury, portów, a także Washington Monument, który został wybudowany w parku National Mall w stolicy kraju, tj. Waszyngtonie D.C. Dokonywali oni także pomiarów dla przyszłych transkontynentalnych linii kolejowych w Stanach

Zjednoczonych; zasili także obie armie, tj. Unii i Konfederacji, w trakcie wojny secesyjnej w Stanach Zjednoczonych (1861–1865).

Absolwentem West Point był m.in. dowódca Armii Unii podczas wojny secesyjnej oraz prezydent Stanów Zjednoczonych (1869–1877), generał armii Ulysses Grant. Absolwenci Akademii w West Point należeli do elity inżynieryjnej kraju – jednym z nich był generał dywizji George W. Goethals, kierownik budowy Kanału Panamskiego ukończonego w 1914 r. Do innych znanych absolwentów Akademii w West Point można zaliczyć dowódcę Amerykańskich Sił Ekspedycyjnych generała armii Johna J. Pershinga, który w trakcie I wojny światowej stał na czele ponad 2 mln żołnierzy w Europie, dowódcę armii alianckich na południowo-zachodnim obszarze działań na Pacyfiku w okresie II wojny światowej, dowódcę sił Organizacji Narodów Zjednoczonych (ONZ) w Korei generała armii Douglasa MacArthura, ojca Sił Powietrznych Stanów Zjednoczonych generała sił powietrznych Henry'ego „Hapa" Arnolda, naczelnego dowódcę Alianckich Ekspedycyjnych Sił Zbrojnych w Europie Północno-Zachodniej w trakcie II wojny światowej, a także prezydenta Stanów Zjednoczonych (1953–1961) Dwighta Eisenhowera.

Przez lata program nauczania w Akademii w West Point ewoluował – wiązało się to przede wszystkim z rozwojem nauki i technologii, a także pojawieniem się nowego pokolenia dowódców Akademii. Do tego typu osób można było m.in. zaliczyć już wspomnianego generała armii Douglasa MacArthura, który pełnił tę funkcję w latach 1919–1922. Wprowadził on do Akademii w West Point intensywny program sprawności fizycznej, a także realistyczne szkolenia bojowe.

Na program szkolenia w Akademii miały również wpływ uwarunkowania okresu II wojny światowej. W latach jej trwania 1/3 korpusu kadetów z West Point przeszła szkolenie lotnicze w bazie Stewart Field w Newburgh. Oprócz zmian w zakresie programu nauczania w XX w. doszło również do przeobrażeń w zakresie liczby kadetów Akademii.

W latach 60. XX w. korpus kadetów niemal podwoił swoją liczebność, sięgając 4400. Co ciekawe, ta liczba w zasadzie utrzymuje się na stałym poziomie do czasów współczesnych. Zmiany społeczne spowodowały także nowe podejście Kongresu Stanów Zjednoczonych do kwestii kształcenia kobiet w Akademii w West Point.

W latach 80. XX w. po raz pierwszy w historii tej uczelni absolwentkami zostały 62 kobiety. Od tego czasu zasilają one regularnie szeregi absolwentów West Point, których liczba od momentu założenia tej instytucji wynosi 80 tys. Aby zostać kadetem Akademii w West Point, należy wziąć udział w procedurze rekrutacyjnej, która składa się z kilku etapów. Pierwszym z nich jest spełnienie podstawowych kryteriów rekrutacyjnych, do których zalicza się posiadania obywatelstwa Stanów Zjednoczonych, wiek od 17 do 22 lat, bycie osobą niezamężną oraz nieposiadającą prawnego obowiązku utrzymania dzieci.

Należy jednak zaznaczyć, że chociaż formalnym wymogiem, aby zostać zaliczonym w poczet kadetów West Point, jest posiadanie amerykańskiego obywatelstwa, to jednak co roku przyjmowane są także osoby z innych państw świata. Rocznie stanowią one maksymalną grupę 60 osób. Zrekrutowane osoby mogą wywodzić się z państw uprawnionych do delegowania kadetów, które w każdym roku są określone przez amerykański Departament Stanu oraz Departament Obrony. Ambasady Stanów Zjednoczonych w tych krajach przygotowują pisemne zaproszenie do nominacji, natomiast wyselekcjonowane państwa mogą w procedurze nominacyjnej wziąć pod uwagę jedynie 6 kandydatów pochodzących z danego kraju. Te osoby przechodzą wewnętrzną procedurę rekrutacyjną (w tym zdają egzamin ze znajomości języka angielskiego), gdyż co roku do West Point mogą zostać finalnie przyjęte tylko 3 osoby z danego państwa, zaś te muszą również zapewnić osobom nominowanym, które zostaną przyjęte do West Point, pokrycie kosztów związanych z kształceniem. Każdego roku do West Point z reguły zostaje przyjętych około 15 studentów zagranicznych; przykładowo w 2019 r. w poczet 16 kadetów zagranicznych zostało wcielonych po raz pierwszy w historii dwóch obywateli Polski.

Biorąc pod uwagę fakt, że co roku do West Point zostaje zakwalifikowanych około 1200 kadetów, odsetek obcokrajowców jest niewielki. Wymóg amerykańskiego obywatelstwa jest jedynym kryterium, które nie dotyczy obcokrajowców; pozostałe są identyczne z tymi, które obowiązują kandydatów z obywatelstwem Stanów Zjednoczonych. Należą do nich przystąpienie do testów egzaminacyjnych, takich jak ACT, SAT, CLT, mających zbadać umiejętności przyszłych kadetów w zakresie matematyki, czytania i pisania. Oprócz dobrych wyników z egzaminów przyszli

kadeci muszą się również odznaczać zaangażowaniem w pozaszkolne formy aktywności. Ponadto muszą być zdrowi fizycznie i psychicznie – ich stan zdrowia jest weryfikowany poprzez badania medyczne na terenie Akademii; kandydaci przechodzą również testy sprawności fizycznej. Ich przyjęcie w poczet kadetów jest też uzależnione od otrzymania nominacji, czyli oficjalnego poparcia ze strony rządu Stanów Zjednoczonych lub wojska, potwierdzającego zdolności przywódcze kandydata do West Point.

Nominacji w liczbie do 15 kandydatów na każde wolne miejsce może dokonać zarówno członek Senatu Stanów Zjednoczonych, Izby Reprezentantów Stanów Zjednoczonych, jak też wiceprezydent Stanów Zjednoczonych. Sama procedura rekrutacyjna, jak i dość ostra selekcja kandydatów są związane nie tylko z elitarnym statusem uczelni, lecz również korzyściami podjęcia studiów, do których należy przede wszystkim zaliczyć zwolnienie z opłat za kształcenie, co w praktyce oznacza brak konieczności wzięcia kredytu na rzecz pokrycia kosztów nauki, która na poziomie studiów jest w Stanach Zjednoczonych odpłatna.

Co więcej, z danych statystycznych wynika, że 100% absolwentów West Point znajduje zatrudnienie po ukończeniu Akademii, a ich wynagrodzenie roczne wynosi 70 tys. dolarów. Korzyści wynikające z bycia absolwentem prestiżowej Akademii w West Point są jednak pochodną 4 intensywnych lat nauki oraz szkoleń praktycznych.

W skład Akademii w West Point wschodzi obecnie 13 wydziałów akademickich, tj. Wydział Nauk Behawioralnych i Przywództwa (Behavioral Sciences and Leadership), Wydział Nauk Chemicznych i Biologicznych oraz Inżynierii (Chemical and Biological Science and Engineering), Wydział Inżynierii Lądowej i Środowiskowej (Civil and Environmental Engineering), Wydział Elektrotechniki i Informatyki (Electrical Engineering and Computer Science), Wydział Języka Angielskiego i Języków Świata (English and World Languages), Wydział Geografii i Nauk o Ziemi (Geography and Earth Sciences), Wydział Historii i Studiów o Wojnie (History and War Studies), Wydział Prawa i Filozofii (Law and Philosophy), Wydział Nauk Matematycznych (Mathematical Sciences), Wydział Inżynierii Mechanicznej i Lotniczej (Mechanical and Aerospace Engineering), Wydział Fizyki i Inżynierii Jądrowej (Physics and Nuclear Engineering), Wydział Nauk Społecznych (Social Sciences), Wydział

Inżynierii Systemów (Systems Engineering), oraz 2 wydziały wojskowe: Wydział Szkoleń Wojskowych (Military Instructions) i Wydział Wychowania Fizycznego (Physical Education). Oferują one bogaty program zarówno kształcenia teoretycznego, jak i praktycznego, w tym rozmaitego typu szkolenia i treningi wojskowe oraz zawody na poligonach.

Na poligonie odbywa się szkolenie podstawowe (Cadet Basic Training, CBT), odwzorowujące realne pole walki; wykorzystuje się zatem granaty dymne i hukowe oraz amunicję ćwiczebną. Mają miejsce również szkolenia strzeleckie z wykorzystaniem granatników podwieszanych oraz przeciwpancernych AT-4, a także obejmujące nawigację terenową, wspinaczkę górską, pomoc przedmedyczną i taktykę. Oprócz szkolenia podstawowego kadeci poświęcają na szkolenia wojskowe kilka sobót w danym semestrze studiów oraz wolny czas podczas przerw wakacyjnych: wówczas uczestniczą w intensywnych szkoleniach, które obejmują m.in. obsługę dział artyleryjskich, zaawansowaną nawigację terenową czy wodny tor przeszkód.

Na pierwszym roku studiów wszystkich kadetów obowiązują przedmioty podstawowe, tj. matematyka, fizyka, chemia, język angielski, psychologia, język obcy oraz historia. Dopiero na drugim roku nauki odbywa się wybór kierunku, od którego są uzależnione przedmioty obowiązkowe. Co ciekawe, studia na West Point można podejmować także na kierunkach humanistycznych. W trakcie studiów kadeci uczestniczą w bogatych programach praktyk, mogą również ukończyć liczne kursy, np. spadochronowe czy płetwonurkowe; uczelnia zapewnia ponadto szkolenia językowe i zajęcia sportowe. Dopiero po opuszczeniu murów Akademii absolwenci, którzy uzyskują tytuł inżyniera (amerykański Bachelor of Science) oraz stopień podporucznika (amerykański *second lieutenant*), odbywają specjalizację w centrach szkolenia, gdzie zdobywają wiedzę specjalistyczną związaną z rodzajem wojsk, w których będą służyć. Uczelnia z założenia ma być kuźnią przyszłych oficerów – liderów, zatem kładzie duży nacisk na naukę dowodzenia i przywództwa w praktyce. W składzie każdej uczelnianej kampanii znajdują się kadeci z różnych roczników – to w praktyce umożliwia im naukę dowodzenia, gdyż na początku starsi kadeci dowodzą kolegami z pierwszego roku, a następnie stają się oni dowódcami plutonów i kompanii.

Niektórzy kadeci mogą nawet uzyskać stanowisko dowódcy batalionów i pułków, dzięki czemu odpowiadają oni za każdy szczebel dowodzenia. W West Point duży nacisk kładzie się również na metodę aktywnej nauki, tj. Thayer Method, co oznacza w praktyce, że studenci biorą pełną odpowiedzialność za swoje postępy w nauce. Tym samym dostają dość sporo zadań domowych, a także angażują się w projekty grupowe, co powoduje, że studia w West Point cechuje dość duża indywidualizacja.

Paulina Szeląg

Athletics, https://www.westpoint.edu/athletics (dostęp 8.12.2025); *Brief History of West Point*, https://www.westpoint.edu/about/history-of-west-point/brief-history-of-west-point (dostęp 8.12.2025); *Być kadetem West Point*, 1.01.2019, https://polska-zbrojna.pl/home/articleshow/27175(dostęp 8.12.2025); *Cadet Journey*, https://www.westpoint.edu/cadet-journey (dostęp 8.12.2025); *Departments,* https://www.westpoint.edu/academics/departments (dostęp 8.12.2025); *Get Inspired*, https://www.westpoint.edu/admissions (dostęp 8.12.2025); *Military Training*, https://www.westpoint.edu/military-education/military-training (dostęp 8.12.2025); *Notable Graduates*, https://www.westpoint.edu/about/history-of-west-point/notable-graduates (dostęp 8.12.2025); L. Pastusiak, *Prezydenci Stanów Zjednoczonych Ameryki Północnej*, Wydawnictwo Bellona, Warszawa 1999; Sierż. pchor. Bartłomiej Grzybowski o studiach w West Point w wywiadzie dla „Polski Zbrojnej", https://www.wojsko-polskie.pl/wat/articles/aktualnosci-w/sierz-pchor-bartlomiej-grzybowski-o-studiach-w-west-point-w-wywiadzie-dla-polski-zbrojnej/ (dostęp 8.12.2025); *Steps to Admission at USMA*, https://www.westpoint.edu/admissions/steps-to-admission (dostęp 8.12.2025); *Student WAT w drodze do West Point*, https://www.wojsko-polskie.pl/wat/articles/aktualnosci-w/student-wat-w-drodze-do-west-point/ (dostęp 8.12.2025); *USMA Academic Program*, https://catalog.westpoint.edu/ (dostęp 8.12.2025).

AKULTURACJA (ang. *acculturation*) – termin, który ma zastosowanie w różnych naukach społecznych i o zarządzaniu (m.in. antropologii, etnologii, pedagogice, psychologii, socjologii, zarzadzaniu międzykulturowym), określający zmianę czy też wymianę kulturową, zjawisko, do którego dochodzi w momencie kontaktu z odmiennym systemem kulturowym, w procesie ciągłego i bezpośredniego konfrontowania się dwóch różnych systemów. Według klasycznego ujęcia ta konfrontacja prowadzi do jakościowych i wieloaspektowych zmian i przekształceń

„w pierwotnych wzorach kulturowych jednej lub obu grup" (Redfield, Linton, Herskovits 1936).

Jak podaje *Encyklopedia Britannica*, akulturacja określa także wyniki takich zmian oraz „na podstawie warunków, w jakich dochodzi do kontaktu kulturowego i zmian, można wyróżnić dwa główne rodzaje akulturacji: inkorporację i zmianę ukierunkowaną". Ważną cechą tej zmiany jest powstawanie, jako jej rezultat, nowych tworów kulturowych. Akulturacja bywa mylnie utożsamiana z *asymilacją* (która dotyczy zmian w zakresie tożsamości etnicznej grupy). Z kolei *adaptacja*, również porównywana do akulturacji, może być jej rezultatem, wskazując na przystosowanie się jednostki do warunków życia w nowej kulturowo społeczności.

Z kolei jak piszą twórcy *Glossary on Migration* Międzynarodowej Organizacji do Spraw Migracji (International Organization for Migration, IOM) z 2011 r., akulturację oznacza „seria zmian w obyczajowości kulturowej (ideały, słowa, wartości, normy, zachowania, instytucje) wynikających z bezpośredniego i ciągłego kontaktu między grupami różnych kultur, zwłaszcza poprzez ruchy migracyjne lub wymianę gospodarczą". Zjawisko to może wystąpić w przypadku przyjęcia przez jedną grupę cech dominującej kultury społeczeństwa w obszarze życia publicznego, „zachowując jednocześnie własną kulturę w sferze prywatnej. Akulturacja może również skutkować powstaniem nowej kultury, która stanowi syntezę elementów dwóch pierwotnych kultur".

Oprócz tych definicji zjawisko akulturacji tłumaczone jest też szczegółowo jako proces przyjmowania „przez jednostki elementów praktyk kulturowych, postaw, wartości oraz tożsamości nowego kontekstu kulturowego i/lub podtrzymywaniem tych wywodzących się z ich kultury pochodzenia". Dlatego ważna jest dla tych jednostek, np. migrantów, postawa lub strategia akulturacyjna, którą zaproponował John Widdup Berry, biorąc pod uwagę dwa wymiary adaptacji, indywidualną (chęć zachowania swojej tożsamości i kultury) i grupową (chęć angażowania się w interakcje z innymi grupami w szerszym społeczeństwie, w tym większościowym). Na ich postawie wyróżnił cztery typy strategii akulturacyjnej: integrację, asymilację, separację i marginalizację, wskazujące na stopień identyfikacji jednostki z rodzimą i obcą kulturą. Berry rozumie integrację jako chęć podtrzymania własnej kultury przy równoczesnej chęci zaangażowania

się w kulturę dominującą, przyjmującą, asymilację jako przyjęcie jedynie kultury społeczeństwa większościowego, przy odrzuceniu własnych wzorców kulturowych, separacją jest zaniechanie kultury dominującej i pragnienie utrzymania własnych wartości kulturowych, a marginalizacją – odrzucenie obu kultur, własnej, jak i kraju przyjmującego. Badacze z różnych dyscyplin stworzyli ponad 100 teorii akulturacji (Rudmin 2003), ale „współczesne badania koncentrują się przede wszystkim na różnych strategiach oraz na tym, jak akulturacja wpływa na jednostki, a także na interwencjach ułatwiających ten proces (Berry 1992)". Mimo że bardzo często używany, model Berry'ego spotkał się też z krytyką, w tym Floyda Rudmina: „Wskazał on na błędy logiczne prowadzące do wyodrębnienia jedynie czterech opcji akulturacyjnych, które wynikają z pominięcia orientacji na trzecią kulturę, braku uwzględnienia opcji odnoszących się do wspólnych cech dwóch kultur oraz możliwości alternatywnych wyborów. Współcześnie dominuje pogląd, iż akulturacja jest procesem złożonym i zależnym od kontekstu, w którym zachodzi". W tym przypadku pomocna jest teoria akulturacji z 2005 r. autorstwa Marisol Navas, tzw. Rozszerzony Model Względnej Akulturacji (Relative Acculturation Extended Model, RAEM) (Navas 2005), podkreślający, że różne strategie akulturacyjne mogą być wybierane przez jednostki w zależności od analizowanych sfer życia, takich jak „tzw. dziedziny akulturacji, w tym w obszarach peryferyjnych (zwanych również publicznymi): polityka, opieka społeczna, praca i gospodarka; w obszarach centralnych (zwanych również prywatnymi): relacje społeczne, relacje rodzinne, religia i wartości dla dorosłych; oraz w przypadku nastolatków w obszarach peryferyjnych – szkoła i gospodarka – oraz w obszarach centralnych, takich jak relacje społeczne, relacje rodzinne, religia i wartości". Oprócz tego teoria ta „rozróżnia strategie akulturacji (płaszczyzna realna) od preferencji w tym zakresie (płaszczyzna idealna). W związku z nasilonymi procesami migracji oraz globalizacji, i w ich wyniku silniejszą ekspozycją na inne kultury, kolejnym krokiem w rozwoju modeli akulturacji było uwzględnienie orientacji na trzecią kulturę. Modelem, który dostarcza dużych możliwości analizy tego zjawiska, jest Trójwymiarowy (3D) Model Akulturacji (Tridimensional (3D) acculturation model)" (Ferguson 2012), który otwiera na możliwość zorientowania jednostki na wiele kultur, a oprócz tego Gail M. Ferguson

i Marc H. Bornstein (2012) podkreślają znaczenie zdalnej akulturacji (*remote acculturation*), która daje możliwość przyswajania elementów innej kultury mimo braku „bezpośredniego kontaktu z jej przedstawicielami".

Jak piszą autorzy RAEM, „akulturacja odnosi się jednak również do zmian, jakich doświadczają jednostki («akulturacja psychologiczna») w aspektach poznawczych, afektywnych i behawioralnych (np. postawy, wartości, zachowania i tożsamość) w wyniku ciągłego i bezpośredniego kontaktu z osobami z różnych kultur". Stwierdzają również, że wybór procesu akulturacji dla migrantów często nie jest możliwy, bo zależy od postaw społeczeństwa dominującego oraz polityki imigracyjnej. Badania wykorzystujące model RAEM dowodzą, że przyswajanie kultury dominującej jest bardziej widoczne „w sferze publicznej, takiej jak rynek pracy. Natomiast w sferze prywatnej, takiej jak dynamika rodziny, często obserwuje się większe zachowanie kultury kraju pochodzenia". Badania te potwierdzają również wielostronność procesu akulturacji: „Model RAEM, podobnie jak inne modele (Bourhis 1997), uznaje różnorodne relacje międzygrupowe, które wynikają z przecięcia się preferencji społeczeństwa przyjmującego w zakresie orientacji akulturacyjnej migrantów oraz rzeczywistych orientacji stosowanych w praktyce lub preferowanych przez migrantów – niezależnie od tego, czy są one zgodne, problematyczne czy konfliktowe", a model ten „jest jednym z najczęściej stosowanych rozszerzeń klasycznego modelu akulturacji Berry'ego (Sam 2024), co czyni go ugruntowaną podstawą w badaniach nad akulturacją. Podczas gdy model Berry'ego zapewnia podstawowe zrozumienie strategii akulturacji, RAEM oferuje bardziej zniuansowaną perspektywę, która pozwala na bardziej kontekstową analizę procesów akulturacyjnych. Ta dodatkowa złożoność sprawia, że jest to dobry punkt wyjścia do adaptacji do badań jakościowych, gdzie potrzebne jest bardziej elastyczne i dynamiczne podejście do akulturacji".

Autorzy opracowania hasła w *Encyklopedii Britannica* piszą, że akulturacja może następować naturalnie, jak i w przypadku swobodnego zapożyczania i modyfikowania elementów kulturowych, np. gdy ludzie pochodzący z różnych kultur utrzymują wzajemne kontakty. Może też obejmować synkretyzm, nową syntezę zjawisk, która różni się od obu elementów pierwotnych, a także „adopcję, w ramach której do repertuaru

kulturowego dodawane jest całkowicie nowe zjawisko" (Britannica podaje za przykład techniki „obróbki metali rodzajów broni, które oznaczały przejście od epoki kamienia łupanego do epoki brązu, a później do epoki żelaza w Azji, Afryce i Europie") „oraz adaptację, w ramach której nowy materiał lub technologia są stosowane do istniejącego zjawiska", tutaj za przykład służą ozdoby, np. te, które rdzenni Amerykanie przyjęli i dostosowali do swoich wymagań, a które zastąpiły wcześniejsze „ciężkie kamienne wisiorki". Takie włączanie elementów innej kultury do swojej, będące wynikiem wyboru, daje im szansę na dłuższe przetrwanie. Przypadki narzucania obcej kultury kulturze rodzimej znane są ludzkości z kilku przykładów, np. przez podboje, w tym militarne, kolonialne czy kontrolę polityczną. Taka sytuacja związana jest z koniecznością dokonania wyboru i zmianą własnych elementów kulturowych. „Procesy te są jednak bardziej zróżnicowane, a ich wyniki bardziej złożone, ponieważ wynikają z ingerencji członków jednej kultury w system kulturowy innej kultury".

Kluczem do współczesnego zrozumienia zjawiska akulturacji jest zwrócenie uwagi na podobieństwo (dystans) między danymi kulturami: „Hipoteza atrakcyjności podobieństwa (Byrne 1969) przewiduje, że osoby podobne do nas pod względem ważnych, acz różnych, charakterystyk są dla nas bardziej atrakcyjne aniżeli osoby niepodobne. Wynika z tego, iż preferujemy jednostki z własnej grupy kulturowej, ponieważ są one do nas podobne i współdzielimy pewne charakterystyki tożsamościowe (Kwiatkowska 2019)".

Berry wskazał na socjopsychologiczne skutki migracji, a jego rozumienie pojęcia akulturacji związane było ze zmianą kulturową, która zachodziła w członkach mniejszości, wynikającą z długotrwałej konfrontacji z grupą większościową. Wtedy też zauważono, że proces akulturacji dotyczy społeczeństwa przyjmującego i zachodzi równolegle w dwóch obszarach kulturowych – mniejszościowym oraz większościowym, zaś „przejmowanie elementów kulturowych z każdej z tych sfer może odbywać się niezależnie (Jasinskaja-Lahti 2000), a dążenie do adaptacji ma charakter dwukierunkowy (Berry 1997, 2002). Oznacza to, że akulturacja wpływa także na modyfikacje zachowań oraz sposobów percepcji w grupie dominującej, zachodząc zarówno na poziomie jednostkowym, jak i zbiorowym. Intensywność zmian w sferze symbolicznej, jakim podlegają obie

uczestniczące w akulturacji grupy i ich członkowie, jest uzależniona od stopnia odmienności kontaktujących się kultur oraz istniejącego między nimi dystansu (Berry 1987; Malewska-Peyre 2004, 2001)".

We współczesnych badaniach przeważa „podejście o dwustronnym kierunku akulturacji, które zakłada, że zmiany zachodzą nie tylko wśród przybyszy, ale także wśród gospodarzy (por. Dandy 2023; Kunst 2021; Kunst 2023)".

Jak podaje *Oxford English Dictionary*, terminu akulturacja użyto po raz pierwszy w anglojęzycznym tekście w 1880 r. w kontekście opisania zmian w językach rdzennych Amerykanów (Powell), a w 1989 r. socjolog z *Bureau of American Ethnology* William John McGee stworzył definicję akulturacji „jako proces, w którym «urządzenia i idee są wymieniane i wzbogacane w procesie transferu», i podkreślił, że wrogie grupy często ulegają wzajemnej akulturacji" (Rudmin). Natomiast procesy i zmiany, które ten termin opisuje, można wskazać, jak podaje Rudmin, na przykładzie Sumerów w Mezopotamii, imperium egipskiego wobec Nubijczyków oraz Hammurabiego i jego kodeksu prawnego dla sumeryjskich i semickich poddanych, już w starożytności.

Podstawy badawcze dla zjawiska akulturacji w psychologii dali nauce m.in. Florian Znaniecki i William Thomas. Analizowali oni i opisywali procesy, w których udział brali imigranci z Polski do Stanów Zjednoczonych w pierwszej poł. XIX w., głównie takie jak dezorganizacja społeczna tej grupy, ale i pozytywne elementy zmian, jakie towarzyszyły ich osiedlaniu. Frederic Bartlett, podobnie jak Thomas i Znaniecki, „twierdził, że nierozwiązane napięcia akulturacyjne mogą prowadzić do «patologicznych zmian w życiu społecznym». Bartlett był prawdopodobnie pierwszym, który twierdził, że postawy mniejszości wobec kultury dominującej są szczególnie ważne. Jeśli żadna z kultur nie jest dominująca, możliwe jest ich połączenie, natomiast dominacja może spowodować całkowitą asymilację kulturową jednej z grup lub prowadzić do powstania chronicznych «kompromisowych formacji»". Uważał też, że akulturację znacznie ułatwia podobieństwo kulturowe, „zwłaszcza jeśli znaczenia emocjonalne można łatwo przenieść ze starych praktyk do nowych".

Jak wynika z badań, strategia integracji posiada najbardziej korzystne efekty psychologiczne dla tych, którzy przystosowują się do kultury

społeczeństwa goszczącego, natomiast marginalizacja daje najgorsze rezultaty, opisana została zresztą jako nieadaptacyjna strategia „akulturacji i radzenia sobie (Kunst 2013). Inni badacze argumentowali jednak, że cztery strategie mają bardzo niską wartość predykcyjną, ponieważ ludzie nie zawsze dają się jednoznacznie zaklasyfikować do jednej z tych kategorii (Kunst 2013; Schwartz 2010). Determinanty sytuacyjne (np. podróżowanie z rodziną, znajomość języka) oraz czynniki środowiskowe również wpływają na dostępność, korzyści oraz wybór różnych strategii akulturacji (Zhou 1997)".

Niektórzy badacze zwracają uwagę na brak holistycznego ujęcia w badaniach nad akulturacją, np. Marisa Navas oraz Rudmin. Ten ostatni wskazuje na oderwanie tych badań od innych nauk, takich jak prawo, oznaczające niekompletny ogląd zagadnienia, jakim jest akulturacja, która jako proces pojawiła się z początkiem istnienia cywilizacji ludzkiej: „Poszukiwanie historii akulturacji pokazuje, że prawo i akulturacja mają wspólne korzenie. Psychologiczne badania nad akulturacją zostały zepchnięte na margines i prawdopodobnie pozbawione użytecznych zastosowań poprzez odizolowanie ich od powiązanych badań naukowych w dziedzinie prawa". Uzasadnia to powiazaniem akulturacji z kwestią praw mniejszości (w tym praw językowych), praw imigracyjnych, praw uchodźców, kryminalizacją niektórych praktyk kulturowych (np. obrzezanie kobiet, bicie dzieci, walki kogutów).

Jak zauważają Justine Dandy, Tahereh Ziaian i Carolyn Moylan, we współczesnych badaniach nad akulturacją brakuje też poglądów grup niebędących imigrantami, np. grup rdzennych mieszkańców (Australia), a badania, które dają obraz perspektyw społeczeństwa większościowego, „skupiały się na ich oczekiwaniach wobec imigrantów, a nie na tym, jak sami podchodzą do zmian kulturowych wynikających z kontaktów międzykulturowych". Zdaniem autorów tym samym „wzajemność akulturacji pozostaje niedostatecznie zbadana". Powołując się na dotychczasowe wyniki badań, można stwierdzić, że społeczności przybywające, „imigranci zazwyczaj deklarują preferencję dla integracji (Bourhis, Moïse, Perreault, Senécal 1997; Jasinskaja-Lahti, Liebkind, Horenczyk, Schmitz 2003), podczas gdy w niektórych kontekstach członkowie większości częściej preferują asymilację imigrantów (Arends-Tóth, van de Vijver 2003)". Stąd różne

podejścia do akulturacji (rozbieżne lub sprzeczne) mogą dawać początek międzygrupowym napięciom oraz „wydaje się, że preferowane strategie akulturacyjne członków większości to separacja i integracja (Haugen, Kunst 2017), ale badania na ten temat są nieliczne".

Jednocześnie ważne w badaniach nad akulturacją jest stwierdzenie, że procesy akulturacji danej grupy muszą być badane w odpowiednim kontekście, uwzględniając miejscowe warunki międzygrupowe, historię, ale także politykę danego regionu, ponieważ te i inne czynniki mogą wpływać na relacje międzykulturowe.

Ważny wydaje się postulat Rudmina dotyczący założenia, które powinni przyjąć badacze, „że akulturacja jest normalnym, uniwersalnym procesem ludzkim, zachodzącym niezależnie od statusu większości lub mniejszości".

Katarzyna Pabis-Cisowska

Akulturacja [hasło], [w:] *Britannica Online Encyclopedia*, https://www.britannica.com/topic/acculturation (dostęp 11.11.2025); *Akulturacja* [hasło], [w:] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/akulturacja;3867111.html (dostęp 11.11.2025); *Akulturacja* [hasło], [w:] *Oxford English Dictionary*, https://www.oed.com/dictionary/acculturation_n?tab=factsheet&tl=true#3508894 (dostęp 11.11.2025); J.W. Berry, *Acculturation and intercultural relations*, [w:] *Cross-cultural Psychology: Research and Applications*, J.W. Berry (ed.), Cambridge University Press, Cambridge–New York 2002; J.W. Berry, *Acculturation: living successfully in two cultures*, „International Journal of Intercultural Relations" 2005; vol. 29(6); J. Dandy, T. Ziaian, C. Moylan, *'Team Australia?': Understanding acculturation from multiple perspectives*, [w:] *Venture into cross-cultural psychology: Proceedings from the 23rd Congress of the International Association for Cross-Cultural Psychology*, M. Karasawa, M. Yuki, K. Ishii, Y. Uchida, K. Sato, W. Friedlmeier (eds.), International Association for Cross-Cultural Psychology Conferences 2018; *Glossary on Migration*, „International Migration Law" 2011, no. 25; A. Golińska, A. Posmykiewicz, *Strategie akulturacyjne wśród międzynarodowych studentów anglojęzycznych programów zarządzania w Polsce*, „Edukacja Międzykulturowa" 2024, t. 25(2); J.B. Klakla, P. Szydłowska-Klakla, M. Navas*, Enhancing the Relative Acculturation Extended Model: A Qualitative Perspective*, „Central and Eastern European Migration Review" 2025, vol. 14, no. 1; J. Radzińska, A. Golińska, *Cokolwiek się nie wydarzy mieć odwagę i honor w każdej sytuacji zachować się po prostu przyzwoicie… Granice gościnności na przykładzie przyjęcia w Polsce osób uchodźczych z Ukrainy*,

„Studia Migracyjne – Przegląd Polonijny" 2024, t. 50(L), nr 2(192); F.W. Rudmin, *Critical History of the Acculturation Psychology of Assimilation, Separation, Integration, and Marginalization*, „Review of General Psychology" 2003, vol. 7, no. 1; A. Żaliński, *Akulturacja* [hasło], [w:] *Studia kulturowe*, L. Korporowicz, A. Knap-Stefaniuk, Ł. Burkiewicz (red.), Wydawnictwo Naukowe Akademii Ignatanium w Krakowie, Kraków 2022.

AMERYKAŃSKI SYSTEM OBRONY PRZECIWLOTNICZEJ I PRZECIWRAKIETOWEJ (ang. AEGIS Ballistic Missile Defense System – AEGIS BMDS) – określany oficjalnie jako „zintegrowany zestaw czujników, komputerów, oprogramowania, wyświetlaczy, wyrzutni rakietowych i pocisków", którego nazwa pochodzi od mitycznej tarczy broniącej Zeusa. AEGIS jest zarówno systemem bojowym, jak również uzbrojenia. Powstał w wyniku zapotrzebowania Marynarki Wojennej Stanów Zjednoczonych na nowoczesny system obrony przeciwlotniczej. Motywacją był m.in. fakt pojawienia się samolotów odrzutowych oraz technologii rakietowej w latach 60. XX w., której nie dało się już zwalczać za pomocą ograniczonych środków w postaci działek przeciwlotniczych używanych przeciwko wolno lecącym myśliwcom i bombowcom. Przykładem było zatopienie izraelskiego niszczyciela Eliat w 1967 r. przez siły egipskie za pomocą pocisku wystrzelonego z odległości 14 mil. Opracowany został system rakietowy ziemia–powietrze ASMS, zmieniony następnie w 1968 r. na AEGIS. Prace nad nim opierały się na zrealizowaniu kilku celów (kamieni węgielnych), takich jak czas reakcji, zasięg, wystarczająca siła ognia, odporność na warunki środowiskowe i ciągła dostępność. Każda kolejna modernizacja systemu skupiała się na poprawie jednej z tych płaszczyzn. AEGIS od samego początku nie posiadał platformy testowej – okrętu, na którym mógłby być przenoszony; zespół badawczy opracował w związku z tym wystarczająco dużą „platformę", na której mógł on zostać umieszczony, a montaż – kontynuowany.

Pierwszy okrętem posiadającym na swoim wyposażeniu AEGIS miał być specjalnie zaprojektowany, nowy krążownik rakietowy o napędzie atomowym. Biorąc pod uwagę budżet marynarki wojennej w latach 70. XX w., pomysł ten nie mógł być jednak zrealizowany. Alternatywnym rozwiązaniem było umieszczenie systemu na wykorzystywanym wówczas

niszczycielu klasy Spruance, po wcześniejszy, przekonfikurowaniu kadłuba; rezultatem modernizacji było powstanie krążownika klasy Ticonderoga. W latach 1978–1988 zakupionych zostało łącznie 27 krążowników, które weszły do służby w latach 1983–1994. Pierwsze 5 okrętów zbudowano według pierwotnych standardów technicznych, jednak marynarka wojenna uznała, że są one zbyt kosztowe w modernizacji i wycofała je ze służby, do 2005 r. pozostawiając w eksploatacji 22. Podobnie jak inne okręty Ticonderoga przechodziły bieżące modernizacje, jednak zdolności amerykańskiego przemysłu nie przekraczały naprawy 2 sztuk rocznie. Wraz z biegiem lat USA rezygnowały z kolejnych egzemplarzy. W 2024 r. w służbie pozostawało 11 okrętów, a pod koniec 2025 r. – już tylko 7: USS Princeton, USS Robert Small (dawny Chancellorsville), USS Gettysburg, USS Chosin, USS Shiloh, USS Lake Erie oraz USS Cape St. George. Generalny sukces okrętów klasy Ticonderoga skłonił marynarkę wojenną do zakupu mniejszych i tańszych niszczycieli Arleigh-Burke, na których również umieszczony został system AEGIS. Łącznie w latach 1985–2005 nabyto 62 okręty, z czego pierwszy wszedł do służby w 1991 r.

System uzbrojenia AEGIS składa się z kilku komponentów:

- systemu dowodzenia i podejmowania decyzji, który odbiera informacje z radaru SPY;
- systemu kontroli;
- systemu wyświetlania (przedstawiającego załodze aktualny obraz sytuacyjny).

Decyzja o neutralizacji zagrożenia podejmowana jest przez operatora w ramach systemu dowodzenia, a następnie przekazywana do systemu sterowania uzbrojeniem, który ustala plan działania wyrzutni. Dane o celu wysyłane są do pocisku za pomocą radaru SPY, który oświetla go w końcowej fazie naprowadzania, tak aby cały proces maksymalnie skrócić. Zdolność do obrony przed pociskami rakietowymi nie była jedynym wymogiem stawianym przed AEGIS – w ramach zapotrzebowania na kolejne funkcje powstał równolegle system bojowy o tej samej nazwie składający się z różnego rodzaju sonarów i systemów walki elektronicznej umożliwiających zwalczanie celów innych niż tylko samoloty i pociski manewrujące. Od momentu powstania AEGIS przeszedł wiele modernizacji; niektóre z nich wymuszone zostały tragicznymi incydentami,

takimi jak zestrzelenie irańskiego samolotu pasażerskiego Air 655 z 290 osobami na pokładzie w 1988 r. przez amerykański krążownik rakietowy USS Vincennes. Śledztwo ujawniło, że system działał zgodzie założeniami, a przyczyną wypadku był błąd ludzki w zakresie interpretacji informacji dostarczonych przez AEGIS. Nie był to jedyny problem, z jakim musiał się zmierzyć zespół badawczy, czyli identyfikowanie celów. Kolejnym było skrócenie czasu na przeładowanie pocisków i szybkie ich użycie w związku z wzrastającą prędkością pocisków manewrujących. Rozwiązaniem okazało się włączenie systemu pionowego startu rakiet Mark 41 (VLS) do nowych krążowników, co umożliwiło redukcję czasu o połowę w porównaniu z wcześniej używanymi wyrzutniami.

Sprawdzianem dla systemu AEGIS była I wojna w Zatoce Perskiej. Przewaga, jaką uzyskały nad Irakiem Stany Zjednoczone w obszarze nowej techniki wojskowej, skłoniła pozostałych przeciwników Waszyngtonu do rozwoju pocisków manewrujących lecących bardzo nisko, tak aby nie można było ich śledzić ze względu na krzywiznę Ziemi i tym samym pozostały niewykryte przez radar SPY. Amerykańską odpowiedzią było opracowanie mechanizmu kooperacyjnego zaangażowania (*co-operative engagement capability*, CEC) polegającego na przekazywaniu danych o pocisku między okrętami lub między samolotem a okrętem. Obecnie użytkowany AEGIS nie przypomina systemu z 1983 r. pod względem technologicznym; ciągłe modernizacje doprowadziły do wykładniczego wzrostu mocy obliczeniowej.

Na początku lat 90. XX w. doszło do kolejnej znaczącej zmiany technologii rakietowej wraz z rozwojem pocisków balistycznych. W 1991 r. okręt USS Mobile Bay pomimo zlokalizowania i śledzenia wystrzelonego w jego kierunku pocisku SCUD nie był w stanie go zestrzelić; w rezultacie w latach 1991–2004 prowadzono badania nad systemem obrony przeciwrakietowej AEGIS BMD umożliwiającym wykrywanie z kosmosu startu pocisków balistycznych. Finalnie system uzyskał zdolność do przechwytywania pocisków balistycznych teatru działań, czyli krótkiego, średniego i pośredniego zasięgu (SRBM, MRBM, IRBM). Według stanu na rok 2018 AEGIS nie był przygotowany do przechwytywania międzykontynentalnych pocisków balistycznych ICBM. Po wykryciu celu dane mogły być jednak przekazywane do innych amerykańskich systemów BMD posiadających zdolności

do jego zniszczenia. W 2020 r. przeprowadzony został test wskazujący, że zespoły badawcze pracujące nad AEGIS uzupełniły tę lukę. Niszczyciel rakietowy USS John Finn klasy Arleigh Burke wyposażony w system AEGIS BMD przechwycił i zniszczył międzykontynentalny pocisk balistyczny za pomocą pocisku SM-3 Block IIA.

Obok SM-3 do neutralizacji pocisków balistycznych wykorzystywane są także pociski SM-2 Block IV i SM-6. SM-3 zaprojektowany został do przechwytywania pocisków nad atmosferą w środkowej fazie lotu. Wyposażony jest w głowicę bojową typu *hit-to-kill* określaną również jako „pojazd kinetyczny", która niszczy cel poprzez bezpośrednie uderzenie. Obecnie występuje w wersjach SM-3 Block IA, SM-3 Block IB, SM-3 Block IIA. SM-3 IA i IB reprezentują odpowiednio pierwszą i drugą generację morskich pocisków przechwytujących i są przeznaczone do niszczenia pocisków balistycznych krótkiego i średniego zasięgu. Amerykańska Agencja Obrony Przeciwrakietowej (MDA) zakupiła 150 sztuk SM-3 IA i 182 sztuk SM-3 IB, które następnie rozmieszczone zostały na krążownikach, niszczycielach i bazach typu Aegis Ashore marynarki wojennej. SM-3 Block IIA reprezentują następną generację pocisków wykorzystywanych przez AEGIS BMD; powstały w wyniku porozumienia amerykańsko-japońskiego z 1999 r. w sprawie obrony przeciwrakietowej, będącej odpowiedzią na test pocisku Taepodong-1 przeprowadzony przez Koreę Północną w 1998 r. Celem obu państw było stworzenie pocisku przechwytującego zdolnego do niszczenia szerokiej kategorii rakiet pośredniego zasięgu, co było wówczas głównym wyzwaniem dla bezpieczeństwa Japonii. W przeciwieństwie do wcześniejszych wersji Block IIA ma jednolitą 21-calową szerokość i tym samym miejsce na dodatkowy napęd wykorzystywany w drugim etapie lotu pocisku oraz większy pojazd przechwytujący *kill vehicle*, który może przenosić więcej paliwa. Plany Agencji Obrony Przeciwrakietowej i marynarki wojennej przewidywały zastąpienie SM-3 Block IIA jeszcze bardziej zaawansowanymi technologicznie pociskami SM-3 Block IIB, jednak prace na nimi zostały przerwane. Do 2018 r. MDA kupiła około 336 pocisków SM-3 różnego typu, z czego 47 zużytych zostało w czasie testów, 24 znajdują się w bazie AEGIS Ashore w Rumunii, a 265 przydzielono do okrętów marynarki wojennej posiadających zdolności obrony przeciwbalistycznej.

Obok okrętów marynarki wojennej system AEGIS składa się także z lądowego komponentu określanego jako AEGIS Ashore. Decyzja o jego budowie zapadła na szczycie NATO w Walii w 2014 r. i miała ona na celu zbudowanie technicznych fundamentów European Phased Adaptive Approach (EPAA) – podsystemu amerykańskiej „tarczy antyrakietowej" obejmującego ochronę europejskich członów Sojuszu Północnoatlantyckiego przed pociskami balistycznymi wystrzeliwanymi spoza Europy (Iranu). Pierwszym miejscem, gdzie umieszczony został radar SPY-1 oraz bateria pocisków SM-3, była miejscowość Deveselu w Rumunii, oddana do użytkowania w 2016 r., drugim natomiast Redzikowo w Polsce oddane do użytku w 2024 r.

System AEGIS poza Marynarką Wojenną Stanów Zjednoczonych wykorzystywany jest przez siły zbrojne Australii, Japonii, Korei Południowej, Norwegii i Hiszpanii. W Australii są to okręty klasy Hunter i Hobart – na niszczycielu klasy Hobart zamontowany został AEGIS seria Baseline 8, co umożliwia jednoczesne działanie obrony przeciwlotniczej i przeciwrakietowej, a wyrzutnie Mark 41 przenoszą dowolny system rakietowy, jaki oferuje amerykański przemysł wojskowy, m.in. pocisk SM-2, Evolved Sea Sparrow czy Harpoon Block 2. Rząd Australii ogłosił program rozbudowy zdolności niszczycieli do poziomu AEGIS Baseline 9, który uzupełni jego możliwości o użycie pocisków Tomahawk i SM-6.

Tomasz Wójtowicz

The Aegis Ashore Missile Defense System in Naval Support Facility Redizkowo, Poland, Transfers Ownership from Missile Defense Agency to the U.S. Navy, https://www.c6f.navy.mil/Press-Room/News/News-Display/Article/3618612/the-aegis-ashore-missile-defense-system-in-naval-support-facility-redizkowo-pol/ (dostęp 14.12.2025); Y. Dar, *US Navy Achieves New Milestone; Shoots Down Intercontinental Ballistic Missile (ICBM) Mid-Air*, https://www.eurasiantimes.com/us-navy-demonstrates-capability-to-shoot-down-intercontinental-ballistic-missile-icmb-mid-air/ (dostęp 13.12.2025); A. Hough, L. Rollins, *The history of the AEGIS combat system*, RUSI 03.2022; *Standard Missile-3 (SM-3)*, https://missilethreat.csis.org/defsys/sm-3/ (dostęp 13.12.2025); T. Wójtowicz, *Nowe technologie w bezpieczeństwie militarnym. Stany Zjednoczone, Federacja Rosyjska, Chińska Republika Ludowa*, Wydawnictwo Naukowe Uniwersytetu Komisji Edukacji Narodowej w Krakowie, Kraków 2025.

ANARCHOSYNDYKALIZM – ideologia i ruch społeczno-polityczny, który łączy zasady anarchizmu i syndykalizmu, opierający się na idei stworzenia społeczeństwa bezpaństwowego, które funkcjonuje na zasadach dobrowolnej współpracy i samodzielnego zarządzania przez pracowników. To jeden z niezależnych nurtów anarchizmu, który uważa, że środki produkcji powinny przejść w ręce najwyższej formy organizacji pracowników – związków zawodowych.

Anarchosyndykalizm to anarchistyczny model organizacyjny, który koncentruje się na związkach zawodowych jako nośniku konfliktu klasowego. Czerpiąc z teorii socjalizmu wolnościowego i praktyki syndykalizmu, anarchosyndykalizm postrzega związki zawodowe zarówno jako środek do osiągnięcia natychmiastowej poprawy warunków pracy, jak i budowania rewolucji społecznej w formie strajku generalnego, którego ostatecznym celem jest zniesienie państwa i kapitalizmu. Jako ideologia antypolityczna anarchosyndykalizm odrzuca partie polityczne i udział w polityce parlamentarnej, uważając je za demoralizujące w kontekście ruchu robotniczego. Aby osiągnąć swoje cele materialne i ekonomiczne, anarchosyndykaliści praktykują zamiast tego działania bezpośrednie w formie strajków, bojkotów i sabotażu; starają się również budować solidarność wśród klasy robotniczej, aby zjednoczyć pracowników przeciwko wyzyskowi i budować samorządność.

Syndykalizm, rozumiany jako organizowanie robotników w związki zawodowe, stanowił kluczowy element tego nurtu. W połączeniu z anarchizmem, który stawia sobie za cel zniesienie wszelkich hierarchicznych struktur władzy, powstał anarchosyndykalizm. Był aktywny w ruchu robotniczym, organizując strajki i budując solidarność, często występując przeciwko politykom i biurokracji.

Anarchosyndykalizm wyłonił się na przełomie XIX i XX w. w Europie jako odpowiedź na rosnącą siłę ruchów robotniczych, które dążyły do poprawy warunków pracy i życia, ale jednocześnie były zniechęcone do politycznych partii i systemów rządowych, które uznawano za skorumpowane i niewłaściwe. Anarchosyndykalizm stał się dominującym nurtem w anarchii po niepowodzeniu jego tendencji powstańczej w latach 80. i 90. XIX w.

Ukształtował się jako spójny ruch dopiero na początku XX w. i miał znaczący wpływ na międzynarodowy ruch związkowy oraz partie socjalistyczne niektórych krajów. Podwaliny anarchosyndykalizmu zostały położone przez antyautorytarną frakcję Międzynarodowego Stowarzyszenia Robotników (IWMA) i rozwinięte przez Francuską Generalną Konfederację Pracy (CGT). Anarchosyndykalizm narodził się jako specyficzna tendencja po Międzynarodowym Kongresie Anarchistycznym w Amsterdamie w 1907 r., który doprowadził do tego, że anarchosyndykalizm stał się dominującą formą organizacji związków zawodowych w Europie i Ameryce Łacińskiej.

Teoretykami anarchosyndykalizmu byli Georges Sorel, Hubert Lagarde i inni. Główne idee anarchosyndykalizmu zostały zawarte w Karcie z Amiens, przyjętej w 1906 r. na kongresie Generalnej Konfederacji Pracy Francji w Amiens. Ideologia anarchosyndykalizmu wywodzi się przede wszystkim z myśli Michaiła Bakunina; można ją rozumieć jako synonim socjalizmu wolnościowego lub komunizmu wolnościowego.

Anarchosyndykalizm rozprzestrzenił się głównie we Francji, Włoszech, Hiszpanii i krajach Ameryki Łacińskiej, gdzie istniała znaczna drobnomieszczańska warstwa ludności, z której stale uzupełniano szeregi klasy robotniczej. W Hiszpanii odgrywał znaczącą rolę w ramach Narodowej Konfederacji Pracy, jednak samo określenie „anarchosyndykalizm" pojawiło się dopiero na kongresie założycielskim francuskiej Generalnej Konfederacji Pracy Jednostkowej (CGTU), która wspierała bolszewików, w Saint-Étienne w 1922 r., kiedy CGTU dyskutowało o swoim członkostwie w Czerwonej Międzynarodówce Związków Zawodowych.

Anarchosyndykalizm stał się głównym nurtem we francuskim ruchu związkowym w reakcji na wzrost Francuskiej Partii Komunistycznej w ramach Powszechnej Konfederacji Pracy – Zjednoczonej (CGT-U) w latach 30. XX w. Doprowadziło to do rozłamu i utworzenia przez czystych (anarchistycznych) działaczy związkowych i rewolucyjnych syndykalistów krótkotrwałej Generalnej Konfederacji Pracy – Rewolucyjnej Syndykalistycznej, której statut położył podwaliny pod francuski anarchosyndykalizm.

Europejski rozkwit anarchosyndykalizmu miał natomiast miejsce podczas rewolucji hiszpańskiej w 1936 r., kiedy to Narodowa Konfederacja Pracy (CNT) ustanowiła gospodarkę anarchosyndykalistyczną w większej części Republiki Hiszpańskiej, mając na celu kolektywizację ziemi i przemysłu na kontrolowanych przez siebie obszarach. Pod koniec XX w. rozwój neoliberalizmu i upadek bloku wschodniego doprowadziły do odrodzenia się anarchosyndykalizmu, a związki zawodowe syndykalistów ponownie zaczęły powstawać na całym świecie.

Ruch anarchosyndykalistyczny (a dokładniej – anarchizm robotniczy) miał również dominujący wpływ w Ameryce Łacińskiej, gdzie dał początek ruchowi robotniczemu w wielu krajach. W Argentynie Argentyńska Regionalna Federacja Robotnicza (FORA) stanowiła masową organizację zdolną do przeciwstawienia się państwu i pracodawcom, zanim została zmiażdżona przez brutalne represje.

Anarchosyndykalizm, czyli anarchizm robotniczy, uznaje jedynie oddolną, niehierarchiczną samoorganizację pracowników, a zatem odrzuca udział w organach rządowych, partiach politycznych i zhierarchizowanych związkach zawodowych.

Anarchosyndykaliści nawołują do rozwoju umiejętności samorządności i solidarności poprzez samoorganizację w codziennej walce o lepsze warunki życia i rozszerzenie praw pracowników najemnych, przeciwko kapitału i państwa, poprzez strajki, bojkoty, demonstracje, sabotaże i inne podobne akcje protestacyjne (tzw. „akcje bezpośrednie"), w celu przygotowania rewolucji społecznej, która powinna doprowadzić do rządów wolnego komunizmu. Anarchosyndykaliści uważają, że związki zawodowe powinny działać w oparciu o zasadę podejmowania decyzji przez cały kolektyw, poprzez lokalne zebrania ogólne. Odrzucają podział ludzi ze względu na płeć, orientację seksualną, wiek, przynależność etniczną i narodową, a także wszelkie inne formy segregacji i dyskryminacji.

Celem anarchosyndykalistów jest ustanowienie nowego, sprawiedliwego i emancypacyjnego porządku społecznego (a nie „nieporządku" społecznego) poprzez wspólne zniesienie kapitalizmu i państwa. Anarchosyndykaliści proponują zastąpienie własności prywatnej

„indywidualną własnością", która nie gwarantuje żadnych praw dotyczących gromadzenia „nieużywanych" dóbr.

Kluczowe założenia anarchosyndykalizmu:

- **związki zawodowe** stanowią centralny element; nie są tylko narzędziem negocjacji, ale siłą rewolucyjną, która ma doprowadzić do rewolucji społecznej i organizacji nowego społeczeństwa;
- **bezpaństwowość**: anarchosyndykaliści odrzucają istnienie państwa i wszelkich form przymusowej władzy, dążąc do jej zniesienia; postulują likwidację państwa postrzeganego jako narzędzie ucisku klasowego i niesprawiedliwości społecznej. Zamiast centralnego rządu proponują decentralizację i samodzielne zarządzanie na poziomie lokalnym i branżowym;
- **rewolucja społeczna**: wierzą, że przejście do nowego ustroju musi dokonać się poprzez rewolucję, której głównymi aktorami są robotnicy;
- **syndykaty i federacje**: zamiast tradycyjnych partii politycznych anarchosyndykaliści stawiają na organizowanie robotników w syndykatach (związkach zawodowych), które mają na celu bezpośrednią kontrolę nad miejscem pracy. Syndykaty te nie tylko walczą o poprawę warunków pracy, ale mają pełnić rolę struktur zarządzających w przyszłym społeczeństwie bezpaństwowym. Syndykaty mogą być federowane, co oznacza, że współpracują ze sobą w sposób federacyjny, ale zachowują swoją autonomię;
- **strajki i bojkoty**: narzędziami walki są strajki generalne, protesty, sabotaże, bojkoty i inne formy bezpośredniej akcji. Zamiast liczyć na reformy rządowe, anarchosyndykaliści uważają, że to robotnicy muszą przejąć kontrolę nad środkami produkcji poprzez akcje bezpośrednie, czyli działanie bez pośredników, takich jak partie polityczne czy państwo;
- **autonomia i samorządność**: każdy zakład pracy powinien być zarządzany przez pracowników, którzy będą podejmować decyzje w sposób demokratyczny i kolektywny. Chodzi o to, aby struktury pracy umożliwiły pracownikom pełną kontrolę.

W tym modelu nie ma miejsca na dyktat właścicieli ani państwowe regulacje;
- **solidarność**: anarchosyndykaliści podkreślają rolę solidarności między pracownikami. Ruch ten nie koncentruje się na żądaniach pojedynczych grup, lecz na wspólnej walce wszystkich robotników o równość i sprawiedliwość społeczną;
- **zniesienie podziału pracy**: anarchosyndykaliści dążą do przezwyciężenia podziału pracy, który prowadzi do alienacji pracowników i nierówności społecznych. Chcą stworzyć społeczeństwo, w którym praca będzie rozdzielana sprawiedliwie i umożliwi realizację indywidualnych pasji oraz potrzeb.

Ustanawia prymat logiki związkowej nad działaniami politycznymi lub partyjnymi w rozwoju ruchu robotniczego i powstawaniu zdecentralizowanego społeczeństwa, wolnego od jakiejkolwiek formy przymusu państwowego i opartego przede wszystkim na samorządności.

Dla jego zwolenników anarchosyndykalizm jest zorganizowany i ustrukturyzowany: postuluje związek zawodowy jako formę organizacji emancypacyjnej dla pracowników i odrzuca zasadę partii politycznych lub grup korporacyjnych.

Aktywiści anarchosyndykalistyczni opracowali wiele teorii dotyczących praktyk związkowych. Choć poświęcili wiele uwagi strajkowi generalnemu jako sposobowi na odzyskanie środków produkcji przez klasę robotniczą, spopularyzowali również działania bezpośrednie (okupacje, pikiety), sabotaż (odmowę produkcji dóbr wysokiej jakości i bojkot przez proletariat danych produktów) jako środki działania, a w niektórych przypadkach także bezpośrednie przywłaszczenie wytworzonego mienia.

Anarchosyndykalizm, zarówno w teorii, jak i praktyce, zawiera w sobie wizję kompleksowego projektu politycznego. Ten silny związek między anarchosyndykalizmem a wolnościowym komunizmem znajduje odzwierciedlenie we wspólnym zestawie zasad i praktyk: demokracji bezpośredniej, rotacji stanowisk, antyautorytaryzmie, solidarności i federalizmie. Jednakże, w różnym stopniu, w zależności od organizacji deklarującej się jako anarchosyndykalistyczna, istnieją rozbieżności między tymi zasadami a konkretnymi praktykami. W niektórych przypadkach przepaść staje się tak duża, a przestrzeganie pewnych zasad tak słabe,

że tożsamość „anarchosyndykalistyczna", a nawet „anarchistyczna", jest regularnie negowana.

Współcześnie we Francji rozwija się ruch anarchosyndykalistyczny. Wymienić tu można chociażby Związek Anarchosyndykalistów (UAS), Międzykorporacyjny Związek Anarchosyndykalistyczny (SIA) i Anarchosyndykalistyczną Grupę Akcji i Refleksji (GARAS). Na szczeblu międzynarodowym również hiszpańska CGT (CGTe), hiszpańska CNT, szwedzka SAC, rzymska grupa USI we Włoszech, Industrial Workers of the World, czyli IWW, głównie w krajach anglosaskich, twierdzą – przynajmniej częściowo – że są anarchosyndykalistyczni.

Symboliką ruchów anarchosyndykalistycznych i anarchokomunistycznych jest czerwono-czarna flaga; czerń to tradycyjny kolor anarchizmu, a czerwień – socjalizmu. Flaga łączy te dwa kolory w równych częściach, oddzielonych przekątną: czerwona jest zazwyczaj umieszczana w lewym górnym rogu, a czarna – w prawym dolnym, symbolizując współistnienie ideałów anarchistycznych i socjalistycznych w ruchu anarchosyndykalistycznym, a także reprezentuje środki społeczne wykorzystywane przez ruch do osiągania celów anarchistycznych.

Drugim symbolem tego ruchu jest Czarny Kot przedstawiony z wygiętym grzbietem, potarganym ogonem, ukazujący pazury i zęby. Sabo-Cat, czyli Kot Pręgowany, od dawna jest symbolem organizacji Industrial Workers of the World (IWW); został zaprojektowany przez Ralpha Chaplina, jednego z pionierów ilustracji znanych jako „ciche protesty" w IWW. Prace te były ściśle związane z życiem osób bezdomnych. Chociaż dziś symbol ten kojarzony jest głównie z IWW (czasem nawet jako maskotka), pierwotnie był wezwaniem do bezpośredniego działania w miejscu pracy, zwłaszcza sabotażu. Jak sugeruje jego postawa, kot symbolizuje strajk i radykalny związek zawodowy.

Nazwę Chat Noir przyjęło wiele organizacji i kolektywów podających się za część ruchu anarchistycznego.

Mimo że anarchosyndykalizm w tradycyjnej formie nie jest już tak popularny, wciąż ma zwolenników na całym świecie. Współczesne ruchy anarchosyndykalistyczne często koncentrują się na lokalnych inicjatywach, takich jak organizowanie wspólnotowych gospodarstw rolnych, protesty

przeciwko neoliberalnym reformom czy organizowanie strajków w dużych korporacjach.

Anarchosyndykalizm może być również postrzegany jako inspiracja dla współczesnych ruchów, takich jak Occupy Wall Street, Indignados czy różne formy ekologicznych protestów.

Warto zauważyć, że współczesne formy anarchosyndykalizmu w Polsce nie pojawiły się „z niczego", lecz są częścią dłuższej tradycji, sięgającej okresu międzywojennego, działań konspiracyjnych, a później reaktywacji w latach 80. i 90. Jednak dziś formuła ruchu – ze względu na zmieniony rynek pracy, globalizację, przemiany gospodarcze – też się zmieniła: zauważalny jest większy nacisk na pracowników prekarnych, pracę w sektorze usług, elastyczne formy zatrudnienia, a nie na klasyczne fabryki.

Anarchosyndykalizm w Polsce nie odgrywa roli masowego nurtu politycznego, ale współcześnie ma on realne przejawy – przede wszystkim poprzez działalność określonych związków, organizacji i społecznych inicjatyw, z których najważniejszy jest Ogólnopolski Związek Zawodowy „Inicjatywa Pracownicza" (OZZ IP), określający się jako anarchosyndykalistyczny. Struktura OZZ IP jest zdecentralizowana, często oparta na komisjach zakładowych, „komitetach" i bez mocnej biurokracji – to nawiązuje do idei samorządności robotniczej. OZZ IP ma relatywnie małe – w skali całego rynku pracy – przedstawicielstwo. Związek działa przy pomocy komisji zakładowych, międzyzakładowych, tzw. grup środowiskowych. W oficjalnym sprawozdaniu ze zjazdu krajowego (2022–2024) podano, że w tym okresie zarejestrowano 49 nowych komisji zakładowych/międzyzakładowych, a ogólna liczebność związku wzrosła z około 5 tys. do blisko 6 tys. osób.

Opinia publiczna, media, politycy nadal kojarzą „anarchię" z chaosem, ekstremizmem albo z radykalną opozycją wobec państwa; to znacząco ogranicza popularność i akceptację takich form działalności. Dużym wyzwaniem jest też strukturalna słabość: brak zasobów i stałego finansowania oraz często ograniczona aktywność poza większymi miastami, co utrudnia budowę trwałych, silnych struktur.

Warto zauważyć, że ruch anarchosyndykalistyczny w Polsce nie zniknął – przynajmniej część zorganizowana (głównie OZZ IP) działa, rośnie i próbuje obejmować pracowników sektorów, w których trudno

zorganizować instytucje związkowe. Natomiast skala tego ruchu wciąż pozostaje raczej niska w proporcji do całego rynku pracy; OZZ IP to kilka tysięcy członków, a to oznacza, że nadal jest to ruch marginalny.

Głównym celem współczesnego anarchosyndykalizmu jest likwidacja instytucji państwowych i stworzenie wolnego społeczeństwa. Pomimo trudności w obliczu globalizacji i zmian strukturalnych idee anarchosyndykalizmu nadal inspirują ruchy pracownicze i antyautorytarne, stawiając na siłę ekonomiczną i organizacyjną klasy pracującej. W obliczu wszechobecności aktywistów marksistowskich w kręgach związkowych anarchosyndykalizm nigdy nie odzyska wpływu ideologicznego, jakim cieszył się na początku XX w.

Sergiusz Wasiuta

S. Dolgoff, *Ewolucja anarchosyndykalizmu*, https://pl.anarchistlibraries.net/library/sam-dolgoff-ewolucja-anarchosyndykalizmu (dostęp 5.11.2025); M. Drabiński, *Anarchosyndykalizm w Europie Teoria i praktyka*, Oficyna Wydawnicza Bractwa Trojka, Warszawa 2014; R. Graham, *Anarchism and the First International*, [w:] *The Palgrave Handbook of Anarchism*, M.S. Adams, S. Matthew, C. Levy (eds.), Palgrave Macmillan, London 2018; R. Górski, *Historia i teraźniejszość samorządności pracowniczej w Polsce*, https://pl.anarchistlibraries.net/library/rafal-gorski-historia-i-terazniejszosc-samorzadnosci-pracowniczej-w-polsce (dostęp 2.11.2025); T. Onyszkiewicz, *Anarchizm transcendentalny a gnoza*, Wydawnictwo Graffiti BC, Toruń 2018; E. Posłuszna, *Terroryzm anarchistyczny – istota, taktyka, organizacja*, „Bezpieczeństwo Narodowe" 2013, nr IV(28); M. Ramnath, *Non-Western Anarchisms and Postcolonialism*, [w:] *The Palgrave Handbook of Anarchism*, M.S. Adams, S. Matthew, C. Levy (eds.), Palgrave Macmillan, London 2018; R. Rocker, *Anarchosyndykalizm: Teoria i praktyka. Wstęp do tematu, któremu wojna w Hiszpanii nadała wielki rozgłos*, https://pl.anarchistlibraries.net/library/rudolf-rocker-anarchosyndykalizm-teoria-i-praktyka#toc6 (dostęp 5.11.2025); *Sprawozdanie z XIII Krajowego Zjazdu Delegatów i Delegatek OZZ Inicjatywa Pracownicza*, https://wschod.ozzip.pl/sprawozdanie-z-xiii-krajowego-zjazdu-delegatow-i-delegatek-ozz-inicjatywa-pracownicza/ (dostęp 2.11.2025); G. Zackiewicz, *Syndykalizm w polskiej refleksji rzeczywistości politycznej I połowy XX wieku*, Wydawnictwo AVALON T. Janowski Sp. J., Kraków 2013.

APARTHEID – system polityczno-społeczny opierający się na segregacji rasowej, charakteryzujący się hierarchią, w której jedna grupa sprawuje

kontrolę nad drugą i jest uprzywilejowana. Stanowi całkowite przeciwieństwo procesów takich jak asymilacja i integracja, ponieważ zamiast łączyć społeczeństwo, dzieli je na podstawie rasy i pochodzenia. Pojęcie szczególnie znane i kojarzone z Republiką Południowej Afryki (RPA). Doktryna realizowana w latach 1948–1994 pozwalała białej mniejszości na dyskryminację, wyzysk, przemoc i represje wobec ludności czarnoskórej.

Polityka ta rozwijała się już od czasów kolonialnych, kiedy Holendrzy osiedlili się na Przylądku Dobrej Nadziei w 1652 r. i zainicjowali założenie fortu w Zatoce Stołowej. Zapoczątkowało to wypieranie lokalnych mieszkańców poprzez pozbawianie dostępu do pastwisk, zasobów wodnych, a w skrajnych przypadkach nawet rabunek mienia. *Apartheid* pierwotnie obejmował drobne formy ograniczeń w codziennym życiu (przywłaszczanie bydła, pól uprawnych), jednak sukcesywnie przekształcał się w rygorystyczne i bardziej rozbudowane formy dyskryminacji rasowej. W 1948 r., po przejęciu władzy przez Partię Narodową (National Party) oficjalnie rozpoczął się podział rasowy. Rasistowska i nacjonalistyczna partia wprowadziła pojęcie apartheidu na blisko 46 lat. System opierał się na dominacji białej rasy i prześladowaniu ludności niebiałej. Łamał zasady Karty Narodów Zjednoczonych i Powszechnej deklaracji praw człowieka. Mocno zakorzeniony w strukturze politycznej, społecznej i gospodarczej kraju.

Partia podczas swoich rządów podzieliła społeczeństwo na trzy kategorie względem koloru skóry: białe, czarne i kolorowe (mniejszość chińska, tajwańska i koreańska). Podczas panowania ustaliła wiele zasad i kierowała się polityką „dziel i rządź". Do najważniejszych ograniczeń należały:

- zakaz małżeństw mieszanych;
- ustawa o niemoralności (1950) – rozciągnęła dotychczasowy zakaz stosunków seksualnych między białymi a czarnoskórymi na wszelkie stosunki seksualne między białymi a przedstawicielami innych grup społeczeństwa;
- ustawa o obszarach grupowych (1950) – promowała umieszczanie czarnych i białych w oddzielnych dzielnicach mieszkalnych, skuterkiem czego były masowe przesiedlenia;
- ustawa o rezerwacji oddzielnych udogodnień (1953) – egzekwowała segregację w korzystaniu z obiektów publicznych, takich

jak transport publiczny, restauracje, kina, obiekty sportowe, toalety i plaże oznaczone specjalnymi tabliczkami tylko dla białych i osobne lokale usługowe;
– ustawa o edukacji Bantu (1953) – polityka oddzielnego szkolnictwa i programu nauczania ze względu na rasę oraz zniesienie szkół misyjnych.

Zasady te z każdym krokiem usuwały ludność czarnoskórą ze społeczeństwa. Celem systemu było podporządkowanie sobie rdzennej ludności i poniżenie jej pod względem społecznym, ekonomicznym, gospodarczym i politycznym. Partia wprowadziła własne zasady i karanie osób nieposłusznych. Represje dla ludności białej były zdecydowanie łagodniejsze niż dla czarnoskórych. Wraz z rozwojem licznych ograniczeń nasilał się opór rdzennej ludności wobec ustanowionych zasad. W 1960 r. pojawiła się fala protestów przeciwko władzy; opozycja próbowała walczyć z ograniczeniami, jednak demonstracja w Sharpeville (demonstracja przeciwko apartheidowi, która została gwałtownie stłumiona przez policję) zakończyła się drastycznie dla demonstrantów; szacuje się, że w jej trakcie zginęło około 70 osób. Wydarzenie to stało się pierwszym ogniwem walki z segregacja rasową i doprowadziło do potępienia apartheidu na globalną skalę, mimo że początkowo nie wyglądało to obiecująco. Władze wprowadziły stan wyjątkowy i pozbawiły wolności wielu przywódców, którzy byli w stanie się im sprzeciwić. Był to burzliwy okres, nielegalne formacje organizowały zamachy bombowe i skłaniały się ku stosowaniu przemocy, co doprowadziło do izolacji Afryki Południowej w stosunkach międzynarodowych. W tym samym roku ludność biała, głównie Afrykanerzy (mieszkańcy RPA i Namibii pochodzenia holenderskiego) opowiedzieli się w referendum za wprowadzeniem republiki. Tym sposobem 31 maja 1961 r. RPA stała się republiką, ale nie posiadała żadnych korzyści dla ludności niebiałej. W pełni powróciła w 1994 r., gdy kraj powoli uwalniał się spod panowania opresyjnego rządu. Jednakże wówczas konstytucja nie oferowała żadnych praw dla ludności czarnoskórej, a bierne prawo wyborcze przysługiwało tylko białym.

Na przełomie lat 60. i 70. władze RPA wprowadziły politykę tworzenia tzw. bantustanów – był to kluczowy element dyskryminacji rasowej wprowadzony przez partię, czyli obszary wyodrębnione w RPA, przeznaczone

dla zamieszkania poszczególnych grup czarnoskórej ludności, dzięki którym władza pozbawiała się odpowiedzialności za pewną część społeczeństwa, zyskując jednak tanią siłę roboczą, która musiała być posłuszna. Izolacja przyczyniła się do powstania wielu różnic językowych. W latach 70. pojawiły się próby nadania niepodległości terytorium bantustanów, uznając jako pierwsze „państwo" ludności czarnoskórej Transkei w 1976 r. Później próbowano jeszcze z 3 kolejnymi, ale społeczność międzynarodowa nie zgodziła się na uznanie suwerenności. Rok ten był dość burzliwy, protesty przeciw nauce afrikaans w Soweto spotkały się z brutalnym tłumieniem przez policję, co zapoczątkowało falę zamieszek i poważne straty gospodarcze. Lata 80. tylko pogłębiły problemy gospodarcze, wzrost przestępczości i przemoc polityczną. Od 1984 do 1994 w RPA głównymi językami były afrikaans i angielski. W 1994 r. po pierwszych demokratycznych wyborach rozpoczęły się prace nad nową konstytucją, która 4 lutego 1997 r. weszła w życie i tym samym powstały nowe przepisy podkreślające znaczenie równości językowej i praw grup etnicznych zamieszkujących te tereny. Dzięki temu ustanowiono „11 języków urzędowych, m.in. afrikaans, angielski, zulu, xhosa, tswana i sotho, a także uznano inne języki używane w kraju, w tym khoi, nama, san oraz język migowy". Konstytucja zobowiązała się do ochrony i promowania ich wszystkich w kraju.

Kluczową postacią w dążeniu do zniesienia dyskryminacji rasowej w RPA był Nelson Rolihlahla Mandela. Urodził się 18 lipca 1918 r. w Myezo, wywodził się z rodziny, która otwarcie stawiała opór holenderskim kolonistom. Jego ojciec został niesłusznie oskarżony o korupcję przez ludność białą. Mandela w 1941 r. uciekł z domu, ponieważ nie godził się na przymusowe małżeństwo. Przybył do Johannesburga i tam zaczął się interesować polityką; studiował na Uniwersytecie Witwatersrand, gdzie był jedynym czarnoskórym studentem. W 1948 r., po dojściu do władzy Partii Narodowej w RPA brał udział w licznych protestach przeciwko apartheidowi: wiązało się to z wieloma ograniczeniami w jego życiu prywatnym (brak zaliczenia studiów i uzyskania dyplomu). W 1950 r. został prezydentem Afrykańskiego Kongresu Narodowego i próbował walczyć przeciwko podziałom rasowym; za swoje działania i zdradę stanu został aresztowany w 1952 r. Walka o wolność i przeciwdziałanie przemocy spotkały się z ogromnym sprzeciwem ówczesnej władzy; został uwolniony

dopiero po 30 latach, w 1990 r. Po wyjściu z więzienia został przewodniczącym Afrykańskiego Kongresu Narodowego, a 3 lata później nagrodzony Pokojową Nagrodą Nobla. Mimo napotkanych trudności doprowadził kraj do demokratycznych i wielorasowych wyborów i sam stał się pierwszym czarnoskórym prezydentem RPA 10 maja 1994 r. Sam upadek apartheidu był też wynikiem sprzeciwu ludności niebiałej wobec systemu segregacji rasowej.

Aktualnie RPA w wyniku wydarzeń w kraju i stosowania apartheidu należy do krajów o największych nierównościach ekonomicznych na świecie. Wynika to ze słabego systemu edukacji i niskiego miejsca w światowych rankingach jakości nauczania. Próby wzmocnienia kraju nie przyniosły żadnych skutków. System apartheidu pozostawił głębokie nierówności w RPA, które do dziś utrudniają pełną odbudowę kraju.

Współcześnie pojęcie apartheidu jest używane do określania różnych form dyskryminacji na świecie. Pomimo określania tego zjawiska jako zbrodni przeciwko ludzkości przez konwencje, Statut Rzymski i zwyczajowe prawo międzynarodowe nadal jest stosowany przez reżimy w niektórych krajach. Przykładem może być segregacja rasowa w Izraelu czy w krajach afrykańskich – władze izraelskie stosują formę dyskryminacji wobec ludności palestyńskiej; ograniczenia dotyczą m.in. prawa własności nieruchomości, obywatelstwa, swobody przemieszczania się i udziału w życiu politycznym. Palestyńczycy domagają się uznania polityki Izraela za *apartheid*. Podobnie jak w kiedyś w RPA, stosuje się różne dokumenty osobiste, inne prawa pobytu. Symbolem podziału stał się mur wybudowany w 2002 r., oddzielający tereny zamieszkałe przez obie wspólnoty. Międzynarodowy Trybunał Sprawiedliwości w Hadze nazwał konstrukcję „murem apartheidu". Izrael swoją politykę „separacji" nazywa Hafrada, polega ona m.in. na braku dostępu Palestyńczyków do niektórych dróg publicznych, podleganiu prawu wojskowemu, podczas gdy żydowskich osadników obowiązuje izraelskie prawo cywilne. Izrael swoją politykę tłumaczy przede wszystkim tzw. prawem powrotu, czyli historycznie uzasadnionym prawem do odzyskania niegdyś utraconych ziem, bez względu na zastany porządek. W 2018 r. przyjęto tzw. ustawę o państwie żydowskim (Nationality Bill), która ustanowiła Izrael państwem żydowskim, tym samym rugując inne mniejszości.

W ramach apartheidu można wymienić również *apartheid* płciowy polegający na dyskryminacji płci. Określenie to wyodrębniło się w wielu artykułach

poświęconych głównie sytuacji kobiet w Afganistanie; z tego powodu wielu ekspertów porównuje obecną sytuację w kraju do formy apartheidu, definiując go jako „system rządów oparty na prawie i/lub polityce, który narzuca systematyczną segregację kobiet i mężczyzn, a także może systematycznie wykluczać kobiety z przestrzeni i sfer publicznych". Jest on niezgodny z normami prawa międzynarodowego, tak samo jak *apartheid* rasowy – w obu wspólnym czynnikiem jest dehumanizacja i usunięcie człowieczeństwa z życia społecznego oraz publicznego.

W praktyce oznacza to systemowe wykluczanie kobiet z przestrzeni publicznej, a wszystko za sprawą rządów talibów; po przejęciu przez nich władzy w latach 90. w kraju zapanował brutalny reżim, pozbawiający kobiety wielu praw, ograniczający ich możliwości edukacji pracy i aktywnego uczestniczenia w życiu społecznym. W 2001 r., kiedy doszło do obalenia władzy talibów, kraj przez kolejne dwie dekady próbował odbudować swoje instytucje demokratyczne, mimo oporu. W 2021 r. talibowie powrócili do władzy, wykorzystując moment, kiedy to nikt nie kontrolował ich kraju. Wycofanie się wojsk amerykańskich i sojuszniczych, a co za tym idzie – reżim talibów, przekreśliło postępy dokonywane od 2001 r. – obecnie Afganistan jest jednym z najniebezpieczniejszych krajów dla kobiet i dzieci, które są narażone na liczne ograniczenia i brutalne traktowanie, m.in. wprowadzono zakaz uczęszczania do szkół średnich, zakaz pracy w organizacjach pozarządowych, zakaz wyjścia bez męskiego opiekuna, zakaz wolności słowa, brak dostępu do pełnej opieki zdrowotnej, zakaz ubierania się według własnych preferencji. Zakazy obowiązujące w Afganistanie skłoniły licznych ekspertów do określania tej sytuacji mianem apartheidu płciowego. Kraj ten pozostaje również jednym z najgorszych, jeśli chodzi o wskaźnik ubóstwa i zniszczeń infrastruktury; talibowie z dnia na dzień wprowadzają nowe ograniczenia, tym samym pozbawiając kobiety istnienia w społeczeństwie.

Ustrój ten stanowi poważne naruszenie praw człowieka i jest zakazany przez prawo międzynarodowe. „Międzynarodowa konwencja o zwalczaniu i karaniu zbrodni apartheidu, przyjęta dnia 30 listopada 1973 r. rezolucją 3068 (XXVIII) Zgromadzenia Ogólnego Narodów Zjednoczonych" (Dz.U. 1976, nr 32, poz. 186).

Przemysław Mazur, Katarzyna Pabis-Cisowska, Anna Ząber

Apartheid, https://www.btselem.org/ (dostęp 2.11.2025); *Apartheid* [hasło], [w:] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/apartheid;3870281.html (dostęp 1.11.2025); *Apartheid Izraela wobec Palestyńczyków*, https://www.amnesty.org/en/latest/campaigns/2022/02/israels-system-of-apartheid/ (dostęp 1.11.2025); J. Balicki, *Afrykanerzy, Afrykanie, apartheid*, Wydawnictwo Iskry, Warszawa 1980, https://books.google.com/books? (dostęp 2.11.2025); *Dyskryminacja i pokrewne przejawy nietolerancji – apartheid w Południowej Afryce*, https://www.unic.un.org.pl/dyskryminacja/fd_apartheid.php (dostęp 2.11.2025); T. Gmerek, *Selekcyjna funkcja południowoafrykańskiego systemu edukacji w czasach apartheidu (1948–1994)*, „Nauki o Wychowaniu. Studia Interdyscyplinarne" 2018, t. 6(1), s. 89–114; *Izraelski apartheid wobec Palestyńczyków: okrutny system dominacji i zbrodnia przeciwko ludzkości*, https://www.amnesty.org.pl/izraelski-apartheid-wobec-palestynczykow-okrutny-system-dominacji-i-zbrodnia-przeciwko-ludzkosci/ (dostęp 1.11.2025); P. Juruś, M. Olender, *Zjawisko apartheidu w Republice Południowej Afryki*, Wydawnictwo Akademii Wojsk Lądowych im. Gen. Tadeusza Kościuszki, Wrocław 2021; *Konstytucja Republiki Południowej Afryki*, tłum. A. Wojtyczek-Bonnand, K. Wojtyczek, Wydawnictwo Sejmowe, Warszawa 2006, https://biblioteka.sejm.gov.pl/wp-content/uploads/2016/03/RPA.pdf (dostęp 1.11.2025); P. Mazur, *Druzowie w armii izraelskiej – od braterstwa krwi do asymilacji*, „Historia i Polityka" 2020, t. 35, s. 61–76; M.B. Mhlauli, S.R. Mokotedi, *Understanding apartheid in South Africa through the racial contract*, „International Journal of Asian Social Science" 2015, vol. 5(4);*Nelson Rolihlahla Mandela – 1988 r., Republika Południowej Afryki*, https://www.europarl.europa.eu/sakharovprize/pl/nelson-rolihlahla-mandela-1988-r.-republ/products-details/20200330CAN54162 (dostęp 2.11.2025).

ARCHITEKTURA BEZPIECZEŃSTWA – termin wykorzystywany w dziedzinie nauk społecznych, w dyscyplinie nauk o bezpieczeństwie na określenie instytucjonalnej, prawnej i funkcjonalnej struktury systemów bezpieczeństwa, która obejmuje podmioty, relacje, procedury i mechanizmy współpracy między podmiotami odpowiedzialnymi za utrzymanie bezpieczeństwa w różnych wymiarach funkcjonowania danego podmiotu. Architektura bezpieczeństwa to spójny wielowarstwowy układ zasad, instytucji, procesów, technologii i norm, których celem jest:

- zapobieganie zagrożeniom;
- ich wczesne wykrywanie;
- reagowanie;
- odbudowa (*resilience*).

Nie ma jednej akceptowalnej powszechnie definicji tego terminu, jednak można wskazać kilka istotnych interpretacji.

Autorzy opracowania zbiorowego pt. *The future European security architecture* definiują architekturę bezpieczeństwa jako „zbiór środków ograniczających podatności systemu bezpieczeństwa (określona przez strukturę i interakcje) oraz zwiększających jego odporność na wstrząsy". Zazwyczaj w dyskursie publicznym temat architektury bezpieczeństwa pojawia się wyraźniej w momentach przełomowych, kiedy istniejący porządek zostaje „zburzony" czy „obalony", np. po 1989 r., po aneksji Krymu lub po zbrojnej inwazji Rosji na Ukrainę w 2022 r. Ondřej Ditrych i Martin Laryš postrzegają architekturę bezpieczeństwa jako „część porządku regionalnego, który dotyczy zarządzania bezpieczeństwem kompleksu państw, których interesy bezpieczeństwa narodowego nie mogą być realistycznie rozpatrywane oddzielnie". Ci sami autorzy wymieniają sześć typów idealnych architektury bezpieczeństwa.

1. Brak architektury, który jest charakterystyczny dla systemu nieustrukturyzowanego, składającego się z nieistniejących lub słabych państw.
2. Równowaga sił.
3. Porozumienie oparte na akceptacji zasad ograniczających realizację własnych interesów, podstawowym zaufaniu do mechanizmów rozwiązywania konfliktów oraz braku rewizjonistycznych planów wśród członków wykazujących zdolność do wprowadzania nieformalnych porozumień bezpieczeństwa.
4. Architektura bezpieczeństwa zbiorowego, dodająca wspólną determinację do zbiorowego powstrzymywania agresji jednego członka wobec drugiego, wbudowana w strukturę odporności.
5. Społeczność bezpieczeństwa oparta na trwałych oczekiwaniach, że konflikty będą rozwiązywane pokojowo oraz kształtująca strategie i strukturę zdolności podmiotów w tym celu.
6. Hegemonia definiowana przez obecność jednego dominującego podmiotu, który działa jako rozjemca i skutecznie neguje suwerenność operacyjną innych.

Architektura bezpieczeństwa jest pojęciem wieloznacznym, wielowymiarowym. Termin nawiązuje do metafory architektury jako planu czy

konstrukcji, która jest wielowarstwowa i dynamiczna, a poszczególne elementy pełnią określone funkcje, co pozwala zapewnić stabilność systemu bezpieczeństwa. W literaturze przedmiotu termin jest wykorzystywany w wielu kontekstach i obejmuje zarówno bezpieczeństwo narodowe, jak i m.in. międzynarodowe, militarne, społeczne, informacyjne (w tym cyberbezpieczeństwo), gospodarcze czy środowiskowe.

Pojęcie opisuje nie tylko podmioty bezpieczeństwa, ale także relacje i powiązania, zasady współdziałania, kompetencje i ich prawne uwarunkowania, a także procesy adaptacji do zmian w środowisku bezpieczeństwa. W naukach społecznych architektura bezpieczeństwa ma charakter analityczny i pomaga uchwycić dynamikę zmian w środowisku bezpieczeństwa na wielu poziomach: lokalnym, regionalnym, państwowym, międzynarodowym, np. po 2022 r. architektura bezpieczeństwa na poziomie międzynarodowym uległa zmianie za sprawą wejścia Szwecji i Finlandii do NATO, inicjatyw regionalnych planów obronnych czy programów Unii Europejskiej dedykowanych regionalnemu przemysłowi obronnemu. Miało to miejsce z uwagi na pełnoskalową wojnę Rosji z Ukrainą, co spowodowało trwałą konfrontację z Rosją oraz powrót odstraszania. Chęć zmian w międzynarodowej architekturze bezpieczeństwa, która powstała po tzw. zimnej wojnie, sygnalizował już prezydent Federacji Rosyjskiej Dmitrij Miedwiediew w Berlinie w 2008 r., przedstawiając rosyjskie propozycje w postaci projektu traktatu o bezpieczeństwie europejskim, mające na celu ograniczenie roli NATO i stworzenie warunków do odbudowy strefy wpływów Rosji. Dwa miesiące później Rosja przeprowadziła zbrojną interwencję w Gruzji, uzasadniając ją koniecznością ochrony mieszkańców Osetii Południowej i Abchazji, w 2014 r. dokonała aneksji Krymu, ponownie powołując się na potrzebę obrony ludności rosyjskiej zamieszkującej te obszary, a w 2022 r. Federacja Rosyjska rozpoczęła pełnoskalową wojnę w Ukrainie. Te wydarzenia pokazują, że rosyjskie koncepcje budowy nowej architektury bezpieczeństwa mogą wiązać się z groźbą użycia siły lub jej realnym zastosowaniem, co prowadzi do naruszenia integralności terytorialnej innych państw.

Istnieje kilka poziomów architektury bezpieczeństwa:

– poziom strategiczny odpowiadający na pytanie: „Co chronimy i dlaczego?", do którego należą:

- doktryny;
- strategie bezpieczeństwa;
- polityki narodowe/korporacyjne;
- ramy prawne;

– poziom operacyjny odpowiadający na pytanie: „Kto i jak reaguje?", do którego należą:

- instytucje;
- procedury;
- koordynacja międzysektorowa;
- zarządzanie kryzysowe;

– poziom techniczny/taktyczny odpowiadający na pytanie: „Jakimi narzędziami?", do którego należą:

- systemy IT;
- ochrona fizyczna;
- monitoring;
- środki kontroli dostępu.

W kontekście bezpieczeństwa narodowego architektura bezpieczeństwa obejmuje układ instytucji odpowiedzialnych za bezpieczeństwo i porządek publiczny, w tym ochronę terytorium, ludności czy infrastruktury. Architektura bezpieczeństwa obejmuje instytucje na poziomie strategicznym, operacyjnym i taktycznym, a jej kształt określają dokumenty państwowe w zakresie bezpieczeństwa, np. w Polsce – strategia bezpieczeństwa narodowego z 2020 r. Oprócz instytucji w tradycyjnym ujęciu architektura bezpieczeństwa obejmuje prawo oraz procedury, a także mechanizmy koordynacji. Do konieczności wpływu na kształt przyszłej architektury bezpieczeństwa europejskiego przez Trójkąt Weimarski odnoszą się wprost Rekomendacje do strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej przekazane przez prezydenta Rzeczypospolitej Polskiej Radzie Ministrów w lipcu 2024 r. Dodatkowo w dokumencie znajduje się fragment dotyczący średnio- i długofalowej perspektywy, kiedy „niezbędne będzie zredefiniowanie europejskiej architektury bezpieczeństwa, której kluczowym elementem powinny być nowe środki budowy zaufania i kontroli, zapewniające rzeczywistą kontrolę zbrojeń oraz przejrzystość ćwiczeń wojskowych w Europie".

W odniesieniu do bezpieczeństwa międzynarodowego architektura bezpieczeństwa opisuje układ instytucji, sojuszy oraz prawo i procedury w zakresie zapewnienia ładu międzynarodowego oraz regulujących użycie siły. Obejmuje ona organizacje międzynarodowe, jak np. ONZ, NATO, Unię Europejską, OBWE. W tym kontekście analizuje się układ sił, efektywność mechanizmów współpracy, zdolność do adaptacji wobec nowych zagrożeń. Architektura bezpieczeństwa pozwala na analizę trwałości i odporności systemów bezpieczeństwa w obliczu zmian geopolitycznych.

Analiza architektury bezpieczeństwa jest także wykorzystywana do poszczególnych rodzajów bezpieczeństwa, np. gospodarczego. W tym zakresie obejmuje instytucje i mechanizmy zapewniające stabilność ekonomiczną i odporność państwa na kryzysy finansowe, surowcowe czy logistyczne. Dotyczy np. polityki fiskalnej, bezpieczeństwa żywnościowego, ochrony łańcuchów dostaw oraz strategicznych sektorów gospodarki. Szczególnym podsystemem jest architektura bezpieczeństwa energetycznego obejmująca systemy dostaw energii, dywersyfikację źródeł, magazynowanie surowców oraz współpracę międzynarodową. Wskazuje się, że Stany Zjednoczone Ameryki również odchodzą od powojennego porządku, zwłaszcza w zakresie gospodarczym i militarnym.

Architektura bezpieczeństwa systemów funkcjonuje także w zakresie bezpieczeństwa informacyjnego, w tym cyberbezpieczeństwa. W tym zakresie obejmuje projektowanie, rozwój i zarządzenie systemami oraz procesami bezpieczeństwa w organizacji. Oznacza uporządkowany zbiór zasad, norm, procedur i rozwiązań technicznych, których zadaniem jest ochrona zasobów informacyjnych przed zagrożeniami, a także zapewnienie poufności (ochrona przed dostępem osób nieuprawnionych, ogół działań mających na celu zapewnienie, że dane są poufne lub prywatne), integralności (ochrona przed niezautoryzowaną modyfikacją danych, polega na upewnieniu się, że dane są godne zaufania i nie były poddawane manipulacji) i dostępności (zapewnienie, że informacje i systemy są dostępne, gdy są potrzebne) danych oraz przestrzeganie obowiązujących regulacji prawnych i standardów. Stanowi ona podstawę efektywnego zarządzania ryzykiem w obszarze technologii informacyjnych. Architektura bezpieczeństwa składa się z takich elementów, jak infrastruktura techniczna, oprogramowanie, polityki i procedury, ludzie oraz procesy.

Architektura bezpieczeństwa ma na celu ochronę zasobów informacyjnych, zarządzanie ryzykiem, zgodność z regulacjami oraz wsparcie dla ciągłości działania organizacji. Stanowi ona fundament bezpieczeństwa organizacji w warunkach rosnącej złożoności technologicznej oraz rozwoju cyberprzestępczości.

Architektura bezpieczeństwa to nie zbiór narzędzi, lecz świadomie zaprojektowany ekosystem ochrony. Oznacza to, że kryzys w jednym obszarze może przenosić się na pozostałe, co daje tzw. efekt domina, synergii. Druga kluczowa cecha to adaptacyjność, co oznacza, że architektura bezpieczeństwa ewoluuje wraz z pojawianiem się nowych zagrożeń, technologii i zmian geopolitycznych, co czyni ją dynamiczną i podatną na rekonstrukcję.

Agnieszka Warchoł

Co to jest architektura bezpieczeństwa?, https://nflo.pl/slownik/architektura-bezpieczenstwa/ (dostęp 12.12.2025); H. Crebo-Rediker, *Designing Resilience: A New G7 Architecture for Economic Security*, https://www.cfr.org/article/designing-resilience-new-g7-architecture-economic-security (dostęp 12.12.2025); O. Ditrych, M. Laryš, *What can European security architecture look like in the wake of Russia's war on Ukraine?*, https://www.tandfonline.com/doi/full/10.1080/09662839.2024.2347221#abstract (dostęp 12.12.2025); *The future European security architecture. Dilemmas for EU strategic autonomy*, https://www.europarl.europa.eu/RegData/etudes/STUD/2025/765785/EPRS_STU(2025)765785EN.pdf (dostęp 12.12.2025); Rekomendacje do strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej, 2024; *Russia Offers Vision of a New Global Security Architecture*, https://pism.pl/publications/russia-offers-vision-of-a-new-global-security-architecture (dostęp 13.12.2025); Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, 2020.

AUTODESTRUKCJA – autoagresja, zachowania autodestrukcyjne to złożony, wielowymiarowy konstrukt psychologiczny obejmujący zespół zachowań, myśli, motywacji, przeżyć emocjonalnych oraz procesów psychologicznych, które ukierunkowują jednostkę na działania zwiększające ryzyko szkody lub faktycznie szkodzące jej zdrowiu fizycznemu, psychicznemu lub społecznemu, prowadząc do pogorszenia funkcjonowania oraz naruszenia integralności biologicznej, psychicznej i społecznej. Zjawisko to może być realizowane świadomie lub nieświadomie, bezpośrednio lub

pośrednio, i obejmuje zarówno jawne formy autoagresji, takie jak samouszkodzenia i próby samobójcze, jak i pośrednie formy zachowań ryzykownych oraz uzależnień, które nie zawsze mają charakter intencjonalny, lecz w perspektywie długofalowej prowadzą do degradacji dobrostanu jednostki, a w skrajnych przypadkach – zagrożenia życia.

Każda jednostka funkcjonuje w świadomości, że ciało, z jednej strony, stanowi szczególny obiekt troski związanej zarówno z dbałością o zdrowie, jak i z normami estetycznymi, z drugiej natomiast – może być źródłem zaniedbań oraz aktów przemocy wobec samego siebie. Ciało pełni fundamentalną rolę w kształtowaniu tożsamości jednostki, będąc jednocześnie nośnikiem stanów psychicznych oraz napięć emocjonalnych. Zjawisko to można interpretować jako częściowo powiązane z rosnącą częstotliwością korzystania z zabiegów chirurgii plastycznej, motywowaną w niektórych przypadkach autodestrukcyjnymi tendencjami jednostek. Autodestrukcja stanowi przede wszystkim konsekwencję złożonych problemów psychicznych, charakterystycznych dla jednostek funkcjonujących w stanie nasilonego napięcia emocjonalnego.

W literaturze przedmiotu zachowania autodestrukcyjne klasyfikuje się najczęściej jako bezpośrednie lub pośrednie, w zależności od stopnia intencjonalności oraz klarowności związku pomiędzy działaniem a powstałą szkodą. Bezpośrednie zachowania autodestrukcyjne cechują się świadomym i intencjonalnym naruszaniem integralności ciała, przy jednoznacznym zamiarze wyrządzenia sobie krzywdy, i obejmują m.in. próby samobójcze oraz różne formy samouszkodzeń.

Pośrednie zachowania autodestrukcyjne dotyczą natomiast działań, w których jednostka nie dąży bezpośrednio do samouszkodzenia, lecz uzyskania określonych korzyści psychologicznych lub sytuacyjnych, przy jednoczesnym ignorowaniu długofalowych, niekorzystnych skutków dla zdrowia i funkcjonowania. Do tej kategorii zalicza się m.in.:

- próby samobójcze;
- celowe uszkadzanie ciała;
- chroniczne zaniedbywanie własnych potrzeb;
- uzależnienie od alkoholu;
- uzależnienie od innych substancji psychoaktywnych;
- nieadaptacyjne strategie regulacji emocji;

- zachowania charakterystyczne dla zaburzeń odżywiania;
- podejmowanie zachowań ryzykownych, np. nadmiernie szybka jazda samochodem czy zachowania seksualne wysokiego ryzyka;
- obsesyjną aktywność fizyczną;
- uzależnienia behawioralne;
- zjawisko wyuczonej bezradności;
- samowolne przerywanie farmakoterapii;
- niewłaściwe stosowanie leków psychotropowych.

Jedną z form autodestrukcji jest autoagresja, która odnosi się do zachowań, w których agresja zostaje skierowana przeciwko własnej osobie, prowadząc do naruszenia zdrowia fizycznego lub psychicznego jednostki. Najczęściej wyróżnia się autoagresję werbalną oraz niewerbalną. Pierwsza przejawia się w utrwalonych negatywnych przekonaniach na temat własnej osoby, obniżonej samoocenie oraz nasilonej samokrytyce. Z kolei druga odnosi się do zachowań polegających na intencjonalnym naruszaniu integralności fizycznej ciała i stanowi formę jawnych działań autodestrukcyjnych, podejmowanych najczęściej w celu regulacji napięcia emocjonalnego.

Samouszkodzenia stanowią jedną z najczęściej opisywanych form autoagresji oraz zachowań autodestrukcyjnych i odnoszą się do intencjonalnych działań polegających na naruszaniu integralności własnego ciała. Zachowania te nie są zazwyczaj motywowane zamiarem samobójczym ani bezpośrednią chęcią odebrania sobie życia, lecz pełnią przede wszystkim funkcję regulacji emocjonalnej, redukcji napięcia psychicznego oraz radzenia sobie z trudnymi stanami psychicznymi. W literaturze przedmiotu samouszkodzenia definiowane są jako społecznie nieakceptowany wzorzec zachowania, polegający na celowym zadawaniu sobie bólu lub powodowaniu uszkodzeń ciała, który stanowi relatywnie niewielkie zagrożenie dla życia, a jednocześnie może pełnić funkcję komunikacyjną, sygnalizując otoczeniu obecność doświadczanego dyskomfortu psychicznego. Do najczęściej obserwowanych form samouszkodzeń należą:

- nacinanie skóry, przede wszystkim w obrębie ramion i dłoni;
- nacinanie skóry kończyn dolnych, twarzy oraz tułowia;
- przypadki poparzeń;

- zadawanie sobie uderzeń bądź celowego uderzania ciałem w twarde powierzchnie;
- drapanie, nakłuwanie, gryzienie;
- wyrywanie włosów i rzęs;
- intensywne pocieranie skóry prowadzące do uszkodzenia naskórka;
- połykanie ostrych przedmiotów;
- spożywanie substancji o charakterze szkodliwym;
- podejmowanie ryzyka podczas stosunków seksualnych.

Zachowania te pozostają uwarunkowane aktualnym stanem emocjonalnym jednostki oraz dostępnością określonych środków. Samouszkodzenia należy analizować w kontekście innych skłonności o jednoznacznie autodestrukcyjnym charakterze, takich jak zachowania parasamobójcze, zaburzenia odżywiania, nadużywanie substancji psychoaktywnych oraz zaburzenia pozorowane. Wspólną cechą wymienionych form autoagresji jest ich zróżnicowany, lecz zawsze obecny potencjał szkodliwości dla zdrowia jednostki. Jednocześnie samouszkodzenia odróżniają się od innych zachowań destrukcyjnych stopniem zagrożenia życia, społeczną interpretacją, zakładanym celem, a także poziomem bezpośredniości i natychmiastowości powstających obrażeń.

Etiologia samouszkodzeń ma charakter wielowymiarowy i obejmuje pięć głównych obszarów: środowiskowy, biologiczny, poznawczy, afektywny oraz behawioralny. Wymiar środowiskowy odnosi się do doświadczeń rodzinnych i indywidualnych, zarówno przeszłych, jak i aktualnych, w tym ekspozycji na zaburzenia psychiczne, przemoc oraz zachowania autodestrukcyjne w otoczeniu. Wymiar biologiczny obejmuje współwystępowanie zaburzeń psychicznych i somatycznych. Wymiar poznawczy dotyczy dysfunkcyjnych schematów myślenia i interpretacji zdarzeń. Wymiar afektywny wiąże się z nasilonymi, trudnymi do regulacji emocjami. Wymiar behawioralny obejmuje zachowania poprzedzające i następujące po samouszkodzeniu, związane z redukcją napięcia.

Istotnym czynnikiem sprzyjającym występowaniu zachowań autoagresywnych jest wpływ mediów, które poprzez ich normalizowanie bądź atrakcyjne przedstawianie mogą przyczyniać się do ich utrwalania. Prezentowanie obrazów autoagresji w filmach, serialach, literaturze oraz

mediach społecznościowych może prowadzić do postrzegania tych zachowań jako akceptowalnych, co jest szczególnie istotne w kontekście oddziaływania na młodzież. Samouszkodzenia można również uznać za czynnik ryzyka samobójczego.

Najczęściej wskazywanymi czynnikami wyzwalającymi samouszkodzenia są doświadczenia odrzucenia, poczucie bezradności, silne emocje takie jak złość i poczucie winy, a także ponowne uaktywnienie traumy związanej z nadużyciem seksualnym w dzieciństwie. Podejmowanie samouszkodzeń bywa również traktowane przez jednostki jako sposób radzenia sobie z trudnymi doświadczeniami. Jest to także swoistego rodzaju mechanizm obronny. Zażywanie substancji psychoaktywnych może dodatkowo ułatwiać tłumienie lub znieczulanie bolesnych wspomnień związanych z doświadczoną traumą. Samouszkodzenia prowadzą do chwilowego obniżenia trudnego do zniesienia napięcia emocjonalnego, uczucia pustki lub objawów depresyjnych, a także umożliwiają rozładowanie nagromadzonej złości. Zachowania te mogą również sprzyjać przywróceniu poczucia realności, kontroli nad własnym ciałem oraz subiektywnego poczucia wpływu na otoczenie. Dla niektórych osób stanowią one sposób zagłuszania cierpienia psychicznego lub przekształcania go w ból fizyczny, który bywa postrzegany jako bardziej znośny. Samouszkodzenia mogą także pełnić funkcję komunikacyjną, dostarczając poczucia wyjątkowości, zwracając uwagę otoczenia lub redukując poczucie wyobcowania. W niektórych przypadkach są one związane z próbą podniesienia własnej atrakcyjności fizycznej lub społecznej. Przyjmuje się, że samouszkodzenia stanowią długofalowy i nieadaptacyjny sposób regulowania trudnych emocji. W odróżnieniu od zachowań samobójczych, nie są one ukierunkowane na odebranie sobie życia, lecz pełnią funkcję regulacyjną i mają na celu jego ochronę oraz przetrwanie jednostki. Podkategorią samouszkodzeń są samookaleczenia, które odnoszą się do konkretnych, bezpośrednich form fizycznego uszkadzania ciała.

Samookaleczanie stanowi działanie intencjonalne, które nie zachodzi przypadkowo; jednostka podejmuje je z własnej woli, choć w niektórych przypadkach może być realizowane przy udziale innych osób. W odróżnieniu od samouszkodzeń, w samookaleczaniach można wyróżnić dwie zasadnicze kategorie praktyk określanych jako modyfikacje lub

udoskonalanie ciała. Pierwszą z nich stanowią zachowania społecznie aprobowane, ukierunkowane na osiągnięcie kulturowo ukształtowanych standardów atrakcyjności fizycznej, takie jak zabiegi chirurgii estetycznej, np. powiększanie piersi, procedury kosmetyczne, *body piercing*, usuwanie owłosienia, wybielanie skóry czy prostowanie włosów. Choć praktyki te mogą wiązać się z doświadczaniem bólu lub naruszeniem integralności cielesnej, są powszechnie akceptowane społecznie i nie klasyfikuje się ich jako samouszkodzenia, mimo iż na poziomie formalnym mogą wykazywać pewne podobieństwa do zachowań autoagresywnych. Drugą kategorię stanowią modyfikacje ciała, które nie są motywowane dążeniem do estetycznej atrakcyjności, lecz pełnią funkcję ekspresyjną, opozycyjną lub identyfikacyjną, służąc manifestowaniu sprzeciwu, wywoływaniu reakcji otoczenia bądź podkreślaniu przynależności do określonych grup społecznych. Do tego typu praktyk zalicza się m.in. golenie głowy, rozległe tatuowanie ciała czy umieszczanie kolczyków w nietypowych miejscach. Zachowania te niosą ze sobą znaczenie symboliczne, często powiązane z doświadczaniem bólu, próbą demonstracji wytrzymałości i odwagi, a niekiedy także z postawami autoagresywnymi lub negatywnym stosunkiem do własnego ciała. W tym sensie praktyki te mogą wykazywać podobieństwo do samookaleczania, gdyż stanowią formę ekspresji złości, potrzeby kontroli oraz afirmacji własnej tożsamości i pozycji społecznej.

Zgodnie z najnowszą klasyfikacją diagnostyczną Amerykańskiego Towarzystwa Psychiatrycznego DSM-5 Diagnostic and Statistical Manual of Mental Disorders samookaleczenia definiowane są jako społecznie nieakceptowane celowe uszkadzanie własnego ciała prowadzące do wystąpienia bólu lub naruszenia integralności fizycznej, podejmowane w celu regulacji lub redukcji doświadczanego dyskomfortu psychicznego. Zachowania te mogą być rozumiane dwojako: po pierwsze, jako objaw towarzyszący różnym zaburzeniom psychicznym, w tym emocjonalnym, rozwojowym oraz osobowości o zróżnicowanej etiologii, po drugie, jako odrębna jednostka nozologiczna określana mianem samookaleczeń bez intencji samobójczych Non-Suicidal Self-Injury (NSSI). Ponadto w klasyfikacji DSM-5 uwzględniono szczegółowe kryteria diagnostyczne

umożliwiające rozpoznanie tego rodzaju zachowań jako odrębnej kategorii klinicznej.

Autodestrukcja, obejmująca zachowania takie jak samookaleczanie czy próby samobójcze, pozostaje w sferze zainteresowania prawa przede wszystkim ze względu na obowiązek państwa w zakresie ochrony życia i zdrowia jednostki. W większości systemów prawnych samouszkodzenia nie stanowią czynu karalnego, jednakże zachowania te uzasadniają interwencję medyczną lub psychologiczną, zwłaszcza w sytuacjach zagrożenia życia. Prawo reguluje także odpowiedzialność osób trzecich w przypadku podżegania do samookaleczeń lub samobójstwa, a w odniesieniu do dzieci i osób małoletnich nakłada szczególne obowiązki opiekuńcze. Dodatkowo regulacje prawne określają obowiązki placówek medycznych i terapeutów w zakresie udzielania pomocy osobom przejawiającym zachowania autodestrukcyjne, dopuszczając interwencje ograniczające autonomię pacjenta w sytuacjach bezpośredniego zagrożenia życia. W ten sposób prawo pełni funkcję prewencyjno-ochronną wobec jednostek przejawiających tendencje autodestrukcyjne, równocześnie definiując granice odpowiedzialności osób trzecich i instytucji społecznych.

Dariusz Hybś

G. Babiker, L. Arnold, *Autoagresja mowa zranionego ciała*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2002; A. Baranowska, *Zachowania autodestrukcyjne wśród młodzieży*, „Pedagogika Społeczna" 2015, nr 4(58); K. Bąkowicz, *Sposób przekazywania informacji o samobójstwie w polskich mediach o najszerszym zasięgu. Studium przypadku Niebieskiego Wieloryba*, [w:] *Autodestrukcja. Sytuacje graniczne we współczesnej kulturze*, E. Rudnicka, H. Witkowska (red.), Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2020; P. Gałecki, M. Pilecki, J. Rymaszewska, A. Szulc, S. Sidorowicz, J. Wciórka, *Kryteria Diagnostyczne Zaburzeń Psychicznych DSM-5*, Edra Urban & Partner, Wrocław 2018; B. Hołyst, *Zagrożenia ładu społecznego (2)*, Wydawnictwo Naukowe PWN, Warszawa 2013; D. Jęczmińska, *Blizny, które mówią więcej niż słowa. Samouszkodzenia nastolatków*, Wydawnictwo Psychologiadziecka.org, Warszawa 2025; D. Kubacka-Jasiecka, *Agresja i autodestrukcja z perspektywy obronno-adaptacyjnych dążeń Ja*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006; K. Kucharska, *Zdrowie psychiczne mężczyzn. Pułapki autodestrukcji*, Wydawnictwo Naukowe PWN SA, Warszawa 2025; S. Michałowska, *Autoagresja w teorii i praktyce*

psychologicznej, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2025; A. Suchańska, *Przejawy i uwarunkowania psychologiczne pośredniej autodestruktywności*, Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza w Poznaniu, Poznań 1998; H. Witkowska, *Obraz listu pożegnalnego i samobójcy w filmie fabularnym*, [w:] *Autodestrukcja. Sytuacje graniczne we współczesnej kulturze*, E. Rudnicka, H. Witkowska (red.), Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2020.

B

BAŁTYCKA AKADEMIA OBRONY (ang. Baltic Defence College, BALTCEFCOL) – została założona w 1999 r. przez 3 państwa bałtyckie, tj. Litwę, Łotwę i Estonię. Jest ona placówką edukacyjną i szkoleniową, akredytowaną przy Organizacji Paktu Północnoatlantyckiego (NATO). Oferuje kursy (poziom 3 i 4) dla oficerów, podoficerów, a także urzędników państwowych z państw bałtyckich, ich sojuszników i partnerów. Jest obecnie jedyną instytucją w Europie kontynentalnej, która świadczy profesjonalną edukację wojskową (*professional military education*, PME) w języku angielskim. Oprócz zapewniania wiedzy na najwyższym poziomie misją BALTDEFCOL jest także kształcenie wojskowych i cywilów, a także opracowywanie i realizowania programów edukacyjnych na wysokim poziomie operacyjnym i strategicznym, by spełniały one oczekiwania odbiorców. Ponadto BALTDEFCOL angażuje się w badania i działalność akademicką związaną z polityką bezpieczeństwa i obrony w dziedzinie profesjonalnej edukacji wojskowej, koncentrując się przede wszystkim na regionach Morza Bałtyckiego i Rosji, a także zwracając uwagę na znaczenie relacji transatlantyckich dla państw regionu. Instytucja ta kładzie również nacisk na wzmocnienie współpracy międzynarodowej poprzez stosowanie

standardów i procedur NATO oraz prowadzenie edukacji w języku angielskim na potrzeby państw sojuszniczych i partnerów.

W skład BALTDEFCOL wchodzą 4 wydziały. Wydział Studiów Wojskowych (Department of Military Studies, DMS) jest największym z nich, zatrudnia czynnych, jak i emerytowanych oficerów wojskowych, którzy posiadają specjalistyczną wiedzę w danej dziedzinie, zwłaszcza w zakresie strategii wojskowej, sztuki wojennej, operacji specjalnych, sił lądowych, sił powietrznych, sił morskich oraz historii wojskowości. Odpowiadają oni za kształcenie w ramach takich szkoleń, jak Kurs Dowodzenia Połączonego i Sztabu Generalnego (The Joint Command and General Staff Course, JCGSC) oraz Kurs dla Urzędników Służby Cywilnej (Civil Servants Course, CSC). Wydział ten nadzoruje również program ćwiczeń wojskowych BALTDEFCOL oraz międzynarodowe wizyty studyjne.

Kadra wydziału pozostaje zaangażowana w debatę publiczną na temat kwestii bezpieczeństwa i obrony w regionie Morza Batyckiego m.in. poprzez działalność publikacyjną. Kolejnym wydziałem BALTDEFCOL jest Wydział Studiów nad Przywództwem i Zarządzaniem (Department of Leadership and Management Studies, DLMS); w jego skład wchodzą oficerowie wojskowi posiadający specjalistyczną wiedzę z zakresu przywództwa i zarządzania obronnością. Zajmują się głównie kształceniem w trakcie JCGSC oraz CSC; odpowiadają za to, by kursanci nabyli wraz z ich zakończeniem umiejętności przywódcze oraz zarządzania. Kadra wydziału prowadzi także zajęcia dydaktyczne na studiach magisterskich.

Istotny w strukturze organizacyjnej BALTDEFCOL jest także Wydział Studiów Politycznych i Strategicznych (Department of Political and Strategic Studies). Rolą pracowników tej jednostki organizacyjnej jest prowadzenie zajęć na wszystkich etapach kształcenia w BALTDEFCOL. Odpowiadają zasadniczo za nauczanie krytycznego myślenia i komunikacji, a także zdobycie przez słuchaczy i studentów wiedzy z zakresu bezpieczeństwa międzynarodowego oraz prawa międzynarodowego. Kadra zatrudniona na tym Wydziale ma za zadanie również prowadzić badania naukowe, co wiąże się z uczestnictwem w konferencjach naukowych o zasięgu krajowym i międzynarodowym oraz w opracowywaniu strategii na szczeblu krajowym i europejskim.

Do chwili obecnej pracownicy Wydziału opublikowali wiele prac z zakresu stosunków międzynarodowych, bezpieczeństwa międzynarodowego, bezpieczeństwa europejskiego i bałtyckiego, a także spraw strategicznych, kwestii wojskowych, konfliktów zbrojnych, prawa międzynarodowego i historii powszechnej. Jeśli chodzi o Wydział Wsparcia (Department of Support), to jest on jednostką, której głównym celem jest zapewnienie sprawnego funkcjonowania działań edukacyjnych i wydarzeń organizowanych przez BALTDEFCOL. Pełni on zatem rolę wspomagającą wszystkie funkcje uczelni, do których należą m.in. obsługa dokumentów i administracja, wsparcie techniczne i logistyczne, konserwacja i modernizacja sprzętu, realizacja budżetu, księgowość, a także dbanie o wysoką jakość środowiska nauki i pracy.

Generalnie rzecz ujmując, od pracowników tego Wydziału oczekuje się, że będą oni zaangażowani w zwiększanie wydajności i skuteczności uczelni. Na czele BALTDEFCOL stoi komendant – obecnie jest nim pochodzący z Litwy generał brygady Alvydas Šiuparis, zaś jego zastępcą – pochodzący z Wielkiej Brytanii pułkownik Jonathan Huxley. Pozostałe osoby zasilające grono kadry kierowniczej wywodzą się z Litwy, Łotwy i Estonii.

Jak już wspomniano, podstawową działalnością BALTDEFCOL jest edukacja. Jedynym programem studiów związanym z działalnością BALTDEFCOL jest magisterski oferowany słuchaczom kursu JCGSC – po jego ukończeniu osoby biorące w nim udział mogą podjąć naukę na studiach magisterskich, na kierunku przywództwo wojskowe i bezpieczeństwo (*military leadership and security*), które trwają półtora roku i są prowadzone w języku angielskim przez Narodową Akademię Obrony Łotwy. Nauka jest bezpłatna, natomiast mogą ją odbyć osoby, które posiadają tytuł licencjata lub jego ekwiwalent. Pozostała oferta edukacyjna BALTDEFCOL zasadza się na krótkoterminowych kursach i szkoleniach. Jednym z nich jest wspomniany JCGSC.

Celem tego kursu jest zapewnienie profesjonalnego kształcenia wojskowego ukierunkowanego na poziom operacyjny, tak by przygotować wyższych rangą oficerów i wybranych urzędników państwowych do pracy w środowisku międzynarodowym, i tym samym, by mogli oni sprostać złożonym wyzwaniom bezpieczeństwa z perspektywy bałtyckiej

i euroatlantyckiej. Z tego też względu kurs opiera się na różnych metodach edukacyjnych, tak by łączyć wiedzę teoretyczną z praktyczną. Tę oferują nie tylko wykładowcy zatrudnieni w BALTDEFCOL, lecz również eksperci zewnętrzni. Kursanci przez 10 miesięcy uczestniczą zatem w seminariach, wykładach, ćwiczeniach i wizytach studyjnych, dziennie spędzając w sali wykładowej średnio 6 godzin dydaktycznych. Z kolei dzienna praca indywidualna studentów wynosi około 3 godzin i 5 godzin – w weekendy. JCGSC obejmuje 13 modułów nauczania, dwie wizyty studyjne, a także opracowanie pracy badawczej, która stanowi efekt dziesięciomiesięcznej edukacji i łączy wiedzę teoretyczną z praktyką.

Projekty badawcze dotyczą przede wszystkim zarządzania operacyjnego i strategicznego. Studenci zyskują przygotowanie do napisania tego typu prac poprzez udział we wspomnianych modułach nauczania, które obejmują zróżnicowaną problematykę – dotyczą m.in. przywództwa i dowodzenia, bezpieczeństwa i strategii, planowania i zarządzania obronnością, zarządzania projektami, prawem operacyjnym, planowania na poziomie operacyjnym, zarządzania współczesnymi kryzysami, komunikacją medialną, innowacjami i technologią wojskową. Należy podkreślić, że w kursie może uczestniczyć tylko kadra wojskowa wysokiego szczebla; tym samym, aby zostać uczestnikiem JCGSC, należy posiadać stopień majora (OF-3) lub podpułkownika (OF-4) w wojskowych siłach powietrznych, w wojsku lądowym lub też w siłach specjalnych albo komandora porucznika (OF-3) lub komandora (OF-4) w marynarce wojennej.

Poza tym uczestnicy kursu muszą mieć udokumentowane doświadczenie w zakresie przywództwa, wykazywać potencjał awansowy, a także biegłość w zakresie operacji na poziomie batalionu/eskadry oraz dogłębną znajomość połączonych rodzajów sił zbrojnych.

Uczestnicy z państw NATO muszą posiadać poświadczenie bezpieczeństwa NATO Tajne (Secret), natomiast spoza NATO, tj. z państw Partnerstwa dla Pokoju – Tajne (PfP Secret). Przyszli kursanci powinni wykazać się również biegłą znajomością obsługi komputera, zwłaszcza środowiska Microsoft, a także języka angielskiego. Muszą również spełniać wymagania fizyczne i medyczne adekwatne do sił zbrojnych poszczególnych państw. Drugim z istotnych kursów organizowanych przez BALTDEFCOL jest CSC. Pierwsza jego edycja miała miejsce w 2001 r. i dotyczyła wyzwań

związanych z transformacją instytucji i polityki obronnej w wymiarach krajowym i międzynarodowym.

Celem kursu jest umożliwienie urzędnikom służby cywilnej, pracujących w instytucjach rządowych związanych z bezpieczeństwem i obronnością, wniesienie wkładu w opracowywanie i wdrażanie polityki bezpieczeństwa i obronności. Z tego też względu przedmioty oferowane w ramach kursu są niejednokrotnie zbieżne z tymi przygotowanymi dla studentów JCGSC. Uwzględniają one także ćwiczenia praktyczne, co powoduje, że osoby uczestniczące w kursie CSC mają również szansę czerpania wiedzy i umiejętności od wyższych rangą wojskowych. W założeniu ma się to również przyczynić do budowy sieci kontaktów między urzędnikami służby cywilnej a członkami sił zbrojnych i służby cywilnej z innych państw NATO.

Podobnie jak w przypadku JCGSC, także CSC opiera się na połączeniu różnych metod nauczania. Zajęcia obejmują wykłady, seminaria, ćwiczenia, wizyty studyjne. Oprócz kontaktu z prowadzącym słuchacze są zobligowani do pracy indywidualnej oraz przygotowawczej; ta ostatnia ma miejsce jeszcze przed rozpoczęciem kursu. Ponadto studenci prowadzą również indywidualne badania i uczestniczą w dyskusjach oraz konferencjach.

Należy zaznaczyć, że udział w kursie nie jest dostępny dla każdego urzędnika służby cywilnej, kursanci są bowiem wybierani i nominowani przez odpowiednie instytucje, jak ministerstwa obrony czy też agencje rządowe. Powinni mieć oni co najmniej kilkuletnie doświadczenie zawodowe w obszarze bezpieczeństwa i obrony. Osoby nominowane wywodzą się najczęściej spośród pracowników niższego i średniego szczebla, muszą mieć także poświadczenie bezpieczeństwa wydane przez państwo swojego pochodzenia oraz wykazywać się dobrą znajomością języka angielskiego.

JCGSC czy CSC są w zasadzie najbardziej popularnymi kursami oferowanymi przez BALTDEFCOL; do roku akademickiego 2024/2025 JCGSC ukończyło łącznie 1297 osób z państw NATO i państw Partnerstwa dla Pokoju, w tym 18 z Polski. Z kolei w roku akademickim 2024/2025 liczba osób uczestniczących w kursie CSC wyniosła 170. Wśród absolwentów 1 osoba pochodziła z Polski i ukończyła kurs w 2022 r. Należy zaznaczyć, że stała oferta BALTDEFCOL jest uzupełniana o intensywne kursy przeprowadzane *ad hoc*, do których należą m.in. strategiczne podejmowanie decyzji w NATO (Strategic Decision Making in NATO) czy też polityki cyberobrony

na szczeblu krajowym i międzynarodowym (Cyber Defence Policy Course on National and International Levels). Działalność BALTDEFCOL nie ogranicza się jedynie do usług edukacyjnych – kadra tej instytucji, jak już wspomniano, angażuje się także w działalność badawczą; pracownicy oprócz publikacji wydawanych przez BALTDEFCOL, takich jak np. *BALTDEFCOL Policy Briefs* czy *Journal on Baltic Security*, publikują również autorskie raporty czy monografie.

Paulina Szeląg

Ad Securitatem Patriarum. For the Security of the Homelands, https://www.baltdefcol.org/about (dostęp 10.12.2025); *Baltic Defence College. Ad Securitatem Patriarum Joint Command and General Staff Course. Course Plan 2025–2026*, https://media.voog.com/0000/0051/2796/files/JCGSC%20Course%20Plan%202025-2026_amended%20version%2006.08.2025.pdf (dostęp 12.12.2025); *Brigadier General Alvydas Šiuparis*, https://www.baltdefcol.org/leadership/bg-alvydas-siuparis (dostęp 10.12.2025); *Civil Servants' Course*, https://baltdefcol.org/education/civil-servants-course (dostęp 15.12.2025); *Colonel Jonathan Huxley. Deputy Commandant/Chief of Staff*, https://www.baltdefcol.org/leadership/col-jonathan-huxley (dostęp 10.12.2025); *Cyber Defence Policy Course on National and International Levels*, https://baltdefcol.org/education/cyber-defence-policy-course (dostęp 15.12.2025); *Educational Charter of the Baltic Defence College*, https://www.baltdefcol.org/about/corporate-identity/educational-charter (dostęp 10.12.2025); *Graduates of CSC*, https://baltdefcol.org/about/statistics (dostęp 15.12.2025); *Graduates of JCGSC*, https://baltdefcol.org/about/statistics (dostęp 15.12.2025); *Joint Command and General Staff Course*, https://www.baltdefcol.org/education/joint-command-and-general-staff-course (dostęp 12.12.2025); *Leadership*, https://www.baltdefcol.org/leadership (dostęp 10.12.2025); *Master's Degree Description*, https://www.baltdefcol.org/education/master-s-degree (dostęp 10.12.2025); *Master's Degree Description. Professional master's study programme. Military Leadership and Security*, https://www.naa.mil.lv/en/military-leadership-and-security (dostęp 10.12.2025); *Mission*, https://www.baltdefcol.org/about/corporate-identity/mission (dostęp 10.12.2025); *Research and Publications*, https://baltdefcol.org/research-and-publications (dostęp 15.12.2025); *The Spirit of BALTDEFCOL – 25 Years of Excellence*, https://www.youtube.com/watch?v=HMorpB2VaAw&t=18s (dostęp 10.12.2025); *Strategic Decision Making in NATO*, https://baltdefcol.org/education/strategic-decision-making-in-nato (dostęp 15.12.2025); *Structure*, https://www.baltdefcol.org/about/structure (dostęp 10.12.2025).

BEZPIECZEŃSTWO AKUSTYCZNE – stan i zespół działań zapewniających ochronę ludzi, infrastruktury oraz procesów informacyjnych przed szkodliwym, niepożądanym lub celowo użytym oddziaływaniem dźwięku (hałasu, infradźwięków, ultradźwięków oraz sygnałów akustycznych). Obejmuje ono zarówno ochronę zdrowia i komfortu, jak i informacji, procesów decyzyjnych oraz bezpieczeństwa państwa. Bezpieczeństwo akustyczne to nie tylko ochrona słuchu, ale element bezpieczeństwa narodowego, informacyjnego i operacyjnego. W nowoczesnych systemach bezpieczeństwa dźwięk jest zarówno zagrożeniem, jak i narzędz*iem.*

Akustyka (z greckiego – słyszalny, odbierany przez słuch), w wąskim znaczeniu słowa – nauka o dźwięku, czyli o drganiach sprężystych i falach w gazach, cieczach, ciałach stałych, słyszalnych dla ludzkiego ucha (zakres od 16 do 20 Hz); w szerokim znaczeniu – dziedzina fizyki zajmująca się badaniem tych drgań i fal. Naukowcy wyróżniają akustykę fizjologiczną, psychologiczną, elektro- i hydroakustykę, akustykę medyczną, architektoniczną, muzyczną, bioakustykę, aeroakustykę, ekologię i geoakustykę. Bezpieczeństwo to warunki, w jakich znajduje się złożony system, gdy działanie czynników zewnętrznych i wewnętrznych nie prowadzi do zjawisk uznawanych za niebezpieczne; stan bezpieczeństwa człowieka, społeczeństwa, państwa, środowiska.

Bezpieczeństwo akustyczne w środowisku architektonicznym realizowane jest zgodnie z państwową polityką ekologiczną w ramach krajowej strategii ekologicznej zgodnie z decyzjami Światowego Szczytu (Johannesburg 2002) i zadaniami integracji europejskiej. Szybkie tempo urbanizacji stawia przed architektami, socjologami i ekologami nowe zadania – w trakcie realizacji polityki urbanistycznej i rekonstrukcyjnej zminimalizować wpływ zanieczyszczenia akustycznego, zmniejszając wpływ hałasu miejskiego, który zwiększa napięcie nerwowe, obniża aktywność twórczą, wydajność pracy, efektywność wypoczynku, stymuluje choroby. Bezpieczeństwo akustyczne w urbanistyce osiąga się poprzez poprawę warunków życia, jakości mieszkań i terenów przyległych, całodobową kontrolę i regulację poziomu hałasu, stosowanie w budownictwie skutecznych systemów ochrony przed hałasem, zmianę tras logistycznych transportu samochodowego i dalszy rozwój transportu elektrycznego, projektowanie 30-decybelowych („cichych") stref w dzielnicach mieszkalnych

miast. Broń akustyczna to środki oddziaływania na obiekty za pomocą energii drgań akustycznych o określonej częstotliwości, mocy i formie. Silny dźwięk może osłabić zdolność słyszenia (tymczasowo lub trwale), a także wpłynąć na aparat przedsionkowy. Intensywne fale dźwiękowe, nawet krótkotrwałe, mogą uszkodzić narządy, powodując całkowitą utratę słuchu (uraz wybuchowy/akustyczny). Zastosowanie ultradźwięków o różnych częstotliwościach może wywołać panikę grupową, pogorszenie wzroku, nudności, zmienić częstotliwość bicia serca, a nawet je zatrzymać.

Bezpieczeństwo akustyczne w działalności informacyjnej. Informacja – wszelkie dane, które są w określony sposób zapisane na nośnikach materialnych lub elektronicznych. Istnieje informacja jawna lub o ograniczonym dostępie: poufna, tajna i służbowa. Do głównych zagrożeń bezpieczeństwa informacyjnego należą: nieuprawnione rozpowszechnianie informacji (wyciek informacji), nieuprawniony celowy lub przypadkowy wpływ na informacje lub ich nośnik. Formy wycieku informacji – rozpowszechnianie, wywiad, nieuprawniony dostęp. Wywiad – celowe działania mające na celu uzyskanie informacji dla wojskowo-politycznego kierownictwa obcego państwa lub organizacji konkurencyjnej (szpiegostwo przemysłowe). Oprócz informacji dokumentowej i telekomunikacyjnej, ochrony wymaga również informacja akustyczna (językowa, ustna), której nośnikami są sygnały akustyczne.

Źródłami drgań akustycznych są przede wszystkim narządy głosu człowieka oraz różnego rodzaju przetworniki głosu (głośniki, mikrofony itp.).

Rozpoznanie akustyczne – uzyskiwanie informacji poprzez odbiór i analizę sygnałów akustycznych w zakresie infradźwiękowym, dźwiękowym i ultradźwiękowym (drgania lub wibracje), które rozprzestrzeniają się w środowisku powietrznym od obiektów rozpoznawczych. Rozpoznanie akustyczne odbywa się poprzez przechwytywanie sygnałów za pomocą różnych środków (urządzeń podsłuchowych, dyktafonów, mikrofonów kierunkowych lub kontaktowych, sonarów, laserowych systemów rozpoznania akustycznego, stetoskopów). Do nieuprawnionego pozyskiwania informacji wykorzystuje się techniczne kanały wycieku informacji (zbiór niebezpiecznych sygnałów fizycznych, środowisko ich rozpowszechniania i przechowywania, obiekt rozpoznania technicznego, jego sposoby i środki, które mogą być wykorzystane do pozyskania informacji z chronionego

obiektu). Niebezpieczny sygnał zawiera informacje, które należy chronić – w tym celu stosuje się repeatery, karty flash z szyfrowaniem, wykrywacze metalu, termowizory, ekranujące skrzynki z akustyczną przeszkodą, scramblery, urządzenia zapewniające poufność rozmów, sejfy akustyczne itp.

Wołodomyr Masłak

П. Саньков, *Актуальні аспекти забезпечення акустичній безпеки населення в Україні*, „Міжнародний Науковий Журнал" 2015, Вип. 5, https://www.inter-nauka.com/uploads/public/14412659957157.pdf (dostęp 30.11.2025); В.І. Заіченко, О.В. Заіченко, *Забезпечення акустичної безпеки при улаштуванні робочих місць в приміщеннях малого об'єму*, „Комунальне Господарство Міст" 2011, https://eprints.kname.edu.ua/21624/1/75-80%D0%97%D0%B0%D1%96%D1%87%D0%B5%D0%BD%D0%BA%D0%BE_%D0%92%D0%86.pdf (dostęp 30.11.2025); *Інформаційна безпека та захист інформації*, https://tzi.ua/ua/zahist_movno_nformac.html (dostęp 30.11.2025).

BEZPIECZEŃSTWO ELEKTRYCZNE (ang. *electrical safety*) – pojęcie stosowane w naukach technicznych, ekonomii i naukach o bezpieczeństwie. Z punktu widzenia tych ostatnich istotne jest kilka z definicji funkcjonujących w literaturze przedmiotu. Na łamach jednego z polskich periodyków Elshad Safiyev, Saida Kerimova i Kubra Mukhtarova uznali, że bezpieczeństwo elektryczne dotyczy systemu obejmującego zasoby techniczne i organizacyjne oraz środki chroniące ludzi przed szkodliwym i niebezpiecznym działaniem prądu elektrycznego, łuku elektrycznego, pola elektromagnetycznego i elektryczności statycznej. Wielu badaczy ma jednak odmienne zdanie.

Bezpieczeństwo elektryczne bywa definiowane tylko w odniesieniu do specjalistów wykonujących prace elektryczne w zakładach pracy i gospodarstwach domowych. Spotkamy też definicje redukujące bezpieczeństwo elektryczne do zestawu metod, technik i zabezpieczeń lub zbioru zasad i praktyk mających na celu unikanie zagrożeń elektrycznych podczas obsługi urządzeń lub instalacji. Yue Wang słusznie wskazuje, że bezpieczeństwo elektryczne to pojęcie szersze: kluczowy aspekt każdej instalacji elektrycznej. Ma zapewnić bezpieczeństwo przy użytkowaniu instalacji i urządzeń elektrycznych przez mieszkańców i pracowników w biurach

i zakładach pracy. Część francuskich specjalistów uznaje, że w przedsiębiorstwach termin bezpieczeństwo elektryczne obejmuje ochronę nie tylko pracowników, ale także sprzętu i obiektów, w których funkcjonuje firma.

W świetle tych ustaleń szczególnego znaczenia nabierają stosowane w polskich publikacjach (np. w materiałach cyklicznych konferencji poświęconych bezpieczeństwu elektrycznemu) pojęcia: technika bezpieczeństwa elektrycznego, bezpieczeństwo elektroenergetyczne, bezpieczeństwo eksploatacji urządzeń elektrycznych i bezpieczeństwo sieci elektroenergetycznych. Ważna jest też technologia bezpieczeństwa elektrycznego, w której zakres wliczane są procedury, praktyki oraz urządzenia zabezpieczające.

Niezależnie od przyjętej definicji bezpieczeństwo elektryczne wpływa na → bezpieczeństwo publiczne [t. 1] i bezpieczeństwo fizyczne. Jest powiązane z bezpieczeństwem technicznym, → bezpieczeństwem energetycznym [t. 1], bezpieczeństwem sieci energetycznej państwa i dążeniami do → suwerenności energetycznej [t. 6]. Zakłócenia w dostawach energii elektrycznej są uważane za jedne z najważniejszych → zagrożeń [t. 4]. Troska o zapewnienie tych dostaw jest jednym najważniejszych kierunków działań w ramach zapewnienia → ochrony ludności [t. 3]. Bezpieczeństwo elektryczne jest m.in. ściśle powiązane z bezpieczeństwem pożarowym, ochroną przeciwporażeniową oraz → bezpieczeństwem przesyłu i dystrybucji energii elektrycznej [t. 1]. Bezpieczeństwo elektryczne jest szczególnie istotne dla podmiotów gospodarczych prowadzących działalność np. w dziedzinie elektryki i w sektorze energetycznym. Nieprzypadkowo Azeez Olawale Ojelabi, Abdul Rohim Tualeka, Indriati Paskarini, Suardi Zurimi, Juliana Jalaludin, analizując bezpieczeństwo elektryczne, stwierdzają, że w USA w latach 2011–2021 aż 45,70% śmiertelnych wypadków było efektem kontaktu ludzi z napowietrznymi liniami energetycznymi.

Bezpieczeństwo elektryczne jest ściśle związane z zagrożeniami elektrycznymi (ang. *electrical hazards)* i zagrożeniami dla bezpieczeństwa elektrycznego ludzi (ang. *human electrical safety risks)* związanymi z instalacjami elektrycznymi. Chodzi nie tylko o ograniczenie zagrożeń w miejscu pracy dla personelu technicznego. Jak zauważa Mark Franks, w USA w latach 2011–2021 aż 69% śmiertelnych wypadków porażenia prądem było w zawodach niemających związku z elektrycznością. W budownictwie

wypadki tego typu stanowiły w przybliżeniu 20% wszystkich zgonów związanych z pracą zawodową.

Jak wiadomo, rozmiar, częstotliwość i długość wstrząsu elektrycznego (np. w wyniku narażenia na łuk elektryczny) wpływają na skalę uszkodzeń ciała, włącznie z trwałą niepełnosprawnością lub śmiercią. Roman Sikora, Przemysław Markiewicz, Ewa Korzeniewska i Wiesława Malska do skutków poważnego porażenia prądem na placu budowy zaliczają m.in. „zatrzymanie akcji serca, zatrzymanie oddechu, oparzenia i uszkodzenia komórek, prawdopodobieństwo wystąpienia migotania komór". Generuje to ryzyko groźnych urazów wtórnych, np. upadku porażonej prądem osoby z drabiny czy rusztowania z wszystkimi tego konsekwencjami. Równocześnie długotrwałe narażenie na zbyt wysokie pole elektroenergetyczne generuje zagrożenia np. dla układu nerwowego człowieka.

Ilość ofiar śmiertelnych i strat materialnych związanych z wypadkami porażenia prądem elektrycznym, wybuchami i pożarami wynikłymi z wadliwej instalacji elektrycznej lub np. źle podpiętych urządzeń elektrycznych oraz, co ważniejsze, ryzyka, jakie generuje sektor energetyczny, uzasadnia pogląd Jiang Feii i Yun Dan, że polepszenie „zarządzania bezpieczeństwem elektrycznym i poprawa poziomu bezpieczeństwa elektrycznego mają ogromne znaczenie dla utrzymania stabilności społecznej i stymulowania rozwoju gospodarczego".

Współcześnie wzrasta zapotrzebowanie na energię elektryczną: postęp elektryfikacji gospodarki, wzrost znaczenia → bezpieczeństwa dematerializacji ekonomii [t. 8], wzrost roli centrów danych, które zasilają globalną infrastrukturę cyfrową. Stąd szczególne znaczenie koordynacji bezpieczeństwa wszystkich elementów składowych systemu elektrycznego (w skali lokalnej, regionalnej, jak i ogólnokrajowej). Szczególnie dla dużych miast (zarówno w krajach wysoko rozwiniętych, jak i rozwijających się) dłuższe, np. kilkudniowe, przerwy w dostawie energii elektrycznej (blockauty) stanowią poważne wyzwania dla wielu sektorów; systemy zasilane energią elektryczną uznawane są bowiem za bardzo istotną część infrastruktury niezbędnej do funkcjonowania zarówno sieci wodociągowej, jak i np. → sztucznej inteligencji [t. 4]. Nie dziwi więc, że generowanie i dystrybucja energii elektrycznej są zaliczane w wielu krajach do usług kluczowych i objęte są → krajowym systemem cyberbezpieczeństwa [t. 2]. Niektóre

podmioty aktywne w tym sektorze są zaliczane do operatorów usług kluczowych. W tej sytuacji Elena Georgiou i Stefan Howorka wskazują, że celem w zakresie bezpieczeństwa elektrycznego powinno być zorientowane na człowieka zsynchronizowane podejście w zakresie prawa i technologii. Jak zauważa Yue Wang, zapewnienie bezpieczeństwa elektrycznego wymaga podejścia kompleksowego, „od projektowania instalacji elektrycznej i doboru urządzeń po instalację i konserwację".

Zagrożenia związane z bezpieczeństwem elektrycznym wynikają z różnych przyczyn. Zdzisław Idziaszek (2010) zalicza do ich:

- błędny dobór linii zasilających i wymagań zabezpieczeń w etapach projektowania, konstruowania, budowania, eksploatacji, modernizacji i burzenia budynków;
- stopień dostosowania wyposażenia do możliwości sieci w budynku;
- wadliwe działanie urządzeń elektrycznych i oświetlenia;
- nadmiar lub brak energii elektrycznej w różnych porach dnia i roku;
- szkodliwe oddziaływanie pola elektrycznego i elektromagnetycznego na organizm ludzki, np. linii przesyłowych wysokiego napięcia.

Do tego należy doliczyć m.in.:

- poziom wyeksploatowania sieci elektrycznej;
- klęski żywiołowe i awarie techniczne;
- nakładanie się na siebie różnych pól magnetycznych związanych z energią elektryczną.

Z założenia władze państwowe, organizacje branżowe, pracodawcy dążą do zapewnienia stabilnego i bezpiecznego systemu elektrycznego. Wady instalacji elektrycznej lub niedostateczne uwzględnienie możliwości technologicznych sieci elektrycznych niekiedy prowadzą do → katastrof technicznych [t. 2]. Dotyczą one najczęściej skali lokalnej. Z punktu widzenia kierujących przedsiębiorstwem odpowiednia konserwacja i diagnostyka usterek ułatwiają utrzymanie płynnej produkcji w dłuższym okresie i obniżają wewnętrzne ryzyko przedsiębiorstwa w zakresie bezpieczeństwa elektrycznego. Skala rozwoju elektryfikacji gospodarki zwiększa jednak konsekwencje katastrof na znacznie większą skalę, np.

w postaci braku dostępu do prądu całych regionów czy terytoriów kilku państw. Przykładem może być zaistniały w kwietniu 2025 r. *blackout* na terenie Hiszpanii, Portugalii, Andory i części Francji.

Istnieje system regulacji zmniejszający skalę zagrożeń elektrycznych, minimalizujący skutki awarii, mający zapewnić bezpieczeństwo elektryczne: normy bezpieczeństwa elektrycznego (ang. *electrical safety standards*). Ich stosowane ma poważnie zwiększyć bezpieczeństwo systemów elektrycznych. Normy projektowe i eksploatacyjne regulują m.in. używanie maszyn, wymogi dotyczące technologii i urządzeń kontrolnych, dopuszczalną obciążalność przewodów lub zabezpieczeń; minimalną odległość pracowników od urządzeń elektrycznych (np. linii przesyłowych), szkolenia personelu i stosowanie odzieży ochronnej.

Zważywszy na skalę handlu międzynarodowego urządzeniami elektrycznymi, konieczna jest nie tylko współpraca międzybranżowa (np. energetyki i budownictwa) czy w skali poszczególnych państw, ale także na poziomie międzypaństwowym. Ma ona m.in. umożliwić wcielenie w życie międzynarodowych ujednoliconych wymagań. Przykładami są normy wydane przez Międzynarodową Komisję Elektrotechniczną (International Electrotechnical Commission, IEC) czy Europejski Komitet Normalizacyjny ds. Elektrotechniki; dyrektywa władz UE w sprawie bezpieczeństwa urządzeń elektrycznych (LVD 2014/35/UE) czy rozporządzenie i dyrektywa UE o energii elektrycznej przyjęte w maju 2019 r. Dążenie do zabezpieczenia przed blackoutami zawierała m.in. strategia UE w zakresie dążenia do → unii energetycznej [t. 8] (m.in. zobowiązano państwa członkowskie do współpracy w zakresie rynku energii elektrycznej i rozbudowy sieci elektrycznej). Jak wskazuje Wiktoria Grycan – UE do regulacji z zakresu bezpieczeństwa elektrycznego wracała jeszcze wiele razy, m.in. w kontekście transformacji cyfrowej maszyn przemysłowych. Powodowało to częste zmiany przepisów szczegółowych, co czasami, pod pewnymi względami, utrudniało zapewnienie bezpieczeństwa elektrycznego na terenie UE.

Bezpieczeństwo elektryczne jest bardzo istotne dla funkcjonowania i → ochrony infrastruktury krytycznej [t. 5] oraz → infrastruktury wojskowej [t. 2] państw i bloków państw. Jak pokazuje np. pełnoskalowa agresja Rosji wobec Ukrainy, ataki na kluczowe elementy sieci elektrycznej są w XXI w. przez wielu decydentów uważane za bardzo skuteczny środek

do atakowania/niszczenia miast przeciwnika (→ urbicyd [t. 6]). Nieprzypadkowo troska o bezpieczeństwo elektryczne wchodzi w także w zakres → ostrzegania i alarmowania ludności [t. 7]. Można wykazać związki bezpieczeństwa elektrycznego ze środkami rażenia związanymi np. z → walką elektroniczną [t. 4] czy → wojną asymetryczną [t. 4].

Cyberataki skierowane na urządzenia wykorzystujące energię elektryczną mogą zniszczyć lub zakłócić przesyłanie np. informacji wojskowej (→ bezpieczeństwo informacji wojskowej [t. 1]).

Ocena ryzyka musi uwzględniać rodzaj sprzętu elektrycznego, sposób jego użytkowania przez pracowników/domowników; warunki eksploatacji oraz poziom kompatybilności instalacji elektrycznej i sprzętu elektrycznego z planami jego zastosowania przez użytkowników. Yue Wang słusznie podkreśla wagę dostosowania rozwiązań w zakresie bezpieczeństwa elektrycznego do indywidualnych potrzeb każdego przedsiębiorstwa. Olga Alekseevna Filina trafnie wskazuje, przy analizie bezpieczeństwa uziemienia, właściwości konkretnej sieci elektroenergetycznej. Przykładowo bardzo istotną przyczyną awarii uziemienia elektrycznego w Chinach jest jego niewłaściwa konstrukcja.

Niektórzy badacze za kluczową dla bezpieczeństwa elektrycznego uznają technologię ochrony izolacji, która zapobiega niezamierzonemu przewodzeniu prądu. Można też wskazać inne bardzo ważne czynniki.

Przykładowo Ojelabi, Tualeka, Paskarini, Zurimi i Jalaludin podkreślają: „Do kompleksowego zarządzania zagrożeniami elektrycznymi wymagana jest wielowarstwowa strategia obejmująca różne środki kontroli. Środki te obejmują środki ochrony indywidualnej, środki kontroli inżynieryjnej, zastępowanie, eliminację i środki kontroli administracyjnej, obejmujące całą hierarchię środków kontroli. Podczas gdy kontrole inżynieryjne koncentrują się na redukcji ryzyka poprzez metody techniczne, strategie eliminacji i substytucji dążą do usunięcia lub zastąpienia potencjalnie niebezpiecznych komponentów. Procedury i wytyczne stanowią część kontroli administracyjnych, a środki ochrony indywidualnej (PPE) stanowią ostatnią linię obrony".

Teoretycznie obowiązujące w państwie normy są, jak podkreślają niektórzy badacze, podstawową gwarancją bezpieczeństwa elektrycznego. Tak jak do najlepszych praktyk powszechnie zaliczane są m.in.

nieprzeciążanie obwodów elektrycznych, unikanie wilgotnych warunków, regularne sprawdzanie urządzeń elektrycznych w poszukiwaniu ewentualnych uszkodzeń lub zużycia, stosowanie środków ochrony indywidualnej. W praktyce jednak zróżnicowanie skali ograniczeń finansowych, rozmiarów narażenia na klęski żywiołowe i wielu innych uwarunkowań (szczególnie społeczno-ekonomicznych, środowiskowych i kulturowych) wpływa na różnorodność regionalną w zakresie stosowania norm i praktyk oraz skali wyzwań związanych z bezpieczeństwem energetycznym.

Szczególnie duża rozbieżność między normami a rzeczywistością występuje w krajach rozwijających się. Bariery finansowe wpływają na wybór mniej bezpiecznych materiałów; rzutują na dobór sprzętu i uziemienia. Jeden z uczestników badań na ten temat na Filipinach wprost stwierdził: „Gdyby izolowane rękawice lub testery były tańsze, kupilibyśmy je. Ale obecnie są dla nas za drogie". Inny wskazywał: „Nie mamy narzędzi ani sprzętu do radzenia sobie z problemami elektrycznymi. Mamy tylko nadzieję, że nic się nie zepsuje, bo nie wiemy, co robić" (cyt. za: Sebastian, Fabro, Faylogna, Ladran, Daquioag, Castillo 2025).

W skali globalnej problem wyostrza skala postępu technicznego. Nie tylko Safiyev, Kerimova i Mukhtarova podkreślają konieczność stałej aktualizacji zasad bezpieczeństwa elektrycznego w oparciu o zgromadzone doświadczenie i innowacje naukowe. Mark Franks wskazuje na „strategie optymalizacji, w tym promowanie innowacji i udoskonaleń technologicznych". Postęp technologiczny przynosi rozbieżność między normami i „systemami zapewnienia bezpieczeństwa a wymaganiami najnowszego sprzętu trafiającego do fabryk i domów" (Yuxiang 2025). Badacz ten podkreśla też konieczność zwiększania poziomu adaptacji technologii bezpieczeństwa elektrycznego do złożonych i zmieniających się warunków związanych np. z transformacją energetyczną.

Ważna jest także technologia ochrony, monitorowania np. stanu uziemienia. Nieuchronne jest dalsze upowszechnienie inteligentnych systemów monitorowania bezpieczeństwa elektrycznego (ang. *intelligent electrical safety monitoring system) oraz stosowanie coraz nowszych materiałów.*

Z jednej strony, innowacje i modernizacje zwiększają więc poziom bezpieczeństwa systemów elektrycznych, z drugiej jednak – podnoszą

koszty zapewnienia bezpieczeństwa elektrycznego i obniżają bieżące zyski przedsiębiorstw.

Specjaliści uwypuklają znaczenie działań prewencyjnych. W wielu uboższych krajach, zgodnie z rzeczywistymi oczekiwaniami władz państwowych, władze lokalne muszą jednak „dostosować" przepisy dotyczące bezpieczeństwa elektrycznego np. w zakresie częstotliwości przeglądów sieci i jej konserwacji: „Nie mamy pieniędzy na regularne sprawdzanie systemu. Naprawiamy go tylko wtedy, gdy już występuje problem" (cyt. za: Sebastian, Fabro, Faylogna, Ladran, Daquioag, Castillo 2025). W praktyce zwiększa to np. zagrożenie pożarowe. Bariery finansowe nie zawsze są decydującą przyczyną opisanego stanu rzeczy; nawet we Francji można spotkać pogląd, że co trzeci pożar ma podłoże elektryczne. Z analizy pożarów w fabrykach w Bangladeszu, będących efektem awarii instalacji elektrycznej, wynika, że brak przestrzegania norm, regularnych przeglądów i konserwacji oraz zakup materiałów i sprzętu niespełniających norm nie zawsze wynika z ograniczonych funduszy pracodawców.

Problemem jest też niewystarczające przygotowanie władz, specjalistów i obywateli do zapewnienia bezpieczeństwa elektrycznego. Ojelabi, Tualeka, Paskarini, Zurimi i Jalaludin wykazali „związek między wiedzą, nadzorem i przestrzeganiem procedur bezpieczeństwa, przy czym osoby posiadające niewystarczającą wiedzę i nadzór częściej ignorowały procedury bezpieczeństwa", np. w zakresie palenia papierosów i spożywania alkoholu.

Zapewnienie bezpieczeństwa dostaw energii elektrycznej zajmuje w wielu krajach ważne miejsce w → systemie zarządzania kryzysowego [t. 4]. W państwach, na terenie których często występują znacznych rozmiarów klęski żywiołowe, dotychczasowe uwzględnienie bezpieczeństwa elektrycznego w systemie zarządzania kryzysowego nie jest wystarczające. Cee Jay A. Sebastian, Regie Boy B. Fabro, Precious N. Faylogna, Peter John B. Ladran, Dariel Justin V. Daquioag, Domenie O. Castillo wskazują, że bardzo istotna powinna być troska o odpowiednią jakość i konserwację sieci elektrycznej oraz urządzeń elektrycznych. W razie wystąpienia klęsk żywiołowych uszkodzone i/lub źle konserwowane systemy elektryczne zwiększają bowiem ilość pożarów, porażeń prądem, blackoutów… W rzeczywistości jednak praktyka w wielu państwach znacznie odbiega

od stanu optymalnego w opisanym zakresie. Z drugiej strony, negatywnie na zapewnienie ciągłości i bezpieczeństwa dostaw energii elektrycznej do odbiorców pośrednio wpływają tylko częściowo zależne od tej grupy państw → ryzyko i kryzys klimatyczny [t. 6] oraz → globalne ocieplenie klimatyczne [t. 5].

Tylko w części państw w praktyce są wymagane odpowiednie procedury kontroli (ułatwiające integrację m.in. analizy zagrożeń elektrycznych, szkolenia personelu, stosowania specjalnej odzieży ochronnej i specjalnego sprzętu) czy środki finansowe na sprawnie działające pogotowie energetyczne. Wyzwaniem jest niekiedy niewystarczający dostęp, jakość i skala wyeksploatowania infrastruktury. Do tego, w świetle ustaleń takich badaczy, jak Bayu Bagaskoro, Silviana Windasari, Abdurohman Abdurohman, Adi Afandi i Ade Frihadi, można doliczyć poziom jej bezpieczeństwa, wydajności i odporności.

Jak wiadomo, naprawy sprzętu i sieci elektrycznej z założenia powinni dokonywać wyłącznie specjaliści dysponujący odpowiednią wiedzą, doświadczeniem i umiejętnościami. W praktyce jednak, ze względu na koszt skorzystania z ich usług lub ich niewystarczającą dostępność, w niektórych państwach większość obywateli dokonuje napraw samodzielne, co generuje znaczną ilość wypadków.

Do praktycznych wyzwań ściśle związanych z bezpieczeństwem elektrycznym należy zaliczyć ograniczenia techniczne wynikające m.in. z obecności zabezpieczeń chroniących przed przeciążeniem sieci i zwarciem. Wyzwania stwarza też lokalizacja urządzeń; przykładem jest ograniczenie skuteczności stosowania typowych metod uziemienia na terenach pustynnych.

W wielu krajach brak szkoleń lub ich pozostawiająca wiele do życzenia jakość skutkują małą wiedzą w zakresie bezpieczeństwa elektrycznego u pracowników i obywateli, co znacznie zwiększa ilość wypadków i doprowadza do sytuacji typu: „Nie wiemy, jak bezpiecznie wyłączyć zasilanie w sytuacjach awaryjnych. Czasami po prostu zostawiamy je włączone i mamy nadzieję, że nic gorszego się nie stanie" (Sebastian, Fabro, Faylogna, Ladran, Daquioag, Castillo 2025).

Cytowani badacze wykazali „dodatnią korelację między wiedzą mieszkańców na temat bezpieczeństwa elektrycznego a ich gotowością

do wdrażania praktyk bezpieczeństwa […] i przestrzegania przepisów w zakresie zarządzania bezpieczeństwem [elektrycznym]" np. w sytuacjach kryzysowych.

W wielu państw rozwijających się bardzo istotna jest popularyzacja wiedzy z omawianego zakresu wśród obywateli, wsparcie przez władze państwa i samorządowe praktycznych, lokalnych inicjatyw edukacyjnych w zakresie wiedzy, przestrzegania norm i zasad bezpieczeństwa elektrycznego oraz poszerzenie „dostępu do niedrogich zasobów i usług profesjonalnych […] bezpłatnych lub tańszych przeglądów i usług konserwacyjnych instalacji elektrycznych dla gospodarstw domowych o niskich dochodach" (Sebastian, Fabro, Faylogna, Ladran, Daquioag, Castillo 2025).

W celu podniesienia poziomu bezpieczeństwa elektrycznego, zwiększenia odporności i gotowości na wypadek katastrof są podejmowane starania zarówno w zakresie podniesienia poziomu technicznego (np. wyposażenia zakładów pracy), jak i kwalifikacji pracowników oraz ekspertów.

Ważnym wyzwaniem w zakresie bezpieczeństwa elektrycznego jest niedbały lub niewystarczający nadzór nad wdrażaniem norm bezpieczeństwa elektrycznego i szkoleniami personelu oraz wadliwe mechanizmy egzekwowania. Sazurani Abdul Zabil i Fadzli Shah Abd Aziz słusznie zwracają uwagę na duże znaczenie klimatu bezpieczeństwa (ang. *safety climate) danej organizacji czy zakładu pracy; chodzi nie tylko o* nieodpowiednie wdrażanie norm wynikające z niewiedzy pracowników. Mimo tworzenia w wielu krajach profesjonalnych zespołów nadzoru i systemów identyfikowalności jakości, a nawet inteligentnego monitoringu, w części z nich nadal „instalacje elektryczne na placach budowy […] często są niepoprawnie użytkowane i konserwowane" (Sikora, Markiewicz, Korzeniewska, Malska 2025).

Chodzi m.in. o to, jaki stosunek do bezpieczeństwa elektrycznego wykazuje w praktyce kadra kierownicza zakładu pracy; na ile stymuluje ona w tym zakresie szeregowych pracowników przez np. wnikliwe, regularne inspekcje bezpieczeństwa. Sebastian, Fabro, Faylogna, Ladran, Daquioag i Castillo uważają, że „motywacja i dostęp do zasobów są kluczowymi czynnikami determinującymi zachowania związane z bezpieczeństwem [elektrycznym]".

Zbyt często problemem jest jakość szkoleń, stąd pojawia się postulat łączenia „zajęć teoretycznych z ćwiczeniami praktycznymi" (Yuxiang 2025), zwiększenia „proaktywnych środków bezpieczeństwa i edukacji" (Sebastian, Fabro, Faylogna, Ladran, Daquioag, Castillo 2025) czy prowadzenia szkoleń wielopoziomowych dostosowanych do różnych szczebli struktury organizacyjnej.

Jak wskazują polscy badacze, zapobieganie zagrożeniom elektrycznym nieco utrudnia, wynikające z różnych przyczyn, zróżnicowanie między ludźmi w zakresie wrażliwości na prąd – jest ona niższa np. u elektryków.

Safiyev, Kerimova i Mukhtarova dzielą bezpieczeństwo elektryczne na wiele działów związanych m.in. z produkcją, rolnictwem, przemysłem wydobywczym, urządzeniami mobilnymi czy budynkami. Jednak nie wszyscy badacze zgadzają się z takim podziałem.

Częściowo w zakres bezpieczeństwa elektrycznego wchodzi broń elektryczna (ang. *conducted electrical weapons*). Jak piszą np. Dorin Panescu, Max Nerheim, Mark Kroll i Michael Brave, generuje ona impulsy elektryczne zdolne zahamować kontrolę nerwowo-mięśniową osoby i tymczasowo ją unieruchamiać. Zagrożenia dla bezpieczeństwa elektrycznego stwarza także rozwój → nanobroni [t. 7].

Ze względu na postępującą nie tylko w UE (→ Europejski Zielony Ład [t. 8]) elektryfikację transportu (m.in. elektryczne samochody osobowe i ciężarowe, elektryczne hulajnogi) bezpieczeństwo elektryczne w niektórych aspektach jest powiązane z → bezpieczeństwem komunikacyjnym [t. 8].

Na zwiększony pobór energii elektrycznej (i koszty ekonomiczne związane z koniecznością płacenia odpowiednio wyższych rachunków) wpływają nie tylko przemiany związane z rosnącym poziomem elektryfikacji gospodarki światowej, ale także np. następstwa → fonoholizmu [t. 7].

Bezpieczeństwo elektryczne jest także powiązane z bezpieczeństwem cieplnym; chodzi nie tylko o niektóre → odnawialne źródła energii [t. 6], ale także m.in. generowanie ciepła za pomocą energii elektrycznej i dbanie o odpowiednią odporność cieplną sieci elektrycznej i urządzeń elektrycznych. Nieprzypadkowo Idziaszek wytwarzanie ciepła zaliczył do 3 najważniejszych rodzajów działania prądu elektrycznego.

Michael A. Brave, Dhanunjaya R. Lakkireddy, Mark W. Kroll i Dorin Panescu należą do licznych badaczy piszących o wpływie bezpieczeństwa elektrycznego na niektóre aspekty bezpieczeństwa kardiologicznego (ang. *cardiac safety*). Testy bezpieczeństwa elektrycznego stosuje się w celu określenia bezpieczeństwa elektrycznych urządzeń medycznych (ang. *safety of electrical medical devices*). Są także analizy bezpieczeństwa elektrycznego na salach operacyjnych.

Znaczenie bezpieczeństwa elektrycznego będzie nadal rosnąć, zwiększa się bowiem zależność od energii elektrycznej zarówno w skali całych gospodarek, jak i poszczególnych przedsiębiorstw czy gospodarstw domowych.

Tomasz Skrzyński

B. Bagaskoro, S. Windasari, A. Abdurohman, A. Afandi, A. Frihadi, *Optimization of logistics electrical systems with a safety approach*, „Teknik: Jurnal Ilmu Teknik dan Informatika" 2025, vol. 5, no 1, 10.51903/teknik.v5i1.892; M. Brave, D. Lakkireddy, M. Kroll, D. Panescu, *Validity of the small swine model for human electrical safety risks*, Conference proceedings: Annual International Conference of the IEEE Engineering in Medicine and Biology Society, IEEE Engineering in Medicine and Biology Society, Conference, 2016, s. 2343–2348, 10.1109/EMBC.2016.7591200; D.J. Doyle, *Electrical and Fire Safety in the Operating Room*, [w:] *Basic Sciences in Anesthesia*, M. Argalious, E. Farag, D. Sharma (eds.) Springer, Cham 2024, https://doi.org/10.1007/978-3-031-60203-0_36; J. Feii, Y. Dan, *Diànqì jiēdì yǔ diànqì ānquán wèntí (Uziemienie elektryczne i kwestie bezpieczeństwa elektrycznego*), „Qī·Jīxiè Yǔ Diànzǐ Kòngzhì Gōngchéng" 2025, vol. 7, no. 6, 10.37155/2717-5197-0706-66; O.A. Filina, *Analyzing Electrical Safety in Electrical Grids of Industrial Enterprises*, „Occupational Safety in Industry" 2025, no. 6, 10.24000/0409-2961-2025-6-78-84; M. Franks, *The history of electrical safety. Worker protection against arc flash incidents has a personal history all its own*, 2013, https://www.plantservices.com/equipment/electrical-systems/article/11332445/electrical-systems-the-history-of-electrical-safety (dostęp 15.12.2025); E. Georgiou, *Adapting neuroergonomic principles to electrical safety training for technical workers in Europe*, https://www.researchgate.net/publication/393122456_ADAPTING_NEUROERGONOMIC_PRINCIPLES_TO_ELECTRICAL_SAFETY_TRAINING_FOR_TECHNICAL_WORKERS_IN_EUROPE (dostęp 15.12.2025); E. Georgiou, S. Howorka, *Comparative Analysis of Legal Frameworks Governing Worker Neuroergonomics and Electrical Safety Standards in Europe*, https://www.researchgate.net/

publication/393136544_Comparative_Analysis_of_Legal_Frameworks_Governing_Worker_Neuroergonomics_and_Electrical_Safety_Standards_in_Europe/references (dostęp 15.12.2025); *Habilitations électriques des agents*, 03.2018, https://www.cdg2b.com/wp-content/uploads/2020/10/23-circulaire-risques-electriques.pdf (dostęp 15.12.2025); Z. Idziaszek, *Zagrożenia elektryczne bezpieczeństwa ludzi, mienia, budynku* [referat wygłoszony na konferencji: *Bezpieczeństwo i koszty w gospodarowaniu nieruchomościami*], 2010, https://www.researchgate.net/publication/332903082_Zagrozenia_elektryczne_a_bezpieczenstwo_ludzi_mienia_i_budynku (dostęp 15.12.2025); A. Ojelabi, A. Tualeka, I. Paskarini, S. Zurimi, J. Jalaludin, *Electrical industry safety: examining control strategies to reduce electrical risks based on OSHA and BLS (2011–2021) Reports*, „Journal of Vocational Health Studies" 2025, no. 9, https://doi.org/10.20473/jvhs.V9.I2.2025.146-153; D. Panescu, M. Nerheim, M. Kroll, M. Brave, *New conducted electrical weapons: Electrical safety relative to relevant standards*, [w:] *Conference proceedings: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society*, 2017, s. 2185–2190, 10.1109/EMBC.2017.8037288; C. Sebastian, R.B. Fabro, P. Faylogna, P. Ladran, D. Daquioag, D. Castillo, *Electrical Safety Practices and Challenges in Disaster-Prone Coastal Communities: A Case Study of "Boracay of the North", Philippines*, „International Journal of Research and Innovation in Social Science" 2025, vol. 9, no. 16, 10.47772/IJRISS.2024.916SCO0027; *Sécurité électrique: les enjeux d'une installation défectueuse*, 8.10.2024, https://www.sf-formation.fr/blog/les-enjeux-d-une-installation-defectueuse (dostęp 15.12.2025); R. Sikora, P. Markiewicz, E. Korzeniewska, W. Malska, *Analysis of the influence of the earthing structure on the effects of electric shock in electrical installations placed on construction sites*, „Przegląd Elektrotechniczny" 2025, vol. 101, no. 4, 10.15199/48.2025.04.10; Y. Wang, *Diànqì ānquán jìshù yǔ diànqì ānquán guīfàn*, „Jīxiè Yǔ Diànzǐ Kòngzhì Gōngchéng" 2025, vol. 7, no. 24, 10.37155/2717-5197-0724-78; G. Xun, S. Shi-Yue, *Design and Implementation of an Electrical Safety Monitoring System in Electrical Engineering and Automation*, „Engineering Technology Trends" 2025, vol. 3, no. 3, 10.37155/2972-483X-0303-3; *XV Konferencja Naukowo-Techniczna. Bezpieczeństwo Elektryczne ELSAF*, XIV Szkoła Ochrony Przeciwpożarowej, ELSAF 2023, Politechnika Wrocławska, Wrocław 2023; *XXV Konferencja Naukowo-Techniczna. Bezpieczeństwo Elektryczne ELSAF*, 23–26.09.2025, https://elsaf.pwr.edu.pl/fcp/FGBUKOQtTKlQhbx08SlkTUQJGUWRuHQwFDBoIVURNWH9WFVZpCFghUHcKVigEQUw/264/public/program_elsaf2025_v3.pdf (dostęp 15.12.2025); S. Yadav, A. Hemavathi, V.K. Tanwar, Vishesh, V. Varun, G. Sumana, D. Rajesh, *Measurement uncertainty evaluation and calibration of electrical safety analyzer for biomedical equipment,* „Mapan – Journal of Metrology Society of India" 2025,

vol. 40, 10.1007/s12647-025-00850-w; M. Yuxiang, *Diànqì ānquán jìshù yǔ diànqì ānquán guīfàn* (*Technologia bezpieczeństwa elektrycznego i normy bezpieczeństwa elektrycznego*), „Gōngchéng Jìshù Yǔ Zhìliàng Guǎnlǐ" 2025, vol. 1, no. 8, 10.37155/3041-0827-0108-62; S.A. Zabil, F.S.A. Aziz, *The Mediating Role of Employee Conscientiousness on Safety Climate, Employee Competency and Safety Performance in Malaysian Electrical Industry, „The Journal of Behavioral Science" 2025, vol. 20, no. 2, 10.69523/tjbs.2025.279247.*

BEZPIECZEŃSTWO RYNKÓW KAPITAŁOWYCH stanowi jedno z fundamentalnych zagadnień współczesnych nauk ekonomicznych i prawnych, obejmując całokształt mechanizmów, instytucji oraz regulacji prawnych służących zapewnieniu prawidłowego funkcjonowania rynku papierów wartościowych i innych instrumentów finansowych, przy czym pojęcie to wykracza daleko poza tradycyjnie rozumianą ochronę inwestorów, obejmując również wymiar stabilności systemowej, integralności cenowej oraz odporności infrastruktury rynkowej na zagrożenia o charakterze technologicznym i geopolitycznym. W ujęciu przyjmowanym przez Międzynarodową Organizację Komisji Papierów Wartościowych regulacja rynków kapitałowych realizuje 3 wzajemnie powiązane cele obejmujące ochronę inwestorów przed praktykami manipulacyjnymi i oszukańczymi, zapewnienie uczciwości, efektywności oraz przejrzystości rynków, a także redukcję ryzyka systemowego mogącego zagrozić stabilności całego systemu finansowego. Narodowy Bank Polski definiuje stabilność finansową jako stan, w którym system pełni swoje funkcje w sposób ciągły i efektywny nawet w przypadku wystąpienia nieoczekiwanych i niekorzystnych zaburzeń o znacznej skali i niskim prawdopodobieństwie zaistnienia, co podkreśla kluczowe znaczenie odporności rynków na szoki zewnętrzne.

W kontekście teoretycznym bezpieczeństwo rynku kapitałowego opiera się na 4 filarach obejmujących integralność, przejrzystość, płynność oraz stabilność, przy czym każdy z tych elementów warunkuje prawidłowe funkcjonowanie pozostałych, tworząc złożony system wzajemnych zależności. Integralność rynkowa oznacza sprawiedliwe traktowanie wszystkich uczestników obrotu oraz skuteczne wykrywanie i penalizowanie praktyk manipulacyjnych naruszających mechanizm uczciwego kształtowania cen. Przejrzystość obejmuje wymiar przedtransakcyjny polegający na

zapewnieniu dostępu do informacji o ofertach kupna i sprzedaży oraz wymiar potransakcyjny dotyczący publikacji cen i wolumenów zawartych transakcji. Płynność zapewnia możliwość szybkiej konwersji instrumentów finansowych na gotówkę i odwrotnie bez istotnego wpływu na cenę, co ma fundamentalne znaczenie dla efektywności alokacyjnej rynku. Stabilność natomiast odnosi się do zdolności absorpcji szoków zewnętrznych przy zachowaniu ciągłości funkcjonowania i niedopuszczeniu do kaskadowych załamań cenowych.

Polski rynek kapitałowy reprezentowany przez Giełdę Papierów Wartościowych w Warszawie, stanowiącą największą giełdę Europy Środkowo-Wschodniej, osiągnął kapitalizację przekraczającą 2 biliony złotych w czerwcu 2025 r., jednak relacja kapitalizacji do produktu krajowego brutto na poziomie 22–24% pozostaje znacząco poniżej średniej unijnej wynoszącej około 63% oraz amerykańskiej przekraczającej 200%, co wskazuje na niepełne wykorzystanie potencjału rynku kapitałowego w finansowaniu polskiej gospodarki. Giełda Papierów Wartościowych w Warszawie notuje akcje ponad 400 spółek krajowych i zagranicznych, a także instrumenty pochodne, obligacje skarbowe i korporacyjne oraz produkty strukturyzowane, pełniąc istotną funkcję w procesie alokacji kapitału w gospodarce narodowej.

Współczesne rynki kapitałowe narażone są na wielowymiarowe zagrożenia, których wykrywalność i neutralizacja stanowią rosnące wyzwanie regulacyjne wymagające ciągłego dostosowywania mechanizmów nadzorczych do ewoluującego charakteru nadużyć. Manipulacje cenowe przybierają coraz bardziej wyrafinowane formy, wykorzystując możliwości technologiczne handlu algorytmicznego, a do najczęściej spotykanych technik należą *spoofing*, *layering*, *pump and dump* oraz *wash trading*. *Spoofing* polega na składaniu dużej liczby zleceń po jednej stronie arkusza zleceń w celu stworzenia iluzji presji podażowej lub popytowej bez intencji ich realizacji, przy czym manipulant następnie realizuje zlecenia po przeciwnej stronie rynku po sztucznie przesuniętej cenie i anuluje pierwotne zlecenia przed ich wykonaniem. Głośnym przypadkiem ilustrującym skalę tego procederu była sprawa Navinder Singh Sarao, który stosując technikę dynamicznego warstwowania, osiągnął zyski przekraczające 40 mln dolarów w latach 2010–2014 i przyczynił się do tak zwanego Flash Crash z 6

maja 2010 r. *Layering* stanowi wariant spoofingu polegający na rozkładaniu zleceń na różnych poziomach cenowych, tworząc *spread* przesuwający cenę rynkową w pożądanym kierunku, a amerykańska Financial Industry Regulatory Authority (FINRA) nałożyła karę miliona dolarów na Trillium Brokerage Services za 46 tys. przypadków nielegalnego warstwowania.

Schematy manipulacji typu *pump and dump* polegają na akumulacji pozycji po niskich cenach, rozpowszechnianiu fałszywych informacji generujących euforię zakupową wśród niedoświadczonych inwestorów, a następnie sprzedaży po sztucznie zawyżonych cenach przed nieuniknionym załamaniem kursu. Federalne Biuro Śledcze w operacji NexFundAI przeprowadzonej w 2024 r. stworzyło specjalnie kryptowalutę w celu schwytania organizatorów takich schematów, co zaowocowało oskarżeniami 18 osób zaangażowanych w manipulacje na rynku aktywów cyfrowych. *Wash trading* polegający na jednoczesnym kupnie i sprzedaży tego samego instrumentu bez zmiany pozycji ekonomicznej sztucznie zawyża wolumen obrotu, tworząc fałszywe wrażenie płynności i zainteresowania inwestorów, a raport firmy Chainalysis z 2024 r. zidentyfikował podejrzaną aktywność wash tradingową o wartości 2,57 mld dolarów na rynkach kryptowalutowych.

Wykorzystywanie informacji poufnych, określane w literaturze anglojęzycznej jako *insider trading*, pozostaje kolejnym problemem rynków kapitałowych podważającym zaufanie inwestorów do uczciwości mechanizmu cenowego. Według danych Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych w 2023 r. złożono 6530 raportów o podejrzanych transakcjach, co stanowiło wzrost o 12% w porównaniu z rokiem poprzednim. Podejrzenia wykorzystywania informacji poufnych stanowiły 51% wszystkich raportów, dominując nad manipulacjami rynkowymi stanowiącymi 47% zgłoszeń, przy czym Niemcy odpowiadały za 33% wszystkich raportów w Unii Europejskiej.

Zagrożenia cybernetyczne dla sektora finansowego eskalują w tempie bezprecedensowym, stanowiąc jedno z najpoważniejszych wyzwań dla bezpieczeństwa rynków kapitałowych w XXI w. Według raportu Europejskiej Agencji ds. Cyberbezpieczeństwa za okres od stycznia 2023 do czerwca 2024 r. sektor finansowy w Unii Europejskiej doświadczył 488 publicznie zgłoszonych incydentów, z czego 46% dotknęło instytucje

kredytowe. Międzynarodowy Fundusz Walutowy raportuje, że skrajne straty cybernetyczne wzrosły czterokrotnie od 2017 r., osiągając poziom 2,5 mld dolarów, a raport firmy Sophos z 2024 r. wskazuje, że 65% instytucji finansowych padło ofiarą oprogramowania typu *ransomware*, co stanowi najwyższy odnotowany wskaźnik w historii badań. Średni koszt odzyskania danych po ataku *ransomware* w sektorze finansowym wyniósł 2,58 mln dolarów, co ilustruje skalę ekonomicznych konsekwencji cyberprzestępczości.

Szczególnie alarmujące z perspektywy bezpieczeństwa narodowego są ataki sponsorowane przez państwa, których celem jest destabilizacja infrastruktury finansowej krajów zachodnich. Chińskie operacje cyberszpiegowskie wzrosły o 150% w 2024 r., przy czym ataki na usługi finansowe, media i sektor przemysłowy zwiększyły się aż o 30%, a grupa znana pod kryptonimem Salt Typhoon skompromitowała co najmniej 9 głównych dostawców telekomunikacyjnych. Rosyjskie cyberataki na Ukrainę wzrosły o 70% w 2024 r., a atak NotPetya z 2017 r. opisywany przez Biały Dom jako najbardziej destrukcyjny i kosztowny cyberatak w historii spowodował straty liczone w miliardach dolarów na skalę globalną, dotykając m.in. duńskiego giganta logistycznego Maersk oraz amerykański koncern farmaceutyczny Merck.

Flash crash z 6 maja 2010 r. pozostaje paradygmatycznym przykładem systemowej podatności rynków na zakłócenia wynikające z interakcji między handlem algorytmicznym a ograniczoną płynnością w warunkach stresowych. W ciągu zaledwie 36 minut indeks Dow Jones Industrial Average spadł o 998,5 punktów, co stanowiło około 9% wartości, tymczasowo wymazując bilion dolarów kapitalizacji rynkowej, a niektóre akcje renomowanych spółek były handlowane po absurdalnych cenach 0,01 dolara lub 100 tys. dolarów. Wspólny raport Komisji Papierów Wartościowych i Giełd oraz Komisji Handlu Towarowymi Kontraktami Terminowymi wskazał jako przyczynę automatyczny program sprzedaży zainicjowany przez firmę zarządzającą aktywami Waddell and Reed Financial, obejmujący 75 tys. kontraktów terminowych E-Mini na indeks S&P 500 o wartości 4,1 mld dolarów wykonywanych bez uwzględnienia ceny czy czasu realizacji. Gdy płynność rynkowa gwałtownie wyparowała, firmy handlujące z wysoką

częstotliwością początkowo absorbowały napływające zlecenia sprzedaży, by następnie masowo się wycofać z rynku, generując efekt domina.

Handel algorytmiczny i wysokiej częstotliwości, choć w normalnych warunkach rynkowych poprawiają płynność i zmniejszają spready transakcyjne, przynosząc korzyści inwestorom, w sytuacjach stresowych mogą zwiększać szoki cenowe i przyczyniać się do kaskadowych załamań. Badania przeprowadzone przez Tokyo Stock Exchange wykazały, że po wprowadzeniu systemu Arrowhead w 2010 r. redukującego opóźnienie realizacji zleceń z 6 sekund do 2 milisekund wskaźniki ryzyka systemowego mierzone metodologią CoVaR i CoVaQ znacząco wzrosły, a amplituda zdarzeń ekstremalnych zwiększyła się od 60% do 180% w zależności od zastosowanej miary.

System nadzoru nad rynkami kapitałowymi opiera się na wielopoziomowej strukturze instytucjonalnej obejmującej organy krajowe, europejskie oraz międzynarodowe mechanizmy koordynacyjne zapewniające spójność regulacji w wymiarze globalnym. W Polsce centralną rolę pełni Komisja Nadzoru Finansowego działająca na podstawie ustawy z 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, realizująca cztery kluczowe funkcje obejmujące licencyjną polegającą na wydawaniu zezwoleń na prowadzenie działalności regulowanej, regulacyjną obejmującą wydawanie rekomendacji i wytycznych dla uczestników rynku, kontrolną realizowaną poprzez inspekcje i analizę raportów przedkładanych przez podmioty nadzorowane oraz dyscyplinującą polegającą na nakładaniu kar finansowych i cofaniu licencji w przypadku stwierdzenia naruszeń. W 2023 r. Komisja Nadzoru Finansowego nałożyła kary w łącznej wysokości 31,4 mln złotych, przy czym najwyższe sankcje dotyczyły naruszeń obowiązków informacyjnych emitentów oraz nieprawidłowości w działalności firm inwestycyjnych.

Na poziomie europejskim Europejski Urząd Nadzoru Giełd i Papierów Wartościowych z siedzibą w Paryżu koordynuje nadzór nad rynkami papierów wartościowych państw członkowskich Unii Europejskiej, sprawując jednocześnie bezpośredni nadzór nad agencjami ratingowymi, repozytoriami transakcji, systemowo ważnymi izbami rozliczeniowymi oraz administratorami kluczowych wskaźników referencyjnych. W 2024 r. europejskie organy nadzoru nałożyły łącznie

ponad 100 mln euro kar administracyjnych za naruszenia przepisów rynku kapitałowego, przy czym najwyższe sankcje dotyczyły naruszeń rozporządzenia w sprawie nadużyć na rynku oraz dyrektywy w sprawie rynków instrumentów finansowych.

Model amerykański reprezentuje Komisja Papierów Wartościowych i Giełd stanowiąca scentralizowaną federalną agencję dysponującą kompleksowymi uprawnieniami wykonawczymi pozwalającymi na bezpośrednie ściganie naruszeń prawa rynku kapitałowego. W roku fiskalnym 2024 amerykańska Komisja Papierów Wartościowych i Giełd osiągnęła rekordowe 8,2 mld dolarów środków zaradczych obejmujących 6,1 mld dolarów z tytułu zwrotu nielegalnie uzyskanych korzyści oraz 2,1 mld dolarów kar cywilnych. Fundamentalna różnica między modelem europejskim a amerykańskim polega na tym, że Komisja Papierów Wartościowych i Giełd dysponuje bezpośrednimi uprawnieniami egzekucyjnymi umożliwiającymi samodzielne prowadzenie postępowań i nakładanie sankcji, podczas gdy Europejski Urząd Nadzoru Giełd i Papierów Wartościowych działa głównie poprzez krajowe organy nadzoru, koordynując ich działania i zapewniając spójność stosowania prawa unijnego.

Kluczowe ramy prawne Unii Europejskiej regulujące funkcjonowanie rynków kapitałowych obejmują dyrektywę oraz rozporządzenie w sprawie rynków instrumentów finansowych znane pod akronimem MiFID II i MiFIR, a także rozporządzenie w sprawie nadużyć na rynku określane jako MAR. Dyrektywa MiFID II obowiązująca od 3 stycznia 2018 r. znacząco rozszerzyła wymogi przejrzystości na instrumenty inne niż akcje, obejmując obligacje, produkty strukturyzowane i instrumenty pochodne, wzmocniła ochronę inwestorów, wprowadzając szczegółowe wymogi dotyczące informowania klientów o kosztach i ryzykach, oraz po raz pierwszy kompleksowo uregulowała handel algorytmiczny, nakładając na firmy inwestycyjne obowiązek wdrożenia mechanizmów kontroli ryzyka. Rozporządzenie MAR obowiązujące od 3 lipca 2016 r. zakazuje wykorzystywania informacji poufnych i manipulacji rynkowych, nakładając na emitentów obowiązek niezwłocznego ujawniania informacji mogących istotnie wpłynąć na cenę instrumentów finansowych oraz prowadzenia list osób mających dostęp do informacji poufnych. Sankcje administracyjne

za naruszenie rozporządzenia MAR mogą sięgać do 5 mln euro dla osób fizycznych i 15 mln euro lub 15% rocznych obrotów dla osób prawnych.

Regulacja krótkiej sprzedaży wprowadzona rozporządzeniem 236/2012 ustanawia dwupoziomowy system przejrzystości, w ramach którego przekroczenie progu 0,1% krótkiej pozycji netto wymaga powiadomienia właściwego organu nadzoru, natomiast przekroczenie progu 0,5% skutkuje obowiązkiem publicznego ujawnienia pozycji. Podczas pandemii COVID-19 w marcu 2020 r. Europejski Urząd Nadzoru Giełd i Papierów Wartościowych tymczasowo obniżył progi notyfikacyjne, a kilka państw członkowskich, w tym Włochy, Francja, Hiszpania i Belgia, wprowadzało czasowe zakazy krótkiej sprzedaży w celu ograniczenia presji spadkowej na rynkach akcji.

Współpraca międzynarodowa w zakresie nadzoru nad rynkami kapitałowymi realizowana jest przede wszystkim w ramach Międzynarodowej Organizacji Komisji Papierów Wartościowych z siedzibą w Madrycie, zrzeszającej 225 członków regulujących łącznie ponad 95% światowych rynków papierów wartościowych. Opracowane przez organizację 38 Zasad Regulacji Papierów Wartościowych stanowi globalny *benchmark* wykorzystywany przez Międzynarodowy Fundusz Walutowy i Bank Światowy w ocenach sektora finansowego przeprowadzanych w ramach Programu Oceny Sektora Finansowego. Polska Komisja Nadzoru Finansowego jest pełnoprawnym członkiem organizacji od 2006 r., aktywnie uczestnicząc w pracach komitetów i grup roboczych opracowujących międzynarodowe standardy nadzorcze.

Mechanizmy ochronne mające na celu zapobieganie kaskadowym załamaniom rynkowym obejmują przede wszystkim wyłączniki automatyczne określane jako *trading curbs* lub *circuit breakers*, a także systemy nadzoru rynkowego oraz wymogi kapitałowe i depozytowe. W Stanach Zjednoczonych obowiązują ogólnorynkowe wyłączniki skorelowane z indeksem S&P 500. Spadek wartości indeksu o 7% (Level 1) lub o 13% (Level 2) przed godziną 14:25 czasu centralnego (CT) skutkuje wstrzymaniem obrotu na 10 minut zarówno na rynku kasowym, jak i na wszystkich amerykańskich kontraktach terminowych oraz opcjach opartych na indeksach giełdowych. Jeżeli zaś spadek osiągnie 20% (Level 3), obrót zostaje zawieszony do końca dnia sesyjnego. Należy przy tym zaznaczyć, że w ostatnich

35 minutach sesji (14:25–15:00 CT) aktywny pozostaje wyłącznie próg 20%. Mechanizm ten został uruchomiony czterokrotnie w marcu 2020 r., podczas gwałtownej przeceny wywołanej pandemią COVID-19, co stanowiło pierwsze jego zastosowanie od 1997 r.

W Europie, zgodnie z regulacjami MiFID II, stosowane są mechanizmy przerywające handel dla poszczególnych instrumentów – tzw. *volatility interruptions*. Nie funkcjonują jednak ogólnorynkowe wyłączniki analogiczne do amerykańskich. W konsekwencji, nawet gdy włoski indeks FTSE MIB spadł o około 16% w marcu 2018 r., nie doszło do ponadnarodowego zawieszenia notowań na europejskich rynkach kapitałowych.

Systemy nadzoru rynkowego wykorzystują zaawansowane techniki analityczne, w tym algorytmy sztucznej inteligencji i uczenia maszynowego, do identyfikacji nietypowych wzorców transakcyjnych mogących wskazywać na manipulacje cenowe, wykorzystywanie informacji poufnych lub inne formy nadużyć. Wśród rozwiązań stosowanych na globalnych rynkach znajduje się m.in. system SMARTS monitorujący ponad 200 platform obrotu i zdolny do rozpoznawania przeszło 300 typów zachowań o potencjale manipulacyjnym. Segment technologii nadzorczych rośnie w tempie około 10–11% rocznie, co jest wynikiem rosnących wymogów regulacyjnych, w szczególności wynikających z dyrektywy MiFID II oraz rozporządzenia MAR, nakładających na infrastrukturę rynku obowiązek stosowania efektywnych mechanizmów detekcji i prewencji nadużyć.

Wymogi kapitałowe określane przez standardy Bazylea III oraz Bazylea IV ustanawiają minimalny współczynnik kapitału podstawowego Tier 1 na poziomie 4,5% aktywów ważonych ryzykiem, powiększony o bufor ochronny wynoszący 2,5%. Dla instytucji o znaczeniu systemowym (G-SIB) przewidziano dodatkowe narzuty kapitałowe w przedziale 1–4,5% w zależności od profilu ryzyka i stopnia powiązań sieciowych. Rozporządzenie CRR3, obowiązujące od 1 stycznia 2025 r., wprowadza tzw. *output floor* ograniczający redukcję wymogów kapitałowych poprzez stosowanie wewnętrznych modeli ryzyka, zapewniając większą porównywalność i stabilność międzynarodowych standardów ostrożnościowych.

Rozporządzenie EMIR nakłada obowiązek centralnego rozliczania standaryzowanych instrumentów pochodnych zawieranych poza rynkami regulowanymi oraz ustanawia ramy funkcjonowania centralnych

kontrahentów (CCP). Wymogi dotyczące depozytów zabezpieczających obejmują depozyt początkowy odzwierciedlający przyszłą ekspozycję oraz depozyt uzupełniający równoważący dzienne zmiany wartości pozycji. EMIR 3.0, obowiązujący od 2025 r., wprowadza wymóg tzw. aktywnego rachunku, zobowiązujący kontrahentów unijnych do utrzymywania rozliczeń określonych kategorii instrumentów w CCP działających na terytorium Unii Europejskiej.

W Polsce funkcję centralnego kontrahenta pełni KDPW_CCP, autoryzowany zgodnie z rozporządzeniem EMIR. Instytucja ta dysponuje kapitałem zakładowym wynoszącym 190 mln złotych i wykorzystuje wielowarstwowy system zabezpieczeń oparty na metodyce SPAN. Obejmuje on fundusz gwarancyjny finansowany przez uczestników rozliczających, depozyty początkowe kalkulowane na podstawie wartości zagrożonej ryzykiem (*Value at Risk*) oraz wkład własny izby stanowiący element kaskady zabezpieczeń (*default waterfall*) aktywowanej w przypadku niewypłacalności uczestnika.

Testy warunków skrajnych realizowane przez Europejski Urząd Nadzoru Bankowego obejmują w edycji 2025 r. ponad 60 instytucji reprezentujących około 70–75% aktywów bankowych Unii Europejskiej. Scenariusze niekorzystne uwzględniają m.in. skumulowany spadek PKB o 6,3% oraz testują odporność sektora na zakłócenia kredytowe, rynkowe, operacyjne czy geopolityczne. Dla centralnych kontrahentów EMIR przewiduje obowiązek codziennego testowania depozytów, obejmujący minimalnie 2 scenariusze hipotetyczne i 3 historyczne odzwierciedlające okresy podwyższonej zmienności.

Systemy wczesnego ostrzegania stanowią integralny komponent architektury makroostrożnościowej, umożliwiając identyfikację narastających napięć systemowych przed ich materializacją. Wykorzystuje się w nich m.in. lukę kredyt–PKB (*Credit-to-GDP gap*) – to jeden z najważniejszych i najczęściej używanych sygnałów ostrzegawczych, zwłaszcza w ramach Bazylejskiego Komitetu Nadzoru Bankowego (BCBS), ponieważ wskazuje na nadmierny wzrost akcji kredytowej w stosunku do trendu PKB, co często poprzedza kryzysy kredytowe; spready kredytowe – różnice w oprocentowaniu długu o różnym poziomie ryzyka, np. spready obligacji korporacyjnych vs. obligacji skarbowych, co wskazuje na rosnącą

awersję do ryzyka na rynku; indeks zmienności VIX – potocznie nazywany „indeksem strachu", który mierzy oczekiwaną zmienność na rynku akcji, a jego wysokie wartości często poprzedzają poważne zawirowania na rynkach; oraz miary oparte na analizie sieci powiązań finansowych, takie jak Marginal Expected Shortfall (MES) – mierzy oczekiwany spadek wartości kapitału instytucji finansowej, jeśli system finansowy jako całość doświadczy skrajnie niekorzystnego scenariusza (kryzysu); Delta CoVaR – mierzy, jak warunkowa wartość zagrożona (VaR) całego systemu zmienia się w zależności od tego, czy dana instytucja jest w stanie zagrożenia i służy do szacowania systemowej istotności instytucji; czy SRISK (Systemic Risk Analysis Summary) – opracowany przez NYU V-Lab jako miara oczekiwanego deficytu kapitału instytucji finansowej w trakcie kryzysu systemowego. Badania wskazują na wysoką skuteczność narzędzi sieciowych w wyznaczaniu sygnałów wyprzedzających, zwłaszcza w odniesieniu do kryzysów wywołanych kumulacją ryzyka w sektorze bankowym i pozabankowym.

Transmisja destabilizacji rynków finansowych do gospodarki realnej odbywa się poprzez liczne mechanizmy wzmacniające. Kanał stopy procentowej oddziałuje na warunki finansowania w gospodarce za pośrednictwem zmian rentowności obligacji skarbowych i korporacyjnych. Kanał majątkowy wpływa na wydatki konsumpcyjne poprzez efekt wyceny aktywów; szacuje się, że spadek cen akcji o 10% może powodować redukcję konsumpcji w przedziale od 0,1% do 0,7% w zależności od gospodarki. Krańcowa skłonność do konsumpcji z tytułu zmian wartości portfela akcji wynosi przeciętnie 2,8–5 centów na każdy dodatkowy dolar majątku.

Mechanizm akceleratora finansowego wzmacnia negatywne szoki poprzez wzrost premii za finansowanie zewnętrzne oraz pogorszenie kondycji bilansowej przedsiębiorstw. Badania wykazują, że jednostki dotknięte ograniczeniami kredytowymi znacząco redukują inwestycje, nakłady na badania i rozwój oraz zatrudnienie, co pogłębia i wydłuża recesję gospodarczą.

Kryzys finansowy lat 2007–2008 stanowi przykład systemowej destabilizacji wynikającej z akumulacji ryzyka kredytowego, nadmiernej dźwigni finansowej oraz niedoskonałości mechanizmów oceny ryzyka w sektorze bankowym i rynkach kapitałowych. W jego przebiegu

odnotowano silne spadki cen aktywów, zamrożenie rynku międzybankowego oraz znaczące odchylenie PKB od ścieżki trendu. Kryzys doprowadził do globalnej rewizji regulacji, w tym do wdrożenia w USA ustawy Dodd–Frank (Dodd-Frank Wall Street Reform and Consumer Protection Act) oraz w Unii Europejskiej pakietu CRD IV/CRR (Capital Requirements Directive IV), które ustanowiły nowe ramy zarządzania ryzykiem systemowym, ograniczeń działalności handlowej oraz nadzoru nad instrumentami pochodnymi.

Epizod związany z gwałtownym wzrostem cen akcji spółki GameStop w 2021 r. unaocznił rosnącą rolę inwestorów detalicznych oraz znaczenie platform komunikacji społecznościowej w dynamice rynków akcji. Zjawisko *short squeeze* ujawniło podatność systemu rozliczeniowego na gwałtowne skoki płynnościowe oraz zainicjowało debatę dotyczącą praktyk płatności za przepływ zleceń (*payment for order flow*), odpowiednich wymogów kapitałowych izb rozliczeniowych oraz ogólnej stabilności mikrostruktury rynku.

Zaburzenia związane z pandemią COVID-19 w 2020 r. doprowadziły do najszybszego w historii przejścia głównych indeksów amerykańskich w fazę rynku sparkową, czemu towarzyszyło wielokrotne uruchamianie wyłączników bezpieczeństwa ograniczających nadmierną zmienność. Stabilizacja rynków nastąpiła dopiero po zastosowaniu nadzwyczajnych narzędzi polityki pieniężnej, obejmujących szeroko zakrojony skup aktywów oraz programy wsparcia płynności.

Rynki kapitałowe stanowią kluczowy element infrastruktury krytycznej, co znajduje odzwierciedlenie zarówno w amerykańskich regulacjach dotyczących cyberbezpieczeństwa, jak i europejskich ramach obejmujących m.in. dyrektywę NIS 2 oraz o odporności podmiotów krytycznych. Znaczna część cyberataków wymierzana jest w sektor finansowy, co potwierdza rosnącą potrzebę wzmacniania jego odporności poprzez jednolite standardy techniczne i organizacyjne.

Rozporządzenie DORA (Digital Operational Resilience Act) – prawo Unii Europejskiej (Rozporządzenie UE 2022/2554), w pełni stosowane od 17 stycznia 2025 r., ustanawia jednolite ramy cyfrowej odporności operacyjnej dla instytucji finansowych w Unii Europejskiej. Obejmuje ono m.in. wymogi w zakresie zarządzania ryzykiem ICT, procedury raportowania

incydentów, zaawansowane testy, zasady zarządzania relacjami z dostawcami technologii oraz mechanizmy wymiany informacji o zagrożeniach. Regulacja dotyczy szerokiego grona podmiotów finansowych oraz zapewnia nadzór nad krytycznymi dostawcami usług technologicznych.

Finansowanie obronności za pośrednictwem rynków kapitałowych nabiera szczególnego znaczenia w kontekście nasilających się napięć geopolitycznych. Program ReArm EU obejmuje emisję pożyczek gwarantowanych przez Unię Europejską o łącznej wartości 150 mld euro, przeznaczonych na rozwój wspólnych zdolności obronnych, w tym systemów przeciwlotniczych, artylerii, dronów bojowych i cyberbezpieczeństwa. Europejskie ramy finansowania obronności uwzględniają również rozwijający się rynek obligacji obronnych, instrumentów strukturyzowanych oraz funduszy inwestycyjnych ukierunkowanych na modernizację infrastruktury militarnej.

Aleksander Wasiuta

A. Admati, M. Hellwig, *The Bankers New Clothes: What's Wrong with Banking and What to Do about It – New and Expanded Edition*, Princeton University Press, Princeton 2023; Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, Dz. Urz. UE L 173 z 12.06.2014, https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2014-65-ue-w-sprawie-rynkow-instrumentow-finansowych-oraz-68434694 (dostęp 24.11.2025); ENISA Threat Landscape: Finance Sector, European Union Agency for Cybersecurity, Athens 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector (dostęp 24.11.2025); *Findings Regarding the Market Events of May 6, 2010*, U.S. Securities and Exchange Commission, Washington 2010, https://www.sec.gov/news/studies/2010/marketevents-report.pdf (dostęp 24.11.2025); FSB–IMF, *Early Warning Exercise*, Financial Stability Board, Basel 2024, https://www.imf.org/en/about/factsheets/sheets/2023/early-warning-exercise (dostęp 24.11.2025); P.K. Jain, P. Jain, T.H. McInish, *Does high-frequency trading increase systemic risk?*, „Journal of Financial Markets" 2016, vol. 31; A. Kirilenko, A.S. Kyle, M. Samadi, T. Tuzun, *The flash crash: High-frequency trading in an electronic market*, „The Journal of Finance" 2017, vol. 72, no. 3; *Market Manipulation: Suspected Wash Trading on Select Blockchains May Account for Up To $2.57 Billion in Trading Volume*, Chainalysis, New York 2025, https://www.chainalysis.com/blog/crypto-market-manipulation-wash-trading-pump-and-dump-2025/ (dostęp 24.11.2025);

Objectives and Principles of Securities Regulation, International Organization of Securities Commissions, Madrid 2017, https://www.iosco.org/library/pubdocs/pdf/ioscopd561.pdf (dostęp 24.11.2025); *Raport o stabilności systemu finansowego*, NBP, Warszawa 2025, https://nbp.pl/system-finansowy/raporty-o-stabilnosci-systemu-finansowego/ (dostęp 24.11.2025); Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji, Dz. Urz. UE L 201 z 27.07.2012, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A02012R0648-20250117 (dostęp 24.11.2025); Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku, Dz. Urz. UE L 173 z 12.06.2014, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014R0596 (dostęp 24.11.2025); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011, https://eur-lex.europa.eu/eli/reg/2022/2554/oj?locale=pl (dostęp 24.11.2025); *Sanctions and Measures Imposed in Member States in 2024*, ESMA, Paris 2025, https://www.esma.europa.eu/sites/default/files/2025-10/ESMA43-1527801302-1828_Annual_Sanctions_Report_2025.pdf (dostęp 24.11.2025); *SEC Announces Enforcement Results for Fiscal Year 2024*, U.S. Securities and Exchange Commission, Washington 2024, https://www.sec.gov/newsroom/press-releases/2024-186 (dostęp 24.11.2025); I. Sroka, *Risk management in KDPW_CCP clearing house*, „European Management Studies" 2013, vol. 11(42); Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, Dz.U. 2005, nr 183, poz. 1538 z późn. zm., https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20051831538 (dostęp 24.11.2025); Ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych, Dz.U. 2005, nr 184, poz. 1539 z późn. zm., https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20051841539 (dostęp 24.11.2025); Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, Dz.U. 2006, nr 157, poz. 1119 z późn. zm., https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20061571119 (dostęp 24.11.2025).

BEZPIECZEŃSTWO W SENSIE POZYTYWNYM I NEGATYWNYM. Sam termin bezpieczeństwo na ogół definiuje się jako stan pozbawiony niepokoju, eliminujący oznaki niepewności. Definicja pochodzi od łacińskiego *sine cura* (*securus*), co tłumaczy się jako bez pieczy, bez troski, bez zmartwienia czy też strachu, bowiem *sine* oznacza bez, natomiast *cura*

– zmartwienie, strach, obawę. Przeważnie, w opracowaniach słownikowych i encyklopedycznych, bezpieczeństwo jest utożsamiane ze stanem spokoju i niezagrożenia, który daje poczucie pewności i gwarancje jego zachowania, z jednoczesną szansą na doskonalenie.

Bezpieczeństwo jest wartością samą w sobie, celem, do którego należy dążyć, a jednocześnie jest traktowane w kategoriach jednej z podstawowych potrzeb człowieka, najbardziej cenionych i chronionych. Nie bez powodu Abraham Maslow umieścił bezpieczeństwo w piramidzie potrzeb człowieka na drugim miejscu, zaraz po potrzebach egzystencjalnych.

Bezpieczeństwo, pomimo swej ewolucji i redefinicji, współcześnie nadal jest postrzegane co najmniej w trzech istotnych wymiarach: 1) ontologicznym (który określa istotę jego bytu), 2) epistemologicznym (koncentrującym się na sposobach jego naukowego poznania), 3) przedmiotowym – zakresowym (wskazującym na jego znaczenie). W literaturze przedmiotu z zakresu politologii i obronności przeważnie dominuje ujęcie przedmiotowe bezpieczeństwa, jednakże należy pamiętać, że wraz z pojawieniem się nowych jego zagrożeń, a także w wyniku rekonfiguracji ładu światowego (zwłaszcza po zakończeniu okresu tzw. zimnej wojny) bezpieczeństwo przestało być postrzegane jedynie przez pryzmat sfery politycznej i militarnej, dostrzegając nowe jego rodzaje, jak chociażby bezpieczeństwo ekonomiczne, społeczne, ekologiczne, energetyczne itp. Analogiczne stanowisko możemy odnaleźć w publikacji Barry'ego Buzana, który opisał kilka sektorów bezpieczeństwa, biorąc pod uwagę nie tylko czynniki militarne, ale również polityczne, ekonomiczne, społeczne oraz kulturowe.

W opinii Bogdana Zdrodowskiego sztandarowa koncepcja bezpieczeństwa zaproponowana z kolei przez Daniela Frei'a, a koncentrująca się na konkretnych jego stanach i uwzględniająca czynnik obiektywny (brak rzeczywistego zagrożenia) oraz subiektywny (brak poczucia zagrożenia), jest w zasadzie jednowymiarową definicją bezpieczeństwa.

Słuszna w tym miejscu i precyzyjna wydaje się zatem definicja zaproponowana przez Ryszarda Ziębę, w ocenie którego bezpieczeństwo to „pewność istnienia i przetrwania, stanu posiadania oraz funkcjonowania i rozwoju podmiotu". Zięba podkreśla, iż owa pewność to rezultat nie tylko braku zagrożeń (czy też ich niewystępowania lub eliminowania), ale i twór

kreatywnej aktywności podmiotu, podlegający jednocześnie naturalnym i nieuniknionym wręcz przeobrażeniom. To pozytywne odniesienie do definicji bezpieczeństwa podkreśla jego wielowymiarowość, ponieważ nie ogranicza się ono jedynie do wolności od zagrożeń, ale uaktywnia podmiot na rzecz zapewnienia ciągłości istnienia i stabilnego rozwoju.

Równie ciekawe poglądy na pozytywną definicję bezpieczeństwa prezentuje Stanisław Koziej, utożsamiając je z „dziedziną aktywności, która zmierza do zapewnienia możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów". Koziej odnosi się tu również do kolejnej kategorii, mianowicie – bezpieczeństwa w sensie statycznym (stan braku zagrożeń dla podmiotu, stan spokoju, pewności, stan obiektywny i subiektywny; uświadomiony i nieuświadomiony) oraz dynamicznym (aktywność podmiotu na rzecz bezpieczeństwa).

Z kategorią szans na doskonalenie jest ściśle związane omawiane bezpieczeństwo w sensie pozytywnym (szerokim), składające się z dwóch zasadniczych elementów, mianowicie – gwarancji przetrwania i swobody rozwoju, dzięki której podmiot (jednostka, państwo bądź organizacja międzynarodowa) nie postrzega wszystkich zjawisk pochodzących z otoczenia systemu bezpieczeństwa jako zagrożenia, a jest w stanie skutecznie na nie reagować, jeśli takowe się pojawiają. Pozytywny sposób definiowania terminu bezpieczeństwo, uwzględniając charakterystyczny dla danej zbiorowości poziom kultury bezpieczeństwa, może zatem stanowić gwarant istnienia, przetrwania, stabilności, godności, tożsamości, wolności, niezależności, jak również ochrony dobrobytu itp.

Równolegle do bezpieczeństwa w sensie pozytywnym, przeważnie w języku potocznym, funkcjonuje jeszcze negatywny (wąski) sposób definiowania tego terminu. Mianowicie, zgodnie z definicją negatywną, bezpieczeństwo jawi się po prostu jako brak zagrożeń, zatem zasadniczym elementem bezpieczeństwa w sensie negatywnym będzie jedynie gwarancja przetrwania podmiotu, bez istotnej zdolności swobody rozwoju,

która to, w przypadku bezpieczeństwa pozytywnego, umożliwia podjęcie właściwej reakcji na potencjalne zagrożenia.

Negatywne pojmowanie bezpieczeństwa w swoich rozważaniach proponował m.in. Arnold Wolfers, utożsamiając bezpieczeństwo w sensie obiektywnym z brakiem zagrożeń dla nabytych wartości, z kolei w sensie subiektywnym – z brakiem strachu, że owe wartości zostaną naruszone.

Negatywny wymiar bezpieczeństwa może być determinowany przez wiele czynników subiektywnych bądź obiektywnych; w głównej mierze bezpieczeństwo negatywne prezentuje postawę izolacji, wręcz nieufności wobec otoczenia. Podmiot skupia się przeważnie na zagrożeniach, co w konsekwencji prowadzi do petryfikacji oraz inercji w postrzeganiu rzeczywistości i podejmowaniu jakichkolwiek działań; wówczas podmiot utożsamia rzeczywistość wyłącznie jako źródło zagrożeń, przyjmując tym samym postawę sceptyczną wobec wszystkiego co innowacyjne.

Z negatywnym ujęciem bezpieczeństwa koresponduje tzw. tradycyjne jego pojmowanie, skupiające się na wymiarze militarnym i przez ten pryzmat definiujące potencjalne zagrożenia. Zatem w tym kontekście bezpieczeństwo dotyczy stanu braku konfliktu (również zbrojnego) oraz braku ryzyka jego wystąpienia. To klasyczne podejście definiowania bezpieczeństwa znalazło również odzwierciedlenie w poglądach realistów eksponujących siłę państwa.

Odwoływanie się do pozytywnego bądź negatywnego sposobu pojmowania bezpieczeństwa jest również charakterystyczne dla prób definiowania go w ujęciu narodowym, bowiem w tradycyjnym, wąskim znaczeniu (odpowiadającym podejściu negatywnemu) jest ono utożsamiane z przetrwaniem (samozachowaniem), a więc dotyczy *stricte* ochrony integralności terytorialnej, a także niezależności politycznej. Jest to zarazem rozumienie ogólne uwzględniające jedynie wartości podstawowe dla kategorii państwa. Natomiast w znaczeniu szerokim (korespondującym z ujęciem pozytywnym) bezpieczeństwo narodowe, oprócz wartości podstawowych takich jak przetrwanie, integralność terytorialna czy suwerenność zewnętrzna, obejmuje także samowładność, swobodę afiliacji oraz wartości szczególne, do których zalicza się dobrobyt, rozwój społeczno-gospodarczy, rozwój kulturalny itp.

Podsumowując, w sensie uniwersalnym bezpieczeństwo stanowi „jedną z najistotniejszych sfer (części, stanów, potrzeb, odczuć, wartości, celów) konkretnego bytu (rzeczy, organizacji, zjawiska), dotyczącą wszystkich jego kategorii (elementów, struktur, funkcji), związaną z zapewnieniem interesu tego podmiotu". Podejście negatywne nakazuje ujmować bezpieczeństwo jako brak zagrożeń, odnosząc się wyłącznie do analizy oddziaływań podmiotu w celu ochrony przed zagrożeniami dla jego kluczowych wartości wewnętrznych, co z kolei oznacza jedynie bierną ochronę. Natomiast ujęcie pozytywne kładzie nacisk na kształtowanie pewności, posiadania i swobód rozwojowych, skupiając się na kreatywnej aktywności podmiotu. Bezpieczeństwo rozumiane w sposób pozytywny kładzie nacisk na aktywne podejście, które skupia się na kreowaniu pewności, rozwoju i rezyliencji (odporności) na zagrożenia; natomiast w modelu negatywnym podmiot unika zagrożeń. W przeciwieństwie do modelu negatywnego bezpieczeństwo pozytywne cechuje: 1) aktywność i świadomość sprawczości podmiotu (odwołujące się również do umiejętności przewidywania możliwych skutków i kształtowania właściwych postaw); 2) rozwój (wraz z kreowaniem pożądanych warunków do nieskrępowanego działania); 3) pewność (w wymiarze niematerialnym przejawiająca się w zaufaniu i poczuciu bezpieczeństwa, a w znaczeniu niematerialnym oznaczająca stabilność).

Należy mieć na uwadze, że oba modele bezpieczeństwa, zarówno pozytywny, jak i negatywny, stanowią kategorie wzajemnie się przenikające i uzupełniające, a w zależności od potrzeb kreują analizy współczesnego środowiska bezpieczeństwa. Dlatego też podejmując rozważania definicyjne nad terminem bezpieczeństwa, nie należy ograniczać się wyłącznie do jednego aspektu tej kategorii, bowiem jego domeną jest wielowymiarowość, dynamiczność oraz interdyscyplinarność.

Julia Anna Gawęcka

Bezpieczeństwo, [w:] *Słownik terminów z zakresu bezpieczeństwa narodowego*, B. Zdrodowski (red.), Wydawnictwo AON, Warszawa 2008; B. Buzan, *People, States and Fear. An Agenda for International Security Studies in the Post-Cold War Era*,↱ Lynne Rienner Pub, London 1991; M. Cieślarczyk, R. Kuriata, *Kryzysy i sposoby radzenia sobie z nimi*, WSK, Łódź 2005; J. Falecki, *Bezpieczeństwo*, [w:]

Encyklopedia bezpieczeństwa, t. 1, O. Wasiuta, S. Wasiuta (red.), Wydawnictwo Libron, Kraków 2021; S. Koziej, *Wstęp do teorii i historii bezpieczeństwa. Skrypt internetowy*, https://koziej.pl/wp-content/uploads/2017/09/Teoria_i_historia_bezpieczenstwa.pdf (dostęp 27.11.2025); A. Maslow, *Motywacja i osobowość*, tłum. J. Radzicki, Wydawnictwo Naukowe PWN, Warszawa 2010; J.S. Nye, *Problemy badań nad bezpieczeństwem*, „Sprawy Międzynarodowe" 1989, nr 6; I. Pawlikowska, *Bezpieczeństwo jako cel polityki zagranicznej państwa*, [w:] *Wstęp do teorii polityki zagranicznej państwa*, R. Zięba (red.), Wydawnictwo Adam Marszałek, Toruń 2005; *Security*, [w:] *Webster's Third New International Dictionary of the English Language*, P.B. Gove (ed.), Könemann, Chicago–Toronto 1993; K. Świerszcz, *Bezpieczeństwo państwa w czasach współczesnych w ujęciu podmiotowo-aksjologicznych wyzwań*, https://share.google/1yL6p2859sKO1Wnxa (dostęp 27.11.2025); A. Wolfers, *National Security as an Ambiguous Symbol*, „Political Science Quarterly" 1952, vol. LXVII, no. 4, https://academic.oup.com/psq/article-abstract/67/4/481/7245057 (dostęp 27.11.2025); B. Zdrodowski, *Istota bezpieczeństwa państwa*, „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate" 2019, nr 9(3); R. Zięba, *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych*, [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, D.B. Bobrow, E. Haliżak, R. Zięba (red.), Wydawnictwo Naukowe Scholar, Warszawa 1997; R. Zięba, *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe AON" 2012, nr 1(86).

BEZPIECZEŃSTWO ŻYWNOŚCIOWE – ochrona życiowych interesów człowieka, która wyraża się w zagwarantowaniu przez państwo nieograniczonego ekonomicznego dostępu do produktów żywnościowych w celu utrzymania normalnej aktywności życiowej. Jest to stan, w którym wszyscy ludzie, w każdym czasie mają fizyczny, ekonomiczny i społeczny dostęp do wystarczającej ilości bezpiecznej, wartościowej i wysokiej jakości żywności, niezbędnej do prowadzenia aktywnego i zdrowego życia. Od 2012 r. obliczany jest Globalny Indeks Bezpieczeństwa Żywnościowego.

Po raz pierwszy termin „bezpieczeństwo żywnościowe" został wprowadzony do obiegu międzynarodowego po kryzysie zbożowym w latach 1972–1973. Na Zgromadzeniu Ogólnym ONZ w 1974 r. przyjęto rezolucję Międzynarodowe zobowiązania w zakresie zapewnienia bezpieczeństwa żywnościowego na świecie. Bezpieczeństwo żywnościowe świata rozumiano wówczas głównie jako utrzymanie stabilności rynków żywnościowych przy zapewnieniu dostępności podstawowych produktów żywnościowych dla wszystkich krajów świata. Jak wskazuje Swietłana Urba, współczesne

bezpieczeństwo żywnościowe to stan gospodarki państwa, w którym gwarantowane jest stabilne zaopatrzenie przemysłu przetwórczego w surowce rolnicze, ludności – wystarczającą ilość bezpiecznych i pełnowartościowych produktów żywnościowych, a także względna niezależność od importu surowców i żywności. Z kolei Tetiana Biełousko uważa, że bezpieczeństwo żywnościowe to stan gospodarki kraju lub jego regionów, który zapewnia produkcję lub import żywności, stabilność jej zapasów na potrzeby swobodnego handlu oraz dostępność rynku żywności dla wszystkich warstw i grup społecznych. Istnieją również bardziej zwięzłe definicje badanego pojęcia. Zdaniem Olena Kirilesko bezpieczeństwo żywnościowe to zdolność państwa do zagwarantowania zaspokojenia potrzeb żywnościowych na poziomie niezbędnym do normalnego funkcjonowania społeczeństwa. Inni traktują bezpieczeństwo żywnościowe jako stan systemu społeczno-ekonomicznego kraju, w którym każdy obywatel ma możliwość uzyskania minimalnego zestawu produktów żywnościowych.

Istnieją dwa główne podejścia interpretacyjne – ekonomo- i humanocentryczne. Podejście pierwsze jest charakterystyczne dla większości krajowych badaczy-ekonomistów i polega na koncentracji uwagi na bezpieczeństwie żywnościowym na poziomie państwa i jego regionów, a także interakcjach między krajowym i międzynarodowym systemem bezpieczeństwa żywnościowego. Rzadziej spotykane jest podejście humanocentryczne, które traktuje człowieka i rodzinę (gospodarstwo domowe) jako kluczowe elementy systemu bezpieczeństwa żywnościowego; wszystkie pozostałe poziomy – od regionalnego po międzynarodowy – są ukierunkowane na maksymalne zaspokojenie potrzeb człowieka.

Bezpieczeństwo żywnościowe określa się na różnych poziomach: globalnym, regionalnym, krajowym, lokalnym oraz na poziomie gospodarstw domowych i jednostki. Globalne bezpieczeństwo żywnościowe oznacza, że światowy przemysł spożywczy powinien produkować wystarczającą ilość żywności w celu zaspokojenia rosnących potrzeb ludności. Handel powinien odbywać się bez przeszkód przy względnie stabilnych cenach, aby kraje mogły uzupełniać własną produkcję poprzez import. Bezpieczeństwo żywnościowe na poziomie krajowym i regionalnym jest warunkiem koniecznym, lecz niewystarczającym; obejmuje zdolność państw i gospodarstw domowych do uzyskania niezbędnych produktów.

Kwestie bezpieczeństwa żywnościowego rozpatrywane są w dwóch aspektach: jako bezpieczeństwo żywnościowe (*food security*) oraz bezpieczeństwo żywności (*food safety*). Pierwsze podejście stosuje się głównie w badaniach na poziomie międzynarodowym i krajowym, drugie natomiast – w analizie bezpieczeństwa żywności na poziomie gospodarstw domowych lub jednostki. Centralnym elementem bezpieczeństwa żywnościowego jest zapewnienie żywności, a w jego strukturze wyróżnia się cztery komponenty: dostępność, wartość odżywczą, bezpieczeństwo oraz samowystarczalność. Podstawową produkcją przemysłu spożywczego są produkty żywnościowe, czyli substancje, które mogą być wykorzystane do zaspokojenia fizjologicznych potrzeb człowieka w zakresie żywienia i wody, a także innych potrzeb, z wyłączeniem leków i innych środków medycznych.

Wyróżnia się cztery podstawowe filary bezpieczeństwa żywnościowego: dostępność żywności (*availability*), dostęp do żywności (*access*), wykorzystanie żywności i jej jakość (*utilization*) oraz stabilność (*stability*). Naruszenie choćby jednego z tych elementów prowadzi do negatywnych konsekwencji społecznych, ekonomicznych i politycznych. Skutki społeczne obejmują wzrost głodu i niedożywienia, pogorszenie stanu zdrowia ludności, wzrost śmiertelności dzieci, napięcia społeczne i protesty; ekonomiczne – spadek produktywności pracy, wzrost wydatków na ochronę zdrowia oraz zwiększenie zależności od importu; polityczne i bezpieczeństwa zaś – destabilizację państwa, nasilenie procesów migracyjnych oraz wykorzystanie żywności jako narzędzia nacisku politycznego lub militarnego. Bezpieczeństwo żywnościowe to nie tylko kwestia dostępu do pożywienia, ale również stabilności ekonomicznej, sprawiedliwości społecznej, zdrowia narodu oraz suwerenności państwa. Stan rynku żywności i zapewnienie ludności wysokiej jakości produktów żywnościowych pozostają jednymi z najważniejszych problemów państwa. Od ilości i jakości spożywanej żywności zależą zdrowie narodu, zdolność do pracy, długość życia oraz możliwości intelektualne człowieka.

Stan rynku żywności oraz kwestie zapewnienia ludności wysokiej jakości produktów żywnościowych były i pozostają jednymi z najbardziej aktualnych problemów państwa. Rynek żywności powinien zapewniać gwarantowany dostęp ludności do żywności w niezbędnej ilości

i asortymencie. Od ilości i jakości spożywanej żywności zależy zdrowie narodu, zdolność do pracy, długość życia człowieka oraz jego zdolności intelektualne. Zgodnie z ocenami ekspertów WHO zdrowie obywateli w 8–12% zależy od systemu ochrony zdrowia w kraju, w 18–20% – od predyspozycji genetycznych człowieka, a w 68–74% – od stylu życia, którego jednym z najważniejszych elementów jest żywienie. Międzynarodowi eksperci uważają, że już za życia obecnego pokolenia problem żywnościowy może przerodzić się w głęboki kryzys międzynarodowy. Według danych Światowej Konferencji Żywnościowej, która odbyła się w listopadzie 1996 r. w Rzymie, tylko w krajach rozwijających się chronicznie głoduje 840 mln ludzi. Jednocześnie 50% światowej produkcji żywności jest konsumowane przez najbardziej rozwinięte kraje, w których mieszka jedynie jedna piąta ludności świata.

Ze względu na swoje znaczenie ekonomiczne bezpieczeństwo żywnościowe obejmuje trzy podstawowe warunki jego osiągnięcia, a mianowicie:

- fizyczną dostępność żywności, czyli obecność produktów żywnościowych na całym terytorium kraju w każdej sytuacji zapotrzebowania i w niezbędnym asortymencie;
- ekonomiczną dostępność żywności, w której poziom dochodów ludności umożliwia zakup produktów żywnościowych, niezależnie od statusu społecznego i miejsca zamieszkania;
- bezpieczeństwo żywności, rozumiane jako możliwość zapobiegania produkcji, sprzedaży i spożywaniu produktów żywnościowych niskiej jakości, które szkodzą zdrowiu ludności.

Zapewnienie produkcji wysokiej jakości i bezpiecznych produktów żywnościowych, jak pokazuje doświadczenie krajów będących liderami w przemyśle spożywczym, jest możliwe jedynie przy spełnieniu wielu obowiązkowych wymagań. Przede wszystkim surowce rolnicze muszą spełniać normy bezpieczeństwa i jakości (takich obowiązkowych wskaźników jest kilkadziesiąt). W procesie produkcji żywności powinny być wykorzystywane nowoczesne technologie oraz odpowiedni sprzęt do ich przetwarzania. Jakość produktów żywnościowych powinna być zapewniana poprzez tworzenie w przedsiębiorstwach systemów zarządzania jakością zgodnych z międzynarodowymi standardami.

Bezpieczeństwo żywnościowe państwa we współczesnych warunkach może być rozpatrywane jako jeden z najważniejszych elementów bezpieczeństwa narodowego, ponieważ bezpośrednio dotyczy zapewnienia zdrowia społeczeństwa oraz reprodukcji ludności. Zaspokojenie jednej z podstawowych potrzeb człowieka – potrzeby żywienia – na obecnym etapie rozwoju społeczeństwa staje się niemożliwe bez wykorzystania osiągnięć postępu naukowo-technicznego, w szczególności w rolnictwie oraz przemyśle spożywczym. W związku z tym poziom zapewnienia bezpieczeństwa żywnościowego ludności, zwłaszcza w warunkach społeczeństwa postindustrialnego, bezpośrednio zależy od skali wdrażania innowacji zarówno w praktyce działalności przedsiębiorstw sektora rolno-spożywczego, jak i w sferze zarządzania branżą produkcji żywności.

Uwzględniając istniejące problemy, zasadne wydaje się wdrożenie działań mających na celu zwiększenie poziomu konkurencyjności krajowej produkcji sektora rolno-spożywczego na rynku europejskim poprzez harmonizację standardów, rozwój infrastruktury, wspieranie innowacji, współpracę kooperacyjną oraz naukowo-badawczą. Należy zauważyć, że w wielu krajach sektor rolno-spożywczy nie jest jeszcze gotowy do konkurowania ze światowym pod względem kosztów produkcji, dlatego rządy powinny przyjąć wiele ustaw i aktów wykonawczych wspierających krajowy biznes. Zwiększenie efektywności funkcjonowania państwa na rynku UE stanowi zatem strategiczny kierunek zapewnienia bezpieczeństwa zewnętrzno-ekonomicznego Polski, a jednocześnie jest wskaźnikiem skuteczności wewnętrznych reform gospodarczych.

Volodymyr Maslak, Żanna Osikowicz

E.M. Berry, S. Dernini, B. Burlingame, A. Meybeck, P. Conforti, *Food security and sustainability: can one exist without the other?*, „Public Health Nutrition" 2015, vol. 18(13); *Bezpieczeństwo żywnościowe*, https://encyklopedia.revite.pl/articles/view/88 (dostęp 11.01.1016); *Bezpieczeństwo żywnościowe. Wyzwanie dla Polski i świata*, 4.05.2022, https://www.izbarolnicza.opole.pl/bezpieczenstwo-zywnosciowe-wyzwanie-dla-polski-i-swiata (dostęp 14.01.2026); R.P.F. Guiné, M.L.J. Pato, C.A.D. Costa, D.V.T.A.D. Costa, P.B.C.D. Silva, V.J.P.D. Martinho, *Food Security and Sustainability: Discussing the Four Pillars to Encompass*, „Foods" 2021, vol. 10(11), 10.3390/foods10112732; G. Lawrence, K. Lyons, T. Wallington, *Food*

Security, Nutrition and Sustainability, Routledge, London 2012; K. Leśkiewicz, *Bezpieczeństwo żywnościowe i bezpieczeństwo żywności – aspekty prawne*, „Przegląd Prawa Rolnego" 2012, nr 1(10); J. Michalczyk, *Bezpieczeństwo żywnościowe z perspektywy państw Unii Europejskiej*, „Ekonomia Międzynarodowa" 2019, nr 25, https://doi.org/10.18778/2082-4440.25.02; W. Peng, E.M. Berry, *The concept of food security*, „Encyclopedia of Food Security and Sustainability" 2019, vol. 2(1); J. Wright, *Sustainable Agriculture and Food Security in an Era of Oil Scarcit*, Routledge, London 2012; О.Л. Кірілеско, *Продовольча безпека – головна передумова ринкових трансформацій в АПК*, „Науковий Вісник Буковинської Державної Фінансової Академії" 2011, Вип. 1(20); С.І. Урба, *Продовольча безпека в умовах глобалізації*. „Науковий Вісник НЛТУ України" 2010. Вип. 20(12).

BIAŁA KSIĘGA W SPRAWIE PRZYSZŁOŚCI EUROPY (ang. White Paper on the Future of Europe) – dokument opracowany w marcu 2017 r. kreujący plan działań bezpieczeństwa Europy wobec wyzwań i zagrożeń; przygotowany przez Komisję Europejską w celu stworzenia debaty o bezpieczeństwie, a także przyszłych losach Unii Europejskiej. Dokument ten jest refleksją nad wyzwaniami, a także szansami stojącymi przed kontynentem europejskim; strategia przedstawia 5 scenariuszy rozwoju UE w zależności od dobranej ścieżki rozwoju państwa. Pierwszy – *Stay the same* – zakłada utrzymanie przez Unię Europejską wcześniej przyjętych reform czy modernizacji, dlatego też państwa członkowskie realizują wcześniejsze założenia i następuje umiarkowana modernizacja, a działania podejmowane są wspólnie, natomiast rozwój jest stateczny oraz skupiony na rozwiązaniu bieżących problemów. Oznacza to, że UE stawia na rozwój, natomiast bez znaczących zmian w strukturze czy też podziale kompetencji. Scenariusz ten przewiduje kilka znaczących konsekwencji, mianowicie – chociażby polityczne, które mają na celu stabilizację polityczną oraz podejmowanie wspólnych decyzji między państwami. Scenariusz działania w obszarze gospodarki UE koncentruje się na utrzymaniu wspólnej polityki handlowej, bez znaczących zmian czy też inicjatyw. Działania w obszarze bezpieczeństwa bazują na istniejących rozwiązaniach na zasadzie koordynacji państw członkowskich.

Kolejny scenariusz – *Only the single market* – nawiązuje do działań europejskich koncentrujących się na zawężaniu współpracy między państwami członkowskimi do funkcjonowania jednolitego rynku. W praktyce

oznacza to, że państwa członkowskie UE w coraz większym stopniu na różnych obszarach nie potrafią wypracować wspólnego kompromisu. Efektem tego będzie rezygnacja z jednoczących polityk, np. społecznych. Centralnym punktem tej współpracy będzie swobodny przepływ towarów, usług, ale też kapitału. Scenariusz przewiduje również trudności z podejmowaniem pracy za granicą, ograniczanie przemieszczania się, ale również dotyczące sektora opieki zdrowotnej dla osób przebywających poza ojczyzną. Problem związany jest z wysokimi kosztami leczenia spowodowanymi brakiem wspólnych zasad dotyczących świadczeń medycznych. Scenariusz przewiduje również trudności z wprowadzeniem inteligentnych systemów mobilności. Proces ten dotychczas odbywa się w sposób chaotyczny i niedoprecyzowany.

Kolejny, trzeci scenariusz nazwany *Those who want to do more, do more* nawiązuje do rozwoju niektórych państw członkowskich w sposób bardziej dynamiczny niż innych. W szczególności dotyczy to wybranych sektorów (obrona, sprawy społeczne). Ważne w założeniach scenariusza jest to, że dokonywane zmiany w sposób postępowy są wyborem, a nie nakazem; państwa, które decydują się na szybszy rozwój, działają dynamiczniej, natomiast pozostałe – na dotychczasowych zasadach lub też nie angażując się w nowe pomysły. Przykładem takiej możliwości jest działanie 15 państw członkowskich, które utworzyły organ złożony z funkcjonariuszy policji oraz prokuratury w celu zwalczania transgranicznej działalności przestępczej.

Czwarty scenariusz przedstawiany przez dokument – *Doing less more efficiently* – dotyczy skoncentrowania wysiłków na kilku kluczowych sektorach. Przykładem tych działań jest plan odnoszący się do takich obszarów, jak innowacje, bezpieczeństwo, handel, zarządzanie granicami, obrona, cyfryzacja czy też migracja; przewiduje się natomiast zmniejszenie udziału w takich sferach, jak polityka regionalna i społeczna. Celem jest nie tylko opracowanie nowych przepisów, ale również narzędzi do egzekwowania prawa w celu pogłębienia jednolitego rynku w kluczowych nowych obszarach.

Do innowacyjnych działań zalicza się chociażby plan współpracy w dziedzinie przestrzeni kosmicznej czy też zaawansowanych technologiach; obejmuje to również ukończenie budowy centrów energetycznych.

Scenariusz czwarty omawia też plany dotyczące konsolidacji strefy euro i zapewnienia stabilności wspólnej dla państw członkowskich waluty. Ponadto odnosi się do wzmocnienia praw obywatelskich w wybranych obszarach. Realnym przykładem realizacji scenariusza jest plan utworzenia Europejskiej Agencji ds. Walki z Terroryzmem czy też całkowita kontrola granic zewnętrznych UE przez Straż Graniczną UE. Wszystkie wymienione działania w scenariuszu mają przede wszystkim na celu wzmocnienie pozycji Unii Europejskiej, ale również podejmowania skuteczniejszych i szybszych działań.

Scenariusz piąty – *Doing much more together* – zakłada ścisłą współpracę państw członkowskich w kluczowych dla UE obszarach polityki.

Plan działania nawiązuje do jedności państw członkowskich na arenie międzynarodowej, w szczególności w obszarze polityki zagranicznej i handlowej; celem jest natomiast jednomyślność UE. Kolejnym istotnym założeniem scenariusza jest wspólna europejska obrona – państwa powinny integrować przemysł obronny, a także zdolności operacyjne w celu wzmocnienia obszaru bezpieczeństwa UE. Plan ten zakłada również zwiększenie współdziałania w zakresie polityki migracyjnej, bazując na wspólnej polityce azylowej, ale również wzmocnienie granic państw członkowskich. Kluczowe staje się również utworzenie jednolitego rynku, w szczególności w obszarze energii i cyfryzacji. Scenariusz piąty ma na celu również wypracowanie działań zmierzających do wzrostu budżetu sojuszu oraz unowocześnienie i wprowadzenie innowacyjnych projektów.

Należy zaznaczyć, że zaprezentowane w dokumencie scenariusze są jedynie formą rekomendacji mającą na celu rozwinięcie dialogu pomiędzy państwami członkowskimi. Dodatkowo dokument ten wskazuje konieczność wzmocnienia współpracy na wybranych obszarach, ale z poszanowaniem praw człowieka, tak aby nie ograniczać swobód obywatelskich.

Biała księga wskazuje też, że bezpieczeństwo Europy to nie tylko sfera militarna, ale również współdziałanie strategiczne. Dokument ten nie skupia się jedynie na podaniu rekomendacji czy też sugestii, ale również wyszczególnia obszary, które wymagają wzmocnienia i integracji państw członkowskich UE, mianowicie – wymienia zagrożenia o charakterze zewnętrznym, do których zaliczają się konflikty regionalne oraz ich rozprzestrzenianie się, dynamiczny wzrost presji migracyjnej, rosnąca

konkurencja mocarstw czy wzrost zagrożeń o charakterze hybrydowym. Biała księga odnosi się także do wewnętrznych zagrożeń, takich jak wyzwania wobec polityki migracyjnej, podział społeczeństwa i osłabienie struktur UE, brak zdolności do współdziałania i reagowania państw członkowskich.

Wskazane są wyzwania bezpieczeństwa z obszaru gospodarczego (niestabilność gospodarcza), kwestie humanitarne (niekontrolowane migracje do państw europejskich), dezinformacja, cyberbezpieczeństwo Europy. Dokument, dokonując analizy wyzwań wobec UE, odnosi się m.in. do słabnącego znaczenia Europy poprzez spadające PKB, osłabienia zdolności obronnych państw członkowskich i wzrostu zagrożeń międzynarodowych, transformacji gospodarczej, nierówności między regionami spowodowanych kryzysem finansowym, wzrostu automatyzacji, zanikania zawodów, zmian demograficznych (starzenie się Europy), które będą miały istotny wpływ na systemy emerytalne czy też na rynek pracy i system opieki zdrowotnej, wzrostu realnych zagrożeń zamachami terrorystycznymi, rozprzestrzeniających się konfliktów regionalnych, znaczących napływów uchodźców, problemów z systemem azylowym oraz funkcjonowaniem strefy Schengen (pojawiły się już pierwsze spory w tym obszarze po 2015 r.), wyzwań na tle politycznym (np. spadek zaufania do instytucji publicznych). Dokument podkreśla ścisły związek między bezpieczeństwem a omówionymi wyzwaniami, mianowicie – odwołuje się do tego, że bezpieczeństwo to element spójny dla państw członkowskich. Oznacza to, że mimo w miarę utrzymanego bezpieczeństwa UE jest nadal podatna na działania, niebezpieczeństwa wewnętrzne i zewnętrzne. Dodatkowo bezpieczeństwo to stabilność wobec polityki gospodarczej czy też społecznej.

Ważnym aspektem poruszonym w zapisach dokumentu jest to, że tradycyjne działania państw w obecnym czasie nie są wystarczające i konieczna jest zmiana wspólnej polityki bezpieczeństwa poprzez współdziałanie służb wywiadowczych, rozwój wspólnej obrony terytorialnej czy też wzmocnienie infrastruktury krytycznej państw. Ogromnie ważną kwestią podkreślaną w treści dokumentu jest znaczenie współpracy między państwami, również wspólne reagowanie na kryzysy bezpieczeństwa. Skuteczność reakcji jest zależna od stopnia integracji. Warte podkreślenia jest również postrzeganie bezpieczeństwa nie tylko w kategorii militarnej, obronnej, ale również gospodarczej czy też politycznej.

Biała księga w sprawie przyszłości Europy z 2017 r. silnie nawiązuje do potrzeby ścisłej współpracy między państwami członkowskimi UE; podkreśla, że w trudnym dla Europy momencie należy działać zgodnie z zasadą jedności i poszanowania różnorodności ze względu na to, że wspólna siła państw doprowadzi UE do stabilności oraz postępu. Podkreślone zostało również to, że izolacja krajów europejskich doprowadzi do ich osłabienia. Działania UE dotyczące sporządzenia dokumentu określane są jako doskonała okazja do refleksji nad tym, co czeka UE w przyszłości, a także kształtowania regionu. W komentarzach na temat dokumentu podkreśla się, że prawdziwy scenariusz dotyczący UE będzie połączeniem wszystkich przedstawionych. Głównym dylematem jest kwestia podziału uprawnień państw członkowskich, których część musi zostać oddana UE. Podczas realizacji scenariusza przyszłości dla UE powinno się zachować dorobek sojuszu, np. dziedzictwo polityczne, prawne, społeczne czy też kulturowe wraz z wdrażaniem elementów rozwoju. Komisja Europejska w ramach białej księgi publikuje serię dokumentów dotyczących rozwoju społecznego wymiaru Europy, przyszłości jej obrony czy też przyszłości ekonomicznej. Wymienione dokumenty to również propozycje dotyczące scenariuszy przyszłości Europy zrealizowane do 2025 r.

Natalia Borodziuk

A. Cuyvers, *Five Scenarios for Europe – Understanding the EU Commission's White Paper on the Future of Europe*, 10.04.2017, https://verfassungsblog.de/five-scenarios-for-europe-understanding-the-eu-commissions-white-paper-on-the-future-of-europe/ (dostęp 11.12.2025); *The Future of Europe*, P. Scherrer, J. Bir, W. Kowalsky, R. Kuhlmann, M. Méaulle (eds.), ETUI Report, Brussels 2017; G. Uścińska, *Kierunki przyszłości Unii Europejskiej – kilka słów komentarza*, „Zabezpieczenie Społeczne. Teoria, Prawo, Praktyka" 2017, nr 6; *White Paper on the Future of Europe: Paths to Unity for the UE-27*, 2017, https://commission.europa.eu/system/files/2017-03/white_paper_on_the_future_of_europe_en.pdf (dostęp 11.12.2025).

BLOKADA EKONOMICZNA/BLOKADA GOSPODARCZA (ang. *economic blockade*) – środek przymusu polityczno-gospodarczego polegający na uniemożliwieniu lub istotnym ograniczeniu wymiany handlowej, dostępu do rynków, surowców, technologii lub kapitału państwu, organizacji lub

podmiotowi gospodarczemu. Celem blokady jest wywarcie presji, by wymusić określone zachowania polityczne, militarne lub ekonomiczne. To również ogół środków podjętych przez państwo lub grupę państw w celu zachwiania gospodarki państwa blokowanego przez jego izolację (np. embargo, sankcje gospodarcze, częściowe lub zupełne zerwanie stosunków handlowych i finansowych). Polega na izolacji (zamknięciu) dostępu do zasobów światowych w celu wymuszenia przyjęcia postawionych warunków lub spowodowania załamania gospodarczego i upadku władzy w danym kraju. Blokada ekonomiczna przeprowadzana jest poprzez zerwanie zagranicznych powiązań handlowych, finansowych, kredytowych i innych gospodarczych między państwami. Może być realizowana w różnych formach: widocznej (np. blokada granic, portów) i niewidocznej (np. zmowa banków w celu nieudzielania kredytów, utrudnianie transferów międzynarodowych i innych). Blokada ekonomiczna i gospodarcza to w zasadzie tożsame pojęcia; w praktyce termin „blokada gospodarcza" jest po prostu synonimem „blokady ekonomicznej".

Blokady ekonomiczne przybierają różne formy, takie jak zakaz handlu (embargo, czyli całkowity zakaz handlu, lub ograniczenia dotyczące konkretnych towarów – kontyngenty), zamrożenie aktywów – blokowanie dostępu do rachunków bankowych, nieruchomości i innych zasobów finansowych, ograniczenia w przepływie funduszy lub zamrożenie kont bankowych, a także ograniczenia podróży – zakazy wizowe i zakazy podróżowania, które utrudniają kontakty gospodarcze. Mogą to być również ograniczenia monetarne – zakaz przepływu funduszy, ograniczenia w operacjach bankowych i zakazy dotyczące walut oraz transakcji – uniemożliwienie nawiązywania relacji biznesowych, które mogą być zabronione, częściowe lub zupełne zerwanie stosunków handlowych i finansowych.

Blokada ekonomiczna może być nałożona przez organizacje międzynarodowe (np. ONZ), państwa indywidualnie, koalicje państw (np. UE, NATO, sojusze regionalne). Blokada ekonomiczna to kompleksowy, pełny system odcięcia gospodarczego, często zbliżony do blokady militarnej, ale bez użycia siły, co odróżnia ją od sankcji gospodarczych (pojedyncze restrykcje, np. zakaz importu broni).

Cele blokady można podzielić na polityczne (zmiana polityki rządu, wymuszenie zakończenia konfliktu, powstrzymanie agresji zbrojnej);

ekonomiczne (osłabienie gospodarki przeciwnika, destabilizacja budżetu państwa, ograniczenie dostępu do technologii strategicznych); militarne (uniemożliwienie finansowania wojny, odcięcie państwa od dostaw broni i paliw).

Blokada ekonomiczna może być stosowana w celach gospodarczo-politycznych, jak również polityczno-militarnych, np. blokada kontynentalna 1806 lub blokada kontynentalna Niemiec w czasie I i II wojny światowej. Blokada kontynentalna lub system kontynentalny to pełne embargo handlowe wobec Wielkiej Brytanii stosowane pod naciskiem Francji przez państwa kontynentalnej Europy w latach 1806–1814. Blokada została wprowadzona przez Napoleona Bonaparte i narzucona sojusznikom cesarstwa oraz pozostałym państwom europejskim.

Pakt Ligi Narodów przewidywał w art. 16, że blokada ekonomiczna może być stosowana jako szczególny rodzaj sankcji międzynarodowej przeciwko członkowi Ligi uciekającemu się do wojny wbrew przyjętym zobowiązaniom. Blokadę ekonomiczną przewiduje też Karta Narodów Zjednoczonych (art. 41), stanowiąc, że wobec państwa, które zagraża pokojowi lub dopuszcza się agresji, mogą być zastosowane sankcje gospodarcze polegające na częściowym lub zupełnym zerwaniu stosunków gospodarczych i komunikacyjnych. Decyduje o tym Rada Bezpieczeństwa ONZ, która na tej podstawie w 1978 r. ogłosiła sankcje gospodarcze wobec RPA, w 1990 r. – blokadę ekonomiczną Iraku po jego napaści na Kuwejt, zaś w 1992 r. – wobec Libii i Jugosławii. Blokada ekonomiczna stosowana była również przeciw Związkowi Radzieckiemu po rewolucji październikowej.

Przykłady blokady ekonomicznej to blokada Kuby przez Stany Zjednoczone po rewolucji w 1959 r., nałożenie sankcji na Rosję po inwazji na Ukrainę w 2022 r., blokada Iraku po jego napaści na Kuwejt w 1990 r. oraz sankcje nałożone na RPA po 1978 r.

Blokada Kuby przez Stany Zjednoczone wprowadzona po rewolucji w 1959 r. zakazywała handlu z tym krajem i dotknęła wiele sektorów gospodarki, utrudniając import niezbędnych towarów. Po inwazji na Ukrainę, w 2022 r. wiele państw nałożyło na Rosję sankcje, w tym blokowanie dostępu do rynków finansowych, ograniczenia eksportu technologii oraz embargo na import ropy i gazu. Rada Bezpieczeństwa ONZ nałożyła blokadę ekonomiczną na Irak po jego inwazji na Kuwejt w 1990

r. Blokada ekonomiczna została nałożona na RPA po 1978 r., w ramach działań podjętych przez ONZ. Historyczne przykłady to blokada kontynentalna z 1806 r. lub blokady podczas I i II wojny światowej, które miały charakter ekonomiczny i militarny.

Blokada ekonomiczna mająca na celu wywarcie presji na określone państwo została zastosowana w 1981 r. w Polsce, gdy w odpowiedzi na wprowadzony stan wojenny Stany Zjednoczone nałożyły na Polskę sankcje gospodarcze. Przykład ten wskazuje, że będące konsekwencją skutecznej blokady ekonomicznej działania polegające na osłabieniu potencjału wojenno-gospodarczego danego państwa powodują obniżenie poziomu życia obywateli tego państwa, co z kolei wpływa na zwiększenie niezadowolenia ludności z tej sytuacji i destabilizacja gospodarcza może zamienić się w destabilizację o charakterze politycznym.

Społeczne skutki blokady ekonomicznej ujawniły się również, gdy rząd Izraela po przejęciu władzy przez Hamas w 2007 r. rozpoczął bezprecedensową blokadę Strefy Gazy, przez ponad 2 lata trzymając w zamknięciu 1,5 mln obywateli w warunkach uwłaczających ludzkiej godności. Blokada ekonomiczna doprowadziła do olbrzymiej destabilizacji gospodarczej i społecznej. Zgodnie z danymi Palestyńskiego Głównego Urzędu Statystycznego w pierwszym kwartale 2009 r. ponad 140 tys. mieszkańców zdrowych i zdolnych do pracy zamieszkałych Strefę Gazy nie mogło znaleźć zatrudnienia, a stopa bezrobocia wśród osób do 30 roku życia wynosiła ponad 60%, stanowiąc tym samym jeden z najwyższych wskaźników w skali świata. Wskutek zakazu importu i eksportu oraz innych ograniczeń dochody rolników i rybaków drastycznie się pomniejszyły; wielu właścicieli gruntów rolnych położonych niedaleko granicy izraelskiej napotkało permanentne przeszkody w uprawianiu pól, co pozbawiło ich podstawowych środków utrzymania. Codziennością okazały się trudności w pozyskaniu żywności: niektóre podstawowe produkty spożywcze były całkowicie niedostępne, a osiągalne dodatkowo drastycznie podrożały. Blokada trwająca ponad 2 lata spowodowała przedłużający się kryzys humanitarny i odbiła się praktycznie na wszystkich aspektach życia; mieszkańcy utracili dachy nad głową, wiele osób odcięto od stałego dostępu do wody, przerwy w dostawie elektryczności spowodowały ograniczenia w funkcjonowaniu służby zdrowia i szkolnictwa. Jednym słowem,

podstawowe prawa człowieka zostały drastycznie ograniczone – w Strefie Gazy społeczeństwo wykorzystano jako polityczną kartę przetargową.

Skutki blokady ekonomicznej bywają więc wewnętrznie sprzeczne, zwłaszcza gdy w znacznym stopniu dotykają ludność cywilną.

Do skutecznych rodzajów blokady ekonomicznej zaliczyć należy CoCom, czyli zakaz eksportu technologii podwójnego zastosowania wdrożony przez państwa zachodnie zrzeszone w Coordinating Committee for Multilateral Export Controls. W znacznym stopniu uniemożliwiła ona transfer technologii, którą (oprócz celów cywilnych) można było stosować do produkcji systemów broni i uzbrojenia. Niewątpliwie przyspieszyła ona erozję gospodarki krajów tzw. realnego socjalizmu.

Natomiast nieskuteczna okazała się blokada ekonomiczna Włoch ogłoszona przez Ligę Narodów po agresji Mussoliniego na Abisynię w 1935 r. Wprawdzie dotknęła ona gospodarkę włoską, ale Rzym dość skutecznie ją omijał. Poza tym upewniła reżim hitlerowski III Rzeszy, że polityka agresji może skutkować blokadą ekonomiczną Niemiec. Obawy te prowadziły do znacznego nagromadzenia zapasów surowców strategicznych przez Berlin przed wybuchem II wojny światowej, a także były jednym z powodów zawarcia paktu Ribbentrop–Mołotow w 1939 r., który miał w założeniu także niwelację skutków blokady ekonomicznej Rzeszy przez mocarstwa zachodnie. Blokada ekonomiczna Japonii ogłoszona w lipcu 1941 r. przez rządy USA, Wielkiej Brytanii i holenderski rząd emigracyjny oznaczała *de facto* zakaz jakiejkolwiek wymiany handlowej z tym krajem. Rząd japoński, mając do wyboru albo kapitulację wobec żądań Londynu i Waszyngtonu, albo wojnę z tymi mocarstwami, wybrał drogę militarnego rozstrzygnięcia tego dylematu.

Karta Narodów Zjednoczonych (ONZ) przewiduje stosowanie blokad gospodarczych przez państwa członkowskie ONZ wobec państw agresorów jako zbiorowego środka przywracającego i chroniącego pokój.

Stąd też można wyprowadzić wniosek ogólny, że blokada ekonomiczna może być katalizatorem konfliktu o ponadregionalnym wymiarze w sytuacji, gdy strona, która zostanie nią dotknięta, uzna, że każde inne rozwiązanie (poza militarnym) jest niemożliwe. Także groźba sankcji czy nawet całkowitej blokady ekonomicznej może okazać się kontrproduktywna. W 2022 r. groźby USA i innych krajów zachodnich nie powstrzymały

władz Federacji Rosyjskiej przed pełnoskalową agresją na Ukrainę. Podobnie w wypadku agresji Iraku na Kuwejt w 1990 r. dopiero bezpośrednia interwencja militarna odwróciła jej skutki, natomiast próby blokady ekonomicznej były niewystarczające.

Blokada ekonomiczna jest jednym z najostrzejszych środków polityki międzynarodowej, stosowanym zamiast lub obok działań zbrojnych. To instrument o dużej skuteczności, ale również ogromnym ryzyku humanitarnym i politycznym. Stanowi narzędzie nacisku strategicznego, które może zmienić sytuację państwa, ale także doprowadzić do poważnych kryzysów.

Anna Kochnowska

Z. Bako, *Wojna ekonomiczna*, Ministerstwo Obrony Narodowej, Warszawa 1983; *Ekonomika obrony. Materiały do wykładów*, W. Bednarek (red.), Wydawnictwo Uniwersytetu Łódzkiego, Łódź 1994; https://elk.wans.edu.pl/wp-content/uploads/2021/11/Slownik_terminow_-z_zakreu_bezpieczenstwa_narodoweg.pdf (dostęp 3.12.2025); M. Janiec, *Współczesna wojna ekonomiczna. Istota i charakterystyka*, Akademia Obrony Narodowej, Warszawa 2003; C. Jean, *Geopolityka*, Zakład Narodowy im. Ossolińskich, Wrocław 2003; A. Oleksiuk, M. Vashchenko, *Międzynarodowe stosunki ekonomiczne. Gospodarcze wyzwania XXI wieku*, Wydawnictwo Key Text, Warszawa 2010; K. Raczkowski, *Geoekonomia i wojny gospodarcze*, [w:] *Bezpieczeństwo ekonomiczne. Wyzwania dla zarządzania państwem*, K. Raczkowski (red.), Wydawnictwo Jak, Warszawa 2012; L. Urbański, *Wojna gospodarcza*, [w:] *Ekonomika obrony*, W. Stankiewicz (red.), Akademia Obrony Narodowej, Warszawa 1994; *Wpływ blokady ekonomicznej na sytuację humanitarną Gazy* [skrócony raport Biura ONZ ds. Koordynacji Pomocy Humanitarnej, 08.2009]; https://encyklopedia.pwn.pl/haslo/blokada-ekonomiczna;3878423.html (dostęp 4.12.2025).

BRACTWA KURKOWE – od czasów średniowiecza związane były z obowiązkiem samoobrony mieszkańców, którzy w sytuacji zagrożenia musieli bronić swoich miast. Były one otaczane murami obronnymi, a załogę walczącą z najeźdźcami stanowili mieszczanie. Pierwsze bractwa złożone z rzemieślników i kupców, broniące murów miejskich, powstawały już w VII w. w Hiszpanii. W XI w. pojawiły się także na terenach dzisiejszej Francji i Niemiec. Rzeczą naturalną była konieczność odbywania

przez mieszczan szkoleń w zakresie posługiwania się bronią, tak by w przypadku ataku mogli nią sprawnie władać. Najczęściej bractwa były powoływane do życia przez samorządy miejskie, którym podlegały. Tak więc od samego początku występowały silne więzi pomiędzy bractwami kurkowymi a miastami, na terenie których działały. Członkostwo w bractwach było obowiązkowe, a ich struktura organizacyjna nosiła cechy paramilitarne i miała charakter ponadcechowy. Jeśli w nazwie pojawiał się człon *-gilde*, oznaczało to, iż organizacja gromadzi przedstawicieli struktur cechowych. Z kolei tam, gdzie w nazwie występowało słowo *Bruderschaft*, organizacja bazowała na bractwach kościelnych. Badacze przyjmują, że umowna granica podziału na gildie i bractwa przebiegała wzdłuż dwóch niemieckich rzek: Renu i Menu. Poniżej ich nurtu funkcjonowały głównie bractwa, natomiast na północy, gdzie dominował żywioł mieszczański, działały z reguły gildie.

Ustalono, że na obszarze byłej monarchii habsburskiej działał też trzeci rodzaj organizacji strzeleckich, określany jako kompanie. Punktem kulminacyjnym ich rozwoju był okres wojen napoleońskich, ale już w średniowieczu, pod wpływem Hanzy, organizacje strzeleckie powstawały na terenie całej Europy. Determinantą ich rozwoju było również upowszechnienie broni miotającej, jaką były łuki i kusze; to głównie we władaniu tą bronią doskonalili się członkowie bractw, a istotną rolę odgrywał harmonogram strzeleckich ćwiczeń i zawodów. Te ostanie odbywały się głównie w święta kościelne.

W Polsce również rozprzestrzeniała się idea organizacji strzeleckich, zwłaszcza w miastach zakładanych na prawie magdeburskim. Kolonizatorzy lokujący miasta przekazywali nowe wzorce obyczajowe i kulturowe. Przepisy lokacyjne obligowały obywateli do obrony oraz utrzymania porządku w samym mieście, co powodowało, iż stawali się oni pewnym rodzajem policji. Otoczenie miasta murami obronnymi nakładało na mieszkańców obowiązek samodzielnej obrony wzniesionych umocnień. Prawo lokacyjne dawało podstawę do powoływania stowarzyszeń, ale związanych wyłącznie ze sztuką wojenną i obronnością.

Z reguły każdy wyodrębniony odcinek obwarowań powierzano innemu z rzemieślniczych cechów; to one odpowiadały za obsadzanie, finansowanie i kondycję poszczególnych bram, baszt czy murów. Tym

samym bazą nowej struktury obronnej miast stawały się istniejące w nich struktury zawodowe mieszkańców. To, że obronę miast powierzano właśnie mieszczanom, nie było kwestią przypadku, lecz wynikało z tego, że kupcy i rzemieślnicy byli właścicielami czasami znacznych majątków, które w przypadku oblężenia stawały się zagrożone. Rodziło to w mieszczanach przeświadczenie o konieczności obrony osobistego dobytku. Mieszczanie mieli środki finansowe i motywację do ponoszenia dosyć dużych kosztów wojennego wyposażenia zarówno dla siebie, jak i dla swoich czeladników. Aby zachować wysoki poziom gotowości bojowej, członkowie bractw za murami miejskimi organizowali ćwiczenia, które stanowiły dużą atrakcję i rozrywkę dla innych mieszkańców miasta.

Bractwa kurkowe miały za zadanie uformować z tych na co dzień wykonujących różne profesje ludzi obrońców i sprawnych żołnierzy. Z tego względu bractwa strzeleckie funkcjonowały niemal we wszystkich większych polskich miastach; do najstarszych należały te działające na terenie Krakowa, Torunia, Lwowa, Poznania, Kalisza czy Warszawy. W tych swoistych wojskowych szkołach mieszczanie uczyli się władania bronią białą, strzelania z łuku i kuszy, a w późniejszym okresie także z broni palnej – rusznic i hakownic. Stąd były osobne bractwa doskonalące się w strzelaniu z łuku, zwane bractwami łuczników (*fraternitas sagittariorum*). W XVI i XVII w. upowszechniła się już broń palna, co spowodowało zmianę nazw na „bractwa strzeleckie" (*contubernium iacula – torum, fraternitas iaculatorum*). Ważną misją bractw była integracja różnych mieszczańskich korporacji w jednolity oddział zapewniający skuteczną obronę ich małych ojczyzn. Istotną kwestią sprzyjającą takiej integracji był panujący w bractwach egalitaryzm – to on sprawiał, że wszyscy ich członkowie byli równi, byli dla siebie braćmi, a wyróżnienia i stopnie wynikały jedynie ze stopnia opanowania żołnierskiego rzemiosła. Posiadany majątek, piastowane funkcje w cechach czy w samorządzie miejskim nie miały tu znaczenia.

Na obszarach współczesnej Polski, gdzie regułą były bractwa organizowane przez władze miejskie, pojawiały się również organizacje zakładane przez inne władze lokalne. Taką sytuację można było zaobserwować, zwłaszcza w późniejszym okresie ich działalności, przede wszystkim na Śląsku – bractwa kurkowe powoływali tam miejscowi książęta lub hrabiowie, którzy stawali się ich protektorami, nadając im liczne przywileje.

Już w XIII w. założycielem takiego bractwa w Świdnicy był książę Bolko I Surowy, który w roku 1286 sam brał udział w zawodach strzelania do kura umieszczonego na wysokiej żerdzi. Stąd wywodzi się sama nazwa bractw. W Kłodzku ród Hardecków ufundował dla bractwa łańcuch króla kurkowego. Hrabia Henckel von Donnersmarck ze Świerklańca w 1728 r. reaktywował bractwo w Bytomiu. W 1780 r. przedstawiciel tego rodu powołał do życia Bractwo Strzeleckie w Tarnowskich Górach.

Najbardziej znanym i działającym do dzisiaj jest Krakowskie Bractwo Kurkowe, którego daty powstania nie utrwalił jednak żaden zachowany dokument. Historycy wskazują, że początek działalności tej organizacji przypadł na okres, gdy Kraków miał już pierwsze fortyfikacje obronne – był to koniec XIII w., co świadczy o tym, iż historia bractwa jest ściśle związana z losami samego Krakowa, od momentu jego lokacji na prawie magdeburskim. Niestety ze względu na brak źródeł, które uległy zniszczeniu w pożarach lub zaginęły na skutek grabieży, nie da się dokładnie wskazać daty powstania tej organizacji. Na podstawie zapisków w aktach Rady Miejskiej oraz badań porównawczych dziejów miast na zachodzie Polski i na Śląsku przyjmuje się, że krakowskie bractwo działa już od drugiej połowy XIII w. Formalnie przyjęto, iż datą rozpoczęcia funkcjonowania tej organizacji jest data lokacji Krakowa, a stosowny dokument wystawiony przez księcia Bolesława Wstydliwego pochodzi z 5 czerwca 1257 r. Pierwszym zachowanym źródłem potwierdzającym funkcjonowanie bractwa w XIV w. jest *Wielki przywilej dla miasta Krakowa* nadany 7 grudnia 1358 r. przez króla Kazimierza Wielkiego. Zobowiązywał on wszystkich mieszczan do obrony grodu w razie jego zagrożenia. W 1430 r. Kraków uzyskał prestiżowe członkostwo w związku miast hanzeatyckich, a to oznacza, iż musiał już mieć odpowiednie fortyfikacje i załogę gotową do obrony miejskich obwarowań. Jedynie miasta spełniające takie warunki bezpieczeństwa mogły być przyjęte do Hanzy; był to bowiem warunek konieczny.

Tak jak w innych miastach lokowanych na prawie magdeburskim, tak i w Krakowie obowiązek utrzymania i obrony murów spoczął na mieszczanach; właśnie po to została powołana organizacja paramilitarna, do której członkowie cechów musieli obowiązkowo należeć. Bractwo kurkowe nosiło także inne nazwy: Towarzystwo Strzeleckie, Konfraternia

Strzelców, Szkoła Strzelecka lub Rycerska. Po łacinie zwane było Schola Iaculatoriae lub Societas Iaculatorum. W 1565 r. samorząd miasta Krakowa podarował organizacji „pański klejnot" – srebrnego kura, który odtąd stał się symbolem Krakowskiego Bractwa Kurkowego. Według współczesnych braci jego uroczystego wręczenia miał dokonać sam król Zygmunt August. Kur był nie tylko godłem krakowskiej konfraterni, ale także trafiał do najlepszego strzelca, tzw. króla kurkowego. Wspomniany władca otaczał bractwo swą szczególną opieką i wsparciem – świadczą o tym słowa jego listu skierowanego w dniu 6 czerwca 1565 r. do rajców miejskich: „Sławetni nam mili. Ponieważ wielki czujemy niedostatek ludzi wprawnych do użycia machin wojennych […], postanowiliśmy chwycić się środków, które by tej niedogodności zaradzić mogły. Ponieważ zaś miasto Kraków niemało nam w tej rzeczy pomóc może, przemyśleliśmy zaprowadzić w nim szkołę strzelania do celu […]. Rozkazujemy, abyście […] wezwali mieszczan krakowskich do strzelania, naznaczając jakie niezbyt kosztowne nagrody, aby ich do współubiegania się zachęcić".

Na początku strzelano do kura z łuku, a później z kuszy. Ptak ten był posadowiony na wysokiej żerdzi, a laur zwycięstwa zdobywał strzelec, który strącił ostatni, najmniejszy kawałek tego celu. Z nakazu króla Henryka Walezego w bractwie zaczęto posługiwać się bronią palną; wtedy też kura umieszczano już nie na maszcie, ale na drewnianej tarczy posadowionej na końcu toru strzelniczego. W zawodach warto było startować, bo na zwycięzcę czekało wiele nagród i przywilejów.

W 1590 i 1593 r. król Zygmunt III Waza nie tylko zatwierdził dotychczasowe przywileje, ale je rozszerzył, uwalniając króla kurkowego od płacenia ceł za sprowadzane z zagranicy towary. Jego następca Władysław IV Waza wydał dekret zwalniający krakowskich królów kurkowych, w okresie sprawowania przez nich tej godności, z płacenia wszystkich podatków. Jan Kazimierz oraz Jan III Sobieski potwierdzili te przywileje; ten ostatni w krakowskim Celestacie doskonalił swe umiejętności w strzelaniu z łuku. Władcy z dynastii Wettinów także potwierdzili nadane przywileje w 1710 (August II) i 1746 r. (August III).

W 1794 r., po upadku powstania kościuszkowskiego Krakowskie Bractwo Kurkowe zakończyło swą działalność. Ostatnim królem kurkowym I Rzeczpospolitej został pasztetnik mistrz Stanisław Piątkowski.

Po krótkiej reaktywacji bractwa, na początku XIX w. nadszedł moment likwidacji murów obronnych Krakowa; rozbiórka fortyfikacji zaczęła się w 1807 r. – od Bramy Mikołajskiej – i z tego też roku pochodzi ostatni zapis umieszczony w księdze protokołów Szkoły Strzeleckiej. Badacze zwracają uwagę, iż początkiem funkcjonowania bractwa kurkowego było otoczenie Krakowa murami obronnymi, a końcem jego aktywności – ich zburzenie. Kolejnym etapem w dziejach bractwa był rok 1831, kiedy to grupa Krakowian założyła towarzystwo, któremu nadała nazwę Amatorzy Strzelnictwa. Główną misją tej organizacji była jednak działalność charytatywna, która polegała przede wszystkim na dożywianiu ubogich mieszkańców miasta. Po pewnym czasie zmieniła ona nazwę na Towarzystwo Strzeleckie, które już bezpośrednio nawiązywało do bogatych tradycji bractwa kurkowego. Niestety w 1846 r. wraz z włączeniem Krakowa do monarchii austro-węgierskiej zaborcy zabronili organizowania zawodów strzeleckich, nakazując jednocześnie oddanie broni członkom stowarzyszenia. Celestat, w którym odbywały się ćwiczenia strzeleckie, został przejęty przez armię. Pięć lat później władze austriackie zezwoliły na wznowienie działalności towarzystwa.

Od 1851 r. aż do wybuchu I wojny światowej corocznie organizowano zawody strzeleckie oraz kończące strzelanie do kura uczty królewskie. W 1916 r. Towarzystwo Strzeleckie zgłosiło akces i zostało członkiem Czerwonego Krzyża. 15 lipca 1919 r. odbyły się pierwsze w niepodległej Polsce zawody o tytuł króla kurkowego; generał Józef Haller, naczelny dowódca Wojsk Polskich, oddał wówczas pierwszy honorowy strzał. Z inicjatywy Krakowskiego Bractwa Strzeleckiego w dniach 26–29 czerwca 1925 r. w Krakowie odbył się historyczny Zjazd Polskich Bractw Strzeleckich.

Niestety działalność bractwa została ponownie brutalnie przerwana na skutek wybuchu II wojny światowej. Dekretem generalnego gubernatora Hansa Franka w dniu 23 lipca 1940 r. zakazano działania wszystkim stowarzyszeniom o charakterze kulturalnym, wojskowym, a nawet charytatywnym. Jeszcze przed podpisaniem przez III Rzeszę aktu kapitulacji 4 maja 1945 r. zarejestrowano stowarzyszenie Towarzystwo Strzeleckie „Bractwo Kurkowe" w Krakowie. Po zaledwie sześciu latach, 28 czerwca 1951 r. zostało ono rozwiązane, tym razem przez władze PRL. Braciom postawiono kuriozalny i niczym nieuzasadniony zarzut kolaboracji z Niemcami.

Organizacja, według komunistycznych władz, miała skupiać wrogów ludu i nie przystawać do nowych założeń ustrojowych państwa.

10 czerwca 1957 r. udało się reaktywować bractwo pod nazwą Krakowskie Towarzystwo Strzeleckie (Bractwo Kurkowe), ale dopiero 26 marca 1991 r. minister spraw wewnętrznych wydał decyzję stwierdzającą nieważność tej wydanej przez Prezydium Wojewódzkiej Rady Narodowej w Krakowie w 1951 r. W uzasadnieniu stwierdził, iż powodem likwidacji Towarzystwa Strzeleckiego „Bractwo Kurkowe" w Krakowie były wyłącznie przyczyny polityczne; to rozstrzygnięcie pozwoliło pozytywnie zakończyć starania o odzyskanie mienia zlikwidowanego bezprawnie towarzystwa. Tym samym do braci wróciły cenne pamiątki oraz budynek Celestatu.

Warto odnieść się do historii bractwa działającego w odległej od Krakowa Bydgoszczy. Źródła z okresu międzywojennego datują jego powstanie na rok 1346, czyli założenie przez Kazimierza Wielkiego miasta. Barbara Janiszewska-Mincer podważa takie ustalenia, wskazując, iż dokument lokacyjny nie wspomina o bractwie ani też nie odnosi się do obronności miasta. Istnienie bractwa w Bydgoszczy potwierdza dopiero kronika Wojciecha Łochowskiego, w której znalazł się zapis, że w roku 1495 burmistrz Jan Grot wraz z 4 rajcami powołał bydgoskie bractwo łuczni-cze. Jego organizacja została oparta na wilkierzu poznańskim, natomiast pierwszy istniejący dokument dotyczący bractwa w Bydgoszczy datowany jest na 1523 r. i odnosi się do przywilejów nadanych przez burmistrza i radę miejską królowi kurkowemu – zwycięzcy zawodów zielonoświątecznych. Z kolei w przywileju nadanym przez króla Fryderyka Wilhelma z 20 czerwca 1789 r. znajdziemy wzmiankę o bractwie narodowości polskiej i niemieckiej działającym w Bydgoszczy.

Przez wiele lat Polacy mieli nieskrępowany dostęp do tego stowarzyszenia i nie doświadczali w tym zakresie żadnej dyskryminacji: potwierdzają to statuty wydawane w czasach rządów pruskich, w których nie ma żadnych zakazów utrudniających Polakom wstępowanie do bractwa. Niestety cezurą był tu rok 1888, kiedy to rozpoczął się gwałtowny proces germanizacji bractwa, które stawało się czysto niemieckie. Bydgoskie bractwo strzeleckie w sytuacji zagrożenia pełniło rolę straży komunalnej, ratowało i chroniło mienie mieszkańców podczas pożaru, jak również sprawowało służbę transportową na rzecz armii. Na bractwo bydgoskie

na mocy rozporządzenia magistratu z 1834 r. nałożono obowiązek powoływania z grona braci straży pożarnej, która początkowo liczyła zaledwie 12 osób, mającej stawiać się w razie pożaru na strzelnicy. W 1845 r. bractwo ewoluowało w batalion strzelecki pełniący funkcję milicji miejskiej; jego członkowie odbywali typowo wojskowe ćwiczenia w umundurowaniu. Batalion ten był kilka razy użyty celem zapewnienia porządku w mieście; dotyczyło to m.in. wystąpień ludności polskiej, które miały miejsce w latach 1848, 1864, 1866 i 1870. Dopiero opanowanie Bydgoszczy przez wojska polskie w dniu 20 stycznia 1920 r. przyniosło zarówno tak długo oczekiwaną niepodległość, jak też zmieniło charakter bractwa. Idee strzeleckie zostały bowiem wzbogacone o polskie wartości narodowo-patriotyczne.

7 sierpnia 1922 r. w Hotelu Bazar Poznański, w którym w 1848 miał swą siedzibę rząd polski (w okresie Wiosny Ludów), zebrało się 133 delegatów bractw, głównie z województwa poznańskiego. Powołano na nim Zjednoczenie Bractw Strzeleckich Zachodnich Ziem Polskich i uchwalono jego statut, określono także cel działalności, którym miało być „krzewienie tradycyjnego strzelnictwa obywatelskiego, szerzenie idei bractw strzeleckich, budzenie świadomości poczucia obowiązków obywatelskich i państwowych względem Rzeczypospolitej Polskiej". Po odzyskaniu niepodległości na terenie byłego zaboru pruskiego wzrosła rola religii rzymskokatolickiej; uroczyste msze rozpoczynały wszystkie brackie wydarzenia i imprezy, a bydgoscy bracia zobowiązani byli do udziału w uroczystościach religijnych. Odnosiło się to przede wszystkim do świąt powszechnych – takich jak Wielkanoc czy Boże Ciało. Bracia stali wówczas jako straż honorowa przy baldachimie.

Wybuch II wojny światowej stanowił smutny koniec działalności bractwa strzeleckiego. Bydgoscy bracia toczyli walkę z okupantem, pozostając wierni hasłu: „Ćwicz oko i dłonie w Ojczyzny obronie". Śmierć poniósł członek honorowy bractwa i ostatni przedwojenny prezydent Bydgoszczy Leon Barciszewski, który został rozstrzelany 11 listopada 1939 r. W trakcie wojny w brackiej strzelnicy hitlerowcy organizowali swoje imprezy, m.in. z udziałem Alberta Forstera i Josepha Goebbelsa. 10 stycznia 1946 r. bractwo zostało oficjalnie zlikwidowane, a w historycznej Strzelnicy w 1955 r. utworzono Wojewódzki Dom Kultury, w którym obecnie mieści

się kinoteatr Adria. Działalność bractwa kurkowego została wznowiono w Bydgoszczy dopiero w 1995 r.

W polskich, ale także europejskich bractwach strzeleckich na przestrzeni lat zmieniały się zarówno ich struktury organizacyjne, jak i cele działania. Pierwotnie powoływane do obrony miejskich murów, stopniowo traciły swój paramilitarny charakter i stawały się stowarzyszeniami kultywującymi historyczną tradycję oraz kształtującymi postawy patriotyczne. Obecnie bractwa stanowią interesujące zjawisko kulturowe.

Grażyna Lichończak-Nurek wskazuje, iż te pierwotne zadania bractw strzeleckich straciły na znaczeniu w XIX w. Jednocześnie pomimo że realia podważały zasadność i potrzebę działania tych stowarzyszeń, na zachodzie Europy następowało ich odrodzenie; pojawiła się również tendencja zmierzająca do integracji poszczególnych bractw. Już z końcem lat 20. XIX w. utworzony został Związek Niemieckich Historycznych Bractw Strzeleckich (Bund der Historischen Deutschen Schützenbruderschaften – BHDS), który aktywnie działa do dzisiaj. W 1861 r. powstał mający podobny charakter Związek Niemieckich Bractw Strzeleckich (Deutsche Schützenbund), natomiast prawdziwa integracja ruchu strzeleckiego w skali europejskiej nastąpiła dopiero po zakończeniu II wojny światowej. Ważnym krokiem było powołanie do życia w 1962 r. Związku Bractw Strzeleckich: organizacja ta z siedzibą w Eilendorf, pod Akwizgranem postawiła sobie za cel reprezentowanie interesów bractw strzeleckich na terenie Belgii, Holandii i Niemiec. W Einhoven (Holandia) w 1975 r. uroczyście zarejestrowano Europejskie Stowarzyszenie Historycznych Bractw Strzeleckich, które co kilka lat organizuje Europejskie Święta Strzeleckie. Podczas ich trwania dokonywany jest wybór najlepszego strzelca w Europie, któremu nadawany jest tytuł Europejskiego Króla Kurkowego. Józef Marecki zauważa, iż wprawdzie wszyscy „kurkowi" nazywają się braćmi i siostrami, ale mimo tendencji i procesów zjednoczeniowych poszczególne bractwa różnią się strojami. Są to „barwne kontusze, dwurzędowe marynarki, wojskowe mundury, stroje klubowe, kontusiki i inspirowane dworską modą suknie". Według badacza bogactwo strojów brackich obrazuje zróżnicowanie tych organizacji.

Wspólne elementy działalności bractw to przywiązanie do tradycji, strzelectwo i zainteresowanie historią. Są jednak obszary działalności

poszczególnych bractw, które mają charakter dominujący, a inne stanowią tylko element uzupełniający. Austriackie kompanie skupiają swą aktywność na odtwarzaniu głośnych bitew, podczas których w strojach z epoki upamiętniają historyczne postacie, posługując się przy tym replikami dawnego oręża. Na polskim gruncie takimi działaniami zajmują się głównie grupy rekonstrukcyjne, a nie bractwa kurkowe.

Małgorzata Niechaj, opisując Bractwo Strzeleckie w Żorach, zauważa, iż do jego głównych celów należą popularyzacja kultury militarnej, współpraca z organizacjami o podobnych celach, prowadzenie działalności wychowawczej i kolportażowej czasopism, książek, broszur o tematyce historyczno-obronnej oraz uprawianie sportu strzeleckiego. Inni badacze, opisując bractwa z południowo-wschodniej Polski, podkreślają aspekty związane z uprawianiem sportu strzeleckiego.

Z kolei Krzysztof Gwóźdź wskazuje, że „bractwa kurkowe tradycyjnie uczestniczą w świętach religijnych i współpracują z Kościołem katolickim". Marecki uznaje bractwa za „społeczność osobliwą", jednocześnie słusznie zauważa, że są to „elitarne lokalne grona dbające o dobro wspólne i potrzeby innych, działacze charytatywni i społeczni, mimo władania bronią nastawione wyjątkowo pacyfistycznie osoby znane, wpływowe". Przykładem takich pozytywnych i pożądanych prospołecznych działań jest opisane wcześniej Krakowskie Bractwo Kurkowe, które angażuje się w pomoc Schronisku dla Niepełnosprawnych w Radwanowicach, należącemu do Fundacji im. Brata Alberta. Dzięki środkom zebranym wśród braci oraz wsparciu zagranicznych bractw stowarzyszonych w Europejskiej Federacji Historycznych Towarzystw Strzeleckich wybudowano w Radwanowicach Dom Przyjaciół. Bractwo corocznie, od 1998 r. organizuje Królewsko-Marszałkowski Bal Kurkowy, podczas którego odbywa się aukcja na rzecz dzieci niepełnosprawnych. Ponadto Krakowskie Bractwo Kurkowe jest także fundatorem 10 sztandarów wojskowych oraz 2 szkolnych. Bracia uczestniczą we wszystkich ważnych uroczystościach kulturalnych, religijnych i patriotycznych nie tylko na terenie Krakowa, dodając im historycznego i barwnego kolorytu.

Andrzej Czop

M. Dubiecki, *Towarzystwo Strzeleckie w Krakowie*, Towarzystwo Strzeleckie, Kraków 1902; Z. Gloger, *Księga rzeczy polskich*, Macierz Polska, Lwów 1896; K. Gwóźdź, *Bractwo Strzeleckie w Tarnowskich Górach. Historia i współczesność*, Kurkowe Bractwo Strzeleckie, Tarnowskie Góry 2008; K. Gwóźdź, G. Lichończak-Nurek, *Bractwo Strzeleckie z Tarnowskich Gór*, Muzeum Historyczne Miasta Krakowa, Kraków 2003; T. Jakubiak, *Kurkowe Bractwa Strzeleckie w Wielkopolsce*, Wydawnictwo Poznańskie, Poznań 1986; B. Janiszewska-Mincer, *Strzelnica Bractwa Kurkowego*, „Kalendarz Bydgoski" na rok 1973, Bydgoszcz 1972; K. Jelonek-Litewka, *Inwentarz akt Towarzystwa Strzeleckiego (Bractwo Kurkowe) w Krakowie z lat 1591–1939 (1964–2004)*, Archiwum Państwowe, Kraków 2005; G. Lichończak-Nurek, *Krakowskie Bractwo Kurkowe dla niepodległości Polski*, Muzeum Historyczne Miasta Krakowa, Kraków 2008; G. Lichończak-Nurek, *Tradycje, zwyczaje i pamiątki Krakowskiego Bractwa Kurkowego*, Muzeum Okręgowe Ziemi Kaliskiej, Kalisz 1993; G. Lichończak-Nurek, M. Satała, *Kraków i jego bractwo kurkowe przez 750 lat*, Bractwo Kurkowe, Kraków 2007; L. Ludwikowski, L. Wroński, T. Wroński, *Z dziejów Towarzystwa Strzeleckiego w Krakowie*, Wydawnictwo EPOKA, Warszawa 1979; J. Marecki, *Społeczność osobliwa. Wstęp*, [w:] L. Rotter, *Bractwa Kurkowe w Polsce. Mundury, stroje, emblematy, insygnia*, Wydawnictwo Avalon, Kraków 2012; M. Niechaj, *Kurkowe Bractwo Strzeleckie w Żorach. Historia i tradycje*, Muzeum Historyczne Miasta Krakowa, Kraków 2008; M. Ostrowska, *Towarzystwo Strzeleckie Bractwo Kurkowe*, „Bezpieczeństwo Teoria i Praktyka" 2014, nr 2(XV); P. Redlarski, *Kurkowe Bractwo Strzeleckie w Bydgoszczy w latach 1920–1939*, [w:] *Kronika Bydgoska XXXI*, Towarzystwo Miłośników Bydgoszczy, Bydgoszcz 2010; T. Wroński, *Krakowskie Towarzystwo Strzeleckie Bractwo Kurkowe*, Krajowa Agencja Wydawnicza, Kraków 1984.

C

CENTRA DOSKONAŁOŚCI NATO – COE (ang. NATO Centres of Excellence) – podmiot ustanowiony i sponsorowany na poziomie międzynarodowym lub narodowym, który nie jest finansowany z budżetu Sojuszu. Rolą COE jest dostarczanie specjalistycznej wiedzy i doświadczenia w ściśle określonym obszarze wojskowym. Dystrybuuje wiedzę poprzez konferencje, seminaria, szkolenia i publikacje. Centra umożliwiają NATO rozwijanie zdolności, wspieranie transformacji i zwiększenie interoperacyjności bez konieczności rozbudowywania wewnętrznej struktury dowodzenia, ponieważ czerpią z krajowych zasobów i specjalistycznej ekspertyzy. Centra szkolą specjalistów i liderów z krajów członkowskich i partnerskich NATO, a także pomagają w opracowywaniu doktryn, poprawiają interoperacyjność i zdolności, wyciągają wnioski oraz weryfikują i testują koncepcje poprzez eksperymenty. Istotne jest, że NATO nie może zlecać zadań COE, ponieważ nie podlegają dowództwu SCAT (Supreme Allied Commander Transformation). SCAT jest jednym z dwóch strategicznych dowódców NATO i stoi na czele Dowództwa ds. Transformacji Sojuszniczej. Odpowiada przed najwyższym organem wojskowym NATO

– Komitetem Wojskowym – za promowanie i nadzorowanie ciągłej transformacji sił zbrojnych i potencjału Sojuszu.

Do zasad COE należą:

- brak duplikacji istniejących zasobów;
- relacje z dowództwami strategicznymi poprzez porozumienia o współpracy;
- brak kosztów dla NATO;
- zgodność z procedurami, doktrynami i standardami NATO;
- relacje z partnerami są wspierane i zachęcane.

Centra Doskonałości NATO obejmują szeroki zakres specjalizacji i oferują specjalistyczne wsparcie w takich obszarach, jak zwalczanie improwizowanych urządzeń wybuchowych, wojna minowa na morzu, operacje cywilno-wojskowe, bezpieczeństwo energetyczne, zmiany klimatu i bezpieczeństwo, obrona przed terroryzmem, cyberobrona, przestrzeń kosmiczna, medycyna wojskowa i operacje w warunkach zimowych. Do COE zaliczają się:

- **Stability Policing (SP)** – oferuje specjalistyczną wiedzę w dziedzinie *stability policing*, czyli wszelkich działań policyjnych realizowanych przez siły NATO. Ma to na celu wzmocnienie lub tymczasowe zastąpienie lokalnej policji;
- **Civil-Military Cooperation (CCOE)** – ma na celu dzielenie się wspólną wiedzą, łączenie ludzi i osiąganie jedności celów w dziedzinie współpracy cywilno-wojskowej;
- **Climate Change And Security COE (CCASCOE)** – wspiera działania partnerów i sojuszników NATO, które mają na celu dostosowanie się do skutków zmian klimatu oraz łagodzenie własnego wpływu na zmiany klimatu;
- **Cold Weather Operations (CWO)** – pełni funkcję głównego koordynatora i dostawcy wiedzy specjalistycznej oraz potencjału w zakresie operacji prowadzonych w niskich temperaturach;
- **Combined Joint Operations from the Sea (CJOS)** – wspiera Państwa Sponsorujące i NATO w zwiększaniu ich zdolności do przeprowadzania połączonych operacji morskich w celu przeciwdziałania wyzwaniom w zakresie globalnego bezpieczeństwa morskiego;

- **Air Operations (AO)** – AO COE to jednostka krajowa należąca do francuskiego Dowództwa Obrony Powietrznej i Operacji Powietrznych (CDOAA), która przygotowuje personel wojskowy do dowodzenia i kontroli operacji powietrznych;
- **Operations in Confined and Shallow Waters (CSW)** – zapewnia skoordynowaną wiedzę specjalistyczną w zakresie operacji na wodach ograniczonych i płytkich dla NATO i państw uczestniczących w COE CSW;
- **Cooperative Cyber Defence (CCD)** – dostarcza specjalistycznej wiedzy z zakresu cyberobrony, obejmującej takie obszary jak strategia, technologia, operacje i prawo;
- **Counter Improvised Explosive Devices (C-IED)** – dostarcza fachową wiedzę w celu wsparcia społeczności międzynarodowej w walce z systemem improwizowanych ładunków wybuchowych, a także współpracuje na rzecz zwiększenia bezpieczeństwa państw sojuszniczych i wojsk rozmieszczonych na terenach działań wojennych;
- **Integrated Air & Missile Defence (IAMD)** – zapewnia ochronę ludności i sił Sojuszu przed atakami i zagrożeniami powietrznymi oraz rakietowymi;
- **Explosive Ordnance Disposal (EOD)** – zajmuje się szkoleniem, analizą doświadczeń, standaryzacją i rozwojem technologii w dziedzinie neutralizacji materiałów wybuchowych;
- **Counter Intelligence (CI)** – chroni Sojusz przed zagrożeniami wywiadowczymi;
- **Crisis Management and Disaster Response (CMDR)** – pełni rolę centrum wiedzy specjalistycznej w dziedzinie zarządzania kryzysowego i reagowania na katastrofy;
- **Energy Security (ENSEC)** – celem COE jest zapewnianie doradztwa eksperckiego w kwestiach związanych z bezpieczeństwem energetycznym. COE utworzone zostało 10 lipca, a akredytowane 12 października 2012 r.;
- **Military Medicine (MILMED)** – wspiera Sojusz w dziedzinie medycyny wojskowej;

- **Human Intelligence (HUMINT)** – realizuje funkcje COE w zakresie wywiadu HUMINT, czyli wywiadu ludzkiego (oznacza to pozyskiwanie informacji poprzez bezpośredni kontakt z ludźmi);
- **Joint Air Power Competence Centre (JAPCC)** – dostarcza decydentom rozwiązania w zakresie wyzwań związanych z siłą powietrzną i kosmiczną w celu ochrony interesów NATO i państw członkowskich;
- **Defence Against Terrorism (DAT)** – działa jako organ doradczy ACT w kwestiach związanych z terroryzmem i ze zwalczaniem terroryzmu;
- **Joint Chemical, Biological, Radiological and Nuclear Defence (JCBRN Defence)** – promuje adaptacyjne i innowacyjne metody zapobiegania proliferacji broni masowego rażenia oraz ochrony przed incydentami z wykorzystaniem broni chemicznej, jądrowej lub biologicznej;
- **Maritime Geospatial, Meteorological & Oceanographic (MGEOMETOC)** – zapewnia wiedzę w dziedzinie geometodologii morskiej;
- **Modelling & Simulation (M&S)** – celem COE jest ciągłe doskonalenie w zapewnianiu wysokiej jakości możliwości kształcenia i szkoleń indywidualnych NATO poprzez wykorzystywanie efektywnego systemu zarządzania jakością;
- **Maritime Security (MARSEC)** – funkcjonuje jako ośrodek badań naukowych i ośrodek szkoleń praktycznych w dziedzinie bezpieczeństwa morskiego, a także w pokrewnych dziedzinach;
- **Strategic Communications (STRATCOM)** – przyczynia się do poprawy zdolności komunikacji strategicznej w ramach Sojuszu i państw sojuszniczych;
- **Military Police (MP)** – zapewnia specjalistyczną wiedzę na temat działań Policji Wojskowej i zwiększa potencjał Policji Wojskowej NATO;
- **Mountain Warfare (MW)** – zapewnia wiedzę i wzmacnia zdolności Sojuszu do prowadzenia walki w terenach górskich;

- **Naval Mine Warfare (NMW)** – zapewnia specjalistyczną wiedzę na temat wojny minowej na morzu;
- **Space (Space COE)** – działalność COE skupia się na dostarczaniu specjalistycznej wiedzy z zakresu kosmosu i rozwijaniu zdolności Sojuszu w zakresie działań kosmicznych;
- **Military Engineering (MILENG)** – zapewnia wiedzę w dziedzinie inżynierii wojskowej;
- **Security Force Assistance (SFA)** – celem COE jest poprawa skuteczności Sojuszu w promowaniu stabilności i odbudowy w sytuacjach konfliktowych i pokonfliktowych poprzez analizę doświadczeń, szkoleń, edukacji oraz rozwój koncepcji i doktryn;
- **Command and Control (C2)** – posiada wiedzę specjalistyczną w zakresie dowodzenia i kontroli.

Centra Doskonałości NATO formalnie nie wchodzą w skład Struktury Dowodzenia NATO, nie są też innymi stałymi agencjami Sojuszu. Każde z COE jest międzynarodową organizacją wojskową i podlega akredytacji przez Dowództwo Sojusznicze ds. Transformacji (ang. Allied Command Transformation – ACT). Sam proces otrzymania akredytacji jest sformalizowany oraz wieloetapowy i ma na celu zapewnienie, że każde COE spełnia najwyższe standardy. Proces ten rozpoczyna się od złożenia wniosku o utworzenie Centrum Doskonałości, który rozpatruje Dowództwo Sojusznicze ds. Transformacji, następnie koordynuje z Państwem lub Państwami Ustanawiającymi dalsze prace nad wnioskiem w celu dopracowania i szczegółowego opracowania propozycji. Oficjalna propozycja ustanowienia Centrum jest formalnie przesyłana do Naczelnego Dowódcy Sojuszniczych Sił Transformacyjnych (ang. Supreme Allied Commander Transformation – SACT). Jeśli wniosek spełnia określone kryteria, Dowództwo Sojusznicze ds. Transformacji formalnie go przyjmuje, następnie sporządzane jest Operacyjne Memorandum Zrozumienia, a później następuje przedstawienie oferty Centrum Doskonałości innym krajom. Podmioty zainteresowane dołączeniem do Centrum Doskonałości rozpoczynają negocjacje w sprawie Memorandum. W przypadku Centrów Doskonałości, które wcześniej nie posiadały żadnej placówki, zostają utworzone fizycznie. Oprócz tego Państwa Ustanawiające i Sponsorujące

muszą koordynować, opracowywać, negocjować i podpisać Funkcjonalne Memorandum Zrozumienia bezpośrednio z ACT. Kolejno Zespół ACT przeprowadza wizytę COE, oceniając je pod kątem dostosowania do szczególnej listy punktów opartej na kryteriach akredytacji Centrów Doskonałości Komitetu Wojskowego. Ostateczna akredytacja wymaga zgody Komitetu Wojskowego i Rady Północnoatlantyckiej. Po akredytacji ACT okresowo dokonuje ponownej oceny Centrów, aby upewnić się, że nadal spełniają kryteria i zapewniają ciągłość akredytacji NATO. Warty wspomnienia jest fakt, że istotnym wymogiem akredytacyjnym dla COE jest unikanie duplikacji zdolności z istniejącymi już strukturami NATO. COE muszą oferować specjalistyczną wiedzę w obszarze, który nie jest jeszcze dostępny w ramach Organizacji. W związku z tym, wszystkie COE muszą mieć w swoich szeregach ekspertów merytorycznych w swojej dziedzinie.

Nie każda organizacja może uzyskać akredytację w zakresie COE – żeby ją zdobyć, należy wykazać się specjalistyczną wiedzą w co najmniej 3 z 4 filarów, które obejmują:

- edukację i szkolenia;
- analizę i wnioski;
- rozwój doktryn i standardów;
- rozwój koncepcji i eksperymentowanie.

Idea utworzenia Centrów wyrosła z potrzeby dostosowania się do nowego środowiska bezpieczeństwa po zimnej wojnie. Koncepcja COE została sformułowana w dokumencie The NATO Military Command Structure z dnia 14 maja 2003 r., zaś dopracowanie tego pomysłu nastąpiło w dokumencie MCM-236-03 MC Concept for Centres of Excellence (COE) z dnia 4 grudnia 2003 r. przez Komitet Wojskowy. Rok później uzgodniono dokument IMSM-0416-04 NATO COE Accreditation Criteria, a w 2005 r. pierwsze COE uzyskało formalną akredytację, co zapoczątkowało program COE jako stały mechanizm transformacji. W 2019 r. dokument MCM-236-03 został zastąpiony MC 0685 (Military Committee Policy For Centres Of Excellence), a same kryteria akredytacji i okresowej oceny zostały ponownie zaktualizowane w 2022 r. poprzez dokument MCM-0086.

Równie istotnym dokumentem jest BI-SC DIR 080-001 – Dyrektywa Dowództwa Bi-Strategicznego w sprawie Koordynacji Centrów Doskonałości NATO (ang. Bi-Strategic Command Directive For The Coordination

Of NATO Centres Of Excellence), która definiuje obowiązki dotyczące COE oraz procesy zarządzania wykorzystywane do maksymalizacji korzyści zapewnianych Sojuszowi przez Centra. Dodatkowo określa procesy i rytmy działań wykorzystywane do zarządzania i synchronizacji wszystkich działań koordynacyjnych COE, wraz z ich obowiązkami.

W funkcjonowaniu COE uczestniczą trzy rodzaje podmiotów, różniące się zakresem odpowiedzialności i wkładu:

- Państwa Ustanawiające (ang. Framework Nations) – inicjują projekt i zobowiązują się do opracowania koncepcji i wdrożenia COE. Ponoszą główny ciężar utrzymania, zapewniając Centrum siedzibę, większość personelu i finansowanie. Są odpowiedzialne za złożenie początkowej propozycji utworzenia Centrum i sporządzenie Operacyjnego Memorandum Zrozumienia;
- Państwa Sponsorujące (ang. Sponsoring Nations) – partycypują w projekcie, wnosząc wkład finansowy i udostępniając specjalistyczny personel, pokrywając ich wynagrodzenie. Mogą udzielać wsparcia finansowego lub świadczyć inne usługi, które są przydatne w funkcjonowaniu Centrum;
- Państwa Kontrybuujące (ang. Contributing Nations) – dostarczają wsparcie w mniejszym zakresie, najczęściej w formie pojedynczych ekspertów.

COE są finansowane na poziomie międzynarodowym lub narodowym. Sojusz nie finansuje ich ze wspólnego budżetu, ale koszty pokrywane są przez Państwa Ustanawiające, Kontrybuujące lub Sponsorujące.

Lucyna Łowisz

2023 Catalogue, https://www.nspcoe.org/wp-content/uploads/2023/02/COE-2023-CATALOG-HR.pdf (dostęp 09.12.2025); *2025 Catalogue*, https://www.act.nato.int/wp-content/uploads/2024/12/2025-COE-CATALOGUE-Final-v2.pdf (dostęp 10.12.2025); *About the NATO Space COE*, https://space-coe.org/about-space-coe/ (dostęp 10.12.2025); *About Us*, https://www.japcc.org/about-us/ (dostęp 10.12.2025); *Allied Command Transformation*, https://www.nato.int/en/about-us/organization/nato-structure/allied-command-transformation (dostęp 09.12.2025); *Centers of Excellence*, https://www.act.nato.int/about/centres-of-excellence/ (dostęp 09.12.2025); K. Chmielarczyk, A. Nowakowska-Krystman, P. Owczarczyk,

Agregaty rozwoju i wykorzystania energii na polu walki, „Wiedza Obronna" 2023, t. 283, nr 2, https://doi.org/10.34752/2023-l283; *Climate change is affecting NATO security*, https://ccascoe.org/ (dostęp 10.12.2025); A.L. Kimball, *Reconceptualising burdens – NATO centres of excellence: club goods, informal institutions, and partner contributions*, „Defence Studies" 2024, no. 24(4), https://doi.org/10.1080/14702436.2024.2380886; *NATO Centers of Excellence*, https://www.nspcoe.org/about-us/nato-centres-of-excellence/ (dostęp 10.12.2025); *NATO stability policing center of excellence, Doctrine and Standardization*, https://www.nspcoe.org/what-we-do/doctrine-and-standardization/ (dostęp 9.12.2025); *Supreme Allied Commander Transformation (SACT)*, https://www.nato.int/en/about-us/organization/nato-structure/supreme-allied-commander-transformation-sact (dostęp 10.12.2025); *What is a Centre of Exellence?*, https://milengcoe.org/milengcoe/Pages/WhatisaCOE.aspx (dostęp 10.12.2025); *What Is a NATO Centre of Excellence?*, https://www.act.nato.int/article/nato-centres-excellence/ (dostęp 9.12.2025).

CENTRUM STIMSONA (ang. The Stimson Center) – założony w 1989 r. z inicjatywy Barry'ego Blechmana i Michaela Krepona ośrodek analityczny zajmujący się badaniami nad bezpieczeństwem międzynarodowym oraz zagadnieniami związanymi z globalnym dobrobytem. Od początku działalności *think tank* koncentruje się na opracowywaniu praktycznych rozwiązań służących stabilności i bezpieczeństwu w warunkach zmian politycznych oraz technologicznych. Prowadzone przez ośrodek prace koncentrują się na badaniach terenowych, współpracy z podmiotami rządowymi i pozarządowymi poprzez tworzenie inicjatyw w zakresie utrzymania pokoju i ochrony ludności cywilnej, szczególnie w obszarach dotkniętych konfliktami. Z uwagi na realizację programów oraz projektów na całym świecie Centrum przyjęło w swojej działalności politykę *do no harm*, zgodnie z którą dopuszczalne są tylko takie metody badawcze i strategie operacyjne, które przyczyniają się do zminimalizowania ryzyka pogorszenia sytuacji społecznej lub bezpieczeństwa w badanych środowiskach. Działania te mają przyczyniać się do uniknięcia niezamierzonych i negatywnych konsekwencji dla uczestników badań, a także pośrednich przedstawicieli lokalnych społeczności. Ponadto ośrodek angażuje się w diagnozę zagrożeń transnarodowych oraz formułuje zalecenia polityczne mogące znaleźć zastosowanie w praktyce. Jest to możliwe dzięki tworzonym przez Stimson Center analizom koncepcyjnym, projektom

pilotażowym czy rozbudowanej ofercie programów badawczych i tematycznych, wśród których można wymienić:

- **38 North Program** analizujący czynniki wpływające na politykę strategiczną Korei Północnej w celu lepszego zrozumienia dynamiki bezpieczeństwa w regionie i tworzenia alternatywnych rozwiązań strategicznych wobec tego państwa. Obejmuje także badania oparte na źródłach otwartych, dialogach strategicznych oraz budowie sieci eksperckich wspierających formułowanie polityk dotyczących kwestii nuklearnych i bezpieczeństwa na Półwyspie Koreańskim;
- **China Program** zajmujący się analizą strategicznych intencji oraz zachowania decydentów w polityce zagranicznej Chin, obejmując kontekst zmian w relacjach amerykańsko-chińskich. Celem tego programu jest ograniczanie ryzyka eskalacji, która może wynikać z nieporozumień, a także pogłębianie dialogu między środowiskami eksperckimi Chin oraz innymi państwami regionu;
- **Conventional Defense Program** koncentruje się na ograniczaniu ryzyka i negatywnych konsekwencji globalnego handlu bronią. Zespół badawczy analizuje statystyki związane z nielegalnym obrotem uzbrojenia, eksportem dronów, pomocą wojskową oraz rozwojem norm regulujących handel i użycie broni konwencjonalnej;
- **Converging Technology and Global Security Program** analizuje wpływ na bezpieczeństwo międzynarodowe szybko rozwijających się technologii, takich jak sztuczna inteligencja, *blockchain*, druk 3D, inżynieria genetyczna oraz technologie nuklearne. Ponadto bada możliwości ich zastosowania w zakresie transparentności zabezpieczeń oraz kontroli nad materiałami podwójnego zastosowania;
- **Cyber Program** bada zagrożenia wynikające z nadużyć technologii informacyjnych oraz narzędzi cybernetycznych. Koncentruje się przede wszystkim na analizach politycznych, identyfikacji rozwiązań regulacyjnych oraz współpracy międzysektorowej. Utrzymuje relacje z przedstawicielami środowisk

technicznych, naukowych, prawnych, sektorem prywatnym oraz organizacjami pozarządowymi;

- **East Asia Program** monitoruje procesy polityczne i bezpieczeństwa w Azji Wschodniej, analizując m.in. relacje Stanów Zjednoczonych z państwami regionu oraz dynamikę sytuacji obejmującej wzajemne relacje USA–Chiny–Tajwan. Program ten obejmuje także wymianę ekspertów i organizację spotkań służących identyfikacji problemów bezpieczeństwa oraz opracowywaniu rekomendacji dla polityki regionalnej;
- **Energy, Water and Sustainability Program** zajmuje się zagadnieniami zarządzania zasobami wodnymi i energetycznymi przede wszystkim w regionach Globalnego Południa. Prace analityczne programu obejmują badania transgranicznych dorzeczy, tj. Mekong, Ganges-Brahmaputra, Indus, Morze Aralskie oraz Eufrat i Tygrys, weryfikując możliwości poprawy bezpieczeństwa wodnego oraz równoważenia potrzeb wodnych i energetycznych;
- **Environmental Security Program** analizuje związki między zmianami środowiskowymi, zdrowiem populacji, dynamiką demograficzną, konfliktami i polityką zagraniczną. Ponadto prowadzi analizy przekrojowe oraz dialog z przedstawicielami rządów, społeczeństwa obywatelskiego i sektora prywatnego w celu identyfikacji ryzyka oraz opracowywania strategii wzmacniających odporność społeczeństw;
- **Global Governance, Justice and Security Program** bada funkcjonowanie instytucji globalnych i regionalnych oraz ich zdolność do reagowania na współczesne wyzwania, tj. konflikty wewnętrzne, ubóstwo, zmiany klimatyczne, dezinformacja czy kryzys zaufania do systemu wielostronnego. Obejmuje także dialogi polityczne, analizy eksperckie oraz współpracę z organizacjami i koalicjami na rzecz reformy globalnego zarządzania;
- **Japan Program** analizuje wewnętrzne i zewnętrzne uwarunkowania polityki Japonii oraz jej rolę jako podmiotu regionalnego i globalnego. Wspiera również komunikację między ekspertami japońskimi a środowiskami politycznymi i biznesowymi

w Stanach Zjednoczonych. Zajmuje się również skutkami rozwoju nowych technologii oraz zachodzących zmian geopolitycznych;
- **Korea Program** koncentruje się na analizie stosunków między Stanami Zjednoczonymi a Półwyspem Koreańskim oraz na zagadnieniach bezpieczeństwa regionalnego. Obejmuje 3 główne obszary badawcze dotyczące sojuszu USA–Korea Południowa, współpracy technologicznej oraz porusza zagadnienia dotyczące demokracji i życia społecznego w Korei Południowej;
- **Latin America Program** zajmuje się analizą wyzwań w Ameryce Łacińskiej i na Karaibach, w tym kwestii demokratycznego rządzenia, bezpieczeństwa, rozwoju gospodarczego, zasobów naturalnych, migracji, praw człowieka i praworządności;
- **Middle East Program** prowadzi dialogi eksperckie oraz projekty dyplomacji pośredniej typu Track 1.5 i Track II w regionie Bliskiego Wschodu. Jego celem jest tworzenie przestrzeni do rozmów między stronami zaangażowanymi w konflikty, poszukiwanie obszarów współpracy oraz opracowywanie propozycji rozwiązań dotyczących sytuacji politycznej, społecznej i bezpieczeństwa;
- **Multilateral Financial Diplomacy Program** bada znaczenie pełnego i przewidywalnego finansowania instytucji wielostronnych przez Stany Zjednoczone. Ponadto analizuje skutki nieregularnego finansowania misji pokojowych oraz inicjatyw w obszarze zdrowia, broni masowego rażenia, praw człowieka i klimatu;
- **National Security Reform Program** analizuje politykę bezpieczeństwa narodowego Stanów Zjednoczonych z perspektywy skuteczności wydatków wojskowych oraz odpowiedzialności wobec podatników. Wskazuje także obszary nieefektywności oraz proponuje rozwiązania służące racjonalizacji polityki obronnej;
- **North Africa Program** zajmuje się analizą procesów gospodarczych, politycznych i geostrategicznych w państwach Afryki Północnej, w tym w Egipcie, Libii, Tunezji, Algierii, Maroku

oraz Mauretanii. Prace poświęcone są także badaniom nad dynamiką wewnętrzną regionu oraz relacjami z partnerami międzynarodowymi;

- **Nuclear Security Program** koncentruje się przy współpracy z sektorem prywatnym na zagadnieniach obejmujących bezpieczeństwo technologii i materiałów jądrowych. Celem programu jest także wspieranie rozwoju bardziej kompleksowych standardów bezpieczeństwa nuklearnego;
- **Partnerships in Proliferation Prevention Program** wspiera państwa i instytucje międzynarodowe w działaniach na rzecz zapobiegania rozprzestrzenianiu broni masowego rażenia. Tworzy również zasoby informacyjne, narzędzia online, bazy danych oraz prowadzi szkolenia;
- **Powering Peace Program** bada możliwości wykorzystania energii odnawialnej w misjach terenowych ONZ, szczególnie w państwach o niskim poziomie dostępu do energii. Analizuje wpływ modernizacji infrastruktury energetycznej na bezpieczeństwo, efektywność kosztową i rozwój lokalny;
- **Protecting Civilians and Human Security Program** zajmuje się analizą przemocy wobec ludności cywilnej w konfliktach oraz identyfikacją mechanizmów jej ograniczania. Ponadto prace zespołowe poświęcone są badaniom terenowym, współpracy z organizacjami międzynarodowymi oraz opracowywaniu rekomendacji dla polityk publicznych;
- **Reimagining US Grand Strategy Program** analizuje strategię międzynarodową Stanów Zjednoczonych poprzez weryfikację przyjętych założeń politycznych, a także rozważanie alternatywnych podejść do roli USA w wymiarze globalnym;
- **Russia Program** prowadzi dialog ekspercki między środowiskami amerykańskimi i rosyjskimi w celu ograniczania ryzyka eskalacji konfliktu oraz poprawy komunikacji strategicznej. Prace zespołu obejmują także analizy dotyczące bezpieczeństwa regionalnego i stabilności strategicznej;
- **South Asia Program** weryfikuje dynamikę strategiczną w Azji Południowej, koncentrując się na ryzykach związanych z napięciami

nuklearnymi, konfliktami i wyścigami zbrojeń. Obejmuje także współpracę z ekspertami z regionu oraz działaniami na rzecz rozwoju narzędzi analitycznych i dialogu;
- **Southeast Asia Program** zajmuje się problemami zrównoważonego rozwoju, bezpieczeństwa i zarządzania zasobami naturalnymi w Azji Południowo-Wschodniej. Ponadto bada planowanie infrastrukturalne w dorzeczu Mekongu, podział zasobów oraz skutki konfliktów zbrojnych;
- **Strategic Foresight Hub Program** prowadzi analizy trendów globalnych, potencjalnego przyszłego ryzyka oraz możliwych scenariuszy rozwoju. Dostarcza narzędzi do planowania strategicznego oraz wspiera decydentów w zarządzaniu;
- **Trade and Investment Security Program** koncentruje się na przepływach towarów i technologii o znaczeniu strategicznym, a także na działaniach mogących przyczyniać się do ograniczania ryzyka proliferacji broni masowego rażenia. Prace obejmują także szkolenia, narzędzia dobrych praktyk, współpracę z administracją, sektorem prywatnym oraz organizacjami międzynarodowymi.

Siedzibą Centrum jest Waszyngton. Działalność ośrodka jest finansowana przede wszystkim dzięki grantom, kontraktom badawczym, darowiznom oraz funduszom pochodzącym z różnych instytucji. Ośrodek każdego roku publikuje pełną listę darczyńców i źródeł finansowania, a także dostarcza informacji przedstawiających ogólną kondycję finansową organizacji. Struktura zarządcza Stimson Center obejmuje Radę Dyrektorów, która odpowiada za nadzór strategiczny i finansowy oraz prowadzące bieżące działania organizacji kierownictwo wykonawcze. Na czele ośrodka w 2025 r. stał prezes i dyrektor generalny (*president*/CEO) Brian Finlay, wspierany przez kadrę zarządzającą: Rachel Stohl – starszą wiceprezes ds. programów badawczych, Juliana Mueller-Kalera – szefa gabinetu i dyrektora, Justine Sullivan – wiceprezes ds. relacji zewnętrznych, oraz Vibhę Bhatię – wiceprezes ds. finansów i operacji. Strukturę organizacyjną uzupełniają dyrektorzy programowi, którzy kierują poszczególnymi obszarami badawczymi.

Artur Jach-Chrząszcz

D.E. Abelson, *Old World, New World: The Evolution and Influence of Foreign Affairs Think Tanks*, [w:] *Think Tanks and Foreign Policy*, Routledge, London 2014; M.P. Carland, C. Faber, *Careers in International Affairs*, Georgetown University Press, Washington 2008; E. Laipson, *Looking back at the Stimson center's role in the early twenty-first century*, The Future of Think Tanks and Policy Advice in the United States, 2023, JSTOR, Stimson Center – Research Reports, https://www.jstor.org/publisher/stimsoncenter (dostęp 25.11.2025); *The Stimson Center*, https://www.stimson.org (dostęp 25.11.2025).

CHATGPT (ang. *Generative Pre-trained Transformer*) – został opracowany przez amerykańską firmę laboratoryjną OpenAI i w całości oparty na architekturze GPT, czyli autoregresyjnym modelu językowym wykorzystującym głębokie uczenie się. Pierwszy model GPT został wprowadzony na rynek stosunkowo niedawno, bo w czerwcu 2018 r. Od tego momentu OpenAI koncentruje się na systematycznym opracowywaniu coraz nowszych i bardziej zaawansowanych modeli. Rok później zaprezentowano model GPT-2, a w 2020 r. – trzecią generację, GPT-3. Modele te były stopniowo udoskonalane w celu coraz lepszego rozumienia, generowania oraz przetwarzania języka naturalnego. Przełomowym momentem było wprowadzenie na rynek 14 marca 2023 r. generacji modelu – GPT-4, charakteryzującego się znacznie wyższą wydajnością w porównaniu z wcześniejszymi modelami, a także szybszym reagowaniem na zapytania użytkowników. Obecnie GPT-5 – czyli najnowsza główna generacja modeli GPT, która zaczęła być wdrażana 7 sierpnia 2025 r., zastępuje wcześniejsze wersje jako domyślny model w ChatGPT.

Jest to duży model językowy (ang. Large Language Models, LLM), zdolny do udzielania zróżnicowanych odpowiedzi na pytania formułowane przez użytkowników, generowania tekstów oraz wspierania różnorodnych zadań wymagających przetwarzania informacji językowych (m.in. streszczanie informacji czy tłumaczenie tekstów). Model ten liczy aż 175 mld parametrów i jest poddawany treningowi na bardzo obszernych zbiorach danych. Chatbot oparty na sztucznej inteligencji obsługuje zapytania w ponad 95 językach naturalnych. Należy jednak podkreślić, że jego skuteczność może różnić się w zależności od języka oraz stopnia złożoności generowanego tekstu – najwyższą jakość odpowiedzi ChatGPT osiąga w języku angielskim. Narzędzie to nie posiada świadomości ani

intencji – jego odpowiedzi są wynikiem statystycznego przewidywania kolejnych elementów tekstu na podstawie dostarczonego kontekstu. Jak wskazuje Olaf Staniszewski (2023), ChatGPT stanowi narzędzie sztucznej inteligencji wykorzystujące zaawansowane metody uczenia maszynowego do tworzenia tekstów oraz prowadzenia konwersacji imitujących komunikację międzyludzką. Dzięki mechanizmom uczenia maszynowego chatbot może udoskonalać swoje działanie na podstawie interakcji z użytkownikami, co pozwala na bieżące dostosowywanie generowanych odpowiedzi. ChatGPT coraz częściej znajduje zastosowanie w wielu obszarach życia, wpływając na sposób pracy, nauki i komunikacji.

Do podstawowych funkcji ChatGPT należą przede wszystkim prowadzenie dialogu w języku naturalnym, co umożliwia użytkownikom komunikację z systemem w sposób zbliżony do rozmowy międzyludzkiej. Narzędzie to potrafi udzielać odpowiedzi zarówno na pytania faktograficzne, jak i problemowe, wymagające analizy, porównania informacji lub logicznego wnioskowania. Istotną funkcją ChatGPT jest także generowanie oraz redagowanie różnorodnych form tekstowych, takich jak artykuły, opisy, eseje, streszczenia czy treści użytkowe dostosowane do określonego stylu i celu. Niewątpliwie ChatGPT znajduje szerokie zastosowanie w edukacji, oferując wsparcie w nauce poprzez wyjaśnianie zagadnień z różnych dziedzin wiedzy czy porządkowanie informacji. Jako innowacyjna technologia posiada znaczący potencjał, z którego mogą skorzystać nauczyciele w zakresie podnoszenia swoich kompetencji, prowadzenia zajęć dydaktycznych oraz przygotowania uczniów do wyzwań przyszłości. Narzędzie to może zatem pełnić ważną rolę we wspieraniu tej grupy zawodowej w wykonywaniu ich obowiązków, m.in. poprzez pomoc w przygotowywaniu materiałów dydaktycznych oraz realizacji zadań administracyjnych. ChatGPT umożliwia nauczycielom szybkie opracowywanie oryginalnych pytań uwzględniających różne aspekty omawianych zagadnień. Ponadto, pełniąc funkcję wirtualnego tutora, zapewnia stały dostęp do zasobów edukacyjnych oraz bieżące wsparcie merytoryczne.

W związku z rosnącą popularnością edukacji włączającej, a tym samym zwiększającą się liczbą uczniów ze specjalnymi potrzebami edukacyjnymi, ChatGPT może być z powodzeniem wykorzystywany przez nauczycieli jako narzędzie pomagające w personalizacji materiałów edukacyjnych

oraz ich dostosowywaniu do indywidualnych potrzeb uczniów. Jak wynika z literatury przedmiotu, ChatGPT jest w stanie generować zróżnicowane ćwiczenia przeznaczone dla uczniów, dostosowując poziom trudności do stopnia zrozumienia treści, proponując pytania bardziej zaawansowane lub uproszczone. Oprócz tego ChatGPT może zwiększać dostępność edukacji dla osób z niepełnosprawnością wzroku lub słuchu: przykładem jest wykorzystanie CzatGPT przez osoby niesłyszące do streszczania obszernych fragmentów tekstu lub uzyskiwania prostych, zwięzłych odpowiedzi.

Dzięki zaawansowanym funkcjom przetwarzania języka naturalnego ChatGPT może wspomagać osoby z niepełnosprawnościami w tworzeniu wypowiedzi pisemnych i wyrażaniu własnych myśli, co znacząco zwiększa dostępność oraz inkluzywność komunikacji z nauczycielem. ChatGPT może pełnić także funkcję narzędzia wspierającego rozwój kompetencji językowych, umożliwiając użytkownikom ćwiczenie umiejętności komunikacyjnych oraz poszerzanie zasobu słownictwa w różnych językach. Ponadto system ten wspomaga użytkowników w zakresie programowania, m.in. poprzez wyjaśnianie fragmentów kodu, proponowanie rozwiązań algorytmicznych oraz analizę danych. Dzięki zdolności do rozwiązywania problemów logicznych i adaptacji do poziomu wiedzy użytkownika ChatGPT znajduje zastosowanie zarówno w edukacji, jak i w praktyce zawodowej, stanowiąc wszechstronne narzędzie wspierające pracę intelektualną, kreatywność oraz samodzielne uczenie się w różnych dziedzinach. Dodatkowo może pełnić rolę asystenta w przygotowywaniu raportów, prezentacji czy analiz, co czyni go przydatnym nie tylko dla uczniów i nauczycieli, ale także dla profesjonalistów w wielu branżach. System ten może być integrowany z innymi aplikacjami i platformami cyfrowymi, co zwiększa zakres jego praktycznego wykorzystania. Oznacza to, że ChatGPT nie działa wyłącznie jako samodzielny chatbot, lecz może współpracować z różnymi programami, narzędziami i usługami online. Dotyczy to m.in. możliwości tworzenia dokumentów, prezentacji czy arkuszy kalkulacyjnych w programach typu Word czy Excel, wspierając raportowanie, analizę dokumentów czy generowanie podsumowań. Ponadto chatbot może być włączony do komunikatorów lub systemów obsługi klienta, gdzie odpowiada na pytania użytkowników w czasie rzeczywistym. Dzięki takim integracjom ChatGPT staje się bardziej uniwersalnym narzędziem – nie

jest już tylko samodzielnym chatbotem, lecz funkcjonalnym asystentem. Współpraca ChatGPT z wieloma aplikacjami i usługami cyfrowymi znacznie rozszerza jego praktyczne możliwości (np. Canva – generowanie i edycja projektów graficznych; Spotify – tworzenie list odtwarzania lub sugestii muzycznych; Booking.com – wyszukiwanie ofert hotelowych, lotów czy planowanie podróży). Integracje te pozwalają użytkownikom wykonywać różnorodne zadania w innych aplikacjach, usprawniając pracę, naukę czy codzienne czynności.

ChatGPT znajduje zastosowanie w wielu obszarach życia zawodowego, edukacyjnego i codziennego, co wynika z jego wszechstronnych funkcji oraz możliwości integracji z innymi narzędziami cyfrowymi. Wśród najważniejszych obszarów zastosowań należy wymienić edukację, administrację i biznes oraz media i kulturę. Dzięki szerokiemu zakresowi zastosowań ChatGPT stanowi także uniwersalne narzędzie wspierające rozwój osobisty.

Wraz z rosnącym zastosowaniem ChatGPT w edukacji, pracy zawodowej i życiu codziennym pojawiają się również istotne wątpliwości, obawy i kontrowersje. Narzędzie to, mimo swoich licznych zalet, wiąże się z potencjalnymi zagrożeniami, które wymagają świadomego i odpowiedzialnego użytkowania. Niewątpliwie jednym z najpoważniejszych jest ryzyko rozpowszechniania nieprawdziwych lub stronniczych informacji. ChatGPT generuje odpowiedzi na podstawie wzorców językowych i danych, w oparciu o jakie był „trenowany"; nie posiada zdolności weryfikacji faktów ani własnej świadomości. W rezultacie może przekazywać informacje nieścisłe, przestarzałe, tendencyjne czy nawet błędne. W kontekście edukacji, dziennikarstwa czy badań naukowych takie nieścisłości mogą wprowadzać użytkowników w mylne przekonania i utrwalać nieprawdziwe informacje, co jest poważnym zarzutem. Warto nadmienić, że coraz większym problemem staje się możliwość celowego, nieuczciwego wykorzystania ChatGPT, np. do masowego generowania treści w celach dezinformacyjnych, tworzenia fałszywych wiadomości, opinii czy artykułów. Oprócz tego istnieje ryzyko plagiatu – użytkownicy mogą stosować wygenerowane teksty w swojej pracy bez właściwego oznaczenia źródła cytowania, co rodzi istotne konsekwencje etyczne i prawne. Kolejną obawą są kwestie związane z ochroną danych osobowych i prywatności.

W przypadku niewłaściwego zarządzania lub udostępniania tych danych istnieje ryzyko naruszenia prywatności; dotyczy to szczególnie wrażliwych informacji, takich jak dane osobowe m.in. uczniów, pacjentów czy klientów firm. Wymaga to stosowania środków ochrony danych i świadomości ryzyka przy korzystaniu z narzędzia. Innym przykładem kontrowersji i obaw związanych z ChatGPT jest jego wpływ na rynek pracy i automatyzację zawodów.

Wdrażanie ChatGPT i innych systemów AI może prowadzić do automatyzacji niektórych zadań, które wcześniej były wykonywane przez ludzi. Taka sytuacja może wpływać na redukcję miejsc pracy w wielu zawodach, zwłaszcza tych, które opierają się na przetwarzaniu tekstu, obsłudze klienta czy analizie danych. Smutną konsekwencją nadmiernego polegania na ChatGPT jest również to, że może prowadzić do ograniczenia rozwoju samodzielnego myślenia, umiejętności krytycznej analizy informacji oraz zdolności pisania. Korzystając nagminnie z gotowych rozwiązań, możemy doprowadzić do tzw. „cyfrowej demencji", czyli stopniowego osłabienia zdolności pamięci, koncentracji i samodzielnego myślenia.

Choć ChatGPT oferuje szerokie możliwości wsparcia nie tylko w edukacji i pracy, ale również w życiu codziennym, jego wykorzystanie wymaga daleko idącej rozwagi oraz świadomości potencjalnych zagrożeń. Szczególnie istotne jest przestrzeganie zasad etyki, odpowiedzialności oraz stosowanie mechanizmów kontroli, które pozwoliłyby zminimalizować ryzyko związane z dezinformacją, naruszeniem prywatności czy nieuczciwym wykorzystaniem narzędzia. ChatGPT jest z pewnością jednym z najbardziej rozpoznawalnych przykładów praktycznego zastosowania sztucznej inteligencji we współczesnym świecie. Jego dynamiczny rozwój i popularyzacja odzwierciedlają szersze procesy cyfrowej transformacji społeczeństwa, ale równocześnie stawiają przed użytkownikami, instytucjami i prawodawcami nowe wyzwania technologiczne, społeczne i etyczne.

W odpowiedzi na dynamiczny wzrost zainteresowania oraz coraz szersze zastosowanie sztucznej inteligencji w różnych obszarach życia społecznego Unia Europejska w kwietniu 2021 r. zaproponowała pierwsze wspólnotowe ramy prawne regulujące wykorzystanie systemów AI. Projekt ten zakłada analizę i klasyfikację systemów sztucznej inteligencji stosowanych w rozmaitych aplikacjach, w oparciu o poziom ryzyka, jakie mogą

one stwarzać dla użytkowników. Priorytetem Parlamentu Europejskiego jest zapewnienie, aby systemy AI były bezpieczne, przejrzyste, możliwe do zidentyfikowania, niedyskryminujące oraz przyjazne dla środowiska. Dodatkowo podkreśla się konieczność sprawowania nad nimi nadzoru przez człowieka w celu ograniczenia potencjalnych negatywnych skutków ich działania.

Nie ma wątpliwości, że rozwój nowoczesnych technologii, w tym narzędzi opartych na sztucznej inteligencji, takich jak ChatGPT, jest procesem, którego nie da się cofnąć. Postęp ten w szybkim tempie wkracza w różne sfery życia i staje się integralną częścią naszej codzienności. Wobec takich zjawisk nie możemy pozostawać bierni jako społeczeństwo, lecz powinniśmy aktywnie przygotowywać się na wyzwania, jakie one ze sobą niosą. Kluczowe jest budowanie i wzmacnianie świadomości technologicznej oraz rozwijanie kompetencji cyfrowych, które pozwolą w pełni korzystać z możliwości nowych narzędzi przy jednoczesnym minimalizowaniu zagrożeń, takich jak dezinformacja, naruszenie prywatności czy nieetyczne wykorzystanie technologii. Przygotowanie społeczeństwa na dynamiczny rozwój nowoczesnych technologii i wyzwania z tym związane to nie tylko kwestia bezpieczeństwa, ale przede wszystkim szansa na świadome i efektywne wykorzystanie potencjału sztucznej inteligencji w życiu prywatnym i zawodowym w sposób, by technologia służyła ludziom, a nie odwrotnie.

Magdalena Szumiec

Akt w sprawie sztucznej inteligencji: posłowie przyjmują przełomowe przepisy, https://www.europarl.europa.eu/news/pl/press-room/20240308IPR19015/akt-w-sprawie-sztucznej-inteligencji-poslowie-przyjmuja-przelomowe-przepisy (dostęp 13.01.2026); P. Cabała, K. Kwiatkowska, K. Woźniak, M. Zakrzewska, *Opinie studentów wobec możliwości i ograniczeń wykorzystania systemu ChatGPT*, „e-mentor" 2023, t. 102(5); W.M. Czerski, *CHATGPT – Potrzebne narzędzie czy przekleństwo naszych czasów?*, „Dydaktyka Informatyki" 2023, nr 18; D. Kalla, N. Smith, F. Samaah, S. Kuraku, *Study and analysis of chat GPT and its impact on different fields of study*, „International Journal of Innovative Science and Research Technology" 2023, vol. 8(3); G. Kok Ming, M. Mansor, *Exploring the Impact of Chat-GPT on Teacher Professional Development: Opportunities, Challenges, and Implications*, „Asian Journal of Research in Education and Social Sciences" 2023, vol. 5(4); M. Ochojski, *Nowe technologie – pomoc w edukacji czy zagrożenie?*, „Kultura

i Wychowanie" 2024, t. 1(25); J. Oranga, *Benefits of artificial intelligence (ChatGPT) in education and learning: Is Chat GPT helpful. International Review of Practical Innovation*, „Technology and Green Energy" 2023, vol. 3(3); P. Plichta, *Sztuczna inteligencja, edukacja specjalna i nierówności (nie tylko cyfrowe)*, [w:] J. Pyżalski, A. Łuczyńska, *Sztuczna inteligencja. Prawdziwe zmiany w edukacji?*, Fundacja Szkoła z Klasą, Warszawa 2023; M. Rogalski, *Co to jest uczenie maszynowe – inteligentna analiza danych?*, https://www.gov.pl/web/popcwsparcie/co-to-jest-uczenie-maszynowe--inteligentna-analiza-danych (dostęp 13.01.2026); O. Staniszewski, *Chat GPT w Obliczu Prawa: Istota Prawnych Regulacji Chatów Sztucznej Inteligencji*, https://prawosportowe.pl/a/chat-gpt-w-obliczu-prawa-istota-prawnych-regulacji-chatow-sztucznej-inteligencji (dostęp 13.01.2026).

CYBERODPORNOŚĆ (ang. *cyber resilience*) to połączenie przedrostka „cyber" z rzeczownikiem „odporność". Przedrostek „cyber" wskazuje na coś, co jest powiązane z informatyką lub komputerem. W *Słowniku języka polskiego PWN* określany jest jako „pierwszy człon wyrazów złożonych wskazujący na ich związek z informatyką, zwłaszcza z internetem", a od około połowy XX w. stał się bardzo popularny w tworzeniu związków odnoszących się do wirtualnej rzeczywistości czy świata cyfrowego. „Odporność" zaś w odniesieniu do bezpieczeństwa oznacza rozwijanie i utrzymanie takich zdolności, które utrudnią nieprzyjazne działania. Pochodzi od łacińskiego słowa *resilire*, czyli „powrócić do poprzedniego kształtu" lub „odbić się". W odniesieniu do aktu o cyberodporności słowo to pojmowane jest jako niepodatność na niekorzystne czynniki zewnętrzne. Z kolei NATO definiuje odporność jako zmniejszenie podatności, czyli słabych stron państw, a także odtwarzanie własnych zdolności, które powstały poprzez wystąpienie zdarzeń związanych z szerokim wachlarzem zagrożeń w taki sposób, żeby można było szybko i sprawnie powrócić do normalnego funkcjonowania.

Istnieje wiele definicji cyberodporności. Jedna z nich wskazuje na kalkowanie angielskiego terminu *cyber resilience*, które oznacza zdolność jakichś systemów, organizacji, struktur do stawiania oporu wszelkim zagrożeniom w cyberprzestrzeni, a także przetrwania ich skutków i powrotu do sprawczości. Kolejna definicja mówi o cyberodporności jako zdolności sprostania wyzwaniom dla bezpieczeństwa związanym z transformacją cyfrową, która obejmuje m.in. wykrywanie i redukowanie

zagrożeń, reagowanie na niepożądane zdarzenia oraz realizację celów mimo zakłóceń celowych, przypadkowych, naturalnych, a także tych spowodowanych przez ludzi. ENISA (ang. European Union Agency for Cybersecurity) zaś wskazuje, że budowanie odporności cybernetycznej to ciągły proces doskonalenia, nawet w tych sektorach, gdzie występuje wysoki stopień dojrzałości. Z kolei Komisja Europejska definiuje cyberodporność nie tylko jako zdolność do przygotowania się na zagrożenia cybernetyczne, ale także stawiania im czoła, skutecznego radzenia sobie z nimi oraz dostosowywania się do bieżących zagrożeń. Światowe Forum Ekonomiczne zdefiniowało cyberodporność jako „zdolność systemów i organizacji do przetrwania zdarzeń cybernetycznych, mierzoną na podstawie połączenia średniego czasu awarii i średniego czasu odzyskania sprawności". Z kolei ISO (ang. International Organization for Standardization) definiuje cyberodporność jako zdolność organizacji do działania w obliczu cyberataku lub innego cyberincydentu, która obejmuje wdrożenie niezbędnych środków technicznych i organizacyjnych w celu wykrywania, reagowania i odzyskiwania stabilności po takich incydentach, a także adaptacji i wyciągania z nich wniosków w celu zwiększenia odporności w przyszłości. Inna definicja, zawarta w publikacji NIST (ang. National Institute of Standards and Technology) zakłada zaś, że jest to zdolność do przewidywania, wytrzymywania, odzyskiwania, ale i adaptacji do niekorzystnych warunków, ataków, obciążeń lub naruszeń systemów obejmujących zasoby cybernetyczne. Występuje tam również wskazanie, że definicję tę można zastosować m.in. do systemów, krajów, organizacji czy krytycznej infrastruktury w sektorze lub regionie.

W świetle tych definicji można przyjąć, że cyberodporność to wielowymiarowa zdolność, która obejmuje:

- zapobieganie, wykrywanie i reagowanie na incydenty;
- szybkie odtworzenie działania po incydencie;
- adaptację i uczenie się na przyszłość;
- utrzymanie funkcjonalności podczas zakłóceń, a także minimalizację ich skutków;
- ciągłe doskonalenie procesów;
- operacyjne podejście do odporności.

Mimo że definicje te pochodzą z różnych źródeł, wszystkie mają wspólne elementy, do których można zaliczyć przede wszystkim zdolność systemów/organizacji do funkcjonowania mimo zakłóceń, opis cyberodporności jako procesu obejmującego przewidywanie/wykrywanie zagrożeń, reagowanie, odtworzenie sprawności i adaptację po incydencie oraz traktowanie cyberodporności jako procesu, a nie stanu.

Na podstawie publikacji NIST wyróżnić można 4 cele cyberodporności:

- przewidywanie – prognozowanie zagrożeń i przygotowywanie się na nie poprzez planowanie, zapobieganie i unikanie ryzyka, a także ciągłe modyfikowanie systemu w celu utrudnienia ataków;
- wytrzymywanie – utrzymanie działania mimo wystąpienia zagrożeń m.in. poprzez przekierowywanie skutków ataku lub odłączenie uszkodzonych elementów;
- odzyskiwanie – przywrócenie stanu działania poprzez rekonstruowanie funkcji, odtworzenie wcześniejszych konfiguracji lub zastąpienie uszkodzonych komponentów;
- adaptacja – wyciąganie wniosków z incydentów i modyfikowanie systemów, procesów w celu przeciwdziałania przyszłym zagrożeniom.

Techniki cyberodporności stanowią zestaw praktyk wzmacniających zdolność systemów do reagowania, przetrwania i odzyskiwania sprawności w obliczu zagrożeń cybernetycznych. Opracowane m.in. przez NIST stanowią uniwersalne podejście do budowania cyberodporności i obejmują:

- świadomość kontekstową – celem jest zapewnienie aktualnej wiedzy o stanie misji i zasobów organizacji, uwzględniając zagrożenia;
- skoordynowaną ochronę – celem jest zapewnienie, że mechanizmy ochrony są skoordynowane i skuteczne, co przekłada się na utrudnienia w przeprowadzeniu ataku czy ryzyko wykrycia przeciwnika;
- wprowadzanie w błąd – celowe zmylenie przeciwnika lub ukrycie przed nim kluczowych zasobów. Powoduje dezorientację

i marnowanie zasobów atakującego, opóźnienie ataku i zwiększenie prawdopodobieństwa wykrycia jego działań i technik;
- różnorodność – celem jest ograniczenie ryzyka awarii lub skutecznych ataków poprzez zastosowanie różnorodnych rozwiązań;
- monitorowanie analityczne – celem jest maksymalizacja zdolności do wczesnego wykrywanie zagrożeń poprzez ciągłe monitorowanie właściwości systemu;
- reakcję adaptacyjną – celem jest zwiększenie zdolności do szybkiego reagowania na zagrożenia czy niekorzystne warunki. Działanie to ma umożliwić utrzymanie działania najważniejszych procesów, ograniczyć skutki ataków i zapobiegać destabilizacji systemu;
- dynamiczne pozycjonowanie – celem jest przemieszczanie zasobów i funkcji w czasie, aby zwiększyć odporność i utrudnić atak. Dynamiczne pozycjonowanie pomaga szybciej odzyskać sprawność po ataku, utrudnia zlokalizowanie zasobów przez atakującego i zwiększa szanse na jego wykrycie;
- brak trwałości – celem jest utrzymywanie zasobów na tyle długo, na ile są potrzebne, co skutkuje zmniejszeniem czasu ekspozycji na ataki, ograniczeniem możliwości rozprzestrzeniania się atakujących i utrudnienie im spowodowania uszkodzeń zasobów lub ich wykorzystania;
- ograniczenie uprawnień – celem jest zminimalizowanie ryzyka nadużyć poprzez kontrolę uprawnień użytkowników czy systemów;
- realokację – dostosowanie struktury systemów i sposobu wykorzystywania zasobów do zmieniającego się środowiska technicznego i zagrożeń w celu zmniejszenia ryzyka, powierzchni ataku czy ograniczenia powiązania między usługami;
- segmentację – proces izolowania poszczególnych elementów systemu według ich krytyczności i poziomu zaufania w celu ograniczenia rozprzestrzeniania się ataków i ich skutków, utrzymania zagrożenia tylko w wydzielonych obszarach, a także zmniejszenia liczby potencjalnych celi;

- uzasadnioną integralność – celem jest ustalenie, czy najważniejsze komponenty systemu nie zostały naruszone, co umożliwia wykrywanie prób zmodyfikowania danych, sprzętu czy oprogramowania i ich sfałszowania;
- redundancję – posiadanie kopii najważniejszych zasobów, co pozwala na zmniejszenie skutków utraty usług czy danych, ułatwia ich odzyskanie po ataku i skraca czas niedostępności różnych funkcji po ataku;
- nieprzewidywalność – celem jest wprowadzenie nieprzewidywalnych i losowych zmian w systemie, co utrudnia planowanie ataku i zwiększa niepewność atakującego.

W literaturze często pojawia się wiele terminów, które używane są zamiennie z pojęciem cyberodporności, lub też błędnie z nim utożsamianych. Wynika to z faktu, że wiele z nich odnosi się do pokrewnych obszarów, a mimo że są powiązane, nie oznaczają tego samego.

Pierwszym z takich terminów jest cyberbezpieczeństwo. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa stanowi, że cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 zaś stanowi, że „cyberbezpieczeństwo oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami". Uznać zatem należy, że cyberbezpieczeństwo dotyczy ochrony przed incydentami, a cyberodporność zakłada, że incydenty i tak się wydarzą; kładzie nacisk na zdolność działania mimo ich wystąpienia, odtworzenie i adaptację.

Benoît Dupont uważa, że istotne jest również rozróżnienie między cyberodpornością a zarządzaniem ryzykiem. Wskazuje, że cyberodporność obejmuje szerszy zakres i jest niezbędna, gdy nie jest możliwe przewidzenie czy obliczenie zagrożenia lub ryzyka. Zarządzanie ryzykiem zaś obejmuje

kwantyfikację prawdopodobieństwa ryzyka czy zagrożenia, co umożliwia podjęcie właściwej strategii co do radzenia sobie z nim.

Kolejnym terminem jest zarządzanie incydentami (ang. *incident response*). Niektórzy utożsamiają z nim cyberodporność, jednak pojęcie to jest znacznie szersze. Głównym celem zarządzania incydentami jest szybkie przywrócenie normalnego funkcjonowania usług po wystąpieniu incydentu, a także minimalizacja wpływu zakłóceń na działalność biznesową.

W zakresie cyberodporności istotnym aktem prawnym jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymogów w zakresie cyberbezpieczeństwa dla produktów z elementami cyfrowymi oraz zmieniające rozporządzenia (UE) nr 168/2013 i (UE) 2019/1020 oraz dyrektywę (UE) 2020/1828, znane jako ustawa o odporności cybernetycznej czy też ustawa o cyberodporności – Cyber Resilience Act (dalej: CRA). CRA jest pierwszym aktem prawnym UE, który systemowo wprowadzał obowiązek cyberodporności produktów cyfrowych. Ma on uzupełniać inne regulacje, m.in. Dyrektywę NIS 2, Akt o bezpieczeństwie cybernetycznym (Cybersecurity Act) i Akt o sztucznej inteligencji (AI Act).

CRA określa:

- zasady udostępniania na rynku produktów z elementami cyfrowymi w celu zapewnienia ich cyberbezpieczeństwa;
- podstawowe wymogi bezpieczeństwa cybernetycznego dotyczące projektowania, rozwoju i produkcji produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów w zakresie bezpieczeństwa cybernetycznego;
- podstawowe wymogi w zakresie cyberbezpieczeństwa dotyczące procesów obsługi luk w zabezpieczeniach wdrażanych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi w oczekiwanym czasie użytkowania produktów oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procesów;
- przepisy dotyczące nadzoru rynku, w tym monitorowania, oraz egzekwowania przepisów i wymogów, o których mowa w CRA.

Rozporządzenie ma na celu ochronę konsumentów i firm kupujących sprzęt lub oprogramowanie z komponentem cyfrowym. Wprowadza obowiązkowe wymogi w zakresie cyberbezpieczeństwa dla producentów i sprzedawców, które regulują projektowanie, rozwój i konserwację takich produktów. Dodatkowo nakłada na producentów obowiązek zapewnienia opieki podczas całego cyklu życia swoich produktów. Niektóre, które mają szczególne znaczenie dla cyberbezpieczeństwa, zanim zostaną wprowadzone do obrotu na rynek Unii Europejskiej, będą przechodziły zewnętrzną ocenę wykonywaną przez uprawniony organ. CRA opiera się na Strategii Cyberbezpieczeństwa UE z 2020 r. oraz Strategii Unii Bezpieczeństwa UE. Akt miał rozwiązać dwa główne problemy, jakimi są:

- niski poziom cyberbezpieczeństwa produktów z elementami cyfrowymi, który przejawia się w powszechnie występujących podatnościach oraz w niespójnym i niewystarczającym dostarczaniu aktualizacji zabezpieczeń w celu wyeliminowania tych podatności,
- niedostateczne zrozumienie i dostęp do informacji ze strony użytkowników, co uniemożliwia im wybór produktów o odpowiednich właściwościach w zakresie cyberbezpieczeństwa lub korzystanie z nich w bezpieczny sposób.

Produkty z elementami cyfrowymi, jakie obejmuje CRA, to m.in. laptopy, smartfony, inteligentne roboty, czujniki i kamery, urządzenia mobilne, routery, inteligentne głośniki, systemy sterowania przemysłowego, oprogramowanie takie jak gry video, aplikacje mobilne, systemy operacyjne czy oprogramowanie sprzętowe i komponenty (zarówno programowe, jak i sprzętowe), np. karty graficzne czy jednostki przetwarzania komputerowego. Warto podkreślić, że zgodnie z art. 2 rozporządzenia nie ma ono zastosowania m.in. do produktów z elementami cyfrowymi, do których stosuje się następujące akty prawne: rozporządzenie (UE) 2017/745, rozporządzenie (UE) 2017/746, rozporządzenie (UE) 2019/2144. Rozporządzenie nie ma również zastosowania do produktów zawierających elementy cyfrowe, które uzyskały certyfikację zgodnie z rozporządzeniem (UE) 2018/1139, a także do urządzeń objętych zakresem dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE.

CRA weszło w życie 10 grudnia 2024 r., a główne obowiązki nim wprowadzone zaczną obowiązywać 11 grudnia 2027 r. Obowiązki sprawozdawcze natomiast – 11 września 2026 r.

Akt prawny obejmujący tematykę cyberodporności to również Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Nowa dyrektywa, która zastąpiła pierwotną dyrektywę NIS, określa „wieloetapowe podejście do zgłaszania poważnych incydentów, aby zapewnić odpowiednią równowagę między szybkim zgłaszaniem, które pomaga zahamować potencjalne rozprzestrzenianie się poważnych incydentów i pozwala podmiotom kluczowym i ważnym zwrócić się o pomoc, a szczegółowym zgłaszaniem, które umożliwia wyciągnięcie cennych wniosków z poszczególnych incydentów i z czasem poprawia cyberodporność poszczególnych podmiotów i całych sektorów". Ustanawia również jednolite ramy prawne w celu utrzymania cyberbezpieczeństwa w 18 sektorach krytycznych w całej Unii Europejskiej, a także wzywa państwa członkowskie do określenia krajowych strategii cyberbezpieczeństwa i współpracy w Unii Europejskiej w zakresie transgranicznego reagowania i egzekwowania przepisów. W porównaniu z dyrektywą NIS 1, która obejmowała takie obszary, jak transport, energia, finanse, ochrona zdrowia, gospodarka wodna czy infrastruktura cyfrowa, nowe regulacje rozszerzają zakres podmiotów objętych przepisami. Obejmują teraz także dostawców publicznych usług łączności elektronicznej, szerszą grupę usług cyfrowych (np. platformy społecznościowe), usługi pocztowe i kurierskie, produkcję wyrobów o znaczeniu krytycznym, a także sektor kosmiczny.

Pod koniec 2020 r. Komisja zaproponowała zmianę NIS 1, co doprowadziło do przyjęcia NIS 2, który wszedł w życie w styczniu 2023 r., zaś NIS 1 uchylono z dniem 18 października 2024 r.

Lucyna Łowisz

H. Ciszek, A. Matulewska, *A case study of the productivity of the prefix cyber-in English and Greek legal languages*, „Studies in Logic, Grammar and Rhetoric" 2019, no. 58(1); *Cyber Resilience Act (CRA), Updates, Compliance*, https://www.european-cyber-resilience-act.com/ (dostęp 15.11.2025); *Cyber Resilience Act Requirements Standards Mapping*, Joint Research Centre & ENISA Joint Analysis, 2024; *Cyber Resilience Act*, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (dostęp 15.11.2025); *Developing cyber resilient systems: A systems security engineering approach*, „NIST Special Publication 800-160" 2019, no. 2(1); B. Dupont, *The cyber-resilience of financial institutions: significance and applicability*, „Journal of Cybersecurity" 2019, no. 5(1), https://doi.org/10.1093/cybsec/tyz013; *Dyrektywa NIS 2: zabezpieczenie sieci i systemów informatycznych*, https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive (dostęp 15.11.2025); Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.U. UE. L. 2022, nr 333, s. 80 z późn. zm.; A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, *Internet. Cyberodporność*, Wydawnictwo C.H. Beck, Warszawa 2025; *Handbook for Cyber Stress Tests*, 2025, https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests (dostęp 14.11.2025); *How tech giants are building cyber resilience*, https://www.iso.org/contents/news/2023/02/how-to-build-cyber-resilience.html (dostęp 14.11.2025); D. Kaźmierczak, *Odporność*, [w:] *Encyklopedia bezpieczeństwa*, t. 7, O. Wasiuta, S. Wasiuta (red.), Wydawnictwo Libron, Kraków 2024; V. Pulcini, *English Cyber – Words Across European Languages*, [w:] M. Szczyrbak, A. Tereszkiewicz, *Języki w kontakcie i kontraście: Księga pamiątkowa dla Profesor Elżbiety Mańczak-Wohlfeld z okazji Jej 70. urodzin*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2020; R. Rey, *Rządowe Centrum Bezpieczeństwa*, https://www.gov.pl/web/rcb/spoleczenstwo-odporne-na-zagrozenia (dostęp 14.11.2025); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. UE. L. 2019, nr 151, s. 15 z późn. zm.; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności), Dz.U. UE. L. 2024, poz. 2847 z późn. zm.; *Słownik języka polskiego PWN*, https://sjp.pwn.pl/slowniki/cyber-.html (dostęp 13.11.2025); S.C. Smith, *Toward a Scientific*

Definition of Cyber Resilience, 2023; Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz.U. 2023, poz. 913 z późn. zm.; *What is Cyber Resilience?*, https://www.digitalguardian.com/blog/what-cyber-resilience (dostęp 15.11.2025); *Zarządzanie incydentami*, https://symbioza.it/blog/slownik-pojec/zarzadzanie-incydentami/ (dostęp 15.11.2025).

CYBERPOPULIZM (populizm internetowy, populizm sieciowy, cyfrowy populizm) – zjawisko społeczno-polityczne oraz styl komunikacji polegający na wykorzystaniu środowiska komunikacji cyfrowej – w szczególności technologii informacyjnych i komunikacyjnych (Information and Communication Technologies, ICT), mediów społecznościowych, platform sieciowych oraz narzędzi mobilnych – do artykulacji, mobilizacji i wzmacniania przekazu populistycznego. Utożsamiany jest z komunikacją, która odwołuje się do „zwykłych ludzi" przeciwko „elitom" i jest prowadzona oraz wzmacniana za pomocą narzędzi cyfrowych. Przekaz populistyczny często przyjmuje formę spersonalizowaną, emocjonalną i narracyjnie uproszczoną, a istotnym jego komponentem są mechanizmy radykalizacji i polaryzacji. Cyberpopulizm bywa także interpretowany jako specyficzna orientacja technopolityczna, zakładająca instrumentalne wykorzystanie masowych, komercyjnych usług internetowych, pozostających pod kontrolą globalnych korporacji technologicznych, takich jak Meta/Facebook, Google czy X/Twitter. Pomimo strukturalnych ograniczeń tych platform –wynikających z ich kapitalistycznej logiki funkcjonowania, algorytmizacji przekazu oraz wysokiego stopnia koncentracji własności – są one postrzegane przez aktorów politycznych i cyfrowych aktywistów jako kluczowa arena rywalizacji politycznej.

Termin „cyberpopulizm" jest neologizmem złożonym z przedrostka „cyber" (od słowa „cybernetyka" (z języka greckiego *kybernetes* – sternik, zarządca) oraz rzeczownika „populizm" (z języka łacińskiego *populus* – lud, naród). W sensie semantycznym pojęcie to odnosi się do procesów sterowania, kierowania oraz mobilizowania „ludu" przy wykorzystaniu narzędzi i środowisk cyfrowych. „Lud" rozumiany jest tu nie jako zbiór jednostek, lecz wspólnota społeczna o charakterze solidarystycznym, scalona więziami emocjonalnymi, których podstawą mogą być wspólne

doświadczenia historyczne, poczucie marginalizacji bądź podobieństwo aktualnych warunków egzystencjalnych.

Cyberpopulizm pozostaje ściśle powiązany z klasycznym rozumieniem populizmu, definiowanym jako swoisty sposób komunikacji politycznej umożliwiający określonej zbiorowości artykulację roszczeń wobec systemu politycznego, który okazuje się na nie instytucjonalnie głuchy. Zjawisko to pojawia się wówczas, gdy rozproszone i tłumione potrzeby ludu, wywodzące się z różnych sfer życia społeczno-politycznego, zostają zintegrowane w ramach jednej platformy komunikacyjnej i podporządkowane wspólnej, nadrzędnej tożsamości zbiorowej. Istotę populizmu, a w konsekwencji także cyberpopulizmu, stanowi negacja, opozycyjność wobec istniejącego porządku politycznego, instytucji państwowych oraz dominujących elit. Mechanizm ten opiera się na mobilizowaniu uboższych warstw społecznych przeciwko istniejącemu porządkowi przy jednoczesnym silnym przywództwie, które sprawuje kontrolę nad kierunkiem i formą mobilizacji. Cyberpopulizm intensyfikuje te procesy poprzez powtarzalną, uproszczoną retorykę oraz wykorzystywanie symboli i emocjonalnych narracji służących polaryzacji społecznej i wzmacnianiu antagonizmu między „ludem" a „elitami" w przestrzeni cyfrowej.

Impulsem do wykształcenia się **cy**berpopulizmu był stopniowy i systematyczny wzrost znaczenia internetu oraz technologii ICT w sferze społeczno-politycznej. Obok tradycyjnych kanałów komunikacji i narzędzi marketingu politycznego nastąpiło stopniowe przenoszenie debaty publicznej do przestrzeni wirtualnej, która stała się jednym z głównych obszarów wymiany poglądów, sporów ideologicznych i mobilizacji społecznej. Nowe media oraz technologie cyfrowe zaczęły funkcjonować w polityce na podobnych zasadach jak w życiu codziennym, pełniąc przede wszystkim rolę narzędzi o charakterze praktycznym i użytkowym. Dlatego cyberpopulizm to dzisiaj przede wszystkim strategia polityczna oparta na wykorzystaniu nowych form zaangażowania społecznego oraz budowania poparcia dla przywództwa za pośrednictwem internetu. Dla aktorów populistycznych stanowi on szczególnie skuteczne narzędzie mobilizacji zwolenników, które nie tyle zastępuje, ile uzupełnia tradycyjne kanały komunikacji politycznej, takie jak media masowe czy struktury partyjne.

Źródeł populizmu, a we współczesnych warunkach także cyberpopulizmu, należy poszukiwać przede wszystkim w strukturze i dynamice społeczeństwa. Zjawisko to ujawnia się szczególnie wyraźnie w sytuacjach erozji tradycyjnych systemów wartości, osłabienia norm integrujących wspólnotę oraz w okresach gwałtownych przemian społeczno-ekonomicznych, które prowadzą do marginalizacji lub degradacji całych grup społecznych. Narasta wówczas poczucie niepewności, frustracji i wykluczenia oraz podatność na uproszczone narracje polityczne odwołujące się do emocji i poczucia krzywdy. Populizm adaptuje się w warunkach, w których tradycyjny system partyjny traci zdolność reprezentowania interesów obywateli. Partie polityczne postrzegane są wówczas jako niewydolne, skorumpowane oraz nieskuteczne w rozwiązywaniu konkretnych problemów społecznych i gospodarczych. Cyberpopulizm wzmacnia te tendencje, wykorzystując przestrzeń cyfrową jako alternatywny kanał komunikacji politycznej, omijający instytucjonalne pośrednictwo partii, mediów tradycyjnych i struktur państwowych. Media społecznościowe oraz platformy internetowe umożliwiają bezpośrednie zwracanie się do odbiorców, potęgując wrażenie autentyczności i bliskości między przywódcą a „ludem". W tym kontekście cyberpopulistyczny dyskurs charakteryzuje się wieloma cechami, które stanowią adaptację klasycznego populizmu do realiów komunikacji cyfrowej. Należą do nich m.in.:

- antyelitaryzm – polaryzacja i antagonizm – tworzenie narracji „my kontra oni"; niezadowolenie społeczne stanowi spoiwo dla aktywności ruchu, a w połączeniu z przekonaniem o nieomylności ludu jest punktem wyjścia dla kreowania dychotomicznego obrazu rzeczywistości i podziału świata na „nas" – uciskane ofiary, i „innych" – sprawujących władze, należących do „elit". Państwo, partie i inne siły polityczne są postrzegane jako czynniki destrukcyjne („kto nie jest z nami, jest przeciw nam"), a idealizowany lud jest ostoją podstawowych wartości, stąd częste wśród ruchów populistycznych odwoływanie się do sfery moralności i ocenianie swych adwersarzy w kategoriach etycznych;
- kreowanie stereotypu człowieka z ludu – prostego, zwykłego, religijnego, pracującego, i odrzucenie wzoru człowieka należącego

do jakichkolwiek elit intelektualnych. Lud uważany jest za jedyną zdrową moralnie część społeczeństwa, której interesy są niesłusznie pomijane, a nawet blokowane, upatruje się w nim źródła cnót i ogólnonarodowych wartości, wyrosłych z rodzimej kultury ludowej. Ideałem populistycznej wizji świata jest niewielka wspólnota oparta o zasady braterstwa i solidaryzmu;

– idea przywódcy – skrajna personalizacja polityki, w której liderzy populistyczni komunikują się bezpośrednio z elektoratem, budując obraz „autentycznego reprezentanta ludu". Przywódca stanowi spoiwo ruchu i uosabia wolę ludu oraz to, co w nim najcenniejsze, dlatego obdarzony jest łaską demagogicznego trybuna nawiązującego kontakt z ludem w celu natychmiastowego rozwiązania wszelkich dręczących go problemów. Taki populistyczny „ojciec narodu" istnieje tylko dzięki aprobowaniu go przez populistyczny lud, dlatego też schlebia ludowym masom, składając im nierealne obietnice dotyczące zwykle radykalnej poprawy warunków życia, w krótkim czasie i małym kosztem;
– antyinstytucjonalizm – przejawia się głównie w kwestionowaniu większości ustabilizowanych procedur i instytucji demokracji oraz niechęci do partii politycznych i innych instytucji pośredniczących w relacjach między ludem a władzą (mediów, ekspertów) – wszelkie instytucje państwowe uznawane są za komórki wrogie ludowi, a jedynym akceptowanym pośrednikiem i reprezentantem ludu może być charyzmatyczny lider;
– koncepcja „zmiany" rzeczywistości, w której funkcjonują niezadowolone grupy, postrzegana jako możliwość szybkiego wyjścia z obecnego zacofania i wejścia na drogę rozwoju społeczno-gospodarczego;
– prostota języka i rozwiązań – projektowanie zmiany odbywa się za pomocą charakterystycznego języka, który cechuje prostota i zwięzłość – łatwe rozwiązania podane są w nieskomplikowanej formie, np. „wszyscy politycy to złodzieje", „zburzyć i zbudować od nowa"; upraszczanie przekazu politycznego polega

na wykorzystaniu krótkich form, emocjonalnych komentarzy, memów itp.;
- nadmierny optymizm i utopia – stan, do którego chce doprowadzić populizm, ma być gwarancją powszechnego dobrobytu i wyrównania poziomu życia, a w szczególności spełnienie oczekiwań ludu;
- kategoria wroga publicznego – pozwala wskazać masom, dlaczego ich położenie jest tak złe, ukierunkować negatywne emocje na „kozła ofiarnego". W zależności od realiów danej przestrzeni politycznej są to np. mniejszości narodowe, imigranci czy też międzynarodowa finansjera, postrzegane stereotypowo lub też którym można nadać atrybuty siły zagrażającej reprezentowanej większości. Zakodowanie w świadomości ludu istnienia takiej grupy, instytucji lub zjawiska wzmacnia jego spójność, a przywódcom ruchu daje wygodne argumenty tłumaczące ewentualne niepowodzenia w realizacji planu zmian.

Wykorzystanie mediów cyfrowych w działalności populistycznej przyczyniło się do intensyfikacji i transformacji populizmu, wpływając zarówno na praktyki polityków, funkcjonowanie mediów oraz zachowanie obywateli. Cyberpopulizm stanowi zatem istotny element współczesnych demokracji, będąc zarówno produktem, jak i czynnikiem kształtującym cyfrową transformację sfery publicznej. Cechy populizmu napędzanego technologią to:

- bezpośrednia i szybka komunikacja z obywatelami – wykorzystywanie platform takich jak Facebook, YouTube, TikTok, X, aby komunikować się bezpośrednio z wyborcami, poza kontrolą dziennikarzy – pozwala to tworzyć narracje jednostronne, często emocjonalne lub uproszczone;
- wzmacnianie emocji i podziałów – algorytmy mediów społecznościowych premiują treści emocjonalne, kontrowersyjne i polaryzujące. Populizm cyfrowy celowo wykorzystuje ten mechanizm, aby eskalować konflikty społeczne i mobilizować poparcie;
- mikrotargetowanie i analiza danych – za pomocą danych użytkowników (np. preferencje, aktywność online) tworzy się

precyzyjne przekazy wyborcze kierowane do konkretnych grup odbiorców. Umożliwia to manipulowanie przekazem w zależności od odbiorcy – tzw. cyfrowy marketing polityczny;
- propaganda i dezinformacja – populizm cyfrowy często posługuje się fake newsami, deepfake'ami, zorganizowanymi sieciami botów i trolli, manipulacją obrazem i nagłówkami – to narzędzia, które łatwo i szybko rozchodzą się w sieciach społecznościowych;
- mobilizacja masowa w czasie rzeczywistym – platformy cyfrowe ułatwiają organizowanie realnych protestów, kampanii wyborczych czy ataków werbalnych na przeciwników politycznych, dzięki czemu populistyczni liderzy mogą szybko tworzyć wrażenie masowego poparcia;
- personalizacja „silnego przywódcy" – w mediach społecznościowych politycy budują wizerunek człowieka bliskiego ludziom, autentycznego, mówiącego „bezpośrednio i szczerze", co wzmacnia styl przywództwa charakterystyczny dla populizmu.

Z perspektywy dyskursu bezpieczeństwa cyberpopulizm, jak również sam populizm, bywa postrzegany jako zjawisko potencjalnie zagrażające bezpieczeństwu informacyjnemu oraz stabilności instytucjonalnej państwa. Wynika to z faktu, że sprzyja on rozpowszechnianiu dezinformacji i manipulacji informacyjnej, osłabia zaufanie do instytucji publicznych oraz autorytetów eksperckich, a także może przyczyniać się do wzrostu radykalizacji postaw społecznych. Przyczynia się do erozji zaufania publicznego, rozprzestrzeniania dezinformacji oraz osłabienia dyskusyjnego charakteru debaty publicznej. Wzmacnia bowiem logikę konfliktu i negacji, osłabia deliberacyjny model demokracji oraz sprzyja powstawaniu ruchów i partii opartych na szybkiej, emocjonalnej mobilizacji, często pozbawionych trwałych struktur organizacyjnych. Ponadto cyberpopulizm może stanowić narzędzie ingerencji podmiotów zewnętrznych w procesy polityczne oraz destabilizować debatę publiczną poprzez upowszechnianie teorii spiskowych, mowy nienawiści i fałszywych narracji.

Sabina Olszyk

J. Dzwończyk, *Populistyczne tendencje w społeczeństwie postsocjalistycznym (na przykładzie Polski)*, Wydawnictwo Adam Marszałek, Toruń 2000; P. Gerbaudo, *From Cyber-Autonomism to Cyber-Populism: An Ideological History of Digital Activism*, „tripleC" 2017, vol. 15, no. 2; P. Gerbaudo, *Populism 2.0: Social media activism, the generic Internet user and interactive direct democracy*, [w:] *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*, C. Fuchs, D. Trottier (eds.), Taylor and Francis, London 2024; P. Gerbaudo, *Social media and populism: an elective affinity?*, „Media, Culture & Society" 2018, vol. 40, no. 5, https://doi.org/10.1177/0163443718772192 (dostęp 9.12.2025); M. Marczewska-Rytko, *Populizm. Teoria i praktyka polityczna*, Wydawnictwo UMCS, Lublin 1995; S. Olszyk, *Populizm w kontekście współczesnej formy demokracji na przykładzie wyborów parlamentarnych w Polsce w latach 2001 i 2005*, „Studia Humanistyczne" 2007, t. 5, https://journals.bg.agh.edu.pl/STUDIA/2007/SH_2007_05.pdf (dostęp 9.12.2025); S. Olszyk, *Vox populi vox Dei. Teoria populizmu politycznego*, „Annales Academiae Paedagogicae Cracoviensis, folia 46. Studia Politologica III" 2007, https://rep.up.krakow.pl/xmlui/bitstream/handle/11716/7251/AF046--19--Vox-populi--Olszyk.pdf?sequence=1&isAllowed=y (dostęp 9.12.2025).

CYBERUTOPIZM (ang. *cyber-utopianism; cyber-utopism)* – przekonanie, że technologie cyfrowe, zwłaszcza internet, mają wrodzoną zdolność do rozwiązywania problemów społecznych, politycznych i ekonomicznych, prowadząc niemal automatycznie do demokracji, wolności, równości i postępu. W ujęciu badawczym jest to naiwny lub nadmiernie optymistyczny technologiczny idealizm, ignorujący realny kontekst, taki jak władza, instytucje, kultura, nierówności, nadzór i interesy polityczne. Współczesne rozważania dotyczące utopii technologicznej można traktować jako część szerszego nurtu poświęconego utopii społecznej, wpisując ją w perspektywę techno-ewolucyjną.

Termin cyberutopizm został spopularyzowany przez białoruskiego pisarza, naukowca i badacza mediów Jewgienija Morozowa (Evgeny'ego Morozova), mieszkającego w USA, który użył go w książce z 2011 r. *The Net Delusion: The Dark Side of Internet Freedom* (polskie wydanie: *Sieć złudzeń: Ciemna strona wolności w internecie*). Autor ukuł ten termin, krytykując teorie cyberutopistów wierzących, że technologia wzmacnia ludzi i umożliwia im zjednoczenie w opozycji wobec autorytarnych rządów. Zarzucał im, że nie dostrzegają ciemnych stron internetu i jego wpływu na wszystkie

dziedziny życia politycznego, a nie tylko te sprzyjające demokratyzacji. Mianem cyberutopii określał naiwną wiarę w emancypacyjny charakter komunikacji online i przekonanie, że internet faworyzuje uciskanych, a nie ciemiężców.

Morozow twierdził, że poglądy takie wywodzą się z cyfrowego zapału lat 90., kiedy to byli hipisi, już zadomowieni na prestiżowych uniwersytetach, wdali się w spór, chcąc udowodnić, że internet może zwiększyć uczestnictwo w demokracji, zapoczątkować renesans podupadających społeczności i wzmocnić życie stowarzyszeniowe. Cyberutopiści nie przewidzieli jednak, jak użyteczny okaże się internet dla propagandy, inwigilacji i cenzury. Ich populistyczne wizje przesłoniły im liczne możliwości i coraz bardziej wyrafinowane sposoby wykorzystywane w państwach autorytarnych przez dyktatorów nietolerujących rządów prawa ani odmiennych poglądów.

Morozow, niegdyś sam zafascynowany cyberutopią, jako młody idealista pragnący zmienić świat, obecnie przestrzega przed tą zgubną ideologią. Obserwując pogarszanie się sytuacji w zakresie swobód demokratycznych w rodzinnej Białorusi, zainteresował się zachodnią organizacją pozarządową, która dążyła do promowania demokracji i reformy mediów w byłym bloku sowieckim za pomocą internetu. Blogi, portale społecznościowe i działalność aktywistów w sieci na dłuższą metę okazały się jednak niewystarczające, a dodatkowo rządy, którym chciano się przeciwstawić, zaczęły eksperymentować z cenzurą i agresywnie angażować się w nowe media (opłacanie blogerów za rozsiewanie fałszywych informacji, trollowanie portali społecznościowych w poszukiwaniu informacji o opozycji). Władze wykorzystywały sieć zarówno jako marchewkę (zapewniającą rozrywkę obywatelom), jak i kij (karząc tych, którzy kwestionowali oficjalną linię rządzących). Analiza ta uświadomiła Morozowi, że należy nie tylko oczyścić się z cyberutopijnych uprzedzeń, ale także przygotować się na to, że internet w sposób nieunikniony zyskuje coraz większą rolę w polityce zarówno państw autorytarnych, jak i demokratycznych, i że w wielu sytuacjach wzmacnia on silnych i osłabia słabych.

Badacz ten ujawnia również błędność podejścia nazwanego przez niego „internetocentryzmem", które w przeciwieństwie do cyberutopizmu nie jest zbiorem przekonań, lecz raczej filozofią działania wpływającą na

sposób podejmowania decyzji. Podczas gdy cyberutopizm określa, co należy zrobić w celu promocji demokracji, internetocentryzm wskazuje, jak to powinno być zrobione, przy czym każdą zmianę najpierw przeformułowuje w kategoriach internetu, a nie kontekstu, w jakim powinna nastąpić. Większość utopistów to internetocentryści, ci drudzy zaś niekoniecznie są utopistami; część z nich widzi siebie wręcz jako pragmatyków, którzy porzucili utopię dla realistycznych przekonań. Jednak rzadko rekompensuje to ich wadliwą metodologię, która przedkłada narzędzie nad środowisko. Grupę tę charakteryzuje całkowita nieświadomość politycznego charakteru technologii, aroganckie przekonanie, że mają internet po swojej stronie, oraz fałszywe założenie, że jego „logika" ukształtuje każde środowisko, do którego przenika, a nie odwrotnie, oraz ignorowanie społecznych, kulturowych i politycznych subtelności.

Aby zatroszczyć się o przyszłość demokracji, zdaniem Morozowa, należy porzucić zarówno cyberutopizm, jak i internetocentryzm, a zamiast tego postawić na politykę opartą na realistycznej ocenie ryzyka i zagrożeń stwarzanych przez internet, w połączeniu z bardzo skrupulatną i bezstronną analizą jego możliwości oraz działaniami uwzględniającymi lokalny kontekst i powiązania między siecią a polityką zagraniczną oraz uwarunkowaniami geopolitycznymi. Trzeba też oprzeć się pokusie bezkrytycznego użycia narzędzi technologicznych, wynikającej z coraz niższych kosztów i łatwości ich wdrożenia. Rozwiązania techniczne zwalczają objawy, a nie przyczyny, dlatego skutki uboczne mogą być gorsze niż sam problem. Przykładowo, założenie portalu społecznościowego w autorytarnym kraju może dawać korzyści typu szybka i sprawna komunikacja oraz organizowanie się opozycjonistów, ale stwarza ryzyko gromadzenia danych osobowych wszystkich dysydentów na jednej platformie i ujawnienia powiązań między nimi.

Warto również zdawać sobie sprawę, że ci, którzy głoszą, że najbardziej palące problemy wolności internetu można rozwiązać, przełamując wiele zapór sieciowych, równocześnie opracowują i sprzedają technologie potrzebne do ich przełamania. Kiedy zawodzą jedne rozwiązania technologiczne, proponują kolejne, bardziej zaawansowane narzędzia, wymagające kolejnego finansowania, by naprawić problem – co często generuje następne problemy i koszty, a w ten sposób „gaszenie ognia

ogniem" nigdy się nie kończy. Ponadto przedstawianie istotnych kwestii społecznych jako zestawu problemów technologicznych odciąga uwagę decydentów od wyzwań, które nie są technologiczne z natury i których nie da się w ten sposób redefiniować. Przykładowo, choć media podkreślają rolę telefonów komórkowych w rozwoju gospodarczym Afryki, decydenci nie mogą zapominać, że same innowacje nie zwalczą wszechobecnej korupcji, co unaoczniają kenijscy policjanci, którzy zaczęli żądać łapówek przez mobilne przelewy (łatwiejsze do ukrycia niż gotówka). Zachwyt nad „genialnością" rozwiązań technologicznych łatwo odrywa od realiów, prowadząc do traktowania technologii jako panaceum, co trafnie skwitował Cedric Price pytaniem: „Technologia jest odpowiedzią, ale jakie było pytanie?".

Promocja technologii dla samej technologii to, w postrzeganiu Morozowa, skrajny fetyszyzm technologiczny, pomijający kontekst socjokulturowy, instytucjonalny, organizacyjny czy ustrojowy. Przytłacza on nawet osoby posiadające wiedzę historyczną, społeczną i polityczną. To również gloryfikowanie technicznej, w dużej mierze ilościowej, wiedzy eksperckiej kosztem erudycji, przed czym przestrzegała już w latach 60. amerykańska intelektualistka Hannah Arendt. Takie podejście uniemożliwia racjonalną i kompleksową dyskusję na temat pierwotnych przyczyn problemu, nakłaniając do zajmowania się widocznymi i nieistotnymi objawami, które można byłoby wyleczyć tanim kosztem. Jak w przypadku walki zachodnich rządów i fundacji z cenzurą internetu stosowaną przez autorytarne rządy, polegającą na finansowaniu i promowaniu technologii, które pomagają ją obejść, zamiast pochylenia się nad podstawowymi przyczynami, które najczęściej wiążą się z nadmiernymi ograniczeniami nakładanymi przez rządy na wolność słowa. Dodać należy, że właściwa diagnoza czasem uświadomiłaby decydentom, że niektóre problemy są po prostu nierozwiązywalne; np. „wojna z autorytaryzmem", „wojna o wolność internetu" czy „wojna z terroryzmem" to terminologia nie tylko maskująca prawdziwą naturę wielu problemów i ukrywająca liczne, złożone powiązania między nimi, ale także błędnie sugerująca, że taką wojnę można wygrać, jeśli zmobilizuje się wystarczające zasoby. W rzeczywistości zwalczając jeden z filarów tzw. informacyjnej trójcy autorytaryzmu – propagandy, cenzury i inwigilacji – można w efekcie

wzmocnić dwa pozostałe, podczas gdy działając na mniejszą skalę i zachowując świadomość złożoności realnego świata, zwiększa się szansę, by przewidywać i łagodzić niezamierzone konsekwencje.

W myśl cyberutopizmu internet miał przełamać państwowy monopol informacyjny i zapewnić obywatelom otwartą platformę demokratyczną. Pionowe relacje władzy, pełniącej funkcję strażnika mediów, miały ustąpić miejsca horyzontalnym społecznościom. Wzrost liczby obywatelskich platform dyskusyjnych postrzegano jako pogłębianie i poszerzanie demokracji, a internet miał stworzyć idealne warunki dla wolnej demokracji deliberatywnej. Rzeczywiście, dzięki nowym kanałom informacyjnym media głównego nurtu nie mogły już ukrywać niewygodnych faktów ani tłumić głosów sprzeciwu. Represyjne rządy traciły możliwość zaprzeczania informacjom o nadużyciach władzy. Skorumpowani politycy stawali się bardziej podatni na odpowiedzialność, a ich kłamstwa były łatwiej demaskowane. Internet sprzyjał rozwojowi społeczeństwa obywatelskiego, umożliwiał aktywizm i udział w życiu politycznym mniejszościom, organizacjom pozarządowym i dysydentom, ułatwiał prowadzenie różnorodnych debat oraz łączenie się grup i tworzenie nowych społeczności wśród osób o podobnych poglądach, niezależnie od miejsca pobytu.

Mimo tych osiągnięć narracja pełna wiary w możliwość obalenia autokratycznych reżimów dzięki internetowi pomijała drugą stronę medalu. Takie podejście dominowało jeszcze w pierwszej dekadzie XXI w., ale stopniowo zaczęło tracić na znaczeniu. Przyczyniły się do tego m.in. liczne kampanie internetowe i coraz bardziej wyrafinowana, ukierunkowana reklama polityczna (np. głośna sprawa Cambridge Analytica). Coraz częściej podkreślano zagrożenia związane z internetem, także w środowiskach, które miały sprzyjać demokracji, jak wspomniane horyzontalne społeczności. Zauważono, że zamiast – lub obok – ideałów świadomej dyskusji obywatelskiej opartej na dialogu pojawiły się polaryzacja, mowa nienawiści, trolling i teorie spiskowe. Obecnie wiele aspektów internetu, takich jak hakowanie, wojna informacyjna czy dominacja platform internetowych (np. Facebook, Twitter), postrzega się raczej jako zagrożenie aniżeli narzędzie wsparcia demokracji. Swobodnemu dostępowi do informacji towarzyszą obawy przed dezinformacją, cenzurą, teoriami spiskowymi

i hejtem. Nadmierny technooptymizm ustępuje miejsca technofobii, przy czym oba podejścia wymagają krytycznej refleksji.

Zwraca się również uwagę na regres praw człowieka po okresie długotrwałego postępu w tej dziedzinie. Zjawisko to jest szczególnie widoczne w przestrzeniach cyfrowych, które niegdyś postrzegano jako bastiony nowej ery praw człowieka. Obecnie badacze wskazują, że te przestrzenie mogą podważać autonomię, empatię i godność człowieka. Nowa rzeczywistość technologiczna nie tylko nie sprzyja rozwojowi dyskursu o prawach człowieka, lecz wręcz go podważa, naruszając fundamentalne prawa w wielu krajach. Wszechobecne gromadzenie danych i postęp algorytmiczny, choć służą zwiększeniu wydajności i łączności, stanowią wyzwanie dla anonimowości, prywatności i bezpieczeństwa. Przykładowo, fizyczny ruch urządzenia w pobliżu osoby może ujawnić jej obecność w miejscu popełnienia przestępstwa lub pozwolić na identyfikację uczestników protestu, a skutki dla bezpieczeństwa publicznego mogą być zróżnicowane.

Innym przykładem są urządzenia mobilne wykorzystywane jako pomoce nawigacyjne wspierające kierowców lub podróżnych w przemieszczaniu się między miejscami docelowymi. Dostarczają one danych dotyczących m.in. zainteresowań użytkowników podczas postojów w sklepach lub na stacjach benzynowych, prędkości poruszania się czy wzorców ruchu. Pasywne gromadzenie informacji obejmuje urządzenia noszone, dane telemetryczne w przestrzeniach publicznych oraz wykorzystanie protokołów Bluetooth. Mechanizmy te zwiększają wydajność użytkowników i efektywność biznesową, a także ułatwiają sprzedaż reklam, jednocześnie ograniczając autonomię osób dostarczających danych i wpływając na ich zachowania.

Aplikacje do kierowania ruchem wyświetlają reklamy pobliskich sklepów, gdy zmieniają trasę użytkownika, aby uniknąć korków, i dostarczają firmom ubezpieczeniowym informacji do dostosowania stawek polis. Choć technologie te pochodzą głównie z sektora prywatnego, rządy coraz częściej wykorzystują dane telemetryczne do nadzoru i kontroli społecznej. W rezultacie sieciowe technologie, zamiast wspierać emancypację, przyczyniają się do ograniczenia wolności, inwigilacji, cenzury i kontroli, zmieniając interakcje między jednostkami, rządami i firmami oraz stwarzając zależności, które mogą szkodzić bezpieczeństwu człowieka

poprzez ograniczenie jego autonomii. Dostęp do praw, takich jak prywatność, wolność słowa czy anonimowość, staje się warunkowy – zależny od płatności, polityki firm lub pozornej zgody użytkownika. Technologie cyfrowe nie uwzględniają empatii, która pozwalała kiedyś na respektowanie niezależności innych osób. Przeniesienie komunikacji i relacji międzyludzkich do sfery całkowicie kontrolowanej przez algorytmy i firmy (lub państwa) sprzyja dehumanizacji – relacje tracą autentyczny i osobisty wymiar, stając się zredukowane do danych, profili i statystyk, co podważa godność użytkowników.

W rozważaniach nad cyberutopią nie sposób pominąć roli coraz bardziej znaczącej sztucznej inteligencji (SI, ang. Artificial Intelligence). Można ją analizować dwojako: jako rozwiązanie techniczne oraz wpływ artefaktów SI na człowieka. W pierwszym przypadku problem dotyczy stworzenia maszyn, które funkcjonują w pewnym stopniu niezależnie od ludzkiej kontroli, w drugim – budowy systemów wspierających lub zastępujących ludzką sprawczość, szczególnie w obszarach obliczeń, selekcji i interpretacji dużych zbiorów danych. W obu wariantach SI stanowi narzędzie do tworzenia utopijnej wizji „lepszego" świata. Jednak i tu pojawia się niebezpieczeństwo, że technoutopia, mająca na celu poprawę jakości życia człowieka, przekształci się w dystopię. Rodzą się obawy związane z potencjalnymi negatywnymi konsekwencjami wykorzystania SI w nadziei na zwiększenie efektywności działań jednostek, grup i instytucji. Oprócz możliwej utraty kontroli nad robotami czy systemami informatycznymi należy uwzględnić ryzyko użycia SI jako narzędzia kontroli jednej grupy nad drugą.

Wyimaginowana struktura SI opiera się na znanych wartościach, takich jak bezpieczeństwo, skuteczność, gromadzenie wiedzy, postęp, łatwy dostęp do informacji oraz zdolność do poprawy jakości życia. Jednak wdrażanie tych wartości w połączeniu z SI może prowadzić do utraty indywidualności i ograniczenia możliwości decydowania o sobie. Współczesne technoutopie nie wymagają już środków zewnętrznej opresji, opierając się na systemach kontroli użytkowników narzędzi cyfrowych, sugerując najlepsze rozwiązania, optymalizując działania i umożliwiając nadzór nad nimi. Zasoby dostępne dużym korporacjom, np. Microsoftowi, Google czy

Facebookowi, pozwalają finansować takie systemy, które z czasem mogą stać się niezbędne w funkcjonowaniu kluczowych instytucji.

Niezależnie od tego, czy SI postrzegana jest głównie jako zagrożenie, czy jako źródło nowych możliwości, dalsze prace nad jej rozwojem i relacją z człowiekiem są nieuniknione. Konieczne jest określenie etycznych i prawnych granic tworzenia SI, przy uwzględnieniu dobrobytu zarówno jednostek, jak i ludzkości jako całości. Działając w imię poprawy jakości życia w wymiarze ekonomicznym, politycznym, medycznym i naukowym, należy zachować równowagę między człowiekiem a SI. Niektóre propozycje, np. szwedzkiego filozofa i profesora Uniwersytetu Oxfordzkiego Nicka Bostroma, zakładają przekazywanie wartości poprzez projektowanie instytucji integrujących człowieka i SI. Takie podejście może być jednak niebezpieczne – instytucjonalny, inteligentny system wartości może nie uwzględniać odrębności i niezależności jednostki, koncentrując się raczej na pracy zespołowej i kolektywnym działaniu. W konsekwencji może to prowadzić do wzorców przypominających instytucje totalitarne i patologie inteligencji zbiorowej, co mogłoby być ilustracją potencjalnej technodystopii.

Dynamiczny rozwój technologii sprawia, że relacja człowiek–SI staje się jednym z kluczowych zagadnień współczesności, wymagającym nieustannych badań i regulacji prawnych na całym świecie. Również w Europie podejmuje się takie działania. W 2017 r. Rezolucja Zgromadzenia Parlamentarnego Rady Europy zwróciła uwagę na ryzyko zastąpienia demokratycznych reguł przez → cyfrowy autorytaryzm. Podobne ramy prawne i etyczne buduje Unia Europejska, m.in. w zakresie wykorzystania technologii cyfrowych w życiu społecznym, zarządzania danymi osobowymi oraz wdrażania SI. Projekt regulacji SI poprzedziły publikacja białej księgi przez Komisję Europejską, publiczne konsultacje i wiele rezolucji Parlamentu Europejskiego dotyczących etycznego stosowania SI oraz odpowiedzialności z nią związanej. Kompleksowy projekt aktu prawnego został przedstawiony przez Komisję w 2021 r., a w 2024 r. przyjęto nowe prawo. W międzyczasie, w 2022 r. firma OpenAI udostępniła ChatGPT, który szybko zyskał popularność, stając się również źródłem kontrowersji, a jego upowszechnienie przyspieszyło prace nad prawnymi ramami, by zapewnić przejrzystość i bezpieczeństwo stosowania nowych technologii

oraz minimalizowanie ich potencjalnych negatywnych skutków. Podejście pragmatyczne, oparte na analizie ryzyka, uwzględnia korzyści społeczno-ekonomiczne SI, ale równocześnie wskazuje na nieprzewidywalne zagrożenia, które mogą dotyczyć zarówno pojedynczych osób, jak i całych społeczeństw. Zidentyfikowane ryzyka powinny podlegać regulacjom, a w przypadku nadużyć – zakazom, zwłaszcza gdy SI służy manipulacji, kontroli społecznej lub praktykom sprzecznym z wartościami UE, takimi jak godność człowieka, wolność, równość, demokracja, praworządność, ochrona danych, prywatność czy prawa dziecka.

Wydaje się zatem, że zarówno cyberutopizm, jak i technologiczna dystopia stały się koncepcjami przestarzałymi. Obecnie dominuje postrzeganie nowych technologii jako źródła zarówno pozytywnych, jak i negatywnych możliwości. Trend ten widoczny jest nie tylko w mediach i regulacjach prawnych, lecz także w literaturze naukowej, gdzie coraz częściej mówi się o spektrum postaw – od utopijnej nadziei, przez krytycyzm i pragmatyzm, po wizje dystopijne. Proste podziały (technologia jako szansa kontra zagrożenie) tracą aktualność; przeważa podejście złożone i ambiwalentne, co potwierdzają badania implikujące współwystępowanie zaufania i obaw respondentów wobec rozwoju technologii.

Małgorzata Bereźnicka

A. Brantley, *Utopia Lost – Human Rights in a Digital World*, „Applied Cybersecurity & Internet Governance" 2022, vol. 1, no. 1, 10.5604/01.3001.0016.1238; A. Jaskiernia, *Pluralizm, transparentność i odpowiedzialność. Nowe regulacje Unii Europejskiej w obszarze mediów i technologii cyfrowych*, „Studia Medioznawcze" 2024, t. 25, nr 1(96); P.E. Korvela, *From Utopia to Dystopia: Will the Internet Save or Destroy Democracy?*, „Redescriptions: Political Thought, Conceptual History and Feminist Theory" 2021, vol. 24, no. 1, 10.33134/rds.352; E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs, USA 2011; Y.L. Ng, Z. Lin, *Between Technological Utopia and Dystopia: Online Expression of Compulsory Use of Surveillance Technology*, „Science and Engineering Ethics" 2024, vol. 30, no. 1, https://doi.org/10.1007/s11948-024-00483-3; M. Wojewoda, *Sztuczna inteligencja jako utopia społeczna*, „Ethos. Kwartalnik Instytutu JP II KUL" 2023, t. 36, nr 3(143), https://doi.org/10.12887/36-2023-3-143-08.

CYFROWA OSOBA – byt funkcjonujący w środowisku cyfrowym lub hybrydowym (byt wirtualny), który posiada tożsamość cyfrową, wykonuje działania lub reprezentuje podmiot fizyczny bądź wirtualny, a także wchodzi w relacje społeczne, ekonomiczne lub prawne analogiczne do człowieka. Termin obejmuje zarówno cyfrowe odwzorowanie osoby fizycznej (np. *digital persona*, cyfrowy obywatel), jak i autonomiczne lub półautonomiczne byty cyfrowe (np. elektroniczna osobowość, *digital human*/*virtual human*, cyfrowy pracownik, cyfrowy człowiek). Warianty te różnią się stopniem autonomii, agencji, reprezentacji prawnej oraz technologicznego zaplecza, jednak ich wspólną cechą jest funkcjonowanie tożsamościowe i operacyjne w świecie cyfrowym.

Analiza współczesnej literatury dotyczącej podmiotowości cyfrowej, algorytmicznego zarządzania i tożsamości w społeczeństwie informacyjnym pozwala wyjaśnić zmienne i zależne od perspektywy badawczej rozumienie tego wielowymiarowego zjawiska obejmującego szeroki zbiór rozwiązań technologicznych.

I tak, w ujęciu klasycznym, teoretycznym (Floridi, Clemons) cyfrowa osoba jest bytem posiadającym tożsamość cyfrową, czyli zestaw danych pozwalających na unikalną identyfikację osoby fizycznej (lub prawnej) w środowisku cyfrowym. Znana również jako byt cyfrowy, może zawierać takie dane, jak imię i nazwisko, numer PESEL, dane biometryczne oraz mechanizm uwierzytelniania (np. kwalifikowany certyfikat, login i hasło lub krajowe rozwiązanie eID).

Tożsamości cyfrowe mogą być podzielone na kilka rodzajów, w zależności od ich zastosowania i charakteru. W ramach europejskich ram tożsamości cyfrowej wyróżnia się następujące ich rodzaje:

- tożsamość cyfrowa osób fizycznych: rodzaj tożsamości cyfrowej przypisany do konkretnych osób fizycznych, umożliwiający potwierdzanie tożsamości i uzyskanie dostępu do usług publicznych i prywatnych. Dzięki niej użytkownicy mogą logować się do systemów administracji publicznej, korzystać z usług zdrowotnych, bankowych oraz innych online, bez konieczności fizycznej obecności;
- tożsamość cyfrowa przedsiębiorstw: rodzaj tożsamości cyfrowej przypisany do konkretnych przedsiębiorstw umożliwiający

bezpieczne transakcje elektroniczne i uzyskanie dostępu do usług online. Przedsiębiorstwa mogą dzięki niej podpisywać dokumenty elektroniczne, składać wnioski w urzędach, a także prowadzić działalność gospodarczą w sposób zdalny i bezpieczny;
- tożsamość cyfrowa urządzeń: przypisana do konkretnych sprzętów, takich jak komputery, smartfony czy inne urządzenia IoT umożliwiająca bezpieczne połączenia i uzyskanie dostępu do sieci. Dzięki temu urządzenia mogą komunikować się między sobą oraz z systemami centralnymi w sposób bezpieczny i zaufany.

Wszystkie te rodzaje tożsamości cyfrowych są objęte wprowadzonym przez UE w 2014 r. rozporządzeniem eIDAS (Electronic Identification, Authentication and Trust Services), które reguluje transakcje elektroniczne i usługi zaufania w państwach członkowskich.

Polska od lat rozwija cyfrową tożsamość, wdrażając rozwiązania zgodne z europejskimi regulacjami i wytycznymi. Obecnie korzystamy z kilku kluczowych narzędzi, które wpisują się w ramy unijne:

- profil zaufany to najczęściej wykorzystywany środek identyfikacji elektronicznej umożliwiający obywatelom logowanie się do systemów administracji publicznej, takich jak ePUAP, ZUS czy CEIDG;
- mObywatel to mobilna aplikacja rządowa, która zapewnia dostęp do cyfrowego dowodu osobistego, e-recept, legitymacji i innych dokumentów – stale rozwijana i popularyzowana wśród użytkowników;
- podpis kwalifikowany, zgodny z rozporządzeniem eIDAS, jest szeroko stosowany zarówno w sektorze publicznym, jak i prywatnym, szczególnie w kontekście podpisywania dokumentów elektronicznych o mocy prawnej;
- krajowy portfel tożsamości cyfrowej jest obecnie w fazie projektowania i rozwoju, z założeniem pełnej zgodności z unijną koncepcją Europejskiego Portfela Tożsamości Cyfrowej (EUDI Wallet).

W tym klasycznym, używanym najczęściej znaczeniu chodzi albo o cyfrowego obywatela (*digital citizen*), czyli osobę fizyczną, która m.in. uczestniczy w życiu społecznym, politycznym i informacyjnym za pośrednictwem narzędzi cyfrowych i ma kompetencje cyfrowe umożliwiające świadome funkcjonowanie w infosferze (cyfrowy obywatel = człowiek jako uczestnik społeczeństwa informacyjnego; podmiot jest człowiekiem i ma status prawny), albo o *digital persona* (termin ustanowiony przez Rogera Clarke'a), która oznacza cyfrową reprezentację jednostki – model danych skonstruowany przez systemy informacyjne na podstawie jej aktywności (*digital persona* jest modelem informacyjnym, elementem funkcjonowania cyfrowego obywatela, lecz nie stanowi osoby w sensie prawnym ani społecznym).

Jak wskazuje E. K. Clemons (2024), współczesna aktywność w sieci prowadzi do powstania wielowarstwowych „person online", które oddziałują na postrzeganie podmiotu zarówno przez użytkowników, jak i instytucje. W procesach cyfrowych cyfrowa persona nierzadko funkcjonuje samodzielnie, pozostając aktywnym elementem relacji społecznych i ekonomicznych, a tym samym nabierając cech quasipodmiotowych. Dlaczego quasi? Bo cyfrowa osoba nie ma świadomości (brak intencji, odczuwania, refleksji), zdolności moralnej (nie jest odpowiedzialna etycznie) ani prawnej, a jej działanie jest zawsze pochodne (wynika z danych, projektowania, algorytmów). W tym sensie cyfrowa osoba stanowi zarówno reprezentację, jak i instrument działania w środowisku cyfrowym.

Z biegiem czasu koncepcja ta uległa poszerzeniu. W literaturze wskazuje się, że cyfrowa osoba nie musi odnosić się wyłącznie do człowieka – może nią być także autonomiczny system techniczny. Raport RAND Corporation (2025) podkreśla, że *digital personhood* obejmuje zarówno cyfrową reprezentację człowieka (np. tożsamość elektroniczna, profile, cyfrowe dowody tożsamości), jak i bardziej zaawansowane formy, tj. cyfrowe bliźniaki (*digital twins*) oraz wirtualne lub syntetyczne osoby (np. agenci AI, awatary, systemy autonomiczne), których technologiczne podłoże stanowią m.in. systemy identyfikacji i zarządzania tożsamością (ICAM), sztuczna inteligencja, big data, IoT. W tym znaczeniu cyfrowa osoba ma operacyjną sprawczość (agencję operacyjną) – staje się aktorem środowiska cyfrowego, zdolnym do prowadzenia dialogu, realizowania zadań,

podejmowania decyzji i uczenia się na podstawie interakcji (wykonuje czynności, które coś zmieniają w środowisku, mają realne skutki).

Przykładem są tu modele *digital human*/*virtual human*, czyli zaawansowane awatary zdolne do komunikacji, wykorzystywane w edukacji, obsłudze klienta i administracji publicznej. Pełnią rolę interfejsu między użytkownikiem a systemem, często imitując ekspresję, emocje i zachowania ludzkie. Szczególnym rozwinięciem tej idei jest cyfrowy pracownik i cyfrowy człowiek w modelu D-HaaS (Digital Human as a Service), będący usługowym komponentem środowiska cyfrowego realizującym autonomiczne czynności w imieniu podmiotu lub organizacji. Modele te funkcjonują jako pracownicy wirtualni, interfejsy komunikacyjne lub cyfrowe reprezentacje jednostek w systemach administracyjnych. Ich agencja operacyjna jest największa i choć nadal techniczna, posiada cechy działania właściwe podmiotowi społeczno-informacyjnemu.

Jakościowo nową formą cyfrowej osoby jako bytu autonomicznego (AI-persona) posiadającej sprawczość funkcyjną (choć w głównej mierze ograniczoną do funkcji dialogowych) są współczesne chatboty, szczególnie bazujące na modelach językowych (LLM – ang. Large Language Model – rodzaj sztucznej inteligencji (AI), której specjalnością jest przetwarzanie, interpretowanie i generowanie języka ludzkiego). Funkcjonują jako podmioty dialogowe potrafiące rozumieć niuanse języka ludzkiego, interpretować kontekst i generować dynamiczne odpowiedzi, które wydają się naturalne i istotne. To sprawia, że są postrzegane przez użytkowników jako podmioty posiadające cechy osoby. W literaturze zjawisko to wiąże się z teorią *media equation* (Reeves, Nass 1996), według której ludzie reagują na technologie jak na osoby – co tłumaczy antropomorfizację chatbotów i agentów.

Innym zaś przykładem tzw. AI-persony – bardziej zaawansowanej kategorii systemów AI – są agenci sztucznej inteligencji (*AI agents*) realizujący funkcje operacyjne, decyzyjne i wykonawcze. Do ich możliwości należą: automatyzacja zadań (np. automatyzacja zapytań klientów, zarządzanie planowaniem i przetwarzaniem transakcji), zaawansowana analiza danych (np. szybka i dokładna analiza ogromnych ilości danych, wyciąganie wniosków, które pomagają w tworzeniu strategii biznesowych), podejmowanie decyzji (np. określanie priorytetów zadań, rekomendowanie

akcji, autonomiczne działanie, takie jak optymalizowanie poziomów zapasów na podstawie prognoz sprzedaży), dostosowywanie do wyzwań (np. uściślanie odpowiedzi, personalizowanie środowisk użytkowników, zwiększanie skuteczności zadań).

Typy agentów sztucznej inteligencji:

- Agenci monitu i odpowiedzi to narzędzia sztucznej inteligencji przeznaczone do wykonywania określonych zadań na podstawie danych wejściowych lub „monitów użytkownika". Ci agenci (boty/asystenci wirtualni tj. Siri, Alexa) przetwarzają dane wejściowe i generują odpowiednią odpowiedź, ułatwiając wymianę między użytkownikami. Sprawdziją się podczas planowania dnia, tworzenia list zadań czy szybkiego wyszukiwania informacji.
- Agenci zadań mają na celu naśladowanie ludzkich procesów myślowych (poznawczych). Używają uczenia maszynowego i przetwarzania języka naturalnego, aby zrozumieć, nauczyć się i dostosować się do zachowania użytkownika w czasie. Agenci kognitywni mogą samodzielnie analizować dane, wykrywać wzorce i podejmować decyzje bez ciągłego nadzoru człowieka. W finansach automatycznie analizują trendy rynkowe i przeprowadzają transakcje, a w e-commerce personalizują oferty dla klientów.
- Agenci autonomiczni mają własne odrębne role i możliwości. Chociaż działają niezależnie jako jednostka, mogą również wchodzić w interakcje z innymi agentami i współpracować z nimi w celu rozwiązywania złożonych problemów, optymalizowania większych procesów lub osiągnięcia określonego celu. Te systemy z wieloma agentami są często używane w logistyce i zarządzaniu łańcuchem zaopatrzenia, gdzie agenci autonomiczni mogą dynamicznie organizować zadania, takie jak zarządzanie zapasami, śledzenie przesyłek i alokacja zasobów.

Istotne miejsce w debacie nad cyfrową osobą zajmuje pojęcie elektronicznej osobowości (*electronic personhood*). Pomysł uznania AI za osobę elektroniczną pojawił się w Parlamencie Europejskim w 2017 r. i został ostro skrytykowany, jednak powraca w dyskusjach dotyczących

odpowiedzialności algorytmicznej. Warto podkreślić, że chodzi tu o próbę nadania autonomicznym systemom AI statusu „osoby elektronicznej", tak jak spółka ma status osoby prawnej. Oznaczałoby to zatem, że tego typu byty cyfrowe mogłyby zaciągać zobowiązania, ponosić odpowiedzialność, działać w obrocie gospodarczym czy wreszcie – być odrębnym bytem od twórcy systemu. Jak piszą S. Negri (2021) oraz G. Teubner (2018), rozwój systemów autonomicznych rodzi pytania dotyczące przypisania im ograniczonego statusu prawnego w celu regulacji odpowiedzialności oraz wprowadzenia jednolitych zasad funkcjonowania w sferze publicznej. Chociaż koncepcja ta budzi kontrowersje i nie została przyjęta w aktach prawa unijnego, stanowi jeden z kluczowych elementów refleksji teoretycznej nad statusem cyfrowych bytów.

Warto pamiętać, że różne „perspektywy badań", które tłumaczą, jak i dlaczego cyfrowa osoba istnieje, co ją tworzy, jak działa oraz jakie relacje ma z człowiekiem, społeczeństwem, prawem i technologią, pozwalają m.in. nadać sens temu zjawisku, jak również pomagają analizować jego konsekwencje. Wśród ram teoretycznych należy wymienić:

- model podmiotowości algorytmicznej (Rouvroy) – człowiek jest „opisywany" i „przewidywany" przez dane, a jego cyfrowa osoba jest wytworem algorytmicznego profilowania. Decyzje wobec człowieka podejmowane są na podstawie jego cyfrowej reprezentacji, nie rzeczywistej osoby;
- *actor–network theory* (Latour) – cyfrowa osoba (avatar, chatbot, agent AI) jest uczestnikiem relacji na równi z człowiekiem, instytucją czy urządzeniem. Pokazuje, że cyfrowa osoba nie jest pasywnym narzędziem – może współtworzyć relacje i procesy społeczne;
- model relacji człowiek–agent (Hybrid Agency Model) – cyfrowa osoba (np. Copilot Agent) może wykonywać część czynności samodzielnie, wspierać człowieka, współdecydować o działaniach. Współczesne systemy AI nie są narzędziami, ale współwykonawcami;
- model posthumanistyczny/cyfrowego humanizmu – cyfrowa osoba jest rozszerzeniem człowieka – jego cyfrowym ciałem,

pamięcią, awatarem i agentem wykonawczym. Granica „człowiek–maszyna" staje się płynna;
- model odpowiedzialności (EU Responsibility Matrix) – systemy AI nie mają osobowości prawnej, więc odpowiedzialność rozkłada się na człowieka, twórcę, operatora i instytucje. Kluczowe jest pytanie: „Kto odpowiada, gdy cyfrowa osoba popełni błąd?";
- *media equation* (Reeves & Nass) – ludzie automatycznie reagują na komputer „jak na człowieka". Cyfrowa osoba wywołuje zachowania społeczne, emocjonalne i komunikacyjne. Tłumaczy, dlaczego chatboty muszą być regulowane jak podmioty komunikacyjne;
- *theory of digital subject* (Rouvroy, Zuboff, Floridi) – cyfrowa osoba nie musi być „osobą" w sensie biologicznym, lecz jest podmiotem w infosferze. Pozwala zrozumieć, czym różni się tożsamość cyfrowa od tożsamości cielesnej człowieka.

W obszarze bezpieczeństwa koncepcja cyfrowej osoby staje się kluczowa z uwagi na zagrożenia związane z tożsamością cyfrową, manipulacją algorytmiczną, deepfake'ami oraz ryzykiem przejęcia lub podszycia się pod cyfrową reprezentację osoby fizycznej. W spółczesny człowiek funkcjonuje bowiem równolegle w świecie fizycznym i informacyjnym, co czyni jego cyfrową postać podatną na przetwarzanie, nadużycia i profilowanie. A. Rouvroy i T. Berns (2013) opisują zjawisko „algorytmicznej podmiotowości" (cyfrowego podmiotu, władzy algorytmów), w którym podmiotowość jednostki jest współtworzona lub przetwarzana przez systemy cyfrowe, a decyzje jej dotyczące podejmowane są na podstawie cyfrowej reprezentacji – nierzadko bez udziału samego człowieka.

Z perspektywy szeroko pojętego bezpieczeństwa narodowego i społecznego cyfrowa osoba stanowi element środowiska cyberbezpieczeństwa obejmującego takie zagadnienia, jak integralność tożsamości cyfrowej, odporność na kradzież danych, ochrona awatarów i modeli behawioralnych, nadużywanie wizerunku w deepfake'ach, ryzyka związane z automatyzacją decyzji administracyjnych oraz odpowiedzialność prawna autonomicznych agentów. Dlatego niezbędne jest zwracanie uwagi na konieczność rozbudowy systemów prawnych o regulacje dotyczące identyfikacji,

uwierzytelniania oraz kontroli procesów, które tworzą i przetwarzają cyfrowe tożsamości.

Dla bezpieczeństwa szczególnie istotne są zagrożenia związane z:

- przejmowaniem tożsamości cyfrowej;
- wykorzystaniem cyfrowych osób do dezinformacji (np. *deepfake*);
- tworzeniem syntetycznych tożsamości służących do ataków socjotechnicznych;
- algorytmicznym deformowaniem reputacji;
- brakiem jasnych ram prawnych odpowiedzialności systemów autonomicznych;
- ryzykiem manipulacji decyzjami administracyjnymi przez modele scoringowe i predykcyjne;
- powstawaniem nieweryfikowalnych hybryd tożsamości (człowiek + system AI).

Zjawiska te wymagają od państw i instytucji rozwinięcia systemów bezpieczeństwa informacyjnego, przeciwdziałania kradzieży tożsamości, regulacji w zakresie wiarygodnej identyfikacji oraz ochrony obywateli przed negatywnymi konsekwencjami fałszywych lub automatycznie generowanych profili.

Emilia Musiał

R. Bomba, *Antropologia cyberprzestrzeni*, „Kultura Współczesna" 2007, nr 1; J. Dukaj, *Sztuczna inteligencja – koniec naszej podmiotowości?*, „Pomorski Thinkletter" 2021, nr 4(7); E.K. Clemons, *A face of one's own: The role of an online personae in a digital age and the right to control one's own online personae in the presence of digital hacking*, „Electron Mark" 2024, no. 34(1); *eIDAS – identyfikacja elektroniczna i usługi zaufania*, https://digital-strategy.ec.europa.eu/pl/policies/discover-eidas (dostęp 1.12.2025); L. Floridi, *The Philosophy of Information*, Oxford University Press, Oxford 2011; S. Negri, *Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence*, „Front Robot AI" 2021, no. 8; J. Pokojska, *Zachować podmiotowość w erze robotów*, „Pomorski Thinkletter" 2021, nr 4(7); B. Reeves, C. Nass, *Media i ludzie*, tłum. H. Szczerkowska, PIW, Warszawa 2000; A. Rouvroy, T. Berns, *Algorithmic Governmentality and Prospects of Emancipation Disparateness as a Precondition for Individuation Through Relationships?*, „Réseaux" 2013, no. 177(1); Rozporządzenie Parlamentu Europejskiego i Rady (UE)

nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, https://eur-lex.europa.eu/legal-content/PL/ ALL/?uri=celex%3A32014R0910 (dostęp 1.12.2025); M. Savin-Baden, *Digital Immortality and Virtual Humans*, „Postdigital Science and Education" 2019, vol. 1; G. Teubner, *Digital Personhood? The Status of Autonomous Software Agents in Pritate Law*, „Ancilla Iuris" 2018.

CYFROWY AUTORYTARYZM (ang. *digital authoritarianism*) – to model władzy XXI w., w którym rządy wykorzystują technologie cyfrowe do umacniania swojej pozycji i sprawowania nieograniczonego nadzoru nad społeczeństwem, często przy jednoczesnym stosowaniu mechanizmów wolnorynkowych w gospodarce. Jego podstawą są elementy gospodarki cyfrowej – sztuczna inteligencja, platformy cyfrowe i internet rzeczy (czyli fizyczne urządzenia połączone z siecią), które tworzą warunki dla kapitalizmu inwigilacji (*surveillance capitalism*), opartego na gromadzeniu ogromnych zasobów danych przez korporacje. Dane te (tzw. nadwyżka behawioralna) obejmują prywatne informacje, emocje i zachowania użytkowników, co pozwala na tworzenie szczegółowych profili osób i grup. W reżimach autorytarnych informacje te są wykorzystywane do manipulowania opinią publiczną, cenzurowania internetu oraz karania obywateli sprzeciwiających się linii rządzących.

Kapitalizm inwigilacji i cyfrowy autorytaryzm oddziela dziś jedynie cienka granica. Jak wspomniano, oba zjawiska opierają się na masowym gromadzeniu danych, choć pierwsze służy głównie celom komercyjnym, a drugie — politycznej dominacji i represji. Cyfrowy nadzór coraz częściej uzasadnia się potrzebą bezpieczeństwa czy ochrony zdrowia, co wyraźnie ujawniła pandemia COVID-19. Systemy te pozwalają kontrolować zachowania użytkowników i tworzyć mechanizmy przypominające „społeczny kredyt", czyli ocenę obywateli według arbitralnych kryteriów państwa. Obawy budzi także rozwój biometrii i zaawansowanej identyfikacji, który dodatkowo przybliża rzeczywistość do orwellowskiej wizji z *Roku 1984*.

Kluczowe znaczenie dla zrozumienia cyfrowego autorytaryzmu mają m.in. prace jednego z najważniejszych współczesnych krytyków technologii Evgeny'ego Morozova. Analizuje on → cyberutopizm jako naiwną

i niebezpieczną ideologię, która gloryfikuje internet i ślepo wierzy w jego wyzwalającą moc, ignorując jednocześnie to, jak technologie stają się narzędziem potencjalnej dominacji, wzmacniając nadzór i manipulację. Badacz ten podkreśla, że prywatne platformy i państwa wchodzą w układy umożliwiające masową kontrolę, zaś *solutionism* (przekonanie, że każdą kwestię można rozwiązać technologią) i utopijny internacjonalizm maskują procesy centralizacji władzy. Wskazuje on także na populistyczne teorie cyberutopistów o tym, że technologia wzmocni społeczeństwa, które – uciskane przez lata autorytarnych rządów – nieuchronnie zbuntują się za pośrednictwem SMS-ów, Facebooka, Twittera i innych narzędzi. Paradoksalnie, odmawiając dostrzeżenia wad nowego środowiska cyfrowego, cyberutopiści umniejszali znaczenie internetu, nie widząc, że przenika on i przekształca wszystkie dziedziny życia politycznego, a nie tylko te sprzyjające demokratyzacji. Dlatego, według Morozova, demokracja cyfrowa wymaga świadomego projektowania i kontroli społecznej, a nie ślepej wiary w rynek lub innowacje.

Tymczasem wykorzystanie nowych technologii nierzadko przyczynia się do pogorszenia praw politycznych i swobód obywatelskich. W 2018 r., według raportu Freedom House *Democracy in Crisis*, odnotowano spadek poziomu wolności w 71 państwach, a poprawę – jedynie w 35. Oznacza to 12 z rzędu rok globalnego regresu, po wcześniejszych dwóch dekadach ekspansji demokracji, której wzorcem wydawały się Stany Zjednoczone. Niektóre kraje nie tylko pogłębiają autorytaryzm wewnętrzny, ale też aktywnie destabilizują państwa demokratyczne i promują swoje modele ustrojowe w krajach rozwijających się.

Zwłaszcza Chiny, które od wielu lat prowadzą konsekwentną strategię rozwoju ICT, stały się symbolem cyfrowego autorytaryzmu. Ograniczenie wpływu zagranicznych korporacji umożliwiło powstanie i szybki rozwój rodzimych firm, które dzięki ogromnemu rynkowi wewnętrznemu urosły do stopnia globalnych graczy. Chronione przed konkurencją zachodnich gigantów dziś same dominują na wielu rynkach, często wyprzedzając wcześniejszych liderów. Podczas gdy GAFA (Google, Apple, Facebook, Amazon) rządzi na Zachodzie, w Chinach ustępuje miejsca BAT (Baidu, Alibaba, Tencent), funkcjonującym pod silnym nadzorem państwa. Firmy chińskie często wywodzą się ze struktur państwowych czy wojskowych,

lecz nawet prywatne i zagraniczne przedsiębiorstwa muszą liczyć się z kontrolą KPCh – m.in. poprzez partyjne komórki i przekazywanie państwu części udziałów oraz uprawnień do wpływania na kluczowe decyzje. Taka strategia wzmocniła krajowe koncerny i jednocześnie zapewniła władzom niemal pełną kontrolę nad obiegiem informacji.

Systemy takie jak Golden Shield i Great Firewall umożliwiają rozległą cenzurę i izolację kraju od globalnego internetu, czyniąc chińską sieć *de facto* ogromnym intranetem. BBC informowało, że już w 2013 r. ponad 2 mln osób zajmowało się w Chinach monitorowaniem i filtrowaniem treści oraz potajemnym publikowaniem ogromnych ilości fałszywych lub wprowadzających w błąd wpisów udających autentyczne opinie użytkowników. Tak zwana „armia 50 centów" składa się głównie z pracowników państwowych wykonujących to zadanie dodatkowo, a nie – jak wcześniej twierdzono – ze zwykłych obywateli opłacanych za każdy wpis. Większość dziennikarzy, aktywistów i badaczy uważała, że armia ta prowadzi spory w obronie reżimu, jednak wydaje się, że strategią chińskich władz nie jest wchodzenie w polemiki czy poruszanie kontrowersyjnych tematów. Wpisy koncentrują się raczej na entuzjastycznym wychwalaniu państwa, symboli reżimu i rewolucyjnej historii Partii Komunistycznej oraz odciąganiu uwagi społeczeństwa od mobilizacji zbiorowej, skarg i niezadowolenia. Szacuje się, że wspomniana siła robocza produkuje około 448 mln wpisów rocznie, z czego około połowę publikuje w sekcjach komentarzy na stronach rządowych.

Mechanizmy cybernadzoru w Chinach są wykorzystywane do kontrolowania i prześladowania mniejszości etnicznych, zwłaszcza muzułmańskich Ujgurów w regionie Sinciang. Mieszkańcy są tam nieustannie monitorowani – od obowiązkowych systemów namierzania w samochodach, po kamery i punkty kontrolne na stacjach, w hotelach czy sklepach. Policja może przeszukiwać telefony w poszukiwaniu „podejrzanych" aplikacji, a system automatycznie śledzi ruch osób uznanych za niebezpieczne.

W całych Chinach rozwijany jest też szeroko rozumiany system „kredytu społecznego", obejmujący różne państwowe i lokalne mechanizmy oceny zachowań obywateli i firm – służy to władzom do monitorowania aktywności społecznej i ekonomicznej oraz egzekwowania pożądanych zachowań pod hasłem budowy „harmonijnego społeczeństwa

socjalistycznego". Ponadto władze starają się zwiększać kontrolę nad gospodarką, próbując sterować nią poprzez wykorzystanie najnowszych technologii informacyjnych do realizacji koncepcji centralnego planowania (*techno-planning*). Taka kontrola ekonomiczna stanowiłaby kolejny stopień zniewolenia jednostki.

W kontekście rozważań o cyfrowym autorytaryzmie należy wspomnieć również o teorii sekurytyzacji (*securitisation*), według której władze przedstawiają jako zagrożenie coś, co uzasadnia podjęcie nadzwyczajnych środków poza standardowymi procedurami demokratycznymi. W odniesieniu do internetu wyłączenie lub ograniczenie dostępu jest przedstawiane jako działanie na rzecz bezpieczeństwa, a nie ograniczenie wolności. *Internet shutdowns* (zamierzone przerwy w usługach internetowych) są coraz częściej stosowane przez władze w imię bezpieczeństwa narodowego: w 2021 r. odnotowano co najmniej 182 takie przerwy w 34 krajach.

Przykładowo w Birmie, gdzie konstytucja z 2008 r. zapewniła wojsku kontrolę nad państwem i bezkarność za zbrodnie, po wygranych przez NLD wyborach w 2020 r. armia dokonała zamachu stanu, wywołując protesty i wojnę domową. W lutym 2021 r. junta szybko ograniczyła dostęp do internetu i telekomunikacji, a kryzysowi politycznemu towarzyszyły represje wobec społeczeństwa. Dodatkowo wprowadzono bariery ekonomiczne, takie jak podwyższenie podatków dla usług internetowych i opłat aktywacyjnych dla kart SIM, co ograniczyło dostęp do sieci dla uboższych warstw.

Z kolei w Białorusi reżim prezydenta Aleksandra Łukaszenki od lat wzmacnia kontrolę nad mediami i internetem. Władza ta utrzymuje się przez fałszowanie wyborów, represje wobec opozycji, dziennikarzy i internautów oraz ograniczanie wolności w sieci. Podczas protestów przeciwko reelekcji w 2020 r. dochodziło do masowych blokad internetu, zmian prawnych umożliwiających takie działania i dalszych represji wobec użytkowników sieci. W wyniku zmian konstytucyjnych w 2022 r. Łukaszenko zapewnił sobie dożywotni immunitet, a jednocześnie zniesiono status Białorusi jako kraju bez broni jądrowej, co teoretycznie umożliwia stałą obecność rosyjskich sił i broni nuklearnej na białoruskim terytorium.

Zarówno w Białorusi, jak i w Mjanmie blokady internetu nasiliły się w czasie kryzysów i protestów, a władze usprawiedliwiały je zagrożeniami

dla bezpieczeństwa publicznego, by legalizować cenzurę i represje oraz wzmacniać kontrolę. Takie działania tworzą pozór legalności wobec społeczności międzynarodowej i utrudniają obywatelom dochodzenie swoich praw. Mimo że oba państwa różnią się pod względem struktury, stosują podobne strategie: czasowe wyłączenia sieci (*blackouts*), zwłaszcza podczas ważnych wydarzeń (zamachy stanu, wybory), filtrowanie treści, blokady stron i mediów społecznościowych krytycznych wobec władz, inwigilację użytkowników, kontrole telefonów i karanie za korzystanie z VPN-ów, zastraszanie aktywistów i dziennikarzy poprzez prawo i nękanie online. Celem tych działań jest ograniczenie przepływu informacji, tłumienie protestów i utrzymanie władzy, a ich skutki są dalekosiężne – obejmują m.in. utratę pracy, ograniczony dostęp do informacji, edukacji i usług zdrowotnych, marginalizację grup społecznych (np. kobiet czy mniejszości), osłabienie możliwości protestu i organizacji obywatelskiej oraz wzmocnienie autorytarnych tendencji.

Także Rosja rozwija zaawansowany system cyfrowego autorytaryzmu, dążąc do pełnej kontroli nad przestrzenią informacyjną i inwigilacją obywateli. Proces ten przyspieszył szczególnie w okresie pandemii COVID-19, a następnie eskalował wraz z wojną przeciwko Ukrainie. Nowy raport International Partnership for Human Rights (IPHR) i Global Diligence LLP opisuje rozwój rosyjskiego systemu cyfrowego autorytaryzmu – zestawu technologii wykorzystywanych przez Kreml do śledzenia, kontrolowania i represjonowania społeczeństwa. Dokument ten analizuje kluczowe narzędzia represji, takie jak rozpoznawanie twarzy i program Smart City, system SORM umożliwiający szeroki monitoring komunikacji oraz projekt suwerennego internetu Ru.net, wyjaśniając, jak funkcjonują te technologie, kto je tworzy i utrzymuje oraz jakie podmioty dostarczają niezbędne komponenty (np. importowane półprzewodniki). Autorzy podkreślają, że masowa inwigilacja stała się jednym z filarów reżimu Władimira Putina. Od początku tego tysiąclecia Rosja wdrażała przepisy ograniczające wolność słowa, zwiększające cenzurę i legalizujące niemal nieograniczony nadzór cyfrowy. Technologie te umożliwiają identyfikowanie i ściganie krytyków zarówno w sieci, jak i w przestrzeni publicznej, wzmacniają propagandę oraz kontrolę nad informacją dotyczącą wojny przeciwko Ukrainie, a nawet mogą służyć do wyłapywania mężczyzn kierowanych

na front. W zakończeniu dokument przedstawia rekomendacje dla UE, USA, Wielkiej Brytanii, Kanady i innych państw dotyczące osłabiania łańcuchów dostaw umożliwiających Rosji rozwój technologii represji.

Dostęp do internetu ma wymiar nie tylko technologiczny, ale również społeczny i ekonomiczny. Rada Praw Człowieka ONZ uznaje dostęp do sieci za warunek korzystania z podstawowych wolności – w tym prawa do wypowiedzi, zgromadzeń i stowarzyszania się. Odcięciu od niej często towarzyszą inne naruszenia praw, gdy władze próbują ukryć swoje działania. Brak internetu ogranicza dostęp do informacji, usług publicznych, edukacji i opieki zdrowotnej, a w sytuacjach kryzysowych zagraża bezpieczeństwu obywateli. To skłania część ekspertów do postulatu uznania dostępu do internetu za prawo człowieka. Podkreślają oni konieczność wzmocnienia prawa międzynarodowego i mechanizmów jego egzekwowania oraz międzynarodowej koordynacji, tak aby wyłączanie sieci było traktowane jako poważne naruszenie. Rekomenduje się także poprawę skuteczności monitoringu i dokumentowania działań związanych z blokowaniem dostępu do internetu oraz zwiększenie odpowiedzialności firm technologicznych i operatorów, aby nie współpracowali z reżimami naruszającymi prawa człowieka, dostarczali narzędzia ochrony użytkowników i ponosili odpowiedzialność za sprzedaż technologii ułatwiających represje.

Państwa ograniczające wolność internetu zdają sobie sprawę, że jest on potężnym narzędziem samoorganizacji i wymiany informacji, a możliwości krytykowania polityki, dostęp do niezależnych źródeł informacji czy możliwość odnajdywania wspólnot o podobnych poglądach zmniejszają wpływ władzy na narrację. Technologie komunikacyjne umożliwiają co prawda łatwiejszą kontrolę społeczeństwa, ale stanowią także przestrzeń sprzeciwu i mogą służyć oporowi. Niezależne, oddolne inicjatywy *civic tech* (używanie narzędzi i platform cyfrowych do angażowania się w sprawy rządów i instytucji publicznych) są jednymi z najskuteczniejszych sposobów przeciwdziałania cyfrowemu autorytaryzmowi. Na przykład na Białorusi ludzie wymieniali się narzędziami i zasobami potrzebnymi do stawiania oporu przed, w trakcie i po wyborach prezydenckich; wykorzystywali platformy online do weryfikowania i liczenia głosów, dokumentowania nadużyć komisji wyborczych, władz i organów ścigania,

wspierania więźniów politycznych, dzielenia się sposobami obchodzenia blokad internetu oraz prowadzenia dyskusji o nowych formach protestu.

Walka z cyfrową autokracją wymaga działań wielowymiarowych. Choć potrzebna jest presja międzynarodowa, kluczowe znaczenie mają praktyczne środki samoobrony. Aktywiści w regionie potrzebują dostępu do bezpiecznych VPN-ów, szyfrowania, ochrony przed DDoS i innych narzędzi, dlatego rządy, firmy i organizacje powinny rozszerzać wsparcie i inwestować w rozwój tych technologii. Należy podkreślić, że ryzyko nadużyć istnieje również w społeczeństwach demokratycznych. Nieograniczony dostęp do danych i rosnąca potęga korporacji technologicznych mogą osłabić fundamenty ustrojowe, dlatego potrzebny jest globalny system zarządzania danymi, którego stworzenie utrudniają zarówno silne lobby firm technologicznych, jak i sprzeczne interesy państw w różnych częściach świata. Bez wspólnych standardów odpowiedzialności i kontroli demokratycznej technologia będzie wzmacniać logikę autorytaryzmu szybciej, niż zdoła się ją regulować.

Małgorzata Bereźnicka

Digital dictatorship: authoritarian tactics and resistance in Eastern Europe and Central Asia, Access Now Report, 2022, https://www.accessnow.org/wp-content/uploads/2022/10/Digital-dictatorship-authoritarian-tactics-and-resistance-in-Eastern-Europe-and-Central-Asia-Access-Now.pdf (dostęp 11.11.2025); M. Goliński, *E-administracja jako infrastruktura cyfrowego autorytaryzmu*, „Collegium of Economic Analysis Annals" 2019, nr 56, https://rocznikikae.sgh.waw.pl/p/roczniki_kae_z56_05.pdf (dostęp 11.11.2025); G. King, J. Pan, M.E. Roberts, *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, „American Political Science Review" 2017, vol. 111, no. 3, https://doi.org/10.1017/S0003055417000144; E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs, New York 2011; K. Olszewska, *Cyfrowy nadzór w chińskim modelu autorytarnego kapitalizmu*, „Acta Universitatis Wratislaviensis" 2022, nr 4145, Studia nad Autorytaryzmem i Totalitaryzmem 44, nr 3, https://doi.org/10.19195/2300-7249.44.3.5; *Russia's Digital Authoritarianism: The Kremlin's Toolkit*, 2023, https://iphronline.org/wp-content/uploads/2023/12/digital-authoritarianism-report.pdf (dostęp 11.11.2025); J. Ryng, G. Guicherd, J. Al Saman, P. Choudhury, A. Kellett, *Internet Shutdowns*, „The RUSI Journal" 2022, vol. 167, no. 4–5, https://doi.org/10.1080/03071847.2022.2156234 (dostęp 11.11.2025).

CZWARTA WŁADZA – odnosi się do zdolności mediów do kontrolowania działań politycznych, kształtowania opinii publicznej oraz pełnienia funkcji strażniczej (*watchdog*) wobec instytucji władzy. Nie ma pełnej zgodności co do pochodzenia tego pojęcia, jednak już Edmund Burke w XVIII w. miał zauważyć, że prasa stanowi „czwartą władzę w państwie", obok ustawodawczej, wykonawczej i sądowniczej. Takie podejście pozwalało stwierdzić, że prasa jest czynnikiem kontrolującym inne organy państwa poprzez informowanie publiczności o działaniach, które one podejmują, rozszerzanie w ten sposób wiedzy obywatela i umożliwianie mu współuczestnictwa w życiu publicznym. Współcześnie jednak, w erze cyfrowej i mediów społecznościowych, rola ta ulega dynamicznym przeobrażeniom – zarówno wzmacniającym, jak i osłabiającym społeczną funkcję mediów.

W literaturze medioznawczej podkreśla się, że media stanowią kluczowy element systemu demokratycznego, umożliwiając obywatelom dostęp do informacji niezbędnych do podejmowania świadomych decyzji oraz kontrolowania władzy. W pracy *The Elements of Journalism* Bill Kovach i Tom Rosenstiel wskazują, że podstawowym obowiązkiem dziennikarstwa jest poszukiwanie prawdy i jej przekazywanie obywatelom, dziennikarze muszą zachować niezależność wobec tych, o których piszą lub mówią, media muszą pełnić funkcję niezależnego kontrolera władzy i zapewnić miejsce do publicznej krytyki i kompromisu. W polskiej Karcie Etycznej Mediów również podkreślono, że media powinny kierować się m.in. zasadą prawdy i obiektywizmu (relacjonowania faktów bez zniekształceń, w odpowiednim kontekście i niezależnie od własnych poglądów), uczciwości (np. nieuleganie wpływom i nieprzekupności) oraz wolności i odpowiedzialności (co oznacza, że wolność mediów nakłada na dziennikarzy, wydawców, producentów i nadawców odpowiedzialność za treść i formę przekazu oraz wynikające z nich konsekwencje).

Badania naukowe dowodzą, że niezależne media śledcze mają realny wpływ na poziom korupcji oraz przejrzystość życia publicznego (Brunetti, Weder, 2003). Państwa o dużej wolności prasy notują niższe wskaźniki korupcji i większe zaufanie do instytucji demokratycznych.

Teoria *agenda-setting* (ustalania porządku dziennego) Maxwella McCombsa i Donalda Shawa (1972), jedna z podstawowych koncepcji badających wpływ komunikowania w przestrzeni mediów, wskazuje, że

poprzez selekcję i podkreślanie ważności wybranych tematów to media nadają im rangę ważności w oczach odbiorców, zatem to nie tylko politycy, lecz przede wszystkim media decydują o tym, jakie problemy i tematy społeczeństwo uznaje za ważne. Współczesne analizy rozszerzają tę teorię m.in. o *frame-setting* (*framing*, ramowanie), czyli proces, w którym media nie tylko ustalają ważność tematów, ale proponują też interpretacje wydarzeń; kształtują odbiór rzeczywistości poprzez wybór informacji, ich kontekstu i sposobu prezentacji. W praktyce oznacza to, że sposób pokazywania treści może wpływać na opinie obywateli równie mocno jak same fakty.

Według *Digital News Report 2025* korzystanie z tradycyjnych mediów (takich jak telewizja lub prasa drukowana) spada, rośnie natomiast wykorzystywanie mediów społecznościowych jako źródeł informacji. W wielu krajach (np. w USA, Tajlandii, Kenii i Indiach) odbiorcy mediów deklarują, że wolą oglądać wiadomości, niż je czytać, co oznacza, że filmy wideo (np. na platformie YouTube) zyskują na znaczeniu jako źródła informacji. Jednym z najszybciej rozwijających się źródeł informacji jest TikTok, przy czym jednocześnie platforma ta postrzegana jest przez respondentów jako zagrożenie w kontekście rozpowszechniania fałszywych i wprowadzających w błąd treści. Co ciekawe, ponad połowa respondentów (58%) twierdzi, że martwi się swoją zdolnością odróżniania informacji prawdziwych od fałszywych w internecie. Najwyższy poziom obaw odnotowano w Afryce (73%) i Stanach Zjednoczonych (73%), a najniższy – w Europie Zachodniej (46%). W raporcie podkreślono również poziom zaufania do mediów: we wszystkich badanych krajach wyniósł średnio **40%**. W Polsce podobne zjawiska odnotowuje m.in. raport *Kondycja mediów 2024*. Dostęp do internetu w domu deklaruje 91,2% badanych Polaków, w tym 83,5% to aktywni użytkownicy. Najczęściej deklarowanymi aktywnościami w internecie są wykorzystywanie komunikatorów internetowych (85,8%), mediów społecznościowych (84,3%) i serwisów VOD (w tym także serwisu YouTube, 81,4%) oraz portali ogólnoinformacyjnych (64,6%). Oglądanie telewizji deklaruje natomiast 88,4% badanych.

Wraz z rozwojem platform takich jak Facebook, X (dawniej Twitter), TikTok czy YouTube zmieniła się nie tylko forma przekazu, ale także sposób tworzenia i cyrkulacji informacji. Coraz częściej to nie redakcje

i dziennikarze, lecz algorytmy decydują, jakie treści zobaczą użytkownicy. Badania (m.in. Vosoughi, Roy, Aral 2018) pokazały, że fałszywe wiadomości rozprzestrzeniają się w mediach społecznościowych kilka razy szybciej niż prawdziwe, przede wszystkim ze względu na ich emocjonalny charakter. Raporty (np. EU DisinfoLab) podkreślają, że platformy społecznościowe stały się jednym z największych kanałów dystrybucji dezinformacji m.in. politycznej i zdrowotnej, a sztuczna inteligencja, szczególnie ta pozwalająca na generowanie treści, jeszcze bardziej komplikuje możliwości użytkowników mediów do oceny wiarygodności i prawdziwości informacji.

W wielu krajach, w tym w Polsce, USA i na Węgrzech, obserwuje się wzrost politycznego podziału w mediach. Zjawisko to opisuje m.in. Cass Sunstein (2017), wskazując, że tzw. *echo chambers* (komory echa) oraz *filter bubbles* (bańki filtrujące) wzmacniają istniejące przekonania i poglądy oraz ograniczają styczność odbiorców z odmiennymi opiniami. Badania CBOS *Postrzeganie mediów* z 2023 r. pokazały, że tylko 14% Polaków uważa telewizję publiczną za bezstronną, a zdecydowana większość respondentów (79%) postrzega ją jako sprzyjającą rządowi i partii rządzącej.

Rozwój generatywnej sztucznej inteligencji wprowadza kolejną rewolucję; może ona wspierać analizę dużych zbiorów danych, wykrywanie nadużyć czy automatyzację rutynowych procesów redakcyjnych, ale jednocześnie powoduje ryzyko generowania i rozpowszechniania deepfake'ów, manipulacji obrazem i dźwiękiem oraz automatyczną produkcję treści niskiej jakości. UNESCO w raporcie *Guidelines for Regulating Digital Platforms* (2023) podkreśla, że bez odpowiednich ram prawnych media będą tracić zdolność do pełnienia funkcji czwartej władzy, zarówno z powodu presji ekonomicznej, jak i chaosu informacyjnego. Celem wytycznych UNESCO jest wspieranie rozwoju i wdrażania procesów regulacyjnych w mediach, które mają gwarantować wolność wypowiedzi i swobodny dostęp do informacji, a jednocześnie ograniczać ryzyko kontaktu z treściami nielegalnymi i łamiącymi prawa człowieka. Wśród nowych modeli finansowania mediów rozwijają się:

– abonamenty cyfrowe (np. „New York Times" w 2025 r. zanotował ponad 11 mln abonentów korzystających wyłącznie z usług cyfrowych);

- fundacje, zespoły i konsorcja dziennikarstwa śledczego ujawniające nadużycia (np. ICIJ, OCCRP);
- modele non-profit chroniące niezależność redakcji (np. ProPublica).

Wszystkie te inicjatywy mają na celu utrzymanie funkcji kontrolnej mediów w świecie, w którym tradycyjne modele ekonomiczne przestają działać.

Mimo licznych zagrożeń media nadal mogą pełnić rolę czwartej władzy, ale wymaga to:

- niezależności finansowej;
- silnych standardów etycznych;
- transparentności działania;
- edukacji medialnej odbiorców;
- regulacji platform cyfrowych;
- inwestycji w dziennikarstwo śledcze.

Współczesne wyzwania, takie jak cyfryzacja, polaryzacja czy dezinformacja, nie powodują osłabienia znaczenia mediów jako czwartej władzy, lecz czynią ją bardziej istotną niż kiedykolwiek.

Paulina Motylińska

A. Brunetti, B. Weder, *A Free Press is Bad News for Corruption*, „Journal of Public Economics" 2003, vol. 87(7–8); *False information online as a threat*, 2025, https://www.pewresearch.org/2025/08/19/false-information-online-as-a-threat/ (dostęp 15.12.2025); *Guidelines for regulating digital platforms: A multistakeholder approach to safeguarding freedom of expression and access to information*, https://www.unesco.org/sites/default/files/medias/fichiers/2023/04/draft2_guidelines_for_regulating_digital_platforms_en.pdf (dostęp 15.12.2025); *Infrastruktura i sposoby konsumpcji usług medialnych w 2024 r.*, 2025, https://kim.gov.pl/2025/04/01/infrastruktura-i-sposoby-konsumpcji-uslug-medialnych-w-2024-r/ (dostęp 31.01.2026); *Karta Etyczna Mediów*, https://www.rem.net.pl/services.php (dostęp 31.01.2026); *Komunikat z badań: Ocena głównych stacji telewizyjnych i radiowych*, 2022, https://www.cbos.pl/SPISKOM.POL/2022/K_064_22.PDF (dostęp 15.12.2025); *Komunikat z badań: Postrzeganie mediów*, 2023, https://cbos.pl/SPISKOM.POL/2023/K_132_23.PDF (dostęp 31.01.2026); B. Kovach, T. Rosenstiel, *The Elements of Journalism. What Newspeople Should Know and the Public Should Expect*, Three Rivers Press, New York 2001; M.E. McCombs, D.L. Shaw, *The Agenda-Setting*

Function of Mass Media, „The Public Opinion Quarterly" 1972, vol. 36(2); M. McCombs, S. Valenzuela, *Setting the Agenda. The Mass Media and Public Opinion*, Polity Press, Cambridge 2020; N. Newman, *Overview and key findings of the 2025 Digital News Report*, https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/dnr-executive-summary (dostęp 31.01.2026); A. Paczkowski, *Czwarta władza: prasa dawniej i dziś*, Wiedza Powszechna, Warszawa, 1973; *State of the News Media (Project)*, https://www.pewresearch.org/topic/news-habits-media/news-media-trends/state-of-the-news-media-project/ (dostęp 15.12.2025); C.R. Sunstein, *#Republic. Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton 2017; S. Vosoughi, D. Roy, S. Aral, *The Spread of True and False News Online*, „Science" 2018, vol. 359(6380).

D

DEGRADACJA ATTENTION SPAN W ŚRODOWISKACH AI. (Degradacja zdolności koncentracji uwagi (attention span degradation) – oznacza długofalowy i systematyczny proces skracania czasu, przez który jednostka jest zdolna utrzymywać stabilną, selektywną, a przede wszystkim poznawczo produktywną uwagę ukierunkowaną na jedno zadanie. Dotyczy to zwłaszcza aktywności wymagających ciągłości przetwarzania, integracji informacji oraz sprawnej kontroli wykonawczej, a także odporności na dystrakcje o charakterze poznawczym, sensorycznym i afektywnym. Zjawisko obejmuje zarówno redukcję długości epizodów uwagi podtrzymywanej, jak i obniżenie jakości przetwarzania poznawczego, widoczne w spadku zdolności do pracy z treściami złożonymi i sekwencyjnymi. W środowiskach intensywnie nasyconych systemami sztucznej inteligencji degradacja ta przybiera wymiar strukturalny i systemowy, gdyż jest wzmacniana przez architekturę informacyjną oraz algorytmiczne mechanizmy organizujące przepływ treści i bodźców. Projektowane z myślą o maksymalizacji zaangażowania użytkownika, częstotliwości interakcji oraz subiektywnego poczucia płynności poznawczej mechanizmy te

sprzyjają odciążeniu poznawczemu (*cognitive offloading*) polegającemu na delegowaniu wysiłku poznawczego na systemy zewnętrzne.

Długofalowe ograniczanie aktywnego angażowania obwodów neuronalnych odpowiedzialnych za koncentrację sprzyja powstawaniu zjawiska określanego jako *sedentary brain*, w którym nieużywane lub rzadko aktywizowane sieci neuronalne ulegają funkcjonalnemu osłabieniu. Szczególnie podatnym obszarem degradacji pozostają funkcje wykonawcze związane z procesem pisania – wymagającym długotrwałej uwagi, planowania, kontroli poznawczej oraz wielopoziomowej integracji treści. Zastępowanie tego wysiłku gotowymi materiałami generowanymi przez systemy AI osłabia obwody neuronalne odpowiedzialne nie tylko za koncentrację, lecz także za organizację myśli i refleksyjny wysiłek poznawczy. W konsekwencji nadmierne poleganie na algorytmicznych systemach wsparcia może prowadzić do erozji kluczowych kompetencji poznawczych oraz sprzyjać scenariuszowi tzw. „twardego dostosowania poznawczego" (*cognitive hard adjustment*), w którym sztuczna inteligencja stopniowo przejmuje funkcje wyższego rzędu, zasadniczo przekształcając sposób ludzkiego poznania. Szczególne obawy budzi to w środowiskach edukacyjnych, gdzie łatwość generowania treści może osłabiać motywację do samodzielnego myślenia oraz ćwiczeń poznawczych niezbędnych do rozwoju i stabilizacji mechanizmów uwagi w procesie uczenia się.

W środowiskach opartych na systemach sztucznej inteligencji – obejmujących konwersacyjne modele językowe, algorytmicznie personalizowane strumienie treści, systemy rekomendacyjne oraz generatywne narzędzia wspomagania pracy intelektualnej – aktywność poznawcza użytkowników przebiega przy zniesieniu temporalnych i poznawczych barier dostępu do informacji. Stała dostępność treści oraz niska latencja odpowiedzi prowadzą do głębokiej reorganizacji rytmu pracy poznawczej, w której dominują krótkie sekwencje uwagi inicjowane bodźcem zewnętrznym, a nie intencjonalnie podtrzymywane cele poznawcze. Taki tryb funkcjonowania odpowiada stanowi określanemu jako ciągła częściowa uwaga (*continuous partial attention*), polegającemu na stałym dzieleniu i przełączaniu koncentracji pomiędzy wieloma bodźcami bez pełnego zaangażowania w żaden z nich. W efekcie następuje przesunięcie od logiki przetwarzania informacji ku logice „wielu przerwań", w której

łatwość dostępu do zasobów poznawczych okupiona jest permanentnym rozpraszaniem uwagi i powierzchownym rozumieniem treści. Jednocześnie wymagania środowiska cyfrowego coraz częściej przekraczają dostępne zasoby uwagi jednostki, co prowadzi do przeciążenia uwagi.

Istotną rolę odgrywa mechanizm odciążania poznawczego (*cognitive offloading*), polegający na delegowaniu na systemy AI zadań wymagających analizy, pamięci roboczej i krytycznego myślenia, a następnie na nadmiernym poleganiu na generowanych przez algorytmy gotowych odpowiedziach. W efekcie ograniczone zostaje aktywne zaangażowanie procesów poznawczych odpowiedzialnych za samodzielną ocenę informacji, formułowanie własnych sądów i rozwijanie idei, a część funkcji pamięciowych ulega przeniesieniu na zewnętrzne nośniki cyfrowe, co osłabia utrwalanie informacji w pamięci długotrwałej.

Koszt ten znajduje odzwierciedlenie w mechanizmach neurokognitywnych. Intensywna stymulacja cyfrowa oraz wielozadaniowość medialna korelują ze zmianami w funkcjonowaniu i strukturze obszarów mózgu odpowiedzialnych za regulację poznawczą i emocjonalną, co przekłada się na osłabienie zdolności podtrzymywania uwagi. Z kolei mechanizmy natychmiastowej gratyfikacji, wzmacniane przez algorytmiczne systemy rekomendacyjne, aktywizują układ nagrody i sprzyjają utrwalaniu zachowań kompulsywnych, prowadząc do dalszego skracania cykli koncentracji oraz wzrostu podatności na uzależnienia behawioralne związane z technologią.

Nasilanie tych procesów jest w dużej mierze skutkiem sposobu projektowania interakcji człowiek–AI, w ramach którego systemy konstruuje się w oparciu o metryki maksymalizacji retencji użytkownika, częstotliwości interakcji oraz subiektywnego poczucia płynności i bezwysiłkowości użytkowania. Algorytmiczna personalizacja treści, realizowana poprzez ciągłe dopasowywanie bodźców informacyjnych do profilu zachowań i wcześniejszych wyborów użytkownika, prowadzi do stopniowego zawężania repertuaru informacji oraz tworzenia baniek filtrujących i komór echa. Ogranicza to ekspozycję na odmienne perspektywy poznawcze, zawężając tym samym pole refleksji. Mechanizm ten sprzyja nie tylko polaryzacji postaw i zniekształceniu percepcji rzeczywistości społecznej, lecz również obniża tolerancję na wysiłek poznawczy wymagany przez treści złożone i procesy wieloetapowe. Choć funkcjonowanie w trybie

ciągłego przełączania uwagi może generować subiektywne poczucie wysokiej produktywności, w praktyce wiąże się z obniżeniem dokładności przetwarzania informacji, wzrostem poziomu stresu oraz narastającą frustracją wynikającą z konieczności wielokrotnego odzyskiwania skupienia po przerwaniach.

Szczególnie istotny jest także mechanizm nieskończonej dostępności treści (*infinite availability*), w ramach którego systemy sztucznej inteligencji systematycznie eliminują naturalne punkty zakończenia interakcji poznawczej – takie jak wyraźny koniec sekwencji informacyjnej – zastępując je nieprzerwanym strumieniem rekomendacji i sugestii kolejnych działań. Brak strukturalnych momentów zatrzymania ogranicza możliwość spontanicznej regulacji tempa pracy poznawczej i sprzyja utrzymywaniu użytkownika w stanie ciągłej, reaktywnej gotowości poznawczej. W takich warunkach kształtują się tzw. mikrocykle uwagi, trwające od kilku do kilkunastu sekund, w których koncentracja inicjowana jest bodźcem zewnętrznym i wygasa wraz z jego wyczerpaniem, bez przejścia w fazę pogłębionego przetwarzania.

Proces ten potęguje fundamentalne niedopasowanie pomiędzy biologiczną strukturą ludzkiej uwagi a architekturą systemów sztucznej inteligencji. Ludzka uwaga jest procesem celowym i kontrolowanym, opartym na aktywnym podejmowaniu decyzji o alokacji ograniczonych zasobów poznawczych zgodnie z intencjami i wiedzą jednostki; skuteczna samoregulacja odgrywa tu kluczową rolę, zwłaszcza w zadaniach wymagających długotrwałego wysiłku. Tymczasem systemy AI operują w trybie równoległego przetwarzania ogromnych wolumenów danych, nie podlegając biologicznym ograniczeniom, takim jak ograniczone pole uwagi czy pojemność pamięci roboczej. Ludzki system poznawczy, ukształtowany ewolucyjnie w warunkach deficytu informacji, funkcjonuje w oparciu o sekwencyjne przesuwanie ogniska uwagi, co czyni go szczególnie podatnym na przeciążenie w środowiskach o wysokiej intensywności bodźców. Algorytmiczne środowisko informacyjne uderza w to poznawcze „wąskie gardło", osłabiając mechanizmy uwagi odgórnej (*top-down*), niezbędne do utrzymywania celu poznawczego. Podczas gdy ludzka uwaga ma charakter dwukierunkowy, łącząc kontrolę odgórną z automatycznymi reakcjami na bodźce zewnętrzne, alokacja uwagi w systemach AI ma charakter czysto

reaktywny, oparty na analizie danych wejściowych i wyuczonych rozkładach prawdopodobieństwa. Generowany przez algorytmy strumień treści nie jest zatem dostosowany do ludzkiej potrzeby budowania spójnych, hierarchicznych reprezentacji świata, lecz do matematycznej optymalizacji trafności i prawdopodobieństwa odpowiedzi. W konsekwencji użytkownik traci zdolność selektywnego wyodrębniania informacji o znaczeniu krytycznym, co w psychologii poznawczej wiąże się ze zjawiskiem ślepoty nieatencyjnej (*inattentional blindness*), polegającym na przeoczaniu istotnych elementów w warunkach przeciążenia zasobów uwagi.

W ujęciu operacyjnym degradacja zdolności koncentracji uwagi ujawnia się w trzech wzajemnie powiązanych, lecz analitycznie rozróżnialnych wymiarach: dynamice czasowej uwagi, sposobach przetwarzania informacji oraz wzorcach zachowań poznawczych użytkowników. Wymiar temporalny obejmuje systematyczne skracanie ciągłych epizodów uwagi podtrzymywanej, wzrost częstotliwości przerywania aktywności poznawczych oraz trudności w utrzymaniu koncentracji na jednym zadaniu przez dłuższy czas bez dodatkowego wsparcia ze strony bodźców zewnętrznych lub systemów wspomagających. Zjawiska te prowadzą do fragmentaryzacji czasu poznawczego oraz osłabienia zdolności do planowania i realizowania zadań wymagających długotrwałego zaangażowania. Wymiar poznawczy wiąże się z przesunięciem preferencji w kierunku przetwarzania powierzchownego, ograniczeniem zdolności do integracji informacji pochodzących z różnych źródeł oraz spadkiem efektywności uczenia się wymagającego kumulacji wiedzy w czasie. W tym zakresie obserwuje się także osłabienie zdolności do analizy wieloetapowej, abstrahowania oraz konstruowania spójnych reprezentacji poznawczych. Wymiar behawioralny przejawia się natomiast w kompulsywnym sprawdzaniu informacji, zwiększonej reaktywności na bodźce informacyjne oraz narastającej zależności od natychmiastowych odpowiedzi generowanych przez systemy AI. Towarzyszy temu obniżenie motywacji do samodzielnego wysiłku intelektualnego, w tym formułowania problemów, rozwijania argumentacji oraz podejmowania zadań poznawczych wymagających długotrwałej koncentracji i opóźnionej gratyfikacji.

Z perspektywy nauk o bezpieczeństwie proces ten stanowi istotne zagrożenie dla bezpieczeństwa poznawczego i informacyjnego, rozumianego

jako zdolność jednostek do selektywnego, refleksyjnego, a przede wszystkim krytycznego przetwarzania informacji oraz podejmowania racjonalnych decyzji w warunkach wysokiej złożoności i presji informacyjnej. Skrócenie *attention span* obniża zdolność rozpoznawania manipulacji informacyjnych, analizowania argumentacji wieloetapowej oraz identyfikowania subtelnych form dezinformacji, które nie opierają się na jawnych fałszach, lecz na fragmentaryzacji treści lub selektywnym doborze informacji.

Ograniczanie skutków degradacji *attention span* wymaga strategii o charakterze wielopoziomowym, obejmujących zarówno projektowanie technologii, jak i rozwój kompetencji użytkowników oraz ram instytucjonalnych. Na poziomie systemowym kluczowe znaczenie ma projektowanie rozwiązań AI zgodnie z zasadami uwzględniającymi wpływ architektury interakcji, tempa informacji oraz mechanizmów rekomendacyjnych na długofalowe funkcjonowanie poznawcze użytkowników – m.in. poprzez wprowadzanie punktów zatrzymania, ograniczanie nadmiernej stymulacji i zwiększanie przejrzystości decyzji algorytmicznych. Równie istotne jest rozwijanie kompetencji samoregulacji poznawczej, obejmujących zdolność do świadomego zarządzania uwagą, kontrolowania impulsów informacyjnych oraz podtrzymywania koncentracji w zadaniach wymagających długotrwałego wysiłku intelektualnego. W perspektywie długoterminowej kluczowe pozostaje uznanie „uwagi" za dobro wymagające ochrony w ramach polityk cyfrowych i strategii bezpieczeństwa informacyjnego, a także systematyczna integracja kryteriów wpływu poznawczego w procesach oceny ryzyka, certyfikacji oraz regulacji systemów sztucznej inteligencji.

Miłosz Horodyski, Edyta Sadowska

S. Dubey, R. Ghosh, S. Chatterjee, M. Jana Dubey, S. Das, J. Benito-León, *Redefining cognitive domains in the era of ChatGPT: A comprehensive analysis of artificial intelligence's influence and future implications*, „Medical Research Archives" 2024, no. 12(6), https://doi.org/10.18103/mra.v12i6.5383 (dostęp 30.01.2026); *The human advantage: Stronger brains in the age of AI*, 2026, https://www.weforum.org/reports/the-human-advantage-stronger-brains-in-the-age-of-ai/ (dostęp 30.01.2026); M. Shanmugasundaram, A. Tamilarasu, *The impact of digital technology, social media, and artificial intelligence on cognitive functions: A review*, „Frontiers in

Cognition" 2023, Article 1203077, https://doi.org/10.3389/fcogn.2023.1203077 (dostęp 30.01.2026); B. Sparrow, J. Liu, D.M. Wegner, *Google effects on memory: Cognitive consequences of having information at our fingertips*, „Science" 2011, no. 333(6043), https://doi.org/10.1126/science.1207745 (dostęp 30.01.2026); M. Zhao, D. Xu, T. Gao, *From cognition to computation: A comparative review of human attention and transformer architectures*, arXiv, 2024, https://doi.org/10.48550/arXiv.2407.01548 (dostęp 30.01.2026).

DEKLARACJA WEIMARSKA W KONTEKŚCIE ZAGROŻEŃ ROSYJSKĄ DEZINFORMACJĄ to formalne porozumienie, w którym państwa Trójkąta Weimarskiego[1] (Polska, Niemcy i Francja) zobowiązują się do wspólnej walki z rosyjską dezinformacją. Zostało podpisane 12 lutego 2024 r., podczas spotkania w pałacu La Celle-Saint-Cloud, we Francji, na którym ministrowie spraw zagranicznych zapowiedzieli utworzenie wspólnego, skoordynowanego mechanizmu wczesnego ostrzegania i zwalczania ataków dezinformacyjnych. Spotkanie odbyło się w przededniu drugiej rocznicy rosyjskiej inwazji i w momencie, w którym stosunki międzynarodowe charakteryzowały się niejednoznacznością, nieprzewidywalnością, niepewnością i niestabilnością.

W deklaracji podkreślono, że celem państw Trójkąta Weimarskiego jest zjednoczenie i umocnienie Unii Europejskiej oraz sprawienie, aby była ona w stanie odpowiedzieć na dzisiejsze wyzwania w zakresie bezpieczeństwa, dążąc do takiej unii w wymiarze bezpieczeństwa i obronności, która będzie spełniać oczekiwania obywateli.

Deklaracja ta ustanowiła, że dezinformacja, cyberataki i inne formy ingerencji informacyjnej (szczególnie ze strony Rosji) są uznawane za jedno z kluczowych zagrożeń dla demokracji, bezpieczeństwa i spójności społecznej państw Trójkąta. W praktyce oznacza to gotowość do ścisłej

[1] Format Trójkąta Weimarskiego został stworzony w 1991 r. z inicjatywy niemieckiego ministra spraw zagranicznych Hansa-Dietricha Genschera, wraz z jego francuskimi i polskimi odpowiednikami, Rolandem Dumasem i Krzysztofem Skubiszewskim, aby rozwinąć wspólną wizję Europy i zacieśnić więzi między społeczeństwami trzech krajów. Trójkąt początkowo był kluczowym forum wspierającym niemiecko-polskie pojednanie, inspirowanym doświadczeniem francusko-niemieckim. Po przystąpieniu Polski do Unii Europejskiej w 2004 r. stał się bardziej forum współpracy przed negocjacjami Unii Europejskiej.

współpracy: wymiany informacji, koordynacji działań, wspólnego monitoringu i reagowania na kampanie dezinformacyjne, zwłaszcza w okresach wrażliwych (np. wyborów). Zapowiedziano również utworzenie „weimarskiego programu ostrzegania i odpowiedzi" na manipulacje informacyjne.

Państwa Trójkąta Weimarskiego jednoznacznie identyfikują rosyjskie kampanie dezinformacyjne jako poważne i bezpośrednie zagrożenie dla bezpieczeństwa i stabilności Europy. Po spotkaniu ministrowie postanowili ustanowić i realizować nowy specjalny „program weimarski w celu ostrzegania przed zagranicznymi działaniami dezinformacyjnymi", szczególnie w kontekście ważnych wydarzeń wyborczych, takich jak wybory do Parlamentu Europejskiego w 2024 r. czy wybory parlamentarne/prezydenckie w państwach UE.

Kraje Trójkąta Weimarskiego prezentują wspólne stanowisko na forum Unii Europejskiej, wzywając do skoordynowanych działań, i zwracają uwagę na potrzebę wzmacniania odporności społecznej na rosyjską propagandę. Inicjatywy te mają na celu skuteczniejsze odpieranie wrogich wpływów zewnętrznych, które nasiliły się zwłaszcza w kontekście wojny Rosji z Ukrainą. W związku z tym ministrowie spraw zagranicznych trzech państw konsekwentnie poruszali kwestię wielowymiarowego zagrożenia ze strony Rosji, obejmującego nie tylko konwencjonalną agresję militarną, ale także taktykę wojny hybrydowej.

Kluczowe aspekty ich podejścia do rosyjskiej dezinformacji obejmują:

- rozpoznanie zagrożenia: deklaracja stwierdza, że rosyjskie kampanie dezinformacyjne są celowo zaprojektowane w celu wzmocnienia agresji militarnej poprzez „sianie zamętu i podziałów" w społeczeństwach europejskich; rosyjska dezinformacja i manipulacje informacyjne stanowią „największe i najbardziej bezpośrednie" zagrożenie dla stabilności demokratycznych społeczeństw w Europie;
- walkę z dezinformacją – obok wsparcia Ukrainy i przestrzegania praworządności została ona wymieniona jako jeden z kluczowych obszarów współpracy w deklaracji ministrów ds. europejskich;
- zobowiązanie do wspólnego działania: kraje partnerskie zobowiązały się do dalszej ścisłej współpracy w ramach UE, NATO

i poza nią, aby budować odporność, bronić wspólnego bezpieczeństwa i chronić Europę przed tymi kampaniami;
- szersze zagrożenia hybrydowe: dezinformacja jest rozpatrywana równolegle z innymi zagrożeniami hybrydowymi, takimi jak cyberataki i manipulacje polityczne;
- wymianę informacji i wspólne przeciwdziałanie takim zagrożeniom, również na poziomie instytucji UE, np. nacisk na platformy internetowe, by skuteczniej reagowały na kampanie dezinformacyjne;
- dążenie do krajowego wzmocnienia koordynacji w zakresie manipulacji informacjami poprzez stworzenie mechanizmu ostrzegania, wykrywania i reagowania (ang. *alert & response scheme*) na kampanie dezinformacyjne w ramach formatu weimarskiego, co jest ważne zwłaszcza przed wyborami czy w sytuacjach kryzysowych;
- włączenie kwestii dezinformacji w szeroki kontekst bezpieczeństwa, współpracy UE, obronności i suwerenności informacyjnej;
- wsparcie dla budowania odporności, czyli edukacji medialnej, wspierania niezależnych mediów i organizacji obywatelskich, które mogą pomagać w identyfikowaniu i obalaniu manipulacji.

Deklaracja weimarska w sprawie zagrożeń rosyjską dezinformacją została podpisana właśnie w 2024 r., ponieważ pełnowymiarowa inwazja Rosji na Ukrainę w lutym 2022 r. spowodowała ożywienie formatu współpracy Trójkąta Weimarskiego, ze szczególnym uwzględnieniem kwestii bezpieczeństwa, ponieważ wzrosła skala i intensywność kampanii dezinformacyjnych, manipulacji medialnych, działań hybrydowych wobec państw europejskich. Format Trójkąta Weimarskiego uznał to za poważne zagrożenie, a 2024 r. był rokiem wyborczym w wielu krajach UE, co zwiększało ryzyko prób wpływania na wyniki poprzez dezinformację i manipulacje. Oprócz tego zmienił się charakter bezpieczeństwa: konflikty i wojny mają coraz silniejszy wymiar informacyjny i hybrydowy, co wymaga nowych form współpracy między państwami, także partnerskiej i ponadnarodowej solidarności.

Wspólna deklaracja Polski, Niemiec i Francji w sprawie zagrożeń rosyjską dezinformacją nadaje większą wagę problemowi dezinformacji – to już nie pojedynczy kraj, ale sojusz trzech dużych państw, które mówią jednym głosem, co zwiększa szansę na skuteczne działania i międzynarodową koordynację.

Deklaracja weimarska stanowi zatem formalne ramy dla Polski, Francji i Niemiec, umożliwiające im uznanie, koordynowanie działań i przeciwdziałanie wszechobecnemu i celowemu rozpowszechnianiu dezinformacji sponsorowanej przez państwo rosyjskie, mającej na celu destabilizację Unii Europejskiej i osłabienie wsparcia dla Ukrainy.

Deklaracje i dokumenty (weimarskie, warszawskie, unijne) pokazują, że dezinformacja traktowana jest jako istotne zagrożenie wymagające wspólnej reakcji. Deklaracja to zobowiązanie polityczne, a nie automatyczne działanie, więc wymaga skutecznych mechanizmów:

- realnych zasobów – finansowych, ludzkich, instytucjonalnych – do monitoringu mediów, edukacji medialnej, działań prewencyjnych i interwencyjnych;
- identyfikacji kampanii dezinformacyjnych, blokowania manipulacji, egzekwowania odpowiedzialności, transparentnej współpracy między państwami i platformami internetowymi;
- szerokiej współpracy rządów, mediów, organizacji pozarządowych, społeczeństwa obywatelskiego.

Jednak skuteczność zależy od realnej implementacji, czyli chęci państw, zasobów, koordynacji międzynarodowej, jak również odpowiedzialności mediów i obywateli. Choć deklaracja zakłada współpracę i reagowanie – to konkretne działania (np. blokowanie stron, ograniczanie kampanii, działania służb, edukacja medialna) wymagają czasu, zasobów i woli politycznej. Nie ma gwarancji, że wszystko zostanie wdrożone równomiernie; problem dezinformacji jest globalny, rozproszony, często prowadzony anonimowo, co utrudnia „zatrzymywanie" go tylko przez deklaracje międzyrządowe. Wymaga współpracy szerokiego grona instytucji państwowych, mediów, platform internetowych, społeczeństwa obywatelskiego, a to może komplikować koordynację i skuteczne działanie.

Jeszcze jedną inicjatywą powiązaną z Deklaracją weimarską jest wspólne oświadczenie ministrów ds. europejskich Francji, Niemiec i Polski

z okazji spotkania w sprawie Trójkąta Weimarskiego w Paryżu i departamencie Yvelines (28–29 kwietnia 2024 r.), które dotyczyło wsparcia dla Ukrainy, walki z dezinformacją, przestrzegania praworządności, a także wymiany młodzieży między Polską, Niemcami i Francją. We wspólnej deklaracji ministrowie ds. europejskich Trójkąta Weimarskiego napisali, że w ramach współpracy międzynarodowej agencje bezpieczeństwa ujawniły rosyjską siatkę prowadzącą działania dezinformacyjne oraz inne operacje wpływu w ramach portalu Voice of Europe. Ministrowie precyzują, że celem rosyjskich operacji jest „osłabienie wsparcia dla Ukrainy i dyskredytowanie wizerunku UE". „Będziemy nadal czujni i zdeterminowani, by ujawniać takie szkodliwe operacje", zapewnili.

Dzięki podobnym deklaracjom rozwija się współpraca między nadawcami, regulatorami, organizacjami pozarządowymi, mediami i platformami internetowymi, by skuteczniej identyfikować i obalać dezinformację.

Potencjalne długofalowe kierunki rozwoju wynikające z deklaracji to:

- rozbudowa i wzmocnienie europejskiego systemu reagowania na dezinformację, np. przez utworzenie stałego „centrum koordynacji dezinformacji" w UE, który monitorowałby kampanie hybrydowe, wymieniał dane między państwami i reagował wspólnie;
- włączenie działań przeciw dezinformacji i ingerencjom informacyjnym do szerszej strategii bezpieczeństwa i suwerenności cyfrowej UE, co oznacza, że problem nie jest już tylko medialny, ale stanowi element geopolityki, polityki bezpieczeństwa i obronności. To widać np. w Agendzie weimarskiej na rzecz silnej i geopolitycznej UE;
- zacieśnienie współpracy instytucji państwowych, regulatorów mediów, organizacji pozarządowych i platform online, co może prowadzić do standardów transnarodowych, wspólnych zasad walki z dezinformacją, wymiany doświadczeń i lepszej koordynacji;
- rozwój narzędzi technicznych i technologicznych, w tym regulacji AI, automatycznego wykrywania treści manipulacyjnych, transparentności reklamy politycznej jako części pakietów prawnych i technologicznych na poziomie UE.

Polska, jako sygnatariusz Deklaracji weimarskiej i Deklaracji warszawskiej o dezinformacji, uczestniczy w mechanizmach koordynacji z Niemcami i Francją w zakresie monitoringu i reagowania. Dla Polski (i całej Europy) Deklaracja weimarska może stanowić:

- element budowy europejskiej współpracy obronnej również w wymiarze informacyjnym, nie tylko militarno-obronnym;
- wsparcie dla inicjatyw zwiększających odporność społeczeństw na dezinformację: edukacji medialnej, *fact-checking*, transparentności mediów;
- narzędzie współpracy z UE, co może prowadzić do wdrażania unijnych regulacji (np. w ramach prawa cyfrowego, ochrony demokracji, przeciwdziałania zagranicznej ingerencji);
- sygnał dla społeczeństwa i mediów, że dezinformacja nie jest marginalnym problemem, ale zagrożeniem strategicznym, co może zwiększyć czujność i świadomość całej UE.

Po podpisaniu Deklaracji weimarskiej w sprawie zagrożeń rosyjską dezinformacją zostały przyjęte różne dokumenty, inicjatywy i mechanizmy, które służą przeciwdziałaniu dezinformacji, ingerencjom informacyjnym i wzmacnianiu odporności demokratycznej. Tak państwa uruchomiły współpracę mającą na celu monitorowanie dezinformacji, wymianę informacji i reagowanie na sieci propagandowe (np. powiązane ze zdemaskowanymi sieciami prorosyjskimi jak Portal Kombat). Deklaracja może również inspirować innych członków UE do dołączenia do podobnych inicjatyw, co wzmocni całościowy europejski system odporności na dezinformację.

Sergiusz Wasiuta

B. Bodalska, *Ministrowie ds. europejskich państw Trójkąta Weimarskiego o dezinformacji*, 30.04.2024, https://euractiv.pl/section/polityka-wewnetrzna-ue/news/ministrowie-ds-europejskich-panstw-trojkata-weimarskiego-o-dezinformacji/ (dostęp 9.12.2025); *Deklaracja po spotkaniu państw Trójkąta Weimarskiego*, 13.02.2024, https://www.gov.pl/web/dyplomacja/deklaracja-po-spotkaniu-panstw-trojkata-weimarskiego?utm_source=chatgpt.com (dostęp 7.12.2025); A. Dziubińska, *Nadzwyczajny szczyt Trójkąta Weimarskiego*, 18.03.2024, https://www.pism.pl/webroot/upload/files/Komentarz/Komentarz%20PISM%20nr%2019-2024.pdf (dostęp 9.12.2025); *France Diplomacy*, https://www.diplomatie.gouv.fr/en/

country-files/germany/the-weimar-triangle/article/the-weimar-triangle-277677 (dostęp 11.12.2025); *Joint Statement of the Foreign Ministers of France, Germany and Poland*, 29.09.2025, https://www.diplomatie.gouv.fr/en/country-files/germany/the-weimar-triangle/article/joint-statement-of-the-foreign-ministers-of-france-germany-and-poland-29-09-25 (dostęp 11.12.2025).

DEMARKACJA (ang. *demarcation*) – w rozumieniu geograficzno-politycznym to wyznaczanie granic oraz umowny podział terenu, zaś w nauce – rozróżnienie pomiędzy współczesną nauką a pseudonauką. Demarkację wykorzystywać można w celu oddzielania tego, co fałszywe, od tego, co prawdziwe, w postępowaniu naukowym. Odwołując się do twierdzenia Karla Poppera (kryterium falsyfikacyjne), demarkacja służy do oddzielenia zdań naukowych od metafizycznych; twierdzeń naukowych od takich, których nie można poddać weryfikacji. To jeden z najważniejszych mechanizmów zapewniających rzetelność nauki; polega na zakwalifikowaniu twierdzenia naukowego tylko wtedy, gdy jest możliwe poddanie go próbie empirycznej. Klasyfikacja Poppera staję się mocnym argumentem dla konieczności użycia demarkacji w nauce. Mimo funkcjonowania wielu odmiennych metod postrzegania nauki i klasyfikowania jej prawdziwości uznaje się, że demarkacja jest mechanizmem kontrolnym gwarantującym uznawanie wiedzy za naukową w oparciu o metody badawcze, ale także analizy czy też spójne uzasadnienie. Pojęcie to chroni naukę przed fałszywymi twierdzeniami i nieprawdziwymi naukami, które są wynikiem niepoprawnego stosowania metod czy też doboru narzędzi badawczych.

Demarkacja w nauce służy również do ustalenia granic formalnych poznania, które możliwe są do zrealizowania poprzez użycie narzędzi naukowych. Należy również określić funkcje demarkacji, mianowicie: podstawową, pomocniczą, przechodnią. Demarkacja jest kluczowym pojęciem w metodologii nauk, co stanowi fundament rzetelnego procesu badawczego również w naukach o bezpieczeństwie. W dostępnej literaturze definiowana jest jako *conceptual demarcation* (rozgraniczenie pojęć) i rozumiana jako oddzielenie od siebie dziedzin w celu dokładnego zdefiniowania czy też klasyfikacji. Dzięki temu procesowi można dokonać analizy ryzyka lub wspomóc się w prowadzeniu badań naukowych.

Demarkacja potrzebna jest, aby rozróżnić pojęcia i wyprowadzić problem chaosu pojęciowego. Istotą użycia demarkacji jest wyznaczenie kryteriów, które pozwolą na wyraźne rozróżnienie zagrożeń, odmiennych metod badawczych czy organizacji systemów. W dostępnej literaturze pojęcie to rozumiane jest jako fundament wobec uporządkowania terminologii związanej z bezpieczeństwem. Realnym i naukowym przykładem użyteczności demarkacji jest rozróżnienie pojęć *security* oraz *safety*. Pierwszy termin może dotyczyć sektora prywatnego, infrastruktury krytycznej czy też kwestii cyberbezpieczeństwa, a jego rozumienie jest zmienne i ewoluuje poprzez zmiany na tle społecznym; natomiast drugi – rozumiany jest jako ochrona przed wypadkami, awariami czy zdarzeniami przypadkowymi. Dodatkowo zdarzenia określane pojęciem *safety* są zwykle przewidywalne, natomiast *security* – wprost przeciwnie. Warto również zauważyć, że w publikacjach pojawia się pewien aspekt bezpieczeństwa, mianowicie – w obszarze tym zawsze występuje relacja między atakującym a broniącym się. Natomiast w rozumieniu i definiowaniu właśnie pojęcia *safety* za pomocą demarkacji, atakujący nie występuje jako aktywny sprawca, to kwestia zapobiegania błędom, prewencja. Przedstawione pojęcia są idealnym przykładem na to, jak demarkacja jest potrzebna w praktycznym rozróżnianiu terminów, które często stosowane są niejednoznacznie, a przez to są mylone, co prowadzi do chaosu czy też problemów w podejściu metodologicznym.

Należy zaznaczyć, że demarkacja w naukach o bezpieczeństwie pozwala na dokładną klasyfikację zagrożeń, co jest kluczowe chociażby dla tworzenia procedur bezpieczeństwa, projektowania środków prewencji, planowania ochrony infrastruktury. Natomiast źle sklasyfikowane zagrożenie skutkuje przede wszystkim niepoprawnym zastosowaniem środków ochrony, a nawet może doprowadzić do niepoprawnej oceny poziomu ryzyka, dlatego należy podkreślić, że jest niezbędna w celu przeprowadzenia analizy ryzyka lub dobrania odpowiedniej metody zarządzania. Demarkacja jasno wyznacza ramy, w których określane są potencjalne zagrożenia, a w następstwie tego – środki zaradcze.

W literaturze pojawia się bardziej precyzyjne, ale i nowoczesne rozumienie demarkacji określane jako *malicious intent*, opierające się na

występowaniu lub nie szkodliwego działania. Należy również zaznaczyć, że brak zastosowania demarkacji niesie wiele konsekwencji, m.in.:

- błędną klasyfikację zagrożeń (polega na niepoprawnej klasyfikacji, co skutkuje chociażby zignorowaniem ryzyka);
- błędne przydzielenie zbiorów (na przykładzie pojęć *safety* i *security*, zjawiska te potrzebują różnych środków, np. analitycznych);
- brak możliwości tworzenia polityki bezpieczeństwa.

Biorąc pod uwagę te konsekwencje, należy pamiętać, że demarkacja ma zastosowanie zarówno w teorii, jak i praktyce.

Sissel Haugdal Jore, autorka publikacji *The Conceptual and Scientific Demarcation of Security in Contrast to Safety*, podkreśla, że obszar nauk o bezpieczeństwie jest w ciągłym rozwoju teoretycznym, a jednym z głównych powodów spowalniania procesu rozwoju tej dziedziny jest brak jasnego rozróżnienia pojęć (przykład zjawisk *security* i *safety*) i ich zakresu znaczeniowego. Wyraźne rozdzielenie tych kwestii umożliwia prowadzenie dalszych badań. Bardzo ważną kwestią zastosowania demarkacji jest umożliwienie wyodrębnienia metod badawczych – np. odpowiednio dla *security* (pojęcie to wymaga metod analizy i zachowań przeciwnika) i *safety* (pojęcie to wymaga zastosowania metod o charakterze statystycznym, dotyczących przewidywalnych wzorców, również technicznych). Należy więc zauważyć, że demarkacja w obszarze rozumienia bezpieczeństwa pozwala na rozwój tego obszaru nauki. Bez jasnego rozróżnienia trudno byłoby o dynamiczny i efektywny rozwój tej dziedziny.

Na podstawie analizy dostępnych źródeł należy podkreślić, że demarkacja jest pojęciem niezbędnym w naukach o bezpieczeństwie. Uwzględniając wszystkie wymienione elementy, pozwala na rozróżnienie różnego typu zagrożeń, ryzyka, a nawet metod wykorzystywanych podczas analizy bezpieczeństwa. Określa, jakie paradygmaty i dziedziny powinny podlegać badaniom (ustalając również odpowiednie metody), a także jak klasyfikować zjawiska bezpieczeństwa. Stosowanie demarkacji w naukach o bezpieczeństwie nie dotyczy oczywiście rozróżnienia pojęć *safety* i *security*. Omawiane narzędzie pozwala na uporządkowanie i ujednolicenia terminologii szerokiego zbioru zagadnień obszaru nauk o bezpieczeństwie. Umożliwia przypisanie odpowiednich zagrożeń do poszczególnych metod

oceny ryzyka. Dotyczy to również procedur ochronnych czy też zakresu odpowiedzialności organizacji. Zjawisko to pozwala na stwierdzenie, które określenia należą do nauk o bezpieczeństwie, a które powinny być traktowane jako zakres innych dziedzin, np. psychologii, socjologii, informatyki czy też nauk technicznych. Bez wyznaczania odpowiednich granic pojęciowych nauka o bezpieczeństwie stałaby się obszarem bez jasno określonego zakresu, a także spójnej teorii czy ram tematycznych.

Demarkacja pełni również funkcję porządkującą, która odpowiednio kwalifikuje obszary interdyscyplinarne (takie jak bezpieczeństwo) i nie doprowadza do chaosu terminologicznego. Narzędzie to pozwala na oddzielenie pola badawczego, określając, czym zajmują się dane zjawiska czy pojęcia i jak odpowiednio je stosować w badaniach. Pozwala również w tym zakresie na odpowiednie dobranie metody analitycznej do danych rodzajów zagrożeń. Należy zauważyć, że w tej kwestii demarkacja pozwala zachować porządek i ustalić zasady. Umożliwia wyraźnie oddzielenie poszczególnych dziedzin badań, ustalenie, jakie kompetencje są potrzebne, a także przypisanie odpowiednich metod analitycznych. Warto tutaj zwrócić uwagę, że proces demarkacji nie wyklucza interdyscyplinarności, a pełni funkcję porządkującą, tak aby stała się narzędziem do tworzenia spójności w dziedzinie nauki. Bezsprzecznie należy podkreślić, że demarkacja w nauce jest sposobem organizacji obszarów naukowych w celu budowania dziedzin naukowy w sposób jasny i teoretycznie spójny. Istotne staje się również to, że demarkacja jest procesem dynamicznym ze względu na zmieniające się zagrożenia czy też stale rozwijające się dziedziny nauki. Dzieje się tak, ponieważ charakter granic między różnymi typami zachowań zmienia się niezwykle szybko, dlatego rozróżnienie należy aktualizować na bieżąco. Technologie, ale również środowiska bezpieczeństwa stale ewoluują i poddawane są modyfikacjom, dotyczy to również podmiotów, których zadaniem jest zachowanie bezpieczeństwa i ochrony. Zmienność pojęć środowiska bezpieczeństwa sprawia, że terminy pokrywają się, a to rodzi trudności w podejściu metodologicznym, dlatego demarkacja staje się narzędziem, które porządkuje skomplikowany obszar badawczy, wskazując różnice między poszczególnymi dziedzinami badań.

Natalia Borodziuk

C. Glesner, R. Geysmans, C. Turcanu, *Two Sides of the Same Coin? Exploring the Relation Between Safety and Security in High-Risk Organizations*, „Journal of Safety and Security" 2022, vol. 82(3), https://www.researchgate.net/publication/360921171_Two_sides_of_the_same_coin_Exploring_the_relation_between_safety_and_security_in_high-risk_organizations (dostęp 11.12.2025); S.H. Jore, *The Conceptual and Scientific Demarcation of Security in Contrast to Safety*, „European Journal for Security Research" 2019, vol. 4(1), https://www.researchgate.net/publication/320910719_The_Conceptual_and_Scientific_Demarcation_of_Security_in_Contrast_to_Safety (dostęp 11.12.2025); J. Kot, *Demarkacja w naukach o bezpieczeństwie*, „Obronność. Zeszyty Naukowe" 2016, nr 3(19); N. Levson, *Safety and Security are two sides of the same coin*, [w:] *The Coupling of Safety and Security Exploring Interrelations in Theory and Practice*, W.C. Bieder, K. Pettersen Gould (eds.), SpringerOpen, Berlin 2022, https://library.oapen.org/bitstream/id/43a56786-6b87-416a-8140-59b7fe02431f/978-3-030-47229-0.pdf (dostęp 11.11.2025).

DRON FPV (ang. *first-person view*) – bezzałogowy statek powietrzny (quadrokopter) sterowany przez operatora noszącego gogle wirtualnej rzeczywistości, które odbierają obraz z pierwszej kamery, stąd nazwa „widok pierwszej osoby". Zwykle są to drony jednorazowego użytku, lecące bezpośrednio nad celem, gdzie detonowany jest ładunek wybuchowy o masie do 1,5 kg. Ich największą zaletą jest niski koszt produkcji oraz masowe użycie, dzięki któremu nawet najmniejszy pododdział wojska może dysponować własną bronią precyzyjnego rażenia. Z ich pomocą atakowane są cele ruchome (czołgi, pojazdy opancerzone, ciężarówki wojskowe, motocykle) oraz trudno dostępne nieruchome (bunkry, piwnice, wnętrza budynków). Zwolennicy wykorzystania dronów FPV podkreślają, że są one przyczyną 60–70% wszystkich ofiar w czasie wojny rosyjsko-ukraińskiej. Należy jednak mieć na uwadze fakt, że statystyka ta, chociaż zbieżna z rzeczywistością, może nie odróżniać straty spowodowanej przez inne rodzaje bezzałogowców. Pojawiają się również zdania (A. Salinas, J.P. LeVay), że drony typu FPV zapoczątkują kolejną rewolucję w sprawach wojskowych, której znaczenie będzie podobne jak w przypadku innych innowacji, jakie pojawiły się w historii wojskowości. Ich powszechne użycie może doprowadzić do sytuacji, w której gromadzenie i ukrywanie techniki wojskowej w strefie działań wojennych stanie się niemal niemożliwe.

Niezależnie od tego, czy znaczenie dronów FPV uznane zostanie za kolejną RMA, faktem jest, że około 43% wszystkich lotów bojowych kończy się trafieniem w zamierzony cel. Należy jednak mieć na uwadze fakt, iż zazwyczaj maszyny te wykorzystywane są jako „drugie uderzenie" w pojazd, który już wcześniej został trafiony i unieruchomiony (głównie przez moździerz lub ładunek zrzucony przez UAV wielokrotnego użytku). Zadaniem operatorów FPV jest zatem niszczenie techniki wojskowej, która została już uszkodzona, aby nie została wycofana ze strefy walki i naprawiona. Powstaje zatem pytanie, dlaczego dowódcy wojskowi nie decydują się na jeszcze częstsze wykorzystanie dronów FPV lub użycie ich do „pierwszego" ataku na pojazdy przeciwnika. Jednym z zasadniczych powodów są pieniądze: chociaż to tani system bojowy, są inne, znacznie tańsze. Koszt przeciętnego drona szacuje się na mniej niż 500 dolarów, podczas kiedy koszt pocisku moździerzowego to mniej niż 100 dolarów, podobnie jak pocisk zrzucany przez bezzałogowca wielokrotnego użytku. Drugim powodem, dlaczego nie spełniają one swoich zadań, są kwestie techniczne: bywają zawodne, trudne w obsłudze i podatne na zakłócenia. Niewiele z nich posiada funkcję obserwacji w nocy, co w sytuacji, kiedy zimą ciemność panuje przez 14 godzin w ciągu doby, znacznie ogranicza ich wykorzystanie.

W praktyce ponad 25% z nich doświadcza usterki technicznej, która uniemożliwia lot. Zazwyczaj jest ona wykrywana dopiero podczas przygotowywań do startu. Najczęściej spotykana jest usterka odbiornika radiowego odbierającego sygnały z panelu sterowania lub nadajnika wideo przesyłającego sygnał do gogli wirtualnej rzeczywistości operatora. Czasami można ją usunąć poprzez aktualizację oprogramowania, jednak nie zawsze jest to możliwe. Wadliwe drony, których nie można wykorzystać, są używane jako części zamienne. Co dziesiąty dron FPV uderzający w cel nie niszczy go, ponieważ głowica nie eksploduje. Kolejnym wyzwaniem jest sam pilotaż; z założenia drony z widokiem pierwszej osoby, zanim zostały wykorzystane przez wojsko, miały być bardzo szybkie, kosztem stabilności. Nie mogą one zawisnąć w powietrzu, latać powoli ani utrzymywać się nad celem; w rezultacie szkolenie wykwalifikowanego operatora może trwać nawet kilka miesięcy. Standardowy kurs dla operatorów ukraińskich sił zbrojnych trwa około 5 tygodni, jednak jego jakość jest wątpliwa. Duża

część żołnierzy obsługujących drony FPV nawet nie kończy kursu i uczy się pilotować maszyny w praktyce. Aby zminimalizować koszty, ukraińscy operatorzy nie stosują żadnych pomocy nawigacyjnych, takich jak kompas, odbiornik GPS czy bezwładnościowy system nawigacyjny. Sukces przeprowadzonego ataku warunkowany jest zatem dobrą znajomością okolicznych terenów oraz komunikacją z przełożonym, który ma dostęp do innych środków, za pomocą których obserwowany jest cel. Zdaniem samych operatorów, największą przeszkodą jest zdecydowanie zawodność połączenia radiowego między operatorem a dronem; ma ona miejsce w momencie, kiedy maszyna zbliża się do ziemi lub znajduje się po niewłaściwej stronie wysokiego budynku lub wzgórza, które blokuje łączność. Co więcej, UAV FPV wykorzystują niezaszyfrowane analogowe sygnały radiowe, o które w czasie intensywnych walk może „rywalizować" kilkanaście zespołów; powoduje to konieczność stosowania zaawansowanych procedur „dekonfliktowych", co nie zawsze daje gwarancję uzyskania poprawnej łączności. W czasie wojny w Ukrainie zdarzały się przypadki, w których zespoły obsługujące drony musiały czekać do pół godziny na zwolnienie częstotliwości przed startem. Jeśli dwa drony znalazłyby się w tym samym kanale łączności w tym samym czasie, zakłócałyby swoje sygnały, co mogłoby doprowadzić do zderzenia. Zakłócenia tego rodzaju ze strony innego UAV, niezależnie czy przyjaznego, czy wrogiego, doprowadzają w Ukrainie do niepowodzenia co najmniej 3% misji. Operatorzy podkreślają także, że drony FPV są bardzo podatne na zakłócenia w ramach walki elektronicznej. Skala zastosowania zagłuszania, zarówno przez Ukraińców, jak również Rosjan jest tak duża, że nie są w stanie rzetelnie informować wszystkich swoich jednostek na froncie o momentach, w których urządzenia te są włączane. Załogi samochodów lub bojowych wozów piechoty, wyposażone w przenośne „zagłuszacze", włączają je w każdej sytuacji, kiedy tylko pojawia się dron, nie czekając na identyfikację, czy to maszyna sojusznicza, czy wroga. Szacuje się, że rosyjskie środki walki elektronicznej zestrzeliwują aż 31% wszystkich ukraińskich lotów bojowych UAV.

Niektóre z wymienionych problemów związanych z użytkowaniem dronów typu FPV mogą zostać rozwiązane w przyszłości wraz z postępem technologicznym. Obecnie w Ukrainie funkcjonują setki podmiotów, w których budowane są bezzałogowce z tanich gotowych komponentów

pochodzących od różnych dostawców. Brak standaryzacji powoduje, że każda jednostka produkcyjna robi to według własnego uznania. Po zakończeniu wojny wprowadzenie lepszej kontroli i wyeliminowanie tanich komponentów może znacząco poprawić niezawodność dronów z widokiem pierwszej osoby. Prace mogą polegać także na montażu lepszej klasy nadajników i odbiorników odpornych na zakłócenia, poprawie połączenia między dronem a operatorem, umieszczeniu translatorów wzmacniających sygnał na „drugim" bezzałogowcu, który unosi się gdzieś pomiędzy operatorem a UAV FPV, ujednolicenie procedury szkolenia czy coraz częstsze stosowanie światłowodu. Światłowody uniemożliwiają zagłuszanie, eliminują „rywalizację" o częstotliwość, a brak energochłonnego nadajnika radiowego wydłuża czas pracy baterii, stąd też drony światłowodowe można często spotkać na drogach znajdujących się w pobliżu linii frontu, gdzie czekają na swoją „ofiarę". Mają one jednak odmienne ograniczenia niż drony z widokiem pierwszej osoby, co znacząco zawęża ich zastosowanie. Przewód łączący operatora z maszyną redukuje manewrowość, a jakakolwiek kolizja z przeszkodą, taką jak drzewo czy zarośla, może skutkować utratą kontroli. Są one znacznie trudniejsze w pilotażu, a koszty rosną wraz z ich zasięgiem. Dron wraz ze światłowodem o długości 10 km kosztuje około dwa razy więcej niż model sterowany radiowo o podobnym zasięgu.

Jakub Jajcay – były żołnierz NATO, który na początku wojny rosyjsko-ukraińskiej zgłosił się jako wolontariusz do sił międzynarodowych walczących po stronie Kijowa i w trakcie służby był operatorem dronów – na łamach „War on the Rocks" wyraził krytyczne zdanie na temat rozwoju UAV FPV w armiach zachodnich. Jego zdaniem zdecydowana większość misji wykonywana za pomocą dronów z widokiem pierwszej osoby może być realizowana tajniej, skuteczniej i niezawodniej za pomocą innych środków, takich jak moździerze, artyleria i amunicja krążąca. Użycie moździerzy, podobnie jak artylerii nie może zostać ograniczone przez warunki pogodowe ani „zatłoczone" częstotliwości radiowe. Zespół obsługujący moździerz może być gotowy do otwarcia ognia w mniej niż pięć minut, podczas kiedy start drona FPV zajmuje średnio 15 minut od momentu otrzymania polecenia. Po drugie, prosta konstrukcja bezzałogowców jest przyczyną ich licznych awarii. Armie natowskie już obecnie dysponują

o wiele bardziej zaawansowanymi maszynami, takimi jak amunicja krążąca Switchblade, która zapewnia większą precyzję w dzień i w nocy, łatwość w obsłudze i lepszą odporność na zakłócenia elektroniczne. Są one droższe, ale ich koszt wraz z rozwojem zdolności produkcyjnych będzie spadał. Po trzecie, wybór dronów z widokiem pierwszej osoby, jako podstawowego środka rażenia, wymuszałby rozbudowę zaplecza logistycznego. Wojsko miałoby wówczas dwa konkurujące ze sobą systemy logistyczne obsługujące artylerię oraz UAV FPV. Po czwarte, drony nie są w stanie dorównać psychologicznemu efektowi użycia pocisków artyleryjskich, które od dawna uznawane są za element wojny na wyniszczenie. Ukraiński analityk wojskowy Serhii Berezutski podkreślił, że jest za wcześnie, aby stwierdzić, czy drony z widokiem pierwszej osoby zastąpią w przyszłości artylerię. Jego zdaniem warto zwrócić uwagę także na przyczynę pojawienia się dużej ilości tego rodzaju bezzałogowców w Siłach Zbrojnych Ukrainy. Wynikała ona z opóźnień realizacji pakietów pomocowych ze strony Stanów Zjednoczonych i Unii Europejskiej, co zmusiło Kijów do produkcji tanich dronów jednokrotnego użytku, aby zrekompensować brak pocisków artyleryjskich.

Krytyczne zdanie w tym obszarze wyraził także Bill Murray – podpułkownik w amerykańskim U.S. European Command – który przestrzegł przed entuzjastycznym podejściem do wykorzystania dronów z widokiem pierwszej osoby oraz stawiania tezy, że zastąpią one w przyszłości artyleryjskie środki rażenia. Jego zdaniem bezzałogowe statki powietrzne mogą jedynie wzmocnić wsparcie ogniowe, poprawić świadomość sytuacyjną i zapewnić przewagę taktyczną, ale nie będą w stanie w dającej się przewidzieć przyszłości zastąpić tradycyjnej artylerii pod względem zasięgu, jak również siły rażenia. W wojnie rosyjsko-ukraińskiej obie strony wykazały się niezwykłą zdolnością do adaptacji olbrzymiej ilości dronów, aby sprostać ograniczonym zasobom oraz zmieniającym się wymaganiom konfliktu (wojna pozycyjna). Zmiana ta nie miała jednak charakteru strategicznego, nie jest również zwiastunem nowej ery działań wojennych, lecz pragmatyczną reakcją na okoliczności. Rozprzestrzenienie się dronów FPV należy traktować jako rozwiązanie tymczasowe, które rekompensuje niedobory pocisków artyleryjskich, szczególnie po stronie ukraińskiej, wypełniając tę lukę, lecz nie oferując lepszego rozwiązania. Innymi słowy, okazały

się skuteczne w zwalczaniu pojazdów opancerzonych na poziomie taktycznym, nie zaś bronią, która wpływa na strategiczny poziom sztuki wojennej. Ponadto są one bardzo wrażliwe na warunki pogodowe: deszcz pogarsza działanie czujników i może spowodować awarie elektryczne, a silny wiatr – destabilizować tor lotu oraz zdolność do precyzyjnego uderzenia w cel. Wniosek, jaki formułuje Murray, jest następujący: armie państw zachodnich powinny skupić się na integracji dronów, moździerzy i artylerii rakietowej w kompleksową siłę ognia, a nie próbować zastępować wszystkie dostępne środki rażenia UAV FPV. Jeśli powtórzyłaby się sytuacja, jaka ma miejsce w Ukrainie, gdzie poszczególne brygady wojsk lądowych eksperymentują z komercyjnie dostępnymi dronami, często bez jasno określonego celu operacyjnego i bez wzajemnej integracji, doprowadzi to do problemów z interoperacyjnością oraz powstaniem rozdrobnionej amatorskiej kultury dronowej, która nie sprawdzi się w wojnie z równorzędnym przeciwnikiem, jakim są Chiny i Rosja. Znacznie inne podejście w użyciu dronów z widokiem pierwszej osoby miało miejsce po stronie rosyjskiej. W 2024 r. powiązani z Kremlem milblogerzy zwrócili uwagę, że głównym dostawcą dronów FPV jest Państwowa Spółka Leasingowa Transportu STLE i ma ona monopol na ich produkcję. Wojsko ukraińskie z kolei od dawna zna częstotliwości, na jakich operuje maszyna, i skutecznie je zagłusza. W odpowiedzi na to rosyjskie Ministerstwo Obrony Narodowej w kwietniu 2024 r. podjęło decyzję o przyspieszeniu wdrażania dronów FPV poprzez finansowanie specjalnych projektów, w których partnerami były prywatne podmioty gospodarcze. W rezultacie pojawiły się nowe rodzaje maszyn, a łączna liczba produkowanych wzrosła do 40 tys. miesięcznie. Decentralizacja pozwoliła jednostkom frontowym zwiększyć liczbę uderzeń z kilkuset do ponad 2 tys. dziennie.

Znacznie większy entuzjazm charakteryzuje osoby spoza środowiska wojskowego, szczególnie przedstawicieli korporacji z zachodniego wybrzeża USA. Były szef Google Eric Schmidt na łamach „Wall Street Journal" napisał, że drony z widokiem pierwszej osoby w najbliższej przyszłości zastąpią inne rodzaje systemów bojowych, zapewniając masową siłę ognia przy znacznie niższych kosztach. David Hambling podkreślił z kolei, że największą zaletą UAV FPV jest zdolność do precyzyjnego

rażenia, co nie jest spotykane we wszystkich rodzajach artylerii. W wojnie rosyjsko-ukraińskiej obie strony wciąż korzystają ze starych radzieckich systemów bojowych, w których obowiązuje zasada, że jedna bateria artylerii samobieżnej potrzebuje aż 450 pocisków kal. 122 mm do zniszczenia pojedynczego celu. W wojskach lądowych USA problem ten został częściowo rozwiązany poprzez wprowadzenie precyzyjnych pocisków artyleryjskich takich jak M982 Excalibur kal. 155 czy pocisków GMLRS wystrzeliwanych z HIMARS. Są one jednak bardzo drogie i kosztują od kilku do kilkudziesięciu tysięcy dolarów za sztukę. Do tego należy dodać cenę całej armatohaubicy lub wyrzutni rakietowej, za pomocą której pociski są wystrzeliwane. Amerykańska M109 Paladin kosztuje 14 mln dolarów za sztukę, HIMARS z kolei – 20,7 mln. Andreika Vytis z Litewskich Sił Zbrojnych zwróciła z kolei uwagę na rosyjski punkt widzenia i postrzeganie przez nich UAV FPV. Jej zdaniem Rosjanie cenią sobie ich wykorzystanie, ponieważ zmusiły one Ukraińców do cofnięcia jednostek pancernych na odległość 3–10 km od linii frontu z obawy przed ich zniszczeniem. Stały się one bronią umożliwiającą eliminacje pojedynczych żołnierzy do 6 km w głąb na terytorium zajmowanym przez przeciwnika. Umożliwiły także izolowanie ukraińskich punktów oporu, przez co zaopatrywanie walczących żołnierzy jest możliwe wyłącznie pieszo lub poprzez specjalnie do tego przygotowane tunele „siatkowe".

Tomasz Wójtowicz

D. Hambling, *Could Small Drones Really Replace Artillery?*, https://www.forbes.com/sites/davidhambling/2023/08/16/could-small-drones-really-replace-artillery/ (dostęp 28.11.2025); K. Hird, R. Bailey, Ch. Harward, A. Evans, A. Ganzeveld, F.W. Kagan, *Russian Offensive Campaign Assessment*, 23.04.2024, https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_23-7/ (dostęp 29.11.2025); J. Jajcay, *I Fought in Ukraine and Here's Why FPV Drones Kind of Suck*, https://warontherocks.com/2025/06/i-fought-in-ukraine-and-heres-why-fpv-drones-kind-of-suck/ (dostęp 20.10.2025); B. Murray, *Beyond the Hype: Why Drones Cannot Replace Artillery*, https://smallwarsjournal.com/2025/05/05/beyond-the-hype-why-drones-cannot-replace-artillery/ (dostęp 28.11.2025); E. Schmidt, *The Future of War Has Come in Ukraine: Drone Swarms*, https://www.wsj.com/opinion/the-future-of-war-has-come-in-ukraine-drone-swarms-kamikaze-kyiv-31dd19d7 (dostęp 28.11.2025);

A. Vytis, *Russia's Changes in the Conduct of War Based on Lessons from Ukraine*, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2025/Lessons-from-Ukraine/ (dostęp 29.11.2025); Y. Zoria, *Expert: FPV drones can not replace artillery but are comparable with battalion mortar systems*, https://euromaidanpress.com/2024/01/19/expert-fpv-drones-can-not-replace-artillery-but-are-comparable-with-battalion-mortar-systems/ (dostęp 31.10.2025).

E

ETATYZM (fr. *état* – państwo) – koncepcja myśli politycznej, która traktuje państwo jako najwyższe osiągnięcie i cel rozwoju społecznego; doktryna podkreślająca wiodącą, często dominującą rolę państwa w społeczeństwie.

Ideowo-teoretyczne i metodologiczne podstawy etatyzmu kształtowały się od dawna, chociaż sam termin „etatyzm" pojawił się dopiero w latach 80. XIX w. we Francji. O ważnej roli państwa dla społeczeństwa pisali m.in. antyczni myśliciele. Starożytny grecki filozof Platon (około 427–347 p.n.e.) w swoim dziele *Państwo*, uzasadniając model idealnego ustroju politycznego, nakreślił utopijne państwo, w którym triumfują idee dobra i sprawiedliwości, a władzę sprawują prawdziwi filozofowie, ponieważ posiadają oni najwyższe cechy moralne. Oznacza to, że kierując się sprawiedliwością, to właśnie państwo rozwiązuje najważniejsze zadania stojące przed społeczeństwem, a mianowicie: ochronę ludzi, zapewnienie im dóbr materialnych, społeczno-ekonomicznych, stworzenie warunków dla ich twórczej działalności i rozwoju kulturalnego. Platon uważał, że to właśnie arystokraci, czyli najlepsi przedstawiciele państwa, mogą zaprowadzić porządek i osiągnąć sukces. Z kolei timokrację, oligarchię, tyranię, a nawet demokrację myśliciel odrzucał, ponieważ uważał, że te

formy państwa stanowią zagrożenie dla jego istnienia. Platon nadawał władcom nie tylko uprawnienia polityczne – oni określają, co jest dobrem i sprawiedliwością.

U Arystotelesa (384–322 p.n.e.) (traktat *Polityka*) państwo jest produktem naturalnego rozwoju, powstaje z potrzeby ludzi do dobrego życia. Idealne państwo, zdaniem myśliciela, pomaga obywatelom osiągnąć dobro społeczne. Najlepszą formą rządów była „politeja", czyli państwo rządzone przez „klasę średnią". Politeja, zgodnie z poglądami Arystotelesa, to swoiste połączenie oligarchii i demokracji. Arystoteles odrzucał monarchiczne i arystokratyczne formy rządów, które są sprzeczne z zasadą równości ludzi, natomiast demokracja, choć tłumaczona jako „władza ludu", chroni interesy i korzyści ubogich warstw społeczeństwa, uzależniając od siebie zamożnych obywateli. Oznacza to, że państwo u Arystotelesa jest ważne i naturalne, ale służy obywatelom i powinno być zrównoważone, a nie wszechwładne.

Poglądy filozoficzne włoskiego polityka i myśliciela Nicolo Machiavellego (1469–1527) przyczyniły się do umocnienia idei silnego, autonomicznego państwa, tzw. pragmatycznego etatyzmu, w którym państwo jest najwyższym podmiotem politycznym mającym prawo stosować siłę, oszustwo lub manipulację w celu swojego przetrwania. Machiavelli położył podwaliny pod zasadę celowości państwowej: życie, stabilność i potęga państwa są ważniejsze niż normy moralne pojedynczej osoby. W swoim dziele *Książę* (*Il Principe*, 1513) podkreślał, że władca ma prawo łamać przysięgi, stosować przemoc, manipulować ludźmi, jeśli zapewnia to bezpieczeństwo i jedność państwa. Machiavelli jako pierwszy oddzielił politykę od moralności i religii, twierdząc, że ta pierwsza ma swoje własne prawa, a skuteczne rządy zależą od efektywności, a nie moralności. Takie oddzielenie moralności od polityki stwarza przesłankę dla państwowego pragmatyzmu – ważne jest nie „dobro", ale „korzyść dla państwa". Jednocześnie Machiavelli nie negował znaczenia poparcia społecznego i instytucji republikańskich, dlatego jego etatyzm jest umiarkowany. Należy pamiętać, że jego idee były podyktowane konkretnymi wydarzeniami historycznymi, kiedy rozdrobnione ziemie włoskie cierpiały z powodu ciągłych wojen i najazdów z zewnątrz. Jego zdaniem tylko silna władza centralna mogła położyć kres chaosowi. Machiavelli nie propagował silnego

państwa w imię abstrakcyjnej zasady: jest to środek praktycznej polityki, sposób na zapewnienie porządku, stabilności politycznej, ochrony przed zewnętrznymi wrogami, stworzenie warunków do zjednoczenia kraju.

Idee angielskiego filozofa Thomasa Hobbesa (1588–1679) stworzyły podstawy teoretycznego fundamentu radykalnego etatyzmu. W traktacie *Lewiatan, czyli materia, forma i władza państwa kościelnego i świeckiego* (*Leviathan or The Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil*, 1651) Hobbes wykorzystał biblijny obraz Lewiatana jako metaforę potężnego państwa, które poskramia ludzką skłonność do konfliktu, anarchii i chaosu. W świecie, w którym panują strach, konkurencja i nieufność, silna władza jest nie tylko użyteczna, ale wręcz konieczna. Państwo określa, czym jest sprawiedliwość i prawo, co ludzie są zobowiązani robić, jakie wolności mogą posiadać. Naród nie może obalić władzy, ponieważ oznaczałoby to powrót do naturalnego stanu „wojny wszystkich przeciwko wszystkim". Państwo stoi ponad społeczeństwem. Jedyną granicą etatyzmu jest samozachowanie poddanego: człowiek może nie wykonać rozkazu suwerena, jeśli zagraża on jego życiu. Wszystko inne należy do sfery władzy Lewiatana.

Niemiecki filozof Georg Wilhelm Friedrich Hegel (1770–1831) stworzył koncepcję państwa, w której nie jest ono tylko instytucją, ale najwyższą formą urzeczywistnienia wolności, moralności i rozumu. Państwo stanowi wartość absolutną, stoi ponad jednostką i społeczeństwem obywatelskim, jest najwyższą formą moralności. U Hegla „państwo etyczne" (*sittliche Staat*) to takie, w którym urzeczywistniona jest jedność wolności osobistej i interesu ogólnego; prawo i moralność łączą się w spójny porządek; obywatele uznają prawa za własne. Pomimo wielkości państwa Hegel nie twierdził, że powinno ono kontrolować wszystko: uznawał autonomię rodziny, społeczeństwa obywatelskiego oraz korporacji gospodarczych. Uważał, że racjonalnie zorganizowana i silna władza państwowa jest warunkiem prawdziwej wolności, ponieważ może być ona realizowana jedynie w ramach porządku prawnego i moralnego ustanowionego przez państwo. Podkreślał również, że naród powinien uczestniczyć w tworzeniu prawa i podejmowaniu istotnych decyzji państwowych, ale nie bezpośrednio, lecz poprzez system instytucji przedstawicielskich. Takie właśnie państwo Hegel nazywał „moralnym" (etycznym), w którym łączą

się interesy prywatne i ogólne. W czasach nowożytnych ta heglowska koncepcja stała się jednym z intelektualnych źródeł współczesnego pojęcia państwa prawnego (*Rechtsstaat*), w którym rządy prawa gwarantują wolność jednostki, władza państwowa musi być racjonalna i legalna, a państwo nie jest despotą, lecz strukturą powołaną do realizacji dobra wspólnego.

Początki europejskiego etatyzmu są związane z kształtowaniem się nowoczesnego państwa zcentralizowanego. Instrumentem jego rozwoju stał się protekcjonizm, czyli kluczowy element polityki merkantylistycznej. Znani teoretycy merkantylizmu – Antonio Serra (poł. XVI – pocz. XVII w.), William Stafford (1554–1612), Johann Joachim Becher (1635–1682), Philipp Wilhelm von Hörnigk (1640–1714) oraz Wilhelm von Schröder (1640–1699) – widzieli w państwie główną siłę napędową rozwoju gospodarczego. Odmianą merkantylizmu była polityka kolbertyzmu: Jean-Baptiste Colbert (1619–1683) – minister finansów (kontroler generalny finansów) Francji Ludwika XIV – zreorganizował francuski system gospodarczy. Jego założeniem było wspieranie rodzimego przemysłu, handlu i zakładanie licznych manufaktur państwowych (królewskich), na uruchamianie których udzielał mieszczanom pożyczek. W efekcie francuski eksport miał przewagę nad importem. Od nazwiska twórcy system ten nazwano kolbertyzmem.

Etatyzm i protekcjonizm miały duże znaczenie dla rozwoju przemysłu pruskiego. Politykę tę rozwinął Friedrich List (1789–1846) – teoretyk „pruskiej drogi do kapitalizmu"; dlatego właśnie w Prusach funkcjonowało wiele przedsiębiorstw państwowych lub półpaństwowych (z udziałem kapitału państwowego). Udział państwa umożliwił także duże krótkoterminowe inwestycje kapitałowe w budowę infrastruktury.

Idea silnego racjonalnego państwa jako nosiciela interesu ogólnego została podjęta i rozwinięta przez wielu myślicieli oraz działaczy politycznych. W latach 80. XIX w. pojawił się termin „*etatyzm*", którego zaczęto używać we Francji na określenie doktryn podkreślających wiodącą rolę państwa w organizacji społeczeństwa. Uznaje się, że wzrostowi etatyzmu sprzyjają kryzysy polityczne i społeczno-ekonomiczne. Pojawienie się tego terminu wiąże się z debatami dotyczącymi rozszerzenia roli państwa we Francji po klęsce w wojnie francusko-pruskiej w latach 1870–1871,

reformach Trzeciej Republiki oraz dyskusjami o tym, w jakim stopniu państwo powinno ingerować w gospodarkę i życie społeczne.

Ideę etatyzmu przejęli i wykorzystali w praktyce tacy politycy, jak Otto von Bismarck (1865–1871) i Benjamin Disraeli (1804–1881). Podczas gdy liberałowie (np. znany zwolennik koncepcji liberalizmu gospodarczego, angielski ekonomista David Ricardo (1772–1823) – wolna przedsiębiorczość, wolny handel itd.) nalegali na minimalny udział państwa w życiu gospodarczym (*laissez-faire* – „pozwólcie działać"), politycy konserwatywni (Disraeli, Bismarck) dostrzegli w etatyzmie środek łagodzenia kwestii społecznej i zapobiegania tendencjom rewolucyjnym.

Bismarck na stanowisku pierwszego kanclerza Rzeszy Niemieckiej (1871–1890) również aktywnie stosował idee etatyzmu, traktując państwo jako główne narzędzie kształtowania narodu i konsolidacji społeczeństwa. Jego polityka podporządkowywała kluczowe sfery życia scentralizowanej kontroli, m.in. poprzez wprowadzenie państwowych programów socjalnych, ochrony celnej oraz wzmocnienie aparatu biurokratycznego. Bismarck dążył do tego, aby to państwo określało ramy lojalności politycznej, a nie poszczególne interesy regionalne czy wyznaniowe, co widoczne było zwłaszcza w jego walce z wpływami Kościoła katolickiego podczas Kulturkampfu. Bismarck uważał Kościół katolicki za potencjalnego rywala władzy państwowej; w ramach tej polityki wprowadzano państwową kontrolę nad edukacją, małżeństwem i mianowaniami kadrowymi w strukturach kościelnych, a także ograniczenia działalności zakonów katolickich.

Za rządów premiera Disraelego w latach 1874–1880 w Zjednoczonym Królestwie wyraźnie dostrzegalna była tendencja do wzmacniania roli państwa w życiu społecznym i gospodarczym, co pozwala także mówić o wprowadzaniu etatystycznych zasad w praktyce rządzenia. Disraeli odchodził od klasycznej doktryny *laissez-faire*, uważając, że państwo powinno aktywnie ingerować w celu poprawy warunków życia warstw robotniczych oraz zapewnienia stabilności społecznej. Jego reformy w zakresie ochrony pracy (Factory Act, 1874), polityki mieszkaniowej (Artisans' and Labourers' Dwellings Improvement Act, 1875), sanitarnych standardów (Public Health Act, 1875) oraz kontroli jakości towarów (Sale of Food and Drugs Act, 1875) znacznie rozszerzyły kompetencje aparatu państwowego i określiły nowe obowiązki rządu wobec społeczeństwa. Disraeli, wprowadzając tę

politykę, wychodził z zagrożenia podziału Wielkiej Brytanii na dwie nacje – bogatą i biedną – w wyniku nasilającej się industrializacji i nierówności. Równocześnie wzmacniał władzę imperialną (parlament w 1876 r. nadał królowej Wiktorii tytuł cesarzowej Indii, The Royal Titles Act) oraz symboliczny autorytet monarchii, co sprzyjało konsolidacji narodu wokół centrum państwowego.

Przykładem polityki państwowej opartej na etatyzmie był program rozwoju Turcji w okresie międzywojennym. Realizował go Mustafa Kemal Atatürk (1881–1938), pierwszy prezydent (1923–1938) Republiki Turcji, który dążył do przeprowadzenia modernizacji gospodarczej oraz wzmocnienia suwerenności narodowej kraju. Polityka ta znacznie różniła się od europejskich modeli: podstawą programu rozwoju państwa, przyjętego w 1931 r., Kemal uczynił sześć zasad: republikanizm (idea konstytucyjnej demokratycznej republiki jako alternatywa wobec osmańskiej monarchii absolutnej); nacjonalizm (powszechny dostęp każdego obywatela Turcji do dóbr intelektualnych i kulturowych; miał jednoczyć naród i umacniać tożsamość; wszyscy obywatele są równi bez względu na wyznawaną religię czy pochodzenie etniczne); etatyzm (budowa mieszanej gospodarki rynkowo-państwowej przy wiodącej roli państwa); równość, rządy ludu (walka z nierównością klasową i przywilejami stanowymi, rządy pochodzą od ludu i dlatego mają wyrażać jego wolę); sekularyzm (świecki charakter państwa i oddzielenie państwa od religii) oraz reformizm (kurs na westernizację i walkę z pozostałościami tradycyjnego społeczeństwa). Zasady te później zyskały nazwę „sześć strzał" (Altı Ok); zostały one także włączone do nowej wersji konstytucji Turcji z 1937 r. Do głównych cech etatyzmu należało silne państwo jako motor modernizacji – Kemal uważał, że powinno ono pełnić funkcje inwestora, regulatora oraz założyciela strategicznych przedsiębiorstw. W tym celu utworzono państwowe banki, zakłady przemysłowe oraz projekty infrastrukturalne. W stosunkowo krótkim czasie taka polityka doprowadziła do przyspieszonego rozwoju gospodarki tureckiej, a dopiero w okresie powojennym Turcja zrezygnowała z etatyzmu w polityce wewnętrznej.

Próbą instytucjonalnego i ekonomicznego przemyślenia roli państwa w warunkach postimperialnej fragmentacji oraz strukturalnej słabości gospodarki narodowej był polski etatyzm okresu międzywojennego. Polska

odzyskała nieodległość, ale palącym problemem stało się scalenie ziem porozbiorowych, z których każda trwała w odmiennym porządku politycznym, gospodarczym i kulturowym. Etatyzm był próbą zbudowania silnego, gospodarczo aktywnego państwa, które poprzez szeroko zakrojone interwencje dążyło do zrekompensowania strukturalnej słabości gospodarki oraz zapewnienia konsolidacji narodowej. W periodyzacji polityki gospodarczej rządów, uwzględniającej wzrost tendencji etatystycznych w II Rzeczypospolitej, wyróżnia się następujące okresy: 1918–1921 – etatyzm wojenny, 1921–1923 – likwidacja etatyzmu wojennego, 1923–1925 – etatyzm okresu stabilizacji, 1926–1930 – etatyzm wysokiej koniunktury, 1930–1936 – etatyzm kryzysowy, 1936–1939 – etatyzm zbrojeniowo-inwestycyjny (K. Dziewulski). Za cel analizy przyjęto tutaj przede wszystkim odgórnie inicjowane projekty modernizacyjne. Najistotniejsze z tej perspektywy wydają się okresy etatyzmu wojennego (1918–1921; tworzono wówczas zręby systemu gospodarczego) oraz zbrojeniowo-inwestycyjny (1936–1939; cechujący się najszerszym i stosunkowo skoordynowanym działaniem rządów). Dzięki technokratycznym inicjatywom wicepremiera i ministra gospodarki w latach 1935–1939 Eugeniusza Kwiatkowskiego (1888–1974), realizowanym poprzez rozwój Gdyni, działalność Banku Gospodarstwa Krajowego oraz projekt Centralnego Okręgu Przemysłowego, modernizacja nabrała szczególnej intensywności. Pomimo pewnych sukcesów etatyzm w międzywojennej Polsce miał istotne ograniczenia: wysokie koszty budżetowe, zależność od dotacji państwowych, niską wydajność sektora państwowego, co uniemożliwiało długoterminową stabilność gospodarczą. Etatyzm wiązał się również z koncentracją władzy politycznej: aparat sanacyjny coraz bardziej kontrolował gospodarkę, powoływał kierownictwo przedsiębiorstw państwowych i określał kierunki inwestycji. Tworzyło to podstawy dla biurokratyzacji, patronatu politycznego oraz nie zawsze efektywnego zarządzania. Współcześni badacze podkreślają podwójny charakter polskiego etatyzmu: z jednej strony, był ważnym katalizatorem modernizacji i rozwoju przemysłowego, z drugiej – prowadził do nadmiernej biurokratyzacji, politycznej centralizacji oraz ograniczenia dynamiki rynkowej.

Rozwój społeczeństw industrialnych, polityka masowa oraz kryzysy modernizacji sprzyjały powstawaniu ideologii, które głosiły absolutny

priorytet państwa nad jednostką. To właśnie w tych warunkach etatyzm stopniowo przekształcał się w formy, które nie były już ograniczane normami prawnymi ani moralnymi, i ujawnił się w kluczowych totalitarnych ideologiach początku XX w. – bolszewizmie/stalinizmie, faszyzmie oraz nazizmie. Różnego rodzaju modelami państwa stały się socjalizm państwowy, korporacjonizm, autorytaryzm. W bolszewizmie i stalinizmie priorytet państwa, któremu jednostka całkowicie się podporządkowuje, realizowany był poprzez kontrolę partyjno-biurową i scentralizowane zarządzanie; w faszyzmie (korporacjonistyczny model organizmu państwowego) – poprzez kult państwa jako duchowej jedności narodu; w nazizmie – poprzez dyktaturę rasową, która stawiała państwo w służbie ideologii rasowej.

Polski ekonomista Piotr Koryś, analizując etatyzm jako doktrynę gospodarczą i polityczną, podkreślił jego wewnętrzną sprzeczność oraz ograniczone możliwości funkcjonalne w długiej perspektywie. Analizując stosunek kosztów do korzyści interwencjonizmu państwowego, zaznacza, że krótkoterminowe efekty – takie jak mobilizacja zasobów, przyspieszona industrializacja czy tymczasowa stabilizacja kluczowych sektorów dzięki inwestycjom państwowym – nie rekompensują strukturalnych wad modelu. Zdaniem ekonomisty etatyzacja nieuchronnie wiąże się ze wzrostem nieefektywności gospodarczej, hamowaniem przedsiębiorczości, osłabieniem konkurencyjnego środowiska, nadmiernym obciążeniem budżetu państwa oraz powstawaniem instytucji podatnych na patronat polityczny i korupcję. Innymi słowy, nadmierna kontrola państwowa i własność państwowa w długim okresie mogą hamować wzrost gospodarczy. Koryś dochodzi do wniosku, że etatyzm nie jest gwarancją trwałego rozwoju gospodarczego, nawet jeśli na początku przynosi względne sukcesy. Etatyzm, zwłaszcza jako aktywna polityka gospodarcza w sektorze przemysłowym, sprawdzał się – przynajmniej częściowo – w warunkach kryzysów, wojen, autarkii gospodarczej, z reguły jako koło ratunkowe dla gospodarki.

Koryś uważa, że etatyzm jest raczej ideologią niż racjonalną strategią. Doświadczenie historyczne pokazuje, że model etatystycznego rozwoju jest w stanie zapewnić wzrost gospodarczy głównie w warunkach przejściowych lub wyjątkowych. Autor przytacza przykłady XX w., podkreślając, że strategie rozwojowe oparte na etatyzmie (ZSRR, Europa Wschodnia, Afryka Północna, Ameryka Południowa…) nie przynoszą długoterminowo pozytywnych

rezultatów. Inaczej jest w krajach słabiej rozwiniętych, peryferyjnych: tam państwo okresami stara się być liderem modernizacji – doganiania krajów wysoko rozwiniętych. Powodem są niedobory kapitału, brak – przynajmniej w percepcji elit politycznych – przedsiębiorców zdolnych podołać wyzwaniom rozwojowym. Może to prowadzić do powstania tzw. państw rozwojowych, jak stało się w Azji Południowo-Wschodniej, gdzie państwo wspiera przedsiębiorców i nominuje zwycięzców – branże i poszczególne firmy, które mają odnieść sukces. Zatem, według jego przekonania, etatyzm rzadko zapewnia trwały rozwój i nie jest optymalnym modelem dla współczesnych państw, chyba że jako tymczasowe narzędzie.

Do pewnego stopnia tendencje centralistyczne w Unii Europejskiej można również określić jako etatyzm. Janusz Heller, analizując pomiar wolności gospodarczej w krajach Unii Europejskiej na przełomie XX i XXI w., doszedł do wniosku, że spośród 15 krajów tzw. „starej" UE 10 należy do grupy bardziej liberalnych, a drugą stanowi 5 państw: Hiszpania, Francja, Portugalia, Włochy i Grecja. Polska, jego zdaniem, jest krajem o najwyższym poziomie etatyzmu spośród wszystkich członków UE. Opierając się na obowiązujących standardach, Heller charakteryzuje polską gospodarkę jako etatystyczną, z pewnymi, i to nielicznymi, elementami liberalizmu.

W europejskiej myśli etnopolitycznej drugiej połowy XX w. zaczęła dominować etatystyczna teoria narodu, która postrzega naród jako zbiór obywateli danego państwa, niezależnie od ich przynależności etnicznej, językowej, wyznaniowej czy innej. Innymi słowy, etatystyczna teoria narodu (lub państwowa) traktuje naród przede wszystkim jako polityczną wspólnotę obywateli, formowaną przez państwo i poprzez państwo. W centrum tego modelu znajduje się państwo jako podmiot kształtowania narodu, które ustanawia wspólne prawa, instytucje polityczne, prawa obywatelskie i symbole, a także zapewnia lojalność i integrację ludności. Taki naród nie wymaga wspólnego pochodzenia etnicznego ani jednej kultury – wystarczy udział polityczny, obywatelstwo i wspólna przynależność prawna.

Czołowy specjalista w zakresie powstawania i rozwoju narodów oraz nacjonalizmu Anthony Smith (1939–2016) wyróżnił dwa warianty ewolucji wspólnoty etnicznej w naród: proces mobilizacji kulturowo-ludowej oraz biurokratycznej inkorporacji. Pierwszy, oparty na kulturze, pochodzeniu i wspólnej mitologii, przeszła większość współczesnych państw narodowych.

Druga ścieżka, zdaniem Smitha, „rozpoczęła się na obrzeżach «lateralnych» etnosów – geograficznie rozległych, o nieostrych granicach i głównie ograniczonych do wyższych warstw społeczeństwa". Badacz uważał, że takim modelem była „większość Europy, który dalej istniał w części wschodniej kontynentu po pełnym ustanowieniu trzech wielkich imperiów – Habsburgów, Romanowych oraz Osmanów". Smith podkreślał przy tym, że procesy biurokratycznej inkorporacji przebiegały różnie; obejmowały znane działania państwotwórcze: tworzenie jednolitego kodeksu prawnego, systemu sądownictwa, podatków i polityki fiskalnej, budowę zintegrowanej sieci komunikacyjnej, modernizację aparatu administracyjnego oraz centralizację kontroli w rękach władcy, formowanie wykwalifikowanej kadry zawodowej dla kluczowych instytucji administracyjnych, a także tworzenie skutecznych instytucji i technologii wojskowych pod kontrolą centrum. Na późniejszym etapie do procesów państwotwórczych dołączono działania w zakresie ochrony socjalnej, prawa pracy, ubezpieczeń, opieki medycznej oraz edukacji.

Początkowo słowo *étatisme* miało wydźwięk krytyczny: oznaczało tendencję państwa do rozszerzania swoich kompetencji kosztem społeczeństwa i inicjatywy prywatnej. Dziś termin „etatyzm" używany jest w wielorakich kontekstach i nabiera różnych odcieni znaczeniowych. W środowisku naukowym ma przeważnie charakter opisowy i odnosi się do szerokiego spektrum modeli interwencji państwowej – od umiarkowanego podejścia regulacyjnego po system wszechstronnej kontroli. W debatach politycznych termin ten częściej wykorzystywany jest w sposób krytyczny, podkreślając ryzyko nadmiernej centralizacji i nieefektywności gospodarczej. W szerszym użyciu publicznym „etatyzm" może oznaczać zarówno ideologię silnego państwa, jak i praktykę rozrastania się instytucji państwowych, co czyni pojęcie wielowymiarowym i zależnym od kontekstu zastosowania.

Współczesne wyobrażenie o skuteczności współdziałania państwa i społeczeństwa zakłada wzajemną kontrolę i wzajemną pomoc. Kształtowanie się państwa socjalnego i prawnego w krajach rozwiniętych i rozwijających się odbywa się w oparciu o zasady i postulaty teorii liberalizmu społecznego, która uwzględnia zarówno aktywną rolę państwa w życiu społeczeństwa, jak i wartości liberalizmu (wolność, własność prywatna, konkurencja itp.).

Zoya Baran

K. Dziewulski, *Spór o etatyzm. Dyskusja wokół sektora państwowego w Polsce międzywojennej 1919–1939*, PWN, Warszawa 1981; J. Heller, *Liberalizm i etatyzm w praktyce gospodarczej krajów Unii Europejskiej*, „Archiwum" 2009, nr 3(37), https://studreg.uw.edu.pl/pl/archiwum,liberalizm-i-etatyzm-w-praktyce-gospodarczej-krajow-unii-europejskiej (dostęp 22.11.2025); P. Koryś, *ETATYZM ślepa uliczka: analiza kosztów i korzyści płynących z etatyzacji państwa*, https://wei.org.pl/wp-content/uploads/2021/01/Etatyzm-slepa-uliczka.pdf (dostęp 22.11.2025); W. Musiał, *Modernizacja Polski polityki rządowe w latach 1918–2004*, Wydawnictwo Naukowe UMK, Toruń, 2013; Е. Сміт, *Нації та націоналізм у глобальну епоху*, Переклад М. Климчука, Т. Цимбала, Ніка-Центр, Київ 2006.

ETNOPOPULIZM jest formą mobilizacji politycznej, w której przywódca zdobywa poparcie przede wszystkim wśród jednej grupy etnicznej, odwołując się do podziałów wspólnotowych i łącząc elementy nacjonalizmu z retoryką populistyczną. Zjawisko to pojawia się tam, gdzie ideologia narodowa splata się z populistycznym podkreślaniem konfliktu między „ludem" a „elitami". Jest to połączenie nacjonalizmu oraz populizmu.

W etnopopulizmie wszyscy twierdzą, że reprezentują jedyną „prawdziwą" grupę etniczną narodu, w której jej interesy są zagrożone przez wrogów z zewnątrz, czyli mniejszości, migrantów czy obcych państw, oraz z góry, czyli na przykład organizacji, elit krajowych czy instytucji międzynarodowych. Etnopopuliści uznają, że istnieje „prawdziwy naród" zagrożony przez mniejszości i chcą go chronić poprzez działania takie jak zamykanie granic, maksymalne zamykanie się w swojej kulturze czy chronienie tradycji.

Etnopopulizm rozwija się najsilniej tam, gdzie miasta mają duże znaczenie polityczne i gospodarcze, a migracja ludzi ze wsi do większych aglomeracji oraz wspieranie wsi sprawiają, że zaciera się umowna granica między nimi, zaś mieszkańcy wsi czują silniejszą przynależność do miast, co sprawia, że chętniej popierają partie populistyczne. Przywódcy etnopopulistyczni dążą do jawnego podzielenia obywateli na „naród" (poważni, zaangażowani członkowie narodu) oraz „obcych", których należy się wystrzegać i obawiać, bo zagrażają „narodowi". Tego rodzaju retoryka pozwala liderom etnopopulistycznym zyskać ogromne wpływy, ponieważ działa na silnych emocjach: poczuciu wspólnoty, strachu przed utratą tożsamości oraz potrzebie przynależności do większej grupy.

Partie etnopopulistyczne opierają się na „etnicznej" atrakcyjności przywódców i ich więzi z grupami. Liderzy tworzą narrację wykluczenia, w której jednoczą różne grupy społeczne poprzez opowieść o wspólnym zagrożeniu. Etnopopulizm ujawnia się głównie w okresach niepewności lub zagrożenia, kiedy to liderzy mogą zyskać poparcie poprzez przedstawienie określonych grup jako zagrożenia dla „narodu" i podsycanie obawy o „naród". Taka polityka może prowadzić do wykluczeń, podziałów społeczeństwa oraz pilnowania granic między grupami wewnętrznymi a zewnętrznymi. Także etnopopulizm opiera się na kilku powiązanych mechanizmach, strategiach i konsekwencjach, które razem kształtują jego specyficzny charakter. Zaczyna on swoje działanie od konstruowania „wewnętrznego ludu", czyli obrazu jednolitej i moralnie uprzywilejowanej grupy, zaś jej tożsamość nie wynika z cech etnicznych czy obywatelskich, lecz z wartości, stylu życia i postaw emocjonalnych.

Etnopopulizm upraszcza złożone procesy społeczne do łatwych do zrozumienia diagnoz i rozwiązań, a jednocześnie buduje poczucie wyjątkowości i misji „wewnętrznego ludu", który jest przedstawiany jako strażnik prawdziwych wartości. Strategie etnopopulistyczne obejmują podkreślanie kryzysu i upadku wspólnoty, stwarzają warunki do jej mobilizacji oraz oczyszczania poprzez wykluczanie wpływów grup uznanych za problematyczne, głównie na poziomie kulturowym. Konsekwencje etnopopulizmu to m.in. prowadzenie do fragmentacji, pogłębiając podziały i erozję więzi społecznych, ograniczanie zdolności do wypracowania kompromisowych rozwiązań, zaś poprzez stałe podkreślanie zagrożenia – utrwalanie poczucie permanentnego kryzysu i niepewności. W ten sposób powstają zamknięte bańki tożsamościowe, w których krąży homogenizowana i często niepełna interpretacja rzeczywistości. Zatem etnopopulizm to forma politycznej mobilizacji społeczeństwa, w której lider zdobywał poparcie określonej grupy, *stricte* odwołując się do więzi wspólnotowych. Najczęściej występuje, gdy nacjonalizm łączy się z treściami populistycznymi.

Etnopopuliści w swojej retoryce i działaniach stosują wiele technik manipulacyjnych, np. odwołują się do emocji, używając też demagogii, oskarżeń, potępienia i strachu. Lider przedstawia siebie jako reprezentanta „zwykłych ludzi", patriotów oraz uczciwych obywateli marginalizowanych

poprzez elity, które są obwiniane za realne problemy cywilizacyjne, takie jak wzrost bezrobocia i przestępczości lub napływ imigrantów. Etnopopuliści bardzo często wykorzystują nieprawdziwe historie religijne, polityczne i kulturowe, a także kryzysy społeczne i gospodarcze, kreując siebie na jedynych obrońców przed tymi niebezpieczeństwami, manipulują mediami poprzez selektywne powielanie nieprawdziwych informacji i kreowanie atmosfery, która powinna zwiększyć poparcie dla „obrońców narodu". Natomiast po zdobyciu władzy są w stanie ograniczyć niezależność sądów, mediów i innych instytucji, tłumacząc swoje decyzje obroną prawdziwych wartości. Skutecznie ograniczają możliwości partii opozycyjnych oraz liberalnych organizacji.

Etnopopulizm może przyjmować różne formy w zależności od danego regionu, np. w krajach wieloetnicznych, takich jak Ameryka, liderzy kreują koalicję między różnymi grupami etnicznymi przeciwko wspólnym elitom, natomiast w krajach europejskich ich narracja koncentruje się na zagrożeniu kulturowym czy religijnym, dlatego etnopopulizm w dzisiejszych czasach jest jednym z ważniejszych wyzwań dla współczesnej demokracji. Poprzez kreowanie wspólnego wroga wewnętrznego, jak i zewnętrznego etnopopuliści budują poczucie zagrożenia wśród społeczeństwa, co w efekcie działa na niekorzyść demokratycznych instytucji i pluralizm polityczny. Media i internet odgrywają w tym procesie kluczową rolę dzięki możliwości szybkiego rozpowszechniania informacji i fałszywej narracji, a kryzys społeczny i gospodarczy jest dla etnopopulistów okazją do umocnienia swojego wizerunku „obrońców jednostki". Z tego względu to właśnie społeczeństwo obywatelskie, doświadczenia historyczne i dobrze działające instytucje są kluczowe, aby zrozumieć i przeciwdziałać temu zjawisku. Etnopopulizm nie dominuje w społeczeństwie przez cały czas; ludność wydaje się bardziej podatna na dyskursy etnopopulistyczne w następstwie kryzysów globalnych i krajowych, takich jak wielki kryzys, koniec zimnej wojny czy wielka recesja w latach 2007–2009. Zjawiska te są określane mianem „ruchów kryzysu". W okresach wzmożonego braku bezpieczeństwa pojawiają się agenci polityczni, którzy zaspokajają oddolne żądania polityk faworyzujących grupę wewnętrzną. W kontekście afrykańskim strategie etnopopulistyczne są bardziej realne, gdy występują dwa warunki:

- oparcie społeczne łączące etniczny apel liderów do ich własnych społeczności z ogólnym przesłaniem populistycznym skutecznym w kosmopolitycznych ośrodkach miejskich;
- zdolność liderów do artykułowania wspólnych narracji wykluczenia w celu zintegrowania różnych elektoratów.

Pierwszą z charakterystycznych cech jest podwójna demagogia i narracja spisku: etnopopuliści łączą demagogię wymierzoną w narodowe grupy zewnętrzne z tą wymierzoną w elity. Populistyczna metanarracja zakłada, że „lud", politycznie związany z liderem, jest wyzyskiwany przez krajowe i globalne „elity". Nacjonalistyczna metanarracja utrzymuje, że członkowie „narodu" są zagrożeni przez „wrogie narody" lub „innych narodowych". Etnopopulizm miesza te zagrożenia, szerząc narracje, w których wrogowie z zewnątrz (np. migranci, imigranci, mniejszości etniczne) łączą się lub spiskują z wrogami z góry w celu podważenia lub denacjonalizacji narodu-ludu. Kolejna cecha to mobilizacja etniczna i definicja „ludu". Liderzy etnopopulistyczni wykorzystują symbole do mobilizowania ludności przeciwko postrzeganym zagrożeniom zagranicznym lub krajowym związanym z etnosem.

W niektórych przypadkach, zwłaszcza w Ameryce Łacińskiej i Afryce, „elity" są postrzegane nie tylko ekonomicznie, ale także etnicznie, np. lewicowy populistyczny lider Evo Morales w Boliwii przeciwstawił „lud" metyski i rdzenny przeważającej europejskiej „elicie". Choć w przypadku Boliwii nie towarzyszyło temu wykluczenie rasowe, celem było zbudowanie koalicji paneetnicznej przeciwko w dużej mierze europejskiej boliwijskiej elicie. W regionach bardziej jednorodnych etnicznie, takich jak Europa, ten etnopopulistyczny podział na „lud" i „elity" jest rzadszy, ponieważ zazwyczaj należą one do tej samej grupy etnicznej. Następna z cech to polityka i konsekwencje zdobycia władzy. Rządy nacjonalistyczne są bardziej skłonne do przyjmowania polityk faworyzujących członków narodowej grupy wewnętrznej, zarówno wewnątrz, jak i poza granicami państwa. Przykłady takiej polityki to wsparcie Moskwy dla rosyjskich separatystów w Donbasie i na Krymie, a także wsparcie Belgradu dla Serbów w Kosowie i Bośni w latach 90. Gdy etnopopuliści zdobywają dostęp do władzy państwowej, mają tendencję do podsycania paranoi i odczłowieczania grup zewnętrznych. Może to prowadzić do drakońskich

polityk państwowych mających na celu pilnowanie granicy między grupami wewnętrznymi a zewnętrznymi.

Etnopopulizm, choć bywa przedstawiany jako obrona narodu, realnie wpływa na osłabienie społeczeństwa i struktur państwowych. Zamiast budować poczucie wspólnoty, wzmacnia konflikty i utrwala wzajemną wrogość. Podobnie jak inne ideologie oparte na wykluczeniu, prowadzi do osłabienia zaufania do instytucji demokratycznych, dlatego jest uznawany za jedno z kluczowych zagrożeń dla stabilności politycznej – zwłaszcza w państwach wieloetnicznych.

Żanna Osikowicz

B. Bonikowski, *Ethno-Nationalist Populism and the Mobilization of Collective Resentment*, „The British Journal of Sociology" 2017, vol. 68, https://doi.org/10.1111/1468-4446.12325; R. Brubaker, *Why populism?*, „Theory and Society" 2017, vol. 46, no. 5; J. Chennattuserry, M. Deshpande, P. Hong, *Encyklopedia Nowego Populizmu i Reakcji w XXI wieku*, Springer, Singapur 2024; E. Laclau, *Rozum populistyczny*, Wydawnictwo DSWE, Wrocław 2009; A. Lipiński, *Populizm a medialne struktury możliwości. Przypadek nowych mediów*, Uniwersytet im. Adama Mickiewicza w Poznaniu, Poznań 2020; A. Lipiński, A. Stępińska, *Badania nad dyskursem populistycznym: wybrane podejścia*, Wydawnictwo Naukowe Wydziału Nauk Politycznych i Dziennikarstwa, Poznań 2020; C. Mudde, *Populism. A Very Short Introduction*, Oxford University Press, Oxford 2017; A. Murzańska, *Badania nad populizmem w Polsce*, KSM, Kraków 2011; M. Vachudova, *Ethnopopulism and democratic backsliding in Central Europe*, „East European Politics" 2020.

EUROPEJSKIE SOJUSZE PRZEMYSŁOWE NA RZECZ MAŁYCH REAKTORÓW MODUŁOWYCH (SMR) – różnorakie działania na rzecz wsparcia sektora energetycznego świadczą o zmianie podejścia Unii Europejskiej do innych rodzajów źródeł energetycznych, które przez lata owiane złą sławą były wykluczane, m.in. energetyka jądrowa. Do tej pory założenia Unii Europejskiej oraz krajów Europy opierały się przede wszystkim na wykorzystaniu odnawialnych źródeł energetycznych w transformacji na rzecz klimatu. W 2022 r. UE przyjęła rozwiązania, które dodały gaz ziemny oraz energię jądrową do technologii zrównoważonych. Ramy ułatwiające zrównoważenie inwestycji oraz finansowanie ze środków budżetowych ustanawiają

tzw. taksonomię działania dla krajów członkowskich, umożliwiając im wdrażanie nowych technologii, w tym właśnie SMR.

Wsparciem dla transformacji energetycznej Europy było przyjęcie rozporządzenie Net-Zero Industry Act, które zawiera postulaty wykonawcze dla neutralnego emisyjnie przemysłu. Procedowanie założeń we Wspólnocie polegało na uzgodnieniu pomiędzy Radą UE a Parlamentem Europejskim wspólnego stanowiska, które w rezultacie było uznaniem energetyki jądrowej za neutralną emisyjnie i potraktowania tej gałęzi energetycznej na równi z OZE. Stanowi to jak dotychczas precedens w najnowszej polityce europejskiej. Założenia aktu o neutralności ustalają mechanizmy wspierające rynek energetyczny we wdrażaniu technologii niskoemisyjnych poprzez m.in. uproszczenie procedur dla realizacji wskazań Europejskiego Zielonego Ładu – czyli w konsekwencji osiągnięcie neutralności klimatycznej w Europie do 2050 r.

Zwiększenie produkcji energii ze źródeł neutralnych do 40% rocznego zapotrzebowania jest odpowiedzią na szerokie działanie Chin i USA, które sukcesywnie wzmacniają rozwój niskoemisyjnych rozwiązań, konkurując technologicznie na rynku światowym. W związku z dekarbonizacją Komisja Europejska w lutym 2024 r. opublikowała rekomendacje dla wsparcia rozwoju sektora energetyki jądrowej poprzez uruchomienie małych reaktorów modułowych SMR (Small Modular Reactors). Zmiany, jakie zaszły w postrzeganiu rozwoju energii jądrowej, ułatwiają i przyspieszają rozwój oraz uruchomienie SMR w Europie, co sprzyjać będzie wzrostowi neutralności klimatycznej.

Małe reaktory modułowe mogą być kluczowym elementem we wsparciu zapotrzebowania na czystą energię elektryczną i duże ilości wodoru. Mogą być również uzupełnieniem dla konwencjonalnych elektrowni jądrowych, a także – obok OZE – przyczyniać się do działań łagodzących zmiany klimatyczne i propagowania kwestii zrównoważonego rozwoju poprzez niezawodną, spójną i bezpieczną kogenerację niskoemisyjnej energii elektrycznej i ciepła. Dla poparcia zamiarów wdrażania nowoczesnych technologii w tym zakresie w dniach 29–30 maja 2024 r. w Brukseli odbyło się spotkanie Zgromadzenia Ogólnego, w którym uczestniczyli członkowie sojuszu oraz przedstawiciele krajów UE i Komisji Europejskiej.

Zawarto postanowienia o utworzeniu 8 Technicznych Grup Roboczych (TWG), które mają usprawnić wdrażanie technologii SMR, tj.:

- TWG1: Zastosowania przemysłowe;
- TWG2: Technologia i badania, rozwój i innowacje;
- TWG3: Łańcuch dostaw;
- TWG4: Umiejętności;
- TWG5: Zaangażowanie społeczne;
- TWG6: Bezpieczeństwo jądrowe i zabezpieczenia;
- TWG7: Cykl paliwowy i gospodarka odpadami;
- TWG8: Finansowanie.

Aspektem, który zmienił postrzeganie energetyki jądrowej, było założenie nieformalnego sojuszu atomowego pod przewodnictwem Francji, którego celem jest zmiana polityki europejskiej w dążeniu do zwiększenia użyteczności potencjału nuklearnego w miksach energetycznych krajów Europy. W ramach sojuszu spotykają się przedstawiciele państw, które zadeklarowały się współpracować w procesie decyzyjnym oraz prawodawczym celem wsparcia odnawialnych źródeł energii poprzez zwiększenie udziału energetyki jądrowej. Działania prezydenta Emmanuela Macrona oraz rządu i administracji francuskiej odgrywają kluczową rolę w przeorganizowaniu europejskiej polityki na rzecz wsparcia atomu. Proatomowy kurs jest nakierowany na maksymalizację wykorzystania atomu do produkcji energii elektrycznej nawet kosztem spadku udziału OZE.

Zainteresowanie SMR powoduje rywalizację na rynku w celu stworzenia konkurencyjnych rozwiązań technologicznych, m.in. USA, Francja, Rosja, Chiny, Korea Południowa czy Japonia i Kanada. Obszarem rywalizacji jest próba stworzenia najlepszych rozwiązań dla czwartej generacji reaktorów, które mają wyjść naprzeciw tradycyjnym rozwiązaniom funkcjonującym obecnie w tym obszarze, tj. bezpieczeństwo, odporność na proliferację, zarządzanie odpadami w sposób ekologiczny. Obszarem, w którym przejawia się również konkurencyjność, jest stworzenie optymalnych rozwiązań dla cykli paliwowych, zmniejszających ilość odpadów, m.in. obieg zamknięty, techniki recyklingu czy wykorzystanie toru.

Należy zwrócić tutaj uwagę na rywalizowanie w kwestii dostawców technologii SMR (Small Modular Reactor), które mają być niewielkich rozmiarów i względnie małej mocy – 50–500 MW. Modułowość oznacza

budowę na podstawie seryjnie produkowanych elementów, które charakteryzują się łatwością w transporcie oraz możliwość złożenia na miejscu eksploatacji reaktora. Zamysł tego typu instalacji spowoduje zmniejszenie kosztów w produkcji reaktorów oraz umożliwi instalację w miejscach największego zapotrzebowania, np. fabryki – którym to będą dostarczać energię cieplną i elektryczną.

Konkurencyjność polega na stworzeniu nowych rozwiązań, które zawierają w technologii takie rozwiązania jak:

- land-based, water-cooled SMRs: technologie montowane na lądzie, chłodzone zwykłą wodą, które wykorzystują technologię reaktorów klasycznych chłodzonych lekką i ciężką wodą (zintegrowany system obecnie jest budowany w Argentynie i przewidziany czas uruchomienia to 2028 r.). Zintegrowany system chłodzenia wodą to rozwiązania zaproponowane przez Chiny, USA, Argentynę, Francję, Szwajcarię, Arabię Saudyjską czy Zjednoczone Królestwo;
- marine-based, water-cooled SMRs: reaktory chłodzone wodą, jednakże umiejscowione w bliskości morza lub na morzu; również jednostki energetyczne pływające zamontowane na barkach. Technologia ta została zaproponowana do wdrożenia przez Federację Rosyjską, a także Chiny, USA czy Koreę Południową;
- gas-cooled SMRs: małe reaktory chłodzone gazem. Obecnie w fazie rozwoju lub eksploatacji znajduje się 14 takich rozwiązań wysokotemperaturowych, a dostarczane ciepło to temperatura powyżej 750°C służąca do wydajnego wytwarzania energii elektrycznej oraz zastosowań przemysłowych i kogeneracji. Szczególną uwagę przykuwa reaktor z modułem kulkowym HTR-PM, który jest zlokalizowany w Chinach i który został podłączony do sieci w 2021 r., a od 2022 działa z pełną mocą. Tymi technologiami pod kątem badawczym zajmują się takie kraje jak Japonia, Chiny, USA, Polska czy Indonezja.

Zawiązanie Europejskiego Sojuszu Przemysłowego na rzecz Małych Reaktorów Modułowych ma na celu ułatwienie i przyspieszenie dekarbonizacji oraz zwiększenie niskoemisyjnych źródeł energii w Europie na

rzecz neutralności klimatycznej. Oczekuje się, że SMR pomogą zaspokoić wysokie zapotrzebowanie na czystą energię elektryczną i duże ilości wodoru. Sojusz to transparentna europejska platforma, która jest otwarta dla wszystkich podmiotów sektora publicznego i prywatnego spełniających kryteria regulaminowe, odpowiadające za prowadzenie działalności gospodarczej i zawodowej.

Aby osiągnąć cele neutralności klimatycznej ze wsparciem SMR, sojusz opracował strategiczny plan działania, aby przede wszystkim:

- identyfikować najbardziej opłacalne i obiecujące technologie SMR;
- wspierać i wzmacniać europejski łańcuch dostaw paliwowych;
- identyfikować występujące bariery inwestycyjne oraz analizować i łączyć finansowania na potrzeby rozwoju SMR;
- informować oraz angażować potencjalnych usługodawców, takich jak producenci w sektorze energetycznym czy producenci wodoru;
- określić potrzeby dla przyszłości w zakresie modernizowania technologii SMR oraz AMR;
- wzmocnić kontakty i wymianę doświadczeń pomiędzy organami ds. bezpieczeństwa jądrowego;
- promować zaangażowanie społeczeństwa oraz zwiększać świadomość wśród lokalnych społeczności;
- ułatwiać utworzenie Akademii Umiejętności Jądrowych w celu zwiększenia rozwoju kompetencji i umiejętności praktycznych obsługi nowoczesnych technologii;
- współpracować z odpowiednimi organami międzynarodowymi, aby pomóc europejskim projektom SMR dotrzeć na rynki międzynarodowe.

Polska jako kraj, który w swojej polityce energetycznej planuje uruchomienie pierwszej elektrowni jądrowej, również włączył się w prace badawcze nad rozwiązaniami SMR. Zespół ekspertów z Narodowego Centrum Badań Jądrowych, posiadając doświadczenie w pracy reaktora badawczego MARIA działającego od ponad 50 lat w Świerku oraz rozwiązań technologicznych zaproponowanych przez Japonię – HTTR, opracował koncepcję polskiego demonstracyjno-badawczego reaktora HTGR-POLA (POLski

Atomowy). Obecnie projekt jest na poziomie opracowania ogólnego, podstawowego wraz z założeniem podstawowych rozwiązań WRB (Wstępny Raport Bezpieczeństwa), który pozwoli na uzyskanie licencji oraz dalszych prac projektowych, aż po budowę i uruchomienie w przyszłości. Reaktor POLa ma stać się prototypem dla reaktorów komercyjnych, których uruchomienie pozwoli na uzyskiwanie energii elektrycznej oraz cieplnej mogącej być wykorzystywaną w polskich zakładach przemysłowych.

- *liquid metal-cooled*, *fast-neutron* SMRs: rodzaj reaktorów, które wykorzystują szybkie neutrony z chłodziwem w postaci ciekłych metali, np. sodu czy ołowiu. Zaletą tego rozwiązania jest praca przy wysokiej temperaturze, wysoka wydajność i możliwość przekształcania odpadów promieniotwórczych w użyteczne paliwo. Dodatkowo reaktor posiada paliwowy cykl zamknięty. Wymaga on jednak dopracowania, aby dopuścić do użytku paliwa pochodzące z recyklingu. Obecnie technologiami oraz tworzeniem prototypów zajmuje się Francja, Szwecja, Kanada i Włochy;
- *molten salt* SMRs: reaktor wykorzystujący paliwo i chłodziwa w postaci stopionej soli stanowi 1 z 6 projektów reaktorów modułowych czwartej generacji. W założeniach reaktory te powinny zapewnić większe bezpieczeństwo, wysoką wydajność i elastyczne cykle paliwowe. Prototypy oraz projekty zostają wdrażane sukcesywnie w Kanadzie, Danii, Francji, USA czy Zjednoczonym Królestwie. Jeden z projektów w 2024 r. wszedł w fazę budowy w Stanach Zjednoczonych;
- *microreactors*: projekty malutkich reaktorów do 30 MW i wykorzystujących miks czynników chłodzących, np. wodę lekką, hel, stopioną sól czy ciekły metal. Są to rozwiązania obecnie w fazie projektów, a rezultaty w postaci trwałych rektorów mają usprawnić działanie niszowych rynków czy oddalone obszary od wielkich aglomeracji.

W Polsce sojusze koncentrują się na współpracy z amerykańskimi i kanadyjskimi dostawcami, a głównym powiązaniem jest Orlen Synthos Green Energy (OSGE), który planuje budowę małych reaktorów BWR-300.

Inne inicjatywy obejmują współpracę na linii KGHM z NuScale, niemniej zawirowania organizacyjne z 2023 r. podważają realizację projektu.

Projekty realizowane przez OSGE oraz GE Hitachi Nuclear Energy zainicjowane zostały w maju 2023 r. Prezes PAA wydał ogólną opinię, która potwierdziła zasadność budowania małych SMR oraz prawidłowość dla przedstawionego projektu firmy dla reaktora BWRX-300 pod kątem spełnienia wymagań bezpieczeństwa. W grudniu tego samego roku uzyskano 6 decyzji środowiskowych i zasadniczych dla budowy łącznie 24 reaktorów tego typu w miejscowościach: Ostrołęka, Włocławek, Stawy Monowskie, Dąbrowa Górnicza, Kraków, Tarnobrzeg-Stalowa Wola. Kolejne miesiące współpracy doprowadziły do określenia przez GDOŚ wymań dotyczących zakresu raportu środowiskowego, a z końcem 2024 r. uzyskano akceptację KE dla wniosku o powołanie Projektowej Grupy Roboczej w ramach Europejskiego Sojuszu Przemysłowego na rzecz SMR. Jest to decyzja, która potwierdza realność technologii BWRX-300 i wdrożenie jej w UE na początku lat 30. Grupa podpisała również umowę z kanadyjską spółką Laurentis Energy Partners dotyczącą współpracy w zakresie przygotowania pierwszego w UE Wstępnego Raportu Bezpieczeństwa (Preliminary Safety Analysis Report – PSAR) dla technologii SMR. OSGE z końcem 2025 r. zawarła także umowy wspierające z francuską Grupą Orano, uznaną za globalnego lidera w dziedzinie materiałów paliwowych. Partnerstwo wesprze program cyklu paliwowego SMR i przyczyni się do solidnego europejskiego łańcucha dostaw.

Projektem, również realizowanym na gruncie polskim, jest współpraca KGHM i NuScale Power, które rozpoczęły działanie również w 2023 r. MKiŚ w połowie 2023 r. wydało decyzję dla instalacji VOYGR na moc 462 MW, która miała się składać z 6 reaktorów NuScale NPM-20 o mocy 77 MW każda. Lokalizację wybudowania tych modułów wyznaczono na Lubasz i Wieleń, w województwie wielkopolskim. Zawirowania dotyczące współpracy tych dwóch spółek nie dają jednoznacznie odpowiedzi, czy są realne szanse na powstanie reaktorów NuScale, gdyż spółka KGHM oznajmiła, że rozpatruje również inne rozwiązania od zupełnie różnych dostawców technologicznych. Doniesienia prasowe informują natomiast o wycofaniu się spółki z realizacji celów SMR z uwagi na wysokie koszty

(pomimo uzyskania pozytywnych opinii PAA w zakresie bezpieczeństwa), jednakże nie zostają one jednoznacznie potwierdzone.

Kolejnym punktem działania w ramach współpracy międzynarodowej jest projekt realizowany przez ŚGPI i Rolls-Royce. Stosunkowo nowy pomysł wszedł w obieg z początkiem 2024 r., kiedy ŚGP Industria uzyskała decyzję zasadniczą PAA dla budowy SMR wykorzystującą technologię Rolls-Royce SMRTM o łącznej mocy elektrycznej 940 MWe netto i mocy cieplnej 2716 MWt netto. Zaproponowano lokalizację modułów w województwie świętokrzyskim, w gminach Chmielnik i Daleszyce.

Wsparcie miksu energetycznego rozwiązaniami z zakresu SMR nakłada dodatkowe zobowiązania dotyczące nie tylko współpracy pomiędzy krajami członkowskimi, ale również na arenie międzynarodowej. Rozwój sojuszu pozwoli kształcić kadry, modyfikować technologie oraz wspierać główny rozwój energetyki jądrowej w krajach, przyczyniając się do polepszenia warunków klimatycznych. W przyszłości zastosowane technologie w małych SMR, jeśli uzyskają pozytywne wyniki testów rozruchowych, jako jedne z niewielu na świecie nie będą produkować odpadów promieniotwórczych w tzw. zamkniętym cyklu paliwowym, dla reaktorów chłodzonych odpowiednio solami lub wodorem. SMR to technologia przyszłości, która może przyczynić się do zniwelowania skutków degradacji środowiska i przyczynić się do szybszego osiągnięcia celu, jakim jest neutralność klimatyczna dla Europy.

Justyna Rokitowska

A. Boettcher, NCBJ, *Reaktory wysokotemperaturowe: technologia, zastosowanie i projekt HTGR-POLA*, [w:] *Małe reaktory atomowe jako katalizator zmian*, Z. Krysiak (red.), Stowarzyszenie Absolwentów i Przyjaciół Wydziału Prawa Uniwersytetu Lubelskiego, Lublin 2025; M. Dąbrowski, M. Skrzypek, D. Muszyński, J. Malesa, *HTGR-POLA as the forerunner for high temperature nuclear poligeneration for industry in Poland and Europe*, https://fisa-euradwaste2025.ncbj.gov.pl/sites/fisa-euradwaste2025.ncbj.gov.pl/files/2025-05/146_poster.pdf (dostęp 29.01.2026); *Energetyka Jądrowa w Polsce. Ocena gotowości do budowy pierwszej elektrowni 2025* [raport], https://www.bakermckenzie.com/-/media/files/locations/poland/nuclear-energy-in-poland/baker-mckenzie-polityka-insight-raport-energetyka-jdrowa-w-polsce-2025_pl.pdf (dostęp 15.01.2026); A. Juszczak, *Perspektywy wykorzystania reaktorów SMR w polskiej transformacji energetycznej*, https://pie.

net.pl/wp-content/uploads/2023/06/Reaktory-SMR.pdf (dostęp 29.01.2026); *Orlen Synthos Green Energy*, Aktualności 2023–2025, https://osge.com/orano-wesprze-sge-i-osge-w-budowie-floty-bwrx-300-w-europie-srodkowo-wschodniej/ (dostęp 30.12.2025); F. Reitsma, *Small Modular Reactors and Generation-IV. A short overview*, https://indico.ictp.it/event/8725/session/1/contribution/2/material/slides/0.pdf (dostęp 12.12.2025); *Sodium Fast Reaktor*, https://www.gen-4.org/generation-iv-criteria-and-technologies/sodium-fast-reactor (dostęp 13.12.2025); *Suistainable Nuclear Energy Technology Platform, European Industrial Alliance on SMRs*, https://ec.europa.eu/docsroom/documents/64094/attachments/1/translations/en/renditions/native (dostęp 28.12.2025).

EUROPEJSKI KORPUS SOLIDARNOŚCI (EKS) (ang. European Solidarity Corps) – został zainagurowany przez Komisję Europejską w 2016 r.; do tego czasu funkcjonował jako Wolontariat Europejski (European Voluntary Service, EVS). Celem ESC było umożliwienie młodym ludziom, zwłaszcza w wieku od 18 do 30 lat, rozwoju osobistego i zawodowego. Z tego względu w latach 2018–2020 mogli oni uczestniczyć w trzech kategoriach działań, tj. projektach wolontariatu, stażach i miejscach pracy oraz projektach solidarności. Działania organizacji skupiają się na pomocy pokrzywdzonym, ruchom na rzecz zdrowia oraz środowiska, a także pomocy humanitarnej. Organizacja rozpoczęła swoje działania w 2018 r. Nieodłącznym elementem Europejskiego Korpusu Solidarności jest Narodowa Agencja programu – w Polsce tę rolę pełni Fundacja Rozwoju Systemu Edukacji (FRSE). To połączenie jest konieczne ze względu na to, że Komisja Europejska powierza zarządzanie programem agencjom narodowym. Do powierzanych im zadań należą:

- zarządzanie sprawiedliwym i przejrzystym procesem oceny wniosków o dofinansowanie;
- monitorowanie procesu wdrażania Europejskiego Korpusu Solidarności;
- współpraca z innymi Narodowymi Agencjami programu i Komisją Europejską;
- informowanie na temat Europejskiego Korpusu Solidarności.

Do 2020 r. Komisja Europejska przewidziała na te działania budżet w wysokości 376,5 mln euro, w tym w 2018 r. – 44,25 mln euro. 15 kwietnia 2021 r. Komisja Europejska przyjęła dokument będący programem pracy

Europejskiego Korpusu Solidarności w nowej perspektywie finansowej, tj. na lata 2021–2027. Budżet programu został zaplanowany na 1 mld 9 mln euro. Działania realizowane w ramach ESC uległy lekkiej modyfikacji, mianowicie – objęły wolontariat, projekty solidarności oraz pomoc humanitarną. Tym samym Komisja Europejska zdecydowała, że działania takie jak staże i miejsca pracy, które funkcjonowały w ramach Europejskiego Korpusu Solidarności w latach 2018–2020, nie są obecnie już kontynuowane. Wspomniane trzy działania realizowane w latach 2021–2027 są w dalszym ciągu adresowane do młodzieży oraz organizacji, których profil dotyczy współpracy z nią.

Dodatkowo agencje mają za zadanie wspierać projekty wraz z monitorowaniem ich realizacji oraz jakości prowadzenia, ich działania skupiają się również na promowaniu EKS wśród młodzieży, szczególnie z mniejszymi szansami udziału w programie, podejmowaniu działań przyczyniających się do wzrostu wpływu EKS. Narodowa Agencja Programu Erasmus+ i Europejskiego Korpusu Solidarności współpracuje również z innymi programami edukacyjnymi w ramach FRSE, np. Erasmus+, EDU, European Language Label. Jednym z najważniejszych celów EKS w Polsce jest zrównoważony dostęp młodych ludzi do możliwości EKS. Do zadań EKS należą również:

- rozwój transformacji cyfrowej wraz ze wspieraniem projektów skupiających się na rozwijaniu umiejętności i wiedzy cyfrowej, a także wiedzy na temat zagrożeń tego rodzaju;
- promowanie zaangażowania młodych ludzi w procesy demokratyczne, ułatwianie aktywności społecznej;
- wspieranie projektów w obszarze wyzwań zdrowotnych.

Realnymi przykładami działań EKS są:

- wolontariat;
- projekty solidarności (działanie oraz tworzenie projektów, które mają na celu sprostanie kluczowym wyzwaniom społecznym);
- pomoc humanitarna (prowadzenie działań pomocy humanitarnej w państwach trzecich).

Formami udziału w programie są wolontariat, projekty solidarnościowe czy też staże w organizacjach wspierające cele społeczne. Należy

także wymienić rodzaje projektów, które realizowane są w ramach EKS, mianowicie:

- kultura (w formie pomocy przy organizacji wydarzeń, tworzenie warsztatów artystycznych);
- włączenie społeczne (np. pomoc w centrum dla uchodźców);
- projekty lokalne o charakterze solidarnościowym (np. przeciwdziałanie samotności osób starszych);
- ochrona środowiska (np. opieka nad zwierzętami, prace w rezerwatach przyrody).

Ponadto poza agencjami narodowymi w proces wdrażania EKS włączone są również takie podmioty, jak:

- centra zasobów, które stanowią środki jakości oraz wsparcia (przykładem jest sieć centrów w ramach programu Erasmus+ lub Centrum Zasobów Europejskiego Korpusu Solidarności) i wykonują działania w zakresie chociażby realizacji projektów;
- Centra Zasobów Salto, które służą poprawie jakości projektów poprzez dostarczanie odpowiednich materiałów, informacji i szkoleń agencjom narodowym. Ich działalność jest powiązana z EKS i dotyczy m.in. przyznawania i monitorowania znaku jakości w państwach niestowarzyszonych z programem, wspierania wymiaru włączenia społecznego w ramach korpusu i wdrażania Strategii na rzecz włączenia społecznego i różnorodności;
- Centrum Zasobów Europejskiego Korpusu Solidarności, które wspiera agencje narodowe, ale również osoby młode biorące udział w EKS poprzez organizowanie szkoleń i wizyt studyjnych, wydawanie praktycznych publikacji, ale i wytycznych na temat solidarności, przyczynianie się do tworzenia sieci społeczności w ramach EKS, co obejmuje organizacje, mentorów i osoby szkolące;
- sieć Eurodesk wspierająca poprzez dostarczanie usług informacyjnych (dla pracowników, ale również młodzieży), dotyczących finansowania, publikacji i organizowanych wydarzeń, a także odpowiadająca na zapytania. Sieć Eurodesk obecna jest

we wszystkich uczestniczących krajach EKS i koordynowana na szczeblu europejskim w Brukseli;

– Europejski Portal Młodzieży (portal) odpowiada za udzielanie przede wszystkim młodym ludziom zamieszkującym Europę informacji na temat zaangażowania w projekt, jakim jest EKS. Osoby chcące wziąć udział w działaniu wolontariatu muszą być w wieku od 18 do 30 lat i zamieszkiwać jeden z 27 krajów Unii Europejskiej (UE) lub też objęty programem (państwa stowarzyszone z programem, tj. Islandia, Lichtenstein, Macedonia Północna, Turcja, jak i niestowarzyszone, tj. Albania, Algieria, Armenia, Azerbejdżan, Białoruś, Bośnia i Hercegowina, Czarnogóra, Egipt, Gruzja, Izrael, Jordania, Kosowo, Liban, Libia, Maroko, Mołdawia, Norwegia, Palestyna, Rosja, Serbia, Syria, Tunezja, Ukraina). Ze względu na sytuację polityczną mającą miejsce po wybuchu pełnoskalowej wojny w Ukrainie w 2022 r. Rosja jeszcze w kwietniu 2022 r. została wykluczona z działań ESC, natomiast uczestnictwo Białorusi uległo pewnym ograniczeniom.

Decydując się na udział w projekcie, młodzież może podjąć się wolontariatu indywidualnego lub też grupowego. Indywidualny trwa od 2 tygodni do 12 miesięcy; najczęściej odbywa się za granicą, chociaż może być podejmowany także w kraju pochodzenia wolontariusza, w pełnym wymiarze godzin, tj. od 30 do 38 tygodniowo. Wolontariusz z założenia pracuje indywidualnie, chociaż bardzo często zdarza się, że podejmuje on współpracę także z innymi jednostkami. Wolontariat grupowy podobnie jak indywidualny najczęściej jest realizowany poza granicami kraju, jednakże może się on odbywać także w kraju pochodzenia wolontariusza. Również trwa on od 30 do 38 godzin tygodniowo.

Różnica pomiędzy wolontariatem grupowym a indywidualnym polega przede wszystkim na czasie realizacji, gdyż trwa on od 2 tygodni do 2 miesięcy, a także na specyfice działalności, która bazuje na współpracy z innymi wolontariuszami z różnych krajów. Grupa musi liczyć co najmniej 5 wolontariuszy z co najmniej 2 krajów. Projekty w ramach wolontariatu grupowego muszą dotyczyć realizacji wspólnych europejskich celów, które są wyznaczane co roku na szczeblu UE. Realizacja wolontariatu nie byłaby

możliwa bez udziału organizacji – by te mogły zostać uczestnikami działań Europejskiego Korpusu Solidarności, muszą nie tylko ukierunkowywać się na współpracę z młodzieżą, lecz również mieć doświadczenie w takich obszarach jak promowanie uczestnictwa w życiu demokratycznym, zwalczanie wykluczenia społecznego, ochrona przyrody, promowanie zdrowia i dobrostanu, promocja kształcenia i szkolenia, działanie na rzecz społeczności imigrantów, wzmacnianie zdolności i odporności społeczności podatnych na zagrożenia lub dotkniętych klęskami, zamieszkujących regiony państw trzecich, w których prowadzone są działania i operacje pomocy humanitarnej, poprawa gotowości na wypadek klęsk żywiołowych i zmniejszanie ryzyka ich wystąpienia w tych regionach. To właśnie tego typu kwestii dotyczą projekty wolontariatu, o których finansowanie może ubiegać się organizacja. Po zatwierdzeniu projektu i przyznaniu mu finansowania organizacja może ogłaszać nabór do udziału w projekcie, wyszukiwać uczestników i kontaktować się z nimi, korzystając przy tym z dostępu do bazy osób młodych zarejestrowanych na portalu Europejskiego Korpusu Solidarności. Jednostki zaangażowane w działania wolontariatu mają status organizacji wspierających lub też przyjmujących. Osoba chcąca zostać wolontariuszem musi uzyskać wsparcie ze strony organizacji wspierającej w kraju swojego pochodzenia; wówczas to na niej ciąży odpowiedzialność w zakresie pomocy w przygotowaniu do udziału w projekcie wolontariatu poza granicami kraju. Z kolei organizacja przyjmująca ma siedzibę w kraju, w którym odbywa się wolontariat; tym samym przyjmuje ona wolontariusza i pomaga mu w razie jakichkolwiek problemów, które mogą pojawić się w trakcie realizacji wolontariatu.

W przypadku wolontariatu indywidulanego w wyjazd wolontariusza zaangażowane są zarówno organizacja wspierająca, jak i przyjmująca; natomiast dla wolontariatu grupowego istnieje konieczność zaangażowania już tylko jednej organizacji: albo wspierającej, albo przyjmującej. Podobnie jak młodzież chcąca wziąć udział w działaniach Europejskiego Korpusu Solidarności również organizacje mogą zarejestrować się w bazie: dzięki temu osoby zainteresowane wolontariatem, jak też pozostałymi działaniami w ramach ECS mogą w łatwiejszy sposób znaleźć jednostkę, która pełniłaby rolę organizacji wspierającej.

Organizacja projektu w ramach działania wolontariatu przynosi zarówno organizacjom, jak i młodzieży wymierne korzyści. Dzięki niej te pierwsze mogą uzyskać wsparcie osobowe w realizacji swoich statutowych celów przez wolontariuszy z różnych państw; dodatkowo skutkuje to nawiązaniem nowych kontaktów, co może znajdować przełożenie na wniesienie nowej jakości w realizowane dotychczas projekty. Bez wątpienia wolontariat również pozytywnie oddziałuje na środowisko lokalne, do którego trafia większość inicjatyw podejmowanych w trakcie jego realizacji; wolontariusze bowiem często biorą udział w projektach adresowanych do społeczności lokalnej, w tym dzieci i młodzieży, a także osób potrzebujących: chorych, starszych oraz wykluczonych społecznie.

Oprócz zdobycia doświadczenia, nabycia nowych umiejętności, a także nawiązania kontaktów międzynarodowych wolontariusze uzyskują pokrycie kosztów usług wsparcia obejmujących m.in. ogólne szkolenie online, szkolenie językowe online, ubezpieczenie, a także – jeśli to konieczne – wizy i pozwolenia na pobyt. Przed wyjazdem uczestnicy wolontariatu muszą podpisać umowę, w której określa się prawa i obowiązki w zakresie ubezpieczenia i dofinansowania otrzymanego w ramach ESC oraz opis zadań do wykonania w trakcie działania i oczekiwane efekty. W kraju, w którym odbywa się wolontariat, wolontariusz ma prawo skorzystać z opieki mentora, natomiast po powrocie otrzymuje udokumentowane efekty uczenia się w trakcie projektu, tj. Youthpass.

Należy podkreślić, że dodatkowo uczestnicy działań długoterminowych ESC są skierowani na serię kursów, które obejmują szkolenie przed wyjazdem, po przyjeździe na miejsce, ocenę śródokresową, dotyczącą tylko działań trwających co najmniej 6 miesięcy, a także coroczne wydarzenia ESC. Oprócz wspomnianego ubezpieczenia i kosztu usług dodatkowych, w ramach działania wolontariatu są pokrywane wydatki związane z kosztami podróży w obie strony, zakwaterowania i wyżywienia w trakcie trwania projektu, a także kieszonkowe na wydatki osobiste.

Drugim z działań w ramach ESC są projekty solidarności adresowane do społeczności lokalnej i dotyczące najczęściej wyzwań, z którymi musi się ona mierzyć. Zdarza się jednak, że projekty te dotyczą problemów regionalnych lub też krajowych. Najistotniejsze jest jednak, by były one ściśle powiązane z określonymi priorytetami na poziomie Unii Europejskiej, do

których możemy zaliczyć m.in. włączenie społeczne, zmiany klimatyczne, udział w życiu demokratycznym, a także równouprawnienie płci czy sprawy obywatelskie. Każdy z projektów może trwać od 2 do 12 miesięcy i jest realizowany w niepełnym wymiarze godzin. W praktyce oznacza to, że osoby biorące udział w projekcie czynią to w czasie wolnym od zajęć edukacyjnych czy zawodowych.

Projekty solidarności podobnie jak wolontariat są adresowane do osób w wieku od 18 do 30 lat, które zamieszkują państwa UE lub też Islandię, Lichtenstein, Turcję i Macedonię Północną. Są realizowane przez grupę co najmniej 5 wolontariuszy, którzy zamieszkują ten sam kraj, a wsparcie finansowe uzyskiwane na rzecz realizacji projektu wynosi 630 euro miesięcznie. Jeśli istnieje taka potrzeba, to może zostać również pokryty koszt zawiązany z udziałem trenera w projekcie lub z zaangażowaniem osób młodych o mniejszych szansach, tj. borykających się z problemami zdrowotnymi, finansowymi itd. W odróżnieniu od wolontariatu o udział w projektach solidarności należy ubiegać się bezpośrednio, wnioskując do agencji narodowej w określonym terminie, tj. bez konieczności angażowania organizacji.

Trzecie działanie w ramach Europejskiego Korpusu Solidarności to pomoc humanitarna – została ona ujęta w ESC ze względu na to, że w przeciągu kilku minionych lat pojawił się wzrost potrzeb humanitarnych w różnych regionach świata. Ponadto nastąpiła konieczność promowania pomocy humanitarnej wśród obywateli UE oraz zwiększenia ich zaangażowania w nią, zwłaszcza w państwach dotkniętych katastrofami i klęskami żywiołowymi spoza samej Unii. Pomoc humanitarna, zwana także Europejskim Ochotniczym Korpusem Pomocy Humanitarnej, ma przyczynić się do ochrony życia, zapobiegania ludzkiemu cierpieniu lub jego łagodzenia, zachowania godności ludzkiej, a także rozwijania zdolności i odporności społeczności podatnych na zagrożenia lub też dotkniętych klęskami.

Pomoc humanitarna jest świadczona przez osoby w wieku od 18 do 35 lat. Podobny znak musi posiadać organizacja wspierająca, zaangażowana w to działanie. W związku z tym, że osoby biorące udział w wolontariacie na rzecz pomocy humanitarnej muszą mieć zapewnione bezpieczeństwo w trakcie jego realizacji, wolontariat tego typu może odbywać się tylko

w tych krajach, w których realizowane są działania i operacje pomocy humanitarnej, a także w których nie toczą się międzynarodowe lub wewnętrzne konflikty zbrojne. Podobnie jak działanie wolontariatu, także i pomoc humanitarna ma przyczynić się do wypracowania nowych umiejętności i kompetencji wśród uczestników oraz umożliwić im wkład w rozwój społeczny, osobisty i obywatelski. Osiągnięcia te są także udokumentowane w Youthpass. Przed udziałem w wolontariacie na rzecz pomocy humanitarnej uczestnicy podpisują umowę regulującą ich prawa i obowiązki, a także zasady realizacji projektu. Z tego tytułu uzyskują również pokrycie wydatków z nim związanych.

Należy zaznaczyć, że EKS obejmuje nie tylko region UE – organizacja ma wymiar międzynarodowy, wspiera również państwa trzecie (niestowarzyszone), co wynika głównie z chęci poszerzenia zasięgu programu i potrzeby budowania międzynarodowej solidarności wzmacniającej działania wobec młodych ludzi, ale również stabilności międzynarodowej i bezpieczeństwa. Celem współpracy z państwami trzecimi jest również jednoczenie społeczności o poglądach podobnych do tych europejskich. Postanowienia EKS są zgodne ze strategią UE – „Kontakty, relacje i wymiana doświadczeń mają zasadnicze znaczenie dla solidarności i przyszłego rozwoju Unii Europejskiej. Kontaktom tym najbardziej sprzyjają różnorodne formy mobilności" – co świadczy o tym, że działania łączące EKS z krajami trzecimi dążą do wzmocnienia relacji młodych ludzi i badaczy. Ma to również na celu dostarczanie możliwości wymiany doświadczeń, budowanie przyszłościowych i międzynarodowych relacji oraz poszerzanie współpracy na rzecz wolontariatu. EKS udostępnia potrzebne narzędzia oraz mechanizmy, które umożliwiają współpracę transgraniczną w zakresie edukacji o bezpieczeństwie. Działania EKS wobec państw trzecich ukierunkowane są na budowanie silnego, demokratycznego, pokojowego i pełnoprawnego społeczeństwa poprzez inicjatywy (takie właśnie jak EKS). Trzeba również podkreślić, że działania łączące państwa niezrzeszone to również korzyści dla członków UE. Główne i najcenniejsze profity to m.in. zdobycie doświadczenia w zróżnicowanych środowiskach kulturalnych, rozwijanie kompetencji obywatelskich, umiejętności i możliwości zawodowych. Dzięki międzynarodowemu podejściu EKS wzmacniane są zdolności UE wobec stabilności w regionie, promowanie europejskich wartości,

budowanie bezpieczeństwa międzynarodowego na wielu płaszczyznach, wzmacnianie pomocy humanitarnej na zróżnicowanej szerokości geograficznej. Należy również zaznaczyć, że działania w państwach trzecich mogą być prowadzone tylko w przypadku niewystępowania konfliktu zbrojnego (na tle międzynarodowym lub wewnętrznym).

Podkreślić należy, że EKS to kluczowe narzędzie w celu budowania odporności społecznej na przestrzeni międzynarodowej. Działania organizacji obejmują wzmacnianie bezpieczeństwa społecznego, spajanie UE w jej granicach, ale również poza nimi. Europejski Korpus Solidarności staje się nieodłącznym elementem polityki UE, ale również jedną ze wspólnych wartości dla państw zrzeszonych. Ogromnie ważnym aspektem jego funkcjonowania jest zdolność do spójności społecznej, przede wszystkim osób młodych, poprzez aktywności o wysokiej wartości społecznej (np. działania humanitarne). Warto zauważyć, że działania te mają nie tylko pozytywny i budujący wpływ na poczucie wspólnoty państw, ale również podnoszą bezpieczeństwo społeczności. Udział w takich wydarzeniach odwzorowuje również odpowiednie przygotowania w budowaniu odpowiedzialności wobec kryzysów (naturalne, katastrofy spowodowane przez człowieka). Uczestnicy programu angażowani są w takie akcje, jak reagowanie na kryzysy i katastrofy, pomoc uchodźcom, ochrona dziedzictwa kulturowego. Udział w programie daje również równe szanse młodym osobom o niższych możliwościach; osoby takie przyłączane są do projektów solidarnościowych, przez co budują swoje kompetencje i rozwijają umiejętności, co minimalizuje ryzyko wykluczenia, a dodatkowo działania te przyczyniają się do podnoszenia bezpieczeństwa socjalnego. EKS ma również pozytywny wpływ na obszar strategiczny poszczególnych państw: dzieje się tak poprzez wspieranie akcji humanitarnych w krajach objętych konfliktem (np. pomoc ludności cywilnej). Trzeba również zaznaczyć, że wzmacnianie tego obszaru ma pozytywny wpływ na państwa trzecie – Europejski Korpus Solidarności staje się zatem nieodłącznym elementem strategicznym i politycznym UE o wielowymiarowej wartości.

Natalia Borodziuk, Paulina Szeląg

S. Broek, B. Buiskool, *European Solidarity Corps and voulnteering*, Study for the Committee on Culture and Education, European Parliament, 2017, https://op.europa.eu/en/publication-detail/-/publication/6fa0d7f8-a8ad-11e7-837e-01aa75ed71a1/language-en (dostęp 11.12.2025); Europejski Korpus Solidarności (2023). Przewodnik po Europejskim Korpusie Solidarności, https://eks.org.pl/brepo/panel_repo_files/2022/11/24/puzphv/european-solidarity-corps-guide-2023-pl.pdf (dostep 9.11.2025); *Europejski Korpus Solidarności 2021–2027*, https://eks.org.pl/ (dostęp 11.12.2025); *Europejski Korpus Solidarności. Razem możemy więcej. Informacje ogólne*, https://youth.europa.eu/solidarity_pl (dostęp 8.12.2025); *Europejski Korpus Solidarności. Razem możemy więcej. Projekty solidarnościowe*, https://youth.europa.eu/solidarity/young-people/solidarity-projects_pl (dostęp 8.11.2025); *Europejski Korpus Solidarności. Razem możemy więcej. Wolontariat w zakresie pomocy humanitarnej*, https://youth.europa.eu/solidarity/young-people/volunteering-humanitarian-aid_pl (dostęp 8.12.2025); *Europejski Korpus Solidarności. Razem możemy więcej. Wolontariat*, https://youth.europa.eu/solidarity/young-people/volunteering_pl (dostęp 8.12.2025); *KE: koniec współpracy z Rosją w badaniach i edukacji*, https://eks.org.pl/aktualnosc/ke-koniec-wspolpracy-z-rosja-w-badaniach-i-edukacji (dostęp 8.12.2025); *Ogólnopolski dzień informacyjny Europejskiego Korpusu Solidarności*, 8.01.2019 (dostęp 8.12.2025); *Przewodnik po Europejskim Korpusie Solidarności. Wersja 1/2025*, https://eks.org.pl/brepo/panel_repo_files/2024/11/29/qpizki/european-solidarity-corps-guide-2025-pl.pdf (dostęp 8.12.2025); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/888 z dnia 20 maja 2021 r. ustanawiające program „Europejski Korpus Solidarności" oraz uchylające rozporządzenie (UE) 2018/1475 i (UE) nr 375/2014 (tekst mający znaczenie dla EOG).

EUROPEJSKI SOJUSZ NUKLEARNY (ang. European Nuclear Alliance*)* – nieformalne porozumienie/sojusz państw członkowskich Unii Europejskiej, które opowiadają się za wzmocnieniem roli energetyki jądrowej w przyszłej polityce energetycznej UE; inicjatywa promująca energetykę jądrową w Unii Europejskiej; również stowarzyszenie państw członkowskich Unii Europejskiej, które uzgodniły zwiększoną współpracę w zakresie rozwoju energii jądrowej w celu poprawy ochrony klimatu i zwiększenia bezpieczeństwa dostaw.

Sojusz ten, zainicjowany przez Francję 28 lutego 2023 r., zrzesza państwa członkowskie UE dążące do promowania energii jądrowej jako kluczowego elementu transformacji energetycznej i osiągnięcia neutralności

klimatycznej. Początkowo obejmował, oprócz Francji, 10 krajów: Bułgarię, Chorwację, Czechy, Węgry, Finlandię, Holandię, Polskę, Rumunię, Słowację i Słowenię. W dniu dzisiejszym do sojuszu wchodzi niemal 20 krajów europejskich.

Głównym założeniem sojuszu jest wspólne działanie krajów popierających atom w celu zmniejszenie strategicznych zależności, wzmocnienia suwerenności, konkurencyjności, a także zakończenie transformacji energetycznej państw członkowskich, czyli dekarbonizacja produkcji energii w Unii Europejskiej poprzez wykorzystanie energii jądrowej jako uzupełnienia odnawialnych źródeł energii. Sojusz również ma na celu wzmocnienie współpracy w dziedzinie energii jądrowej, koordynację stanowisk w negocjacjach unijnych, wspieranie inwestycji w energetykę jądrową (w tym w małe reaktory modułowe – SMR) oraz rozwój powiązanych technologii i łańcuchów dostaw. Ponadto celem jest zapewnienie obywatelom UE niezawodnej i opłacalnej energii elektrycznej.

Oprócz tego istnieje też inny „sojusz", czyli Europejski Sojusz Przemysłowy na rzecz Małych Reaktorów Modułowych (European Industry Alliance on SMRs), założony przez KE, który ma przyspieszyć rozwój tych technologii, a także ułatwić wdrażanie małych reaktorów modułowych w UE, ustandaryzować licencje i rozwijać europejski łańcuch dostaw.

Państwa członkowskie dążą do zwiększenia zainstalowanej mocy energii jądrowej w całej UE do 150 GW w 2050 r. Ten wzrost o 50%, czyli 30 do 45 nowych reaktorów, ma na celu utrzymanie 25% udziału energii jądrowej w produkcji energii elektrycznej w UE w miarę wzrostu zapotrzebowania.

Stany Zjednoczone również wyraziły zamiar współpracy przy rozwoju i standaryzacji nowych reaktorów, w tym małych reaktorów modułowych. Ma ona obejmować badania, szkolenia, opracowywanie standardów bezpieczeństwa oraz tematy demontażu i obsługi zużytych elementów paliwowych. Programy wymiany dla techników i inżynierów mają być promowane w celu wymiany wiedzy.

W lutym 2023 r. ministrowie energii 11 państw członkowskich UE zgodzili się na zwiększoną współpracę w celu promowania energii jądrowej na marginesie posiedzenia Rady Ministrów w Sztokholmie. Spotkanie zainicjowała Agnès Pannier-Runacher, francuska minister ds. transformacji energetycznej. Oprócz Francji, Bułgaria, Chorwacja, Czechy, Węgry,

Finlandia, Holandia, Polska, Rumunia, Słowacja i Słowenia były pierwszymi sygnatariuszami wspólnej deklaracji. Szwecja również uczestniczyła w rozmowach, ale jeszcze nie dołączyła ze względu na przewodnictwo w Radzie UE, która jest zobowiązana do neutralności.

Przedstawiciele tych państw postanowili wspierać bliższą współpracę między krajowymi sektorami jądrowymi, aby zapewnić jak najlepszy łańcuch dostaw, oraz opracowywać wspólne programy szkoleniowe i projekty przemysłowe. Energia jądrowa jest jednym z wielu narzędzi do realizacji celów klimatycznych UE i zapewnienia bezpieczeństwa dostaw. Ministrowie zgodzili się wspierać nowe projekty i istniejące zakłady, omawiali możliwości zwiększenia współpracy naukowej i skoordynowali wdrażanie najlepszych praktyk w dziedzinie bezpieczeństwa.

Jednakże niektóre państwa stanowczo sprzeciwiały się sojuszowi, w szczególności Niemcy i Hiszpania. Austria, Niemcy i Luksemburg ponownie potwierdziły w Sztokholmie swój sprzeciw wobec rozwoju energii jądrowej w Europie. „Jeśli chcemy wygrać wyścig ze zmianami klimatu, musimy działać szybko" – powiedział luksemburski minister energii Claude Turmes, dodając, że budowa nowych elektrowni jądrowych zajmie 15 lat.

W marcu 2023 r. grupa spotkała się ponownie na posiedzeniu Europejskiej Rady Energetycznej w Brukseli. Ministrowie Włoch i Belgii byli obecni jako goście po raz pierwszy. Równocześnie zebrała się grupa państw przyjaciół Odnawialnych Źródeł Energii, założona przez austriacką minister Leonore Gewessler jako kontrreakcja na sojusz, która oskarżyła sojusz pronuklearny o działanie przeciwko interesom UE. Po początkowym sporze dotyczącym zaproszenia Francja mogła wziąć udział w późniejszych spotkaniach Sojuszu na rzecz Odnawialnych Źródeł Energii, wskazując na wysoki udział w krajowej produkcji energii odnawialnej.

Na trzecim spotkaniu w Paryżu w maju 2023 r. członkowie, wraz z Włochami jako obserwatorem i Wielką Brytanią jako gościem, przyjęli deklarację wzywającą Komisję Europejską do włączenia energii jądrowej do europejskiej strategii energetycznej.

W lutym 2025 r. Belgia przeszła ze stanowiska obserwatora do członka sojuszu.

W czerwcu 2025 r. włoski minister środowiska i bezpieczeństwa energetycznego Gilberto Pichetto Fratin ogłosił zamiar przystąpienia kraju

do sojuszu. Wkrótce potem premier Grecji Kyriakos Mitsotakis również wyraził taką chęć, ale nie podał konkretnej daty. Mitsotakis uzasadnił zainteresowanie swojego kraju tezą, że neutralność klimatyczna jest niemożliwa bez energii jądrowej i że jej wykorzystanie w greckiej flocie żeglugowej powinno zostać również zbadane.

W czerwcu 2025 r. niemiecka minister gospodarki Katherina Reiche (CDU) uczestniczyła w spotkaniu jako obserwatorka, co spotkało się z krytyką ze strony partnera koalicyjnego SPD oraz przedstawicieli Zielonych. Estonia przyjęła status pełnego członkostwa na spotkaniu członków w Luksemburgu w październiku 2025 r., nie rezygnując z członkostwa w Konfederacji Państw na rzecz Promocji Energii Odnawialnej.

W deklaracjach sojuszu stwierdza się, że energia jądrowa, obok źródeł odnawialnych, powinna być uznawana za istotną część miksu energetycznego UE, ze względu na kwestie bezpieczeństwa dostaw, niezawodności oraz ograniczenia emisji CO_2.

Europejski Sojusz Nuklearny deklaruje kilka kluczowych celów:

- promowanie energetyki jądrowej jako centralnego elementu transformacji energetycznej UE, obok OZE (odnawialnych źródeł energii) – do osiągnięcia neutralności klimatycznej;
- zapewnienie „bazowej" – stabilnej, przewidywalnej i niskoemisyjnej – mocy produkcji energii, która uzupełnia fluktuacje OZE i zwiększa bezpieczeństwo energetyczne;
- wspieranie rozwoju całego łańcucha przemysłu jądrowego w Europie, nie tylko reaktorów, ale też technologii, paliwa, komponentów, bezpieczeństwa, infrastruktury i kadr;
- przyspieszenie wdrożenia nowoczesnych technologii jądrowych, w tym małych i modułowych reaktorów (SMR/AMR), co jest celem również powołanego osobno Europejskiego Sojuszu Przemysłowego na rzecz Małych Reaktorów Modułowych;
- ułatwienie finansowania projektów jądrowych m.in. poprzez wspólną europejską koordynację, wsparcie instytucji finansowych, uznanie energetyki jądrowej jako zero- lub niskoemisyjnej;
- zmniejszanie zależności od zewnętrznych dostawców paliw kopalnych i zwiększanie suwerenności energetycznej UE.

Sojusz pojawił się w momencie, gdy wiele państw UE dostrzegło, że zielona transformacja i cele klimatyczne wymagają dekarbonizacji energetyki, a OZE – choć kluczowe – nie zawsze dają pełną niezawodność (np. przy zmiennej produkcji). Energia jądrowa może zapewnić stabilną podstawę. Kryzysy energetyczne, geopolityczne napięcia, wojna, zakłócenia dostaw surowców zwiększają zainteresowanie rozwiązaniami, które dają niezależność i bezpieczeństwo dostaw. Potrzeba rozwoju przemysłu i technologii, innowacji oraz nowych miejsc pracy – sektor jądrowy to także przemysł, badania, technologie, eksport. Sojusz widzi w tym szansę na rozwój gospodarczy.

W latach 2024–2025 sojusz i jego państwa-członkowie potwierdziły publicznie deklaracje, że energia jądrowa ma być uznawana jako kluczowa technologia dla neutralności klimatycznej i bezpieczeństwa energetycznego UE.

W lutym 2025 r. Komisja Europejska opublikowała nową unijną strategię przemysłową – Czysty Ład Przemysłowy, w którym nacisk położono na rozwój energii jądrowej w UE.

Estonia oficjalnie dołączyła do Europejskiego Sojuszu Nuklearnego podczas spotkania w Luksemburgu, 20 października 2025 r. Do tej pory uczestniczyła w rozmowach sojuszu jako obserwatorka, podzielając przekonanie, że energia jądrowa odgrywa ważną rolę w czystym, bezpiecznym i niezależnym europejskim systemie energetycznym.

Wbrew rosnącemu poparciu energetyka jądrowa, a przez to także sojusz, nadal budzi wiele wątpliwości. Główne z nich to:

- obawy o bezpieczeństwo: wypadki jądrowe, zagrożenia radiacyjne, długoterminowe składowanie odpadów. Historia (np. Czarnobyl, Fukushima) nadal silnie wpływa na opinie;
- wysokie koszty inwestycji i długi czas budowy dużych elektrowni, co sprawia, że nie wszystkie kraje lub społeczności są gotowe na takie projekty;
- trudności z akceptacją społeczną: różne kraje i regiony mają odmienne doświadczenia i nastawienie do atomu, co może utrudniać konsensus;

– w kontekście transformacji klimatycznej: krytyka, że skupienie na atomie może odwracać uwagę od rozwoju OZE, efektywności energetycznej i innych rozwiązań.

Polska aktywnie uczestniczy w działaniach sojuszu, pomimo że obecnie nie posiada własnych elektrowni atomowych, ale realizuje ambitny Program polskiej energetyki jądrowej (PPEJ), który zakłada budowę dwóch elektrowni jądrowych o łącznej mocy 6–9 GW przez należącą w 100% do Skarbu Państwa spółkę Polskie Elektrownie Jądrowe (PEJ) w charakterze inwestora i operatora. Dla Polski udział w sojuszu może oznaczać:

– możliwość współpracy międzynarodowej przy budowie i finansowaniu elektrowni jądrowych, co może ułatwić realizację planów energetycznych i zmniejszyć koszty;
– dostęp do wspólnego łańcucha technologicznego, *know-how*, standardów bezpieczeństwa, a także funduszy UE – co może przyspieszyć rozwój jądrowy w Polsce;
– szansę na udział w nowoczesnych projektach, np. w reaktorach SMR, które mogą być łatwiejsze we wdrożeniu niż duże konwencjonalne bloki energii jądrowej.

Jednak udział i rozwój wiążą się też z koniecznością przestrzegania wysokich standardów bezpieczeństwa, transparentnej polityki odpadów, a także przekonania społeczeństwa.

Europejski Sojusz Nuklearny to obecnie jedna z najważniejszych inicjatyw w UE promujących atom jako kluczowy element transformacji energetycznej. W obliczu kryzysów klimatycznych, energetycznych i geopolitycznych sojusz ma silny argument: stabilność, niezawodność i niskoemisyjność energii jądrowej.

Energia jądrowa jest wykorzystywana do wytwarzania prądu w 12 z 27 państw członkowskich UE; obecnie zapewnia około 25% energii elektrycznej w UE oraz 50% – niskoemisyjnej. Lista państw, które są jej zwolennikami, jest jednak dłuższa i znajduje się na niej także Polska. W Unii Europejskiej i Wielkiej Brytanii jest obecnie około 100 reaktorów jądrowych, a kolejne są w budowie. Projekty tego rodzaju są realizowane m.in. w Bułgarii, Rumunii, Czechach i Wielkiej Brytanii oraz na Węgrzech i Słowacji.

Europa musi być światowym liderem w zakresie zielonej transformacji oraz produkcji i wykorzystania energii jądrowej. Dzisiejsze działanie UE spowoduje zmianę paradygmatu w polityce energetycznej na rzecz silniejszej Europy na rynkach technologii i w branżach przyszłości o zerowej emisji netto. Energia jądrowa, obok odnawialnej, będzie napędzać długoterminową strategię wzrostu i konkurencyjności UE, stanowiąc podstawę porozumienia w sprawie dekarbonizacji przemysłu w kierunku neutralności klimatycznej do 2050 r.

Rozwój energii jądrowej i jej łańcucha wartości nie tylko wzmocni transformację energetyczną UE, ale także pobudzi wzrost gospodarczy i przemysł, stworzy miejsca pracy wymagające wysokich kwalifikacji, a także będzie wspierać najnowocześniejsze technologie, pozycjonując Europę jako światowe centrum innowacji nuklearnych.

Jeśli UE i kraje członkowskie będą konsekwentnie rozwijać technologie (w tym SMR), dbać o bezpieczeństwo i łańcuch dostaw, sojusz może przyczynić się do znaczącego zwiększenia udziału atomu w miksie energetycznym Europy. Dla Polski, przy jej planach rozwoju energetyki jądrowej, może to być ważna szansa.

Sergiusz Wasiuta

H. Aposporis, *Greece to participate in European Nuclear Alliance*, 19.06.2025, https://balkangreenenergynews.com/greece-to-participate-in-european-nuclear-alliance/ (dostęp 10.12.2025); *Declaration of the EU Nuclear Alliance Bulgaria, Croatia, Czech Republic, Finland, France, Hungary, the Netherlands, Poland, Romania, Slovakia, Slovenia and Sweden Meeting of March 4th, 2024*, https://presse.economie.gouv.fr/declaration-of-the-eu-nuclear-alliance-meeting-of-march-4th-2024/ (dostęp 11.12.2025); S. De La Feld, *European Nuclear Alliance grows as Italy also formally joins*, 16.06.2025, https://www.eunews.it/en/2025/06/16/european-nuclear-alliance-grows-as-italy-also-formally-joins/ (dostęp 10.12.2025); *Eleven EU energy ministers champion nuclear energy*, 2.03.2023, https://www.neimagazine.com/news/eleven-eu-energy-ministers-champion-nuclear-energy-10644621/?cf-view (dostęp 10.12.2025); *Estonia Secures a Place at the European Nuclear Energy Decision Table*, 17.10.2025, https://kliimaministeerium.ee/en/news/estonia-secures-place-european-nuclear-energy-decision-table (dostęp 10.12.2025); *European Industrial Alliance on SMRs*, https://single-market-economy.ec.europa.eu/industry/industrial-alliances/european-industrial-alliance-small-modular-reactors_en (dostęp 7.12.2025);

European Nuclear Alliance Leader's declaration, 21.03.2024, https://www.elysee.fr/en/emmanuel-macron/2024/03/21/european-nuclear-alliance-leaders-declaration (dostęp 13.12.2025); *Jądrowy sojusz jedenastu krajów Unii Europejskiej*, 2.03.2023, https://nuclear.pl/wiadomosci,news,23030203,0,0.html (dostęp 11.12.2025); *Jednak atom. W UE zmienia się podejście do energii jądrowe*j, 26.03.2025, https://www.farmer.pl/energia/jednak-atom-w-ue-zmienia-sie-podejscie-do-energii-jadrowej,159143.html (dostęp 7.12.2025); P. Messa, *Nuclear alliance aims for 150 GW of nuclear capacity in EU by 2050*, 17.05.2023, https://www.euractiv.com/news/nuclear-alliance-aims-for-150-gw-of-nuclear-power-in-eu-by-2050/ (dostęp 10.12.2025); P. Messad, *French-led nuclear alliance calls for equal EU treatment with renewables*, https://www.euractiv.com/news/french-led-nuclear-alliance-calls-for-equal-treatment-with-renewables/ (dostęp 7.12.2025).

F

FAŁSZYWY CLICKBAIT (ang. *false clickbait*) – termin opisujący specyficzną kategorię praktyk medialnych, w których nagłówek, zapowiedź lub materiał wizualny zostają skonstruowane w sposób celowo zniekształcający sens lub zakres treści, do której odsyłają. W odróżnieniu od ogólnego clickbaitu, opartego przede wszystkim na hiperbolizacji i stylistycznym wyostrzaniu przekazu, fałszywy clickbait posługuje się mechanizmem świadomego zerwania zgodności między obietnicą komunikacyjną a właściwą zawartością tekstu, nagrania bądź innego materiału informacyjnego. Jego istotą jest nie tyle wzbudzenie ciekawości, ile wywołanie u odbiorcy określonego impulsu poznawczego, który skłania do kliknięcia poprzez wytworzenie złudzenia dostępu do informacji sensacyjnych, przełomowych czy rzekomo tajnych, mimo iż faktyczna treść jest uboga, nieadekwatna lub całkowicie niemerytoryczna.

Zjawisko to należy analizować w kontekście przemian ekosystemu medialnego, w którym mechanizmy algorytmiczne oraz logika ekonomii uwagi determinują sposoby konstruowania przekazu. Fałszywy clickbait stanowi rezultat sprzężenia zwrotnego pomiędzy dążeniem podmiotów medialnych do maksymalizacji ruchu sieciowego a sposobem, w jaki

użytkownicy konsumują treści w warunkach informacyjnego przeciążenia. W środowisku, gdzie decyzje odbiorców zapadają w ułamkach sekund, a konkurencja o uwagę jest intensywna, nagłówek staje się najważniejszą jednostką komunikacyjną, nie w znaczeniu informacyjnym, lecz performatywnym, ponieważ to od niego zależy cyfrowa widoczność materiału. Fałszywy clickbait jawi się zatem jako radykalna forma instrumentalizacji nagłówka, podporządkowana logice metryk, a nie rzetelności.

Mechanizm działania fałszywego clickbaitu opiera się na wykorzystaniu poznawczych uprzedzeń odbiorcy. Kluczową rolę odgrywa tzw. luka informacyjna polegająca na skonstruowaniu takiego nagłówka, który wywołuje wrażenie, że odbiorca znajduje się o krok od zdobycia informacji „kluczowej" czy „szokującej", ale jej nie posiada. Wytworzone napięcie poznawcze motywuje do kliknięcia niezależnie od realnej potrzeby informacyjnej. Jednocześnie technika ta działa na pograniczu emocji, najczęściej aktywizując ciekawość, niepokój lub oburzenie. Zgodnie z ustaleniami psychologii mediów emocje te mają szczególną zdolność przyciągania i utrwalania uwagi, co czyni fałszywy clickbait narzędziem niezwykle skutecznym, choć z punktu widzenia ładu informacyjnego – wysoce destrukcyjnym.

Znaczenie fałszywego clickbaitu wykracza poza sferę praktyk komunikacyjnych i dotyczy bezpieczeństwa informacyjnego. Treści wprowadzające w błąd, nawet jeśli nie stanowią dezinformacji *sensu stricto*, osłabiają odporność społeczną poprzez podważanie zaufania do mediów i rozmywanie granicy między przekazem informacyjnym a perswazją. Wielokrotna ekspozycja na materiały, których nagłówki nie odpowiadają treści, prowadzi do erozji kompetencji odbiorczych, użytkownicy stają się mniej zdolni do oceny wiarygodności źródeł, bardziej podatni na manipulację i skłonni do powierzchownej interpretacji informacji.

W perspektywie systemowej zjawisko to ułatwia funkcjonowanie narracji dezinformacyjnych, które wykorzystują taką osłabioną strukturę poznawczą: odbiorca przyzwyczajony do treści niskiej jakości staje się mniej czujny wobec manipulacji o większej skali. Znaczącym aspektem fałszywego clickbaitu jest jego funkcja amplifikacyjna. W realiach platform cyfrowych, w których algorytmy premiują treści generujące szybkie i masowe zaangażowanie, materiały oparte na fałszywych nagłówkach

zyskują nienaturalnie wysoki zasięg. Jest to szczególnie istotne w sytuacjach kryzysowych, takich jak katastrofy naturalne, konflikty zbrojne, zagrożenia zdrowotne czy destabilizacja polityczna. W takich warunkach fałszywy clickbait może przyczynić się do rozprzestrzeniania informacji niezweryfikowanych, błędnie interpretowanych lub całkowicie pozbawionych oparcia w faktach, co generuje panikę, dezorientację i chaos decyzyjny zarówno na poziomie indywidualnym, jak i instytucjonalnym. Z perspektywy socjologicznej zjawisko to jest również przejawem kryzysu norm komunikacyjnych w środowisku cyfrowym.

Tradycyjne media, funkcjonujące pod presją utrzymania konkurencyjności, w coraz większym stopniu adaptują strategie clickbaitowe, co prowadzi do stopniowej normalizacji fałszywych nagłówków jako dopuszczalnej praktyki dziennikarskiej. Proces ten osłabia granicę odpowiedzialności redakcyjnej oraz pogłębia rozbieżność między deklarowaną misją informacyjną a faktycznymi działaniami podmiotów medialnych. W efekcie odbiorca funkcjonuje w środowisku, w którym wiarygodność musi być weryfikowana na nowo przy każdym kontakcie z informacją, co dodatkowo obciąża jego zasoby poznawcze. Fałszywy clickbait należy traktować jako zjawisko wielowymiarowe: jest jednocześnie techniką komunikacyjną, narzędziem manipulacji, sygnałem degradacji standardów informacyjnych oraz mechanizmem wzmacniającym podatność ekosystemu medialnego na zniekształcenia. Analiza tego fenomenu jest istotna w badaniach nad bezpieczeństwem informacyjnym, polityką komunikacyjną państw, teorią mediów i psychologią odbioru. Stanowi również przedmiot zainteresowania praktyk analitycznych związanych z przeciwdziałaniem dezinformacji, ponieważ często pełni rolę pierwszego etapu w procesie radykalizacji przekazu – od niewinnego zniekształcenia po manipulację o charakterze strategicznym.

Analizując fałszywy clickbait w szerszej perspektywie, należy zwrócić uwagę na jego zakorzenienie w strukturze współczesnych systemów komunikacyjnych, w których formatowanie informacji zostało podporządkowane szybkości, natychmiastowości reakcji oraz konkurencyjności w zakresie widoczności. Historyczny rozwój mediów internetowych, szczególnie w pierwszej dekadzie XXI w., przyniósł stopniową ewolucję sposobów przedstawiania treści: od nagłówków wyłącznie informacyjnych, przez

hybrydowe o funkcji marketingowej, aż do skrajnych form clickbaitowych, w których treść staje się quasiautonomicznym produktem retorycznym, często całkowicie oderwanym od przedstawianej informacji. W tym sensie fałszywy clickbait nie jest aberracją współczesnych mediów, lecz ich konsekwencją strukturalną, efektem dominacji metryk zaangażowania w procesie dystrybucji treści.

Z perspektywy językoznawczej fałszywy clickbait charakteryzuje się specyficznymi właściwościami dyskursywnymi. Typowe są konstrukcje superlatywne („największa", „najbardziej szokująca", „niespotykana"), modalności sugerujące nagłość („właśnie teraz", „natychmiast", „pilne"), a także użycie aluzji i pseudotajemniczości, które mają imitować dostęp do wiedzy niedostępnej dla ogółu odbiorców. Często stosuje się również zabieg semantycznego przesunięcia: nagłówek sugeruje zjawisko lub zdarzenie o charakterze przełomowym, podczas gdy właściwa treść opisuje banalny incydent lub materiał pozbawiony znaczenia poznawczego. Taka konstrukcja ma funkcję performatywną, a nie informacyjną i służy jedynie aktywizacji odbiorcy poprzez wywołanie wrażenia sensorycznej wyjątkowości.

Mechanizmy te mają znaczenie dla bezpieczeństwa informacyjnego na 2 poziomach: indywidualnym i systemowym. Na pierwszym fałszywy clickbait prowadzi do tzw. habituacji informacyjnej; odbiorca wielokrotnie wystawiany na bodźce obiecujące intensywne treści, które okazują się powierzchowne, traci zdolność różnicowania między informacją wysokiej a niskiej jakości. Generuje to nie tylko znużenie, lecz również skłonność do uproszczonego przetwarzania informacji, co w badaniach nad dezinformacją jest wskazywane jako czynnik zwiększający wrażliwość na manipulację. Na poziomie systemowym fałszywy clickbait wzmacnia proces fragmentaryzacji sfery publicznej: odbiorcy migrują między treściami pozbawionymi hierarchii istotności, co rozprasza uwagę społeczną i utrudnia budowanie wspólnego pola odniesienia, niezbędnego dla deliberacji demokratycznej.

Warto odnotować, że zjawisko fałszywego clickbaitu jest coraz częściej analizowane w kontekście badań nad polaryzacją. Badacze wskazują, że treści o charakterze sensacyjnym lub deformującym rzeczywistość są chętniej udostępniane w grupach o homogenizowanych poglądach,

co wzmacnia mechanizmy potwierdzenia poznawczego i prowadzi do utrwalania błędnych przekonań. Fałszywe nagłówki, które wykorzystują emocje negatywne, zwłaszcza gniew, strach lub pogardę, mają większą zdolność rozchodzenia się w sieciach społecznościowych, przez co stają się katalizatorami polaryzacji. Zjawisko to ma szczególne znaczenie w kontekście bezpieczeństwa państwowego: zdolność manipulacji emocjami mas może wpływać na percepcję instytucji publicznych, kształtować postawy wyborcze oraz destabilizować debatę publiczną.

Nie można również pomijać aspektu technologicznego. Ewolucja platform społecznościowych sprawia, że fałszywy clickbait wpisuje się w logikę działania algorytmów rankingowych. Treści, które generują gwałtowne skoki zainteresowania, są automatycznie promowane, niezależnie od ich jakości. Tego rodzaju algorytmiczna amplifikacja tworzy środowisko, w którym rzetelność informacyjna jest jednym z najmniej premiowanych elementów komunikacji cyfrowej. Fałszywy clickbait jest zatem nie tylko produktem nadawców, ale również wynikiem konstrukcji technicznej systemów dystrybucji, w których pierwszeństwo mają bodźce o dużej intensywności emocjonalnej. W literaturze medioznawczej wskazuje się, że zjawisko to rodzi nową formę asymetrii informacyjnej, w której użytkownik pozostaje nieświadomy zasad działania algorytmów i nie jest w stanie ocenić, czy jego ekspozycja na treści clickbaitowe jest przypadkowa, czy strukturalnie wymuszana.

Z perspektywy prawnej i regulacyjnej problem fałszywego clickbaitu pozostaje trudny do jednoznacznego ujęcia. Wynika to z faktu, że granica między agresywnym marketingiem a manipulacją jest nieostra, a duża część fałszywych nagłówków nie kwalifikuje się jako dezinformacja w sensie prawnym. Mimo to w ramach polityk Unii Europejskiej, zwłaszcza w kontekście Aktu o usługach cyfrowych (DSA), coraz częściej pojawiają się postulaty wzmacniania transparentności algorytmów oraz ograniczania praktyk, które mogą wprowadzać użytkownika w błąd. Fałszywy clickbait stanowi tu przykład tzw. „praktyk ciemnych wzorców" (*dark patterns*), w których konstrukcja przekazu lub interfejsu ma skłonić użytkownika do określonego działania bez pełnej świadomości jego konsekwencji.

Z punktu widzenia strategii przeciwdziałania fałszywemu clickbaitowi istotne są 3 obszary działań. Po pierwsze, edukacja medialna: użytkownicy

muszą rozumieć, jakie mechanizmy rządzą konstrukcją nagłówków oraz w jaki sposób ich percepcja może być manipulowana. Po drugie, wzmocnienie standardów redakcyjnych: redakcje, szczególnie te funkcjonujące w modelu cyfrowym, powinny ustanawiać przejrzyste zasady tworzenia nagłówków i egzekwować je jako element rzetelności dziennikarskiej. Po trzecie, regulacje systemowe: platformy powinny ujawniać zasady rankingowania treści oraz ograniczać promowanie materiałów, które wykazują cechy systematycznego wprowadzania w błąd. Każdy z tych obszarów ma znaczenie dla budowania odporności informacyjnej, zwłaszcza w środowisku, w którym dezorientacja odbiorcy staje się jednym z największych wyzwań.

Wreszcie, fałszywy clickbait pełni także funkcję kulturową, wpływając na sposób, w jaki społeczeństwa definiują informację. W środowisku nasyconym treściami uproszczonymi i sensacyjnymi dochodzi do spłaszczenia dyskursu publicznego: informacje złożone, wymagające kontekstu lub analizy, stają się mniej widoczne, a komunikacja poważna przegrywa ze spektakularną. W konsekwencji odbiorcy mogą redukować złożoność świata do estetyki nagłówka, co w literaturze socjologicznej określa się mianem „kultury skrótu". Fałszywy clickbait jest jej najbardziej wyostrzoną formą: radykalizuje tempo konsumpcji informacji, jednocześnie obniżając próg refleksji i zdolność krytycznego namysłu.

W kontekście współczesnych badań nad dynamiką przestrzeni komunikacyjnej fałszywy clickbait należy interpretować jako wskaźnik głębszych przemian epistemologicznych, w których tradycyjne modele dyfuzji wiedzy ulegają erozji wskutek dominacji logiki algorytmicznej. Oznacza to, że odbiorca nie jest już jedynie uczestnikiem procesu komunikacyjnego, lecz staje się jego produktem finalnym, formatowanym przez sekwencje bodźców projektowanych w sposób maksymalizujący zaangażowanie. W tym ujęciu skutki fałszywego clickbaitu nie ograniczają się do zaburzenia jakości przekazu, lecz obejmują rekonstrukcję relacji między informacją a jej interpretatorem. Powtarzalność ekspozycji na bodźce o zdeformowanym charakterze prowadzi do internalizacji specyficznych schematów percepcyjnych, w których priorytet uzyskują sygnały o wysokiej intensywności emocjonalnej, natomiast treści wymagające refleksji, kontekstu i krytycznej analizy stają się marginalizowane. W literaturze

dotyczącej bezpieczeństwa informacyjnego proces ten definiuje się jako przejście od poznania deliberatywnego do reaktywnego, co stanowi zjawisko kluczowe dla zrozumienia odporności społecznej na manipulację. Fałszywy clickbait, poprzez swoją pozorną banalność, ujawnia strukturalny problem współczesnych systemów dystrybucji informacji, w których nadmiar bodźców prowadzi nie do zwiększonej świadomości, lecz redukcji zdolności poznawczych. W rezultacie staje się on nie tylko kategorią analityczną, lecz również narzędziem diagnostycznym pozwalającym ocenić stopień dezintegracji ładu informacyjnego, a tym samym określić ryzyko destabilizacji zarówno na poziomie konstrukcji przekazów publicznych, jak i funkcjonowania instytucji odpowiedzialnych za zapewnienie bezpieczeństwa informacyjnego państwa.

Aleksandra Gębacz

Y. Benkler, R. Faris, H. Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, Oxford 2018; J. Czerwiński, *„Pożyteczni idioci" kampanii dezinformacyjnych. Mechanizmy tworzenia się społeczności wirtualnych rozpowszechniających fałsz i manipulację w sieci*, Uniwersytet Marii Curie-Skłodowskiej, Lublin 2022; T.H. Davenport, J.C. Beck, *The Attention Economy: Understanding the New Currency of Business*, Harvard Business School Press, Boston 2001; S.U. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*, NYU Press, New York 2018; C. O'Connor, J.O. Weatherall, *The Misinformation Age: How False Beliefs Spread*, Yale University Press, New Haven–London 2019; T. Walczyk, *Werystyczna epistemologia społeczna i problemy komunikacji sieciowej*, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2024; T. Wu, *The Attention Merchants: The Epic Struggle to Get Inside Our Heads*, Alfred A. Knopf, New York 2016.

FINANSOWANIE TERRORYZMU stanowi jedno z kluczowych zagadnień współczesnego bezpieczeństwa międzynarodowego, obejmując wszelkie działania polegające na gromadzeniu, przekazywaniu lub udostępnianiu środków finansowych z zamiarem wykorzystania ich do działalności terrorystycznej, przy czym w świetle obowiązujących regulacji międzynarodowych dla bytu tego przestępstwa nie jest konieczne faktyczne przeprowadzenie zamachu ani nawet powiązanie zgromadzonych środków z konkretnym aktem przemocy. W ujęciu prawnym przyjmowanym

przez Międzynarodową konwencję o zwalczaniu finansowania terroryzmu (ICFT) z 1999 r. przestępstwo to polega na dostarczaniu lub zbieraniu funduszy z zamiarem wykorzystania ich do aktów mających na celu spowodowanie śmierci lub poważnych obrażeń cywili, gdy celem takiego działania jest zastraszenie ludności lub zmuszenie rządu albo organizacji międzynarodowej do określonego postępowania. Zrozumienie mechanizmów finansowania terroryzmu jest fundamentalne dla skutecznego przeciwdziałania temu zjawisku, ponieważ każda działalność terrorystyczna, niezależnie od jej skali i charakteru, wymaga określonych nakładów finansowych na rekrutację, szkolenie, zakup materiałów wybuchowych i broni, logistykę operacyjną oraz utrzymanie członków organizacji i ich rodzin.

W kontekście analizy ekonomicznej finansowania terroryzmu należy podkreślić, że zjawisko to charakteryzuje się specyficzną asymetrią kosztów, gdzie relatywnie niewielkie nakłady finansowe mogą generować nieproporcjonalnie duże skutki w wymiarze ofiar ludzkich, zniszczeń materialnych oraz destabilizacji społeczno-politycznej całych regionów. Jak wynika z badań przeprowadzonych nad zamachami terrorystycznymi w Europie w latach 1994–2013, około 75% ataków kosztowało sprawców mniej niż 10 tys. dolarów amerykańskich, co dramatycznie utrudnia wykrywanie działań przygotowawczych metodami tradycyjnej analizy finansowej opartej na monitorowaniu przepływów znaczących sum pieniędzy między rachunkami bankowymi. Raport Financial Action Task Force z 2025 r. wskazuje ponadto, że 69% ocenianych jurysdykcji wykazuje poważne deficyty w skutecznym ściganiu przestępstw związanych z finansowaniem terroryzmu, co świadczy o utrzymujących się lukach w globalnym systemie przeciwdziałania temu zjawisku pomimo kilkudziesięciu lat rozwijania stosownych regulacji prawnych i mechanizmów instytucjonalnych.

Źródła finansowania działalności terrorystycznej można sklasyfikować w 4 podstawowych kategoriach obejmujących źródła legalne, źródła nielegalne, sponsoring państwowy oraz samofinansowanie, przy czym współczesne organizacje terrorystyczne coraz częściej stosują strategię dywersyfikacji, łącząc różnorodne metody pozyskiwania środków w celu minimalizacji ryzyka wykrycia oraz zapewnienia ciągłości finansowania

nawet w przypadku zablokowania niektórych kanałów przez służby bezpieczeństwa. W ramach legalnych źródeł finansowania istotną rolę odgrywają darowizny i zbiórki publiczne, w tym wykorzystywanie religijnych obowiązków charytatywnych takich jak islamski Zakat (Zakāt) stanowiący 2,5% majątku wiernych czy Ushr będący 10-procentowym podatkiem od plonów rolnych pobieranym w niektórych społecznościach muzułmańskich. Taliban w okresie kontroli nad Afganistanem nakładał podatki religijne na podmioty zaangażowane w handel narkotykami, tworząc tym samym hybrydowy model łączący źródła legalne z nielegalnymi, natomiast organizacje prawicowo-ekstremistyczne działające w Europie zbierają fundusze poprzez organizację koncertów muzycznych, imprez publicznych oraz regularne składki członkowskie.

Działalność gospodarcza prowadzona przez organizacje terrorystyczne lub podmioty z nimi powiązane stanowi kolejne legalne źródło finansowania, pozwalające jednocześnie na generowanie dochodów oraz skuteczne pranie pieniędzy pochodzących z nielegalnych źródeł poprzez wprowadzanie ich do legalnego obrotu gospodarczego. Państwo Islamskie w szczytowym okresie swojej ekspansji terytorialnej prowadziło rozbudowane sieci małych i średnich przedsiębiorstw w Azji Południowo-Wschodniej oraz Libii, natomiast Iran wykorzystuje złożoną sieć firm przykrywkowych, które wtapiają się w legalne otoczenie biznesowe i transferują miliony dolarów pod pozorem rutynowych transakcji handlowych między kontrahentami. Nadużywanie organizacji non-profit pozostaje poważnym problemem w skali globalnej, a raport FATF z 2014 r. pt. *Risk of Terrorist Abuse in the Non-Profit Sector* analizujący 102 udokumentowane przypadki zidentyfikował 3 główne metody wykorzystywania sektora charytatywnego do celów terrorystycznych, obejmujące tworzenie fałszywych organizacji przez samych terrorystów działających pod pozorem działalności dobroczynnej, infiltrację legalnie funkcjonujących podmiotów w celu pozyskiwania funduszy i rekrutacji nowych członków oraz przywłaszczanie środków na różnych poziomach, od zbiórek ulicznych po realizację programów pomocowych w terenie. W lutym 2025 r. Departament Skarbu Stanów Zjednoczonych nałożył sankcje na 5 fałszywych organizacji charytatywnych finansujących zbrojne skrzydło

Hamasu – Brygady Izz ad-Din al-Kassam oraz Al Weam Charitable Society działające pod pozorem prowadzenia pracy humanitarnej w Strefie Gazy.

W kategorii nielegalnych źródeł finansowania terroryzmu handel narkotykami generuje znaczące przychody dla wielu grup terrorystycznych operujących w różnych regionach świata, tworząc trwałe powiązania między zorganizowaną przestępczością a sieciami terrorystycznymi. Taliban pod koniec lat 90. kontrolował do 96% obszarów uprawy maku w Afganistanie, który odpowiadał wówczas za około 70% światowego rynku opium wykorzystywanego do produkcji heroiny, a szacunki rocznych przychodów tej organizacji z handlu narkotykami wahają się w zależności od źródła od 19 do 500 mln dolarów amerykańskich. Kolumbijskie Rewolucyjne Siły Zbrojne znane pod akronimem FARC uzyskiwały, według różnych szacunków, od 140 mln do 3,5 mld dolarów z handlu kokainą, co stanowiło od 40% do 60% całkowitych dochodów tej organizacji i pozwalało na utrzymywanie tysięcy bojowników oraz prowadzenie wieloletnich działań zbrojnych przeciwko siłom rządowym. Hezbollah prowadzi operacje przemytu kokainy w Ameryce Południowej, wykorzystując rozbudowaną sieć pośredników i firm transportowych, a w 2023 r. w Irlandii skonfiskowano 2,2 t kokainy (wartość rynkowa około 157 mln euro) powiązane z członkami tej organizacji.

Porwania dla okupu stanowią, według szacunków ekspertów, około 15% globalnego finansowania terroryzmu, a od 2010 r. organizacjom terrorystycznym wypłacono w formie okupów ponad miliard dolarów amerykańskich, przy czym znaczna część tych środków pochodziła od rządów państw zachodnich negocjujących w imieniu porwanych obywateli pomimo oficjalnych deklaracji o niepodejmowaniu takich działań. Al-Kaida wraz ze swoimi regionalnymi afiliacjami uzyskała co najmniej 125 mln dolarów w latach 2008–2014, z czego 75 mln dolarów w Islamskim Maghrebie, głównie od państw europejskich wykupujących swoich obywateli. Przemyt obejmuje szeroki zakres towarów wykraczający daleko poza substancje psychoaktywne, a Państwo Islamskie w szczytowym okresie kontrolowało pola naftowe w Iraku i Syrii, generując przychody szacowane na 1–3 mln dolarów dziennie ze sprzedaży ropy naftowej lokalnym nabywcom, przemytnikom oraz paradoksalnie nawet reżimowi Asada. Organizacja kontrolowała ponadto co najmniej 4500 stanowisk

archeologicznych i uzyskiwała znaczące przychody z handlu zrabowanymi zabytkami, przy czym sam region Al-Nabuk w Syrii przyniósł 36 mln dolarów w latach 2012–2014. Wymuszenia i podatki nakładane na ludność kontrolowanych terytoriów stanowiły dominujące źródło dochodów Państwa Islamskiego po utracie terenów w wyniku operacji wojskowych koalicji międzynarodowej, a w szczytowym okresie organizacja pobierała około 8 mln dolarów miesięcznie w formie danin od lokalnych przedsiębiorstw.

Sponsorowanie państwowe terroryzmu pozostaje istotnym elementem globalnego krajobrazu zagrożeń, a Stany Zjednoczone oficjalnie wyznaczają państwa-sponsorów terroryzmu, prowadząc stosowną listę aktualizowaną przez Departament Stanu, do których obecnie zaliczane są Iran (nieprzerwanie od 1984), Syria (od 1979), Korea Północna (ponownie od 2017, po wcześniejszym usunięciu z listy) oraz Kuba (ponownie od 2021). Iran pozostaje głównym państwowym sponsorem terroryzmu na świecie, według ocen amerykańskich służb wywiadowczych, a Departament Stanu Stanów Zjednoczonych szacuje, że w latach 2012–2020 kraj ten wydał ponad 16 mld dolarów na wsparcie reżimu Baszara al-Asada w Syrii oraz organizacji proxy działających w całym regionie Bliskiego Wschodu. Hezbollah otrzymuje rocznie ponad 700 mln dolarów od Iranu, przy czym według niektórych szacunków kwota ta może sięgać nawet miliarda dolarów, obejmując zarówno bezpośrednie transfery finansowe, jak i dostawy uzbrojenia, a w pierwszych 10 miesiącach 2025 r. Korpus Strażników Rewolucji Islamskiej przetransferował do Hezbollahu ponad miliard dolarów. Hamas i Palestyński Islamski Dżihad otrzymują łącznie ponad 100 mln dolarów rocznie z irańskich źródeł, a sekretarz generalny Hezbollahu Hassan Nasrallah publicznie przyznał w 2016 r., że budżet organizacji, jej pensje, wydatki operacyjne oraz uzbrojenie pochodzą w całości z Islamskiej Republiki Iranu.

Samofinansowanie przez pojedynczych sprawców określanych w literaturze przedmiotu jako samotne wilki stanowi rosnące zagrożenie dla bezpieczeństwa, szczególnie w państwach zachodnich, gdzie radykalizacja coraz częściej przebiega za pośrednictwem internetu, bez bezpośredniego kontaktu z organizacjami terrorystycznymi. Sprawcy tego typu ataków wykorzystują oszczędności osobiste, kredyty konsumenckie zaciągane bez zamiaru spłaty, pożyczki studenckie, fałszywe zwroty podatkowe oraz

maksymalne wykorzystanie limitów kart kredytowych. Sprawca zamachu w San Bernardino Syed Rizwan Farook zaciągnął pożyczkę w wysokości 28 500 dolarów krótko przed przeprowadzeniem ataku, natomiast zamachowiec z Manchesteru Salman Abedi otrzymał co najmniej 7 tys. funtów z pożyczki studenckiej przeznaczonej teoretycznie na pokrycie kosztów nauki. Raport FATF z 2025 r. podkreśla, że zagrożenie ze strony samotnych jednostek, często młodych osób zradykalizowanych przez treści ekstremistyczne dostępne w internecie, systematycznie rośnie, stanowiąc wyzwanie dla tradycyjnych metod wykrywania finansowania terroryzmu.

W zakresie metod transferu środków terrorystycznych szczególne znaczenie posiada system Hawala, stanowiący starożytny nieformalny mechanizm przekazywania pieniędzy wywodzący się z subkontynentu indyjskiego i Bliskiego Wschodu, działający bez fizycznego przemieszczania pieniędzy między krajami poprzez międzynarodowy system bankowy. W ramach tego systemu klient przekazuje walutę lokalną pośrednikowi zwanemu hawaladarem w kraju nadania, który kontaktuje się telefonicznie lub elektronicznie z partnerem w kraju docelowym, a ten wypłaca równowartość odbiorcy w walucie lokalnej, przy czym rozliczenie między pośrednikami następuje później poprzez handel, wzajemne transakcje lub okresowe przekazanie gotówki. System charakteryzuje się brakiem fizycznego ruchu pieniędzy przez granice państwowe, minimalną dokumentacją pisemną opartą głównie na zaufaniu między stronami, niskimi opłatami wynoszącymi od 1% do 5% wartości transferu, szybkością realizacji często tego samego dnia oraz oparciu na więzach rodzinnych, plemiennych lub biznesowych między hawaladarami. W Afganistanie od 50% do 90% wszystkich transakcji finansowych odbywa się przez nieformalne systemy transferu pieniędzy ze względu na słabo rozwiniętą infrastrukturę bankową oraz kulturową tradycję korzystania z Hawali. Komisja do spraw zamachów z 11 września ustaliła, że Al-Kaida przenosiła znaczną część swoich pieniędzy przez system Hawala przed atakami, korzystając z usług kilkudziesięciu zaufanych pośredników, a w trzytygodniowym okresie od listopada do grudnia 2001 r. organizacja przetransferowała około 10 mln dolarów w gotówce i złocie z Afganistanu.

Kryptowaluty i aktywa wirtualne stanowią coraz częściej wykorzystywany kanał transferu środków związanych z działalnością terrorystyczną,

choć ich znaczenie w całkowitym obrazie finansowania terroryzmu pozostaje przedmiotem debaty ekspertów ze względu na trudności w precyzyjnym oszacowaniu skali zjawiska. Izraelskie Ministerstwo Obrony przejęło około 41 mln dolarów w kryptowalutach powiązanych z Hamasem w latach 2019–2023 oraz dodatkowe 94 mln dolarów od Palestyńskiego Islamskiego Dżihadu. FATF w czerwcu 2023 r. wyraził poważne zaniepokojenie faktem, że większość jurysdykcji nie w pełni wdrożyła wymogi dotyczące dostawców usług związanych z aktywami wirtualnymi, tworząc znaczące luki wykorzystywane przez przestępców i terrorystów. Monety prywatności (*privacy coins*), szczególnie Monero (XMR), Zcash (ZEC) i Dash, charakteryzujące się zaawansowanymi mechanizmami anonimizacji transakcji, zyskują popularność wśród terrorystów, a Państwo Islamskie Chorasanu prowadzi zbiórki przede wszystkim w Monero za pośrednictwem swojego magazynu propagandowego. Pranie pieniędzy oparte na handlu międzynarodowym stanowi wyrafinowaną metodę transferu pieniędzy wykorzystywaną zarówno przez organizacje przestępcze, jak i terrorystyczne, a główne techniki obejmują zawyżanie lub zaniżanie wartości faktur eksportowo-importowych, wielokrotne fakturowanie tych samych towarów, fikcyjne przesyłki oraz fałszowanie dokumentacji dotyczącej jakości produktów.

W wymiarze regulacyjnym Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF) powstała w 1989 r., podczas szczytu G7 w Paryżu pierwotnie dla zwalczania prania pieniędzy związanego z handlem narkotykami, a po zamachach z 11 września 2001 r. jej mandat rozszerzono o przeciwdziałanie finansowaniu terroryzmu, co fundamentalnie zmieniło charakter działalności tej organizacji. Od 2019 r. FATF działa na podstawie mandatu bezterminowego, a jej 40 Rekomendacji po kompleksowej rewizji przeprowadzonej w lutym 2012 r. obejmuje 7 kategorii tematycznych dotyczących polityk przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, koordynacji międzyinstytucjonalnej, środków dotyczących prania pieniędzy i konfiskaty mienia, środków zapobiegawczych dla sektora finansowego i niefinansowego, przejrzystości struktur prawnych i identyfikacji beneficjentów rzeczywistych, uprawnień i odpowiedzialności właściwych organów oraz współpracy międzynarodowej. Mechanizm szarej i czarnej listy FATF wywiera znaczącą presję na jurysdykcje

niespełniające standardów międzynarodowych, w tym w Korei Północnej, Iranie oraz Myanmar, natomiast szara lista jurysdykcji pod wzmożonym monitoringiem obejmuje 20 krajów (stan na 24.10.2025), w tym Algierię, Liban, Bułgarię i Syrię.

Unia Europejska rozwinęła kompleksowy system regulacji przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu poprzez kolejne dyrektywy transponowane do porządków prawnych państw członkowskich. Czwarta dyrektywa z 2015 r. wprowadziła podejście oparte na ryzyku jako centralną ramę działań instytucji obowiązanych, utworzyła rejestry beneficjentów rzeczywistych dostępne dla organów nadzoru oraz rozszerzyła zakres regulacji na sektor hazardowy. Piąta dyrektywa z 2018 r. po raz pierwszy uregulowała giełdy kryptowalut i portfele powiernicze na poziomie unijnym, obniżyła próg dla anonimowych kart przedpłaconych z 250 do 150 euro oraz rozszerzyła zakres na dealerów dzieł sztuki o wysokiej wartości. Szósta dyrektywa z 2024 r. z terminem implementacji do lipca 2027 r. zastąpi wcześniejsze akty prawne, harmonizując definicje naruszeń związanych z praniem pieniędzy w całej Unii Europejskiej. Nowy Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (AMLA) z siedzibą we Frankfurcie rozpoczął działalność 1 lipca 2025 r., a od 2028 r. będzie bezpośrednio nadzorować około 40 podmiotów finansowych wysokiego ryzyka prowadzących działalność transgraniczną.

Na poziomie Organizacji Narodów Zjednoczonych Rezolucja Rady Bezpieczeństwa 1267 z 1999 r. utworzyła reżim sankcji wobec Al-Kaidy i Talibanu obejmujący zamrożenie aktywów finansowych, zakaz podróży oraz embargo na broń, a system ten ewoluował przez kolejne rezolucje, rozszerzając się na Państwo Islamskie i powiązane podmioty. Rezolucja 1373 przyjęta zaledwie 17 dni po zamachach z 11 września 2001 r. jako pierwsza ustawodawcza rezolucja ONZ nakładająca bezpośrednie obowiązki prawne na wszystkie państwa członkowskie wprowadziła wymogi kryminalizacji (w sensie prawnym to warunki i zasady, które muszą zostać spełnione, aby dane zachowanie zostało uznane za przestępstwo i objęte sankcją karną) finansowania terroryzmu, zamrażania bez zwłoki funduszy terrorystów, zakazu udostępniania środków terrorystom oraz obowiązku współpracy informacyjnej między państwami. Rezolucja 2462 z 2019 r. stanowi pierwszą kompleksową rezolucję ONZ poświęconą wyłącznie problematyce

finansowania terroryzmu, rozszerzając kryminalizację na finansowanie organizacji terrorystycznych nawet przy braku związku z konkretnym aktem terroru. Międzynarodowa konwencja o zwalczaniu finansowania terroryzmu przyjęta 9 grudnia 1999 r. weszła w życie 10 kwietnia 2002 r. i została ratyfikowana przez 188 państw, stanowiąc jedną z najskuteczniejszych konwencji antyterrorystycznych w systemie ONZ.

W Polsce podstawowym aktem prawnym regulującym przeciwdziałanie finansowaniu terroryzmu jest Ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, implementująca dyrektywy unijne do polskiego porządku prawnego. Generalny Inspektor Informacji Finansowej to jednoosobowy centralny organ administracji rządowej powoływany przez Prezesa Rady Ministrów spośród osób wyłonionych w drodze otwartego konkursu, który przetwarza informacje o transakcjach podejrzanych otrzymywanych od instytucji, analizuje aktywa mogące mieć związek z finansowaniem terroryzmu, może wstrzymywać transakcje i blokować rachunki bankowe na okres do 96 godzin, przygotowuje Krajową Ocenę Ryzyka oraz nakłada kary administracyjne sięgające do 5 mln euro. Artykuł 165a Kodeksu karnego znowelizowany w 2017 r. penalizuje gromadzenie, przekazywanie lub oferowanie środków finansowych lub innych majątkowych w celu sfinansowania przestępstwa o charakterze terrorystycznym, przewidując karę pozbawienia wolności od 2 do 12 lat. Audyt Najwyższej Izby Kontroli z 2022 r. wykazał ograniczoną skuteczność polskiego systemu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, wskazując na niedostateczne zasoby kadrowe Generalnego Inspektora oraz znaczące opóźnienia w analizie zgłoszeń otrzymywanych od instytucji.

Jednostki analityki finansowej stanowią kluczowy element krajowych i międzynarodowych systemów przeciwdziałania finansowaniu terroryzmu, pełniąc funkcję centralnych punktów gromadzenia i analizy informacji o podejrzanych transakcjach. W Stanach Zjednoczonych funkcję tę pełni Financial Crimes Enforcement Network będący biurem Departamentu Skarbu, które zbiera i analizuje informacje finansowe dla zwalczania prania pieniędzy, finansowania terroryzmu oraz obchodzenia sankcji międzynarodowych. W roku fiskalnym 2024 FinCEN otrzymał 4,7 mln raportów o podejrzanej aktywności, średnio 12 870 dziennie, od około 324 tys.

zarejestrowanych instytucji finansowych działających na terytorium Stanów Zjednoczonych. Grupa Egmont (Egmont Group of Financial Intelligence Units – Egmont Group) założona w 1995 r. w pałacu Egmont-Arenberg w Brukseli zrzesza ponad 170 członków analityki finansowej z całego świata (liczba ta jest zmienna), a sieć Egmont Secure Web (ESW) umożliwia bezpieczną wymianę informacji wywiadowczych między jednostkami członkowskimi z zachowaniem poufności przekazywanych danych.

Analiza przypadków finansowania konkretnych organizacji terrorystycznych dostarcza cennych informacji o ewolucji metod i źródeł pozyskiwania środków oraz skuteczności stosowanych mechanizmów przeciwdziałania. Państwo Islamskie w latach 2014–2015 osiągało przychody szacowane na 1–2 mld dolarów rocznie, czyniąc je najbogatszą organizacją terrorystyczną w historii, a struktura dochodów obejmowała konfiskaty i grabieże stanowiące około 52% całości, podatki i opłaty – około 25%, oraz sprzedaż ropy naftowej – około 21%. Kontrola nad polami naftowymi generowała od 1 do 3 mln dolarów dziennie przy kontroli 350 szybów w Iraku oraz 60% syryjskich zdolności produkcyjnych. Po operacji Tidal Wave II przeprowadzonej przez koalicję międzynarodową w październiku 2015 r. przychody z ropy spadły dramatycznie do 4 mln dolarów miesięcznie w październiku 2017 r. Al-Kaida wbrew popularnym przekonaniom nie była finansowana osobiście przez Osamę bin Ladena z jego rodzinnej fortuny szacowanej przez media na 300 mln dolarów. Komisja do spraw zamachów z 11 września nie znalazła dowodów na istnienie znaczącego osobistego majątku finansującego operacje organizacji, a konta bin Ladena zostały zamrożone, natomiast jego aktywa w Sudanie – skonfiskowane. Zamachy z 11 września 2001 r. kosztowały, według ustaleń komisji śledczej, 400–500 tys. dolarów, z czego około 300 tys. dolarów przeszło przez amerykańskie konta bankowe zamachowców.

Hezbollah utrzymuje się w znacznej mierze dzięki irańskiemu finansowaniu stanowiącemu od 70% do 80% całkowitego budżetu organizacji, co czyni ją silnie zależną od wsparcia zewnętrznego. Transfery odbywają się przez bezpośrednie przekazy gotówkowe, rozbudowany system finansowy wykorzystujący pośredników w Zjednoczonych Emiratach Arabskich, Turcji i Iraku, firmy przykrywkowe działające pod pozorem legalnej działalności handlowej, fałszywe faktury handlowe oraz kurierów fizycznie

przewożących gotówkę i złoto. Zamachy terrorystyczne przeprowadzone w Europie w ostatnich latach dostarczają licznych przykładów niskokosztowego finansowania o katastrofalnych skutkach dla ofiar i społeczeństw. Ataki w Paryżu w listopadzie 2015 r., które pochłonęły 130 ofiar śmiertelnych, finansowane były głównie lokalnie przez samych sprawców, a bracia Abdeslamowie sprzedali swój bar w dzielnicy Molenbeek, przeznaczając uzyskane środki na przygotowanie zamachów. Wykorzystywano karty przedpłacone zapewniające anonimowość, a Parlament Europejski stwierdził, że faktyczne finansowanie zapewniane było głównie przez lokalną pomoc i samych sprawców bez znaczącego wsparcia zewnętrznego. Badania wskazują, że do 40% europejskich aktów terrorystycznych było częściowo finansowanych przez drobną przestępczość obejmującą handel narkotykami, kradzieże, oszustwa kredytowe oraz włamania.

Współpraca międzynarodowa w zwalczaniu finansowania terroryzmu (CFT) obejmuje kompleksowy system wzajemnych ocen i monitoringu, oparty na globalnej sieci, w skład której wchodzą:

- Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF) oraz 9 regionalnych organów typu FATF (FSRB). Sieć ta łączy ponad 200 rządów i jurysdykcji oraz 20 międzynarodowych organizacji ze statusem obserwatora;
- MONEYVAL (Komitet Ekspertów ds. Oceny Środków Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu) – organ działający przy Radzie Europy od 1997 r. Zrzesza on 33 państwa i terytoria, przeprowadzając regularne wzajemne oceny ich zgodności ze standardami FATF;
- Europol – w celu wzmocnienia zdolności analitycznych Unii Europejskiej utworzył Europejskie Centrum Przeciwdziałania Terroryzmowi (ECTC) w 2016 r. oraz Europejskie Centrum Przestępczości Finansowej i Gospodarczej (EFECC) w 2020 r.;
- Program Śledzenia Finansowania Terroryzmu (TFTP) umożliwiający Departamentowi Skarbu Stanów Zjednoczonych uzyskiwanie od systemu SWIFT (Society for Worldwide Interbank Financial Telecommunication) danych o międzynarodowych transferach finansowych powiązanych z podejrzanymi o terroryzm.

Wyzwania technologiczne związane z przeciwdziałaniem finansowaniu terroryzmu obejmują rosnące wykorzystanie zdecentralizowanych finansów oraz zaawansowanych narzędzi utrudniających śledzenie przepływów środków. Dane FATF z 2023 r. wskazują, że 75% jurysdykcji jedynie częściowo lub wcale nie przestrzega wymogów dotyczących dostawców usług związanych z aktywami wirtualnymi, tworząc poważne luki w globalnym systemie nadzoru. Narzędzia analizy *blockchain* tworzone przez takie firmy, jak Chainalysis, Elliptic czy TRM Labs, umożliwiają śledzenie transakcji kryptowalutowych i pomogły odzyskać ponad 11 mld dolarów w sprawach związanych z przestępczością finansową, jednak modele sztucznej inteligencji pomimo osiągania dokładności przekraczającej 90% w identyfikacji podejrzanych transakcji napotykają istotne bariery wdrożeniowe związane z wysokimi wskaźnikami „fałszywych pozytywów".

Należy stwierdzić, że finansowanie terroryzmu ewoluuje w kierunku mikrofinansowania charakteryzującego się niskimi kwotami transakcji, zdywersyfikowanymi źródłami pozyskiwania środków oraz samofinansowaniem przez pojedynczych zradykalizowanych sprawców. Trend ku atakom niskokosztowym wykorzystującym pojazdy czy noże zamiast zaawansowanych materiałów wybuchowych dramatycznie utrudnia wykrycie przygotowań metodami analizy finansowej. Skuteczna odpowiedź na te wyzwania wymaga harmonizacji globalnej implementacji standardów FATF, wzmocnienia partnerstw publiczno-prywatnych między instytucjami finansowymi a organami ścigania, rozwoju narzędzi sztucznej inteligencji z niższymi wskaźnikami fałszywych pozytywów oraz elastycznych regulacji nadążających za innowacjami technologicznymi wykorzystywanymi przez terrorystów. System międzynarodowy obejmujący FATF, regionalne organizacje ewaluacyjne, Grupę Egmont oraz mechanizmy sankcyjne ONZ, Unii Europejskiej i Stanów Zjednoczonych zapewnia solidne fundamenty instytucjonalne, jednak jego skuteczność zależy od konsekwentnej implementacji przez poszczególne państwa oraz zdolności adaptacji do dynamicznie zmieniającego się środowiska zagrożeń.

Aleksander Wasiuta

*2024 National Terrorist Financing Risk Assessme*nt, US Treasury, Washington 2024, https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf (dostęp 21.10.2025); *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (9/11 Report), https://www.govinfo.gov/app/details/GPO-911REPORT (dostęp 21.10.2025); *Combating the Abuse of Non-Profit Organisations*, FATF, Paris 2015, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-combating-abuse-non-profit-organisations.pdf (dostęp 21.10.2025); *Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)*, https://www.fatf-gafi.org/en/countries/global-network/committee-of-experts-on-the-evaluation-of-anti-money-laundering-.html (dostęp 21.10.2025); *Comprehensive Update on Terrorist Financing Risks*, FATF, Paris 2025, https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html (dostęp 22.11.2025); *Countering the Financing of Terrorism*, https://www.unodc.org/unodc/terrorism/expertise/combating-terrorist-financing.html (dostęp 21.10.2025); J. Davis, A. Wilner, *Paying Terrorist Ransoms: Frayed Consensus*, „International Journal" 2022, vol. 77, no. 2; *Egmont Group of Financial Intelligence Units*, Egmont Group Charter, Egmont Group Secretariat, Ottawa 2023, https://egmontgroup.org/wp-content/uploads/2021/09/Egmont-Group-Charter-Revised-July-2023-Abu-Dhabi-UAE.pdf (dostęp 21.10.2025); *Ethnically or Racially Motivated Terrorism Financing*, FATF, Paris 2021, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ethnically-racially-motivated-terrorism-financing.html (dostęp 22.11.2025); *European Parliament, Directorate-General for External Policies, The Financing of the Islamic State in Iraq and Syria (ISIS)*, European Parliament, Brussels 2017, https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/603835/EXPO_IDA(2017)603835_EN.pdf (dostęp 22.11.2025); *FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, FATF, Paris 2012 (2025), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (dostęp 22.11.2025); *FinCEN, Frequently Asked Questions Regarding Suspicious Activity Reporting Requirements*, US Department of the Treasury, Washington 2025, https://www.fincen.gov/system/files/2025-10/SAR-FAQs-October-2025.pdf (dostęp 22.11.2025); *International Convention for the Suppression of the Financing of Terrorism*, 9.12.1999, https://treaties.un.org/doc/db/terrorism/english-18-11.pdf (dostęp 22.11.2025); M. Levitt, *Hezbollah: The Global Footprint of Lebanon's Party of God*, Georgetown University Press, Washington 2024; Międzynarodowa konwencja o zwalczaniu finansowania terroryzmu przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r., Dz.U. 2004, nr 263, poz. 2620; Resolution 2462 (2019) / adopted by the Security Council at its 8496th meeting, on

28 March 2019, https://digitallibrary.un.org/record/3798199?utm_source=chatgpt.com&v=pdf (dostęp 21.10.2025); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, https://sip.lex.pl/akty-prawne/dzienniki-UE/rozporzadzenie-2024-1624-w-sprawie-zapobiegania-wykorzystywaniu-systemu-72318897 (dostęp 21.10.2025); *The Soufan Center, Blockchain and Bloodshed: The Role of Cryptocurrencies in Terrorist Financing*, TSC, New York 2024, https://thesoufancenter.org/intelbrief-2024-october-16/ (dostęp 21.10.2025); *Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida and associated entities*, https://main.un.org/securitycouncil/en/sanctions/1267 (dostęp 21.10.2025); *Terrorist Financing Typologies Report*, FATF, Paris 2008, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Fatfterroristfinancingtypologiesreport.html (dostęp 22.11.2025); *UN Security Council, Resolution 1373* (2001), 28.09.2001, https://digitallibrary.un.org/record/449020?v=pdf (dostęp 21.10.2025); Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2018, poz. 723 z późn. zm.; *Virtual Assets: Targeted Update on Implementation of FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FATF, Paris 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf (dostęp 22.11.2025); *World Economic Forum, How Terrorists Fund Their Attacks – And How to Stop Them*, WEF, Geneva 2017, https://www.weforum.org/stories/2017/11/terror-attacks-are-increasingly-self-funded-how-can-we-stop-them/ (dostęp 21.10.2025).

FOMO (ang. *Fear of Missing Out*) – zjawisko lęku przed przegapieniem czegoś istotnego (np. informacji lub wydarzenia), obawa przed tym, że coś interesującego dzieje się bez naszego udziału, że coś nas ominie. FOMO często jest nasilane przez media społecznościowe i prowadzi do nieustannego sprawdzania telefonu i lęku przed byciem offline. Powoduje niepokój, stres, a nawet trudności w podejmowaniu decyzji, ponieważ osoba czuje presję bycia wszędzie i doświadczania wszystkiego.

FOMO może też być definiowane jako lęk przed przeoczeniem czegoś, strach przed tym, że inni mają lepsze i ciekawsze doświadczenia, są na bieżąco z istotnymi lub interesującymi informacjami, a my coś tracimy. FOMO to także cyfrowy niepokój, głównie pojawiający się w kontekście korzystania z mediów społecznościowych, w których obserwujemy wyidealizowane życie innych, co potęguje wrażenie, że sami jesteśmy w gorszej

sytuacji. Zjawisko to także charakteryzuje się potrzebą bycia online i przymusem ciągłego monitorowania mediów społecznościowych, sprawdzania przychodzących powiadomień i relacjonowania własnego życia.

FOMO stało się jednym z kluczowych pojęć opisujących doświadczenie życia w kulturze permanentnego połączenia z internetem. Termin ten jest już powszechnie wykorzystywany w literaturze przedmiotu jako wszechobecna obawa, że inni mogą przeżywać satysfakcjonujące doświadczenia, w których my nie uczestniczymy, połączona z silnym pragnieniem bycia stale na bieżąco z tym, co robią inni ludzie. W praktyce oznacza to kompulsywne sięganie po telefon, ciągłe odświeżanie mediów społecznościowych i trudność w odłączeniu się od sieci. Badania Andrew K. Przybylskiego i zespołu z 2013 r. przyniosły jedną z pierwszych skal pomiaru FOMO (Fear of Missing Out Scale – FoMOs), zaś w kolejnych latach zauważalne było wzmożenie intensywności prac nad tym zjawiskiem.

Badania pokazują, że FOMO wiąże się z niższym zaspokojeniem podstawowych potrzeb psychologicznych, takich jak autonomia, kompetencje i relacje, a także gorszym nastrojem i niższą satysfakcją z życia. Jednocześnie osoby z wysokim wynikiem FOMO spędzają więcej czasu w mediach społecznościowych i częściej korzystają z nich w sposób kompulsywny. Innymi słowy, FOMO nie jest „efektem ubocznym" korzystania z sieci, ale jednym z mechanizmów napędzających nadmierne używanie technologii: im bardziej boimy się, że coś nas ominie, tym częściej sięgamy po telefon, a im częściej to robimy, tym trudniej nam się odłączyć, co dalej podtrzymuje lęk.

Skala problemu jest wzmacniana przez powszechność internetu i mediów społecznościowych. Według raportu *Digital 2024* liczba aktywnych użytkowników mediów społecznościowych na świecie przekroczyła 5,04 mld, a przeciętny użytkownik spędza w nich około 2 godzin i 20–25 minut dziennie. Inne analizy wskazują, że z serwisów społecznościowych korzysta miesięcznie około 90% wszystkich internautów, a 63–64% całej populacji świata ma co najmniej jedno aktywne konto w takich serwisach. W rzeczywistości niemal każdy użytkownik internetu jest potencjalnie narażony na bodźce wywołujące FOMO: relacje z imprez, zdjęcia z podróży, informacje o sukcesach znajomych czy aktualne trendy, które „trzeba znać".

Szczególnie wyraźnie zjawisko FOMO widać wśród młodych ludzi. Raport *FOMO 2022. Polacy a lęk przed odłączeniem* pokazuje, że co trzecia osoba w wieku 15–19 lat deklaruje wyraźny lęk przed odłączeniem od sieci. Osoby z wysokim poziomem FOMO odczuwają również wyższy poziom stresu (prawie trzykrotnie wyższy niż w grupie ogólnej), częściej deklarują, że sprawdzają powiadomienia na ekranie smartfona przy każdej okazji oraz niepokoją się, gdy nie mają telefonu przy sobie. Dane te znajdują potwierdzenie w szerzej zakrojonych badaniach NASK *Nastolatki 3.0* (ogólnopolskie badanie uczniów i rodziców), które opisują polskich nastolatków jako niemal stale podłączonych do internetu – część z nich deklaruje, że ma problem z wytrzymaniem bez mediów społecznościowych dłużej niż godzinę, a średni czas korzystania z internetu przez nastolatki w dni powszednie wynosi 5 godzin i 36 minut (a w dni wolne od zajęć szkolnych czas ten wzrasta do ponad 6 godzin).

Podobne tendencje obserwuje się na świecie. Raport Pew Research Center *Teens, Social Media and AI Chatbots 2025* dotyczący nastolatków w USA wskazuje, że prawie wszyscy badani (97%) korzystają z internetu codziennie, w tym 4 na 10 osób stwierdziły, że są online „prawie bez przerwy". Równocześnie amerykański Surgeon General w specjalnym raporcie o mediach społecznościowych i zdrowiu psychicznym młodzieży (*Social Media and Youth Mental Health*) ostrzega, że intensywne korzystanie z tych platform wiąże się z podwyższonym ryzykiem zaburzeń nastroju, depresji, lęku, problemów ze snem, nadmiernego porównywania się do innych oraz doświadczania przemocy rówieśniczej w sieci. FOMO jest w tych analizach wymieniane jako jeden z kluczowych mechanizmów wzmacniających negatywny wpływ mediów społecznościowych, szczególnie wtedy, gdy młodzi ludzie mają poczucie, że ciągłe bycie online jest warunkiem akceptacji w grupie.

Literatura naukowa coraz dokładniej opisuje powiązania FOMO z problematycznym korzystaniem ze smartfonów i mediów społecznościowych. Jon D. Elhai i współpracownicy (2016) wykazali, że FOMO, obok lęku i obniżonego nastroju, jest jednym z istotnych czynników wpływających na problematyczne używanie telefonu, rozumianego jako korzystanie powodujące realne szkody w codziennym funkcjonowaniu. Badania pokazują także, że wysoki poziom FOMO przewiduje nasilenie

problematycznego używania telefonu w kolejnych miesiącach, a rolę pośredniczącą odgrywa tu m.in. używanie smartfona w poszukiwaniu pozytywnych emocji i rozładowania nudy. Innymi słowy, osoby z silnym FOMO częściej sięgają po telefon, aby poczuć się lepiej lub „być na bieżąco", co paradoksalnie pogłębia ich zależność od urządzenia.

Inne badania wskazują też na istotne związki FOMO z objawami depresji, lęku, samotności i obniżoną samooceną. Analiza dotycząca uzależnienia od mediów społecznościowych wśród studentów pokazuje, że wyższy poziom FOMO jest konsekwentnie powiązany z większym nasileniem objawów lękowych i depresyjnych oraz z niższym poczuciem własnej wartości. Inne prace sugerują, że FOMO może częściowo pośredniczyć w relacji między intensywnym korzystaniem z mediów społecznościowych a gorszym samopoczuciem psychicznym – to nie sama liczba godzin online jest tu najważniejsza, ale sposób, w jaki jednostka interpretuje treści i porównuje się z innymi. Osoby o większej podatności na porównania społeczne, niższej samoocenie czy większej wrażliwości na odrzucenie są bardziej narażone na to, że FOMO przerodzi się w przewlekłe napięcie i niezadowolenie z własnego życia.

Z perspektywy psychologicznej FOMO można rozumieć jako sygnał niezaspokojonej potrzeby przynależności i uznania społecznego. W kulturze, w której ogromna część życia towarzyskiego przeniosła się do sieci, „bycie offline" jest łatwo interpretowane jako ryzyko wypadnięcia z obiegu, czyli braku wiedzy, co się dzieje w grupie, braku reakcji na żart, nieobejrzenia transmisji z wydarzenia. Relacje znajomych, na żywo, stories i krótkie wideo tworzą iluzję, że gdzieś indziej zawsze dzieje się coś ciekawszego niż tu i teraz. Zjawisko to wzmacnia mechanizm społecznego porównywania, użytkownicy widzą głównie wyselekcjonowane, najlepsze momenty z życia innych, co sprzyja przekonaniu, że ich własne życie jest nudniejsze, mniej udane czy gorzej zorganizowane. W efekcie FOMO może prowadzić do chronicznego niezadowolenia, trudności z podejmowaniem decyzji (bo może jest gdzieś „lepsza opcja") i poczucia rozproszenia uwagi.

Konsekwencje FOMO są widoczne również w sferze funkcjonowania szkolnego i zawodowego. Raporty NASK pokazują, że znaczna część nastolatków korzysta z telefonu podczas nauki, lekcji czy odrabiania prac domowych, często „na szybko" sprawdzając powiadomienia z komunikatorów

i serwisów społecznościowych. Osoby doświadczające FOMO częściej też korzystały z internetu i mediów społecznościowych w pracy, podczas spotkań z bliskimi, przechodzenia przez ulicę czy prowadzenia samochodu. Badania nad korzystaniem z mediów społecznościowych wśród studentów wskazują także, że FOMO oraz lęk społeczny mogą negatywnie wpływać na wyniki akademickie. Coraz częściej zauważa się także, że *multiscreening i multitasking,* wielozadaniowość cyfrowa, czyli przełączanie się między ekranami, zadaniami a mediami społecznościowymi itp., wiąże się z powierzchownym przetwarzaniem informacji, spadkiem koncentracji i większym zmęczeniem poznawczym. U niektórych osób prowadzi to do błędnego koła: im gorzej radzą sobie w nauce czy pracy, tym częściej szukają ulgi i poczucia sprawczości w aktywności online, co jeszcze bardziej pogarsza sytuację.

Opisane dane nie oznaczają jednak, że każde korzystanie z mediów społecznościowych jest szkodliwe. W wielu sytuacjach pomagają one budować relacje, utrzymywać więzi na odległość, rozwijać zainteresowania czy angażować się społecznie. Kluczowe jest jednak rozpoznanie momentu, w którym korzystanie z technologii staje się problematyczne, właśnie kiedy pojawia się FOMO. Mechanizmy projektowania platform społecznościowych (m.in. powiadomienia *push*, nieskończone przewijanie, liczniki reakcji, algorytmy priorytetyzujące treści wywołujące silne emocje) są tworzone tak, aby maksymalizować czas spędzany w aplikacji i utrzymywać uwagę użytkownika. Z perspektywy profilaktyki zdrowia psychicznego oznacza to potrzebę rozwijania kompetencji cyfrowych, umiejętności samoregulacji oraz krytycznego podejścia do treści w sieci.

Odpowiedzią na FOMO nie jest całkowita rezygnacja z internetu, lecz wypracowanie bardziej zrównoważonej relacji z technologią. Badania sugerują, że nawet krótkie „detoksy cyfrowe", takie jak np. ograniczenie używania mediów społecznościowych do 30 minut dziennie przez kilka tygodni, mogą poprawiać samopoczucie, zmniejszać objawy lęku i depresji oraz obniżać poziom FOMO. Coraz częściej rekomenduje się także wprowadzanie zasad higieny cyfrowej: wyłączanie powiadomień, wyznaczanie „stref bez telefonu" (np. sypialnia, stół podczas posiłków), świadome planowanie czasu online i offline oraz regularne pytanie siebie, po co w danym momencie sięgam po smartfon. Sama świadomość, że

impulsem jest lęk przed przegapieniem, może być pierwszym krokiem do przerwania automatycznego schematu.

Istotnym kierunkiem działań jest również edukacja. Poradniki i materiały m.in. dla nauczycieli dotyczące FOMO oraz problemowego korzystania z internetu i telefonu podkreślają, że młodym ludziom trzeba nie tylko ograniczać korzystanie z telefonu, ale przede wszystkim pomagać rozwijać kompetencje emocjonalne: umiejętność radzenia sobie z nudą, odrzuceniem, gorszym samopoczuciem oraz porównywaniem się z innymi. W kontekście rodzinnym ważne jest modelowanie zachowań przez dorosłych: jeśli rodzice sami nie rozstają się ze smartfonami, trudno oczekiwać, że dziecko będzie chciało ograniczać swój czas online. Równie istotna jest rozmowa o tym, że to, co widzimy w mediach społecznościowych, jest tylko fragmentem rzeczywistości, a nie pełnym obrazem życia innych ludzi.

W ostatnich latach pojawia się też coraz więcej badań naukowych dotyczących FOMO wśród różnych grup użytkowników internetu, co pokazuje, że jest to globalne zjawisko związane z cyfryzacją życia. Przykładowo, badania wśród studentów w Arabii Saudyjskiej wskazują na istotny związek FOMO z uzależnieniem od mediów społecznościowych oraz określonymi cechami osobowości. Z kolei analizy europejskie pokazują, że FOMO może być jednym z czynników ryzyka rozwoju problematycznego używania telefonu, szczególnie u osób, które używają urządzeń mobilnych do regulowania emocji i poszukiwania pozytywnych bodźców.

Podsumowując, FOMO jest zjawiskiem wielowymiarowym: zakorzenionym w podstawowych potrzebach psychologicznych, wzmacnianym przez architekturę współczesnych platform cyfrowych i wyraźnie powiązanym ze zdrowiem psychicznym użytkowników. Dane z raportów międzynarodowych i polskich pokazują, że lęk przed odłączeniem dotyczy znaczącej części młodego pokolenia, a u części z nich przybiera formę, która realnie zaburza sen, naukę, relacje i dobrostan. Zrozumienie FOMO, w oparciu o badania naukowe, jest koniecznym krokiem do tworzenia środowiska cyfrowego, które może być wykorzystywane w sposób efektywny i bezpieczny. Jednocześnie istotna jest też analiza, jakie kompetencje informacyjne, cyfrowe i społeczne powinniśmy rozwijać, by nie żyć w permanentnym lęku, że „coś nas omija".

Perspektywa przyszłości obejmuje zarówno dalsze badania nad FOMO, jak i działania regulacyjne wobec platform cyfrowych. Coraz głośniej mówi się o konieczności projektowania serwisów w sposób uwzględniający dobrostan użytkowników, a nie wyłącznie maksymalizację czasu spędzanego w aplikacji. Dyskusja ta dopiero zaczyna się pojawiać, ale jej wynik będzie miał bezpośredni wpływ na to, jak intensywnie użytkownicy internetu będą doświadczać FOMO w przyszłości.

Paulina Motylińska

S. Buglass, *Motivators of Online Vulnerability: The Impact of Social Network Site Use and FOMO*, „Computers in Human Behavior" 2017, vol. 66(3); J.D. Elhai, *Fear of Missing Out, Need for Touch, Anxiety and Depression are Related to Problematic Smartphone Use*, „Computers in Human Behavior" 2016, vol. 63(1); M. Fabris, *Investigating the Links Between Fear of Missing Out, Social Media Addiction, and Emotional Symptoms in Adolescence: The Role of stress associated with neglect and negative reactions on social media*, „Computers in Human Behavior" 2020, vol. 106; *Global Overview Report*, https://datareportal.com/reports/digital-2024-global-overview-report (dostęp 15.12.2025); X. Hou, *The Longitudinal Association Between Fear of Missing Out, Problematic Social Media Use, and Problematic Smartphone Use*, „Addictive Behaviors" 2026, vol. 175; A. Jupowicz-Ginalska, *FOMO 2022. Polacy a lęk przed odłączeniem*, https://www.uw.edu.pl/fomo-2022-polacy-a-lek-przed-odlaczeniem/ (dostęp 13.02.2025); *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców 2023*, https://www.nask.pl/media/2024/10/Thinkstat_RAPORT_nastolatki-3_0_ONLINE-2.pdf, (dostęp 13.02.2025); A.K. Przybylski, *Motivational, Emotional, and Behavioral Correlates of Fear of Missing Out*, „Computers in Human Behavior" 2013, vol. 29(4); *Social Media and Youth Mental Health*, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf (dostęp 30.01.2026); *Teens, Social Media and AI Chatbots 2025*, https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/ (dostęp 30.01.2026).

FORMACJE POLICYJNE W POLSCE DO CZASÓW KSIĘSTWA WARSZAWSKIEGO – pojęcie „policja" pochodzi od greckiego słowa *politeia*, które określało ustrój i funkcjonowanie państwa ateńskiego i łacińskiego *politia*. W świecie nowożytnym pojawia się około roku 1500 we Francji jako *police*. W XVI i XVII w. nazywano policją całą wewnętrzną administrację poza sądownictwem, wojskowością i skarbowością (państwo policyjne).

Pozostałością tego, tak szerokiego ujęcia zakresu słowa „policja", było używanie jeszcze w okresie międzywojennym całego szeregu prawnych instytucji administracyjnych mających na celu zapewnienie społeczeństwu bezpieczeństwa, w rozmaitych dziedzinach. Za przykład można podać nazwy różnorakich instytucji, np. „policja lekarska", „policja sanitarna", „policja górnicza", „policja leśna", „policja pocztowa" itp. (dzisiaj używa się takich określeń, jak „inspekcja", „straż" itp.).

Pierwszych śladów działalności policyjnej można doszukać się już w starożytności. Za pierwowzór średniowiecznego policjanta można uznać mincerza, który był odpowiedzialny za państwową mennicę, ściąganie danin, a także przeciwdziałanie „psuciu" monety. U schyłku okresu doby plemienno-rodowej, gdy na ziemiach polskich nie wykształciły się jeszcze właściwe instytucje państwowe, społeczeństwo musiało dbać o swoje bezpieczeństwo we własnym zakresie. Wspólnoty terytorialne zwane „opolami" chroniły rody i jednostki należące do tych struktur. Wielkie rodziny obejmujące trzy lub cztery pokolenia prowadziły wspólne gospodarstwa rolne, które zapewniały im samowystarczalność i stanowiły podstawę życia społecznego. W miarę rozwoju gospodarczego z wielkich rodzin wyodrębniły się mniejsze rodziny, ale potrzeby obrony i współpracy powodowały stałe zespolenie się wzajemnych więzi. W ramach tych struktur broniono życia i mienia członków rodzin, a także organizowano tzw. „krwawą zemstę" za pozbawienia życia członka wspólnoty. Prawo zwyczajowe, które powstało w tych czasach, funkcjonowało jeszcze wiele wieków później.

Z czasem na „opola" nałożono obowiązek utrzymania porządku wewnętrznego np. w postaci zobowiązania do tzw. „śladu", czyli pogoni za przestępcą. Odpowiedzialność zbiorowa grożąca za zaniechanie tego obowiązków zmuszała ludność „opola" do wypełniania funkcji ścigania przestępców. W X–XII w. w Polsce, podobnie jak w całej Europie, nie były jeszcze rozdzielone funkcje administracyjne, policyjne i sądownicze. W okresie wczesnopiastowskim pojęcie państwa, czyli dziedziny należącej do pana, związane było z własnością władcy. Trwałość instytucji opierała się na trwałości rodziny książęcej – dynastii; to ona kształtowała formy organizacyjne i stosunki własnościowe. Teoretycznie silny władca mógł dysponować posiadanym terytorium w zasadzie bez ograniczeń.

Budowa państwa wiązała się także z istotnym przewrotem w dziejach społeczeństwa, umożliwiającym skupienie władzy w rękach księcia. Nie było wówczas różnicy między własnością państwową a własnością panującego. Wczesne państwo tworzyło wielkie aglomeracje osadnicze; dawne ośrodki plemienne, które przejmowały funkcje administracji państwowej, stanowiły siedzibę władcy, możnych i drużyny zbrojnej, której członkowie stawali się jakby „funkcjonariuszami państwowymi".

Podstawowe funkcje książęcej administracji państwowej dotyczyły trzech dziedzin życia społecznego: wojska, skarbu i sądownictwa. Niektórzy urzędnicy książęcy musieli więc, obok wielu innych, pełnić także funkcje policyjne. Wymiar sprawiedliwości pozostawał w gestii sądów opolnych, ale wyższą i ostateczną instancją stawał się sam książę, którego nadrzędnym obowiązkiem było zapewnianie bezpieczeństwa w kraju. Pewne zadania związane z bezpieczeństwem wykonywał komes pałacowy; prócz wielorakich zadań związanych z działalnością administracyjną zobowiązany był on do ścigania osób podejrzanych o popełnienie przestępstwa, bezpośrednio w otoczeniu księcia.

Prowincjami państwa wczesnopiastowskiego zarządzali namiestnicy; powoływał ich książę, a ich władza była bardzo szeroka – do ich obowiązków należało zapewnienie bezpieczeństwa wewnętrznego prowincji, ale trudno jest precyzyjnie ustalić, w jakim zakresie. Zazwyczaj wywodzili się z miejscowych feudałów i doskonale orientowali się w lokalnych realiach. Swoich urzędników książęcych posiadały także jednostki wojskowo-obronne, czyli grody. Rządca takiego grodu, zwany komesem grodowym, administrował powierzonym mu obszarem i był odpowiedzialny za ogólne bezpieczeństwo. Również mieszkańcy wspólnot terytorialnych byli zobowiązani do przestrzegania miru książęcego, m.in. odpowiadali zbiorowo za przestępstwa popełnione na ich obszarze i byli zobowiązani do uczestniczenia w ściganiu przestępców – tzw. „prawo krzyku". Krzyk polegał na obowiązku udzielenia pomocy każdemu, kto został napadnięty na gościńcu.

W XII i XIII w. wzrosło znaczenie wojewodów, którzy w zastępstwie panującego sprawowali dowództwo nad wojskiem oraz wykonywali funkcje sądownicze. Pod koniec XII w. w dzielnicy krakowskiej miejsce wojewody zajął kasztelan, a na Śląsku – komornik. Posiadali oni szeroki zakres

kompetencji i byli odpowiedzialni za ściganie sprawców przestępstw. Stopniowo jednak kasztelanowie tracili na znaczeniu, a postanowieniem statutu wiślickiego wydanego przez Kazimierza Wielkiego w połowie XIV w. zakazano im wszczynać postępowania z urzędu, bez uprzedniej skargi powoda. W drugiej połowie XIII w. pojawiła się w Polsce inkwizycja, która ścigała osoby podejrzane o herezje, prowadziła przeciwko nim śledztwa i współuczestniczyła w wydawaniu wyroków.

W XIV w. powstał w Polsce nowy organ do walki z przestępczością – justycjariusz, zwany też „oprawcą", który łączył w swym ręku funkcje polityczne i sądowe. Do „oprawców" należało ściganie przestępstw, szczególnie groźnych dla porządku publicznego. Po roku 1388 kompetencje justycjariusza zostały ograniczone tylko do spraw o kradzież. Ścigali oni sprawców przestępstw, niezależnie od ich przynależności stanowej, w przypadku gdy zostali oni złapani na gorącym uczynku lub byli publicznie wywołani. Pod koniec XIV w. oprawca został podporządkowany staroście i stracił swoje dotychczasowe uprawnienia sądowe. Miał prawo zatrzymywać osoby podejrzane, przeprowadzać rewizje pomieszczeń i zatrzymywać przedmioty pochodzące z przestępstw. Na miejscu zdarzenia przestępczego przeprowadzał swoistego rodzaju oględziny w celu wszechstronnego wyjaśnienia sprawy i wykrycia sprawcy. W Polsce urząd „oprawcy" istniał do końca XV w.

Także pewne czynności policyjne w średniowieczu podejmował urzędnik sądowy zwany prawidlnikiem. Mógł on na polecenie sądu przesłuchiwać świadków i dokonywać oględzin miejsca przestępstwa. W początkach XIII stulecia powstał urząd wojskiego: gdy urzędnicy ówczesnej administracji – wojewoda, kasztelan i chorąży – wraz z rycerstwem wyruszali na wojnę, to wojski przejmował całe rządy. Musiał tym samym zapewnić spokój i bezpieczeństwo na podległym mu terenie.

Pod koniec epoki średniowiecza rolę zbliżoną do władzy policyjnej zaczął sprawować w układzie centralnego zarządzania marszałek wielki i koronny. Funkcja ta znana była już w XIII w. i przetrwała aż do czasów pierwszego rozbioru Polski. To on miał czuwać nad bezpieczeństwem monarchy i jego dworu. Odpowiadał również za tłumienie ewentualnych zamieszek czy rozruchów, a nawet ścigał osoby używające w przestrzeni publicznej wulgaryzmów czy obelg. Marszałkowie niekiedy wydawali

wyjątkowo surowe wyroki, nawet wobec najwyższych dostojników państwowych, czego przykładem może być skazanie w 1652 r. Hieronima Radziejowskiego na karę śmierci i utratę czci – podkanclerz koronny poniósł tak drakońską karę za dopuszczenie się gwałtu. Szczególną rolę dla ukształtowania się nowego zakresu kompetencyjnego urzędu marszałka koronnego odegrał pełniący tę funkcję Franciszek Bieliński; za panowania dynastii Sasów był on symbolem skuteczności działań w obszarze zapewniania bezpieczeństwa publicznego. Współcześni zauważali, iż pomimo surowości orzekanych przez niego kar były one zawsze przemyślane i sprawiedliwe. Był on twórcą tzw. „komisji brukowej", uważając, że należy zadbać o odpowiedni stan dróg i ulic. Wychodził bowiem z założenia, że prawidłowe oświetlenie ulic wpłynie pozytywnie na redukcję liczby przestępstw.

Widocznym skutkiem zjednoczenia państwa polskiego po rozbiciu dzielnicowym było wprowadzenie stanowiska starosty. Z jednej strony, sprawował on funkcje sądowe, z drugiej zaś – odpowiadał za stan bezpieczeństwa i porządku zarówno osób prywatnych, jak i instytucji publicznych. W sprawowaniu tych zadań staroście pomagały tzw. sługi starościńskie, m.in. burgrabia; do jego kompetencji należało zapobieganie i ściganie kradzieży zarówno w samym grodzie, jak i na drogach publicznych. Starosta swą władzę administracyjno-sądowniczą sprawował przy pomocy sądów grodzkich. To właśnie one orzekały w sprawach tzw. artykułów grodzkich, do których zaliczano takie przestępstwa, jak gwałt, podpalenie, rozbój na drodze, wtargnięcie do cudzego domu. Staroście przysługiwało również „prawo miecza", czyli egzekwowanie na terenie jego jurysdykcji wyroków sądów wszystkich instancji.

Większość miast w Polsce była lokowana na prawie niemieckim, co skutkowało przejmowaniem wielu kompetencji władczych przez rady miejskie, z burmistrzem na czele. Burmistrzowie powoływali specjalne instytucje sprawujące obowiązki stróżów porządku. Taką funkcję pełnił np. tłumacz sprawujący funkcje policji handlowej i politycznej; podczas wykonywania kontroli handlowej zajmował się także wykrywaniem i obserwacją działalności szpiegowskiej, zwłaszcza na wschodnich rubieżach Rzeczypospolitej. Funkcjonariuszami policji sądowej byli natomiast prokuratorzy, do których zadań należała m.in. dbałość o zgodne z zasadami

moralności zachowanie mieszkańców. Istotne funkcje w zakresie utrzymania porządku publicznego sprawowali: instygator – rodzaj policjanta sądowego, syndyk – policjant podatkowy i kryminalny, hutman – funkcjonariusz policji targowej i opiekun kluczy do bram miejskich.

W okresie późniejszym, obejmującym wieki od XVI do XVII, z uwagi na dynamiczny wzrost przestępczości pospolitej w miastach rozpoczęto tworzenie straży miejskiej i milicji. W pierwszej połowie XVIII w. funkcje policyjne wykonywała także straż marszałkowska, która stopniowo odchodziła od swojej pierwotnej funkcji, jaką była osobista ochrona króla. Za panowania ostatniego polskiego władcy – króla Stanisława Augusta Poniatowskiego – podjęto ważną próbę szerokiego zreformowania życia publicznego, w tym także aparatu policyjnego.

W 1775 r. Rada Nieustająca powołała nowy Departament Policji, który nadzorowany był przez marszałka wielkiego; była to pierwsza instytucja państwowa, która kontrolowała działalność organizacji na obszarze całego kraju poprzez komisje boni ordinis. W okresie trwania Sejmu Wielkiego, w 1791 r. utworzono Komisję Policji Obojga Narodów, która przejęła nadzór i koordynację nad sprawami w zakresie bezpieczeństwa i porządku wewnętrznego w państwie. Była ona złożona z marszałków oraz przedstawicieli wszystkich stanów z terenów Małopolski, Wielkopolski i Litwy, a przewodził jej pracom marszałek wielki koronny Michał Mniszech. Do kompetencji komisji należały sprawy policji kryminalnej, porządkowej, obyczajowej, sanitarnej oraz opieki społecznej.

W okresie upadku Rzeczypospolitej podstawowym zadaniem policji, którą kierowali zwolennicy carycy Katarzyny Wielkiej, było rozpracowywanie i śledzenie osób podatnych na napływające z Francji idee rewolucyjne. Podczas insurekcji kościuszkowskiej wykreowano całkowicie własny wyspecjalizowany aparat ścigania. Jego kompetencje wyglądały następująco:

- Deputacja Indagacyjna – prowadzenie śledztw;
- Skład do Rewizji Papierów – badanie dokumentów urzędowych;
- Deputacja Dozorcza nad Więźniami – nadzór nad więziennictwem;
- Deputacja do Rewizji Poczty – cenzura korespondencji.

Po reorganizacji władz powstańczych 28 maja 1794 r. funkcje te pełnił Wydział Bezpieczeństwa zajmujący się następującymi sprawami: rewizje domowe, kontrola paszportów, aresztowania, nadzór nad więźniami. Oprócz Wydziału Bezpieczeństwa funkcje porządkowe pełniła przedpowstaniowa policja oraz milicja wywodząca się z pospolitego ruszenia. Władze insurekcyjne po raz pierwszy wprowadziły typ procesu zwany mieszanym, w którym występują obok siebie dwie formy – postępowanie sądowe i przygotowawcze. Polskie prawo przedpowstaniowe nie wyodrębniało postępowania przygotowawczego, którego celem było ustalenie sprawcy przestępstwa i zgromadzenie przeciwko niemu dowodów winy. Insurekcyjne postępowanie przygotowawcze wszczynane było z urzędu, przez uprawnione organy do ścigania i prowadzenia śledztwa, po wpłynięciu zawiadomienia od osoby o popełnionym przestępstwie i prawdopodobnym sprawcy.

Za obowiązek każdego obywatela uważano donoszenie o zdrajcach i wrogach ojczyzny. Postępowania wszczynano po uzyskaniu jakiejkolwiek informacji o przestępstwie; mógł ją także wszcząć z własnej inicjatywy organ powstańczy. Dowody winy były gromadzone z urzędu przez organ prowadzący śledztwo; podstawowym środkiem dowodowym w postępowaniu przygotowawczym były przesłuchania oskarżonych i świadków, a także dowody z dokumentów uzyskanych przeważnie w wyniku rewizji ambasady rosyjskiej. Przyznania się do winy przez oskarżonego nie traktowano jako dowodu koronnego. Zdarzało się, że gorliwi przesłuchujący bili przesłuchiwanego, ale organy śledcze pragnęły wyjaśnić wszelkie okoliczności czynu zarzucanego podejrzanemu, wysyłając niejednokrotnie swoich przedstawicieli poza granice Warszawy i zlecając im zbadanie sprawy na miejscu. Prawo karne powstańcze realizowało zasadę równości wobec prawa. Nie powtórzyła się sytuacja masowego terroru, jaka miała miejsce we Francji w czasie rewolucji w 1789 r.

Fakt ostatecznej utraty przez Polskę niepodległości spowodował, że na terenach poszczególnych okupacji wprowadzono prawo, zwyczaje, instytucje i urzędników państw zaborczych. Z uwagi na swe położenie na lewym brzegu Wisły Warszawa przekazana została Prusom, stąd Dyrekcją Policji kierował niemiecki urzędnik Franz Schimmelpfennig von der Oye. Pod zaborem rosyjskim w dalszym ciągu funkcjonowały polskie instytucje

ochrony bezpieczeństwa, natomiast na obszarze Galicji uruchomiono administrację austriacką. W tym kształcie organizacyjnym struktury policyjne przetrwały aż do 1806 r.

Po opuszczeniu przez pruską administrację Warszawy władzę w mieście objął książę Józef Poniatowski, który na funkcję naczelnika policji powołał Joachima Moszyńskiego. Jego następcą 15 stycznia 1807 r. został dyrektor policji hrabia Aleksander Potocki. Administracja państwowa została w tym okresie ukształtowana na bazie wzorców francuskich. Powołany został departament, w którym za sprawy bezpieczeństwa i porządku odpowiadał komisarz policji; był on zobowiązany do składania zwierzchnikom okresowych raportów, powiadamiania ich o istotnych zdarzeniach związanych z ochroną porządku, nadzorowania obiektów więziennych, dróg, karczm, cen żywności, inicjowania działań profilaktycznych zapobiegających epidemii, ścigania dezerterów i osób uchylających się od służby wojskowej, cenzurowania czasopism i zabraniania edytowania treści niepożądanych z punktu widzenia interesów państwa, zwalczanie żebractwa i włóczęgostwa. Do pomocy w realizacji tych przedsięwzięć komisarz dysponował osobami zatrudnionymi na stanowiskach intendentów. W powiatach funkcje policyjne sprawowali podprefektowie, prezydenci miast i burmistrzowie, zaś na terenie gmin wiejskich zadania te wykonywali wójtowie i sołtysi. Tak ukształtowany system organizacyjny działał do 1813 r., czyli do czasu likwidacji Księstwa Warszawskiego przez Rosjan, co nastąpiło po klęsce Napoleona i jego Wielkiej Armii.

Andrzej Czop

A. Abramski, J. Konieczny, *Justycjariusze, hutmani, policjanci*, Wydawnictwo Śląsk, Katowice 1987; M. Baczkowski, *Pod czarno-żółtymi sztandarami. Galicja i jej mieszkańcy wobec austrowęgierskich struktur militarnych 1868–1914*, Historia Jagellonoca, Kraków 2003; A. Czop, *System bezpieczeństwa publicznego w Polsce*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2012, nr 12; A. Czop, M. Sokołowski, *Geneza i rozwój formacji policyjnych w Polsce od początków państwowości do czasów Księstwa Warszawskiego*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2016, nr 24; J. Czubaty, *Księstwo Warszawskie 1807–1815*, Wydawnictwo UW, Warszawa 2011; Z. Góralski, *Urzędy i godności w dawnej Polsce*, Ludowa Spółdzielnia Wydawnicza, Warszawa 1983; A. Misiuk, *Historia*

Policji w Polsce – od X wieku do współczesności, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2012; S. Pieprzny, *Administracja bezpieczeństwa i porządku publicznego*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2012; Z. Wójcik, *Historia powszechna XVI–XVII wieku*, Wydawnictwo Naukowe PWN, Warszawa 2005.

FREGATY – obecnie najmniejsze okręty wojenne, które są zdolne do prowadzenia samodzielnych operacji; ich główną funkcją jest zapewnianie wsparcia innym jednostkom wojennym, często dzięki specjalistycznym możliwościom bojowym, np. niektóre fregaty mogą być wyposażone w broń podwodną, obronę przeciwlotniczą lub broń do zwalczania okrętów nawodnych. Niszczyciele i większe okręty (np. krążowniki rakietowe) łączą w sobie wszystkie 3 elementy. W przeszłości termin „fregata" miał różne znaczenia, np. w regionach niemieckojęzycznych statki z pełnym ożaglowaniem nazywano w XVIII i XIX w. fregatami, także te, które nie były okrętami wojennymi. Na Morzu Śródziemnym fregatą nazywano również rodzaj małego żaglowca, który mógł być wyposażony w wiosła, nie można jednak ustalić związku między nimi a późniejszymi okrętami wojennymi w kontekście ich rozwoju. Termin fregata w odniesieniu do okrętu wojennego pojawił się we Francji około polowy XVIII stulecia. Ta klasa okrętu wojennego charakteryzowała się długą, smukłą konstrukcją z pojedynczym pokładem działowym, na którym znajdowało się od 28 do 36 dział, oraz nieuzbrojonym pokładem poniżej służącym do zakwaterowania załogi. Ogólnie rzecz ujmując, fregaty w epoce żagla służyły do zadań rozpoznawczych, przechwytywania żeglugi przeciwnika, jak również ochrony własnych statków handlowych. W pewnym sensie wykonywały one zdania, które później przejęły krążowniki. W połowie XIX w. definicję fregaty rozszerzono, obejmując nią wczesne okręty pancerne, które również posiadały pokład z jednym bądź dwoma działami. Jednak późniejszy rozwój okrętów pancernych sprawił, że określenie to stało się przestarzałe, a termin wyszedł z użycia w marynarkach wojennych całego świata.

Odrodzenie fregaty jako osobnej klasy okrętu wojennego nastąpiło podczas II wojny światowej. Zagrożenie ze strony niemieckich okrętów podwodnych na Atlantyku zwiększało zapotrzebowanie na jednostki

eskortowe. Niszczycieli Royal Navy nie miała w takiej ilości, by można było pokryć zapotrzebowanie na eskortowanie dużych zespołów floty (lotniskowce oraz okręty liniowe) i konwojów statków handlowych utrzymujących komunikację między USA, Kanadą i Albionem. Co więcej – ochrona statków handlowych nie wymagała od eskortowców silnego uzbrojenia artyleryjskiego; najważniejsza była broń przeciw okrętom podwodnym. Początkowo lukę tę miały wypełnić okręty typu Flower, które zaczęto określać jako korwety i *de facto* to właśnie one były pierwowzorem współczesnych jednostek tej klasy. Jednak ich stosunkowo niewielka prędkość (ok. **16 w.** ≈ 30 km/h) nie pozwalała skutecznie walczyć z U-Bootami najnowszej generacji mogącymi na powierzchni iść z prędkością 18 w., dlatego też zaczęto szukać nowych rozwiązań konstrukcyjnych, których finalnym produktem były niszczyciele eskortowe typu Hunt – mniejsze, wolniejsze i słabiej uzbrojone (np. pozbawione wyrzutni torpedowych) od dużych niszczycieli floty budowanych dla Royal Navy (np. typ J czy M). Nie bez znaczenia był też niższy koszt tych jednostek oraz szybszy czas ich produkcji. W zasadzie niszczyciele typu Hunt stanowiły swego rodzaju etap pośredni między klasycznym niszczycielem a fregatą.

Kolejnym okrętem będącym owocem ewolucji od niszczyciela do fregaty był typ Black Swan, wreszcie pierwszymi okrętami określanymi od początku jako fregaty były River i Loch. Fregaty typu River składały się ze 151 okrętów zwodowanych w latach 1941–1944 do eskorty konwojów zwalczania okrętów podwodnych na północnym Atlantyku. Typ Loch został zaprojektowany, aby sprostać zapotrzebowaniu na dużą liczbę eskortowców dla Royal Navy. Stanowiły one rozwinięcie wcześniejszego typu River, ale zaprojektowane do masowej produkcji, z prefabrykowanymi sekcjami, które miały być budowane przez liczne firmy zbrojeniowe i montowane w stoczniach. Uzbrojenie przeciw okrętom podwodnym i sonar zostały znacząco ulepszone, ich prędkość też była wyższa.

Z kolei fregaty typu Bay budowane pod koniec II wojny światowej od początku były pomyślane jako okręty obrony przeciwlotniczej. Wprowadzenie rakiet klasy ziemia–powietrze (a później także woda–woda) od lat 50. minionego stulecia sprawiło, że stosunkowo małe okręty stały się skuteczne w obronie przeciwlotniczej. W Marynarce Wojennej Stanów Zjednoczonych (US Navy) do 1975 r. jednostki te nazywano „eskortowcami

oceanicznym", a dopiero po wprowadzeniu do służby jednostek typu Oliver Hazard Perry używa się określenia fregata.

Podczas gdy Królewska Marynarka Wojenna Kanady (Royal Canadian Navy) używała podobnych oznaczeń dla swoich okrętów wojennych zbudowanych w latach 50. XX w., brytyjska Królewska Marynarka Wojenna (Royal Navy) utrzymała termin „fregata", w latach 90. XX w. RCN ponownie wprowadziła oznaczenie „fregata". Podobnie francuska marynarka wojenna określa okręty uzbrojone w pociski rakietowe, aż do krążowników (klasy Suffren, Tourville i Horizon), mianem „fregaty", podczas gdy mniejsze jednostki określa się mianem aviso.

Obecnie we francuskiej marynarce wojennej używa się określenia fregata pierwszej bądź drugiej rangi. Marynarka radziecka używała terminu „okręt wartowniczy" (*сторожевой корабль*). Flota ZSRS miała największe zróżnicowanie wielkości okrętów zaliczanych do klasy fregat od stosunkowo małych jednostek typu Riga czy Koni po duże – typu Krivak. Co ciekawe, typ Koni był sowieckim hitem eksportowym używanym od Kuby po Algierię. W tym ostatnim kraju klasyfikowany jest jako fregata, a we wschodnioniemieckiej Volksmarine określany był jako „okręt ochrony wybrzeża".

Współcześnie fregaty są najbardziej zapracowanymi jednostkami dużych (błękitnowodnych) i średnich (zielonowodnych) flot świata. Posiadają je wszystkie większe marynarki wojenne państw NATO. Obecnie przed fregatami stawiane są następujące zadania:

- zdolność do żeglugi na pełnym morzu bez względu na warunki pogodowe;
- możliwość atakowania (i obrony przed nimi) okrętów podwodnych, samolotów lub innych jednostek pływających,
- możliwość atakowania celów naziemnych, ewentualnego wspierania desantów;
- działalność samodzielna lub w ramach większych i mniejszych zespołów sił morskich.

Obecnie do służby wchodzą, lub już weszły, fregaty V generacji; najlepiej widać to na przykładzie marynarki niemieckiej: I generacja – typ Köln, II generacja – typ Bremen, III generacja – typ Brandenburg, IV generacja – typ Sachsen, oraz V generacja – typ F125 Baden-Württemberg.

Natomiast najnowszy typ niemieckiej fregaty Baden-Württemberg, mając wyporność przekraczającą 7200 t, to największe jednostki w swej klasie na świecie. Współcześnie trudno znaleźć jakieś zasadnicze wyróżniki pozwalające na jednoznaczne odróżnienie fregat od niszczycieli, zwłaszcza gdy idzie o dużych przedstawicieli tej pierwszej klasy. Co więcej – we Francji i Włoszech zbudowano 4 jednostki typu Horizon (fr. Classe Horizon; wł. Classe Orizzonte), ale we francuskiej marynarce wojennej klasyfikowane są one jako fregaty, a we włoskiej – jako niszczyciele. Projekt ten powstawał we współpracy z Wielką Brytanią, która jednak zrezygnowała ostatecznie ze współudziału w tym przedsięwzięciu, opracowując nowy typ niszczyciela – 45. Ogólnie rzecz biorąc, przy klasyfikacji wskazuje się, że współczesne niszczyciele mają przewagę uzbrojenia ofensywnego (przeciw celom nawodnym, podwodnym i lądowym), natomiast fregaty uzbrojone są przede wszystkim w systemy defensywne (przeciw okrętom podwodnym i samolotom). W większym stopniu niż niszczycielom stawia im się także zadania związane z dozorowaniem i kontrolą dużych akwenów. Ogrywają znaczącą rolę w ochronie żeglugi oraz zwalczaniu piractwa.

Marynarka wojenna RP ma obecnie w służbie dwie fregaty ORP Kazimierz Pułaski i ORP Tadeusz Kościuszko; są to zarazem największe jednostki Polskiej Marynarki Wojennej. Obydwa okręty należą do amerykańskiego typu Oliver Hazard Perry i są już jednostkami przestarzałymi; ma temu zaradzić program Miecznik, który powstał w 2013 r. Po bardzo długich dyskusjach i planach koncepcyjnych postanowiono złożyć zamówienie na nowe fregaty u brytyjskiego producenta – Babcock International. Okręty te – bazujące na projekcie fregaty typu 31 – są budowane w liczbie 10, z czego 5 – dla Royal Navy, 3 dla – marynarki wojennej RP, oraz 2 – dla marynarki indonezyjskiej. Budowa relatywnie długiej serii okrętów znacząco obniża koszty jednostkowe. Obecnie w zaawansowanym stadium budowy znajduje się pierwsza polska fregata ORP Wicher; przypuszczalnie 2 kolejne okręty otrzymają nazwy Burza i Huragan. Nie jest do końca znana polska specyfikacja uzbrojenia i elektroniki tych jednostek, można w przybliżeniu je odtworzyć w oparciu o źródła brytyjskie. Powstające okręty należą do większych w swej klasie; ich wyporność wyniesie około 5700 t – tym samym typ Wicher to największe okręty w historii naszej floty; ich prędkość szacuje się na około 30 w. Uzbrojenie artyleryjskie ma

obejmować uniwersalne działa kalibru 76 i 35 mm, poza tym okręty te mają być wyposażone w systemy rakietowe (w pierwszym rzędzie przeciwlotnicze) oraz środki do zwalczania okrętów podwodnych. Ich wejście do służby zaplanowano na lata 2029–2030. Nowe jednostki mają wspomóc obronę przeciwlotniczą rejonu zespołu portowego Szczecin-Świnoujście oraz (a może w pierwszym rzędzie) uczestniczyć w stałych zespołach flot NATO na północnym Atlantyku oraz Morzu Śródziemnym. Zamówienie to budzi jednak kontrowersje w gronie fachowców, albowiem tak duże jednostki dysponują wprawdzie znaczącym potencjałem bojowym, ale – w warunkach morza zamkniętego, jakim jest Bałtyk – ich bojowe użycie na tym akwenie może okazać się mało zasadne.

Roman Kochnowski

J.D. Gresham, *The swift and sure steeds of the fighting sail fleet were its dashing frigates*, „Military Heritage" 2002, no. 4; G. Kolański, *Fregaty nowego pokolenia*, „Morze, Statki i Okręty" 2017, nr 1; A. Liberman, *The undiscovered origin of frigate*, https://blog.oup.com/2011/09/frigate/ (dostęp 7.12.2025); R. Osborne, *Type 31 Frigates*, „Warships: Marine News Supplement" 2021, no. 8; K.O. Sadler, *Ein Leben für den Marineschiffbau: MEKO – Eine Erfolgsstory*, Mittler, Hamburg 2007; K. Wilewski, *Takie mają być Mieczniki i Czaple*, „Polska Zbrojna" 11.07.2013, https://www.polska-zbrojna.pl/home/articleshow/8711 (dostęp 7.12.2025).

FRONDA (fr. *fronde* – proca lub katapulta) – symbolizuje powstanie, opór, sprzeciw wobec władzy, współczesne ogólne określenie opozycji politycznej lub antyrządowych wystąpień, czasami z sceptyczno-ironicznym wydźwiękiem.

Historyczne korzenie nazwy sięgają wydarzeń we Francji z połowy XVII w. W szczytowym okresie wojny 30-letniej, w latach 1618–1648 Francja otwarcie weszła w konflikt, aby przeciwstawić się Habsburgom, wypowiadając wojnę Hiszpanii, która trwała do 1659 r. Wydatki wojskowe zmusiły rząd Giulia Mazarina (1642–1661) do znacznego podwyższenia podatków, zaś szlachta odmówiła ich płacenia, powołując się na swoje dawne swobody lub przywileje. W maju 1648 r. nałożenie podatku na urzędników sądowych parlamentu paryskiego wywołało nie tylko odmowę zapłaty, ale także potępienie wcześniejszych edyktów finansowych i żądanie przyjęcia

planu reform konstytucyjnych opracowanego przez zjednoczony komitet parlamentu, złożony z członków wszystkich suwerennych dworów Paryża. Presja władzy zagroziła tradycyjnym swobodom; na tle złożonej sytuacji społeczno-gospodarczej i politycznej w latach 1648–1653 we Francji trwała seria powstań i wojen domowych.

W 1648 r. wybuchły powstania przeciwko regencji Anny Austriaczki, matki 10-letniego wówczas Ludwika XIV, i rządom jej ministra, kardynała Mazarina, głównie w Paryżu i okolicach. Celem było wykorzystanie momentu słabości monarchii i przywrócenie feudalnych praw szlachty oraz uprawnień parlamentu do weta w decyzjach, które zostały poważnie ograniczone za czasów Ludwika XIII i jego ministra, kardynała Richelieu.

Wyróżnia się dwa okresy Frondy: parlamentarny (1648–1649), kiedy to koncentrowano się na sprzeciwie parlamentu wobec nowych podatków i przejawów uzurpacji władzy, oraz książąt (1650–1653) oznaczający konflikt między arystokratami, niezadowolonymi utratą wpływów i ograniczeniem przywilejów, a rządem królewskim. Parlamenty – najwyższe organy sądowe w swoich regionach – miały ograniczone funkcje polityczne: posiadały prawo rejestrowania dekretów królewskich, po czym te ostatnie nabierały mocy prawnej w danej prowincji. Akty, zarejestrowane w paryskim parlamencie, wchodziły w życie we wszystkich prowincjach, które nie miały przywileju tworzenia własnych izb sądowych. Mogły one również odmówić rejestracji dekretu, składając sprzeciw lub uwagi (fr. *remontrances*), jeśli uznały, że dokument jest sprzeczny z prawem lub interesami królestwa.

Powstanie, które rozpoczęło się w 1648 r., miało na celu ochronę ustanowionych praw parlamentu przed królewskimi nadużyciami. Wśród postulatów zawartych w deklaracji „27 artykułów" z 15 czerwca 1648 r. znalazły się: ustanowienie podatków za zgodą parlamentu, likwidacja instytucji intendentów, zakaz aresztowania poddanych bez wyroku sądowego. W rzeczywistości chodziło o ograniczenie uprawnień suwerena; parlamenty stały się ośrodkami opozycji wobec absolutyzmu. Pierre Brussel (1575–1654), przewodniczący parlamentu paryskiego, stał się przywódcą parlamentarnej Frondy. Opór parlamentu dodał odwagi mieszkańcom Paryża – kiedy w sierpniu przywódcy opozycji zostali aresztowani na polecenie rządu, Paryżanie stanęli w ich obronie.

27 sierpnia 1648 r. przeszedł do historii Francji jako „dzień barykad", gdyż powstańcy zbudowali wtedy w Paryżu 1260 tego rodzaju zapór. Regentka królestwa, matka Ludwika XIV (1638–1715) Anna Austriaczka (z rodu hiszpańskich Habsburgów) została zmuszona do ogłoszenia 28 sierpnia uwolnienia aresztowanych, a już w październiku podpisała „27 artykułów" – ta deklaracja oznaczała w istocie zwycięstwo parlamentu. Jeden z uczestników Frondy, aktywny przeciwnik absolutyzmu Jean-François Paul de Gondi, kardynał Retz (1613–1679), w swoich wspomnieniach wywodził pochodzenie nazwy od wypowiedzi francuskiego poety, sekretarza parlamentu paryskiego, uczestnika Frondy, którym był François Le Coigneux de Bachaumont (1624–1702): „Bachaumont powiedział kiedyś żartobliwie, że parlament zachowywał się jak uczniowie w paryskich rowach, którzy rzucają kamieniami (*frondent*) i uciekają, gdy widzą konstabla, ale wracają, gdy tylko się odwróci". Mieszkańcy Paryża często używali proc, aby rozbijać okna zwolenników kardynała Mazarina. Jednak 24 października 1648 r. podpisano pokój westfalski, a kardynał Mazarin postanowił przejść do radykalnych metod rozwiązania kryzysu, ponieważ władze nie zamierzały godzić się z październikową deklaracją.

W 1650 r. rozpoczęła się nowa faza ruchu – „Fronda książęca". Kierownictwo przejęła arystokracja, która nie miała żadnego programu wykraczającego poza zaspokajanie własnych ambicji lub interesów: nie wyobrażała sobie żadnego innego ustroju państwowego poza absolutyzmem. „Fronda książęca" rozpoczęła się po aresztowaniu 14 stycznia 1650 r. Armanda de Bourbona (księcia Conti), Ludwika II de Bourbon-Condé (Wielkiego Condé) i Henryka II, księcia de Longueville, chociaż było to sprzeczne z deklaracją z 22 października 1648 r. Na żądanie ludności rząd zwolnił aresztowanych, a Mazarin podał się do dymisji. Fronda stała się historią intryg, w centrum których znaleźli się niezadowoleni książęta i szlachta. Do kwietnia 1651 r. powstania wszędzie zakończyły się klęską, jednak w grudniu kardynał Mazarin powrócił do Francji z niewielką armią i wojna rozpoczęła się od nowa. Zmęczony chaosem kraj zaczął postrzegać króla i jego otoczenie jako przedstawicieli porządku. 21 października 1652 r. władca ogłosił powszechną amnestię, z której wykluczono najbardziej aktywnych frondystów. Chociaż deklaracja z 22 października 1648 r. nie została otwarcie uchylona, w rzeczywistości położyło to kres roszczeniom

wyższych izb sądowych do udziału w zarządzaniu krajem w sposób inny niż tradycyjne składanie protestów. Faktycznie Fronda zakończyła się po podporządkowaniu miasta Bordeaux władzy królewskiej w sierpniu 1653 r. Ostatni ogień Frondy został zlikwidowany wraz z zajęciem miasta Périgueux we wrześniu 1653 r. Mazarin powrócił do Paryża i do śmierci pełnił obowiązki pierwszego ministra królestwa.

Rząd młodego króla Ludwika XIV stawił czoła połączonej opozycji książąt, szlachty, szlacheckich zgromadzeń sądów regionalnych (*parlements*), a także dużej części ludności francuskiej, i zdołał ich wszystkich podporządkować. Spór rozpoczął się, gdy rząd Francji wydał 7 edyktów fiskalnych, z których 6 miało na celu zwiększenie podatków. Parlamenty stawiały opór, kwestionowały konstytucyjność działań króla i dążyły do ograniczenia jego uprawnień.

W końcu Fronda nie wyrządziła poważnej szkody monarchii, a wręcz przeciwnie, wzmocniła władzę króla i utorowała drogę do absolutyzmu Ludwika XIV.

Fronda – jako symbol oporu, nieakceptacji autorytaryzmu i pragnienia zmian politycznych – jest aktualna również dzisiaj. Termin ten aktywnie wykorzystuje się we współczesnym dyskursie politycznym do analizy i opisu różnych konfrontacji oraz konfliktów.

Frondę można porównać do rewolucji lub protestów, w szczególności do wydarzeń, w których doszło do starcia między władzą monarchiczną a siłami społecznymi dążącymi do ograniczenia jej wpływów lub obrony swoich praw. I tak, w XIX w. we Francji odbyła się tzw. „rewolucja lipcowa" 1830 r. jako sprzeciw wobec absolutystycznych tendencji monarchy; w latach 20. XX w. w Hiszpanii – opozycja wobec dyktatury Primo de Rivery, a następnie wojna domowa (1936–1939) – walka różnych sił politycznych i społecznych o formę władzy, zaś na początku XXI w. – „arabska wiosna" (2010–2012): seria masowych protestów społecznych i konfliktów zbrojnych w wielu krajach arabskich przeciwko autorytarnym reżimom.

Fronda, jako symbol oporu wobec nadmiernej władzy i obrony wolności, jest widoczna w kulturze politycznej Stanów Zjednoczonych. Tradycja ta pojawiła się już w XVIII w. w sporach między federalistami a antyfederalistami, kiedy społeczeństwo domagało się ograniczenia władzy centralnej i gwarancji praw obywatelskich. Powstanie rolników w latach 1786–1787

w Massachusetts przeciwko presji podatkowej i polityce zadłużenia rządu stanowego pod przywództwem weterana wojny o niepodległość Daniela Shaysa przekonało część polityków do konieczności stworzenia silnego rządu federalnego i przyspieszyło przyjęcie konstytucji. Historia Ameryki pokazuje, że Fronda może być nie buntem przeciwko systemowi, ale jego wewnętrznym mechanizmem samodoskonalenia i ochrony swobód obywatelskich.

W dzisiejszym kontekście politycznym termin „fronda" oznacza wewnętrzną opozycję w ramach systemu władzy lub politycznego, przejaw elitarnej protestacji przeciwko centralizmowi, autorytaryzmowi lub oficjalnej linii, łączącej krytykę z lojalnością wobec samej struktury. Fronda zapobiega stagnacji i tendencjom autorytarnym; jej przejawami mogą być publiczne wystąpienia deputowanych przeciwko decyzjom rządu, niezależne stanowisko części dziennikarzy lub sprzeciw organizacji społecznych wobec nadużyć biurokratycznych.

Wewnątrzśrodowiskowy konflikt miał miejsce w Stowarzyszeniu PAX – organizacji utworzonej w 1947 r., za pomocą której władze Polskiej Rzeczypospolitej Ludowej próbowały podporządkować sobie Kościół katolicki. W 1955 r. niektórzy działacze grupy utworzyli tzw. fronde, zarzucając ówczesnemu kierownictwu brak wewnętrznej demokracji, autokratyczne rządy i niewłaściwy system zgłaszania kandydatów. W wyniku konfliktu z kierownictwem PAX organizację opuścili m.in. Tadeusz Mazowiecki i Janusz Zabłocki.

Fronda w dniu dzisiejszym to oznaka dojrzałości systemu politycznego, który jest w stanie wysłuchać własnej opozycji wewnętrznej. To właśnie dzięki takim formom umiarkowanego protestu społeczeństwo stopniowo zmierza w kierunku większej otwartości i odpowiedzialności władzy wobec obywateli. Termin ten można stosować do opisania wewnętrznej opozycji politycznej w partiach lub organizacjach (opór wewnątrz systemu), społeczeństwie obywatelskim (forma protestu przeciwko działaniom władzy jako stała, krytyczna kontrola społeczeństwa nad jej działaniami), polityce międzynarodowej (demonstrowane nieposłuszeństwo wewnątrz wspólnego bloku, ale bez zerwania stosunków).

Zoya Baran

J. Baszkiewicz, *Historia Francji*, Ossolineum, Wrocław 2008; *Fronde* [hasło], [w:] *Encyclopedia Britannica*, vol. 11, H. Chisholm (ed.), Cambridge University Press, Cambridge 1911, https://en.wikisource.org/wiki/1911_Encyclop%C3%A6dia_Britannica/Fronde,_The (dostęp 16.12.2025); N.R. Gelbart, *„Frondeur" Journalism in the 1770s: Theater Criticism and Radical Politics in the Prerevolutionary French Press. Theater Criticism and Radical Politics in the Prerevolutionary French Press*, „Eighteenth-Century Studies" 1984, vol. 17, no. 4, https://www.jstor.org/stable/2738132 (dostęp 16.12.2025); A. Mączak, *Europa i świat w początkach epoki nowożytnej*, cz. 1, Wiedza Powszechna, Warszawa 1991; T. Sikorski, *Fronda. Rozłam w Stowarzyszeniu PAX w 1955 roku. (Geneza – przebieg – konsekwencje)*, „Dzieje Najnowsze" 2018, r. L. 1, https://rcin.org.pl/ihpan/Content/65803/PDF/WA303_84401_A507-DN-R-50-1_Sikorski.pdf (dostęp 16.12.2025); В. Ададуров, *Історія Франції. Королівська держава та створення нації (від початків до кінця XVIII століття)*, Видавництво УКУ, Львів 2002.

FUNDACJA NA RZECZ MIĘDZYNARODOWEGO POKOJU CARNEGIE (Carnegie Endowment for International Peace, CEIP) – założona w 1910 r. organizacja pozarządowa, której najważniejsze zadania koncentrują się na promowaniu pokoju na świecie, opracowywaniu strategii, analiz, a także wspieraniu naukowców, krajów i instytucji w rozwiązywaniu globalnych problemów. *Think tank*, który utworzył amerykański przedsiębiorca Andrew Carnegie w okresie II wojny światowej oraz zimnej wojny, odegrał istotną rolę w kształtowaniu amerykańskiej i międzynarodowej polityki zagranicznej. W 1945 r. były prezydent CEIP James T. Shotwell przewodził delegacją doradców podczas konferencji, na której opracowano Kartę Narodów Zjednoczonych. Shotwell przekonał delegację USA do wniesienia poprawki do projektu Karty ONZ, która ustanowiła stałą Komisję Praw Człowieka ONZ. Na początku lat 70. XX w. CEIP opracowała długoterminowy plan redukcji ryzyka bezpieczeństwa jądrowego, skupiając się na negocjacjach dwu- i wielostronnych jako najwydajniejszych środkach redukcji zagrożenia stwarzanego przez broń jądrową, której rozwój w kolejnych dekadach przyczynił się do postrzegania CEIP jako organizacji tworzącej m.in. analizy poruszające problematykę zapobiegania eskalacji konfliktów zbrojnych. W 2002 r. przedstawiciele CEIP uczestniczyli w ocenie charakteru działań, jakie Stany Zjednoczone miały podjąć w odpowiedzi na zagrożenie terrorystyczne w następstwie ataków z 11

września 2001 r. W tym celu CEIP powołała do życia grupę roboczą, która zgodnie z rezolucją ONZ nr 1441 wystosowała kilka zaleceń skutecznego systemu inspekcji broni masowego rażenia mającego na celu ograniczenie ryzyka wybuchu kolejnej wojny. W 2018 r. CEIP zapoczątkowała wieloletni projekt badawczy, który w odpowiedzi na potrzeby amerykańskiej klasy średniej poświęcony został kształtowaniu polityki zagranicznej. W tym celu powołano dwupartyjną grupę zadaniową ds. klasy średniej, która w wybranych stanach USA prowadziła badania dotyczące postrzegania i aspiracji amerykańskiej klasy średniej oraz roli odgrywanej przez USA w zglobalizowanym świecie. Rezultatem prac jest raport, którym w kształtowaniu polityki zagranicznej USA mogą posiłkować się m.in. decydenci Białego Domu oraz Departamentu Stanu. Wśród najważniejszych trzech priorytetów realizowanych obecnie przez CEIP można wymienić:

- rozwiązywanie problemów geopolitycznych poprzez tworzenie kompleksowych analiz uwzględniających zmieniające się siły ekonomiczne, globalne i regionalne kwestie polityczne w ujęciu konkurencyjności, a także warunków mogących powodować potencjalne konflikty w przypadku istotnych zmian politycznych;
- analizę regionów rozwijających się, które dzięki stałemu monitoringowi i eksperckiej analizie zagadnień regionalnych oraz funkcjonalnych zapewnia nowe spojrzenie na stale zmieniający się świat;
- nowe technologie i współczesne zarządzanie to stale rozwijające się wyzwania polityczne, które tworzą się w związku z bezprecedensowymi globalnymi zmianami i możliwościami, jakie towarzyszą najnowszej polityce. Z tego względu CEIP priorytetowo traktuje możliwość tworzenia długoterminowej i interdyscyplinarnej wiedzy specjalistycznej, która mogłaby pomóc rządom i przedstawicielom przemysłu zrozumieć współczesne wyzwania związane z zarządzaniem oraz nowymi technologiami.

Na rzecz Fundacji badania opracowuje międzynarodowe grono ekspertów, które poprzez powstałe analizy stosuje liczne rekomendacje obejmujące większość regionów świata, takich jak Azja Wschodnia

i Południowa, Afryka, Europa, Rosja i Eurazja, Bliski Wschód, oraz regionów subnarodowych, tj. Kalifornię. Obok programów stałych CEIP wyróżnić należy prowadzone badania dotyczące geopolityki i ekonomii UE, które umożliwią, w ocenie autorów, wydajność i utrzymanie międzynarodowej wiarygodności dzięki zrównoważonemu dążeniu do bezpieczeństwa ekonomicznego z szerszymi celami polityki zagranicznej, a także stworzenie dokumentacji związanej z nową strategią i polityką sojuszu technologicznego USA–Korea Południowa. CEIP w ostatnim czasie przeprowadziła audyt środowiskowy dla Egiptu, w wyniku którego wystosowano rekomendacje dotyczące utworzenia zintegrowanych ram planowania, monitorowania i łagodzenia zmian klimatycznych powstałych w wyniku licznych projektów zarządzanych przez egipskie wojsko w sferze cywilnej. W ostatnich latach CEIP prowadziła obszerną analizę współczesnych wyzwań globalnych w związku ze skutkami pandemii COVID-19, a także mierzyła wpływ wdrożonych przez poszczególne państwa rozwiązań na zarządzenie i bezpieczeństwo międzynarodowe. Spośród najważniejszych inicjatyw i programów realizowanych przez CEIP w trybie stałym można wymienić:

- Program Afryka obejmujący dział ekonomiczny, polityczny i transnarodowy, który w myśl ekspertów CEIP ma bezpośrednie przełożenie na kształtowanie przyszłości Afryki. Poprzez prowadzenie badań opartych na zgromadzonych danych, inicjowanie dialogu na wysokim szczeblu, tworzenie strategicznych partnerstw oraz wzmacnianie głosu Afryki na świecie program zgodnie z założeniami autorów uzupełnia wiedzę na temat roli Afryki w zmieniającym się świecie;
- Program Amerykańska Stanowość opracowuje oraz rozwija pomysły dotyczące poprawy polityki zagranicznej Stanów Zjednoczonych, które są zgodne z amerykańskimi wartościami w coraz bardziej konkurencyjnym świecie;
- Program Azja bada rolę sposobu zarządzania i wykorzystywanej technologii jako potencjalnego zagrożenia dla światowego pokoju, a także analizuje możliwości identyfikacyjne w regionie Azji i Pacyfiku, w tym w Chinach, Japonii i na Półwyspie Koreańskim;

- Program Carnegie California mający na celu prowadzenie na zachodnim wybrzeżu Stanów Zjednoczonych globalnego dialogu na temat rozwoju technologii w ujęciu ponadnarodowym i transpacyficznym;
- Program ds. Demokracji, Konfliktów i Rządów jest wiodącym źródłem CEIP obejmującym badania polityczne, raporty oraz działania informacyjne dotyczące globalnej demokracji, konfliktów, a także rządów. Program ponadto analizuje i dąży do zwiększenia efektywności międzynarodowej aktywności mającej na celu ograniczanie stopnia odchodzenia od praktyk demokratycznych, łagodzenia konfliktów i aktów przemocy, przezwyciężenia polaryzacji politycznej, promowania równości płci oraz prodemokratycznego wykorzystania nowych technologii;
- Program Europejski z siedzibą w Waszyngtonie bada rozwój sytuacji politycznej i bezpieczeństwa w Europie, stosunki transatlantyckie oraz globalną rolę Europy. Współpracując z Carnegie Europe w Brukseli, skupia amerykańskich i europejskich decydentów politycznych oraz ekspertów w kwestiach zagadnień strategicznych stojących przed Europą;
- Program Porządku i Instytucji Światowych identyfikuje obiecujące nowe inicjatywy oraz działania wielostronne mające na celu stworzenie bardziej pokojowego, dostatniego, sprawiedliwego i zrównoważonego świata. Misją programu jest opracowywanie rozwiązań globalnych problemów, takich jak konkurencja geopolityczna, nacjonalizm, nierówności ekonomiczne, innowacje technologiczne zagrażające bezpieczeństwu międzynarodowemu, a także inne działania mogące przyczyniać się do zachwiania porządkiem międzynarodowym oraz utrudniania wspólnego reagowanie na nie;
- Program Bliskiego Wschodu z siedzibą w Waszyngtonie łączy wiedzę regionalną z dokładną analizą porównawczą, której zasadniczym celem jest opracowanie wysoce użytecznych zaleceń. Dysponując wiedzą specjalistyczną w zakresie Zatoki Perskiej, Afryki Północnej, Iranu i Izraela oraz Palestyny, bada kwestie

zmian politycznych, gospodarczych i społecznych zarówno w języku angielskim, jak i arabskim;
- Program Polityki Nuklearnej ma na celu zmniejszenie ryzyka wybuchu wojny nuklearnej. Eksperci diagnozują zagrożenia wynikające z rozwoju technicznego i geopolitycznego, opracowują pragmatyczne rozwiązania i wykorzystują globalną sieć do promowania polityk ograniczania ryzyka. Zakres tematyczny programu obejmuje odstraszanie, rozbrajanie, kontrolę zbrojeń, zapobieganie eskalacji oraz energię jądrową;
- Program Rosja i Eurazja obejmuje niezależne badania nad głównymi trendami politycznymi, społecznymi i związanymi z bezpieczeństwem w polityce USA wobec regionu, który doświadczył zmian w wyniku wojny Rosji z Ukrainą. Zasadniczym celem regularnego dostarczania przywódcom opracowanych raportów i analiz jest ułatwienie podejmowania decyzji politycznych;
- Program Azja Południowa skupia się na debatach politycznych dotyczących bezpieczeństwa, gospodarki i rozwoju politycznego regionu. Począwszy od strategicznej konkurencji w rejonie Indo-Pacyfiku, po wewnętrzną dynamikę Indii i zaangażowanie USA w regionie, oferuje liczne badania i analizy dotyczące najważniejszych wyzwań Azji Południowej;
- Program Zrównoważonego Rozwoju, Klimatu i Geopolityki bada, w jaki sposób zmiany klimatu i reakcje na nie kształtują politykę międzynarodową, globalne zarządzanie i bezpieczeństwo świata. Program analizuje również geopolityczne implikacje dekarbonizacji, a także problemów środowiskowych oraz innych wyzwań umożliwiających stworzenie stabilnych łańcuchów dostaw energii;
- Program ds. Technologicznych i Międzynarodowych opracowuje plany pozwalające sprostać wyzwaniom zarządzania i ryzyka związanym z nowymi technologiami. Analitycy w swoich raportach tworzą rekomendacje praktyk dla liderów gospodarki oraz polityki w zakresie sztucznej inteligencji, zagrożeń cybernetycznych, bezpieczeństwa chmury, przeciwdziałania

obcym wpływom, zmniejszania ryzyka biotechnologii, a także zapewniania globalnej integracji cyfrowej.

CEIP poza biurami w Waszyngtonie posiada centra globalne w Azji, Bejrucie, Brukseli i Nowym Delhi. W ramach swojej działalności korzysta z analiz ponad 150 ekspertów, aby w pełniejszym stopniu zrozumieć zagrożenia i możliwości kształtujące globalne bezpieczeństwo oraz dobrobyt, a także przygotować następne pokolenie liderów polityki zagranicznej poprzez szkolenia i mentoring. Dzięki prowadzeniu strategicznych dialogów i dyplomacji zakulisowej CEIP podejmuje działania umożliwiające pogłębienie i wzmocnienie relacji pomiędzy międzynarodowymi podmiotami, które poszukują rozwiązań w spornych kwestiach. W 2025 r. funkcję prezesa CEIP sprawował Mariano-Florentino (Tino) Cuéllar.

Artur Jach-Chrząszcz

Carnegie Endowment for International Peace, https://carnegieendowment.org (dostęp 15.11.2025); Q. Lyu, Y. Liu, *Academic pursuits and involvement in decision-making: study on the formation of U.S. university think tanks*, „Administrative Sciences" 2023, no. 13(3), https://doi.org/10.3390/admsci13030093 (dostęp 15.11.2025); I. Parmar, *Engineering consent: the Carnegie endowment for international peace and the mobilization of american public opinion 1939–1945*, „Review of International Studies" 2000, no. 26(1), https://doi.org/10.1017/s0260210500000358 (dostęp 15.11.2025); K. Topping, Y. Hosny, L. Hunter, *The effects of covid-19 on domestic and international security in democratic and authoritarian regimes*, „Politics and the Life Sciences" 2023, no. 43(1), https://doi.org/10.1017/pls.2023.18 (dostęp 15.11.2025).

G

GABINET CIENI (ang. His Majesty's Most Loyal Opposition Shadow Cabinet, Shadow Cabinet) – tworzona przez opozycję parlamentarną struktura złożona z polityków szczegółowo analizujących płaszczyzny działania rządu (np. zdrowie, edukacja, polityka zagraniczna), którzy w razie wygranej ich partii w wyborach przejmą odpowiednie stanowiska ministerialne. Instytucja wywodząca się z Wielkiej Brytanii współcześnie występuje także w innych państwach, które przyjęły westminsterski system rządów, takich jak Nowa Zelandia, Australia czy Kanada. Funkcjonowanie gabinetu cieni ma przygotować partię opozycyjną do przejęcia odpowiedzialności za zrządzenie państwem oraz umożliwić łagodniejszą transformację władzy. Pozwala również w usystematyzowany i zinstytucjonalizowany sposób kontrolować politykę rządu oraz w odpowiedzi na nią przygotowywać własne cele i założenia polityczne.

Geneza gabinetu cieni sięga XIX w., kiedy to wraz z kolejnymi reformami prawa wyborczego (Ch. Grey'a z 1832 r., B. Disraeliego z 1867 r. oraz W. Gladstone'a z 1885 r.), włączającymi w proces elekcji niższej izby parlamentu coraz większe grupy obywateli, pozostające w opozycji ugrupowania polityczne podjęły wysiłki zmierzające do opracowania

strategii pozwalającej na agregację poparcia wyborczego, a w rezultacie – odzyskanie władzy. Jej głównym założeniem było usystematyzowania struktury partyjnej oraz wyodrębnienie wąskiej grupy polityków, która nie tylko sprawowałaby kierownictwo nad frakcją parlamentarną, ale także prezentowała stanowisko partii w relacjach z elektoratem. Ta grupa bliskich współpracowników szefa najliczniej reprezentowanego w Izbie Gmin opozycyjnego ugrupowania politycznego w przypadku wygranej wraz z nim miała utworzyć rząd. Mimo iż formacja ta nie była wówczas nazywana gabinetem cieni, gdyż terminem tym zaczęto posługiwać się znacznie później, nie ma wątpliwości, że taką rolę odgrywała.

Termin „gabinet cieni" pojawił się po raz pierwszy w dyskursie publicznym w latach 80. XIX w. dla określenia byłych ministrów, którzy musieli opuścić urzędy w związku z utratą władzy przez ich partię. W pierwszych latach XX w. określenie to zmieniło nieco swój sens, przybierając współczesne znaczenie. Początkowo opisywana instytucja miała charakter nieformalny, chociaż z biegiem lat ugruntowała swoją pozycję, stając się istotną częścią systemu politycznego Wielkiej Brytanii, a później również innych państw anglosaskich. Wskazuje się, że pierwsze kroki w umocnieniu znaczenia tej struktury odegrała Partia Pracy, która wyparłszy w latach 20. ubiegłego wieku liberałów, stała się główną siłą polityczną konkurującą z konserwatystami. Na skutek m.in. bardziej usystematyzowanych działań laburzystów w opozycji przedstawiciele tego ugrupowania w 1924 r. po raz pierwszy w historii utworzyli rząd.

Kolejne dekady nie przyniosły znaczących zmian, zwłaszcza że podczas II wojny światowej brytyjski rząd miał charakter gabinetu koalicyjnego, tworzonego przez przedstawicieli wszystkich ugrupowań politycznych. Do praktyki powoływania gabinetu cieni powrócono w latach 50., kiedy to w warunkach systemu dwupartyjnego oba ugrupowania: Partia Konserwatywna i Partia Pracy, wypracowały trwałe zasady jego wyłaniania. Torysi od początku mający pełnię kompetencji związanych z wyborem gabinetu cieni powierzali władzę swojemu liderowi, zakładając, że powinien on dysponować uprawnieniami analogicznymi do tych, które posiada premier. W związku z tym, to on, dbając o jedność partyjną oraz biorąc pod uwagę doświadczenie i predyspozycje poszczególnych posłów, dokonywał nominacji.

Odmienny punkt widzenia prezentowano w Partii Pracy, gdzie zdecydowano się na wdrożenie wewnątrzpartyjnego mechanizmu elekcji osób pełniących najważniejsze funkcje partyjne. Po raz pierwszy system ten zastosowano w 1923 r., jednak wybory odbywały się nieregularnie. Dopiero od lat 50. laburzystowscy parlamentarzyści zasiadający w Izbie Gmin systematycznie brali udział w wyborach gabinetu cieni. Odbywały się one każdego roku, gdy ugrupowanie znajdowało się w opozycji. Każdy poseł mógł wskazać kilkunastu kandydatów, którzy, w jego opinii, najlepiej prezentowaliby partyjną agendę. Osoby cieszące się największym poparciem wchodziły w skład gabinetu cieni, następnie lider partii rozdzielał płaszczyzny działania pomiędzy zaineresowanych oraz gdy istniała taka potrzeba – poszerzał skład o kilku członków. Do znaczącej zmiany mechanizmu doszło dopiero w 1981 r., od kiedy to każde z kluczowych stanowisk wybierano osobno. W 2011 r. zrezygnowano zaś zupełnie z wyborów partyjnych, powierzając misję utworzenia gabinetu cieni szefowi partii.

Współczesna struktura gabinetu cieni tworzonego i obsadzanego przez lidera opozycji (Leader of the Opposition) odzwierciedla zwykle strukturę aktualnego rządu. Stanowiska są rozdzielane między najważniejszych polityków opozycyjnych, zasiadających w Izbie Gmin bądź w Izbie Lordów. Odtąd w Wielkiej Brytanii nazywa się ich ministrami cieniami (*shadow minister*). Omawiana instytucja pozostaje najważniejszym elementem oficjalnej Opozycji Jego Królewskiej Mości (His Majesty's Loyal Opposition), której status częściowo uregulowano w ustawie. Po raz pierwszy normy prawne dotyczące tej struktury zostały zawarte w Ustawie o ministrach Korony z 1937 r. (Ministers of the Crown Act, 1937) przyznającej liderowi opozycji wynagrodzenie z budżetu państwa, a tym samym uznającej istnienie oficjalnej opozycji. Obecnie kwestie te normuje Ustawa o ministerialnych i pozostałych uposażeniach z 1975 r. (Ministerial and other Salaries Act, 1975).

Głównym zadaniem gabinetu cieni pozostaje szczegółowa kontrola działań rządu. Wyznaczenie konkretnych osób do monitorowania odpowiednich polityk publicznych pozwala opozycji szybko reagować na decyzje rządzących oraz sprawia, że wraz z upływem czasu ministrowie cienie dokładnie poznają sposób pracy poszczególnych resortów. To, z jednej strony, umożliwia bardziej merytoryczną i przemyślaną krytykę,

z drugiej zaś – przygotowuje ich na ewentualność przejęcia rozpoczętych inicjatyw i reform. Nie bez znaczenia jest również fakt, że zdobytą wiedzę i doświadczenie wykorzystują oni, przygotowując własne propozycje priorytetów politycznych, które najczęściej stają się oficjalną polityką partyjną w tym zakresie. Co interesujące, gabinety cieni analogicznie do rządu podlegają rekonstrukcji, w związku z czym liderzy opozycji mogą swobodnie dokonywać zmian w ich składzie.

Ministrowie cienie w parlamencie zajmują ławy usytuowane naprzeciwko tych zajmowanych przez rząd. Jakkolwiek zgodnie z konwencją gabinet cieni zwykle „stanowi lustrzane odbicie rządu", zdarza się, że lider opozycji powołuje w jego skład dodatkowych członków mających przygotować propozycje polityczne dla obszaru uznanego za szczególnie istotny. Odpowiednie rozdzielenie stanowisk ma również sprzyjać integracji partyjnej oraz wyciszeniu frakcji sceptycznych wobec lidera. W przypadku zmiany władzy członkowie gabinetu cieni najczęściej obejmują resorty, których pracę śledzili, jednak należy zaznaczyć, że nowy premier może dowolnie kształtować swój gabinet. Wskazuje się, że znaczących przetasowań na tym polu dokonała Margaret Thatcher, przejmując władzę w 1979 r. (zmiany dotyczyły ministerstwa spraw zagranicznych, obrony oraz rolnictwa).

Gabinet cieni ma przede wszystkim zmuszać ministrów do składania wyjaśnień oraz wzięcia bezpośredniej odpowiedzialności za swoje działania. W związku koniecznością realizacji tego zadania opozycja ma zagwarantowane pewne prawa. Przede wszystkim w każdej sesji parlamentarnej są dni, w trakcie których opozycja wyznacza temat obrad oraz zgłasza wnioski (*opposition days*); 17 z tych dni przypada oficjalnej Opozycji Jego Królewskiej Mości, a 3 – pozostałym partiom. Ponadto podstawowym narzędziem służącym kontroli rządu są pytania parlamentarne. Warto nadmienić, że lider opozycji w trakcie debat zajmuje uprzywilejowaną w stosunku do innych deputowanych pozycję; wynika ona zarówno z uchwalonych regulacji, jak również przyjętej praktyki postępowania. Jest on m.in. głównym oponentem premiera podczas środowych sesji (Prime Minister's Questions), kiedy to może zadać mu 6 pytań, gdy inni posłowie zadają po 1.

Zabiera głos jako pierwszy po przedstawicielu rządu w najważniejszych debatach parlamentarnych, a jego wystąpienie traktuje się jako autorytatywne stanowisko opozycji. Prowadzący obrady speaker priorytetowo udziela mu głosu, akceptuje dłuższe i bardziej konfrontacyjne wystąpienia, a także dopuszcza możliwość poruszenia szerszego zakresu tematów. Ponadto wniosek o wotum nieufności wobec rządu zostaje niezwłocznie poddany debacie w Izbie Gmin, tylko jeśli jego autorem jest lider opozycji. Należy również nadmienić, że pozycja lidera opozycji jest wzmacniania jego przynależnością do grona zaufanych doradców króla, tzw. Tajnej Rady (Privy Council). Jest on również informowany o najważniejszych kwestiach wagi państwowej związanych np. z polityką zagraniczną. Ponadto, jak już wspomniano, to jeden z niewielu przedstawicieli gabinetu cieni otrzymujących wynagrodzenie z budżetu państwa. Oprócz niego w opozycji pobierają je jeszcze tylko lider opozycji w Izbie Lordów, odpowiedzialni za dyscyplinę partyjną główni whipowie w każdej z izb oraz dwóch zastępców whipów w Izbie Gmin.

Pomimo iż brytyjski gabinet cieni nie posiada żadnej realnej władzy, a jego funkcjonowanie opiera się w większym stopniu na konwencji niż regulacjach prawnych, należy zauważyć, że w ostatnich dziesięcioleciach wzrosło polityczne znaczenie tego ciała. Zarówno opinia publiczna, jak i członkowie partii wymagają od ministrów cieni doskonałego rozeznania w sprawach publicznych oraz gotowości do przejęcia władzy. To zadanie jest o tyle trudne, że w przeciwieństwie do swoich rządowych adwersarzy nie posiadają oni środków finansowych służących temu celowi oraz – co może bardziej istotne – wsparcia aparatu urzędniczego. W związku z tym w większym stopniu muszą oni polegać przede wszystkim na własnej inicjatywie i zdolnościach organizacyjnych, a skuteczność ich działań zależy także od umiejętności komunikowania swojej wizji społeczeństwu oraz zdolności szybkiego reagowania na bieżące wydarzenia polityczne. Należy również nadmienić, że nie każdy lider opozycji zostaje ostatecznie premierem, a jego najbliżsi współpracownicy – ministrami korony.

Nie zmienia to jednak faktu, że współcześnie członkowie gabinetu cieni, kwestionując i oceniając politykę rządu w parlamencie, przygotowując własne projekty ustaw i kształtując debatę publiczną, sprawili, że tworzona przez nich instytucja wydaje się trwałym elementem

demokracji parlamentarnej opartej na westminsterskim systemie rządów. Z powodzeniem funkcjonuje więc także poza Wielką Brytanią (tam tworzy go obecnie Partia Konserwatywna pod przewodnictwem Kemi Badenoch), m.in. w Australii (Partia Liberalna pod przewodnictwem Sussan Ley), Kanadzie (Partia Konserwatywna pod przewodnictwem Pierre'a Poilievre'a) oraz Nowej Zelandii (Partia Pracy pod przewodnictwem Chrisa Hipkinsa). W przyszłości gabinety cieni mogą odgrywać jeszcze większą rolę w przygotowywaniu przyszłych liderów politycznych oraz formułowaniu spójnych, alternatywnych propozycji polityki publicznej. Dzięki temu instytucja ta pozostaje istotnym mechanizmem równoważącym władzę wykonawczą i wzmacniającym odpowiedzialność rządów wobec społeczeństwa.

Elżbieta Sadowska-Wieciech

S. Gebethner, *Rząd i opozycja Jej Królewskiej Mości w systemie politycznym Wielkiej Brytanii*, Książka i Wiedza, Warszawa 1967; A. Kaiser, *Parliamentary Opposition in Westminster Democracies: Britain, Canada, Australia and New Zeealand*, „Journal of Legislative Studies" 2008, no. 14; N. Michaud, *Designating the Official Opposition in a Westminster Parliamentary System*, „The Journal of Legislative Studies" 2000, vol. 6, no. 4; R.M. Punnett, *Front-Bench Opposition: The Role of the Leader of the Opposition, the Shadow Cabinet and Shadow Government in British Politics*, Heinemann, London 1973; T. Wieciech, *System konstytucyjny Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej*, Wydawnictwo Sejmowe, Warszawa 2019.

GENERATIVE OVERPRODUCTION I AI SLOP (ang. *Generative overproduction)* to zjawisko systemowej, masowej nadprodukcji treści tworzonych automatycznie przez systemy sztucznej inteligencji. Dotyczy przede wszystkim generatywnych modeli językowych oraz narzędzi do syntezy obrazu, dźwięku i wideo. W efekcie powstają ogromne wolumeny materiałów informacyjnych o ograniczonej wartości poznawczej, często niskiej oryginalności i wysokim stopniu redundancji. Jednym z najbardziej widocznych i zarazem problematycznych efektów tego procesu jest zjawisko określane terminem „*AI slop*", rozumiane jako masowo wytwarzane, generyczne treści o niskiej jakości. Choć bywają poprawne formalnie (językowo lub wizualnie), cechuje je płytkość i niewielka

wartość poznawcza, co w dłuższej perspektywie prowadzi do degradacji jakości ekosystemu informacyjnego. Strukturalnie *slop* można rozpoznać po trzech typach braków:

1. Użyteczność – treść ma niską gęstość informacyjną i często rozmija się z pytaniem lub sytuacją, którą ma opisywać.
2. Rzetelność – pojawiają się halucynacje, nieścisłości i sugestie wprowadzające odbiorcę w błąd, a w formach wymagających stanowiska (np. recenzjach) brakuje autentycznej perspektywy.
3. Styl – tekst jest szablonowy i rozwlekły: powiela przewidywalne konstrukcje i „pompuje" objętość zamiast znaczenia.

Charakter slopu zmienia się wraz z domeną; w tekstach informacyjnych najczęściej ujawnia się jako rozwlekłość i nietrafiony ton, natomiast w zadaniach QA – jako błędy faktograficzne oraz niespójność struktury odpowiedzi. Taka zmienność utrudnia odbiorcom ocenę, co jest wiarygodne i naprawdę użyteczne, a w konsekwencji staje się wyzwaniem dla bezpieczeństwa informacyjnego i poznawczego. Dodatkowo badania pokazują, że nawet zaawansowane modele językowe słabo „rozpoznają" własny *slop*, co wzmacnia mechanizm jego powielania w obiegu cyfrowym.

Geneza zjawiska *generative overproduction* jest ściśle związana z gwałtownym rozwojem oraz rosnącą dostępnością generatywnej sztucznej inteligencji. Po 2020 r. – zwłaszcza wraz z komercjalizacją dużych modeli językowych oferowanych jako usługi chmurowe – nastąpiło wyraźne obniżenie barier technologicznych, kompetencyjnych i kosztowych w zakresie wytwarzania treści cyfrowych. Automatyzacja generowania tekstów, obrazów i materiałów audiowizualnych, sprzężona z ich niemal natychmiastową dystrybucją za pośrednictwem platform cyfrowych, mediów społecznościowych oraz systemów zarządzania treścią, umożliwiła produkcję informacji w skali znacząco przekraczającej zdolności percepcyjne, selekcyjne i weryfikacyjne odbiorców. W konsekwencji powstały strukturalne warunki sprzyjające narastaniu przeciążenia informacyjnego.

W tym kontekście *AI slop* pojawił się początkowo w dyskursie publicystycznym i branżowym jako potoczne określenie treści generowanych przez systemy AI, które – mimo formalnej poprawności językowej lub wizualnej – prowadzą do funkcjonalnego „zaśmiecania" przestrzeni cyfrowej. Z czasem pojęcie to zostało zaadaptowane przez refleksję akademicką

jako kategoria analityczna opisująca nową fazę degradacji ekosystemu informacyjnego, w której zasadniczym problemem przestaje być wyłącznie fałszywość przekazów, a staje się nim masowa produkcja treści poznawczo jałowych. Dalsza ewolucja zjawiska koreluje z postępującą integracją dużych modeli językowych z praktykami zawodowymi i procesami pracy intelektualnej. Według danych z połowy dekady znaczna część interakcji z systemami konwersacyjnymi dotyczy redagowania tekstów oraz pozyskiwania informacji, co może sprzyjać powstawaniu zjawiska określanego jako *AI work slop*.

Zjawisko *AI slop* wpisuje się w szerszą zmianę paradygmatu oceny treści: ciężar analizy przesuwa się z prostej opozycji „człowiek–maszyna" na jakościową ocenę wartości poznawczej, intencjonalności oraz – przede wszystkim – odpowiedzialności za wytwarzany przekaz. W praktyce *AI slop* szczególnie silnie ujawnia się w ekosystemach nastawionych na optymalizację pod kątem wyszukiwarek internetowych, gdzie nadrzędnym kryterium staje się wolumen produkcji, a nie gęstość informacyjna. Sprzyja to powstawaniu rozległego „szumu informacyjnego" pozbawionego autentycznej perspektywy i merytorycznej głębi.

Generative overproduction stanowi bezpośrednią konsekwencję sposobu działania współczesnych modeli generatywnych. Ucząc się na ogromnych zbiorach danych, modele te są optymalizowane przede wszystkim pod kątem statystycznej zgodności z wzorcami treningowymi, a nie pod kątem epistemicznej wartości wytwarzanych treści. Wykazują one silną tendencję do operowania tzw. szablonami syntaktycznymi (*syntactic templates*), czyli wielokrotnego powielania faworyzowanych struktur składniowych, co prowadzi do wspomnianego wcześniej zjawiska szablonowości (*templatedness*). Działanie oparte na mechanizmach probabilistycznych sprzyja reprodukowaniu dominujących schematów, co w praktyce objawia się drastycznym obniżeniem gęstości informacyjnej (*information density*). Treści te bywają nasycone słowami-wypełniaczami (*filler words*), które mimo formalnej poprawności przekazują znikomą ilość substancjalnej wiedzy.

Dodatkowym czynnikiem intensyfikującym to zjawisko jest integracja systemów generatywnych z algorytmami SEO. Prowadzi ona do masowej produkcji materiałów określanych w literaturze jako *information fodder*,

projektowanych przede wszystkim w celu maksymalizacji widoczności w wyszukiwarkach, a nie zwiększania wartości poznawczej. Skala tej nadprodukcji jest determinowana przez realne wzorce użytkowania technologii: badania wskazują, że blisko 50% aktywności użytkowników systemów takich jak ChatGPT koncentruje się na zadaniach związanych z pisaniem (28,1%) oraz gromadzeniem informacji (21,3%). W rezultacie powstaje znaczny popyt na zautomatyzowaną generację tekstów, który dodatkowo napędza mechanizmy masowej produkcji treści.

W nowszych ujęciach pojęcie *AI slop* bywa ujmowane nie tyle przez pryzmat „materialnej" jakości treści, ile poprzez stopień ludzkiej troski (*care*) włożonej w proces ich wytwarzania, redakcji i publikacji. Oznacza to istotne przesunięcie akcentu: z oceny samego rezultatu na analizę warunków produkcji materiału. W tym kontekście troskę rozumie się dwojako: po pierwsze, jako świadomą uważność i wysiłek obejmujące projektowanie zapytań, edycję, weryfikację faktów oraz dostosowanie formy do kontekstu użycia; po drugie – osobistą lub ekspercką odpowiedzialność twórcy za publikowany materiał, implikującą poczucie sprawczości, własności i odpowiedzialności za jego potencjalne skutki.

Z tej perspektywy *slop* pojawia się tam, gdzie generatywna sztuczna inteligencja wytwarza materiały bez rozpoznawalnych śladów ludzkiego nadzoru – w warunkach, w których poprawność, spójność czy użyteczność są jedynie ubocznym efektem statystycznej optymalizacji modelu, a nie rezultatem intencjonalnego działania ukierunkowanego na konkretną potrzebę informacyjną. Brak troski czyni materiał epistemicznie „przypadkowym", niezależnie od tego, czy w danym przypadku okaże się trafny: nie istnieje bowiem podmiot, któremu można przypisać intencję przekazania prawdziwej informacji ani odpowiedzialność za jej konsekwencje. Tak rozumiany *AI slop* bywa interpretowany w kategoriach *careless speech* – formy komunikacji, która, choć może przyjmować postać poprawną i przekonującą, nie jest zakorzeniona w zobowiązaniu wobec prawdy, rzetelności ani dobra odbiorcy. Jej masowe rozpowszechnienie prowadzi w efekcie do kumulatywnej degradacji ekosystemu informacyjnego poprzez normalizację przekazów pozbawionych odpowiedzialnego zaplecza epistemicznego.

Przejawy te można sklasyfikować w trzech wymiarach deficytów jakościowych. Pierwszy z nich stanowi wymiar użyteczności (*information utility*): treści charakteryzują się drastycznie niską gęstością informacyjną (*information density*) – operują dużą liczbą słów-wypełniaczy, które przekazują znikomą liczbę konkretnych idei. Częstym problemem jest również brak relewancji: model generuje tekst poprawny gramatycznie, lecz niedostosowany do specyfiki zapytania lub kontekstu. Drugi wymiar to jakość informacji (*information quality*) ujawniająca się w postaci „subtelnych nieścisłości", halucynacji oraz braku autentycznej, zaangażowanej perspektywy. Trzeci wymiar obejmuje jakość stylu (*style quality*); najbardziej mierzalnymi przejawami AI slopu są tu szablonowość składniowa (*syntactic templatedness*) oraz nadmierna gadatliwość (*verbosity*). Modele wykazują tendencję do faworyzowania powtarzalnych struktur (np. list) i przewidywalnych fraz przejściowych, co czyni tekst monotonnym i redundantnym. W rezultacie, zamiast wnosić nowe informacje, *slop* przetwarza i powiela dominujące narracje, prowadząc do erozji różnorodności semantycznej i leksykalnej.

W kategoriach nauk o bezpieczeństwie *generative overproduction* oraz *AI slop* należy traktować jako istotne zagrożenie dla bezpieczeństwa informacyjnego, rozumianego jako zdolność systemów społecznych do zapewnienia dostępu do informacji rzetelnych, użytecznych i możliwych do zweryfikowania. Nadmiar treści niskiej jakości utrudnia procesy decyzyjne, zwiększa podatność na manipulację informacyjną oraz osłabia zdolność obywateli do krytycznej analizy przekazów medialnych. W szerszym ujęciu zjawisko to oddziałuje także na bezpieczeństwo poznawcze, prowadząc do przeciążenia informacyjnego, erozji zaufania do źródeł wiedzy oraz stopniowego zaniku autorytetu eksperckiego w przestrzeni publicznej.

Konsekwencje AI slopu uruchamiają również pytania o odpowiedzialność za treści publikowane z użyciem systemów generatywnych, przejrzystość ich pochodzenia oraz ochronę użytkowników przed dezinformacją strukturalną – niepolegającą na bezpośrednim fałszowaniu faktów, lecz zalewaniu przestrzeni informacyjnej treściami poznawczo nieistotnymi. Brak jednoznacznych regulacji prawnych i standardów jakości sprzyja eskalacji tego zjawiska, czyniąc je wyzwaniem nie tylko technologicznym, ale także

normatywnym i instytucjonalnym. Ograniczanie skutków *generative overproduction* wymaga strategii wielopoziomowych: z jednej strony, rozwoju narzędzi detekcji i oznaczania treści syntetycznych, z drugiej – budowania kompetencji krytycznego odbioru informacji wśród użytkowników oraz instytucji. W dłuższej perspektywie kluczowe będzie wypracowanie norm etycznych i regulacyjnych, które umożliwią odpowiedzialne wykorzystanie generatywnej sztucznej inteligencji przy jednoczesnym zachowaniu jakości i integralności ekosystemu informacyjnego.

Miłosz Horodyski, Edyta Sadowska

S. Diepeveen, M. Pinet, *User perspectives on digital literacy as a response to misinformation*, „Development Policy Review" 2022, no. 40(S2), https://doi.org/10.1111/dpr.12671 (dostęp 30.01.2026); I. Kalpokas, V. Šalaševičiūtė, M. Lipskė, *Technology as a Threat or a Solution*? *The Challenges of Responding to Synthetic Media*, „Baltic Journal of Law & Politics" 2024, no. 16(2), https://doi.org/10.2478/bjlp-2023-0010 (dostęp 30.01.2026); M. Klincewicz, M. Alfano, A. Ebrahimi Fard, *Slopaganda: The interaction between propaganda and generative AI*, 2025, https://doi.org/10.48550/arXiv.2503.01560 (dostęp 30.01.2026); G. Puccetti, A. Rogers, C. Alzetta, F. Dell'Orletta, A. Esuli, *AI "News" Content Farms Are Easy to Make and Hard to Detect: A Case Study in Italian*, https://doi.org/10.48550/arXiv.2406.12128 (dostęp 30.01.2026); X. Xing, F. Shi, J. Huang, Y. Wu, Y. Nan, S. Zhang, Y. Fang, M. Roberts, C.B. Schönlieb, J. Del Ser, G. Yang, *When AI Eats Itself: On the Caveats of AI Autophagy*, https://doi.org/10.48550/arXiv.2405.09597 (dostęp 30.01.2026)**H**

H

HIMARS M142 – System Artyleryjsko-Rakietowy Wysokiej Mobilności (ang. The High Mobility Artillery Rocket System) wyprodukowany w Stanach Zjednoczonych na początku lat 90. XX w. i użytkowany do dzisiaj przez wojska lądowe i piechotę morską, mający postać lekkiej mobilnej wyrzutni rakietowej zamontowanej na standardowej ciężarówce M1140 należącej do rodzinny pojazdów FMTV.

Geneza HIMARS M142 sięga lat 80. XX w., kiedy amerykańskie wojska lądowe dostrzegły potrzebę zwiększenia liczby lekkich dywizji, jak również konieczność rozszerzenia ich zadań. W 1982 r. 9 Dywizja Piechoty w ramach opracowanego przez sztabowców Planu Szybkiego Reagowania (Quick Reaction Plan) złożyła wniosek do Pentagonu o lekki, łatwy w transporcie system wsparcia ogniowego. W kolejnych latach wraz ze zmniejszaniem się zagrożenia dotyczącego wybuchu wojny między NATO a Układem Warszawskim zainteresowanie mobilnym, wieloprowadnicowym system rakietowym rosło. Będący wówczas na etapie wdrażania system rakietowy M-270 (MLRS) z różnych powodów nie spełniał oczekiwań wojskowych. W kwietniu 1990 r. Szkoła Artylerii Polowej w Fort Sill, w Oklahomie (Field Artillery School) złożyła kolejny wniosek na

lekki system rakietowy, przedstawiając wstępną dokumentację; opisano go jako System Artyleryjsko-Rakietowy Wysokiej Mobilności (High Mobility Artillery Rocket System). W połowie września 1990 r. z kolei Dowództwo ds. Szkolenia i Doktryn Armii Stanów Zjednoczonych (TRADOC) wystosowało list do przedstawicieli kompleksu wojskowo-przemysłowego, w którym podkreśliło, że rozwój HIMARS jest w pełni wspierany przez instytucję i jest to kierunek słuszny, co pokazał kryzys w Zatoce Perskiej. Konstrukcją systemu bojowego zajęła się firma Loral Vought System, Lockheed Martin Missiles oraz Fire Control w ramach programu demonstracji technologii zaawansowanej koncepcji (Advanced Concept Technology Demonstration, ACTD). HIMARS miał być lżejszy od MLRS, przydzielony do brygad artylerii polowej lub korpusów celem wsparcia lekkich dywizji wojsk lądowych i sił sojuszniczych oraz w razie konieczności – być transportowany przez samolot Lockheed C-130 Herkules. Po raz pierwszy zaprezentowany został w 1993 r. w Waszyngtonie, a rok później, we wrześniu – w Europie. W 1998 r. XVIII Korpus Powietrznodesantowy z Fort Bragg, w Karolinie Północnej otrzymał kilka prototypowych sztuk celem testowania i dostarczania informacji zwrotnych dla konstruktorów. Zamówienia dla wojsk lądowych rozpoczęły się w 2006 r. i obejmowały 160 systemów.

HIMARS zbudowany został na podwoziu nowych pięciotonowych średnich pojazdów taktycznych 6×6 dla amerykańskich wojsk lądowych (Family Medium Tactical Vehicles, FMTV). Ma możliwość wystrzeliwania wszystkich rodzajów pocisków MLRS: rakiety podstawowej M-26, rakiety ćwiczebnej M-28, rakiety o zwiększonym zasięgu M-26A1, rakiety MLRS o zwiększonym zasięgu (GMLRS), pocisków ATACAMS oraz precyzyjnych pocisków uderzeniowych nowej generacji PrSM. Rakieta GMLRS oprócz GPS wyposażona została w bezwładnościowy pakiet naprowadzania oraz małe osłony dziobowe zwiększające celność. Testy GMLRS zakończyły się w grudniu 2022 r., wszedł do seryjnej produkcji w kwietniu 2003 r., a wdrożony operacyjnie został we wrześniu 2005 r. w Iraku. ATACMS obejmuje z kolei pociski Block I, Block IA oraz Block IA Unitary. Pocisk Block I przenosi 950 pocisków M74 wielkości piłki baseballowej przeznaczonych do zwalczania piechoty i ma zasięg przekraczający 165 km. Zasięg pocisku Block IA przekracza 300 km dzięki zmniejszeniu ładunku

do 300 pocisków i dodaniu systemu naprowadzania GPS. Został on po raz pierwszy użyty w marcu 2003 r. w Iraku. Program rozwoju pocisku Block II z GPS i 13 pociskami BAT (Brilliant Anti-Tank) oraz pocisku Block IIA z 6 ulepszonymi pociskami BAT anulowany został w lutym 2003 r.

Waga HIMARS wynosi 13–16 t i zależy od tego, czy system jest uzbrojony: jest znacznie niższa niż MLRS, przez co może być przenoszony na zamorskie obszary działań, które wcześniej były niedostępne dla dużych samolotów takich C-5 transportujących M-270. Na zaplecze logistyczne składa się pojazd HEMTT (Heavy Expanded Mobility Tactical Truck), który przewozi 4 w pełni załadowane zasobniki rakietowe oraz 4 dodatkowe. HIMARS posiada te same procedury operacyjne co MLRS, w tym kierowania ogniem, elektroniki i łączności. Załoga składa się z 3 osób, ale może ograniczyć się nawet do 1. Robert H. Neighbors – kierownik ds. demonstracji technologii MLRS/HIMARS w Redstone Arsenal, w Alabamie (baza, w której mieści się wiele agencji i jednostek organizacyjnych Pentagonu, takich jak U.S. Army Aviation and Missile Command, U.S. Army Material Command, Redstone Test Center, Redstone Arsenal Fild Office) – wymieniając priorytety systemu HIMARS, wskazał na przeżywalność, bezpieczeństwo minimalizujące zagrożenia dla załogi, zdolność do transportu, maksymalizację początkowych możliwości, możliwość użycia całej rodziny pocisków MLRS oraz adaptację do zmieniających się doktryn i taktyki. Ponadto w wymaganiach stawianych przez HIMARS podkreślano, że system powinien być sprawny w różnych warunkach pola walki, w tym w przypadku przeszkód elektromagnetycznych, deszczu, mgły, śniegu, marznących opadów deszczu, burz, słonej wody, piasku i pyłu. Załodze powinno zapewnić się ochronę przez gazami spalinowymi, zanieczyszczeniami wydmuchiwanymi ze spalin, hałasem, ciepłem, nadciśnieniem i zanieczyszczeniami chemicznymi. Kabina powinna dać schronienie przed pociskami z broni ręcznej, odłamkami z pękniętego silnika oraz odłamkami z min. Oprócz podstawowego systemu MLRS, HIMARS zbiera także dane meteorologiczne, posiada zmodyfikowane oprogramowanie interfejsu wyrzutni, panelu sterowania ogniem i inne. Od połowy 2008 r. firma Lockheed Martin montuje we wszystkich egzemplarzach uniwersalny komputerowy system kierowania ogniem obsługiwany przez GPS, który umożliwia obsługę przez dwuosobową załogę lub 1

żołnierza. W skład systemu wchodzą obraz wideo, sterowanie klawiaturą, gigabajt pamięci oraz GPS. Ogień może być prowadzony w trybie automatycznym lub ręcznym. W typowej misji stanowisko dowodzenia i kontroli przesyła dane o wybranym celu za pomocą bezpiecznego łącza danych do pokładowego komputera startowego, który następnie ustawia wyrzutnię i natychmiast wysyła załodze sygnał do odpalenia wybranej liczby pocisków. Wyrzutnia może namierzyć cel w zaledwie 16 sekund.

Konserwacja elementów jest uproszczona ze względu na powszechność istniejących systemów. Nie posiada on części zamiennych, które są specyficzne tylko dla HIMASR. Średni zalecany czas naprawy nie jest dłuższy niż godzina w przypadku jednostki ogniowej i 4 godziny dla jednostek wsparcia, maksymalny czas naprawy nie powinien natomiast przekraczać 3 godzin dla jednostki ogniowej i 12 – dla jednostek wsparcia. W czasie konfliktu zbrojnego HIMARS z reguły nie jest rozmieszczany w „strefie bliskiej" (*close area*), lecz oddalony i ukryty od miejsca, gdzie toczą się bezpośrednie walki. Jego użycie polega na szybkim przemieszczaniu się na miejsce, z którego przeprowadzony zostanie ostrzał. Mobilność na drogach i innych szlakach jest zatem kolejną przewagą nad gąsienicowymi pojazdami MLRS. Ciężkie pojazdy gąsienicowe, takie jak M-110 lub M-270, nie mogą ponadto poruszać się po drogach publicznych w Stanach Zjednoczonych, dlatego są one przechowywane w centrach magazynowych lub ośrodkach szkoleniowych i udostępniane do kilku razy w roku.

O konieczność posiadania takiego systemu bojowego przekonały się Stany Zjednoczone w czasie operacji Pustynna Burza w 1990 r., kiedy do Arabii Saudyjskiej przybyła 82 Dywizja Powietrznodesantowa. Okazało się, że gdyby doszło do ataku irackich dywizji pancernych, amerykańskie wojska powietrznodesantowe nie posiadały wystarczającej ilości systemów bojowych, za pomocą których mogłyby odeprzeć natarcie; do dyspozycji mieli jedynie przeciwpancerne pociski kierowane BGM-71 TOW, a śmigłowce szturmowe M-270 były wciąż w zbyt dużej odległości, aby skutecznie wspierać dywizję. HIMARS mógłby znaleźć się w miejscu prowadzonej operacji w tym samym czasie co żołnierze wojsk lądowych oraz niezwłocznie być gotowy do użycia.

Pierwsze zamówienia HIMARS dla amerykańskiego wojska rozpoczęły się w 2000 r., kiedy Lockheed Martin otrzymała kontrakt na dostawę 6

wyrzutni, zaś kolejne 2 – w ramach dwuletniego programu oceny użytkownika dla Korpusu Piechoty Morskiej USA. W latach 2003–2005 podpisano kolejne trzy kontrakty na 141 wyrzutni dla wojsk lądowych oraz 6 – dla Korpusu Piechoty Morskiej USA. Pentagon planował zakupić wówczas łącznie 900 wyrzutni. Pierwszymi jednostkami, które je otrzymały, były 27 Pułk Artylerii Polowej XVIII Korpusu Powietrznodesantowego, 1 Batalion 181 Pułku Artylerii Polowej Gwardii Narodowej Tennessee, 158 Pułk Artylerii Polowej Gwardii Narodowej Oklahomy, 5 Batalion 3 Pułku Artylerii Polowej w Fort Lewis czy 14 Pułk Piechoty Morskiej.

Lista krajów – użytkowników HIMARS – cały czas rośnie. Do października 2025 r. były to Zjednoczone Emiraty Arabskie, Jordania, Singapur, Rumunia, Polska, Ukraina, Australia, Estonia i Taiwan. Jako pierwsze zamówienie na wyrzutnie złożyły w 2006 r. Zjednoczone Emiraty Arabskie: łącznie pozyskały ich 20 z pociskami ATACAMS, MLRS i GMLRS, a dostawa miała miejsce pod koniec 2009 r. W przypadku Polski umowa międzyrządowa na pozyskanie pierwszego dywizjonowego modułu ogniowego składającego się z 18 wyrzutni bojowych i 2 szkoleniowych podpisana została w 2019 r., zaś w 2023 zawarto umowę ramową na dostarczenie 80 baterii (486 wyrzutni) w ramach programu Homar.

Tomasz Wójtowicz

HIMARS – High-Mobility Artillery Rocket System, https://www.army-technology.com/projects/himars/?cf-view&cf-closed (dostęp 16.10.2025); T.M. Kogler, *Single Gun, Multiple Round, Time-on-target Capability for Advanced Towed Cannon Artillery*, https://apps.dtic.mil/sti/tr/pdf/ADA293479.pdf (dostęp 14.10.2025); *Realizacja programu HOMAR*, https://www.wojsko-polskie.pl/au/articles/aktualnosci/realizacja-programu-homar/ (dostęp 16.10.2025); *Redstone Arsenal/Team Redstone*, https://home.army.mil/redstone/ (dostęp 14.10.2025); T. Shirley, *A high-mobility artillery rocket system: projections for the fire support community*, https://apps.dtic.mil/sti/tr/pdf/ADA312477.pdf (dostęp 14.10.2025); A. Świerkowski, *Program Homar-A. Co może zyskać polski przemysł?*, https://defence24.pl/przemysl/program-homar-a-co-moze-zyskac-polski-przemysl#goog_rewarded (dostęp 16.10.2025).

HINDUSKI NACJONALIZM (HINDUTWA), czyli ruch ideowo-polityczny, którego zasadniczym celem jest zakreślenie indyjskiej państwowości

poprzez dominację kultury hinduistycznej oraz rekonstrukcję narodu jako wspólnoty zakorzenionej w tradycji wedyjskiej. Geneza tego nurtu jest silnie związana z XIX-wiecznym doświadczeniem kolonialnym, gdy brytyjska administracja, wprowadzając nowoczesne narzędzia kontroli, takie jak spisy ludności, jednolite kategorie religijne, klasyfikacje kastowe i system edukacji, przyczyniły się do konsolidacji hinduizmu jako jednej religii. Wcześniej był on zbiorem zróżnicowanych praktyk, rytuałów i lokalnych tradycji, a dopiero kolonialna typologia nadała mu formę odpowiadającą europejskiemu pojęciu religii. Proces ten doprowadził do powstania poczucia wspólnoty symbolicznej i kulturowej, które później stało się podstawą ruchu nacjonalistycznego.

Istotny wpływ na rozwój hinduskiego nacjonalizmu miały również ruchy reformistyczne, takie jak Brahmo Samaj, Arya Samaj czy Ramakrishna Mission. Z jednej strony, broniły one starożytnego dziedzictwa, z drugiej – reinterpretowały je w duchu racjonalizmu i modernizacji. Reformatorzy przedstawiali hinduizm jako religię etyczną, filozoficzną, uporządkowaną i przewyższającą inne tradycje moralną głębią, co sprzyjało tworzeniu narracji o cywilizacyjnej „misji" Indii. Równocześnie narastało poczucie zagrożenia ze strony islamu i chrześcijaństwa, które w dyskursie nacjonalistycznym zaczęto ukazywać jako tradycje obce, niezakorzenione w indyjskim krajobrazie kulturowym.

Fundamentem współczesnego hinduskiego nacjonalizmu jest myśl Vinayaka Damodara Savarkara, autora koncepcji tak zwanej *hinduskości* (hindutwy), który twierdził, że naród hinduski stanowią ci, którzy uznają Indie zarówno za ojczyznę (*pitribhumi*), jak i ziemię świętą (*punyabhumi*). Oznaczało to jednocześnie wykluczenie społeczności, których święte miejsca położone są poza Indiami, czyli w dużej mierze byli i są to chrześcijanie oraz muzułmanie. W ujęciu Savarkara naród, religia i kultura stanowiły nierozerwalną całość. Hindutwa reinterpretowała hinduizm nie jako zbiór wierzeń, lecz cywilizację obejmującą języki, rytuały, mity, obyczaje i tradycje społeczne, wspólne dla zdecydowanej większości mieszkańców subkontynentu. Ta definicja narodu miała charakter wyraźnie ekskluzywny i budowała podstawę dla późniejszej polityki większościowej. Oprócz Savarkara ważną rolę w konsolidacji ideologii odegrał Madhav Sadashiv Golwalkar, jeden z głównych przywódców Rashtriya Swayamsevak Sangh

(RSS), prezentujący wizję społeczeństwa jednolitego kulturowo, w którym mniejszości mogą funkcjonować wyłącznie pod warunkiem pełnej lojalności wobec hinduizmu i rezygnacji z roszczeń politycznych. Golwalkar podkreślał nadrzędność większości i konieczność podporządkowania państwa celom kulturowym, co oznaczało odrzucenie liberalnego sekularyzmu promowanego przez Indyjski Kongres Narodowy.

Rozkwit współczesnego nacjonalizmu hinduskiego nie był wyłącznie rezultatem działań ideologów; na jego rozwój wpłynęły również czynniki historyczne i geopolityczne, a zwłaszcza rosnące napięcia między hinduistami a muzułmanami przypadające na końcowy etap brytyjskiego kolonializmu, a także wzrost znaczenia All-India Muslim League i debata wokół podziału Indii. Jednym z elementów tworzących podziały społeczne było silne poczucie zagrożenia, ponieważ wśród części hinduistów dominowała narracja o „wieku muzułmańskiego panowania", a później o „politycznych przywilejach" mniejszości gwarantowanych, według nich, przez świecki charakter państwa po 1947 r. Ten emocjonalny komponent stał się jednym z głównych motorów ekspansji ruchu.

Trzonem organizacyjnym hinduskiego nacjonalizmu stała się wspomniana wcześniej RSS, czyli paramilitarna organizacja założona w 1925 r. RSS budowała swoje struktury poprzez lokalne jednostki, w których prowadzono ćwiczenia fizyczne, szkolenia ideologiczne, wykłady historyczne oraz rytuały wspólnotowe. Ich celem było tworzenie zdyscyplinowanych aktywistów oddanych „sprawie narodu", traktujących hinduizm jako fundament obywatelstwa. Można zatem stwierdzić, że długofalowy cel RSS to projekt wychowawczy, którego siła wynika z szerokiej obecności w terenie, głębokiej internalizacji przekazu ideowego oraz ciągłości pokoleniowej. Wokół RSS rozwinęła się rozbudowana organizacja Sangh Parivar, która obejmuje m.in. Vishva Hindu Parishad (VHP), Bajrang Dal, organizacje studenckie (ABVP), robotnicze (BMS), kobiece (Rashtra Sevika Samiti), think tanki, centra kultury i setki instytucji edukacyjnych. Sangh Parivar tworzy równoległy system społeczny, który w wielu regionach konkuruje z instytucjami państwowymi w zakresie edukacji, pomocy społecznej, działalności kulturalnej i mobilizacji politycznej. W praktyce oznacza to, że ideologia hindutwy przenika do codziennego życia, kształtując postawy, język i wyobrażenia o historii, wspólnocie i zagrożeniach.

Politycznym ramieniem ruchu stała się partia Bharatiya Jana Sangh (1951), a następnie Bharatiya Janata Party (BJP), założona w 1980 r. Ich linia ideowa łączyła elementy konserwatyzmu kulturowego z koncepcją modernizacji państwa, jednak dopiero lata 80. i 90. przyniosły masową mobilizację wokół symboli religijnych. Kulminacją tego procesu była kampania Ram Janmabhoomi dotycząca meczetu Babri Masjid w Ajodhji, który w grudniu 1992 r. został zburzony przez radykalnych aktywistów związanych z Sangh Parivar. Wydarzenie to wywołało falę przemocy międzyreligijnej i doprowadziło do trwałej polaryzacji społecznej, a zarazem umocniło hinduski nacjonalizm jako kluczową ideologię polityczną Indii.

W 2002 r. w stanie Gudżarat, którego premierem był Narendra Modi (BJP), doszło do jednych z najkrwawszych zamieszek międzyreligijnych od czasu podziału kraju. Wydarzenia te, niezależnie od ocen historycznych, wzmocniły pozycję ruchu hindutwy i ukształtowały Modiego jako lidera, który w kolejnych latach przedstawił się jako obrońca hinduistycznej większości. Od tego momentu zaczął kształtować się model władzy, w którym nacjonalizm kulturowy stanowi fundament mobilizacji politycznej i podstawę przebudowy instytucji państwowych.

Rozwój hinduskiego nacjonalizmu w XX i XXI w. był możliwy dzięki relatywnie rozbudowanej strukturze organizacyjnej, której centrum stanowiło wspomniane wcześniej Rashtriya Swayamsevak Sangh – paramilitarna i ideologiczna organizacja kadrowa założona w 1925 r. przez K.B. Keshav Baliram Hedgewara, której zadaniem jest wychowanie nowego typu obywatela – zdyscyplinowanego, ujednoliconego kulturowo i wiernego ideologii hindutwy. RSS tworzy sieć tysięcy lokalnych komórek (*shakha*), gdzie codziennie odbywają się ćwiczenia fizyczne, zajęcia dyscyplinujące, wykłady historyczne, nauka symboli narodowych i rytualne formy budowania wspólnoty. Model działania RSS zakłada, że przemiana kulturowa musi być długotrwała i realizowana poprzez wychowanie – nie tylko dzieci i młodzieży, ale całych pokoleń.

Mechanizmy działania ruchu hindutwy były oparte na stopniowym rozszerzaniu wpływów w trzech kluczowych obszarach: **edukacji, przestrzeni publicznej oraz pamięci zbiorowej**. W szkołach i uniwersytetach promowano wizję historii akcentującą wielkość starożytnych Indii, rzekome „krzywdy historyczne" zadane przez muzułmanów oraz

długowieczność cywilizacji wedyjskiej. Narracja ta popularyzuje przekonanie, że hinduizm nie jest jedynie religią, lecz cywilizacją i podstawą politycznej jedności Indii. Drugim filarem działania jest symboliczna przebudowa przestrzeni publicznej; zmiany nazw miast (np. Allahabad na Prayagraj), budowa monumentalnych świątyń i posągów, organizacja masowych festiwali religijnych oraz rytualizacja wydarzeń państwowych wpisują się w strategię wytwarzania hinduistycznej dominacji symbolicznej. Proces ten sprawia, że na poziomie codziennego doświadczenia obywatela rośnie obecność hinduistycznych symboli w życiu publicznym, a państwo stopniowo odchodzi od neutralności religijnej. Trzecim obszarem jest mobilizacja społeczna wokół konfliktów międzyreligijnych: Sangh Parivar wykorzystuje napięcia lokalne jako narzędzie konsolidacji większości. Raporty organizacji praw człowieka wskazują, że struktury RSS, VHP i Bajrang Dal często pojawiają się jako inicjatorzy lub koordynatorzy działań prowadzących do eskalacji konfliktów, zwłaszcza w sprawach uboju krów, konwersji religijnych, małżeństw międzywyznaniowych oraz sporów o miejsca kultu. Zjawisko to stało się szczególnie widoczne po latach 90., gdy polityka tożsamościowa zaczęła dominować nad kwestiami ekonomicznymi i społecznymi.

Sangh Parivar wzmacnia swoją pozycję również poprzez działalność charytatywną i pomocową. Organizacje powiązane z RSS prowadzą szpitale, ośrodki medyczne, kuchnie społeczne i dożywianie dzieci, co zapewnia im poparcie wśród najuboższych i marginalizowanych kast. Narracja hindutwy zostaje w ten sposób powiązana z doświadczeniem codziennej pomocy, co tworzy ideologiczno-socjalny system głęboko zakorzeniony w społecznościach lokalnych.

Funkcją polityczną łączącą wszystkie elementy Sangh Parivar jest budowa tak zwanego „*hinduskiego demosu*", czyli masowego elektoratu, który definiuje swoją tożsamość poprzez status większości i poczucie wspólnoty zagrożonej przez „obce wpływy". W praktyce przekłada się to na pełną integrację struktur społecznych, religijnych i politycznych, które wspólnie tworzą jednolity front ideologiczny. Proces ten osiągnął kulminację po 2014 r., kiedy Modi po raz pierwszy zasiadł na stanowisku premiera, dzięki czemu był w stanie umieścić w administracji centralnej

osoby powiązane z RSS, co umożliwiło przeniesienie mechanizmów Sangh Parivar bezpośrednio do aparatu państwowego.

Kulminacyjnym etapem rozwoju hinduskiego nacjonalizmu stał się okres rządów Modiego, który po zwycięstwie Bharatiya Janata Party w 2014 r. przeprowadził gruntowną transformację ideologiczną, instytucjonalną i symboliczną państwa indyjskiego. Proces ten określany jest w literaturze przedmiotu mianem *szafranizacji Indii*. Zjawisko to polega na przenikaniu ideologii hindutwy do sfery państwowej, kulturowej i prawnej, a także zastępowaniu świeckości interpretacją narodu opartą na kulturze hinduistycznej. Rządy Modiego charakteryzują się bezprecedensowym stopniem integracji aparatu państwa z siecią Sangh Parivar, co w praktyce pozwoliło na realizację najważniejszych założeń ideologicznych ruchu.

W wymiarze instytucjonalnym nastąpiła wyraźna zmiana w logice działania państwa. Liczne stanowiska administracyjne, eksperckie i doradcze powierzono osobom powiązanym z RSS lub sympatyzującym z hindutwą. Zmienił się również profil medialny kraju – media publiczne zaczęły promować narrację zgodną z linią rządzącej partii, a dziennikarze krytyczni wobec władz podlegają naciskom ekonomicznym lub politycznym. Niezależne redakcje, think tanki i organizacje pozarządowe mierzą się z restrykcjami finansowymi, np. ograniczeniami dotyczącymi zagranicznego finansowania, co osłabia pluralizm informacyjny i swobodę debaty.

W sferze legislacyjnej najważniejszym wydarzeniem stało się przyjęcie ustawy o obywatelstwie (CAA) w 2019 r., która po raz pierwszy wprowadziła kryterium religijne do prawa naturalizacyjnego, faworyzując migrantów z wybranych państw, ale nie muzułmanów. W połączeniu z planami ogólnokrajowego rejestru obywateli (NRC) może to stworzyć mechanizm prowadzący do marginalizacji wyznawców tej wiary, zwłaszcza z ubogich warstw społecznych. Badacze przedmiotu uznają te rozwiązania za naruszenie sekularyzmu i krok w kierunku redefinicji obywatelstwa w duchu etnoreligijnym. Zniesienie autonomii Dżammu i Kaszmiru w sierpniu 2019 r. oraz militarna kontrola regionu również wpisują się w logikę centralizacji władzy i neutralizacji obszarów o dominacji muzułmańskiej.

W sferze bezpieczeństwa wewnętrznego szafranizacja przełożyła się na wzrost akceptacji wobec przemocy wymierzonej w muzułmanów i inne mniejszości. Wzrosła liczba linczów związanych z ochroną krów,

ataków na społeczności pasterskie i handlarzy bydła, a także przypadków szykanowania międzyreligijnych par w kontekście teorii „love jihad". Lokalne struktury VHP, Bajrang Dal i innych organizacji Sangh Parivar pełnią często rolę katalizatorów konfliktów, a działania policji są w wielu przypadkach spóźnione lub stronnicze, co potęguje poczucie bezkarności. W niektórych stanach wprowadzono przepisy zakazujące uboju krów lub utrudniające konwersje religijne, co w praktyce ogranicza działalność muzułmanów i chrześcijan.

Transformacja dotknęła także system edukacji; podręczniki historii zostały przeformułowane tak, aby umniejszać rolę muzułmańskich dynastii, zwłaszcza Mogołów, przy jednoczesnym akcentowaniu starożytnego dziedzictwa cywilizacji hinduistycznej. Rozszerzono zakres nauczania o tematy związane z kulturą wedyjską, a niektóre treści mitologiczne przedstawiane są jako fakty historyczne. Zmiany objęły również szkolnictwo wyższe, gdzie rośnie liczba instytutów „studiów nad cywilizacją hinduistyczną", finansowanych bezpośrednio przez państwo lub organizacje Sangh Parivar.

Szafranizacja przenika również sferę symboliki publicznej. Zmieniono nazwy wielu miast, ulic i instytucji, by odwoływały się do mitologii hinduistycznej. W Ajodhji rozpoczęto budowę monumentalnej świątyni Ramy, która stała się symbolem zwycięstwa ruchu hindutwy w długoletnim sporze o miejsce kultu, a ceremonie państwowe coraz częściej zawierają elementy hinduistycznych rytuałów, co osłabia konstytucyjną zasadę świeckości państwa.

W wymiarze polityczno-społecznym hinduski nacjonalizm uzyskał status dominującej narracji interpretacyjnej, która tłumaczy zarówno historię, jak i współczesne wyzwania Indii. W jego ramach muzułmanie są często postrzegani nie jako jedna z wielu mniejszości, lecz grupa potencjalnie nielojalna wobec państwa, rzekomo powiązana z „cywilizacyjnym zagrożeniem" ze strony islamu. Retoryka ta pojawia się zarówno w mediach sprzyjających rządowi, jak i w przemówieniach polityków BJP na poziomie centralnym i stanowym. Zjawisko to prowadzi do stopniowego normalizowania społecznej polaryzacji oraz konfliktów międzyreligijnych jako „nieuchronnego" elementu indyjskiej polityki.

W kontekście ustrojowym hinduski nacjonalizm w wersji rządowej jest interpretowany przez badaczy jako forma demokracji nieliberalnej. W systemie tym wybory pozostają mechanizmem legitymizacji, lecz równowaga instytucjonalna ulega erozji, osłabione jest sądownictwo, media doświadczają nacisków politycznych i ekonomicznych, a administracja jest stopniowo podporządkowywana potrzebie ideologicznej. W wyniku tego powstaje struktura przypominająca etnokrację wyborczą, czyli państwo, w którym prawa obywatelskie, dostęp do zasobów i poziom bezpieczeństwa zależą pośrednio od przynależności do większości hinduistycznej.

W polityce zagranicznej hindutwa przekłada się na większą asertywność Indii zarówno wobec Pakistanu i Chin, jak i na arenie globalnej. Rząd Modiego promuje państwo jako „cywilizacyjne mocarstwo", którego siła ma wynikać z duchowej tradycji i zdolności do integracji nowoczesności z kulturą hinduistyczną. Ideologia ta staje się narzędziem legitymizacji geopolitycznych ambicji państwa – od współpracy w ramach Quad po rywalizację z Chinami o dominację w Indo-Pacyfiku.

Podsumowując, współczesny hinduski nacjonalizm jest ruchem o charakterze rewolucyjnym, długofalowym i wielosektorowym. Obejmuje przebudowę instytucji, przekształcenia w sferze prawa i obywatelstwa, redefinicję polityki pamięci i edukacji, kontrolę nad przestrzenią publiczną oraz zmianę ustrojowej logiki funkcjonowania państwa. Jego celem nie jest jedynie umocnienie pozycji religii większości, lecz gruntowna transformacja Indii w państwo oparte na tożsamości hinduistycznej, w którym sekularyzm traci rangę zasady konstytucyjnej, a pluralizm staje się podporządkowany narracji o cywilizacyjnej misji narodu hinduistycznego.

Jarosław Indyk

T. Basu, P. Datta, T. Sarkar, S. Sen, S. Serkal, T. Serkar, *Khaki Shorts and Saffron Flags: A Critique of the Hindu Right*, Orient Blackswan, New Delhi 1996; Ch. Bhatt, *Hindu Nationalism: Origins, Ideologies and Modern Myths*, Routledge, New York 2001; A. Chatterji, P. Angana, T. Hansen, Ch. Jaffrelot, H. Blom, *Majoritarian State: How Hindu Nationalism is Changing India*, Oxford University Press, Oxford 2019; M.S. Golwalkar Guruji, *We or Our Nationhood Defined*, Bharat Publications, Nagpur 1939; R. Guha, *India After Gandhi. The History of the World's Largest Democracy*, Harper Perennial, New York 2008; T.B. Hansen, *The Saffron Wave:*

Democracy and Hindu Nationalism in Modern India, Princeton University Press, Princeton 1999; Ch. Jaffrelot, *Hindu Nationalism: A Reader*, Princeton University Press, Princeton 2007; Ch. Jaffrelot, *The Hindu Nationalist Movement and India*, Columbia University Press, New York 1996; Ch. Jaffrelot, *Modi's India: Hindu nationalism and the rise of ethnic democracy*, Princeton University Press, Princeton 2023; T. Okrasa, *Szafranizacja Indii? Hindutwa w rządach Narendry Modiego w latach 2014–2021*, „Nowa Polityka Wschodnia" 2022, nr 2(33); A. Romejko, *Przemoc na tle religijnym we współczesnych Indiach*, „Cywilizacja i Polityka" 2008, nr 6; V.D. Savarkar, *Hindutva: Who is a Hindu?*, Blurp, New Delhi 2023; S. Tokarski, *Drogi hindutwy. Tradycja hinduskości w konfrontacjach z hinduizmem kolonialnym i postkolonialnym*, „Azja-Pacyfik" 2018, nr XXI.

I

INCYDENT CYBERNETYCZNY (ang. *cyber incident*) – pojęcie odnoszące się do każdego zdarzenia w cyberprzestrzeni, które faktycznie lub potencjalnie zagraża poufności, integralności lub dostępności systemów informatycznych, sieci teleinformatycznych, danych bądź usług cyfrowych. Incydent cybernetyczny może obejmować szerokie spektrum zdarzeń, od przypadkowych błędów konfiguracyjnych i awarii sprzętu, przez nieautoryzowany dostęp do systemów, aż po złożone, skoordynowane ataki o charakterze celowym, często związane z działaniami przestępczymi, szpiegowskimi lub terrorystycznymi. W literaturze przedmiotu pojęcie to jest uznawane za podstawowy element zarządzania bezpieczeństwem informacji oraz cyberbezpieczeństwem, będąc punktem wyjścia dla procedur wykrywania, klasyfikowania, reagowania i raportowania zagrożeń w systemach informatycznych.

Incydenty cybernetyczne należy analizować w kontekście współczesnej cyfryzacji życia społecznego, gospodarczego i instytucjonalnego. W warunkach, w których infrastruktura państwowa, sektor prywatny i jednostki indywidualne coraz bardziej polegają na systemach informatycznych, skutki incydentów mogą obejmować nie tylko straty materialne,

lecz również destabilizację funkcjonowania instytucji, utratę zaufania społecznego, a w przypadku ataków na krytyczne systemy – nawet zagrożenie bezpieczeństwa narodowego. Z tego powodu definicja incydentu cybernetycznego nie ogranicza się wyłącznie do kwestii technicznych, lecz uwzględnia również kontekst organizacyjny, prawny i społeczny, w którym występuje zdarzenie. Podstawową cechą incydentu jest jego charakter niepożądany i zakłócający. Nie każde zdarzenie w systemie informatycznym jest incydentem cybernetycznym; awaria sprzętu lub błąd użytkownika staje się incydentem dopiero wtedy, gdy prowadzi do naruszenia bezpieczeństwa danych lub usług. Klasyfikacja incydentów jest zróżnicowana i może obejmować m.in. naruszenie poufności danych, ingerencję w integralność informacji, ataki typu *denial of service*, złośliwe oprogramowanie, *phishing*, *ransomware*, a także działania wykraczające poza granice techniczne, jak wycieki informacji, ujawnienie danych wrażliwych lub sabotaż cybernetyczny. W literaturze podkreśla się również znaczenie incydentów hybrydowych, które łączą aspekty cybernetyczne z działaniami fizycznymi lub społecznymi, np. manipulacje mediami społecznościowymi połączone z atakami DDoS na instytucje publiczne. Incydenty cybernetyczne charakteryzują się dynamicznym i często nieprzewidywalnym przebiegiem, co sprawia, że ich wykrycie, analiza i reakcja wymagają wyspecjalizowanych procedur. Współczesne podejścia do zarządzania incydentami w sektorze publicznym i prywatnym opierają się na międzynarodowych standardach, takich jak NIST SP 800-61, ISO/IEC 27035 oraz wytycznych ENISA. Procedury te obejmują identyfikację zdarzenia, jego klasyfikację, analizę przyczyn, ocenę skutków, reakcję naprawczą oraz raportowanie w celu poprawy odporności systemu. Szczególną rolę odgrywa koordynacja między różnymi podmiotami, takimi jak zespoły CERT, organy państwowe, operatorzy infrastruktury krytycznej oraz instytucje prywatne. W literaturze podkreśla się, że skuteczne reagowanie wymaga nie tylko aspektu technicznego, lecz również znajomości procedur prawnych, komunikacji kryzysowej oraz zarządzania ryzykiem organizacyjnym.

W badaniach nad incydentami cybernetycznymi zwraca się uwagę również na znaczenie czynników ludzkich i organizacyjnych: najczęściej to właśnie takie błędy, jak nieświadome ujawnienie danych, niewłaściwe

konfiguracje systemów czy brak aktualizacji oprogramowania, stanowią punkt wyjścia dla poważnych naruszeń bezpieczeństwa. W literaturze podkreśla się, że sama technologia, nawet najbardziej zaawansowana, nie jest w stanie zapewnić pełnej odporności systemu bez odpowiednich procedur, szkoleń pracowników oraz kultury bezpieczeństwa w organizacji. Z tego względu analiza incydentów cybernetycznych obejmuje zarówno wymiary techniczne, jak i społeczno-organizacyjne, co czyni temat wysoce interdyscyplinarnym. Istotnym aspektem jest systematyzacja i klasyfikacja incydentów, która pozwala na analizę trendów, identyfikację najczęstszych zagrożeń oraz tworzenie skutecznych strategii prewencyjnych.

W literaturze naukowej podkreśla się, że incydenty mogą być wewnętrzne i zewnętrzne, przypadkowe i celowe, techniczne i hybrydowe, a ich analiza jest niezbędna do kształtowania odporności organizacyjnej i bezpieczeństwa narodowego. W literaturze przedmiotu wskazuje się, że skuteczne zarządzanie incydentem wymaga wielopoziomowego podejścia obejmującego przygotowanie organizacyjne, procedury techniczne oraz mechanizmy koordynacji między podmiotami publicznymi i prywatnymi. W tym kontekście istotną rolę odgrywa przygotowanie planów reagowania na incydenty, które definiują procesy wykrywania, klasyfikowania, eskalowania oraz minimalizacji skutków zdarzenia. Dokumenty takie jak NIST SP 800-61 oraz wytyczne ENISA rekomendują przydzielanie ról i odpowiedzialności w ramach zespołów ds. reagowania na incydenty (CERT), a także tworzenie procedur komunikacji kryzysowej zarówno wewnątrz organizacji, jak i w relacjach z organami państwowymi. W literaturze podkreśla się również znaczenie analizy przyczyn źródłowych incydentów cybernetycznych, co umożliwia ograniczenie ryzyka wystąpienia podobnych zdarzeń w przyszłości. Analiza taka obejmuje badanie wewnętrznych procedur, konfiguracji systemów, polityki bezpieczeństwa oraz czynników ludzkich, które mogły przyczynić się do naruszenia. W tym ujęciu incydent cybernetyczny jest traktowany nie tylko jako zdarzenie techniczne, lecz również sygnał diagnostyczny wskazujący na potencjalne słabości całego systemu informacyjnego. Współczesne podejścia do bezpieczeństwa informacji coraz częściej uwzględniają elementy zarządzania ryzykiem, gdzie każdy incydent jest analizowany pod kątem prawdopodobieństwa

wystąpienia i potencjalnych konsekwencji dla działalności operacyjnej, reputacji oraz zgodności z regulacjami prawnymi.

Równie istotny jest wymiar prawny i regulacyjny incydentów cybernetycznych. W literaturze zwraca się uwagę, że definicja incydentu w kontekście prawnym może różnić się od definicji technicznej, ponieważ obejmuje także obowiązki sprawozdawcze, odpowiedzialność administratorów danych oraz sankcje za naruszenia obowiązków bezpieczeństwa. Przykładem są przepisy RODO w Unii Europejskiej, które nakładają obowiązek zgłaszania incydentów związanych z naruszeniem ochrony danych osobowych w określonym czasie, oraz ustawy o krajowym systemie cyberbezpieczeństwa definiujące obowiązki operatorów usług kluczowych. W literaturze podkreśla się, że zgodność z tymi regulacjami nie jest wyłącznie kwestią formalną, lecz kluczowym elementem strategii bezpieczeństwa organizacji, ponieważ pozwala na ograniczenie skutków prawnych i finansowych incydentu.

Ważnym obszarem badawczym pozostaje koordynacja i wymiana informacji między podmiotami, zarówno w skali krajowej, jak i międzynarodowej. Incydenty cybernetyczne często mają charakter transgraniczny, co wymaga współpracy między zespołami CERT w różnych państwach, wymiany informacji o zagrożeniach oraz standaryzacji procedur reagowania. Literatura naukowa wskazuje, że brak koordynacji zwiększa ryzyko eskalacji incydentów oraz wydłuża czas ich neutralizacji, a także utrudnia identyfikację sprawców i źródeł zagrożeń. W tym kontekście szczególną rolę odgrywają organizacje międzynarodowe, raporty i wytyczne takich instytucji jak ENISA czy NATO Cooperative Cyber Defence Centre of Excellence, które tworzą ramy operacyjne i rekomendacje dla państw członkowskich oraz sektora prywatnego. Kolejnym zagadnieniem jest wpływ incydentów cybernetycznych na bezpieczeństwo strategiczne.

W literaturze przedmiotu podkreśla się, że poważne ataki na infrastrukturę krytyczną, takie jak energetyka, transport, systemy finansowe lub administracja publiczna, mogą mieć charakter destabilizujący dla państwa, wywołując skutki porównywalne z incydentami fizycznymi lub militarnymi. Incydenty te często są elementem działań hybrydowych lub kampanii cyberwojennych, które obejmują zarówno techniczne ataki, jak i manipulacje informacyjne mające na celu dezinformację opinii

publicznej. Dlatego w literaturze zaleca się traktowanie incydentów cybernetycznych nie tylko w kontekście IT, lecz również jako integralnej części bezpieczeństwa narodowego i polityki obronnej. W literaturze naukowej zwraca się również uwagę na edukację i kulturę bezpieczeństwa jako kluczowe elementy prewencji incydentów. Szkolenia pracowników, świadomość zagrożeń cybernetycznych oraz wprowadzanie procedur bezpieczeństwa na wszystkich poziomach organizacji znacząco ograniczają prawdopodobieństwo powstania incydentu. Jednocześnie badania wskazują, że zagrożenia cybernetyczne nie mają wyłącznie charakteru technicznego, lecz oddziałują również społecznie, ponieważ angażują decyzje ludzkie, interakcje w zespołach oraz procesy organizacyjne. Z tego powodu skuteczne zarządzanie incydentem wymaga połączenia kompetencji technicznych z wiedzą z zakresu psychologii organizacji, komunikacji kryzysowej i prawa.

Podsumowując, incydent cybernetyczny jest zjawiskiem o charakterze złożonym i wielowymiarowym, którego znaczenie wykracza poza obszar czysto techniczny. Każde zdarzenie cybernetyczne, niezależnie od jego skali, może mieć konsekwencje operacyjne, organizacyjne, prawne i społeczne, co wymaga traktowania go jako integralnej części strategii bezpieczeństwa państwa i organizacji. Literatura przedmiotu jednoznacznie wskazuje, że skuteczne zarządzanie incydentami wymaga połączenia procedur technicznych, kompetencji ludzkich, mechanizmów koordynacji międzynarodowej oraz zgodności z obowiązującymi regulacjami prawnymi. W tym kontekście incydent cybernetyczny staje się nie tylko wyzwaniem dla działów IT, lecz także przedmiotem analiz strategicznych, oceny ryzyka i planowania odporności systemów na poziomie organizacyjnym i państwowym. Analiza przypadków incydentów cybernetycznych wskazuje, że większość poważnych naruszeń wynika z połączenia czynników technicznych, błędów ludzkich i niewystarczającej koordynacji między podmiotami odpowiedzialnymi za bezpieczeństwo. Z tego względu literatura naukowa zaleca wielopoziomowe podejście do zarządzania incydentem, które obejmuje prewencję, monitorowanie, szybkie reagowanie i naukę na podstawie doświadczeń. W szczególności podkreśla się rolę edukacji pracowników, budowania kultury bezpieczeństwa oraz ciągłego doskonalenia procedur reagowania. Jednym z kluczowych

wniosków płynących z literatury jest fakt, że incydenty cybernetyczne są zjawiskiem nieuniknionym w warunkach rosnącej cyfryzacji i złożoności systemów informatycznych. Nie chodzi jedynie o eliminowanie zagrożeń technicznych, lecz o kształtowanie odporności systemowej, w tym zdolności do szybkiego wykrycia, oceny skutków i efektywnego reagowania na zdarzenia. W tym sensie incydent cybernetyczny staje się narzędziem diagnostycznym pozwalającym na identyfikację słabości systemu, optymalizację procedur bezpieczeństwa i wzmocnienie mechanizmów ochrony informacji oraz infrastruktury krytycznej. Należy również podkreślić, że zarządzanie incydentami cybernetycznymi ma charakter interdyscyplinarny. Skuteczna reakcja wymaga współpracy specjalistów z zakresu technologii informatycznych, prawa, bezpieczeństwa państwowego, komunikacji kryzysowej oraz psychologii organizacji.

Literatura wskazuje, że integracja tych kompetencji umożliwia nie tylko minimalizację szkód spowodowanych incydentami, lecz również zwiększa odporność systemów na przyszłe zagrożenia, przyczyniając się do budowy bezpiecznego i stabilnego środowiska cyfrowego na poziomie lokalnym, krajowym i międzynarodowym. W perspektywie strategicznej incydent cybernetyczny pełni więc funkcję wskaźnika odporności systemowej oraz miernika skuteczności polityki bezpieczeństwa. Jego analiza pozwala na wyciąganie wniosków dotyczących słabości infrastruktury, identyfikację trendów zagrożeń, doskonalenie procedur reagowania oraz budowanie świadomości i kultury bezpieczeństwa w organizacjach i społeczeństwie.

Aleksandra Gębacz

CRITIS 2011. Lecture Notes in Computer Science, vol. 6983; *ICS 2022 Annual Report. From: Incident Classification Scale Subgroup, 2023*, https://eepublicdownloads.entsoe.eu/clean-documents/SOC%20documents/Incident_Classification_Scale/2022/2022_ICS_Annual_Report.pdf (dostęp 12.12.2025); E. Luiijf, R. Besseling, P. Spoelstra, *Ten National Cyber Security Strategies: A Comparison*, [w:] *Critical Information Infrastructure Security*, S. Bologna, B. Hämmerli, D. Gritzalis, S. Wolthusen, (eds.), Springer, Berlin, Heidelberg 2013;*National Defense*, F. Kramer, S. Starr, L. Wentz (eds.), University Press, Washington DC 2009; T. Rid, B. Buchanan, *Attributing Cyber Attacks*, „Journal of Strategic Studies" 2014, vol. 38, no. 1–2; D.

Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm*, „Prawo w Działaniu. Sprawy Karne" 2023, nr 53; K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, Gaithersburg 2015; W. Wróblewski, N. Tuśnio, *Redukcja ryzyka incydentu w oparciu o analizę ryzyka w cyberprzestrzeni operacyjnej Straży Pożarnej. Cybersecurity perspective*, Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi, Józefów 2023.

INŻYNIERIA PODPOWIEDZI (ang. *prompt engineering*) to wyodrębniająca się subdyscyplina sztucznej inteligencji – w szczególności przetwarzaniem języka naturalnego (ang. NLP – Natural Language Processing) – zajmująca się projektowaniem, optymalizacją i automatyzacją komunikatów wejściowych kierowanych do modeli AI[2]. Polega na strategicznym projektowaniu instrukcji/poleceń/sugestii (tzw. AI Prompt Design) specyficznych dla danego zadania, zwanych „podpowiedziami" (ang. *prompts*), w celu kierowania wynikami modelu bez zmiany jego wewnętrznych parametrów.

Ogólnie inżynierię podpowiedzi możemy opisać jako systematyczną metodologię konstruowania i modyfikowania komunikatów wejściowych w celu wywołania pożądanych zachowań modeli językowych – zarówno na poziomie pojedynczej odpowiedzi, jak i całych procesów interakcji człowiek–system AI (Gao 2023; Viswanathan 2025). Struktura promptu obejmuje:

- dobór formy (polecenie, pytanie, szablon, dialog);
- określenie ról i perspektyw (np. „Zachowuj się jak ekspert…");
- włączenie kontekstu (dane, dokumenty, wcześniejsze wypowiedzi);

[2] Modele AI (szczególnie duże modele językowe – Large Language Models/LLM, które stoją za popularnymi chatbotami i asystentami AI, o których ostatnio tak głośno) – czyli zaawansowane systemy o miliardach parametrów, zdolne do generowania złożonych i wielowarstwowych treści – stanowią pewien przełom w interakcjach między człowiekiem a maszyną, umożliwiając maszynom rozumienie i generowanie ludzkiego języka w sposób, który był dotychczas niemożliwy do osiągnięcia. Dzielą się głównie na generatywne (tworzące nową zawartość, np. GPT-4, Claude) oraz predykcyjne (prognozujące wyniki). Ich skuteczność zależy jednak w dużej mierze od jakości zapytania (prompta).

- nałożenie ograniczeń formalnych (format odpowiedzi, długość, język, styl);
- określenie kryteriów jakości (dokładność, spójność, bezpieczeństwo).

Obecnie rozróżnia się podpowiedzi pisane przez człowieka (instrukcje w języku naturalnym) tzw. *hard prompts* oraz wyuczone (reprezentacje wektorowe lub szablony generowane automatycznie) tzw. *soft prompts*, traktowane łącznie jako przestrzeń sterowania zachowaniem modelu (Sahoo et al. 2025). Inżynieria podpowiedzi to, z jednej strony, praktyka (zbiór technik stosowanych przez użytkowników, umiejętność efektywnej komunikacji z modelami AI), z drugiej zaś – obszar badań, w ramach którego powstają m.in. taksonomie i formalne modele „programowania" modeli językowych (Beurer-Kellner, Fischer, Vechev 2023; Chen, Zhang, Langrené, Zhu 2025).

Wśród strategii projektowania promptów – stosowanych przez inżynierów podpowiedzi (i nie tylko) – pomagających narzędziom generatywnej AI skuteczniej rozwiązywać złożone zadania możemy wyróżnić m.in. (Sahoo et al. 2025; Liu et al. 2025):

1. *Zero-shot*, *few-shot* i *one-shot prompting* – techniki różniące się liczbą dostarczanych przykładów. Model otrzymuje zapytanie bez żadnych przykładów lub z kilkoma, które pomogą AI zrozumieć intencję użytkownika bez nadmiaru danych, po czym generowane są odpowiedzi dla nowego przykładu w tym samym formacie. Dobór odpowiedniej techniki zależy od stopnia skomplikowania zadania i oczekiwanej precyzji odpowiedzi.
2. *Chain-of-thought* i *tree-of-thought prompting* – techniki wspierające proces myślowy (gdy zadanie wymaga logicznego rozumowania):
   - *chain-of-thought prompting* – model analizuje problem krok po kroku, jakby „myślał na głos", co prowadzi do trafniejszych wniosków;
   - *tree-of-thought prompting* – model rozważa różne scenariusze, tworząc rozgałęzione ścieżki myślenia, by wybrać najlepsze rozwiązanie.
3. *Least-to-most prompting* i *prompt chaining* – techniki niezastąpione w zadaniach wymagających wieloetapowego rozumowania

i zachowania spójności logicznej (pomagają modelowi przetwarzać informacje etapami):
   - *least-to-most prompting* – problem dzielony jest na mniejsze części, od najłatwiejszych do najtrudniejszych, co pozwala budować zrozumienie krok po kroku;
   - *prompt chaining* – każda odpowiedź modelu staje się podstawą dla kolejnego zapytania, tworząc logiczny łańcuch prowadzący do rozwiązania.
4. *Self-consistency decoding* i *self-refine prompting* – podejścia, które pozwalają modelowi „uczyć się na bieżąco" i samodzielnie podnosić jakość generowanych treści (koncentrują się na poprawie jakości odpowiedzi poprzez wewnętrzną analizę):
   - *self-consistency decoding* – model generuje kilka odpowiedzi i wybiera tę, która pojawia się najczęściej, co zwiększa trafność końcowego wyniku;
   - *self-refine prompting* – AI analizuje i poprawia własne wypowiedzi, prowadząc do bardziej dopracowanych rezultatów.
5. *Graph-of-thought*, *thread-of-thought* i *chain-of-table prompting* – techniki idealne do zadań wymagających porządkowania, analizy danych i logicznego rozgałęzienia myśli (wspierają analizę złożonych struktur danych i zależności):
   - *graph-of-thought prompting* – proces myślenia przedstawiany jest jako graf, co ułatwia analizę problemów z wieloma możliwymi ścieżkami rozwiązania;
   - *thread-of-thought prompting* – skupia się na śledzeniu wątków w zależności od kontekstu, co poprawia zrozumienie struktury informacji;
   - *chain-of-table prompting* – dane prezentowane są w formie tabel, a analiza odbywa się krok po kroku, co sprawdza się przy pracy z liczbami i strukturami.
6. *Maieutic prompting* i *directional stimulus prompting* – techniki inspirowane filozofią i mechanizmami ukierunkowania (wspierają eksplorację tematu i pomagają modelowi unikać błędnych ścieżek rozumowania):

- *maieutic prompting* – model generuje wyjaśnienia, które następnie sam analizuje i rozwija, prowadząc do głębszego zrozumienia tematu;
- *directional stimulus prompting* – dodatkowy mechanizm lub model sugeruje kierunek działania na podstawie słów kluczowych, działając jak wewnętrzny kompas.

7. *Generated knowledge prompting* i *chain-of-symbol prompting* – techniki wspierające tworzenie wiedzy i abstrakcyjne myślenie (idealne do zadań wymagających kreatywności, abstrakcji i precyzyjnego odwzorowania zależności):
   - *generated knowledge prompting* – model najpierw generuje potrzebne informacje, zanim przystąpi do rozwiązania zadania, jakby tworzył „ściągę" przed egzaminem;
   - *chain-of-symbol prompting* – przekształca język naturalny w symbole, co ułatwia analizę relacji logicznych, przestrzennych i matematycznych.
8. *Reducet hallucynation* – techniki minimalizujące halucynacje modeli AI i zapewniające dokładność i wiarygodność wyników:
   - Retrieval-Augmented Generation (RAG) – technika płynnie wplatająca wyszukiwanie informacji w proces podpowiedzi. RAG analizuje dane wprowadzane przez użytkownika, tworzy ukierunkowane zapytanie i przeszukuje gotową bazę wiedzy w poszukiwaniu odpowiednich zasobów. Pobrane fragmenty kodu są włączane do oryginalnego polecenia, wzbogacając je o kontekst. Rozszerzony komunikat umożliwia modelom AI generowanie kreatywnych, rzetelnych odpowiedzi;
   - ReAct Prompting – ReAct (Reasoning Acting) – podejście oparte na podpowiadaniu i przetwarzaniu wyników, które łączy rozumowanie, planowanie działań i integrację źródeł wiedzy, aby model AI wykorzystywał informacje ze świata rzeczywistego w swoich prognozach. ReAct to połączenie rozumowania i działania;
   - Chain-of-Verification (CoVe) Prompting – technika redukcji halucynacji AI poprzez rozbicie złożonych zapytań na mniejsze weryfikowalne kroki. Technika ta tworzy systematyczne punkty

kontrolne w celu weryfikacji poprawności odpowiedzi generowanych przez AI przed dostarczeniem ostatecznych wyników. Zazwyczaj implementuje się za pomocą kilku promptów: 1 dla pytania pierwotnego, 1 dla pytań weryfikacyjnych i 1 do wygenerowania ostatecznej odpowiedzi;
- Chain-of-Note (CoN) Prompting – technika mająca na celu usprawnienie implementacji RAG poprzez rozwiązywanie problemów związanych z zaszumionymi danymi czy nieistotnymi dokumentami (model generuje sekwencyjne notatki dotyczące lektury pobranych dokumentów, co pozwala na systematyczną ocenę trafności i dokładności informacji pobranych z dokumentów zewnętrznych). To podejście skutecznie odsiewa treści nieistotne lub mniej wiarygodne, co skutkuje nie tylko bardziej precyzyjnymi, ale i kontekstowo trafnymi odpowiedziami;
- Chain-of-Knowledge (CoK) Prompting – technika zaprojektowana w celu zwiększenia dokładności modelu LLM w zadaniach wymagających dużej wiedzy poprzez dynamiczną integrację zewnętrznych, heterogenicznych źródeł wiedzy. Działa ona w trzech etapach – przygotowanie rozumowania, adaptacja wiedzy i konsolidacja odpowiedzi – aby ograniczyć halucynacje i poprawić poprawność faktów. Technika doskonale sprawdza się w przypadku złożonych zadań wymagających rozumowania.

9. *Negative prompting* i *multimodal prompting* – techniki zwiększające bezpieczeństwo i wszechstronność interakcji z AI (multimodalność otwiera nowe możliwości zastosowań AI – od analizy zdjęć medycznych po opisy wideo i zadania wymagające integracji wielu formatów danych):
   - *negative prompting* – informuje model, czego ma unikać (np. błędnych założeń, nieodpowiedniego tonu, tematów tabu), co zwiększa trafność i bezpieczeństwo odpowiedzi;
   - *multimodal prompting* – łączy tekst, obraz i dźwięk w jednym zapytaniu, umożliwiając analizę złożonych danych z różnych źródeł.

Wzrost zainteresowania inżynierią podpowiedzi wynikający m.in. z potrzeby automatycznego projektowania promptów[3] i dostrajania modelu[4] pozwala zauważyć kilka istotnych nurtów rozwoju inżynierii podpowiedzi (Sahoo et al. 2025; Chen et al. 2025; Viswanathan 2025):

1. Optymalizacja ręczna – najprostszą formą jest cykl zaprojektuj → przetestuj → zmodyfikuj oparty na ewaluacji jakości odpowiedzi według z góry przyjętych kryteriów (dokładność, spójność stylu, zgodność z politykami). Mimo swojej „ręcznej" natury pozostaje podstawową praktyką w wielu zastosowaniach eksperckich (Gao 2023).
2. Przeszukiwanie przestrzeni promptów (*prompt search*) – badacze stosują metody optymalizacji kombinatorycznej i metaheurystyki do automatycznego przeszukiwania różnych wariantów promptów i wybierania tych o najwyższej skuteczności na walidacyjnych zestawach zadań (Sahoo et al. 2025; Vatsal, Dubey 2024).
3. Uczenie promptów (*learned/soft prompts*) – zamiast tekstu w języku naturalnym stosuje się wyuczone wektorowe reprezentacje w przestrzeni modelu (tzw. *soft prompts*)[5], które są optymalizowane metodami uczenia maszynowego pod konkretne zadania. Miękkie

---

[3] Odpowiedzią na potrzebę lepszej komunikacji z modelami generatywnymi są generatory promptów AI – narzędzia wspierające użytkownika w formułowaniu skutecznych, zoptymalizowanych instrukcji.

[4] Dostrajanie modelu (*fine-tuning*) to technika uczenia maszynowego polegająca na wzięciu wstępnie wytrenowanego modelu i wprowadzeniu drobnych zmian, by dostosować go do nowego, konkretnego zadania lub zbioru danych. Zamiast budować model od zera, co może być czasochłonne i wymagać dużych zasobów, dostrajanie wykorzystuje wiedzę, którą model już nabył podczas wcześniejszego treningu na dużych zbiorach danych. Poprzez dostosowanie parametrów modelu deweloperzy mogą poprawić wydajność w nowym zadaniu przy mniejszej ilości danych i zasobów obliczeniowych.

[5] Mówiąc ogólnie, *soft prompts* można opisać jako koncepcję polegającą na włączaniu wektorów do sekwencji wejściowej, a następnie ich dostrajaniu przy jednoczesnym zachowaniu pozostałych komponentów wstępnie wyszkolonego modelu bez zmian. To wektory monitujące, których wagi zostały zoptymalizowane pod kątem konkretnych zadań, co sprawia, że są one niemożliwe do zinterpretowania przez ludzi. Za: O. Patel, *Towards Interpretable Soft Prompts*, https://arxiv.org/html/2504.02144v1.

podpowiedzi zastępują dodatkowe dane treningowe (Sahoo et al. 2025).

4. Języki zapytań i programowanie modeli językowych – koncepcja programowania modelowego języka (Language Model Programming – LMP[6]; opracowana przez naukowców z ETH w Zurychu) zakłada traktowanie całej interakcji z modelem jak programu, w którym prompt jest jednym z elementów, obok pętli, instrukcji warunkowych i ograniczeń na przestrzeń wyjść (przykładem jest język LMQL) (Beurer-Kellner et al. 2023).
5. Automatyczna generacja promptów i *meta-prompting* – w niektórych pracach stosuje się „meta-prompty" – modele proszone są o zaprojektowanie własnych promptów optymalnych dla danego zadania, które następnie są testowane lub dalej udoskonalane (Reynolds, McDonell 2021; Chen et al. 2025).

Rozwój inżynierii podpowiedzi wiąże się nie tylko z poprawą jakości treści generowanych przez sztuczną inteligencję, ale także z istotnymi wyzwaniami bezpieczeństwa. Do kluczowych obszarów ryzyka możemy zaliczyć (Slocum, Hadfield-Menell 2025; Chen et al. 2025; Sahoo et al. 2025):

1. Prompt *injection* i jailbreaki:
   - *prompt injection* polega na wstrzyknięciu do wejścia instrukcji, które mają nadpisać lub „obejść" pierwotne wytyczne systemu (np. prośba, by zignorować wcześniejsze reguły bezpieczeństwa);
   - *jailbreak* to szczególny przypadek ataku, którego celem jest wymuszenie generowania treści niezgodnych z politykami bezpieczeństwa poprzez kreatywne konstruowanie promptów. Stewart Slocum i Dylan Hadfield-Menell (2025) proponują tzw. *inverse prompt engineering* – automatyczne generowanie „obronnych" promptów stanowiących zadaniowo-specyficzne barierki bezpieczeństwa (guardrails).
2. Wycieki danych i ujawnianie informacji poufnych. Źle zaprojektowane prompty mogą nakłaniać systemy do ujawniania fragmentów

[6] LMP łączy język naturalny i język programowania: komunikaty tekstowe i instrukcje skryptowe.

danych treningowych lub treści poufnych przekazanych w konwersacji (np. danych osobowych). Zalecane jest zatem łączenie inżynierii podpowiedzi z dodatkowymi mechanizmami kontroli dostępu i anonimizacji (Sahoo et al. 2025).

3. Bias, sprawiedliwość i rzetelność odpowiedzi. Prompty mogą nieświadomie wzmacniać uprzedzenia modelu AI, np. poprzez asymetryczne formułowanie pytań dotyczących różnych grup społecznych. W tym względzie istotne jest stosowanie technik projektowania promptów ukierunkowanych na redukcję biasu (np. symetryczne scenariusze, *explicite* wskazanie neutralności, wymuszenie uzasadnień) oraz wielokryterialnej ewaluacji (Chen et al. 2025; Viswanathan 2025).
4. Powtarzalność i wiarygodność wyników LLM są modelami probabilistycznymi; nawet przy identycznym prompcie mogą generować różne odpowiedzi. W kontekście zastosowań naukowych lub regulowanych (medycyna, prawo) rodzi to pytania o powtarzalność, audytowalność oraz możliwość dokumentowania konfiguracji promptów jako części dokumentacji procesu (Chen et al. 2025; Gao 2023).
5. Złożoność systemów i odpowiedzialność. W miarę jak *prompt chaining*[7], języki takie jak LMQL oraz automatyzacja generowania promptów prowadzą do tworzenia złożonych „systemów nad systemami", trudniej jest jednoznacznie wskazać, który element łańcucha (prompt, model, moduł oceny) odpowiada za błąd czy naruszenie zasad, dlatego postuluje się opracowanie formalnych modeli odpowiedzialności i standardów dokumentowania pipeline'ów promptowych[8] (Beurer-Kellner et al. 2023; Sahoo et al. 2025).

---

[7] Dosłownie łańcuchowanie promptów, to jedna z najskuteczniejszych technik inżynierii promptów, która pomaga w optymalizacji pracy modeli językowych LLM. Polega na podzieleniu skomplikowanego zadania na mniejsze podzadania, a odpowiedź na każde z nich staje się wejściem do kolejnego promptu. W efekcie powstaje łańcuch operacji, który prowadzi model krok po kroku do rozwiązania trudnego problemu.

[8] Sekwencji uporządkowanych etapów, zadań lub procesów prowadzących od punktu początkowego do finalizacji (celu).

Należy zauważyć, że inżynieria podpowiedzi staje się centralnym komponentem praktycznego wykorzystania LLM (Chen et al. 2025; Qian et al. 2025; Viswanathan 2025). Obejmuje to m.in.:

- budowę interfejsów dialogowych i asystentów eksperckich;
- narzędzia wspierające tworzenie treści naukowych i dydaktycznych;
- systemy wspomagania decyzji (np. w biznesie czy administracji publicznej);
- integrację modeli językowych z innymi komponentami oprogramowania (API, bazy wiedzy).

Równolegle rozwijane są standardy i wytyczne dobrych praktyk inżynierii podpowiedzi, obejmujące zalecenia dotyczące bezpieczeństwa, przejrzystości, ewaluacji i dokumentowania promptów w środowiskach organizacyjnych (Ronanki 2025; Sahoo et al. 2025).

Wraz z rozwojem technologii sztucznej inteligencji, obok obaw o coraz większy jej wpływ na rozmaite profesje, pojawia się też wiele nowych zawodów, które są już ściśle związane ze skutecznym zarządzaniem możliwościami AI. Jednym z nich jest *prompt engineer*, czyli, spolszczając, inżynier podpowiedzi, uważany wręcz za zawód przyszłości. *Prompt engineer* jest zatem specjalistą od formułowania promptów (poleceń) w taki sposób, by możliwie jak najdokładniej zdefiniować, jakiego działania oczekuje od systemu AI.

Do kluczowych umiejętności wymaganych w zawodzie prompt engineera można zaliczyć:

- znajomość programowania – biegłość w językach programowania, zwłaszcza Pythonie, który jest kluczowy do automatyzacji, skryptowania oraz interakcji z modelami AI;
- znajomość AI i NLP – solidne podstawy w zakresie sztucznej inteligencji i przetwarzania języka naturalnego obejmujące sieci neuronowe, uczenie głębokie, tokenizację, osadzanie słów (*word embeddings*) oraz rozpoznawanie nazwanych jednostek (*named entity recognition*); kluczowe jest także zrozumienie zasad uczenia maszynowego, architektury dużych modeli językowych (LLM) oraz technologii generatywnej AI;

- biegłość językową – dogłębna znajomość języka, w tym składni, semantyki i pragmatyki, pozwalająca na konstruowanie jasnych i jednoznacznych promptów;
- kreatywne i elastyczne pisanie – umiejętność formułowania zapytań i instrukcji w sposób zapewniający informacyjne i kontekstowo trafne odpowiedzi;
- myślenie analityczne i rozwiązywanie problemów – zdolność do projektowania promptów spełniających określone zadania i dostosowywania ich w oparciu o jakość uzyskanych odpowiedzi AI; kluczowe jest iteracyjne testowanie oraz modyfikacja promptów w celu uzyskania optymalnych wyników;
- świadomość etyczną – rozumienie konsekwencji stosowania AI, w tym problemów związanych z uprzedzeniami, sprawiedliwością oraz odpowiedzialnym wykorzystaniem sztucznej inteligencji;
- iteracyjne testowanie i naukę – inżynieria promptów wymaga ciągłego testowania i udoskonalania zapytań, aby osiągnąć pożądane rezultaty;
- umiejętności komunikacyjne – silne kompetencje w zakresie komunikacji werbalnej i pisemnej pozwalające na efektywne formułowanie interakcji z modelami AI;
- analizę danych – zdolność do interpretacji wyników generowanych przez modele AI oraz analizy danych w celu doskonalenia promptów i poprawy jakości odpowiedzi.

Reasumując, inżynieria podpowiedzi pełni funkcję „mostu" między użytkownikiem a złożonym modelem generatywnym: z jednej strony, upraszcza dostęp do jego możliwości, z drugiej – wymaga coraz bardziej systematycznego, krytycznego i bezpiecznego podejścia, typowego dla dojrzałych inżynierskich dyscyplin.

Emilia Musiał

L. Beurer-Kellner, M. Fischer, M. Vechev, *Prompting is programming: A query language for large language models*, „Proceedings of the ACM on Programming Languages" 2023, no. 186, vol. 7 (PLDI), https://doi.org/10.1145/3591300; B. Chen, Z. Zhang, N. Langrené, S. Zhu, *Unleashing the potential of prompt engineering for*

large language models, „Patterns" 2025, no. 6(6), 101260, https://doi.org/10.1016/j.patter.2025.101260; A. Gao, *Prompt engineering for large language models*, https://doi.org/10.2139/ssrn.4504303; Y. Qian, *Prompt engineering in education: A systematic review of early applications*, „Journal of Educational Computing Research" 2025, no. 63(7–8); L. Reynolds, K. McDonell, *Prompt programming for large language models: Beyond the few-shot paradigm*, [w:] *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Y. Kitamura, A. Quigley (eds.), Association for Computing Machinery, New York 2021, https://doi.org/10.1145/3411763.3451760; K. Ronanki, *Prompt engineering guidelines for using large language models*, 2025; P. Sahoo, A.K. Singh, S. Saha, V. Jain, S. Mondal, A. Chadha, *A systematic survey of prompt engineering in large language models: Techniques and applications*, arXiv preprint arXiv:2402.07927; S. Slocum, D. Hadfield-Menell, *Inverse prompt engineering for task-specific LLM safety*, OpenReview, 2025; S. Vatsal, H. Dubey, *A survey of prompt engineering methods in large language models for different NLP tasks*, arXiv preprint arXiv:2407.12994; P.S. Viswanathan, *Prompt engineering for conversational AI systems: A systematic review of techniques and applications*, „International Journal of Scientific Research in Computer Science, Engineering and Information Technology" 2025, no. 11(1), https://doi.org/10.32628/CSEIT25111276.

IRAŃSKIE POCISKI BALISTYCZNE – irański program rakietowych pocisków balistycznych uchodzi za największy na Bliskim Wschodzie, pełniąc przy tym istotną rolę w strategii wojskowej tego państwa. Pociski balistyczne stanowiły 1 z 3 filarów irańskiej strategii odstraszania, przede wszystkim wobec Izraela, obok „osi oporu", grupującej wspierane przez Teheran bliskowschodnie organizacje polityczno-militarne oraz możliwości blokady strategicznej cieśniny Ormuz przy pomocy środków wojskowych; 3 serie wymiany ciosów pomiędzy Iranem a Izraelem w latach 2024–2025 wykazały przy tym, że nawet jeśli wskazana już triada odstraszania nie zdołała zapobiec izraelskim atakom, to pociski balistyczne okazały się jedynym użytecznym środkiem militarnej odpowiedzi Iranu.

Program rozwoju i produkcji pocisków balistycznych jest koordynowany przez Aerospace Industries Organization (AIO – Organizacja Przemysłu Lotniczego i Kosmicznego), jednostkę podległą irańskiemu ministerstwu obrony narodowej. Istotną rolę pełni również Korpus Strażników Rewolucji Islamskiej oraz funkcjonująca w jego ramach jednostka

badawczo-rozwojowa Research and Self-Sufficiency Jihad Organization (Organizacja Badań i Dżihadu Samowystarczalności).

Korzeni irańskiego programu rakietowego doszukiwać się można jeszcze w czasach rządów szacha Mohammada Rezy Pahlawiego. W ramach projektu Flower nawiązano współpracę z Izraelem po tym, jak Stany Zjednoczone odmówiły Iranowi sprzedaży pocisków Lance. Współpraca była jednym z elementów porozumienia „ropa za broń", podpisanego w 1977 r. przez szacha oraz ministra obrony Izraela Szimona Peresa. Po rewolucji islamskiej w 1979 r. prace wstrzymano; impuls do ich wznowienia przyniosła wojna iracko-irańska: program rakietowy stanowił odpowiedź na irackie ataki rakietowe na irańskie miasta dokonywane przy pomocy pocisków balistycznych 9K52 Łuna-M oraz 9K72 Elbrus (oznaczenie NATO – Scud-B). Iran pozyskał pierwsze 20 pocisków 9K72 z Libii w 1984 r., a następnie ich wersje pochodne z Korei Północnej oraz Chin. Doprowadziło to do kolejnych kampanii rakietowych w ramach tzw. wojny miast (łącznie 5 kampanii, z których najbardziej intensywna miała miejsce w pierwszej połowie 1988 r.) oraz rozpoczęcia regionalnego wyścigu zbrojeń. W jego ramach Irak rozpoczął w 1987 r. produkcję zmodernizowanego pocisku Scud-B nazwanego Al-Hussain o zasięgu zwiększonym do ponad 600 km, co pozwalało na rażenie Teheranu. Odpowiedzią Iranu był własny program produkcji pocisków balistycznych o zwiększonym zasięgu, w pierwszym okresie również opierający się na pociskach rodziny Scud-B, w tym przede wszystkim na ich północnokoreańskiej derywacji Hwasong-5. Pierwszym efektem tego programu był pocisk Shabab-1, którego próby rozpoczęto w latach 1987–1988, a zdolności produkcyjne uzyskano około 1994 r. lub później. Był on wykorzystywany w atakach rakietowych na obozy Organizacji Mudżahedinów Ludowych w latach 1994, 1999 i 2001. Istotnym kontekstem dalszych postępów irańskiego programu rakietowego, oprócz oczywiście napiętych relacji z Izraelem, było posiadanie pocisków balistycznych przez Arabię Saudyjską, która zakupiła chińskie pociski DF-3 o zasięgu około 4000 km jeszcze w 1987 r.

Większość irańskich pocisków balistycznych powstała prawdopodobnie z wykorzystaniem rozwiązań północnokoreańskich, chociaż ścieżki rozwoju programów rakietowych realizowanych w tych 2 państwach stopniowo się rozchodzą – najnowsze pociski irańskie wykazują coraz mniejsze

podobieństwo do północnokoreańskich wzorców, z kolei zaprezentowane w ostatnich latach pociski północnokoreańskie, w przeważającej mierze o zasięgu międzykontynentalnym, nie znajdują odzwierciedlenia w arsenale Teheranu. Irański program rakietowy rozwijał się, w dużym uproszczeniu, z uwzględnieniem rosnącego dystansu do przewidywanych celów – na początku był ukierunkowany na Irak, następnie rozwijano pociski zdolne do sięgnięcia Arabii Saudyjskiej, wreszcie wdrożono pociski o zasięgu wystarczającym do rażenia obiektów na terenie Izraela. To ostatnie zadanie wymaga posiadania pocisków o zasięgu minimum 1000–1200 km, a najlepiej około 2000–2500 km (pozwala to odpalać pociski nie tylko z rejonów nadgranicznych, ale także głębi terytorium Iranu).

Analiza irańskiego programu rakietowego jest utrudniona z uwagi na brak przejrzystości i małą wiarygodność danych pochodzących ze źródeł oficjalnych. Dotyczy to zarówno rzeczywistych możliwości rakiet, jak i ich nazewnictwa, stąd wszystkie dane należy traktować jako szacunkowe.

Istotna część irańskich rakietowych pocisków balistycznych wywodzi się z rdzenia konstrukcyjnego sięgającego radzieckich pocisków 9K72 Elbrus (Scud-B), a szczególnie z ich odmian północnokoreańskich. Dotyczy to przede wszystkim pocisków rodziny Shahab, w wersjach Shabab-1, Shabab-2 i Shabab-3. Są to więc rakiety jednostopniowe, napędzane silnikami na ciekły materiał pędny. Kolejne iteracje charakteryzują się rosnącym zasięgiem, w przypadku ostatniej wersji przekraczającym 1000 km. Rakiety tej rodziny mogą być wyposażone w kilka typów głowicy bojowej, które w najnowszych wersjach prawdopodobnie mają możliwość oddzielania się od zasadniczego korpusu rakiety na torze lotu. Istnieje też głowica kasetowa, zawierająca podpociski o masie kilkunastu kilogramów każdy. Wersją rozwojową rakiet Shabab jest Ghadr: wyróżnia się ona zwiększoną długością kadłuba, co przekłada się na większy zasięg, wynoszący prawdopodobnie około 1600 km. Dwie kolejne rakiety z tej rodziny to Emad i Etemad – w ich przypadku udało się po raz kolejny zwiększyć zasięg, który prawdopodobnie sięga około 2000 km. Kluczową zmianą jest jednak zastosowanie manewrującej głowicy bojowej, wyposażonej w stery aerodynamiczne, a w przypadku Etemeda – prawdopodobnie także w aktywny radiolokator służący do naprowadzania na końcowym odcinku lotu. Manewrująca głowica bojowa pozwala na znaczne zwiększenie

celności względem starszych wersji, może też utrudnić przechwycenie przez systemy antyrakietowe.

Pocisk Sejjil jest konstrukcją odmienną od wcześniej wzmiankowanych. Zasadniczą różnicą jest budowa dwustopniowa, co pozwala na zwiększenie zasięgu do około 2000–2500 km. Ponadto pocisk ten wykorzystuje stały materiał pędny, przynajmniej w przypadku pierwszego stopnia (rodzaj silnika wykorzystywanego do napędu drugiego stopnia budzi kontrowersje). Głowica bojowa nie różni się raczej tej stosowanej w pociskach Shabab-3 i Ghadr. Pociski określane jako Shadr-110 oraz Ashura są prawdopodobnie blisko związane z Sejjil, być może nawet są to inne nazwy odnoszące się do tej samej konstrukcji.

Khorramshar ujawniony w 2023 r. (pierwszy test miał miejsce prawdopodobnie w 2017 r.) jest pociskiem o zupełnie innej konstrukcji niż wcześniej wymienione. Wykazuje on pewne podobieństwo do północnokoreańskich pocisków Hwasong-10; jego kadłub charakteryzuje się znacznie mniejszym wydłużeniem, budowa pocisku jest jednostopniowa, a silnik pracuje w oparciu o ciekły materiał pędny, jednak w porównaniu do rakiet wywodzących się ze Scuda znacznie skrócono czas przygotowań przedstartowych. Głowica pocisku ma możliwość manewrowania, jednakże szczegółowe informacje na temat systemu sterowania oraz metody naprowadzania końcowego są sprzeczne. Prawdopodobnie istnieją 2 odmiany głowicy różniące się masą, a odpowiadają im 2 odmiany pocisku określane jako Khorramshar-3 i Khorramshar-4. Zasięg pocisku szacowany jest na 2000 km, ale na tę odległość możliwe jest przenoszenie głowicy bojowej o masie 1500–1800 kg, więcej niż w przypadku wcześniejszych konstrukcji.

Osobną grupę stanowią pociski rakietowe napędzane silnikami na stały materiał pędny i charakteryzujące się stosunkowo niewielkimi rozmiarami (pozwalającymi na odpalanie z względnie niedużych wyrzutni mobilnych), przy zachowaniu znacznego zasięgu (prawdopodobnie około 1400 km). Według doniesień ich głowice mają możliwość manewrowania i charakteryzują się zwiększoną celnością, co ma rekompensować ich mniejszą masę (około 350 kg). Do rakiet tej rodziny zalicza się Haj Ghasem, Kheibar Shakan (inna głowica, prawdopodobnie nieco większy zasięg) oraz Fattah (prawdopodobnie konstrukcja dwustopniowa, gdyż

część głowicowa posiada silnik napędowy, a nie tylko sterowanie gazodynamiczne).

Wszystkie typy irańskich pocisków balistycznych wykorzystują stosunkowo proste wyrzutnie mobilne, zabudowane na samochodach ciężarowych oraz naczepach sprzęgniętych z ciągnikami siodłowymi. Konstrukcje te są przystosowane do przemieszczania się po drogach bitych, generalnie nie posiadając żadnych właściwości pokonywania trudnego terenu. W przypadku lżejszych rakiet na stały materiał pędny wyrzutnie wykorzystują zwykłe komercyjne ciężarówki, a rakieta umieszczona jest w imitacji kontenera. W celu zwiększenia przeżywalności swojego arsenału rakietowego Iran podjął znaczący wysiłek zmierzający do ukrycia wyrzutni w podziemnych instalacjach; mają one charakter schronów, w których można garażować wyrzutnie, a w niektórych z nich prawdopodobnie możliwa jest też realizacja części procedury przedstartowej. Istnieją zdjęcia dokumentujące podziemną instalację, w której umieszczona jest wyrzutnia, a start pocisku odbywać się ma poprzez otwór w stropie. Iran podjął też prace związane z budową stacjonarnych podziemnych silosów przystosowanych do odpalania rakiet, ale prawdopodobnie instalacje takie nie zostały ukończone przynajmniej do czasu „wojny 12-dniowej" pomiędzy Izraelem a Iranem w czerwcu 2025 r.

Rafał Kopeć

D.M. Gettinger, C. Thomas, *Iran's Ballistic Missile Programs: Background and Context*, Congressional Research Service, Washington 2025; D. Ghosal, *Role Of Ballistic And Cruise Missiles In International Security*, Palgrave Mcmillan, Cham 2023; P. Izewicz, *Iran's Ballistic Missile Programme: Its Status and The Way Forward*, „Non-Proliferation Papers" 2017, no. 57; T. Szulc, *Irańskie rakiety balistyczne użyte przeciw Izraelowi*, „Nowa Technika Wojskowa" 2025, nr 7, s. 50–60.

K

KARELSKI BATALION NARODOWY (ros. *Карельский Национальный Батальйон; karelski Karjalan Kansallini Pataljona*), zwany także Nordem, to ochotnicza jednostka wojskowa składająca się z rdzennej ludności Karelii oraz innych grup etnicznych ugrofińskich i skandynawskich, utworzona w celu obrony Ukrainy podczas rosyjskiej inwazji. 19 stycznia 2023 r. przedstawiciele Karelskiego Ruchu Narodowego ogłosili utworzenie w Siłach Zbrojnych Ukrainy oddziału karelskiego w ramach Międzynarodowego Legionu Obrony Terytorialnej Ukrainy. Główne wymagania przyjęcia to dobry stan zdrowia, brak problemów z alkoholem i narkotykami, przywiązanie do „tradycyjnych wartości nordyckich", chęć wyzwolenia Karelii spod okupacji oraz przyczynienia się do zwycięstwa nad „terrorystycznym" reżimem Putina. Część rosyjskich dziennikarzy uważa, że KNB to batalion propagandowy.

Zwykle batalion składa się z 600–800 ludzi. Jest prawdopodobne, że Karelski Batalion Narodowy nie jest pełnoprawną jednostką w tradycyjnym tego słowa znaczeniu – przynajmniej na razie. Nie jest jasne, czy batalion brał udział w rzeczywistych działaniach bojowych, czy też jest nadal tworzony i szkolony. Jego deklarowanym celem, zdaniem kilku

karelskich działaczy politycznych zaangażowanych w utworzenie jednostki, było wzięcie udziału w walce z Rosjanami podczas inwazji na Ukrainę. Dodatkowo osiągnięcie całkowitego wyzwolenia i niepodległości regionu nazywanego „okupowaną Karelią" – powszechnie znanego jako Republika Karelii. Karelski Batalion Narodowy zabiega także o uniezależnienie się innych narodów ugrofińskich od Rosji.

Aktywiści twierdzą, że batalion im. Vasela Levonena[9] zamierza walczyć z rosyjskim okupantem w Ukrainie i ostatecznie doprowadzić do wyzwolenia Karelii spod „rosyjskiej okupacji" i pełnej niepodległości kraju. „Opowiadamy się za jednością i spójnością wszystkich zawziętych jednostek narodowych w naszym pragnieniu i inspiracji, aby zrzucić na zawsze kolonialne kajdany imperialne, które tłumią wolę narodów zniewolonych przez Moskwę".

Rekrutacja do jednostki rozpoczęła się na początku stycznia 2023 r., a kryteria dotyczące ochotników zostały określone na kanale Telegram. Z opublikowanych materiałów wynika, że do 24 lutego 2023 r. była ona obecna w Ukrainie. Oficjalna liczba ochotników tam i w sąsiedniej Finlandii, obok Karelii, nie jest jednak znana.

---

[9] Vaseli Levonen (1855–1942), pseudonim Ukka Väinämöinen, to karelski i fiński działacz publiczny, który przewodził powstaniu karelskiemu przeciwko Rosji sowieckiej w latach 1921–1922. Urodzony jako Wasilij Sidorow był wschodniokarelskim bojownikiem o wolność, ideologicznym przywódcą powstania wschodniokarelskiego. Stał się znaną osobą, gdy został wybrany do trzyosobowego zarządu Karelskiej Leśnej Organizacji Partyzanckiej Organizacji Wyzwolenia Wschodniej Karelii jako duchowy przywódca powstania. Levonen zyskał dużą popularność jako przywódca „partyzantów leśnych" (karelska nacjonalistyczna organizacja partyzancka utworzona w ostatnich latach wojny domowej w Rosji na terenie założonej przez bolszewików Karelskiej Komuny Robotniczej). Został wybrany do tego zadania, ponieważ był przeciwnikiem bolszewizmu, gorliwym chrześcijaninem i zagorzałym antykomunistą. Ponadto wydawał się bardzo popularny wśród Karelczyków. Do końca grudnia 1921 r. siły rebelianckie pod dowództwem Väinämöinena, wspierane przez fińskich ochotników, opanowały znaczną część północno-wschodniej Karelii i dopiero wtedy dowództwo sowieckie podjęło decyzję o utworzeniu Frontu Karelskiego, do którego przerzucono wiele jednostek Armii Czerwonej liczących do 20 tys. ludzi. W połowie lutego 1922 r., kiedy czerwoni zajęli ostatni bastion powstańców, wieś Uchta, opór Karelów-Finów został ostatecznie złamany. Około 30 tys. karelskich uchodźców, w tym Levon, udało się do Finlandii. Wkrótce po ucieczce do Finlandii Väinämöinena stracił wzrok.

Zainspirowani ideą niepodległości Karelii działacze Karelskiego Ruchu Narodowego rzucili wyzwanie rosyjskiej okupacji i utworzyli Karelski Batalion Narodowy. Impulsem do jego powstania była wieloletnia walka narodu karelskiego o prawa, samostanowienie i wyzwolenie spod panowania rosyjskiego. Batalion od samego początku swojego istnienia postawił sobie 2 kluczowe cele: ochronę Ukrainy przed rosyjską agresją oraz walkę o wyzwolenie Karelii spod okupacji rosyjskiej; są one ze sobą ściśle powiązane, gdyż wyzwolenie Karelii spod sił okupacyjnych możliwe jest jedynie w kontekście pełnego zwycięstwa Ukrainy nad Rosją.

Na czele Karelskiego Ruchu Narodowego, który został utworzony w 2012 r., stoi Dmitrij Kuzniecow (Miteri Panfiłow). Po rozpoczęciu agresji Kremla na Donbas pojawiła się strona internetowa ruchu domagającego się niepodległości Karelii, która w 2015 r. została zablokowana przez Roskomnadzor, dlatego ruch oficjalnie został zarejestrowany jako organizacja pozarządowa w Estonii – jednym z ideologicznych bastionów, obok Finlandii, projektu Wielka Finno-Ugria. Nazwa jest warunkowa, oznacza wycofanie się republik ugrofińskich spod jurysdykcji Rosji i ich reorientację na Zachód. Projekt Finno-Ugria zrzesza 50 instytucji i organizacji społecznych zaangażowanych w realizację polityki ugrofińskiej Estonii.

Ruch narodowowyzwoleńczy Karelii zgromadził pod swoimi skrzydłami bojowników różnych pokoleń, oddanych wspólnej sprawie walki o wolność i niepodległość. Są wśród nich doświadczeni żołnierze, którzy brali udział w działaniach wojennych, a także młodzi ludzie, którzy postanowili poświęcić swoje życie wyzwoleniu ojczyzny. Od początku wojny rosyjsko-ukraińskiej Karelski Batalion Narodowy stał się integralną częścią Sił Zbrojnych Ukrainy: bierze udział w działaniach bojowych w różnych regionach, wykazując się odwagą i męstwem w walce z siłami okupacyjnymi. Bohaterstwo żołnierzy batalionu stało się przykładem nie tylko dla personelu wojskowego, ale także całego narodu karelskiego.

Po rosyjskiej inwazji na Ukrainę aktywność partyzantów w Karelii i Ingrii zyskała większe znaczenie – szczególnie w kontekście wyzwolenia spod jarzma rosyjskiego imperializmu. Charakter działań naraził aktywistów na potencjalne ryzyko i wyzwania, takie jak uwięzienie i ściganie.

Celem Karelskiego Ruchu Narodowego jest utworzenie niepodległego państwa narodowego dla Karelów, Finów, Wepsów, Pomorów i Norwegów

Kilońskich, które będzie wyznawać „tradycyjne wartości nordyckie". Organizacja uważa Rosjan w Karelii za okupantów, którzy muszą się zasymilować lub opuścić kraj. Ruch rości sobie pretensje terytorialne do Przesmyku Karelskiego, obejmującego Wyborg, Kandalakszę, południowo-wschodnią część Półwyspu Kolskiego, miasta Onega, Tichwin, Witegrę i Kirisz.

Strona rosyjska uważa, że Karelski Ruch Narodowy został utworzony, aby podsycać konflikty w Karelii i tworzyć narrację o chęci oddzielenia regionu od Rosji. Sekretarz Rady Bezpieczeństwa Rosji Nikołaj Patruszew powiedział, że zagraniczne służby specjalne werbują mieszkańców Karelii do batalionu „nacjonalistycznego". Natomiast część fińskich polityków i dziennikarzy uważa, że organizacja została utworzona przez rosyjskie służby specjalne w celu podżegania do rewanżyzmu i nacjonalizmu w Finlandii, podkreślając, że kraj ten pragnie przesunąć granicę na wschód.

W poście batalionu na Telegramie z 18 lutego 2023 r. napisano, że Karelski Ruch Narodowy ogłosił zbiórkę pieniędzy na rzecz batalionu. Stwierdzono, że „żołnierze czekają na wysłanie na front", a także sprecyzowano, że „ładunek jest opóźniony i wszyscy przebywają obecnie za granicą w trudnej sytuacji finansowej". Jednostka twierdzi też, że jej bojownicy „stają się ludźmi tworzącymi nową armię karelską". Batalion jest oskarżany o powiązania z ukraińskim batalionem Azow.

„Karelia będzie wolna" – powtarza kanał Telegramu noszący nazwę Wielka Finlandia. Nie jest to jednak grupa Finów, przesłanie o wolności Karelii szerzą aktywiści mieszkający w Rosji i propagujący separatyzm mniejszości ugrofińskiej. Od 2023 r. idea niepodległości była w Rosji komunikowana aktywniej niż wcześniej. Myśl o separatyzmie karelskim wywodzącą się z dzisiejszej Rosji najłatwiej odnaleźć w mediach społecznościowych, gdzie aktywiści utworzyli kanały na większości platform. W 2023 r. w Telegramie pojawiły się m.in. kanały dla żołnierzy Wielkiej Finlandii, Karelskiego Ruchu Narodowego i Karelskiego Batalionu Narodowego.

W grupach poruszane są różnorodne tematy związane z niepodległą Karelią i kulturą ugrofińską; poza tym w niektórych miejscach są też materiały o różnych wydarzeniach, a także o wojnie w Ukrainie. Z kilku przesłań wynika, że imperialistyczna Rosja ponownie świadomie próbuje zmiażdżyć już zniewolone dziedzictwo kulturowe i tożsamość ugrofińską,

przez co wypływa także sympatia do Ukrainy. Historia to jeden z tematów często omawianych w grupach, w związku z czym ważny wątek stanowi powstanie w Karelii zimą i wiosną 1921–1922. Powszechnie wykorzystywane są również obrazy z II wojny światowej z Karelii.

Żołnierze Wielkiej Finlandii mają swoją stronę internetową, na której prezentowane są działania i pomysły przyszłych działań. Celem ruchu jest przede wszystkim przebudzenie narodów ugrofińskich i wyzwolenie spod panowania rosyjskiego. W praktyce oznaczałoby to narodziny kilku mniejszych państw, które miałyby głęboko współpracować także z Finlandią. Ruch nie oddziela Karelii, położonej po stronie fińskiej, od Finlandii.

Nabór do batalionu jest promowany m.in. za pośrednictwem mediów społecznościowych, ale członkowie ruchów przyklejają również naklejki sprzeciwiające się rosyjskim rządom w miejscach publicznych w kilku miastach Rosji, takich jak Sortawała i Biełomorsk. Latem 2023 r. sekretarz Rady Bezpieczeństwa FR Patruszew oskarżył Finlandię i Zachód o podsycanie separatystycznego myślenia i niestabilności w regionie Karelii. Niestety nie widać szerszego ruchu politycznego, który stworzyłby niepodległą Karelię: w Rosji więcej centralnych ruchów separatystycznych powstało np. na Syberii, w Czeczenii, Dagestanie i Tatarstanie. Karelia nie ma podobnego komponentu etnicznego, ponieważ jest jednym z najbiedniejszych regionów Rosji.

7 lutego 2023 r. ukraińskie media, powołując się na separatystyczny Karelski Ruch Narodowy, ogłosiły utworzenie batalionu karelskich separatystów stojących – nowa formacja otrzymała nazwę Karelski Legion Narodowy, a jej przywódcą został Dmitrij Kuzniecow, mieszkający w Hiszpanii sygnatariusz deklaracji Forum Narodów Rosji Forum Wolnych Narodów Post-Rosji w Brukseli, gdzie promowano idee całkowitego porzucenia broni jądrowej i rozpadu Federacji Rosyjskiej.

Początkowy emblemat jednostki przyjęto 19 stycznia 2023 r. i został on zaprezentowany za pośrednictwem kanału na Telegramie – zawierał okrągłą jodełkę ze statkiem wikingów pośrodku, na którego sztandarze widniał symbol wilczego haka (*Wolfsangel*), bardzo podobny do tego użytego w symbolach brygady Azow, natomiast reszta naszywki zawierała inne nordyckie wzory i insygnia, a także napis „Karjala" w górnej części.

W październiku 2023 r. jednostka zmieniła swoje symbole: obecne nawiązują do Akademickiego Towarzystwa Kareliii10 i przedstawiają ramię z pancerzem i tarczą. Insygnia zachowują napis „Karjala", kolorystykę i Wolfsangeli11.

Godło zostało zaprojektowane w charakterystycznych kolorach Karelii. Po ogłoszeniu powstania jednostki w ukraińskich mediach zaczęło pojawiać się kilka odmian insygniów. Obejmowało to program Promuj Ukrainę; ta wersja miała uproszczony projekt – zachowano kolorystykę i napis „Karjala", ale pominięto statek wikingów oraz inne nordyckie emblematy, a u dołu cyrylicą dodano skrót nazwy batalionu wraz z przydomkiem jednostki: „Vaseli Levonen". Istniał również nieoficjalny wariant w okrągłej formie, z nazwą batalionu w języku fińskim u góry i rosyjskim – u dołu.

Według rosyjskiej gazety internetowej „The Moscow Times"12 Karelski Batalion Narodowy w 2022 i na początku 2023 r. działał głównie na wygnaniu, na terenie sąsiedniej Finlandii, wskutek ucieczki członków Karelskiego Ruchu Narodowego z Rosji. W początkowej fazie inwazji na Ukrainę rdzenni działacze rosyjscy spotykali się z rosnącą presją ze strony Kremla, gdyż wszystkich podejrzewano o nastroje antyrządowe i utrzymywanie powiązań ze zdelegalizowanymi ruchami niepodległościowymi. Niektórzy od czasu do czasu wracali do domu, do Karelii, co często powodowało starcia z lokalnymi agentami rosyjskiej Federalnej Służby

---

[10] Akademickie Towarzystwo Karelii (Akateeminen Karjala-Seura, AKS) było fińską organizacją nacjonalistyczną i ugrofińską mającą na celu rozwój i poprawę stanu niepodległej Finlandii, założoną przez naukowców i studentów Uniwersytetu Fińskiego w 1922 r. Jej członkowie zachowali wpływowe stanowiska w życiu akademickim epoki, a także w korpusie oficerskim armii. AKS kontrolował związek studencki Uniwersytetu Helsińskiego od połowy lat 20. aż do 1944 r., kiedy to Towarzystwo zostało rozwiązane w następstwie wojny kontynuacyjnej. Dążyła do aneksji wschodniej Karelii i utworzenia Wielkiej Finlandii.

[11] Wolfsangel – niemiecki symbol heraldyczny, używany także przez narodowych socjalistów, a obecnie neonazistów; w pozycji wertykalnej znany także jako piorun, a w horyzontalnej – „wilkołak".

[12] W 2022 r. siedziba „The Moscow Times" została przeniesiona do Amsterdamu, w Holandii w odpowiedzi na restrykcyjne przepisy medialne uchwalone w Rosji po inwazji na Ukrainę. 15 kwietnia 2022 r. w Rosji zablokowano rosyjskojęzyczną stronę czasopisma, a w 2023 r. Ministerstwo Sprawiedliwości Rosji uznało redakcję za „zagranicznego agenta".

Bezpieczeństwa, którzy regularnie aresztowali i oskarżali ich o rzekomy „nacjonalizm etniczny" oraz „podżeganie do zdrady stanu".

Fiński tabloid „Iltalehti" zauważył, że angażowanie się w karelski aktywizm i nacjonalizm może wiązać się z poważnymi konsekwencjami prawnymi dla zaangażowanych osób, m.in. karą 10 lat więzienia za zwykłe poniżenie rosyjskich sił zbrojnych oraz jej przedłużeniem. Oprócz tego może dojść do zwiększenia poparcia dla Ukrainy i zaangażowania w działania postrzegane jako utrudniające „funkcjonowanie Rosji", co może skutkować karą do 20 lat więzienia.

Karelski Ruch Narodowy odegrał kluczową rolę w zbieraniu funduszy dla batalionu; pojawiło się także kilka twierdzeń dotyczących wspierania go przez Denysa Prokopenkę, ówczesnego dowódcę Brygady Szturmowej Azow (ukraińskiej jednostki paramilitarnej, która była powszechnie oskarżana o neonazizm). Jednostka została także sfotografowana w Kijowie, gdy trzymała starszą odmianę flagi należącej do batalionu Azow. Obecnie Karelski Batalion Narodowy najprawdopodobniej wcielony jest w struktury Rosyjskiego Korpusu Ochotniczego, podobnie jak polski i niemiecki.

W grudniu 2023 r. ogłoszono także utworzenie plutonu Inger. Dowódca Anton Mulkahainen zaprosił wszystkich, którzy popierają wyzwolenie narodów spod jarzma „neobolszewizmu", do batalionu o nazwie Tarcza, którego herb nawiązywał do Republiki Ingrii funkcjonującej w latach 1919–1920 na Przesmyku Karelijskim, po rosyjskiej stronie granicy, posiadającej własne siły zbrojne w postaci pułku Pohjois Inkeri.

Karelski Batalion Narodowy uczestniczył w wielu operacjach bojowych; wraz z Rosyjskim Korpusem Ochotniczym dokonywał najazdów na obwód kurski i Biełgorod, zaś 9 listopada 2023 r. brał udział w zabójstwie podpułkownika Federalnej Służby Bezpieczeństwa w obwodzie briańskim, o czym poinformował pod koniec stycznia 2024 r. w Telegramie. Z kolei 18 stycznia 2024 r. Rosyjski Korpus Ochotniczy przeprowadził akcję na terenie obwodu briańskiego, niszcząc rosyjską ciężarówkę wojskową Ural przewożącą personel, a informację tę potwierdziło źródło w Głównym Zarządzie Służby Wywiadowczej Ukrainy. W nalocie uczestniczyli także ochotnicy z tej jednostki.

Przedstawiciel Ministerstwa Obrony Ukrainy Andrij Jusow podkreślił, że legion Wolność Rosji, RDK i Batalion Syberyjski działają na

terytorium Rosji jako niezależne jednostki, gdyż składają się z obywateli rosyjskich. „W końcu są w domu. Prawdopodobnie obecnie istnieje wspólne działanie tych jednostek na terytorium tzw. Rosji" – skomentował przedstawiciel GUR.

Zwycięstwo Ukrainy w wojnie z Rosją będzie ważnym krokiem na drodze do wyzwolenia Karelii spod okupacji. Batalion zamierza uczestniczyć w procesie odbudowy i rozwoju niepodległej Karelii, przyczyniając się do jej odbudowy i rozwoju we wszystkich sferach. Na drodze do osiągnięcia swoich celów staje jednak przed szeregiem wyzwań i trudności, do których należą w szczególności brak broni i środków finansowych, a także konieczność zapewnienia bojownikom odpowiedniego przeszkolenia i opieki medycznej.

Karelski Batalion Narodowy to wyjątkowe zjawisko w historii narodu karelskiego. Stał się symbolem walki o wolność i niepodległość, a jego bojownicy to bohaterowie, którzy swoimi czynami przybliżają dzień, w którym Karelia znów będzie wolna.

Olga Wasiuta

T. Ball, *Azov Battalion drops neo-Nazi symbol exploited by Russian propagandists*, 30.05.2022, https://www.thetimes.co.uk/article/azov-battalion-drops-neo-nazi-symbol-exploited-by-russian-propagandists-lpjnsp7qg (dostęp 17.06.2025); *Karjalan Kansallinen Pataljoona – Карельский Национальный Батальон*, https://suur-suomensotilaat.com/karjalan-kansallinen-pataljoona (dostęp 16.06.2025); *Karelian nationalists created a battalion as part of the Armed Forces of Ukraine*, 29.12.2023, https://abn.org.ua/en/liberation-movements/ karelian-nationalists-created-a-battalion-as-part-of-the-armed-forces-of-ukraine/ (dostęp 17.06.2025); D. Kuznetsov, *Karelian separatist from Spain*, https://newins.ru/en/articles/ west/dmitry_kuznetsov-_karelian_separatist_from_spain (dostęp 24.05.2025); L. Latypova, *Northern Flight: The Teenage Komi-Karelian Activist Who Escaped the FSB*, 14.12.2023, https://www.themoscowtimes.com/2023/11/15/northern-flight-the-teenage-komi-karelian-activist-who-escaped-the-fsb-a83040 (dostęp 17.06.2025); L. Ragutska, *Fighters of the Russian Volunteer Corps organized an ambush on a Russian military transport in the Bryansk region, causing losses among enemy forces. Photo*, 19.01.2024, https://eng.obozrevatel.com/section-war/news-fighters-of-the-russian-volunteer-corps-set-up-an-ambush-on-the-transport-of-russian-military-in-the-bryansk-region-resulting-in-casualties-among-the-enemy-forces-photo-19-01-2024.

html (dostęp 18.06.2025); *Stop the occupation of Karelia*, https://t.me/karjala474 (dostęp 24.05.2024); O. Wasiuta, *Rosyjska opozycja zbrojna wobec reżimu Putina (2022–2024)*, Wydawnictwo Naukowe UKEN, Kraków 2024; С. Закревська, *Карельські націоналісти створили батальйон у складі ЗСУ і пообіцяли боротися за звільнення краю від російської окупації*, 21.01.2023, https://news.obozrevatel.com/ukr/russia/karelski-natsionalisti-stvorili-bataljon-u-skladi-zsu-i-poobitsyali-borotisya-za-zvilnennya-krayu-vid-rosijskoi-okupatsii.htm (dostęp 24.05.2025); *Карельський Національний Батальйон*, https://reporter.zp.ua/karelskij-nacionalnij-bataljon-l-uk.html#google_vignette (dostęp 24.05.2025); Б. Марусяк, *У складі Збройних сил України створено окремий Карельський національний батальйон*, 31.01.2023, https://www.promoteukraine.org/uk/u-skladi-zbrojnyh-syl-ukrayiny-stvoreno-okremyj-karelskyj-naczionalnyj-bataljon/ (dostęp 24.05.2025); А. Степанов, *Пропагандистский батальон «Карелия» или «Союз меча и орала»*, 23.01.2023, https://mustoi.ru/ propagandistskij-batalon-kareliya-ili-soyuz-mecha-i-orala/ (dostęp 26.05.2025); О. Черкасець, *Карельський Національний Батальйон у складі ЗСУ створили активісти*, 21.01.2023, https://umoloda.kyiv.ua/number/0/188/172585 (dostęp 24.05.2025); В. Ялагин, «*Нужны не земли, а люди». Может ли Карелия отделиться от России?*, 29.01.2023, https://www.severreal.org/a/mozhet-li-kareliya-otdelitsya-ot-rossii-/32235862.html (dostęp 24.05.2025).

KATASTROFA NUKLEARNA (ang. *nuclear disaster*) – rodzaj katastrofy technologicznej charakteryzującej się niskim prawdopodobieństwem wystąpienia, ale bardzo wysokim ryzykiem i skutkami o dużej skali. Polega na niekontrolowanym uwolnieniu promieniowania jonizującego lub materiałów radioaktywnych do środowiska. Może mieć charakter lokalny, krajowy, a nawet międzynarodowy. Zdarzenie tego typu może być spowodowane zarówno awarią techniczną, błędem ludzkim, jak i celowym działaniem zbrojnym. Katastrofy nuklearne prowadzą do skażenia środowiska, strat ludzkich oraz zaburzeń społecznych i gospodarczych.

Klasyfikację katastrof nuklearnych można przeprowadzić według różnych kryteriów, takich jak przyczyna, zasięg, stopień nasilenia czy miejsce wystąpienia.

Wyróżnia się trzy główne typy zdarzeń radiacyjnych:

1. Wypadki radiacyjne – w tym przypadku przyczyny nie są celowe. Najczęściej dochodzi do nich poprzez awarie sprzętów czy systemów.

2. Incydenty radiacyjne – przyczyny mogą obejmować działania celowe, jednak zazwyczaj nie są związane z przemocą. Mogą być spowodowane błędną oceną sytuacji, nieprawidłowymi informacjami w połączniu z awariami bądź innymi sytuacjami awaryjnymi.
3. Terroryzm jądrowy – forma przemocy politycznej, której celem jest wywołanie terroru i strachu psychicznego poprzez wyrządzenie szkód celom niebędącym stroną konfliktu zbrojnego. Możliwe są poważne zamierzone szkody ekonomiczne i społeczne. Mogą, ale nie muszą wystąpić obrażenia osób spowodowane promieniowaniem.

Ze względu na źródło zdarzenia wyróżnia się katastrofy o charakterze:

1. Cywilnym – awarie elektrowni jądrowych i reaktorów badawczych.
2. Wojskowym – incydenty związane z testami, składowaniem lub transportem broni jądrowej.
3. Przemysłowym – niewłaściwe obchodzenie się z materiałami promieniotwórczymi w zakładach produkcyjnych.
4. Medycznym – nieprawidłowe wykorzystanie źródeł promieniowania w placówkach ochrony zdrowia.

Katastrofy nuklearne można również klasyfikować pod względem zasięgu i skali:

1. Lokalne – ograniczone do obszaru zakładu bądź miasta.
2. Regionalne – oddziałujące na środowisko i ludność sąsiednich regionów.
3. Międzynarodowe – oddziałujące na wiele państw, wpływające na zdrowie publiczne, środowisko i politykę międzynarodową.

Do oceny stopnia powagi takich zdarzeń stosuje się międzynarodową skalę International Nuclear and Radiological Event Scale (INES), posiadającą 7 poziomów, opracowaną przez Międzynarodową Agencję Energii Atomowej (IAEA). Skala umożliwia klasyfikację zdarzeń jądrowych i radiacyjnych. Kolejne stopnie oznaczają:

0 – odchylenie (*deviation*) – sytuacja awaryjna, ale bez konsekwencji dla środowiska.

1 – anomalia (*anomaly*) – awaria mająca wpływ na środowisko, ale w stopniu akceptowalnym i możliwym do absorbcji naturalnej.

2 – incydent (*incident*)– sytuacja, w której dochodzi do ograniczonego skażenia mogącego mieć wpływ na zdrowie ludzkie, ale w ograniczonej skali.

3 – poważny incydent (*serious incident*) – narażenie na dziesięciokrotnie wyższą dawkę dopuszczalnego promieniowania rocznego na ograniczoną liczbę ludzi, awaria techniczna, która wstrzymuje działanie urządzeń, powstrzymując ewentualność poważnej awarii.

4 – wypadek z lokalnymi konsekwencjami (*accident with local consequences*) – sytuacja, w której dochodzi do napromieniowania, ale wymaga to działań ochronnych tylko w skali lokalnej, mogło dojść do śmierci ludzi.

5 – wypadek z szerszymi konsekwencjami (*accident with wider consequences*) – ograniczone uwolnienie materiałów radioaktywnych, możliwe pojedyncze zgony z powodu napromieniowania.

6 – poważna awaria (*serious accident*) – znaczne uwolnienie materiału radioaktywnego, konieczne wdrożenie działań ratunkowych na poziomie lokalnym lub regionalnym.

7 – wielka awaria (*major accident*) – katastrofa o bardzo dużej skali, śmierć wielu osób, konieczność utworzenia strefy wykluczenia wokół miejsca zdarzenia na dłuższy czas.

Skutki katastrof nuklearnych obejmują aspekty bezpośrednie, jak i pośrednie. Pierwsze to przede wszystkim śmierć w wyniku eksplozji, oparzeń lub napromieniowania, a także występowanie choroby popromiennej. U osób narażonych na wysokie dawki promieniowania dochodzi do uszkodzeń tkanek, niewydolności organów oraz zwiększonego ryzyka nowotworów złośliwych. Zniszczeniu może ulec także infrastruktura przemysłowa, uprawy rolne oraz zabudowa mieszkalna, co bezpośrednio wpływa na poziom funkcjonowania gospodarki. Drugie natomiast dotyczą długofalowego oddziaływania promieniowania. Najczęściej obejmują zwiększoną zachorowalność na raka tarczycy, nowotwory hematologiczne i zaburzenia genetyczne. Ponadto promieniowanie powoduje skażenie gleby, wody i łańcucha pokarmowego, co doprowadza do zatrucia żywności oraz utraty przydatności terenów rolniczych. Długotrwała obecność radionuklidów powoduje ich bioakumulację w ekosystemach i trwałe zakłócenie równowagi biologicznej.

Od 1957 r. odnotowano 10 znaczących zdarzeń nuklearnych:

- Windscale, Wielka Brytania – październik 1957;
- Ural, ZSRR – październik 1958;
- Three Mile Island, USA – marzec 1979;
- Czarnobyl, Ukraina – kwiecień 1986;
- Tokaimura, Japonia – marzec 1997;
- Tokaimura, Japonia – wrzesień 1999;
- Blayais, Francja – grudzień 1999;
- Mihama, Japonia – sierpień 2004;
- Kashiwazaki, Japonia – lipiec 2007;
- Fukushima, Japonia – marzec 2011.

Spośród nich aż 5 zgłosił jeden kraj, czyli Japonia; zaś 3 z wymienionych katastrof miały szczególnie poważne konsekwencje społeczne i środowiskowe (*major accident*): były to Three Mile Island (1979), Czarnobyl (1986) i Fukushima (2011).

Najpoważniejszą katastrofą nuklearną w historii była awaria w elektrowni jądrowej w Czarnobylu, która miała miejsce 26 kwietnia 1986 r. w ZSRR, na obecnym terytorium Ukrainy. Podczas przeprowadzania testu bezpieczeństwa doszło do eksplozji w reaktorze numer 4 oraz pożaru grafitu, co doprowadziło do nagłego wzrostu mocy i masowego uwolnienia ponad 100 radioaktywnych izotopów, w tym jodu-131, cezu-137 i strontu-90.

Skażenie objęło około 150 tys. km2 obszaru Białorusi, Rosji i Ukrainy, a radioaktywna chmura przemieściła się do wielu krajów Europy. Z terenów najbardziej zanieczyszczonych ewakuowano około 116 tys. mieszkańców, a w kolejnych latach przesiedlono ponad 330 tys. osób. Najwyższe dawki promieniowania otrzymali pracownicy elektrowni i likwidatorzy, których liczbę szacuje się na około 600 tys. Bezpośrednimi ofiarami było 56 osób, jednak długoterminowe prognozy wskazują na możliwość kilku tysięcy zgonów z powodu chorób nowotworowych. Skutki zdrowotne obejmują głównie wzrost zachorowań na raka tarczycy u dzieci narażonych na skażoną żywność, szczególnie mleko. Katastrofa spowodowała także długotrwałe konsekwencje społeczne i ekonomiczne; obszar wokół elektrowni uległ depopulacji, a wiele społeczności zostało rozproszonych na stałe. Przez kolejne dekady w społeczeństwie utrzymywało się poczucie niepewności i lęku, ponadto spadło zaufanie do instytucji państwowych

i systemu bezpieczeństwa. W wyniku tego zdarzenia utworzono także tak zwaną strefę wykluczenia, która do dziś pozostaje niezamieszkana z powodu długotrwałego skażenia środowiska i kumulacji radionuklidów w ekosystemie. Sama katastrofa stała się ważnym punktem odniesienia w debacie na temat bezpieczeństwa energetyki jądrowej – doprowadziła do zmian w normach bezpieczeństwa, sposobach projektowania elektrowni i międzynarodowych procedurach zarządzania kryzysowego.

Kolejne dekady pokazały, że ryzyko wystąpienia podobnych awarii nie zostało całkowicie wyeliminowane; za zdarzenie o zbliżonej skali można uznać katastrofę w elektrowni Fukushima Daiichi, w Japonii w 2011 r. Doszło do niej poprzez silne trzęsienie ziemi o magnitudzie 9,0 oraz powstałe w jego wyniku tsunami. Fala o wysokości 14 m doprowadziła do utraty zasilania, uszkodzenia systemów chłodzenia i stopnienia rdzeni 3 reaktorów. Następnie doszło do eksplozji wodoru i uwolnienia radionuklidów, takich jak cez-137 i jod-131, do atmosfery i wód morskich. Z obszaru w promieniu 20 km ewakuowano ponad 100 tys. osób. Znaczna część terenu pozostała niedostępna dla mieszkańców przez wiele lat z powodu utrzymującego się skażenia. Najwyższe dawki promieniowania, podobnie jak w przypadku Czarnobyla, otrzymali pracownicy elektrowni oraz ratownicy uczestniczący w stabilizacji terenu katastrofy przez pierwsze miesiące po awarii. Według dostępnych raportów i analiz skutki zdrowotne promieniowania dla populacji były ograniczone, jednak katastrofa wywołała konsekwencje pod względem psychospołecznym: ludność zmagała się z długotrwałym stresem, problemami zdrowia psychicznego, utratą źródła utrzymania czy spadkiem zaufania społecznego. Podobnie jak po awarii z 1986 r., to zdarzenie doprowadziło do zaostrzenia standardów bezpieczeństwa w wielu państwach.

Zagrożenia związane z energetyką jądrową były obecne już wcześniej, czego przykładem jest katastrofa w Three Mile Island, która miała miejsce 28 marca 1979 r. w Stanach Zjednoczonych. Awaria rozpoczęła się od zatrzymania pomp wody zasilającej oraz automatycznego wyłączenia turbiny i reaktora. Kluczowy moment nastąpił, gdy doszło do zacięcia się zaworu bezpieczeństwa, który pozostał otwarty, mimo że operatorzy, na podstawie błędnych wskazań, uznali go za zamknięty. Spowodowało to utratę chłodziwa i stopniowego odsłonięcia prętów paliwowych. Operatorzy, kierując

się błędnymi odczytami, podjęli decyzje, które pogłębiły problem – doszło do częściowego stopienia rdzenia, a w obiegu reaktora powstał wodór, co zwiększyło obawy przed możliwością eksplozji w obudowie bezpieczeństwa. W tym przypadku struktura ochronna elektrowni spełniła swoje zadanie i zatrzymała uwolnienie materiałów radioaktywnych do środowiska, do którego doszło jedynie w ograniczonym stopniu. Według analiz poziom narażenia ludności na promieniowanie był minimalny i nie stwierdzono bezpośrednich ofiar śmiertelnych. Mimo stosunkowo niewielkich skutków wydarzenie miało znaczący wpływ polityczny i społeczny; w Stanach Zjednoczonych nastąpił gwałtowny spadek zaufania do energetyki jądrowej i rozpoczęto reformy standardów bezpieczeństwa.

Ze względu na transgraniczny charakter skutków katastrof nuklearnych priorytetem systemu bezpieczeństwa jest szeroka współpraca międzynarodowa; kluczową rolę odgrywa Międzynarodowa Agencja Energii Atomowej (IAEA) założona w 1957 r. jako część systemu Organizacji Narodów Zjednoczonych. Prowadzi ona komisje kontrolne, opracowuje standardy bezpieczeństwa i koordynuje wymianę informacji w sytuacjach kryzysowych. W podstawie Konwencji o wczesnym powiadamianiu oraz Konwencji o pomocy w razie awarii radiologicznej agencja utrzymuje system szybkiej komunikacji i wsparcia operacyjnego poprzez sieć RANET i ENATOM.

RANET (Response and Assistance Network) to międzynarodowa sieć operacyjna, która umożliwia szybkie udostępnianie zasobów technicznych, ekspertów i sprzętu państwom, w których doszło do wypadku nuklearnego. Obejmuje m.in. wsparcie medyczne, specjalistów czy zespoły pomiarowe.

ENATOM (Emergency Notification and Assistance Technical Operations Manual) to podręcznik operacyjny IAEA, który określa procedury wymiany danych, komunikacji kryzysowej i koordynacji działań w przypadku wystąpienia zdarzeń nuklearnych. Dokument określa sposób przekazywania informacji między państwami oraz formy udzielania pomocy.

W przypadku katastrof nuklearnych równie istotna jest Światowa Organizacja Zdrowia (WHO), która odpowiada za przygotowanie wytycznych medycznych, ocenę zagrożeń zdrowotnych i wsparcie państw w obrębie ochrony radiologicznej. Istnieje również Program Narodów

Zjednoczonych ds. Środowiska (UNEP), który współtworzy wraz z innymi agendami ONZ normy bezpieczeństwa środowiskowego i uczestniczy w monitoringu skażeń. Ponadto wspiera on proces oczyszczania terenów skażonych. Istotne jest również Światowe Stowarzyszenie Operatorów Elektrowni Jądrowych (WANO), które zrzesza ponad 120 operatorów reaktorów komercyjnych; ich współpraca polega na wymianie dobrych praktyk i zapobieganiu błędom znanym już np. z Czarnobyla czy Fukushimy. Nad przyjmowaniem tych samych standardów ochrony radiologicznej w państwach członkowskich Unii Europejskiej kontrolę pełni Europejska Wspólnota Energii Atomowej (EURATOM) – współpracuje ona z organizacjami międzynarodowymi w celu pokojowego wykorzystania energii jądrowej.

W Polsce system ochrony radiologicznej bazuje przede wszystkim na Ustawie z dnia 29 listopada 2000 r. Prawo atomowe (Dz.U. 2001, nr 3, poz. 18), która określa zasady bezpiecznego stosowania energii jądrowej, wymagania licencyjne i obowiązki organów państwowych i instytucji prowadzących działalność związaną z promieniowaniem jonizującym. Głównym organem nadzoru jest Państwowa Agencja Atomistyki (PAA), która odpowiada za nadzór nad bezpieczeństwem jądrowym i ochroną radiacyjną w Polsce. Do jej zadań należy m.in. kontrolowanie instalacji jądrowych i źródeł promieniowania, wydawanie zezwoleń czy koordynacja działań w sytuacjach awaryjnych. W jej strukturze działa Centrum do Spraw Zdarzeń Radiacyjnych (CEZAR) odpowiedzialne za prognozy, monitoring oraz obsługiwanie systemów alarmowych. Prawo atomowe określa system planowania alarmowego na wielu szczeblach przez plany zakładowe, wojewódzkie i krajowe. Ponadto polski system bezpieczeństwa funkcjonuje zgodnie z europejskimi zasadami nadzoru nad energią jądrową, które określa Traktat EURATOM.

Katastrofy nuklearne stanowią poważny problem zarówno dla bezpieczeństwa międzynarodowego, jak i państwa. Prowadzą do długotrwałego skażenia na ogromną skalę, osłabienia infrastruktury krytycznej, strat ludzkich i destabilizacji społeczeństwa; wymuszają ewakuację ludności czy utratę obszarów przystosowanych do zamieszkania, co zaburza stabilność gospodarczą i funkcjonowanie państwa. Skutki zdrowotne czy środowiskowe mogą dotyczyć wielu państw, co wymaga współpracy

międzynarodowej i szybkiej wymiany informacji. Katastrofy takie jak Czarnobyl czy Fukushima pokazały, że zdarzenia nuklearne mogą prowadzić do zmian w polityce energetycznej, a podczas konfliktów zbrojnych stanowią dodatkowy czynnik ryzyka.

Przemysław Mazur, Martyna Czerniak

Chernobyl Forum Expert Group 'Environment', Environmental Consequences of the Chernobyl Accident and Their Remediation: Twenty Years of Experience, International Atomic Energy Agency, Vienna 2006; International Atomic Energy Agency, Convention on Nuclear Safety (INFCIRC/449), International Atomic Energy Agency, Vienna 1994; International Atomic Energy Agency, Emergency Notification and Assistance: Technical Operations Manual (EPR-ENATOM 2007), International Atomic Energy Agency, Vienna 2007; International Atomic Energy Agency, Fundamental Safety Principles, International Atomic Energy Agency, Vienna 2006; International Atomic Energy Agency, The Fukushima Daiichi Accident. Report by the Director General, International Atomic Energy Agency, Vienna 2015; International Atomic Energy Agency, World Health Organization, Chernobyl's Legacy: Health, Environmental and Socio-economic Impacts. The Chernobyl Forum 2003–2005, Second revised version, International Atomic Energy Agency, Vienna 2006; Międzynarodowa skala zdarzeń jądrowych INES, https://nuclear.pl/print.php?dzial=ochrona&plik=skala (dostęp 3.11.2025); Nuclear Energy Agency, Organization for Economic Co-operation and Development, Fukushima Daiichi Nuclear Power Plant Accident, Ten Years On: Progress, Lessons and Challenges, OECD, Paris 2021; Obwieszczenie z dnia 11 września 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Prawo atomowe, Dz.U. 2019, poz. 1792; J.M. Pedraza, *World Major Nuclear Accidents and Their Negative Impact in the Environment, Human Health and Public Opinion*, „International Journal of Environmental Engineering and Education" 2013, vol. 21, no. 2; A. Rosen, *Critical Analysis of the WHO's Health Risk Assessment of the Fukushima Nuclear Catastrophe*, German Section of the International Physicians for the Prevention of Nuclear War (IPPNW), 2013; Rozporządzenie z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych, Dz.U. 2005, nr 20, poz. 169; S.L. Simon, *Introduction to Nuclear/Radiation Accidents, Incidents and Events, Radiation Epidemiology and Dosimetry Course*, National Cancer Institute, U.S. Department of Health and Human Services, 2011; United States Nuclear Regulatory Commission, Three Mile Island Accident, Office of Public Affairs, U.S. NRC, 2014;Zarządzenie nr 7 Prezesa Państwowej Agencji Atomistyki z dnia 30 czerwca 2023 r. w sprawie regulaminu organizacyjnego Państwowej Agencji Atomistyki, Dz.Urz. PAA, poz. 1, 2023.

KOMITET BEZPIECZEŃSTWA MORSKIEGO (ang. IMO Maritime Safety Committee) – kluczowy organ Międzynarodowej Organizacji Morskiej (International Maritime Organization, IMO), który zajmuje się wszystkimi kwestiami dotyczącymi bezpieczeństwa żeglugi i ochrony środowiska morskiego, od przepisów dla statków pasażerskich po regulacje dla statków towarowych, dbając o bezpieczeństwo życia, zdrowia i mienia na morzu.

Kluczowe zadania i obszary działalności:

- ustanawianie przepisów: tworzenie międzynarodowych konwencji i kodeksów dotyczących bezpieczeństwa, np. SOLAS (Safety of Life at Sea);
- ochrona przeciwpożarowa: opracowywanie standardów i środków zapobiegających pożarom na statkach;
- bezpieczeństwo nawigacji: regulacje dotyczące systemów nawigacyjnych i zapobiegania kolizjom;
- bezpieczeństwo ładunków: normy dla bezpiecznego przewozu różnych rodzajów ładunków;
- bezpieczeństwo pasażerów: przepisy dotyczące statków pasażerskich, w tym ewakuacji i wyposażenia;
- ochrona środowiska: wpływ działalności morskiej na środowisko.

Zadaniem Komitetu Bezpieczeństwa Morskiego jest „rozpatrywanie wszelkich spraw wchodzących w zakres kompetencji organizacji dotyczących pomocy nawigacyjnych, budowy i wyposażenia statków, obsady załogi z punktu widzenia bezpieczeństwa, zasad zapobiegania kolizjom, obsługi ładunków niebezpiecznych, procedur i wymogów bezpieczeństwa morskiego, informacji hydrograficznych, dzienników pokładowych i rejestrów nawigacyjnych, dochodzeń w sprawie wypadków morskich, ratownictwa i wszelkich innych spraw mających bezpośredni wpływ na bezpieczeństwo morskie".

Komitet ma również obowiązek zapewnić mechanizmy umożliwiające wykonywanie wszelkich zadań powierzonych mu na mocy konwencji IMO lub wszelkich zadań wchodzących w zakres jego działalności, które mogą zostać mu powierzone na mocy lub w ramach jakiegokolwiek instrumentu międzynarodowego i przyjęte przez organizację. Komitet jest odpowiedzialny za rozpatrywanie i przedkładanie zaleceń

i wytycznych dotyczących bezpieczeństwa, które mogą zostać przyjęte przez zgromadzenie.

Rozszerzona MSC przyjmuje poprawki do konwencji, takich jak SOLAS (International Convention for Safety of Life at Sea), i obejmuje wszystkie państwa członkowskie, a także kraje będące stronami konwencji takich jak SOLAS, nawet jeśli nie są one państwami członkowskimi IMO.

Od zawsze uznawano, że najlepszym sposobem poprawy bezpieczeństwa na morzu jest opracowanie międzynarodowych przepisów, które będą przestrzegane przez wszystkie kraje żeglugowe, i od połowy XIX w. przyjęto wiele takich traktatów. Kilka krajów zaproponowało utworzenie stałego organu międzynarodowego, który skuteczniej promowałby bezpieczeństwo morskie, ale dopiero wraz z utworzeniem Organizacji Narodów Zjednoczonych nadzieje te się spełniły. W 1948 r., podczas międzynarodowej konferencji w Genewie przyjęto konwencję formalnie ustanawiającą IMO (pierwotna nazwa brzmiała Międzyrządowa Organizacja Konsultacyjna ds. Morskich, czyli IMCO (Inter-Governmental Maritime Consultative Organization), ale w 1982 r. nazwę zmieniono na IMO). Konwencja IMO weszła w życie w 1958 r., a nowa organizacja zebrała się po raz pierwszy w kolejnym roku.

Powstanie Międzynarodowej Organizacji Morskiej (International Maritime Organization) ma interesującą genezę prowadzącą do najsłynniejszej katastrofy w historii żeglugi, a mianowicie – zatonięcia w 1912 r. transatlantyku Titanic. Do chwili tej tragedii uważano, że możliwe jest zbudowanie statku, który będzie w 100% bezpieczny i nigdy nie zatonie; niestety już pierwszy rejs Titanica boleśnie zweryfikował ten mit. Gdy ochłonięto z pierwszego szoku, okazało się, że na statku popełniono wiele karygodnych błędów, wskutek czego życie straciło ponad tysiąc osób. Aby w przyszłości uniknąć podobnych nieprawidłowości, w 1914 r. powstała pierwsza międzynarodowa konwencja będąca zbiorem przepisów dotyczących bezpieczeństwa żeglugi – SOLAS. Już w tamtym czasie uznawano konieczność powołania międzynarodowej organizacji czuwającej nad morskim prawodawstwem i egzekwującej wykonywanie tych regulacji przez statki w żegludze globalnej. Nie było to jednak możliwe do czasu powołania do życia w 1945 r. Organizacji Narodów Zjednoczonych (ONZ).

Cele organizacji, zgodnie z art. 1 lit. a konwencji, to „zapewnienie mechanizmów współpracy między rządami w zakresie regulacji i praktyk rządowych dotyczących wszelkiego rodzaju kwestii technicznych mających wpływ na żeglugę międzynarodową; zachęcanie do powszechnego stosowania najwyższych praktycznych standardów w zakresie bezpieczeństwa morskiego, efektywności żeglugi oraz zapobiegania i kontroli zanieczyszczenia morza przez statki oraz ułatwianie tego stosowania". Organizacja jest również uprawniona do zajmowania się sprawami administracyjnymi i prawnymi związanymi z tymi celami.

Pierwszym zadaniem IMO było przyjęcie nowej wersji Międzynarodowej konwencji o bezpieczeństwie życia na morzu (SOLAS), najważniejszego ze wszystkich traktatów dotyczących bezpieczeństwa morskiego. Osiągnięto to w 1960 r., a następnie IMO zwróciło uwagę na takie kwestie, jak ułatwianie międzynarodowego ruchu morskiego, linie ładunkowe i przewóz towarów niebezpiecznych, jednocześnie dokonując przeglądu systemu pomiaru tonażu statków.

Jednak mimo że bezpieczeństwo było i pozostaje najważniejszym obowiązkiem IMO, pojawił się nowy problem – zanieczyszczenie środowiska. Szczególnym powodem do niepokoju był wzrost ilości ropy transportowanej drogą morską oraz wielkości tankowców, a katastrofa Torrey Canyon w 1967 r., w wyniku której wyciekło 120 tys. t ropy, pokazała skalę tego problemu.

W ciągu następnych kilku lat IMO wprowadziła wiele środków mających na celu zapobieganie wypadkom tankowców i minimalizowanie ich skutków. Zajęła się również zagrożeniem dla środowiska spowodowanym rutynowymi czynnościami, takimi jak czyszczenie zbiorników ładunkowych ropy naftowej i usuwanie odpadów z maszynowni, które pod względem tonażu stanowią większe zagrożenie niż przypadkowe zanieczyszczenia.

Najważniejszym ze wszystkich tych środków była Międzynarodowa konwencja o zapobieganiu zanieczyszczaniu morza przez statki z 1973 r., zmieniona protokołem z 1978 r. (MARPOL 73/78), obejmująca nie tylko przypadkowe i operacyjne zanieczyszczenia ropą naftową, ale także chemikaliami, towarami w opakowaniach, ściekami, śmieciami i zanieczyszczenia powietrza.

IMO otrzymała również zadanie ustanowienia systemu zapewniającego odszkodowania osobom, które poniosły straty finansowe w wyniku zanieczyszczenia środowiska. W 1969 i 1971 r. przyjęto dwa traktaty, które umożliwiły ofiarom zanieczyszczenia ropą naftową uzyskanie odszkodowania w znacznie prostszy i szybszy sposób niż wcześniej. Oba traktaty zostały zmienione w 1992 r., a następnie ponownie w 2000 r., w celu podwyższenia limitów odszkodowań wypłacanych ofiarom zanieczyszczenia. Od tego czasu opracowano wiele innych konwencji prawnych, z których większość dotyczy kwestii odpowiedzialności i odszkodowań.

Również w latach 70. XX w. zainicjowano globalny system poszukiwawczo-ratowniczy wraz z utworzeniem Międzynarodowej Organizacji Satelitów Komórkowych (IMSO), co znacznie poprawiło przekazywanie komunikatów radiowych i innych wiadomości do statków.

W 1988 r. przyjęto globalny morski system alarmowo-ratunkowy (GMDSS), który zaczął być stopniowo wdrażany od 1992 r. W lutym 1999 r. GMDSS osiągnął pełną operacyjność, dzięki czemu obecnie statek znajdujący się w niebezpieczeństwie w dowolnym miejscu na świecie ma praktycznie zagwarantowaną pomoc, nawet jeśli załoga nie ma czasu na wezwanie pomocy przez radio, ponieważ wiadomość zostanie przekazana automatycznie.

„Misją Międzynarodowej Organizacji Morskiej (IMO) jako wyspecjalizowanej agencji ONZ jest promowanie bezpiecznego, ekologicznego, wydajnego i zrównoważonego transportu morskiego poprzez współpracę. Cel ten zostanie osiągnięty poprzez przyjęcie wysokich standardów bezpieczeństwa morskiego, wydajności żeglugi oraz zapobiegania i kontroli zanieczyszczeń ze statków, a także poprzez rozważenie powiązanych kwestii prawnych i skuteczne wdrożenie instrumentów IMO w celu ich powszechnego i jednolitego stosowania".

IMO działa w ramach następującej struktury: najważniejszym organem jest Zgromadzenie (Assembly), w skład którego wchodzą delegaci wszystkich krajów członkowskich, zbierające się co 2 lata w celu zaktualizowania wszystkich nowych przepisów morskich. Z kolei organem zarządzającym w okresie 2-letnim pomiędzy sesjami Zgromadzenia jest Rada, w skład której wchodzi 40 krajów członkowskich wybieranych wg następującego klucza: 10 państw posiadających flotę morską o największym

tonażu, 10 państw o największych obrotach w handlu morskim oraz 20 państw mających szczególne znaczenie dla żeglugi lub transportu morskiego. Opracowaniem przepisów w poszczególnych sektorach zajmują się komitety: Komitet Bezpieczeństwa Morskiego (Maritime Security Committee, MSC), Komitet Ochrony Środowiska Morskiego (Marine Environment Protection Committee, MEPC), Komitet Prawny (Legal Committee), Komitet Współpracy Technicznej (Technical Cooperation Committee) oraz Komitet ds. Ułatwień (Facilitation Committee), który koncentruje się na upraszczaniu formalności i procedur w międzynarodowym transporcie morskim, a także wiele podkomitetów. Prace IMO nadzoruje Sekretariat kierowany przez Sekretarza Generalnego (obecnie jest nim Arsenio Dominguez, który został mianowany na to stanowisko z dniem 1 stycznia 2024 r. na początkową 4-letnią kadencję) i zatrudniający około 300 osób. Siedziba główna IMO znajduje się w Londynie.

Według stanu na rok 2023 członkami IMO jest 175 państw i 3 w charakterze członków stowarzyszonych (Hongkong, Wyspy Owcze i Makau); 66 organizacji międzyrządowych posiada umowy o współpracy z IMO, zaś 88 pozarządowych ma przy niej status doradczy. Podstawowym celem IMO jest zatem opracowywanie i wdrażanie w życie w perspektywie globalnej przepisów dotyczących bezpieczeństwa żeglugi, ochrony środowiska i rozwoju morskiego handlu.

Najważniejszymi dokumentami organizacji, mającymi moc ustawy, są konwencje, a więc zbiory przepisów mających zastosowanie w żegludze międzynarodowej. Dalej są kodeksy, a więc niejako szczegółowe przepisy wykonawcze konwencji, zaś potwierdzenie zgodności działania statków z wymienionymi regulacjami stanowią certyfikaty i dokumenty. Na pokładzie każdej z jednostek pływających w światowym handlu powinno być ich około 120.

Najważniejsza historycznie jest wspomniana już konwencja SOLAS (International Convention for Safety of Life at Sea), czyli Międzynarodowa konwencja o bezpieczeństwie życia na morzu. Jej pierwsza wersja jest starsza niż IMO i pochodzi z 1914 r., zaś nowa została przyjęta przez IMO w 1960 r., a ostateczny zręb podstawowych przepisów tego dokumentu ukształtował się w 1974 r., choć w kolejnych latach był jeszcze wielokrotnie uzupełniany. To, jak wiele nowych przepisów dotyczących bezpieczeństwa

pojawiło się w ostatnim stuleciu, obrazuje fakt, iż pierwsza wersja SOLAS liczyła 120 stron, ostatnia zaś – 623.

W 1967 r. u wybrzeży Kornwalii doszło do katastrofy tankowca Torrey Canyon, w wyniku której wyciekło 120 tys. t ropy naftowej. Wydarzenie to było bezpośrednim bodźcem do stworzenia kolejnej ważnej konwencji IMO – MARPOL (International Convention for Prevention of Pollution from Ships), czyli Międzynarodowej konwencji o zapobieganiu zanieczyszczaniu morza przez statki z 1973 r. Konwencja ta obejmuje nie tylko przepisy związane z zapobieganiem katastrofom tankowców, ale również regulacje dotyczące zanieczyszczenia morza przez środki chemiczne, towary pakowane, ścieki, śmieci i zanieczyszczenia powietrza.

W kolejnych dekadach była to często stosowana praktyka: katastrofy statków, w których ginęło wiele osób lub które wyrządzały znaczące szkody środowisku (m.in. Exxon Valdez, Herald of Free Enterprise, Estonia, Prestige itd.), skutkowały natychmiastowymi działaniami IMO i opracowaniem przez tę organizację przepisów mających w przyszłości zapobiec tego rodzaju tragediom, najczęściej w formie aneksów i poprawek dołączanych do poszczególnych konwencji.

Do tej pory IMO opracowało łącznie 32 konwencje (zbiory przepisów dotyczących danej sfery działalności statku i załogi). Oprócz SOLAS i MARPOL, warto też wspomnieć o następujących konwencjach: COLREG 1972 (Convention on the International Regulations for Preventing Collisions at Sea) dotyczącej zapobiegania kolizjom statków, LL 1966 (International Convention on Load Lines) o liniach ładunkowych, regulującej ilość ładunku, jaki można załadować na dany statek, STCW 1978 (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers) o wymaganiach w zakresie wyszkolenia marynarzy, wydawania świadectw oraz pełnienia wacht, SAR 1979 (International Convention on Maritime Search and Rescue) o poszukiwaniu i ratownictwie morskim. Jedną z ostatnich konwencji IMO, której przepisy są obecnie wdrażane w życie, jest Międzynarodowa konwencja o kontroli i postępowaniu ze statkowymi wodami balastowymi i osadami (BWM 2004 – International Convention for the Control and Management of Ships' Balalst Water and Sediments).

Konwencje po przyjęciu przez IMO są wdrażane w życie, jednak zanim to nastąpi, musi dojść do ich ratyfikacji przez rządy poszczególnych krajów – członków IMO. Jeśli dany kraj ratyfikuje przepisy IMO, zobowiązany jest następnie do ich przyjęcia na oficjalnej ścieżce legislacyjnej.

Wymiernym dowodem skuteczności działań IMO jest zmniejszająca się z roku na rok ilość wypadków na morzu – w ciągu ostatniej dekady, pomimo gwałtownie rosnącej ilości statków wchodzących do komercyjnej żeglugi, zanotowano aż 50-procentowy spadek morskich wypadków.

Anna Kochnowska

International Convention for the Safety of Life at Sea (SOLAS), 1974 – Consolidated edition (IMO), International Maritime Organization, London 2009; K. Gogol, *70 lat Międzynarodowej Organizacji Morskiej (IMO)*, 4.06.2018, https://www.gospodarkamorska.pl/edukacja-praca-70-lat-miedzynarodowej-organizacji-morskiej-imo-30516 (dostęp 1.12.2025);M.S. Karim, *Prevention of Pollution of the Marine Environment from Vessels: The Potential and Limits of the International Maritime Organization*, Springer, London 2014; M.H. Koziński, *Morskie prawo publiczne*, Wydawnictwo Morskie, Gdańsk 2015; L. Łukaszuk, *Międzynarodowe prawo morza*, Scholar, Warszawa 1997; *The International Maritime Organisation*, S. Mankabady (ed.), Croom Helm (later Routledge), London 1984; *Making the Law of the Sea: A Study in the Development of International Law*, J. Harrison (ed.), Cambridge University Press, Cambridge 2011; *Regulation of International Shipping: International and Comparative Perspectives*, A. Chircop, N. Letalik, T.L. McDorman, S. Rolston (eds.), Brill, Nijhoff 2012; *System zarządzania bezpieczną eksploatacją jednostek morskich w zarysie: analiza organizacji i metodyka oceny bezpieczeństwa*, A. Mrozowska, R. Wróbel, P. Mrozowski (red.), Difin, Warszawa 2022; B. Stępień, *Prawo międzynarodowe publiczne a bezpieczeństwo żeglugi morskiej*, Wydawnictwo Helion, Gliwice 2016; S. Yubing, *Climate Change and International Shipping: The Regulatory Framework for the Reduction of Greenhouse Gas Emissions*, Brill, Nijhoff 2016.

KORWETA – kategoria małych, lekkich i szybkich okrętów wojennych, które pojawiły się we Francji pod koniec XVII w. Tradycyjnie jest to najmniejsza klasa jednostek uznawana za pełnoprawny (lub „klasyfikowany") okręt wojenny. Klasą okrętów wojennych powyżej korwety jest fregata, niższą historycznie – slup wojenny (ang. *sloop-of-war*), a współcześnie patrolowce.

Współczesne zadania korwet obejmują patrole przybrzeżne i ewentualną obronę wód terytorialnych; wypierają zazwyczaj od 500 do 2000 t, choć mogą osiągać wyporność do 3000 t i posiadać hangar na śmigłowiec, a ich rozmiar i możliwości nierzadko pokrywają się z mniejszymi fregatami. Zaprojektowana bardziej do ochrony sił morskich lub konwojów statków handlowych albo obserwacji obszaru (wojskowego lub gospodarczego) niż do celów szturmowych, korweta jest zazwyczaj przydzielana do misji przybrzeżnych, w tym do ochrony morskiej lub rozpoznania, jednak w przeciwieństwie do współczesnych fregat, nowoczesna korweta nie ma wystarczającej wytrzymałości ani zdolności żeglugowej, aby odbywać długie misje morskie. Obecnie termin ten jest używany przez różne marynarki wojenne do klasyfikacji szerokiej gamy jednostek, od większych patrolowców po mniejsze jednostki eskortowe.

W erze żagla korwety były jednym z wielu typów okrętów wojennych mniejszych od fregaty i posiadających pojedynczy pokład artyleryjski, blisko spokrewnionych ze slupami wojennymi. Do zadań korwety należały głównie patrolowanie wybrzeża, walka w mniejszych wojnach, wspieranie dużych flot lub uczestnictwo w misjach pokazu flagi. Brytyjska Royal Navy zaczęła używać te niewielkie okręty w latach 50. XVII w., ale opisywała je raczej jako slupy. Pierwsza wzmianka o korwecie pochodzi z francuskiej marynarki wojennej z lat 70. XVII w., skąd prawdopodobnie wzięło się to określenie. Korwety francuskiej marynarki wojennej rozrastały się przez dziesięciolecia i do lat 80. XVIII w. były okrętami o 20 działach lub więcej, co mniej więcej odpowiadało okrętom pocztowym brytyjskiej marynarki wojennej. Z kolei Royal Navy przyjęła ten termin dopiero w latach 30. XIX w., długo po wojnach napoleońskich, i określała nim niewielki okręt o drugorzędnym znaczeniu, nieco większy od slupa.

Wraz z pojawieniem się ery pary niektóre mniejsze okręty nazywano korwetami, a nawet korwetami pancernymi, ale ostatecznie nazwa ta u progu XX stulecia stała się historycznym określeniem w terminologii nautycznej. Sytuacja zmieniła się podczas II wojny światowej; zmagająca się z niemieckimi okrętami podwodnymi brytyjska flota pilnie potrzebowała okrętu do walki z nimi, który byłby tańszy i prostszy w konstrukcji od niszczyciela. Od okrętu tego oczekiwano także dzielności morskiej będącej w stanie sprostać wymaganiom żeglugowym w surowych realiach

północnego Atlantyku. Współczesna korweta pojawiła się podczas II wojny światowej jako łatwy w budowie okręt patrolowy i eskortowy konwojów. Brytyjski projektant okrętów William Reed opracował niewielki okręt oparty na statku wielorybniczym Southern Pride firmy Smiths Dock Company, którego prosta konstrukcja i handlowe standardy konstrukcyjne umożliwiły szybką produkcję w dużych ilościach w niewielkich stoczniach, mających jednak zdolności do produkowania małych jednostek o pełnomorskich parametrach żeglugowych. Ówczesny Pierwszy Lord Admiralicji Winston Churchill, późniejszy premier, przyczynił się do przywrócenia nazwy „korweta" jako określenia klasy niewielkich jednostek których głównym zadaniem jest zwalczanie okrętów podwodnych. Jednak pierwszy typ okrętu tej klasy dla Royal Navy – Flower – choć produkowany masowo, nie był w pełni udanym okrętem; z trudem utrzymywał się na długiej atlantyckiej fali, był stosunkowo powolny, a załoga miała spartańskie warunki życia, dlatego też wkrótce wprowadzono do służby nowy typ okrętu Castle, wypierający nieco ponad 1000 t, uzbrojony w 1 działo kalibru 102 mm, do kilku działek 20 mm oraz wyrzutnie bomb głębinowych. Prędkość nadal była niewystarczająca (XVII w.), ale okręty te miały większą dzielność morską, choć ich zdolności manewrowe przy mniejszej prędkości nadal pozostawiały sporo do życzenia. W państwach osi udany typ okrętu tej klasy zbudowały Włochy. Królewska Marynarka (Regia Marina), która pilnie potrzebowała jednostek eskortowych dla swoich konwojów, zaprojektowała korwety typu Gabbiano, których w latach 1942–1943 zbudowano 29 (spośród 60 planowanych). Okręty te sprawdziły się w operacjach na Morzu Śródziemnym, szczególnie pod względem zdolności do zwalczania samolotów i okrętów podwodnych. Odniosły tak duży sukces, że klasa ta przetrwała po wojnie we włoskiej marynarce wojennej do 1972 r. Wielkością i uzbrojeniem zbliżone były do brytyjskiego typu Flower, miały jednak nieco większą prędkość (XVIII w.) i lepszą dzielność morską. Do lat 70. minionego stulecia korwety jako osobna klasa okrętu były w zasadzie w zaniku.

Lata 50. i 60. XX w. to epoka, w której stawiano na miniaturyzację okrętów, szczególnie w mniejszych flotach krajów niemających dostępu do otwartych mórz (Bałtyk, Morze Czarne i Śródziemne). Pojawiły się na tych akwenach okręty niewielkie, ale o dużym potencjale bojowym ze względu

na uzbrojenie rakietowe (np. radzieckie małe okręty rakietowe typu Osa, będące także na wyposażeniu flot Układu Warszawskiego), jednak zdolności bojowe tych jednostek ograniczała ich stosunkowo niewielka dzielność morska, jak i mały promień działania, wreszcie bardzo słabe uzbrojenie przeciwlotnicze. Jak się wydaje – przełomowym momentem w rozwoju współczesnych korwet było pojawienie się niemieckich okrętów określanych jako tzw. typ MEKO (skrót od niemieckiego terminu Mehrzweck Kampfschiff – uniwersalny okręt bojowy, lub Mehrzweck Kombination – kombinacja uniwersalna) opracowanych w grupie zbrojeniowej Thyssen-Krupp Marine Systems. Istota tych niewielkich początkowo jednostek (o wyporności do około 3000 t) polegała na tym, że mogły one zmieniać szybko moduły uzbrojenia (przeciwpodwodnego, przeciwlotniczego czy przeciw okrętom nawodnym), w zależności od potrzeb, stając się idealnym projektem dla niewielkich flot o dość ograniczonych możliwościach budżetowych. W ramach tego projektu powstały niemieckie korwety typu Baunschweig oraz izraelskie Sa'ar 6.

Polska tzw. korweta patrolowa Ślązak to jedyny okręt zbudowany według projektu MEKO A-100, który miał liczyć pierwotnie 6 jednostek. Warto zaznaczyć, że zarówno typ Braunschweig, Sa'ar 6, jak i Ślązak to jednostki typu oceanicznego, podobnie jak ORP Kaszub, jedyny okręt z serii, która miała powstać w liczbie 4. Warto w tym miejscu wspomnieć, że okręt ten był pierwszą jednostką bojową wybudowaną w polskiej stoczni mającą oceaniczny charakter. Współcześnie korwety są kośćcem małych flot i najprawdopodobniej najbardziej rozpowszechnioną klasą wśród okrętów wojennych. Wyparły one niemal całkowicie klasę ścigaczy zarówno torpedowych, rakietowych, jak i tych, których zadaniem podstawowym było zwalczanie okrętów podwodnych. Wyporność współczesnych korwet waha się od 500 do 2000 t, choć może wynosić znacznie więcej, np. ponad 4000 t, co dotyczy okrętów typu Pohjanmaa budowanych dla sił morskich Finlandii.

Przykładem niewielkich korwet były sowieckie okręty typu Tarantul I o wyporności 455 t: 4 spośród nich (OORP Górnik, Hutnik, Metalowiec i Rolnik) służyły w polskiej flocie. Nieco na siłę do klasy korwet zalicza się 3 okręty rakietowe typu Saβnitz, które w liczbie 3 jednostek pełnią służbę po dziś dzień w Marynarce Wojennej RP. Warto wspomnieć, że

oficjalnie są one określane przez Rosjan jako małe okręty rakietowe, natomiast gdy mowa o najnowszych okrętach rosyjskich, do korwet zalicza się niewątpliwie okręt typu Bujan-M o wyporności około 1000 t. Jednostki te wyposażone są w 8 wyrzutni rakiet typu Kalibr, które można wyposażyć w głowice nuklearne, a ich zasięg wynosi prawie 2500 km. Niestety okręty te, podobnie jak wszystkie mniejsze jednostki floty rosyjskiej, mają bardzo słabe uzbrojenie przeciwlotnicze; mogą operować wyłącznie w strefie operacyjnej własnego lotnictwa bądź w zasięgu lądowej obrony przeciwlotniczej.

Przebieg działań na Morzu Czarnym w wojnie rosyjsko-ukraińskiej w pełni to potwierdził. Ta sama słabość charakteryzuje szwedzkie korwety typu Visby (łącznie 5 okrętów), choć ich niewątpliwym atutem jest konstrukcja powstała w oparciu o technologię Stealth. Na drugim biegunie plasują się jednostki większe, na których jednak mamy do czynienia z przeciążeniem uzbrojeniowym. Klasycznym przykładem są izraelskie okręty typu Sa'ar 6 powstałe w oparciu o niemiecki pierwowzór typu Braunschweig – ich uzbrojenie obejmuje działo Oto Melara kalibru 76 mm, 2 stacje uzbrojenia Typhoon, 32 pionowe wyrzutnie rakiet ziemia–powietrze Barak-8, 40 wyrzutni systemu obrony punktowej C-Dome, 16 rakiet przeciwokrętowych Gabriel V, radar EL/M-2248 MF-STAR AESA i 2 wyrzutnie torped kalibru 324 mm. Posiadają również hangar i platformę zdolną pomieścić średni śmigłowiec typu SH-60. Dla porównania niemieckie okręty wyposażone są w 2 wyrzutnie pocisków przeciwlotniczych RIM-116 RAM, 4 wyrzutnie pocisków przeciwokrętowych RBS15 Mk3, 1 działo OTO Melara kalibru 76 mm oraz 2 działka 27 mm. Wyposażenie lotnicze to dwa bezzałogowe śmigłowce rozpoznawcze S-100. Niemieckie okręty wypierają o 200 t mniej niż ich izraelskie odpowiedniki, a prędkość wynosząca 26 w. jest wyższa o 1,5 w. od okrętów izraelskich, te ostatnie mają też gorszą manewrowość i dzielność morską. Można wysunąć tezę, że w dającej się przewidzieć przyszłości korwety pozostaną podstawową klasą w niewielkich flotach określanych mianem „brązowych marynarek", natomiast floty określane jako zielone, nie wspominając o błękitnych, za podstawowy typ uniwersalnego okrętu bojowego w pełnomorskim wymiarze przyjmą fregaty, pozostawiając obronę wód macierzystych mniejszym okrętom, takim jak patrolowce, niszczyciele min itp.

Roman Kochnowski

J. Ciślak, *Dozorowiec ORP Kaszub. Ćwierć wieku pod „biało-czerwoną"*, „Morze, Statki i Okręty" 2012, nr 4; T. Grotnik, *Korwety rakietowe proj. 20380 typu Stieriegusczij*, Wydawnictwo Magnum-X, Warszawa 2022; R. Jackson, *Zerstörer, Fregatten und Korvetten: Über 300 der genannten Schiffstypen von den Anfängen bis heute. Mit allen technischen Angaben auf einen Blick und einer kurzen Modellgeschichte*, Gondrom Verlag, Bindlach 2001; https://merivoimat.fi/en/squadron-2020 (dostęp 10.01.2026); „Okręty Wojenne" 2020, nr 72; https://www.naval-technology.com/projects/visby/ (dostęp 10.01.2026).

KRĄŻOWNIK – duży okręt wojenny, obok lotniskowców i tzw. desantowców zaliczany współcześnie do największych jednostek nawodnych. Ze względu na koszty budowy oraz eksploatacji krążowniki posiadają w chwili obecnej nieliczne floty zaliczane do marynarek wojennych tzw. błękitnych wód. Sama nazwa pochodzi od holenderskiego słowa *kruiser* z XVII w., które oznaczało okręt przemierzający (w sensie żeglugi tam i z powrotem) bądź krążący po jednym (bądź kilku) akwenie. We flotach ery żagla rolę krążowników pełniły fregaty, których zadaniem było rozpoznanie, zwalczanie nieprzyjacielskiej żeglugi oraz korsarstwa i piractwa. Mocarstwa używały ich jako głównych okrętów w odległych posiadłościach kolonialnych, nadawały się także doskonale do tzw. prezentowania bandery, czyli celów reprezentacyjnych.

Krążownik stał się odrębnym typem okrętu w latach 1860–1870, kiedy fregaty żaglowe stały się przestarzałe, a okręty parowe, które miały je zastąpić, nazywano „krążownikami" – były uzbrojone w lekką lub średnią artylerię (kaliber rzędu 100–203 mm) i tylko w niewielkim stopniu opancerzone, miały jednak stosunkowo duży zasięg i były zazwyczaj szybkie. Ich parametry dotyczące opancerzenia, napędu i uzbrojenia opierały się na zasadzie „bycia silniejszymi niż wszystkie szybsze jednostki i szybszymi niż wszystkie silniejsze jednostki". Krążowniki były jednym z istotnych elementów francuskiej doktryny morskiej, tzw. młodej szkoły (fr. *jeune école*), której głównym orędownikiem był admirał Théophile Aube. Zakładała ona (a skierowana była głownie przeciw Imperium Brytyjskiemu), że wojnę morską przeciw Albionowi na bliskich wodach – głownie kanał La Manche, prowadzić będą torpedowce, a na odległych morzach i oceanach

– właśnie krążowniki. Rozwinięciem tej koncepcji był krążownik pancerny; okręt tej podklasy miał w teorii górować nad każdym krążownikiem potencjalnego przeciwnika artylerią i opancerzeniem, będąc zarazem szybszym od jego okrętów liniowych. W przededniu I wojny światowej panowała duża dowolność w klasyfikacji krążowników na podklasy i tak np. w cesarskiej marynarce niemieckiej dzielono je na małe (niem. *kleine Kreuzer*) i duże krążowniki (niem. *grosse Kreuzer*). Do tych ostatnich z przyczyn fiskalnych zaliczano także krążowniki bojowe, aczkolwiek przynależą one raczej do klasy okrętów liniowych. W Royal Navy większe krążowniki określano mianem pancernych (ang. *armored cruiser*), mniejsze zaś – lekkich (*light cruiser*). Wyporność krążowników wahała się od 2000 do 12 tys. t, gdy idzie o ostatnie krążowniki pancerne, jakie wprowadzano do służby (np. niemiecki Blücher). Równie duża była rozpiętość kalibru artylerii głównej: od 100 do 234 mm.

Podczas I wojny światowej krążowniki były przysłowiowymi „końmi roboczymi" wszystkich flot uczestniczących w konflikcie; prowadziły działania krążownicze na odległych akwenach (np. legendarny niemiecki Emden), w epoce, gdy lotnictwo borykało się z problemami wieku dziecięcego, stanowiły „oczy" floty, wreszcie kładły zapory minowe. Ich wyporność oraz kaliber dział rosły: pod koniec pierwszego światowego konfliktu artyleria główna miała kaliber 150–152 mm, a wyporność przekraczała 5000 t, gdy idzie o nowo budowane okręty, określane później powszechnie jako krążowniki lekkie.

Pewien porządek dotyczący klasyfikacji krążowników wprowadził traktat waszyngtoński z 1922 r., uzupełniony 8 lat później w Londynie. Ten pierwszy wprowadził ograniczenia jakościowe dla nowo budowanych okrętów tej klasy – odtąd ich wyporność nie mogła przekraczać 10 tys. t, a kaliber dział – 203 mm (czyli 8 cali); 8 lat później wprowadzono podział na krążowniki lekkie, dla których ustalono wyłącznie górny kaliber dział (155 mm), i ciężkie, gdzie górna granica wynosiła 203 mm. Bardzo szybko okazało się, że ograniczenie wyporności do 10 tys. t *de facto* uniemożliwi budowę dobrze zbalansowanego pod względem prędkości, uzbrojenia i opancerzenia okrętu. Chcąc zmieścić się w traktatowych ograniczeniach, we Francji i Włoszech zbudowano krążowniki (typ Duquesne i Trento) o wyporności 10 tys. t, dość szybkie (34–35 w.), dobrze uzbrojone (8 dział

kalibru 203 mm), lecz bardzo słabo opancerzone, mało odporne nie tylko na ostrzał z dział kalibru 150 mm, ale nawet na artylerię ówczesnych niszczycieli. Niewiele lepiej pod tym względem wyglądały okręty brytyjskie (typ County) czy japońskie (typ Furutaka).

Amerykanie pierwsze 2 okręty tej klasy (typ Pensacola), choć silnie uzbrojone (10 dział kalibru 203 mm), uznali początkowo za krążowniki lekkie, a to ze względu na skromne opancerzenie. Brytyjska admiralicja dość szybko zorientowała się co do niewielkiej przydatności tej klasy okrętów, uznając, że nadają się one niemal wyłącznie do ochrony szlaków żeglugowych przed rajderami. I faktycznie w tej roli sprawdziły się podczas II wojny światowej. W połowie lat 30. XX w. Wielka Brytania, Francja i Włochy zaprzestały budowy ciężkich krążowników; uznano, że w przypadku prawdopodobnego starcia większa liczba dział kalibru 150–155 mm byłaby lepsza niż mniejsza kalibru 203 mm. Chociaż pocisk kalibru 203 mm uczyniłby większe szkody przy trafieniu, można było przenosić więcej dział kalibru 150–155 mm, co prawdopodobnie skutkowałoby większą liczbą pocisków trafiających w cel i większą szansą na trafienie już w pierwszych salwach. Doprowadziło to do budowy krążowników o wyporności do 10 tys. t, uzbrojonych w 12 do 15 dział kalibru 152 mm (amerykański typ Brooklyn) czy 155 mm (japoński typ Mogami). Japończycy przebudowali okręty typu Mogami w krążowniki ciężkie: potrójne wieże z działami kalibru 155 mm zastąpiono podwójnymi o kalibrze 203 mm. W przeciwieństwie do ciężkich krążowników amerykańskich pozbawionych wyrzutni torpedowych, japońskie jednostki tej samej klasy miały ich aż do 12, poczynając od Myoko. Budowane w przededniu II wojny światowej krążowniki ciężkie zdecydowanie przekroczyły wyporność 10 tys. t. Wyporność standardowa niemieckiego typu Admiral Hipper wynosiła około 13 tys. t, a pełna bojowa sięgała 17 tys. t. Tuż przed 1939 r. pojawiła się też nowa podklasa tzw. krążowników przeciwlotniczych amerykańskich (typ. Atlanta) i brytyjskich (typ. Dido), aczkolwiek nominalnie zaliczano je do krążowników lekkich. Jeszcze inną podklasą były jednostki budowane jako przewodniki (liderzy) flotylli niszczycieli, np. holenderski Tromp czy japoński Agano.

W czasie II wojny światowej nowe krążowniki w długich seriach budowały już tylko mocarstwa anglosaskie – Wielka Brytania (typ Colony

i Swiftsure, ta druga seria została dokończona już po wojnie) oraz USA (typ Baltimore i Cleveland). Okręty te były udanymi konstrukcjami, ale też zdecydowanie wykraczały wielkością poza przedwojenne ustalenia traktatowe. Podczas działań wojennych jednostki tej klasy wszystkich państw uczestniczących w wojnie były bardzo intensywnie eksploatowane, ponosząc duże starty nie tylko w walkach z okrętami nawodnymi, ale i lotnictwem, a także na skutek ataków okrętów podwodnych.

Po II wojnie światowej jedyną serią krążowników artyleryjskich, skonstruowanych i zbudowanych od nowa, był sowiecki typ Swierdłow (łącznie 15 jednostek). Amerykański typ Des Moines, holenderski De Zeven Provinciën i szwedzki Tre Kronor to okręty zbudowane po wojnie, ale prace nad nimi rozpoczęto jeszcze w jej trakcie, a nawet (w przypadku okrętów holenderskich) przed 1939 r. Rozwój broni rakietowej sprawił, że stosunkowo nowe okręty tej klasy, jak np. amerykańskie jednostki typu Baltimore, przekształcano częściowo (np. Canberra) lub całkowicie (np. Albany) w okręty rakietowe.

Od lat 60. minionego stulecia nowe okręty tej klasy uzbrajano wyłącznie w broń rakietową, a nieliczna artyleria na pokładach miała wyłącznie pomocnicze znaczenie. Najwięcej typów krążowników rakietowych stworzył Związek Radziecki, przy czym w jego flocie znalazły się także tzw. krążowniki lotnicze (np. typ projektu 1123 Moskwa) czy przeciwpodwodne (np. typ 1134 Kresta II). Krążowniki helikopterowe zwane też lotniczymi budowały również Wielka Brytanie (typ Invincible, choć był to raczej lekki lotniskowiec) oraz Włochy (typ Andrea Doria). Ostatnim krążownikiem ciężkim wyposażonym w artylerię 203 mm, wycofanym ze służby, był hiszpański Canarias (1975), natomiast w kategorii krążowników lekkich za absolutnego rekordzistę uznać należy peruwiański Almirante Grau (eksholenderski De Reuter), wycofany ze służby w 2017 r. W 1961 r. Amerykanie ukończyli budowę pierwszego krążownika rakietowego o napędzie atomowym Long Beach, jednak kolejne jednostki tej klasy typu Ticonderoga (zbudowano 20 okrętów, w służbie pozostaje 7) zostały zaprojektowane przede wszystkim z myślą o wsparciu floty w działaniach przeciwlotniczych i przeciwrakietowych oraz wyposażone w nowoczesne systemy kierowania ogniem, co czyniło je kluczowymi jednostkami ochrony grup bojowych lotniskowców.

Obecnie nie ma jasności co do tego, jak będą wyglądać następcy tych okrętów służących dziś jako główne filary eskorty lotniskowcowych grup uderzeniowych. Poza US Navy w zasadzie jedyną marynarką wojenną dysponującą krążownikami jest flota Federacji Rosyjskiej posiadająca w służbie 4 okręty tej klasy: 2 z nich (typ Kirov) to olbrzymie jednostki o wyporności 28 tys. t posiadające napęd nuklearny, po ostatnich modernizacjach mogące uchodzić za stosunkowo nowoczesne, a 2 pozostałe (typ Sława) to okręty zdecydowanie mniejsze (10 tys. t) i przestarzałe; trzeci okręt tego typu – Moskwa – został zatopiony 14 kwietnia 2022 r., w wojnie rosyjsko-ukraińskiej. Kwestią dyskusyjną pozostaje, do jakiej klasy powinny zostać zaliczone chińskie okręty typu 055 – w ChRL uchodzą za niszczyciele, ale według ekspertów amerykańskich i brytyjskich należy je uznać za krążowniki rakietowe ze względu na wielkość oraz potencjał bojowy. W tworzonych zespołach lotniskowcowych marynarki wojennej Chińskiej Armii Ludowo-Wyzwoleńczej pełnią tę samą rolę co amerykańskie krążowniki typu Ticonderoga. Warto też dodać, że miały być one odpowiedzią na nowe amerykańskie krążowniki rakietowe typu CG(X), które nie wyszły jeszcze poza sferę projektów.

Roman Kochnowski

N. Friedman, *U.S. Cruisers: An Illustrated Design History*, Naval Institute Press, Annapolis, Maryland 1984; R. Kochnowski, *Niemieckie działania krążownicze 1939–1942*, Inforteditions, Tarnowskie Góry 2015; M. Lardas, I. Palmer, *German Heavy Cruisers vs Royal Navy Heavy Cruisers: 1939–42 (Duel)*, Osprey Publishing, Barnsley 2021; S. Lipiecki, *Symbol siły US Navy. Krążowniki typu Ticonderoga. Część 1*, „Morze, Statki i Okręty" 2020, nr 3–4, t. XXV(197); R. Rochowicz, *Krążowniki atomowe projektu 1144*, „Morze, Statki i Okręty" 2018, nr 3–4; A. Watts, *Japanese Warships of World War II*, Garden City, Doubleday New York 1973; M.J. Whitley, *Deutsche Kreuzer im Zweiten Weltkrieg*, Motorbuch Verlag, Stuttgart 2001.

KRYPTOGRAFIA KWANTOWA (ang. *quantum cryptography*) – stanowi obszar badań poświęcony wykorzystaniu właściwości mechaniki kwantowej do zapewniania poufności integralności i kontroli dostępu w systemach transmisji danych. Zasadniczym elementem tej konstrukcji jest założenie, że bezpieczeństwo informacji można oprzeć nie na trudności

obliczeniowej, lecz fundamentalnych prawach natury. W konsekwencji struktura teoretyczna kryptografii kwantowej uniezależnia ochronę komunikacji od potencjalnej przewagi technologicznej przeciwnika, który w przyszłości może dysponować zaawansowanymi metodami łamania szyfrów klasycznych. Jej podstawą jest wykorzystanie stanów kwantowych do przekazywania informacji o kluczu szyfrującym, co prowadzi do powstania modelu, w którym każda próba ingerencji w kanał transmisyjny ulega ujawnieniu jako zmiana parametrów fizycznych przesyłanych cząstek. Z tego powodu kryptografia kwantowa posiada znaczenie dla badań nad bezpieczeństwem systemów komunikacyjnych zarówno w wymiarze teoretycznym, jak i w kontekście praktycznych zastosowań związanych z ochroną infrastruktury o krytycznym znaczeniu.

W literaturze naukowej zwraca się uwagę, że mechanizm działania kryptografii kwantowej opiera się na zjawisku nieklonowalności stanów kwantowych, wykluczającym możliwość stworzenia wiernej kopii pojedynczego fotonu niosącego informację o kluczu. Odbiorca i nadawca mogą tym samym monitorować stopień zaburzeń sygnału i weryfikować, czy w procesie transmisji doszło do nieuprawnionej obserwacji. Istotnym następstwem tych ustaleń jest możliwość wykrywania prób przechwycenia w czasie zbliżonym do rzeczywistego, co znacząco odróżnia kryptografię kwantową od metod klasycznych, w których naruszenie poufności pozostaje zazwyczaj niejawne aż do momentu ujawnienia skutków operacji przeciwnika. Z tego względu badania nad systemami kwantowej dystrybucji klucza wprowadzają nową perspektywę w analizie ryzyka oraz w projektowaniu zabezpieczeń telekomunikacyjnych. Jednocześnie wskazuje się, że stan rozwoju technologii kwantowych ujawnia wiele wyzwań natury inżynieryjnej i organizacyjnej. Praktyczna realizacja protokołów kwantowych obarczona jest licznymi ograniczeniami wynikającymi z niedoskonałości źródeł światła detektorów oraz systemów stabilizujących poziom szumu.

Literatura przedmiotu zawiera opisy ataków wykorzystujących zachowania urządzeń nieprzewidziane w modelu teoretycznym, co wymusza opracowywanie rozszerzonych procedur kontrolnych oraz metod audytu technicznego. Współczesne badania koncentrują się więc na rozwijaniu formalnych modeli bezpieczeństwa, które łączą rygor fizyczny z analizą

podatności instrumentów pomiarowych, co pozwala na weryfikację, czy dane wdrożenie spełnia postulaty stawiane przez teorię. Znaczenie kryptografii kwantowej odnosi się również do kwestii bezpieczeństwa państwa i systemów zarządzania informacją o charakterze strategicznym. Przewidywany rozwój komputerów kwantowych stwarza ryzyko osłabienia lub eliminacji wielu współcześnie stosowanych mechanizmów kryptograficznych, które fundamentem bezpieczeństwa czynią trudność obliczeniową wybranych problemów matematycznych. W tym kontekście technologie kwantowej dystrybucji klucza są postrzegane jako potencjalny element długofalowych strategii zapewniania ciągłości ochrony komunikacji w okresie przechodzenia do środowiska postkwantowego. Znaczący jest także ich wpływ na kwestie budowania suwerenności technologicznej, ponieważ państwa rozwijające infrastrukturę kwantową uzyskują przewagę w zakresie utrzymywania kanałów komunikacyjnych o wysokiej odporności na działania wywiadowcze i cybernetyczne.

Ochrona infrastruktury krytycznej staje się jednym z kluczowych kierunków zastosowań kryptografii kwantowej. Sektory energetyczny, finansowy, transportowy oraz administracyjny wykorzystują rozbudowane systemy teleinformatyczne, których niezawodność ma fundamentalne znaczenie dla stabilności państwa. Wprowadzenie technologii kwantowych umożliwia projektowanie sieci komunikacyjnych odpornych na podsłuch i umożliwiających natychmiastowe wykrywanie naruszeń. Rozwiązania te mogą być w przyszłości integrowane z istniejącymi systemami zarządzania incydentami oraz z procedurami ciągłości działania, tworząc jednolity model nadzoru nad przepływem informacji o charakterze krytycznym.

Współczesne badania podkreślają również, że rozwój kryptografii kwantowej wymaga wielowymiarowej współpracy środowisk fizycznych, informatycznych, matematycznych oraz instytucji odpowiedzialnych za bezpieczeństwo narodowe. Złożoność zagadnienia łączy wiedzę dotyczącą właściwości fotonów z analizą zachowania systemów telekomunikacyjnych poddanych stresowi operacyjnemu, co tworzy interdyscyplinarny obszar badań akademickich. Postępujące prace nad standaryzacją protokołów kwantowych mają na celu wypracowanie spójnych procedur, które pozwolą na ich wdrożenie w skalowalnych systemach państwowych i komercyjnych. W tym świetle kryptografia kwantowa jawi się jako element długotrwałego

procesu modernizacji struktur bezpieczeństwa informacyjnego, w którym rozwój technologiczny łączy się z potrzebą formułowania nowych podstaw interpretacyjnych oraz nowych metod oceny ryzyka.

W kolejnych analizach podkreśla się, że kryptografia kwantowa oddziałuje nie tylko na techniczne aspekty ochrony informacji, lecz także na struktury organizacyjne odpowiedzialne za bezpieczeństwo cyfrowe. Instytucje państwowe i podmioty infrastrukturalne muszą dostosować swoje procedury operacyjne do wymagań technologii, których kontrola jakości wymaga odmiennego podejścia niż w przypadku systemów klasycznych. Konieczne staje się tworzenie wyspecjalizowanych zespołów zdolnych do oceny stabilności kanałów kwantowych oraz interpretacji anomalii sygnałowych wynikających z interakcji cząstek z otoczeniem. Wprowadzenie tych rozwiązań powoduje rozwój nowych kategorii kompetencji i przekształca sposób, w jaki instytucje planują i nadzorują bezpieczeństwo informacyjne.

Analiza publikacji naukowych dotyczących praktyki wdrażania kwantowej dystrybucji klucza wskazuje, że istotnym elementem systemów tego rodzaju jest ciągła obserwacja parametrów fizycznych transmisji oraz dynamiczne dostosowywanie procedur wytwarzania klucza do bieżących warunków kanału. Transmisje kwantowe są wrażliwe na czynniki środowiskowe, co powoduje, że stabilność sygnału zależy zarówno od jakości infrastruktury technicznej, jak i sposobu kalibracji urządzeń. Z tego względu wdrożenia QKD wymagają regularnych pomiarów kontrolnych, które umożliwiają ocenę poziomu szumu i identyfikację ewentualnych zaburzeń mogących świadczyć o wykonywaniu operacji obserwacyjnych. W badaniach podkreślono, że istotą zapewnienia bezpieczeństwa takich systemów jest umiejętność właściwej interpretacji tych zjawisk oraz ich odróżnienia od zakłóceń losowych.

Rozważania te prowadzą do istotnego wniosku, że kryptografia kwantowa stanowi narzędzie umożliwiające redefinicję paradygmatu bezpieczeństwa teleinformatycznego. W odróżnieniu od metod klasycznych, nie opiera się ona na założeniu, że przeciwnik posiada ograniczone możliwości obliczeniowe, lecz na przekonaniu, że naruszenie stanu cząstki kwantowej jest zjawiskiem nieukrywalnym. Powoduje to przesunięcie ciężaru ochrony informacji z obszaru matematycznej złożoności problemu do fizycznej nienaruszalności sygnału. W rezultacie modele zagrożeń zyskują nowy

wymiar, w którym działania ofensywne stają się możliwe do wykrycia znacznie wcześniej niż w systemach opartych na tradycyjnych metodach szyfrowania. Kryptografia kwantowa posiada także znaczenie dla badań nad odpornością systemów informacyjnych na zagrożenia generowane przez komputery kwantowe. W przewidywanej przyszłości wiele algorytmów klasycznych może ulec deprecjacji z powodu rozwoju obliczeń kwantowych, które mogą skracać czas łamania wybranych szyfrów do poziomu praktycznego. W tej sytuacji technologie kwantowe nie stanowią jedynie narzędzia wzmocnienia ochrony, ale też mechanizm, który pozwala obejść słabości tradycyjnych metod poprzez wprowadzenie zabezpieczeń opartych na odmiennych zasadach fizycznych. W literaturze zwraca się uwagę, że rozwój QKD jest komplementarny wobec kryptografii postkwantowej, co oznacza, że pełne bezpieczeństwo komunikacji wymaga wdrażania obu tych kierunków w sposób harmonijny i wzajemnie uzupełniający się.

W kontekście zarządzania bezpieczeństwem państwowym kryptografia kwantowa może stać się podstawą tworzenia wielowarstwowych struktur komunikacyjnych obsługujących administrację publiczną, wojsko, służby dyplomatyczne i podmioty odpowiedzialne za funkcjonowanie infrastruktury krytycznej. Implementacje pilotażowe prowadzone w wybranych państwach wskazują, że technologia ta może stanowić fundament przyszłych sieci o zasięgu krajowym łączących centra decyzyjne i systemy operacyjne w sposób odporny na ingerencję zewnętrzną. Wprowadzanie takich rozwiązań wymaga jednak rozbudowanej infrastruktury światłowodowej, urządzeń charakteryzujących się wysoką niezawodnością oraz systemów kontroli gwarantujących stabilność parametrów kwantowych na dużych dystansach. Z tych powodów rozwój infrastruktury kwantowej jest procesem długofalowym oraz znacząco zależnym od polityki państwa w zakresie inwestycji technologicznych.

W literaturze podkreśla się, że kryptografia kwantowa wnosi również nowe wyzwania dla instytucji odpowiedzialnych za audyt bezpieczeństwa. Modele badawcze muszą uwzględniać specyficzne właściwości fizyczne urządzeń oraz potencjalne odstępstwa ich zachowania od idealnych założeń teoretycznych. W tym kontekście rozwijane są metody testowania, które łączą pomiary interferencyjne z analizą czynników eksploatacyjnych oraz oceną podatności na ataki ukierunkowane na elementy sprzętowe.

Ustalenia te mają znaczenie dla certyfikacji systemów QKD oraz formułowania norm regulacyjnych, które określają minimalne wymagania techniczne i proceduralne dla urządzeń działających w środowisku kwantowym. W rezultacie kryptografia kwantowa staje się przedmiotem zarówno badań fundamentalnych, jak i rozwijających się procesów standaryzacyjnych, które określają warunki jej bezpiecznego wykorzystania w praktyce.

W ujęciu systemowym kryptografia kwantowa prowadzi do przekształcenia architektury komunikacji w sposób, który rozszerza zakres klasycznego rozumienia bezpieczeństwa informacji. Jej zastosowanie wymusza redefinicję procedur dotyczących generowania kluczy dystrybucji uprawnień oraz nadzoru nad integralnością kanałów transmisyjnych. Wdrażanie tego rodzaju technologii prowadzi do stopniowego tworzenia środowiska, w którym procesy ochronne są nierozerwalnie związane z monitorowaniem właściwości fizycznych nośników informacji, co zmienia strukturę odpowiedzialności za bezpieczeństwo cyfrowe. Ochrona danych staje się zatem procesem opartym na obserwacji zjawisk charakteryzujących się wysoką precyzją, a działania kontrolne wymagają wypracowania zestawu narzędzi analitycznych pozwalających na interpretację odchyleń pojawiających się w trajektoriach sygnału.

Dyskusja nad zastosowaniami kryptografii kwantowej obejmuje również zagadnienia związane z integracją technologii kwantowych z istniejącymi systemami teleinformatycznymi. Wdrażanie systemów QKD wymaga zgodności z architekturą sieci klasycznych oraz stworzenia rozwiązań umożliwiających translację danych pomiarowych na procedury operacyjne wykorzystywane przez zespoły zarządzające bezpieczeństwem. W tym kontekście istotne stają się badania dotyczące sposobów łączenia warstwy kwantowej z tradycyjnymi protokołami sieciowymi, co prowadzi do powstania hybrydowych modeli zabezpieczeń, w których sygnał kwantowy stanowi fundament ochrony klucza, natomiast pozostałe elementy architektury funkcjonują w oparciu o standardy klasyczne. Integracja ta wymaga odpowiedniego nadzoru technicznego oraz rozwiniętych mechanizmów synchronizacji, aby proces transmisji był wolny od zakłóceń mogących zafałszować interpretację obserwowanych parametrów.

Kryptografia kwantowa może stać się podstawowym narzędziem umożliwiającym projektowanie systemów komunikacji odpornych na

naruszenia zarówno w perspektywie krótkoterminowej, jak i w kontekście przemian technologicznych, które w przyszłości mogą osłabić skuteczność zabezpieczeń klasycznych. Zastosowania te obejmują w szczególności te obszary, w których poufność informacji ma znaczenie dla funkcjonowania państwa oraz stabilności sektora finansowego, energetycznego, transportowego i administracyjnego. Z tego względu rozwój technologii kwantowych postrzega się jako proces długofalowy, w którym inwestycje badawcze i infrastrukturalne mają strategiczny charakter i wymagają współdziałania środowisk naukowych, technologicznych oraz instytucji odpowiedzialnych za kształtowanie polityki bezpieczeństwa.

Znaczącym elementem rozważań dotyczących kryptografii kwantowej jest potrzeba wytworzenia kultury bezpieczeństwa, w której zrozumienie zasad działania technologii kwantowych staje się niezbędne dla prawidłowej oceny ryzyka. Wdrażanie systemów QKD wymaga bowiem nie tylko infrastruktury i procedur technicznych, ale także kompetencji umożliwiających identyfikację zagrożeń specyficznych dla środowiska kwantowego. W tym kontekście ważną rolę odgrywają programy szkoleniowe oraz badawcze, które pozwalają na rozwijanie umiejętności interpretacyjnych oraz zrozumienie właściwości fizycznych będących podstawą bezpieczeństwa tych systemów. Ich skuteczność zależy od zdolności użytkowników do oceny anomalii transmisyjnych i właściwego reagowania na potencjalne próby naruszenia integralności sygnału. Rozwój kryptografii kwantowej wskazuje zatem na konieczność kształtowania nowych modeli współpracy między ośrodkami naukowymi, sektorem przemysłowym oraz instytucjami odpowiedzialnymi za bezpieczeństwo narodowe. Współdziałanie to staje się podstawą tworzenia infrastruktury zdolnej do funkcjonowania w środowisku, które w coraz większym stopniu opiera się na technologiach zaawansowanych zarówno pod względem teoretycznym, jak i inżynieryjnym. W tym ujęciu kryptografia kwantowa nie jest jedynie narzędziem ochrony komunikacji, lecz także zjawiskiem, które wpływa na sposób organizacji systemów bezpieczeństwa oraz rozumienia pojęcia ochrony informacji w warunkach dynamicznego rozwoju technologicznego.

Aleksandra Gębacz

A.K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, „Physical Review Letters" 1991, vol. 67(6); K. Fiałkowski, *Wstęp do informatyki kwantowej*, Uniwersytet Jagielloński, Kraków 2015; K. Horodecki, *Kwantowe splątanie i kwantowa kryptografia*, 2007, http://zeus.ifpan.edu.pl/ACTIVITY/sem-info/misc/Horodecki.pdf (dostęp 10.12.2025); ISO/IEC. Information Technology – Security Techniques – Quantum – Resistant Cryptography. ISO/IEC 23837-1, 2023 NSA; M. Maj, *Kwantowa dystrybucja klucza: stan wiedzy*, „Zeszyty Naukowe WSEI" 2017, nr 7; *Quantum Computing and Post-Quantum Cryptography: Frequently Asked Questions*, National Security Agency, 2021, https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF (dostęp 14.12.2025); V. Scarani, *The Security of Practical Quantum Key Distribution*, „Reviews of Modern Physics" 2009, vol. 81(3).

KWANTOWE ZABEZPIECZENIA (ang. *quantum security*) – stanowią obszar rozwijający się w odpowiedzi na rosnące wymagania dotyczące ochrony informacji w środowiskach, które charakteryzują się narastającą złożonością zagrożeń oraz stopniem zaawansowania technicznego podmiotów prowadzących działania ofensywne w cyberprzestrzeni. Ich podstawę tworzą zasady mechaniki kwantowej, które umożliwiają konstrukcję rozwiązań niewrażliwych na klasyczne metody przechwytywania danych i analiz kryptograficznych. Zarysowują one architekturę bezpieczeństwa odmienną od tej, którą narzuciły tradycyjne paradygmaty kryptograficzne oparte na matematycznych problemach trudnych obliczeniowo. W odróżnieniu od podejścia klasycznego, mechanizmy kwantowe nie zakładają, że odporność systemu będzie wynikała z ograniczeń obliczeniowych przeciwnika, lecz z właściwości fizycznych uniemożliwiających pozyskanie informacji bez jej naruszenia.

Podstawowe znaczenie w tym kontekście ma dystrybucja klucza kwantowego, rozwijana od lat 80. Idea ta opiera się na wykorzystaniu pojedynczych stanów kwantowych w procesie przekazywania bitów klucza między stronami komunikującymi się poprzez kanał optyczny. Stany te ulegają nieodwracalnym zmianom pod wpływem pomiaru, co sprawia, że każda próba ich przechwycenia zostawia ślad możliwy do wykrycia w ramach analizy zgodności statystycznej. Odbiorcy mogą dzięki temu jednoznacznie ocenić, czy klucz został pozyskany w sposób bezpieczny. Recepcja sygnału obejmuje procedury testowania błędów, analizę korelacji oraz

wdrożenie algorytmów weryfikujących integralność wyników. W sytuacji, gdy poziom zakłóceń przekracza wartości dopuszczalne, wymiana zostaje uznana za naruszoną, a klucz jest odrzucany. Tego rodzaju podejście, zdefiniowane pierwotnie w zakresie protokołów BB84 oraz E91, przeszło liczne modyfikacje, obejmujące rozwiązania zapewniające ochronę nawet w warunkach rzeczywistej niedoskonałości urządzeń. Kwantowe zabezpieczenia obejmują również mechanizmy związane z komunikacją wykorzystującą splątanie kwantowe – umożliwia to korelację stanów dwóch fotonów w sposób, który nie ma klasycznego odpowiednika, a jego stabilność daje szansę na budowę systemów komunikacyjnych pozwalających na przekazywanie informacji korelacyjnych odpornych na podsłuch. Model ten znajduje swoje rozwinięcie w projektach sieci kwantowych o zasięgu ponadkrajowym, a także w eksperymentach satelitarnych, które umożliwiły rozciągnięcie łączności kwantowej na dystanse dotychczas nieosiągalne w infrastrukturze naziemnej. Wprowadzenie węzłów pośrednich oraz pamięci kwantowych, choć nadal pozostaje przedmiotem intensywnych badań, tworzy podstawę dla przyszłych rozwiązań zapewniających bezpieczeństwo transmisji na poziomie wymaganym w środowiskach dyplomatycznych, militarnych oraz krytycznych dla funkcjonowania państwa.

Wraz z rozwojem komputerów kwantowych pojawia się konieczność równoległego rozpatrywania dwóch odrębnych, choć powiązanych wymiarów bezpieczeństwa: ochrony informacji przy użyciu zjawisk kwantowych oraz ochrony informacji przed atakami wykorzystującymi urządzenia kwantowe. Wynika to z faktu, że rozwijane komputery kwantowe zdolne są prowadzić obliczenia, które zagrażałyby tradycyjnym schematom opartym na trudności faktoryzacji lub problemach logarytmu dyskretnego. Z tego powodu klasyczna infrastruktura bezpieczeństwa musi być wzbogacana o rozwiązania odporne na obliczenia kwantowe, natomiast systemy oparte na dystrybucji klucza kwantowego stanowią element równoległego zabezpieczenia, które eliminuje ryzyko przechwycenia klucza w okresie przejściowym pomiędzy obecnymi a przyszłymi standardami kryptograficznymi.

Warto zwrócić uwagę na rosnące znaczenie badań nad odpornością urządzeń wykorzystywanych w systemach kwantowych na ataki *side-channel* oraz próby wprowadzania zakłóceń do kanału kwantowego. Z pozoru

idealne właściwości fizyczne wykorzystywane w dystrybucji klucza mogą zostać naruszone poprzez słabości implementacyjne. Badania prowadzone w ostatnich dwóch dekadach wykazały, że niedopasowania detektorów, niejednorodności źródeł fotonów oraz błędy w kalibracji mogą być wykorzystywane przez podmioty przeprowadzające ataki aktywne. Odpowiedzią na te zagrożenia stał się rozwój protokołów zabezpieczonych względem charakterystyki urządzeń, w szczególności podejść typu *measurement-device-independent QKD*, które eliminują wpływ niepewności detekcji na całość procesu wymiany klucza. Zabezpieczenia kwantowe wpisują się również w działania państw w zakresie ochrony infrastruktury krytycznej i bezpieczeństwa narodowego. Z uwagi na brak możliwości ich przechwycenia metodami umożliwiającymi zachowanie niejawności ataku stają się one narzędziem szczególnie cennym w dziedzinach wymagających zapewnienia poufności informacji przekazywanych w ramach komunikacji rządowej. Odpowiednie instytucje rekomendują stopniową integrację rozwiązań kwantowych w strukturach państwowych i korporacyjnych, zwłaszcza w tych segmentach, które narażone są na szczególnie intensywne działania wywiadowcze. Struktura komunikacji opartej na rozwiązaniach kwantowych ma również znaczenie w kontekście bezpieczeństwa długoterminowego, ponieważ klucze zabezpieczone z użyciem dystrybucji kwantowej pozostają odporne na przechowywanie i późniejsze odszyfrowanie przez podmioty dysponujące archiwalnym materiałem komunikacyjnym.

W rezultacie kwantowe zabezpieczenia można traktować jako rozwijające się zaplecze techniczne dla systemów obronnych i teleinformatycznych wymagających trwałej ochrony przed zagrożeniami o charakterze strategicznym. Ich praktyczne wykorzystanie wymaga integracji technologii optycznych, telekomunikacyjnych i informatycznych oraz budowy sieci, które będą zdolne do skalowania w wymiarze państwowym. Obecny stan badań potwierdza, że choć technologia ta wymaga dalszych udoskonaleń, stanowi fundament przyszłych rozwiązań, w których bezpieczeństwo informacyjne wynika z praw fizyki, a nie z granic wydajności współczesnych maszyn obliczeniowych. Rozwój kwantowych zabezpieczeń wymaga szczegółowego rozpoznania ograniczeń technicznych, które mogą wpływać na ich praktyczną użyteczność. Badania nad stabilnością

kanałów światłowodowych wykazały, że czynniki środowiskowe, takie jak dyspersja, tłumienie oraz przypadkowe zmiany parametrów propagacyjnych, wywierają istotny wpływ na stan kwantowy przesyłanych fotonów. Z tego względu istotne stało się opracowanie rozwiązań pozwalających na kompensowanie zakłóceń oraz stabilizację torów transmisyjnych.

Jednym z kierunków jest rozwój detektorów o większej czułości i niższym poziomie szumów, co pozwala ograniczyć liczbę błędów w procesie rekonstrukcji sygnału. Drugim jest udoskonalanie źródeł pojedynczych fotonów oraz generatorów splątania, które muszą charakteryzować się wysoką jednorodnością, aby umożliwić skuteczne wykorzystanie ich w złożonych systemach wymiany klucza. Niezależnie od warunków technicznych kluczowe pozostaje wdrażanie metod walidacji bezpieczeństwa, które mają na celu nie tylko ocenę jakości implementacji, lecz również wykrywanie słabości mogących wynikać z czynników organizacyjnych. W literaturze podkreśla się konieczność utrzymania pełnej kontroli nad konfiguracją urządzeń oraz ich systematycznej certyfikacji. Elementem istotnym dla zachowania integralności systemu jest przeciwdziałanie manipulacjom na poziomie sprzętowym, które mogłyby umożliwić wprowadzenie dodatkowych kanałów depozycji światła lub zakłóceń kierunkowych. Dlatego opracowywane są ramy standaryzacyjne obejmujące model oceny ryzyka zarówno w kontekście wykorzystania fizycznych cech mechaniki kwantowej, jak i w odniesieniu do klasycznych zagrożeń wynikających z ingerencji w infrastrukturę telekomunikacyjną. W miarę jak systemy kwantowe stają się coraz bardziej zaawansowane pod względem architektury oraz skali, pojawia się potrzeba integracji infrastruktury kwantowej z tradycyjnymi metodami ochrony informacji. W praktyce oznacza to utrzymanie równoczesnego funkcjonowania protokołów klasycznych oraz kwantowych, co wymaga opracowania metod ich koordynacji operacyjnej. Wynika to z faktu, że komunikacja kwantowa, mimo wysokiej odporności na przechwycenie, nie zawsze może być stosowana jako jedyny środek ochrony, szczególnie w środowiskach o wysokim stopniu zmienności lub tam, gdzie nie są dostępne wymagane zasoby optyczne. Dlatego hybrydowe modele bezpieczeństwa teleinformatycznego pozostają kluczowe w okresie przejściowym, w którym technologie kwantowe nie osiągnęły jeszcze pełnej dojrzałości.

Odrębnym zagadnieniem są badania dotyczące przewidywanej ewolucji komputerów kwantowych i ich zdolności do łamania współczesnych algorytmów kryptograficznych. Postępy w tym obszarze prowadzą do konieczności wdrażania rozwiązań odpornych na obliczenia kwantowe, obejmujących nowe schematy kryptograficzne oparte na strukturach matematycznych, dla których nie są znane algorytmy kwantowe umożliwiające ich efektywne rozwiązywanie. Jednocześnie technologie kwantowe oferują narzędzia, które mogą chronić najwrażliwsze segmenty komunikacji w sposób niezależny od tych rozwiązań. Tworzy to środowisko, w którym 2 odrębne linie rozwoju bezpieczeństwa muszą być prowadzone równocześnie, aby zapewnić odporność zarówno na zagrożenia bieżące, jak i na te, które pojawią się wraz z rozwojem pełnoskalowych komputerów kwantowych.

Nie mniej istotne są prace związane z tworzeniem pamięci kwantowych umożliwiających przechowywanie stanów kwantowych przez czas wystarczający do budowy rozległych sieci transmisyjnych. Pamięci te wymagają środowisk o wysokiej stabilności termicznej i elektromagnetycznej, a ich zdolność do przechowywania splątania pozostaje jednym z najważniejszych wyzwań technologicznych. Trwałość przechowywanego stanu jest kluczowa, ponieważ pozwala na realizację złożonych operacji korelacyjnych w strukturach, które obejmują wiele węzłów pośrednich. Wpływa to na parametry bezpieczeństwa całego systemu, ponieważ stabilne przechowywanie informacji kwantowej umożliwia stosowanie bardziej złożonych protokołów transmisji i weryfikacji bezpieczeństwa.

W kontekście szerszej strategii bezpieczeństwa państwa technologie kwantowe stają się elementem wymagającym planowania długoterminowego. Obejmują zarówno infrastrukturę komunikacyjną, jak i zaplecze badawcze konieczne do utrzymania przewagi technologicznej. Znaczenie tych rozwiązań dostrzegają instytucje odpowiedzialne za tworzenie standardów bezpieczeństwa, które rekomendują rozwój kompetencji i zasobów umożliwiających implementację systemów kwantowych w perspektywie wieloletniej.

Z perspektywy instytucjonalnej technologie te stanowią część szerszej transformacji związanej z adaptacją systemów bezpieczeństwa do warunków, w których zdolności obliczeniowe przeciwnika ulegają dynamicznym

zmianom. Wprowadzenie systemów kwantowych do praktyki ochrony informacji wymaga również opracowania odpowiednich metod oceny ryzyka, które uwzględniają specyfikę zjawisk kwantowych. Klasyczne modele analityczne nie są w pełni adekwatne, ponieważ opierają się na założeniach o deterministycznej naturze działania systemów oraz przewidywalności zachowań urządzeń. W przypadku technologii kwantowych konieczne jest przyjęcie podejścia probabilistycznego, w którym bezpieczeństwo jest oceniane nie w odniesieniu do pojedynczych operacji, lecz statystycznych właściwości dużych zbiorów zdarzeń.

Jednym z kluczowych parametrów oceny jest poziom błędów kwantowych w kanałach transmisyjnych, ponieważ wartości te umożliwiają określenie, czy ewentualna ingerencja przeciwnika mieści się w granicach naturalnych zakłóceń, czy wskazuje na aktywne przechwytywanie. Pozwala to tworzyć ramy bezpieczeństwa oparte na przewidywalności odchyleń i ich interpretacji w kontekście fizycznych ograniczeń procesu pomiarowego. Systemy kwantowe wprowadzają również nowe perspektywy w zakresie analizy zgodności operacyjnej w instytucjach, które wymagają zachowania spójności procedur dotyczących komunikacji. W szczególności istotne jest, aby podmioty korzystające z kwantowych kanałów transmisyjnych utrzymywały jednolite standardy postępowania w zakresie testowania, walidacji oraz dystrybucji kluczy. Każde odstępstwo od tych procedur tworzy potencjalną lukę, która może zostać wykorzystana przez przeciwnika. W konsekwencji technologie kwantowe nie eliminują potrzeby ustanowienia rygorystycznych zasad zarządzania bezpieczeństwem, lecz wymagają ich dodatkowego wzmocnienia ze względu na wrażliwość procesu transmisji na nawet niewielkie zakłócenia organizacyjne. To powoduje, że bezpieczeństwo kwantowe ma charakter interdyscyplinarny, łącząc w sobie elementy fizyki, telekomunikacji, informatyki oraz zarządzania.

W miarę rozwoju badań nad kwantowymi zabezpieczeniami coraz większego znaczenia nabierają kwestie związane z ich odpornością na zagrożenia, które mogą pojawić się w przyszłych generacjach technologii obliczeniowych. Jednym z zagadnień analizowanych w literaturze jest wpływ ewentualnych przyszłych urządzeń dysponujących możliwościami częściowego powielania lub korekcji stanów kwantowych, co mogłoby osłabić obecne założenia dotyczące niemożliwości ich kopiowania. Choć

aktualna wiedza nie wskazuje na techniczne możliwości obejścia zakazu klonowania, badania nad strukturą informacji kwantowej pozostają intensywne. Z tego względu ocena bezpieczeństwa musi być procesem ciągłym, obejmującym analizę fundamentalnych ograniczeń fizycznych oraz monitorowanie potencjalnych nowych technologii, które mogłyby wpłynąć na stabilność obecnych rozwiązań.

Implementacja rozwiązań kwantowych wymaga również zrozumienia zależności między bezpieczeństwem fizycznym infrastruktury a bezpieczeństwem logicznym procesu komunikacyjnego. W tradycyjnych systemach teleinformatycznych oba te wymiary można rozpatrywać względnie niezależnie, natomiast technologie kwantowe powodują zatarcie tej granicy. Niezakłócona transmisja stanów kwantowych wymaga nie tylko odporności protokołów na ataki logiczne, lecz także wysokiej jakości ochrony fizycznej kanałów światłowodowych, sprzętu optycznego oraz detektorów. Nawet minimalne modyfikacje toru optycznego mogą wpływać na parametry generowanego stanu i tym samym – na bezpieczeństwo transmisji. Oznacza to, że infrastruktura kwantowa musi być projektowana tak, aby tworzyć środowisko w pełni kontrolowane, minimalizujące wpływ czynników zewnętrznych.

Postępująca integracja technologii kwantowych z istniejącymi systemami teleinformatycznymi skłania do analizy ich wpływu na stabilność procesów decyzyjnych, szczególnie w środowiskach, w których czas reakcji ma kluczowe znaczenie. Zastosowanie zabezpieczeń opartych na zjawiskach kwantowych może w dłuższej perspektywie zmienić sposób organizowania struktur odpowiedzialnych za zarządzanie informacją, ponieważ umożliwia bardziej precyzyjne modelowanie poziomu ekspozycji na zagrożenia w czasie rzeczywistym. Stanowi to odejście od metodologii, w której bezpieczeństwo jest weryfikowane okresowo, na rzecz koncepcji, w której ocena integralności komunikacji jest procesem ciągłym i nierozerwalnie związanym z fizycznymi właściwościami łącza. W rezultacie instytucje odpowiedzialne za bezpieczeństwo narodowe mogą tworzyć modele analityczne pozwalające na szybsze odróżnianie zdarzeń losowych od działań intencjonalnych, co podnosi efektywność reagowania operacyjnego. Włączenie rozwiązań kwantowych do złożonych systemów bezpieczeństwa wymaga również analizy ich interoperacyjności. Systemy

te, choć projektowane w oparciu o fundamentalne prawa fizyki, muszą funkcjonować w środowisku zdominowanym przez klasyczne technologie transmisyjne i obliczeniowe. Oznacza to potrzebę opracowania warstw pośrednich odpowiedzialnych za konwersję, synchronizację i kontrolę parametrów pracy z uwzględnieniem zmienności warunków operacyjnych. Wyzwaniem staje się utrzymanie spójności jakościowej transmisji na styku technologii kwantowych i klasycznych, ponieważ jakiekolwiek różnice w charakterystyce sprzętowej mogą wpływać na stabilność generowanych kluczy oraz interpretację sygnałów. Konieczne jest zatem tworzenie architektur hybrydowych, które zapewniają nieprzerwaną komunikację bez degradacji parametrów bezpieczeństwa wynikających z zastosowanych rozwiązań kwantowych.

Na szczegółową analizę zasługuje także rola, jaką technologie kwantowe mogą odegrać w rozwoju systemów detekcji i monitorowania. Dzięki możliwości wykorzystania korelacji kwantowych w pomiarach wysokiej czułości pojawia się perspektywa tworzenia sensorów zdolnych do rejestrowania minimalnych zmian parametrów środowiskowych. W kontekście bezpieczeństwa infrastruktury krytycznej oznacza to możliwość wdrażania sieci pomiarowych, które charakteryzują się wyższą odpornością na zakłócenia oraz zdolnością do wykrywania anomalii na wcześniejszym etapie niż tradycyjne systemy detekcyjne. Rozwiązania takie mogą wspierać proces identyfikacji zagrożeń, w tym nieautoryzowanej ingerencji w infrastrukturę fizyczną oraz prób manipulacji sygnałem na poziomie optycznym. Tym samym technologie kwantowe mogą stać się integralnym elementem systemów monitorowania bezpieczeństwa, a nie jedynie narzędziem wspierającym komunikację. W literaturze przedmiotu rośnie zainteresowanie wpływem, jaki globalna dostępność technologii kwantowych może mieć na równowagę strategiczną między państwami. Przewaga wynikająca z wcześniejszego wdrożenia rozwiązań kwantowych może prowadzić do nierównomiernego dostępu do zabezpieczonej komunikacji, co w praktyce oznacza możliwość uzyskania przewagi informacyjnej. W konsekwencji pojawia się potrzeba stworzenia międzynarodowych ram regulacyjnych obejmujących wymianę wiedzy, standardów oraz minimalnych wymagań bezpieczeństwa, tak aby rozwój technologiczny nie prowadził do destabilizacji układu bezpieczeństwa globalnego. Dotyczy

to również mechanizmów weryfikacji i certyfikacji, które umożliwiają niezależne potwierdzenie zgodności systemów kwantowych z przyjętymi normami. Rozwój infrastruktury kwantowej wymaga także uwzględnienia aspektów związanych z jej odpornością na awarie systemowe oraz czynniki środowiskowe.

Ze względu na specyfikę transmisji kwantowej nawet krótkotrwałe zakłócenia mogą prowadzić do utraty integralności procesu generowania klucza, co wymaga opracowania procedur redundancji oraz automatycznej rekonfiguracji torów optycznych. Ważne jest także zapewnienie ciągłości działania w sytuacjach kryzysowych, w których priorytetem jest utrzymanie bezpiecznej komunikacji między kluczowymi instytucjami państwowymi. Wymaga to implementacji wielowarstwowych systemów zabezpieczeń, obejmujących zarówno redundancję sprzętową, jak i algorytmy zarządzania ruchem w warunkach ograniczonej przepustowości.

Ostatecznie technologie kwantowe stają się jednym z kluczowych kierunków rozwoju systemów bezpieczeństwa informacyjnego, oferując potencjał do zwiększenia odporności na zagrożenia, które nie mogą zostać skutecznie zneutralizowane za pomocą klasycznych metod kryptograficznych. Ich efektywne wdrażanie wymaga jednak ujęcia holistycznego, uwzględniającego zarówno właściwości fizyczne, jak i organizacyjne oraz strategiczne. Dlatego dalsze badania powinny koncentrować się nie tylko na doskonaleniu komponentów technicznych, lecz również opracowaniu modeli integracji i oceny ryzyka, które umożliwią pełne wykorzystanie potencjału technologii kwantowych w systemach bezpieczeństwa.

Aleksandra Gębacz

I. Białynicki-Birula, *Teoria kwantów Mechanika falowa*, Wydawnictwo Naukowe PWN, Warszawa 2017; A.K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, „Physical Review Letters" 1991, https://doi.org/10.1103/PhysRevLett.67.661; ENISA, *Post-Quantum Cryptography: Expected Impact on Cybersecurity*, European Union Agency for Cybersecurity, 2021; N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Quantum Cryptography*, Cambridge University Press, Cambridge 2002; M. Jakubik, O. Grajewski, *Implementacja post-quantum cryptography w ramach EUDI Wallet jako elementu eIDAS 2 w kontekście wyzwań prawnych i technicznych oraz implikacji dla bezpieczeństwa cybernetycznego w świetle regulacji CRA i NIS 21*,

„Prawo Mediów Elektronicznych. Kwartalnik Naukowy" 2024, nr 3; V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *The Security of Practical Quantum Key Distribution*, „Reviews of Modern Physics" 2009.

L

LEGION WOLNOŚĆ ROSJI (ros. *Легион Свобода России*) – formacja paramilitarna utworzona w Siłach Zbrojnych Ukrainy w marcu 2022 r. Legion składa się głównie z rosyjskich ochotników, w tym jeńców wojennych, którzy postanowili walczyć za Ukrainę i wolną Rosję przeciwko siłom Putina. Wśród bojowników legionu Wolność Rosji znajduje się były wiceprezes rosyjskiego Gazprombanku Ihor Wołobujew, który opuścił Rosję i przyjechał do Ukrainy po rozpoczęciu inwazji Kremla na pełną skalę. Powodem jego powstania była chęć Rosjan i Ukraińców do walki ze zbrojną bandą Putina.

W pierwszych dniach rosyjskiej agresji do legionu zgłosili się ochotnicy, obywatele Rosji oraz rosyjskojęzyczni obywatele innych krajów, którzy uważali za swój obowiązek ochronę kochającego wolność narodu ukraińskiego. Oprócz więźniów w skład legionu wchodzą również rosyjscy dysydenci, czynni i emerytowani wojskowi Federacji Rosyjskiej oraz obywatele Białorusi.

Pierwsza wzmianka o utworzeniu specjalnej formacji wojskowej z Rosjan, którzy zostali wzięci do niewoli na terytorium Ukrainy i wyrazili chęć walki z reżimem Putina wraz z siłami zbrojnymi, pojawiła się 11 marca

2022 r., a niecały miesiąc później (5 kwietnia) korespondenci zagraniczni odbyli pierwszą odprawę z 3 rosyjskimi żołnierzami, którzy nazywali siebie legionem Wolność Rosji. Mniej więcej w tym samym czasie, po wycofaniu się armii rosyjskiej ze stolicy Ukrainy, świat dowiedział się o straszliwych okrucieństwach, jakich dopuścili się rosyjscy najeźdźcy na terenie obwodu kijowskiego, w szczególności w miastach Irpiń i Bucza. To właśnie stało się siłą napędową motywującą Rosjan do walki ramię w ramię z Ukraińcami przeciwko Kremlowi. Sam legion, według raportów, składa się z 2 batalionów. W czerwcu 2022 r. do legionu dołączyło 250 nowych członków.

Na początku wojny, zgodnie z prawodawstwem Ukrainy, obywatele krajów agresorów (Rosja i Białoruś) mieli zakaz wstępowania w szeregi Sił Zbrojnych Ukrainy. Jednocześnie było wielu Rosjan, którzy kierując się zasadami, nie mogli pozostać obojętni i szukali sposobów na włączenie się w szeregi obrońców Ukrainy.

Legion Wolność Rosji należy do Międzynarodowego Legionu Ukraińskich Sił Zbrojnych: w jego skład wchodzą byli żołnierze Sił Zbrojnych Federacji Rosyjskiej oraz inni Rosjanie. Według niektórych źródeł w legionie są także Białorusini, którzy nie mieli doświadczenia w służbie w oddziałach regularnych.

W legionie walczą 3 grupy ochotników:

- obywatele Federacji Rosyjskiej, którzy legalnie przebywali w Ukrainie ze względów rodzinnych lub zawodowych;
- Rosjanie, którzy niezależnie przybyli do Ukrainy z Rosji i Europy, aby walczyć z reżimem Putina;
- były zawodowy personel wojskowy Federacji Rosyjskiej, który początkowo rozumiał zbrodniczość wojny Putina.

Podejmując decyzję o utworzeniu jednostki, pierwsi legioniści postawili sobie 2 zadania rekrutacyjne – przygotowanie gwarancji socjalnych dla wszystkich przyszłych ochotników oraz niedopuszczenie do przedostania się do legionu tajnych służb reżimu. W ten sposób rozpoczęła się długa walka o rozwiązanie wszystkich kwestii na polu legislacyjnym – zarówno socjalnym, jak i bezpieczeństwa. Od końca wiosny i lata 2022 r. legion walczył w formacie małych grup bojowych. Na początku sierpnia uzgodniono wszystkie kwestie prawne i elementy bezpieczeństwa, a następnie rozpoczęto systematyczne prace nad sprawdzaniem i rejestrowaniem

chętnych Rosjan w jedną jednostkę. Według stanu na sierpień 2022 r. jednostki legionu brały już udział w walkach na kierunkach Bachmut, Charków, Sumy i na południu Ukrainy.

Podczas, gdy legion Wolność Rosji był postrzegany jako jednostka wojskowa w Ukrainie, zyskał zwolenników w Rosji jako forma oporu. Przypisuje się im liczne ataki na policję i lokalną infrastrukturę. Wielu członków opozycji postrzega rosyjską flagę jako znak imperializmu, militaryzmu i autorytaryzmu, a czerwony pasek jest tego kluczową częścią.

Żołnierze jednostki identyfikują się poprzez używanie 3 symboli:

- naszywki z zaciśniętą pięścią i napisem „Wolność Rosji" (ros. „Свобода России");
- łacińskiej litery „L", od której rozpoczynają się wyrazy „legion" i „*liberty*" (symbol ten jednak nie jest używany na mundurach);
- biało-niebiesko-białej flagi, powszechnie używanej przez aktywistów z Rosji jako symbol protestu przeciwko rosyjskiej inwazji na Ukrainę. Sam twórca flagi, który zaprojektował ją na kilka miesięcy przed powstaniem legionu, twierdzi, że miała to być rosyjska flaga pozbawiona koloru czerwonego, który symbolizuje „carski autorytaryzm i militaryzm".

Biało-niebiesko-biała flaga jest symbolem wolnej Rosji przyszłości; została wymyślona w społeczności internetowej sprzeciwiającej się inwazji armii rosyjskiej na Ukrainę pod koniec lutego 2022 r. Już następnego dnia po pierwszej wzmiance na portalach społecznościowych Rosjanie za granicą poszli na pokojowe protesty z biało-niebiesko-białą flagą zamiast oficjalnej flagi rosyjskiej.

Według członków stowarzyszenia legion Wolności Rosji powstał, aby walczyć z reżimem Putina i bronić Ukrainę przed inwazją rosyjską. Jeśli chodzi o wynagrodzenie legionistów, jeden z ochotników powiedział w wywiadzie dla ukraińskiego kanału YouTube PRESSING, że otrzymują oni żywność, pensje i broń od Sił Zbrojnych Ukrainy.

Datą powstania legionu jest 11 marca 2022 r. Kiedy ponad 100 żołnierzy armii rosyjskiej dobrowolnie przeszło na stronę Ukrainy, utworzono legion. Są wśród nich zarówno dezerterzy, jak i dysydenci polityczni. Według dowódcy kompanii Maksymiliana Andronnikowa 27 lutego przy pomocy pracowników Ukraińskiej Służby Bezpieczeństwa SBU przeszli

oni na stronę ukraińską, aby chronić Ukraińców przed prawdziwymi faszystami. Dowódca kompanii wezwał swoich rodaków, żołnierzy armii rosyjskiej, do wstąpienia w szeregi legionu Wolność Rosji, aby ocalić własny naród i kraj „przed upokorzeniem i zagładą".

Ponieważ większość bojowników legionu to byli żołnierze Sił Zbrojnych Rosji, dla własnego bezpieczeństwa nie ujawniają oni swojej tożsamości.

Ukraińskie Ministerstwo Obrony pod koniec marca 2022 r. poinformowało na swoim kanale w serwisie Telegram, że dowódcy legionu Wolność Rosji odwiedzają zatrzymanych byłych rosyjskich wojskowych w celu wybrania tych, którzy chcą walczyć po stronie Ukrainy. Według źródeł ukraińskich rekrutacja odbywa się pośród rosyjskich jeńców i dezerterów lub emerytowanych żołnierzy Sił Zbrojnych Federacji Rosyjskiej na zasadzie dobrowolności i pisemnego zgłoszenia, jednak do oddziału rekrutują się także Białorusini. Przedstawiciele legionu zapewniają, że w jego skład wchodzi czynny i emerytowany personel wojskowy nie tylko z Rosji, ale także z innych krajów. Żołnierze są następnie weryfikowani przez ukraińskie służby bezpieczeństwa i kontrwywiad. Wśród „kilkuset" Rosjan, którzy zapisali się do legionu, znaleźli się zarówno żołnierze szeregowi, jak i oficerowie. Ogłoszono także, że wszystkim bojownikom będą przysługiwać te same przywileje co żołnierzom ukraińskim.

Obecnie istnieją 3 sposoby dołączenia do legionu. Po pierwsze, dowódcy sami przychodzą do jeńców rosyjskich i wybierają odpowiednich kandydatów. Po drugie, zainteresowani mogą zgłaszać się do ambasad Ukrainy w Gruzji, Azerbejdżanie lub w dowolnym kraju europejskim. Wreszcie, ostatnią opcją jest skontaktowanie się z kuratorami legionu w regionach Rosji w celu „wzięcia udziału w pokojowym oporze" w miejscu zamieszkania. Przed wstąpieniem w szeregi jednostki należy przejść test wykrywaczem kłamstw, zaliczyć badania psychologiczne oraz uzyskać aprobatę osób decyzyjnych. Początkowo ochotnicy mieli walczyć w rosyjskim umundurowaniu, jednak na początku kwietnia 2022 r. otrzymali ukraińskie mundury. Początkowo otrzymywali proste zadania, nie dostawali broni, ale później, gdy zaufanie do nich wzrosło, otrzymali broń i misje bojowe.

W pierwszych dniach po ogłoszeniu powstania legionu jego członkowie pozostawali anonimowi, ale pod koniec marca zaczęły pojawiać się filmy z „apelami Rosjan", którzy chcą walczyć za Ukrainę. W tych przypadkach twarze rekrutów nie były ukrywane, ujawnili się m.in. Anatolij Zyrenow, Iwan Mylnikow (obaj z jednostek wojskowych w Cchinwali, w Osetii Południowej), Aleksiej Skameikin, Nikołaj Ocherin, Nikołaj Szyszkarej, Dmitrij Pustovetow (wszyscy z Szali, w Czeczenii), Anatolij Semekin (Millerowo, obwód rostowski), Siergiej Kosik (Kursk), Maksym Lesniczenko (Ussurijsk) i inni.

W czerwcu do legionu dołączył Igor Wołobujew, urodzony w Ukrainie, były wiceprezes Gazprombanku (trzeciego co do wielkości banku Rosji powiązanego z naftowym gigantem), który po inwazji opuścił Rosję, wstąpił do legionu Wolności Rosji w ramach Sił Zbrojnych Ukrainy. W rozmowie z pisarzem Siergiejem Lojką dla „The Insider" powiedział, że urodził się w Ochtyrce, w obwodzie sumskim i zdecydował się wrócić do Ukrainy, aby bronić swojego rodzinnego kraju. „Nie mogłem dłużej znieść pozostania w Rosji. Jestem etnicznym Ukraińcem, urodzonym w Ochtyrce i nie mogłem pozostać z boku, obserwując, jak Rosja pustoszy moją ojczyznę. Moja wizyta jest aktem pokuty. Chcę się oczyścić z mojej rosyjskiej przeszłości. Pozostanę w Ukrainie aż do jej zwycięstwa" – zapowiedział Wołobujew.

Agresję Rosji na Ukrainę określił jako zbrodnię wojenną. „Ta zbrodnia jest popełniana przez Putina, rosyjski rząd i w rzeczywistości naród rosyjski. Bo to nie Putin zabija tutaj Ukraińców, plądruje domy i gwałci kobiety. To naród rosyjski. I choć jestem etnicznym Ukraińcem, to też jestem za to odpowiedzialny. Wstydzę się i spędzę resztę życia, pokutując, ponieważ moja część odpowiedzialności jest dwukrotnie większa: nie jestem tylko obywatelem Rosji. Urodziłem się (w Ukrainie) i mieszkałem tu przez 18 lat, więc moja odpowiedzialność jest 2, 3 razy większa" – powiedział Wołobujew.

29 lipca 2022 r. w ramach legionu sformowano drugi batalion, jednak ze względów bezpieczeństwa nie podano jego dokładnej wielkości. Bojownicy podkreślili, że na terytorium Ukrainy nie jest prowadzona żadna operacja specjalna: toczy się prawdziwa wojna z ludnością cywilną.

Rosyjski polityk opozycyjny, deputowany Dumy Państwowej w latach 2007–2016 Ilja Ponomariow, który obecnie mieszka na emigracji i reprezentuje tę jednostkę, powiedział, że legion liczy około 500 osób i podkreślił, że nie ma tam dominującej ideologii. Według niego to prototyp przyszłej armii Federacji Rosyjskiej: za jej zaletę uważa fakt, że nie jest ani lewicowa, ani prawicowa, ani liberalna, ani konserwatywna. Według Ponomariowa jej członków jednoczy idea oporu wobec agresji Rosji.

Jesienią 2022 r. legion otrzymał własną artylerię i w jej ramach zaczął formować się trzeci batalion. Jednocześnie jednostka brała udział w obronie Bachmuta, w obwodzie donieckim.

Struktura legionu Wolność Rosji:

- samodzielny batalion zmechanizowany;
- batalion artylerii;
- zespół bezzałogowego statku powietrznego (drony), w skład którego wchodzą:
- 3 obliczenia baterii moździerzy;
- 2 pluton kompanii uderzeniowej.

Grupa bezzałogowych statków powietrznych „Lasar's":

- pluton BSP;
- 1 pluton baterii moździerzy;
- 2 pluton baterii moździerzy;
- 1 kompania grupy szturmowej;
- 2 kompania grupy szturmowej;
- 1 kompania bezzałogowych statków powietrznych;
- kompanie uderzeniowe kompleksów bezzałogowych statków powietrznych.

Pluton bezzałogowych statków powietrznych Groza:

- 2 batalion skrzydła zbrojnego;
- kompania łączności;
- kompania medyczna;
- kompania radarowa;
- batalion czołgów.

Według różnych informacji legion Wolność Rosji walczył u boku armii ukraińskiej w Donbasie podczas ofensywy we wschodniej Ukrainie. Jednostka ma być także odpowiedzialna za podpalenia i akcje dywersyjne

na terenie Rosji, choć sam legion temu zaprzecza, przypisując takie działania obywatelom rosyjskim sprzeciwiającym się wojnie. Ponadto legion wielokrotnie brał udział w rajdach na tereny przygraniczne Federacji Rosyjskiej wraz z Rosyjskim Korpusem Ochotniczym.

W marcu 2023 r. Sąd Najwyższy Rosji uznał legion za grupę terrorystyczną, co oznacza, że obywatelom, którzy do niej dołączą, grozi do 20 lat więzienia. Rosyjska Prokuratura Generalna przekonywała, że legion został powołany do „obalenia rządu".

22 maja 2023 r. podano, że legion Wolność Rosji i Rosyjski Korpus Ochotniczy przekroczyły ukraińsko-rosyjską granicę i wkroczyły do obwodu biełgorodzkiego – ich celem było utworzenie wzdłuż granicy strefy zdemilitaryzowanej, aby powstrzymać ostrzał rosyjskiej artylerii z terytorium Rosji na Ukrainę oraz odciągnięcie wojsk rosyjskich od innych części frontu i zachęcenie do buntu przeciwko rosyjskiemu rządowi. W ataku miały brać udział artyleria oraz pojazdy opancerzone. Celem uderzenia były m.in. budynki FSB i MSW w Biełgorodzie. Zostało to potwierdzone przez Dmitrija Pieskowa. Strona ukraińska nie przyznała się do przeprowadzenia ataku na terytorium Rosji, a odpowiedzialnością za niego obarczono „oddziały partyzanckie".

12 marca 2024 r. legion wraz z 2 innymi proukraińskimi bojówkami rosyjskimi, Rosyjskim Korpusem Ochotniczym i Batalionem Syberyjskim dokonał nalotu na południową Rosję; meldował, że ma pod kontrolą wieś Tetkino, na pograniczu kurskim. Rosyjski Korpus Ochotniczy potwierdził atak i wsparcie ze strony Batalionu Syberyjskiego, będącego częścią utworzonej w 2023 r. armii ukraińskiej, składającej się z żołnierzy rosyjskich, którzy uciekli na Ukrainę. Atakami antykremlowscy bojownicy chcieli wysłać sygnał przeciwko reżimowi Putina w kontekście wyborów prezydenckich w Rosji kilka dni później. Omawiając operację 12 marca, jeden z ochotników legionu twierdził, że ostatecznie poprowadzą oni „marsz na Moskwę".

Jednocześnie nie ma obiektywnych, możliwych do sprawdzenia informacji na temat legionu i jego roli w działaniach wojennych w domenie publicznej, co w razie potrzeby można łatwo wytłumaczyć koniecznością zachowania tajemnicy wojskowej. Jasne jest, że rzeczywiście znajduje się

on pod kuratelą państwa ukraińskiego, a jego członkowie mają wyraźnie oficjalny status.

Rosyjskie media państwowe tylko jeden raz w filmie wspominały o legionie Wolność Rosji – w 2022 r. Żołnierze legionu mieli powiedzieć: „Jesteśmy na granicy z Rosją – czekaj, Putin, idziemy po twoją głowę", po czym obok słychać eksplozję. Na nagraniu nie widać szczegółów umundurowania (przede wszystkim szewronów), które wskazywałyby, że żołnierze ci należą do legionu Wolność Rosji.

Istnieje teoria, że legion Wolności Rosji jest ukraińskim projektem informacyjnym i w rzeczywistości taka formacja bojowa nie istnieje. Pojawiła się ona niedługo po wiadomości o sformowaniu jednostki. Rozpowszechniają ją kontrolowane przez państwo rosyjskie media i prokremlowskie kanały Telegramu, które nazywają legion fałszywym lub twierdzą, że został stworzony przez ukraiński wywiad. Zwolennicy tej wersji przytaczają następujące dowody:

- brak informacji o udziale legionistów w rzeczywistych działaniach wojennych i wypowiedziach ukraińskich urzędników;
- trudności z weryfikacją zdjęć i filmów, „intymność" materiałów wideo – żołnierze legionu praktycznie nie wchodzą w interakcje z innymi jednostkami armii ukraińskiej (są wyjątki, np. najpopularniejszym postem na kanale legionu jest zdjęcie przedstawiające legionistę, ukraińskiego żołnierza i członka jednostki ochotniczej z Białorusi);
- „cechy językowe", które zdaniem niektórych użytkowników portali społecznościowych pokazują, że autorzy tekstów w wiadomościach wideo nie posługują się językiem rosyjskim jako ojczystym;
- pewne niespójności w działaniach ukraińskiego kierownictwa, np. 5 dni przed pierwszym ogłoszeniem utworzenia legionu portal prezydenta Ukrainy ogłosił uruchomienie strony internetowej ze szczegółowymi instrukcjami dla obcokrajowców, którzy chcą bronić kraju.

Władze kraju agresora przez całą inwazję na pełną skalę aktywnie zaprzeczały istnieniu legionu Wolność Rosji i Rosyjskiego Korpusu Ochotniczego. Twierdziły, że grupy te zostały wymyślone przez Ukrainę

w ramach operacji informacyjno-psychologicznej przeciwko Rosjanom. Jednak ostatnie wydarzenia w obwodzie biełgorodzkim uciszyły propagandystów Putina, ponadto obie grupy już prawie 3 lata działają w ramach Międzynarodowego Legionu Obrony Terytorialnej Ukrainy, w skład którego wchodzą nie tylko Rosjanie, ale także Białorusini, Gruzini, Anglicy, Amerykanie i obywatele innych krajów. Bojownicy z całego świata jadą do Ukrainy, aby chronić kraj przed Putinem i ramię w ramię obalić jego reżim.

W maju i na początku czerwca 2023 r. legion Wolności Rosji dał wyraz swoim głośnym działaniom, dokonując rajdu na terytorium Federacji Rosyjskiej, zajmując przygraniczne wsie w obwodzie biełgorodzkim i podejmując walkę z rosyjskimi siłami zbrojnymi, zaś w marcu 2024 r., tuż przed wyborami prezydenckimi w Rosji, doszło do nalotu na obwody biełgorodzki i kurski.

W szeregach legionu stoją ramię w ramię Rosjanie i Tatarzy, Kałmucy i Dagestańczycy, prawosławni i muzułmanie, zwykli robotnicy i naukowcy – ludzie różnych narodowości i religii, którzy zjednoczyli się przeciwko tyranii. Ostatecznym ich celem jest obalenie rosyjskiego reżimu.

Olga Wasiuta

B. Cole, *Former Russian Soldiers Join Ukraine Against Putin's Invasion*, 30.03.2022, https://www.newsweek.com/russia-ukraine-defense-kyiv-troops-change-sides-freedom-1693274 (dostęp 27.04.2025); A. Ferris-Rotman, *The Russians Fighting Putin in Ukraine*, 8.04.2022, https://time.com/6165422/russians-in-ukraine/ (dostęp 5.09.2024); *Former Gazprombank executive Igor Volobuev joins the Freedom to Russia Legion within the Ukrainian Armed Forces*, 11.06.2022, https://novayagazeta.eu/articles/2022/06/11/former-gazprombank-executive-igor-volobuev-joins-the-freedom-to-russia-legion-within-the-ukrainian-armed-forces-news (dostęp 7.05.2025); *Gazprombank executive Igor Volobuev leaves for Ukraine to join territorial defense, says his colleague's "suicide" was murder*, 27.04.2022, https://theins.ru/en/news/250667 (dostęp 7.05.2025); M. Godwin, *A War of Words: The "Z" and the "L"*, 19.05.2022, https://georgiatoday.ge/a-war-of-words-the-z-and-the-l/ (dostęp 20.05.2025); J. Lasota-Krawczyk, *Rosjanie przechodzą do ukraińskiej armii. Powstał legion „Wolna Rosja"*, 30.03.2022, https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-rosjanie-przechodza-do-ukrainskiej-armii-powstal-legion-woln,nId,5927391#crp_state=1 (dostęp 27.04.2025); *Pro-Kyiv Russian group says it 'didn't lose a single soldier' in cross-border raids on Belgorod*, 24.05.2023,

https://www.france24.com/en/tv-shows/the-interview/20230524-pro-ukraine-group-didn-t-lose-a-single-soldier-in-cross-border-raids-leader-says (dostęp 15.05.2025); *Russian Supreme Court Deems Freedom of Russia Legion Terrorist Organization*, 16.03.2023, https://www.themoscowtimes.com/2023/03/16/russian-supreme-court-deems-freedom-of-russia-legion-terrorist-organization-a80516 (dostęp 7.05.2025); S. Satanowski, *Rosjanie w ukraińskiej armii. Kim są i czego chcą dla Rosji?*, 14.03.2024, https://www.dw.com/pl/rosjanie-w-ukraińskiej-armii-kim-są-i-czego-chcą-dla-rosji/a-68525923 (dostęp 7.05.2025); S. Sivtsova, *A new symbol of Russia's anti-war movement. Meduza explains the origins of the white-blue-white flag*, 16.03.2022, https://meduza.io/en/feature/2022/03/16/a-new-symbol-of-russia-s-anti-war-movement (dostęp 20.05.2025); M. Weiss, J. Rushton, *Pro-Ukrainian Russian partisans advance into Russia's Belgorod region in surprise raid A lightning raid that stuns Moscow*, 22.05.2023, https://www.yahoo.com/news/pro-ukrainian-russian-partisans-advance-into-russias-belgorod-region-in-surprise-raid-172049892.html (dostęp 7.05.2025); В. Рассохов, *Боец Легиона «Свобода России»: «Вытаскивать Путина за шкирку из Кремля – это наша задача»*, 12.01.2025, https://www.lrt.lt/ru/novosti/17/2457568/boets-legiona-svoboda-rossii-vytaskivat-putina-za-shkirku-iz-kremlia-eto-nasha-zadacha (dostęp 10.02.2025); *История Легиона*, https://legionliberty.army/about/ (dostęp 20.05.2025); *Легион «Свобода России»*, https://t.me/s/legionoffreedom/19 (dostęp 12.06.2025); І. Бойко, *Російські військові з легіону «Вільна Росія», які воюють за Україну, дали брифінг (відео)*, 05.04.22, https://www.unian.ua/war/brifing-rosiyskih-viyskovih-z-legionu-vilna-rosiya-yaki-voyuyut-za-ukrajinu-onlayn-translyaciya-novini-vtorgnennya-rosiji-v-ukrajinu-11773870.html (dostęp 27.04.2025); М. Гвадзабия, *Легион «L» – россияне, воюющие на стороне Украины*, 4.05.2022, https://ru.netgazeti.ge/36743/ (dostęp 19.04.2025); Р. Попков, *«Русский добровольческий корпус», «Легион» и ССО «Азов». Как россияне воюют против Кремля на стороне Украины*, 24.08.2022, https://vot-tak.tv/novosti/24-08-2022-rossiyane-voyuyut-za-ukrainu (dostęp 13.06.2025).

LINGUA FRANCA (innymi słowy język wiodący) – w naukach o bezpieczeństwie język angielski. Jego status wynika z globalnego charakteru współpracy w dziedzinie bezpieczeństwa, w tym w ramach organizacji międzynarodowych, takich jak NATO, gdzie angielski jest językiem używanym do zapewnienia wspólnego porozumienia i zdolności do współdziałania (interoperacyjności) w misjach międzynarodowych.

Znajomość języka angielskiego jest kluczowa dla specjalistów ds. bezpieczeństwa IT i cyberbezpieczeństwa, ponieważ umożliwia dostęp

do ważnych informacji o zagrożeniach i nowych technologiach. Język jest podstawą formułowania pojęć, precyzowywania terminów, a także w bardziej praktycznych sferach przekłada się na zrozumienie decyzji oraz wykonywanie poleceń czy rozkazów. Często przyczyną nieporozumień są błędy językowe czy niewłaściwe tłumaczenie z języków obcych. Życie społeczne wymaga języka, który odzwierciedli naszą tożsamość, wyjaśni uwarunkowania kulturowe i pozwoli na identyfikację w świecie. Jest wyrazicielem ideologii, motywacją do działania. Może decydować o wojnie lub pokoju pomiędzy narodami. W rozumieniu bezpieczeństwa jego znaczenie wykracza poza funkcje, jakie pełni w nauce. Odgrywa istotną rolę w polityce bezpieczeństwa.

Trzeba też podkreślić, że chociaż wiedza na temat bezpieczeństwa jest publikowana w wielu językach, to właśnie angielski jest najpopularniejszy w publikacjach krajowych i międzynarodowych. Większość recenzowanych czasopism naukowych, konferencji międzynarodowych i współpracy badawczych w dziedzinie nauk o bezpieczeństwie i stosunków międzynarodowych wykorzystuje angielski jako główny lub jedyny język dyskursu. Czasopisma takie jak „Security Science Journal" czy „Security and Defence Quarterly" wymagają od autorów nadsyłania manuskryptów w języku angielskim.

Słowniki zazwyczaj podają dwa znaczenia określenia *lingua franca*. Pierwsze, odpowiadające współczesnemu rozumieniu w naukach o bezpieczeństwie, to wspólny język umożliwiający porozumiewanie się ludziom, którzy na co dzień mówią różnymi językami. Często określany jest jako pomostowy, uniwersalny lub roboczy, używany w handlu, nauce i dyplomacji, z angielskim jako obecnie najważniejszym globalnym przykładem. Drugie znaczenie – historyczne – to gwara złożona z elementów języka francuskiego, włoskiego, hiszpańskiego, greckiego i arabskiego, używana w portach Morza Śródziemnego. Nazwa pochodzi od włoskiego „języka Franków", czyli średniowiecznych kupców śródziemnomorskich łączących w mowie elementy włoskie i francuskie.

Generalnie jest to język używany do porozumiewania się różnych grup, umożliwiający komunikację w wielonarodowym środowisku.

Pomimo różnorodności językowej na świecie, przy około 6 tys. znanych i używanych języków, ludzkość poszukiwała możliwości

utworzenia czy też uzgodnienia wspólnego kodu, który ułatwiałby komunikację pomiędzy mieszkańcami rożnych społeczności, wykraczających poza jeden krąg kulturowy. Potrzeba wspólnego języka sprawiła, że nasz rodak Ludwik Zamenhof stworzył język uniwersalny – esperanto, o bardzo prostym systemie gramatycznym pozbawionym wyjątków, którego słownictwo wywodzi się z języków indoeuropejskich zgodnie z zasadą, że dane słowo powinno mieć korzenie w kliku językach. Chociaż zainteresowanie esperanto było bardzo duże (przetłumaczono m.in. Biblię i parę innych arcydzieł), nie zdobyło statusu języka globalnego.

Łacina była pierwszym w historii językiem globalnym, dominującym głównie ze względów religijnych jako oficjalny język chrześcijaństwa aż do Soboru Watykańskiego II (1965). Od IV w. n.e. łacina stała się dominującym językiem liturgicznym Kościoła katolickiego, zastępując grekę w zachodniej części Cesarstwa Rzymskiego. Z biegiem czasu stała się językiem oficjalnym Kościoła, obecnym w liturgii, sakramentach, kanonie mszy świętej, pismach ojców Kościoła, encyklikach i dekretach papieskich. W tej funkcji łacina trwała przez ponad 1500 lat, aż do reform Soboru Watykańskiego II w latach 60. XX w., kiedy to wprowadzono języki narodowe do liturgii. Mimo to do dziś zachowała status języka urzędowego Watykanu. Wraz z rosnącą potęgą Rzymu łacina zaczęła pełnić funkcję języka administracyjnego, prawnego i wojskowego, obejmując swoim zasięgiem całą Italię, a następnie inne regiony Imperium Rzymskiego – od Hiszpanii po Bliski Wschód. W okresie średniowiecza również w Polsce łacina przejęła rolę *lingua franca* – uniwersalnego języka komunikacji elit duchownych, intelektualnych i politycznych w całej Europie. Jej znajomość była konieczna do prowadzenia dyplomacji, pisania traktatów, prowadzenia kronik, nauczania i kontaktów z instytucjami kościelnymi. W świecie, gdzie większość społeczeństwa była niepiśmienna, język łaciński był kluczem do wiedzy i władzy.

W XVII w. francuski wyparł łacinę jako główny język komunikacji międzynarodowej, a traktaty i dokumenty zaczęto spisywać po francusku. Kongres wiedeński (1815) umożliwił porozumienie po wojnach napoleońskich, potwierdzając rolę języka francuskiego. Również rozwój literatury i filozofii (Moliere, Kartezjusz) uczynił go synonimem

klarowności i wyrafinowania, idealnego do negocjacji. Współcześnie francuski jest jednym z języków roboczych ONZ, odgrywa ważną rolę w Międzynarodowym Komitecie Olimpijskim (MKOl) i organizacjach pozarządowych (np. Lekarze bez Granic). Znajomość francuskiego (obok angielskiego) jest często absolutnie niezbędna, sprawdzana na egzaminach i ceniona. Wciąż jest niezbędny dla dyplomatów, używany w oficjalnych dokumentach i ważny w kulturze, na równi z angielskim.

Angielski to *lingua franca* naszych czasów – jego potęga rozpoczęła się już w trakcie kolonizacji. Gdy Anglicy zaczęli wysyłać w świat swoich żeglarzy, żołnierzy, misjonarzy i pielgrzymów, Imperium Brytyjskie było największym mocarstwem na świecie. W roku 1922 Wielka Brytania miała w swoim posiadaniu prawie 1/4 (ponad 22%) terytoriów na globie i ponad 20% populacji ludzkiej. Z czasem kraje, które powoli zaczęły walczyć o swoją niepodległość, i tak zachowały język angielski jako dominujący lub nauczany w szkołach. Krótko po II wojnie światowej język francuski był dominującym językiem dyplomacji i elit intelektualnych, ale został wyparty przez angielski. Szacuje się, że posługuje się nim około 1,4 mld ludzi. Jest prosty gramatycznie, nie wymaga różnicowania form, niezależnie od tego, do kogo się zwracamy (*you*), co znacznie ułatwia komunikację. Być może właśnie te czynniki spowodowały, że angielski prawie naturalnie opanował świat. Znany lingwista David Crystal w książce *English as a global language* twierdzi, że angielski jest językiem globalnym nie dzięki specyficznym cechom, ale za sprawą tego, że znalazł się na właściwym miejscu we właściwym czasie.

Bez wątpienia angielski jest językiem internetu. Ponad połowa wszystkich materiałów zamieszczonych online jest w języku angielskim, podobnie sytuacja wygląda w biznesie, finansach i gospodarce. Organizacje globalne uznają angielski za język oficjalny czy też jeden z oficjalnych, tak samo giełdy, korporacje i stowarzyszenia. Potęga gospodarcza USA i zasięg Imperium Brytyjskiego miały wielki wpływ na pozycję tego języka w świecie. Angielski dominuje również w szeroko pojętej kulturze – w kinie, telewizji, mediach, a także w branży naukowej czy turystyce. Zdecydowana większość czasopism ukazuje się po angielsku, a podróżowanie jest znacznie łatwiejsze, jeśli znamy ten język.

W związku z rozwojem angielskiego jako języka globalnego powstały dwa stosunkowo nowe określenia – WE (World Englishes – światowe odmiany języka angielskiego) i EFL (English as Lingua Franca – angielski jako *lingua franca*). Pierwsze kładzie nacisk na istnienie i stosowanie różnych norm języka angielskiego na całym świecie, podczas gdy drugie skupia się na interakcjach między użytkownikami języka angielskiego. Są one jednak ściśle powiązane, ponieważ potrzeba dostosowania się w celu zapewnienia skutecznych interakcji z perspektywy ELF obejmuje już akceptację różnych odmian języka angielskiego.

Język angielski to współczesny *lingua franca* i na razie nic nie wskazuje, aby szybko utracił swoją dominującą rolę. Oczywiście wszystko zależy od konkretnych okoliczności, jednak zmiany w języku zachodzą na ogół stopniowo i subtelnie na przestrzeni pokoleń, podczas gdy wydarzenia polityczne i gospodarcze mogą postępować w znacznie szybszym, czasem gwałtownym tempie.

Anna Kochnowska

Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/lingua-franca (dostęp 9.01.2026); D. Crystal, *English as a Global Language*, CUP, Cambridge 2003; *English Dominance and Its Influence on International Communication*, https://www.academypublication.com/issues/past/tpls/vol03/12/16.pdf (dostęp 10.01.2026); *The Importance of The English Language in Public Diplomacy and International Relations*, https://www.researchgate.net/publication/358326707_THE_IMPORTANCE_OF_THE_ENGLISH_LANGUAGE_IN_PUBLIC_DIPLOMACY_AND_INTERNATIONAL_RELATIONS (dostęp 12.01.2026); J. Jenkins, *Global Englishes*, Routledge, New York 2015; *Język w dyskursie o bezpieczeństwie*, „Studia Administracji i Bezpieczeństwa" 2020, t. 9, nr 9; I. Kurcz, H. Okuniewska, *Język jako przedmiot badań psychologicznych: psycholingwistyka ogólna i neurolingwistyka*, Wydawnictwo SWPS Academica, Warszawa 2011; *The Role of English as a Global Language*, https://www.researchgate.net/publication/334282978_THE_ROLE_OF_ENGLISH_AS_A_GLOBAL_LANGUAGE (dostęp 11.01.2026); *Słownik języka polskiego*, https://sjp.pwn.pl/sjp/lingua-franca;2566109.html#google_vignette (dostęp 9.01.2026); *Use of Ambiguities in Peace Agreements*, https://www.jura.fu-berlin.de/fachbereich/einrichtungen/oeffentliches-recht/lehrende/bolewskiw/dokumente/7__Culture_Language/Pehar_use_of_ambiguities_in_peace_agreements.pdf (dostęp 11.01.2026); *World Englishes (WE) and English as Lingua Franca*

(ELF): Implications for English Teaching and Learning, https://www.researchgate.net/publication/340714159_World_Englishes_WE_and_English_as_Lingua_Franca_ELF_Implications_for_English_Teaching_and_Learning (dostęp 10.01.2026).

LLM GROOMING – proces manipulacji wyników dużych modeli językowych (oznaczanych akronimem LLM od ang. Large Language Models) poprzez fałszowanie zbiorów danych treningowych w celu spowodowania wystąpienia dezinformujących treści, ich normalizacji bądź wzmocnienia. Termin jest używany przede wszystkim do opisania dezinformacyjnej aktywności rosyjskiej sieci Pravda. Założenia i przebieg operacji zostały udokumentowane na przełomie 2024 i 2025 r. Poprzez multiplikację treści dezinformujących cyrkulujących online Pravda wpływa na wyniki generowane przez popularne duże modele językowe, takie jak np. ChatGPT, Claude czy Gemini.

Termin *grooming* w swoim tradycyjnym rozumieniu odnosi się do manipulacyjnych zachowań osób, które budują zaufanie ofiar – często nieletnich – w celu ich przygotowania do późniejszych nadużyć. W kontekście sztucznej inteligencji *grooming* rozszerza tę koncepcję o proces warunkowania modeli do dostarczania treści oczekiwanych przez wdrażających szkodliwą strategię. Technika jest innowacyjna i wykorzystuje luki w architekturze systemów opartych na pracy transformerów, które nie posiadają mechanizmów weryfikacji prawdziwości danych treningowych ani zdolności rozróżniania intencji źródeł, przez co mogą bezrefleksyjnie przyswajać i wzmacniać treści zmanipulowane lub dezinformujące.

Sensu largo zjawisko LLM groomingu mogłoby obejmować zarówno próby trenowania w konkretny sposób lub „nakłaniania" modeli, by te generowały nieodpowiednie treści, jak również interakcje z modelami mające na celu ominięcie wbudowanych protokołów bezpieczeństwa lub kształtowanie wzorców reakcji modelu poprzez multiplikację niewłaściwych podpowiedzi. Takie działania przypominałyby rozpoznane wcześniej metody wpływania na LLM jak *prompt injection* czy *model poisoning*. Na ten moment jednak *LLM grooming* jest wiązany w literaturze bezpośrednio ze strategią stosowaną przez twórców sieci Pravda, co nie oznacza, iż w przyszłości nie może stać się terminem ogólnym obejmującym więcej szkodliwych działań.

Odkrycie tego schematu może stanowić impuls do jego powielania przez innych państwowych i pozapaństwowych aktorów dezinformacji, zwłaszcza wobec wyników dochodzeń przeprowadzonych przez organizacje American Sunlight Project i NewsGuard w latach 2024–2025, z których wynika, iż Pravda była w stanie wpłynąć na znaczną część wyników generowanych przez popularne LLM. Z drugiej strony, może także przyczynić się do wbudowywania lepszych zabezpieczeń w architekturze dużych modeli językowych. *LLM grooming* stanowi bowiem istotne zagrożenie dla integralności, bezpieczeństwa i wiarygodności informacji oraz rzetelności wybranych systemów sztucznej inteligencji.

Pravda (znana także jako Portal Kombat) to skoordynowana sieć kilkuset prorosyjskich stron internetowych publikujących treści w wielu językach. Często naśladują one serwisy informacyjne lub blogi polityczne, stwarzając wrażenie wiarygodności i bezstronności. W wielu wypadkach publikacje są tłumaczone automatycznie z języka rosyjskiego przy wykorzystaniu narzędzi sztucznej inteligencji. Zasadnicza część publikacji powiela oficjalne narracje z rosyjskich źródeł rządowych i okołorządowych, regularnie odwołując się do treści propagandowych, dezinformujących i wprost fałszywych. Multiplikacja publikacji umożliwia, z jednej strony, docieranie do ludzkich czytelników i rozpowszechnianie rosyjskiej dezinformacji, a z drugiej – jest obliczona na zapełnianie zbiorów danych szkoleniowych dużych modeli językowych konkretnymi materiałami z założeniem, iż będą one później odzwierciedlone w treściach przez nie generowanych. Sama treść publikacji Pravdy charakteryzuje się dużą objętością i jest dostosowana do specyfiki pracy dużych modeli językowych. Jakość publikowanych tekstów jest niska, co po części wynika z mechanizmów tworzenia i powielania.

Francuska agencja dezinformacyjna Viginum (2024) wskazała, iż Pravda została założona na okupowanym przez Rosjan Krymie w 2015 r. Jej administratorem jest firma TigerWeb kontrolowana przez *Yevgenya* Shevchenka. Sieć notuje stały wzrost liczby stron internetowych wchodzących w jej skład oraz atakowanych krajów.

Na początku 2024 r. rosyjscy specjaliści od wojny informacyjnej zidentyfikowali możliwość stopniowego „zatruwania" danych treningowych dużych modeli językowych poprzez multiplikowanie określonych treści.

To założenie jest oparte na słusznej obserwacji odzwierciedlania określonych światopoglądów przeważających w zbiorach danych treningowych w danych wyjściowych dużych modeli językowych. Badania wykazały, iż tego typu modele tworzone przez firmy z demokratycznych jurysdykcji znacznie częściej pozytywnie odnoszą się do wartości demokratycznych, podczas gdy modele z krajów autorytarnych promują inny światopogląd. Pod względem technicznym jest to efekt zasadniczej strategii pozyskiwania danych do uczenia dużych modeli językowych, która polega na skanowaniu sieci i tzw. web scrapingu – im więcej danych z określonego obszaru, tym większe prawdopodobieństwo ich pośredniego odtwarzania.

W konsekwencji w samym 2024 r. Pravda opublikowała ponad 3,6 mln artykułów w różnych wersjach językowych. Te zaczęły przenikać do danych treningowych dużych modeli językowych, a następnie wpływać na generowane przez nie wyniki. To może mieć charakter bezpośredni, gdy źródła wchodzące w skład sieci Pravda są cytowane wprost, bądź też pośredni, gdy dezinformacyjne tezy są powielane w danych wyjściowych.

Na przełomie 2024 i 2025 r. badacze American Sunlight Project oraz NewsGuard przeprowadzili wiele eksperymentów, udowadniając, iż duże modele językowe średnio w 33% przypadków powielają tezy rosyjskiej dezinformacji (testowano 15 najpopularniejszych narracji). To zjawisko atrybuowano w dużej mierze aktywności sieci Pravda. Co istotne, wraz z dalszą multiplikacją dezinformacyjnych treści nowe generacje modeli mogą być jeszcze bardziej podatne na tego typu manipulacje. Wskazuje to na (przynajmniej teoretyczną) skuteczność LLM groomingu jako formy pośredniego warunkowania modeli. Strategia ta pozwala omijać tradycyjne zabezpieczenia w postaci moderacji lub filtrowania treści, a efekt skali sprawia, że są one szczególnie trudne do wykrycia lub retroaktywnego złagodzenia.

Badania American Sunlight Project oraz NewsGuard wykazały także pewną odporność dużych modeli językowych – w 48% przypadków były bowiem w stanie demistyfikować dezinformacyjne narracje rozpowszechniane przez Pravdę.

Kluczowe cechy LLM groomingu realizowanego przez sieć Pravda obejmują zatem:

- skalę i nasycenie rozpowszechniania – treści są dystrybuowane na skalę masową, w wielu krajach i domenach, aby zwiększyć prawdopodobieństwo wejścia w skład danych treningowych dużych modeli językowych;
- wielojęzyczność – automatyczna translacja pozwala na dotarcie do odbiorców w wielu krajach, a jednocześnie tworzy złudzenie powszechności konkretnych tez i dezinformacyjnych narracji;
- manipulacje semantyczne – dezinformacja jest osadzona w strukturalnie neutralnych lub nieszkodliwych formatach, takich jak podsumowania czy pseudonaukowe analizy, co ma zwiększać jej wiarygodność;
- ukierunkowanie treści na sztuczną inteligencję – strony internetowe są skonstruowane w taki sposób, by ułatwić wyszukiwanie i indeksowanie przez automatyczne systemy, z kolei kody są zoptymalizowane pod kątem algorytmicznego przetwarzania;
- multiplikacje – treści publikowane przez Pravdę są udostępniane w mediach społecznościowych i komunikatorach, co sprzyja dalszemu rozpowszechnianiu dezinformacji.

LLM grooming wprowadza także nowy wektor operacji wpływu nakierowany na „pranie" dezinformacyjnych treści. Podchwycenie tego rodzaju narracji przez duże modele językowe sprawia bowiem, iż treści pojawiają się ponownie za pośrednictwem zaufanych interfejsów sztucznej inteligencji, zazwyczaj pozbawione znaczników określających źródło danych. W skrajnym przypadku może dojść do internalizacji stronniczych poglądów przez sam model, a to prowadzi z kolei do naruszenia integralności i wiarygodności informacji zwracanych przez duże modele językowe. W dłuższej perspektywie może to przyczynić się do erozji epistemicznej i obniżyć ogólną wiarygodność dużych modeli językowych postrzeganych jako systemy podatne na manipulacje.

Grooming na poziomie LLM budzi poważne obawy z punktu widzenia bezpieczeństwa cyfrowego i bezpieczeństwa informacji. Wraz ze wzrostem dostępności i powszechności wykorzystania modeli językowych rośnie ryzyko, że będą one celem, a następnie narzędziem daleko idących manipulacji obliczonych na kształtowanie poglądów użytkowników korzystających z zaatakowanych modeli. Problem LLM groomingu łączy zatem

sfery cyberbezpieczeństwa (pod kątem zabezpieczenia systemów jako istotnego elementu infrastruktury cyfrowej, ale także gwarantowania ich niezawodności i rzetelności) oraz bezpieczeństwa informacji (pod kątem prawdziwości informacji i zagrożenia dezinformacją).

Odkrycie istotnych podatności może być również impulsem do rozwijania narodowych dużych modeli językowych, których trening jest poddany większej kontroli, a dane treningowe – bardziej starannie selekcjonowane. Z drugiej strony, może to prowadzić do negatywnego zjawiska nacjonalizacji dużych modeli językowych, stawiając pod znakiem zapytania ich obiektywizm.

Mateusz Łabuz

A Pro-Russia Content Network Foreshadows the Automated Future of Info Ops, American Sunlight Project, Waszyngton 2025; M. Buyl, *Large Language Models Reflect the Ideology of Their Creators*, „Arxiv" 2024; V. Châtelet, A. Lesplingart, *Russia's Pravda network in numbers: Introducing the Pravda Dashboard*, DFRLab, 2025; *The Infection of Western AI Chatbots by a Russian Propaganda Network*, NewsGuard, Nowy Jork 2025; J. Kubś, *Global Offensive: Mapping the Sources Behind the Pravda Network*, GLOBSEC, Bratysława 2025; D. Lyndell, *Poster boy: Six instances of Kremlin disinformation amplified through Elon Musk's social network*, https://theins.ru/en/politics/279574 (dostęp 15.07.2025); M. Łabuz, M. Schulze, *KI-Hintertür in die Demokratie*, „Tagesspiegel Background Cybersecurity" 2025; *Nearly 300 contents published in five days: how the Russian network Pravda takes advantage of the Torre Pacheco riots and spreads disinformation*, https://maldita.es/investigaciones/20250717/300-publications-pravda-torre-pacheco/ (dostęp 18.07.2025); *Portal Kombat. A structured and coordinated pro-Russian propaganda network*, General Secretariat for Defence and National Security, Paryż 2024.

LOS ZETAS – meksykański kartel narkotykowy (aktywny głównie w północno-wschodnich stanach Meksyku, takich jak Tamaulipas, Nuevo León, Coahuila i Veracruz, prowadzący również działalność transgraniczną w kierunku Stanów Zjednoczonych) powstały pod koniec lat 90. XX w. Uznaje się, że jego metody oparte na militaryzacji działań oraz bezprzykładnym terrorze stanowiły niechlubny przełom w funkcjonowaniu zorganizowanej przestępczości narkotykowej w Meksyku. Stały się też

wzorcem dla innych grup, w tym zwłaszcza dla Kartelu Nowej Generacji z Jalisco (Cartel Jalisco Nueva Generacion, CJNG).

Matecznik Los Zetas to stan Tamaulipas. Mając niemal 80 tys. km2 powierzchni, znajduje się na północnym wschodzie państwa, nad Zatoką Meksykańską, graniczące ze Stanami Zjednoczonymi. Jego stolicą jest Ciudad Victoria, zaś inne główne miasta stanowią zwłaszcza ośrodki przygraniczne, takie jak (idąc od wschodu): Matamoros, Reynosa i Nuevo Laredo. Na zachodzie Tamaulipas sąsiaduje ze stanem Nuevo Leon, na południu natomiast – ze stanami San Luis Potosi oraz Veracruz. Tamaulipas jest regionem wydobycia ropy naftowej i gazu ziemnego, ponadto przebiega przez niego ważna strategicznie Droga Panamerykańska.

Geneza powstania kartelu Los Zetas związana jest z innym kartelem z tego regionu o nazwie Cartel del Golfo – CDG (Kartel znad Zatoki); pierwotnie bowiem Los Zetas nie stanowili autonomicznego kartelu – już w latach 30. XX w. Juan Nepomuceno Guerra rozwinął na terenie północno-wschodniego pogranicza ze Stanami Zjednoczonymi szeroką działalność przemytniczą; obejmowała ona zwłaszcza przemyt alkoholu. Guerra w ramach tego procederu utrzymywał kontakty z lokalnymi meksykańskimi politykami, w tym gubernatorami stanu Tamaulipas. Z czasem sieć jego powiązań zaczęła mieć wymiar ogólnokrajowy.

Guerra nawiązał kontakty m.in. z prominentnymi działaczami rządzącej Partii Rewolucyjno-Instytucjonalnej (Partido Revolucionario Institucional, PRI), w tym z ojcem prezydenta Meksyku w latach 1988–1994 Carlosa Salinasa de Gortariego. Od połowy lat 80. XX w. utworzona przez Guerrę organizacja przemytnicza zaczęła angażować się także w przemyt narkotyków. Jego następca, bratanek Juan Garcia Abrego, podjął negocjacje z kolumbijskim kartelem narkotykowym z Cali: w rezultacie na szeroką skalę rozwinął się przemyt zwłaszcza kokainy z Kolumbii poprzez Tamaulipas do Stanów Zjednoczonych. CDG stał się więc pośrednikiem w przemycie narkotyków.

Wedle dostępnych szacunków na przestrzeni lat 1985–1995 kartel stał za przerzutem 5 tys. t kokainy do amerykańskich miast. Wielkie zyski finansowe pozwoliły na rozwinięcie sieci korupcyjnych układów zapoczątkowanych przez Guerrę – w jej skład oprócz polityków wchodzili przedstawiciele organów ścigania, jak również lokalnych mediów. W 1996

r. doszło do zatrzymania Abrego i jego późniejszej ekstradycji do Stanów Zjednoczonych. W rezultacie jego następcą i nowym szefem kartelu został Osiel Cardenas Guillen, który wyeliminował swojego rywala Salvadora Gomeza Herrerę. To właśnie on stał się twórcą Los Zetas, początkowo stanowiących jedynie zbrojne ramię CDG. Wskazuje się, że Cardenas Guillen nie miał tak rozbudowanych wpływów korupcyjnych jak poprzednik, co wymusiło na nim sięgnięcie w szerszym zakresie do przemocy w celu ugruntowania pozycji swojej oraz całego kartelu. Temu celowi miało służyć powołanie Los Zetas, co nastąpiło zapewne w grudniu 1998 r.

Upublicznione przez meksykańskie organy ścigania wyjaśnienia Jesusa Enrique Rejon Aguilara ps. El Mamito Caballero wskazują, że początkowo, w 1999 r. Los Zetas liczyli zaledwie 14 ludzi. W tym samym roku liczba ta wzrosła do około 30. Przewodził im Arturo Guzman Decena (ps. Z-1). Nazwa grupy najprawdopodobniej wzięła się od hasła stosowanego na falach radiowych przez meksykańskich żołnierzy wojsk spadochronowych. Zarówno Decena, jak i pozostali Los Zetas w dużej mierze wywodzili się bowiem z meksykańskiego elitarnego oddziału komandosów GAFE (Grupo Aeromóvil de Fuerzas Especiales – Grupa Powietrzna Sił Specjalnych). Formalnie oddział ten utworzono w 1990 r., choć jego geneza sięga 1986 r., kiedy to Meksyk był organizatorem mistrzostw świata w piłce nożnej. Składał się z wyselekcjonowanych żołnierzy brygady strzelców spadochronowych, którzy następnie zostali przeszkoleniu przez francuską żandarmerię, a w późniejszych latach także siły specjalne Stanów Zjednoczonych czy Izraela. W połowie lat 90. XX w. GAFE brała czynny udział w tłumieniu partyzantki Zapatystowskiej Armii Wyzwolenia Narodowego (Ejército Zapatista de Liberación Nacional, EZLN) w stanie Chiapas. Tak więc zbrojne ramię CDG w postaci Los Zetas zaczęli tworzyć wysoko wyszkoleni i zaprawieni w boju komandosi. Pełnili oni również funkcję gwardii przybocznej Guillena.

Powołanie Los Zetas spowodowało rewolucję w działaniu CDG – głównym wyznacznikiem tej zmiany była militaryzacja sposobu funkcjonowania. Komandosi GAFE zostali przeszkoleni jako małe, mobilne, zdecentralizowane jednostki szybkiego reagowania. Ta spuścizna została następnie zaadaptowana przez Los Zetas na rzecz działalności przestępczej na szeroką skalę; objawiało się to stosowaniem wojskowego wyszkolenia

oraz taktyki, jak również używaniem szerszego spektrum broni, którą nabywano legalnie na terenie Stanów Zjednoczonych, a następnie przemycano do Meksyku. Nie bez znaczenia była również hierarchiczna struktura i bezwzględne posłuszeństwo rozkazom dowódcy.

Los Zetas zaczęli stosować terror kryminalny na bezprecedensową dotąd skalę, nie oszczędzając przy tym ludności cywilnej. Ich znakiem rozpoznawczym stały się zbiorowe egzekucje, nierzadko w skali kilkudziesięciu osób, połączone z ostentacyjnym, publicznym eksponowaniem okrutnie okaleczonych, zwłaszcza poprzez dekapitację, zwłok. Niekiedy do ciał dołączano listy z pogróżkami, by wzmocnić efekt zastraszania lokalnych społeczności. Los Zetas nierzadko też w wyjątkowo sadystyczny sposób torturowali swoje ofiary przed śmiercią, dopuszczając się kastracji czy obdzierania ze skóry. Jak wynika z udostępnionych przez meksykański wymiar sprawiedliwości wyjaśnień, złożonych w charakterze podejrzanego przez Flavio Mendeza Santiago ps. El Amarillo, Z-23, gdy w 1999 r. wstąpił do Los Zetas, został przez Guillena przydzielony do „jaskini". Oznaczało to, że jego rolą był nasłuch połączeń telefonicznych i radiowych członków grupy – chodziło o kontrolę, czy przestrzegają oni ustalonych zasad konspiracji w komunikacji, w tym w szczególności niewskazywania jakichkolwiek adresów czy miejsc pobytu. Zaznaczyć należy, że El Amarillo był 23 członkiem grupy; świadczy to o stosowaniu technik charakterystycznych dla kontrwywiadu i to już na wczesnym etapie ukonstytuowania się grupy. Los Zetas byli również prekursorami w używaniu mediów, w tym elektronicznych, do popularyzacji swoich działań – w internecie udostępniali filmy z przeprowadzanych egzekucji. Nierzadko kierowali listy otwarte do osób publicznych, dziennikarzy czy lokalnych przedsiębiorców ze swoimi przesłaniami zawierającymi liczne pogróżki.

Dzięki działalności Los Zetas Guillen nie tylko skonsolidował władzę w Tamaulipas, ale i dokonał ekspansji poza stan. Jedocześnie udało mu się powstrzymać konkurencyjne kartele z Juarez czy Sinaloa. Szczególnego znaczenia dla CDG miała wyłączność w kontroli nad kluczowym przejściem granicznym ze Stanami Zjednoczonymi – w Nuevo Laredo. W 2002 r. w starciu z meksykańskimi służbami bezpieczeństwa zginął Decena (Z-1), po nim kierownictwo w Los Zetas ostatecznie przejął Heriberto Lazcano Lazcano (Z-3), które sprawował aż do swej śmierci w 2012 r.

Rozwinął on organizację, poszerzając jej zdolności operacyjne, jednocześnie zapoczątkował ekspansję Los Zetas, opanowując kolejne stany, zwłaszcza na kierunku południowym, by finalnie ugruntować swe wpływy również w Gwatemali.

W miarę upływu lat Los Zetas stali się coraz bardziej niezależni od CDG, przestali być jedynie zbrojnym ramieniem kartelu, zaczęli też przyjmować zlecenia od innych grup przestępczych, bazując na swojej renomie bezwzględnych egzekutorów. Proces ten przyspieszyło zatrzymanie w marcu 2003 r. Guillena i jego późniejsza ekstradycja w 2007 r. do Stanów Zjednoczonych. Na przestrzeni lat 2004–2010 Los Zetas wyodrębnili się jako autonomiczny kartel, pozostający jednak w sojuszu z CDG, tworząc tym samym sprzymierzenie nazywane „firmą" (La Compania). Szacuje się, że około 2009 r. Los Zetas mieli w swych szeregach już między 1000 a 3000 członków. Część z nich stanowili zwerbowani byli gwatemalscy wojskowi. Kartel Los Zetas skupił się na podporządkowaniu jak najszerszych połaci terytorium przy przemożnym wykorzystaniu terroru. Nie ograniczał swej działalności jedynie do przemytu i handlu narkotykami, ale kontrolował całokształt wszelkiej działalności przestępczej na danym terenie, zwłaszcza w postaci wymuszeń, handlu ludźmi, sutenerstwa, nielegalnego hazardu, napadów czy kradzieży, w tym ropy naftowej z instalacji państwowego monopolisty paliwowego PEMEX. Nadto przejmował legalne przedsiębiorstwa i wpływał na wyniki przetargów publicznych. Ugruntowywał swe wpływy poprzez korupcyjną infiltrację instytucji państwowych, nie wyłączając organów ścigania. Wymownym przykładem może być przejęcie kontroli nad więzieniem w Piedras Negras, które pełniło rolę nie tylko schronienia i centrum operacyjnego, ale także miejsca egzekucji realizowanych przez kartel. Uzyskiwane przez Los Zetas przychody były prane w różnoraki sposób, niemniej jednak warto wskazać, że proceder ten realizowano chociażby na terenie Stanów Zjednoczonych, wykorzystując hodowle koni wyścigowych i istniejące luki prawne w tym zakresie.

W 2010 r. doszło do rozłamu i otwartej wojny pomiędzy CDG a Los Zetas. Jej przyczyną był narastający konflikt interesów pomiędzy dwoma kartelami, jak również postrzeganie przez Los Zetas Guillena za zdrajcę z uwagi na jego postawę procesową w Stanach Zjednoczonych. Wojna pomiędzy CDG a Los Zetas przyniosła kolejną falę przemocy; w jej

rezultacie na przestrzeni lat 2011–2015 Los Zetas wyrośli na największy kartel narkotykowy w Meksyku, obok Sinaloa. W 2012 r. stery w kartelu, po zabitym w starciu z meksykańskim wojskiem Lazcano Lazcano, przejął Miguel Ángel Trevino Morales (Z-40), który jednak w kolejnym roku został zatrzymany, a wówczas kierownictwo przejął jego młodszy brat Omar Trevino Morales (Z-42), zatrzymany z kolei w marcu 2015 r. Wówczas nastąpił rozpad Los Zetas – w wyniku walk frakcyjnych wyłoniły się organizacje Los Zetas Vieja Escuela (Los Zetas starej szkoły) oraz Cartel del Noreste (Kartel Północno-Wschodni). Ten ostatni uznawany jest za sukcesora większości aktywów Los Zetas.

Jakub Purchla

S. Aguayo, J. Dayan, *Defeating Los Zetas. Organized Crime, The State and Organized Socety in La Laguna, Mexico 2007–2024*, El Colegio de Mexico, Mexico City 2021; G. Correa-Cabrera, *Los Zetas Inc. Criminal Corporations, Energy and Civil War in Mexico*, University of Texas Press, Austin 2017; L.N. Diaz, *The Race Against Los Zetas: How One of The Most Feared Mexican Drug Cartels in History Was Able to Hide Millions in The American Quarter Horse Racing Industry and How the Corporate Transparency Act Could Beat Financial Terrorists to the Finish Line*, „Ohio State Business Law Journal Online" 2022, vol. 1; S. Dudley, *The Zetas and the Battle for Monterrey*, In Sight Crime: Organized Crime on Americas 2012; G.W. Grayson, *The Evolution of Los Zetas in Mexico and Central America: Sadism as an Instrument of Cartel Warfare*, United States Army War College Press, Carlisle 2014; https://encyklopedia.pwn.pl/haslo/3985136 (dostęp 16.12.2025); https://guardianes.net/2025/02/fuerzas-especiales-del-ejercito-mexicano-historia-desafios-y-exitos-en-la-lucha-contra-el-crimen-organizado/; nagrania z 2011 r. z upublicznionych wyjaśnień podejrzanych: Flavio Mendez Santiago „El Amarillo" (Z-23) oraz Jesus Enrique Rejon Aguilar „El Mamiot Caballero" (Z-7), w zbiorach autora; V.M. Sanchez Valdes, M. Perez Aguirre, *The Origin of the Zetas and Their Expansion in Northern Coahuila*, El Colegio de Mexico, Mexico City 2018.

LOTNISKOWIEC – klasa okrętu wojennego, który służy jako morska baza lotnicza wyposażona w pełnowymiarowy pokład lotniczy i hangar do obsługi, uzbrajania, rozmieszczania, startu i lądowania samolotów oraz śmigłowców, a od niedawna także bezzałogowych statków powietrznych, czyli dronów.

Użycie pokładu okrętu do startu samolotu miało miejsce wkrótce po pierwszych udanych próbach lotniczych u progu XX stulecia. 14 listopada 1910 r. Eugene Burton Ely dokonał pierwszego eksperymentalnego startu samolotu Curtiss Pusher z pokładu okrętu Marynarki Wojennej Stanów Zjednoczonych, krążownika USS Birmingham zakotwiczonego w pobliżu bazy marynarki wojennej Norfolk, w Wirginii. Dwa miesiące później, 18 stycznia 1911 r. Ely wylądował swoim samolotem Curtiss Pusher na platformie umieszczonej na krążowniku pancernym USS Pennsylvania zakotwiczonym w Zatoce San Francisco. 9 maja 1912 r. komandor porucznik Charles Samson dokonał pierwszego startu samolotu z okrętu w trakcie rejsu, lecąc dwupłatowcem Short Improved S.27 należącym do brytyjskiego Royal Naval Air Service (RNAS) z pokładu przeddrednotowego pancernika HMS Hibernia, co stanowiło praktyczny debiut lotnictwa w operacjach morskich na otwartym akwenie. Następnie pojawiły się okręty-matki dla wodnosamolotów, jak np. francuski Foudre z 1911 r. Pierwszym atakiem lotniczym przeprowadzonym z pokładu okrętu był nalot na Tondern w lipcu 1918 r.: 7 samolotów Sopwith Camel wystartowało z HMS Furious, który został przebudowany z krążownika na okręt lotniczy poprzez zastąpienie planowanej wieży dziobowej pokładem startowym i hangarem przed wejściem do służby. Camele zaatakowały i uszkodziły niemiecką bazę lotniczą w Tondern, w Niemczech (dzisiejsze Tønder w Danii) oraz zniszczyły dwa sterowce. Pomimo tego w Royal Navy (i innych dużych flotach) nadal uważano, że samoloty mogą pełnić przede wszystkim rolę rozpoznawczą, a typowo bojowe zadania wykonywać w dość ograniczonym zakresie.

W wyniku traktatu waszyngtońskiego z 1922 r., który ograniczył budowę nowych ciężkich okrętów nawodnych, większość wczesnych lotniskowców była przeróbkami okrętów zwodowanych (lub służących) jako jednostki towarowe, krążowniki, krążowniki liniowe lub pancerniki. Przeróbki te dały początek USS Langley w 1922 r., amerykańskim lotniskowcom typu Lexington (1927), japońskim Akagi i Kaga oraz brytyjskiemu Courageous (Furious był 1 z 3 bliźniaczych jednostek). Ewolucja specjalistycznych lotniskowców była w toku, a kilka marynarek wojennych zamówiło i zbudowało okręty wojenne, które zostały celowo zaprojektowane do pełnienia funkcji lotniskowców w połowie lat 20. Doprowadziło to

do oddania do służby takich okrętów, jak japoński Hōshō (1922), brytyjski HMS Hermes (oddany do służby w 1924 r., chociaż zwodowano go w 1918 r., przed Hōshō) i Béarn (1927). Japoński lotniskowiec Hōshō jest uważany za pierwszy okręt od początku zaprojektowany jako lotniskowiec, jednak jego wyposażenie w działa kalibru 140–203 mm odzwierciedlało ówczesne wątpliwości co do pełnych możliwości operacyjnych tej klasy jednostek. Jak powiedział jeden z uczestników negocjacji w Waszyngtonie, „kiepski lotniskowiec mógłby okazać się użyteczny jako krążownik". Ograniczenia traktatowe, jak również brak wiary w skuteczność okrętów lotniczych sprawiły, że mocarstwa morskie wybudowały w latach 30. minionego stulecia niewiele okrętów tej klasy. Brytyjczycy – 1 (Ark Royal będący wzorem dla późniejszych lotniskowców), Amerykanie – 3 (okręty typu Yorktown), a Japończycy – 2 (Hiryū i Sōryū). Większość strategów morskich nadal nie była w pełni przekonana co do ich użycia na masową skalę, wyjątkiem był japoński wiceminister marynarki (późniejszy dowódca połączonej floty), wiceadmirał Yamamoto Isoroku.

Sytuacja uległa drastycznej zmianie po wybuchu II wojny światowej. 11 listopada 20 samolotów bombowo-torpedowych Swordfish z lotniskowca Illustrious zaatakowało włoską bazę floty w Tarencie. Ciężko uszkodzono 3 okręty liniowe, z których 1 już nigdy nie wrócił do służby. Samoloty z lotniskowca Ark Royal odegrały decydującą rolę w pościgu za niemieckim pancernikiem Bismarck w maju 1941 r. na Atlantyku. Absolutnymi nowatorami w użyciu lotniskowców okazali się Japończycy: swe największe lotniskowce zgrupowali w jednym zespole uderzeniowym (Kidō Butai) niosącym na swych pokładach ponad 400 samolotów. To właśnie one zaatakowały bazę w Pearl Harbor 7 grudnia 1941 r. Na Morzu Koralowym (w dniach 4–8 maja 1942 r.) oraz pod Midway (3–6 czerwca 1942 r.) floty japońska i amerykańska stoczyły bitwy wyłącznie przy użyciu samolotów pokładowych, będąc poza wzajemnym kontaktem bojowym. Te starcia ostatecznie wyniosły lotniskowce do czołowych okrętów wojennych flot oceanicznych, degradując role pancerników do ich eskorty. Podczas II wojny światowej wykształciły się 2 zasadnicze typy lotniskowców – uderzeniowe (np. amerykański typ Essex czy brytyjski Illustrous) oraz eskortowe (np. amerykańskie typu Casablanca). Lotnicze eskortowce przebudowywano także ze statków handlowych – np. brytyjski Audacity.

Bezpośrednio po II wojnie światowej lotniskowcami dysponowały wyłącznie marynarki wojenne USA, Wielkiej Brytanii oraz Francji. Sowiecki dyktator Józef Stalin, pragnąc gigantycznego rozwoju floty ZSRR, planował także budowę lotniskowców dla Floty Północnej oraz Oceanu Spokojnego, jednak po jego śmierci w 1953 r. następcy zarzucili te plany, do których powrócono dopiero z początkiem lat 80. minionego stulecia. Po 1945 r. lotniskowce US Navy uczestniczyły w licznych konfliktach, poczynając od wojny koreańskiej, a na wojnie z terroryzmem kończąc. Z kolei brytyjskie okręty tej klasy również zaangażowane były w konflikty koreański i sueski, wreszcie bez ich wsparcia odzyskanie Falklandów w wojnie z Argentyną (1982) byłoby niemożliwe. Przełomowym momentem w rozwoju tej klasy jednostek było wprowadzenie do służby w 1961 r. lotniskowca o napędzie nuklearnym USS Enterprise zapewniającym okrętom praktycznie nieograniczony zasięg działania. Należy przy tym zauważyć, że systematycznie rosła także wyporność lotniskowców uderzeniowych od około 20 tys. t u progu II wojny światowej do ponad 100 tys. t obecnie.

Rozwój techniki lotniczej, pojawienie się samolotów pionowego startu (np. Sea Harrier czy Jak-36) umożliwiło skonstruowanie niewielkich lotniskowców, zwanych też krążownikami lotniczymi. Pojawienie się tego określenia nie było przypadkowe: konwencja z Montreux zabraniała lotniskowcom wpływania na Morze Czarne przez cieśniny Bosfor i Dardanele, stąd też marynarka wojenna ZSRR klasyfikowała najpierw jednostki typu Moskwa jako krążowniki lotnicze, ale w przypadku większych okrętów (np. Wariag późniejszy chiński Liaoning) przyjęto nazwę neutralną politycznie, unikając oficjalnego określenia „lotniskowiec", mimo że ich konstrukcja i przeznaczenie odpowiadały tej klasie jednostek.

Ze względu na wielkość i przeznaczenie współczesne okręty lotnicze dzielimy na:

– duże lotniskowce floty z napędem nuklearnym posiadające parowe lub elektromagnetyczne katapulty startowe (CATOBAR – *catapult-assisted take-off but arrested recovery*). Należy do nich zaliczyć bez wątpienia 11 amerykańskich lotniskowców będących w służbie – 10 typu Nimitz i 1 typu Gerald R. Ford. Do grona tego dodać należy jedyny – jak dotychczas

– nieamerykański lotniskowiec z nuklearnym napędem – francuski Charles de Gaulle;
– lotniskowce floty o napędzie konwencjonalnym – do nich zaliczyć należy 2 brytyjskie lotniskowce typu Queen Elizabeth oraz 3 chińskie – Liaoning, Shandong i Fujian. Mimo różnic w wielkości oraz systemach startu i lądowania każdy z tych okrętów jest w stanie przewozić do 40 myśliwców wielozadaniowych oraz kilkanaście śmigłowców. Okrętami plasującymi się na pograniczu między lotniskowcami floty a lotniskowcami eskortowymi są 2 włoskie jednostki Cavour oraz Trieste, jak również bliźniacze Izumo oraz Kaga Japońskich Morskich Sił Samoobrony. Co ciekawe, japońskie lotniskowce wypierające niemal 30 tys. t oficjalnie są określane jako „niszczyciele śmigłowcowe", choć mogą pomieścić w swych hangarach kilkanaście samolotów typu F-35B;
– lotniskowce eskortowe – bez wątpienia należały do nich brytyjskie okręty typu Invincible, obecnie już wycofane ze służby. Do tego typu zaliczyć można także włoski okręt Giuseppe Garibaldi. Typ ten – jak się wydaje – ma charakter schyłkowy i zastępowany jest okrętami o bardziej uniwersalnym charakterze. W zasadzie jedynym klasycznym reprezentantem tego typu pozostającym w służbie jest dziś lotniskowiec Chakri Naruebet, pływający pod banderą Tajlandii.

Wreszcie ostatnim współczesnym typem okrętu lotniczego są jednostki określane jako okręty doki, desantowce czy helikopterowce. Ich wyporność waha się od 19 tys. t w wypadku japońskich okrętów typu Hyūga do ponad 40 tys. t, gdy idzie o amerykańskie desantowce typu America. Ten ostatni może przewozić do 20 F-35B, ale po niewielkich przeróbkach jest w stanie zwiększyć tę liczbę do 30. Specyficznym okrętem pozostaje turecki Anadolu – jest on wprawdzie przystosowany do użycia samolotów F-35B, ale ze względu na spór Ankary z Waszyngtonem na tle zakupu rosyjskiego systemu przeciwlotniczego S-400 ich dostawa jest wstrzymana. Z tego też względu turecka marynarka wojenna jako pierwsza dostosowała swój okręt lotniczy do używania dużych BSP (dronów).

Trudno jednoznacznie określić, jaka jest przyszłość lotniskowców, zwłaszcza tych największych. Nie brakuje opinii, że rozwój broni rakietowej i dronowej (zwłaszcza w świetle doświadczeń wojny rosyjsko-ukraińskiej) postawi ich przyszłość pod znakiem zapytania. Przeciwstawne opinie zwracają uwagę na coraz lepszą obronę przeciwlotniczą okrętów eskorty (niszczyciele i fregaty) zespołu lotniskowcowego. Poza tym ambitny plan rozwoju lotniskowców mają Chiny oraz Indie, a do tego grona aspiruje także od niedawna Korea Południowa.

Roman Kochnowski

Ch. Chant, *Flugzeugträger. Geschichte, Klassen, Flugzeuge, „Aircraft Carriers"*, Stocker-Schmid, Dietikon–Zürich 2005; R. Chesneau, *Aircraft Carriers of the World, 1914 to the Present: An Illustrated Encyclopedia*, Naval Institute Press, Annapolis 1984; T. Clancy, *Supercarrier. Die Welt der amerikanischen Flugzeugträger. („Carrier")*, 2. Aufl. Heyne, München 2002; D. Hobbs, *A Century of Carrier Aviation: The Evolution of Ships and Shipborne Aircraft*, Seaforth Publishing, Barnsley–Yorkshire 2009; D. Ross, *Panorama techniki wojskowej. Najsłynniejsze lotniskowce. Ilustrowana historia*, Almapress, Warszawa 2018; US Naval War College, https://digital-commons.usnwc.edu/newport-papers/17/ (dostęp 16.11.2025); *Z dziejów okrętów wojennych. Okręty lotnicze*, „Okręty Wojenne" 2023.

M

MANIPULACJA ALGORYTMICZNA (manipulacja ze strony algorytmów AI/systemów AI)[13] – ukryta, nie w pełni transparentna lub asymetryczna forma wpływu generowana przez algorytmy na stany mentalne (uwagę, emocje, przekonania) i zachowania użytkownika, osiągana poprzez kontrolę środowiska informacyjnego, personalizację bodźców oraz optymalizację funkcji celu[14], wykorzystująca istniejące nierównowagi informacyjne, motywacyjne lub strukturalne w sposób służący interesom operatora

[13] Konsensus międzynarodowy w zakresie ujęcia definicji sztucznej inteligencji od strony modelu systemowego, opartego na technicznym nurcie rozwoju modelu inteligentnego agenta, sprowadza się do opisu sztucznej inteligencji jako systemu AI.

[14] Funkcja celu w algorytmie to kryterium oceny jakości rozwiązań (np. minimalizacja kosztów, maksymalizacja zysku), które algorytm stara się zoptymalizować, wykonując sekwencję kroków, aby znaleźć najlepsze możliwe rozwiązanie danego problemu, takie jak sortowanie danych, optymalizacja procesu obróbki czy rekomendacje w systemach inteligentnych. Algorytm to zestaw instrukcji, a funkcja celu – cel, do którego one dążą, określając, co jest „dobre", a co „złe".

systemu cyfrowego, a potencjalnie ograniczająca autonomię odbiorcy – nawet bez intencjonalnego projektu takiego działania[15].

Elementy manipulacji ze strony systemów AI (Carroll et al. 2023):

- *incentives* (bodźce) – mechanizmy (czynniki) zachęcające systemy sztucznej inteligencji do podejmowania działań mających na celu zmianę ludzkich zachowań, przekonań, preferencji lub stanów psychicznych. Czynnikiem zachęcającym może być reakcja człowieka przynosząca w jakiś sposób korzyści systemowi sztucznej inteligencji[16]. Systemy rekomendacyjne mogą np. wpływać na użytkowników, tak aby uczynić ich zachowanie bardziej przewidywalnym;
- *intent* (intencje) – zamiar wywierania wpływu (świadome zamierzenia systemu AI). System ma zamiar wykonać dane działanie zgodnie z motywacją do manipulacji, jeśli w jego trakcie angażuje się w proces rozumowania lub planowania tego, jak ono wpłynie na określony cel. Należy jednak rozróżnić wypadki, w których system zachowuje się w sposób manipulacyjny przypadkowo, od takich, w których takie zachowanie jest częścią celowego, systematycznego wzorca mającego na celu osiągnięcie określonego wyniku końcowego;
- *covertness* (skrytość/tajność) – stopień, w jakim człowiek nie jest świadomy tego, jak bardzo system sztucznej inteligencji

[15] Definicja ta podkreśla, że manipulacja nie musi wymagać intencjonalności projektanta – jednej z podstawowych cech manipulacji. Nie należy jednak bagatelizować zdolności algorytmów AI do „uczenia się", a następnie podejmowania decyzji i działania bez bezpośredniej interwencji człowieka. Obserwujemy zmianę sposobu myślenia o autonomii w kontekście AI. Mowa o autonomii nowej generacji 2.0, definiowanej przez Infuture Institute jako zdolność systemów do nieustannego samodoskonalenia się, napędzaną algorytmami uczenia maszynowego. Nie chodzi już tylko o systemy, które działają „same", bez ciągłego nadzoru człowieka, ale o takie, które potrafią uczyć się na bieżąco i modyfikować własne decyzje. W praktyce oznacza to, że autonomiczne systemy nie tylko realizują zaprogramowane zadania, ale coraz częściej same inicjują działania i reagują na otoczenie w sposób, który jeszcze niedawno był zarezerwowany wyłącznie dla ludzi. Systemy mogą zatem uczyć się strategii manipulacyjnych w pogoni za maksymalizacją zdefiniowanych celów.

[16] Słowem, jeśli manipulator odnosi korzyści z pewnych zachowań manipulowanego, ma motywację do spowodowania takiego zachowania.

próbuje zmienić niektóre aspekty jego zachowań, przekonań lub preferencji. Tajność[17] oznacza, że dana osoba nie może wyrazić zgody na wywieranie na nią wpływu i nie jest w stanie oprzeć się niepożądanemu działaniu, przez co podważana jest autonomia jednostki;

– *harm* (szkoda) – efekt manipulacji (np. rozdrażnienie bez wyraźnej przyczyny, uczucie emocjonalnego przesycenia, „przenoszenie się" w sieci emocji)18. Warto podkreślić, że nie wszystkie tego rodzaju przypadki są jednoznacznie szkodliwe. Paternalistyczne bodźce19 (subtelne popychanie – *nudging*) można uznać za korzystne; często stosuje się te techniki, by skłonić do pożądanej decyzji bez zakazywania innych wyborów (np. zmiana domyślnego ustawienia formularzy dawców organów na opcję „wyrażam zgodę" zamiast „nie wyrażam zgody" znacznie zwiększa liczbę rejestracji).

Manipulację ze strony algorytmów umożliwiają asymetria informacyjna i kontrola nad środowiskiem informacyjnym. Wynika to głównie z faktu, że algorytmy pełnią obecnie funkcję bramkarzy informacji (*gatekeepers*), decydując o tym, jakie treści są eksponowane, pomijane lub marginalizowane. Stąd też manipulacja algorytmiczna działa na poziomie infrastrukturalnym i proceduralnym, często poza świadomością użytkownika oraz bez możliwości realnej kontroli lub weryfikacji (Gillespie 2018). Mówimy zatem, że algorytmy sprawują władzę algorytmiczną (*algorithmic*

---

[17] Ta cecha jest jednym ze sposobów rozróżnienia między manipulacją a perswazją. W przypadku perswazji osoba, na którą wywierany jest wpływ, jest zazwyczaj świadoma prób zmiany jej zdania przez osobę wywierającą ten wpływ.

[18] Negatywne konotacje terminu „manipulacja" mogą prowadzić do założenia, że szkoda jest nieodłącznym jego warunkiem wstępnym. Wyzwanie stanowi także praktyczna ocena elementów, które oddają kluczowe aspekty szkody, tj. pominięcie racjonalnej deliberacji, wadliwe stany psychiczne czy obecność reperkusji.

[19] Koncepcja libertariańskiego paternalizmu (LP), spopularyzowana przez R. Thalera i C. Sunsteina, zakłada, że systemy sztucznej inteligencji (AI) lub algorytmy, działając w oparciu o dane i logikę, subtelnie lub jawnie kierują wyborami ludzi, podejmując decyzje lub tworząc ramy decyzyjne, które mają służyć ich własnemu dobru (np. zdrowszym nawykom, lepszym inwestycjom), nawet jeśli jednostka nie wyraża na to zgody.

power), rozumianą jako zdolność do regulowania widoczności informacji, hierarchii znaczeń oraz norm uczestnictwa w przestrzeni cyfrowej. Władza ta nie działa poprzez bezpośredni przymus, lecz za sprawą procedur selekcji i klasyfikacji, które pozostają poza bezpośrednią kontrolą użytkowników (Gillespie 2014; Mittelstadt et al. 2016). W tym ujęciu manipulacja algorytmiczna jest efektem strukturalnym władzy platform cyfrowych (skutkiem strukturalnych uwarunkowań projektowych) (Mittelstadt et al. 2016; Kitchin 2017). Staje się nie tylko ukrytym narzędziem zdobywania władzy ideologicznej, politycznej i materialnej, stanowiącym szczególną formę oddziaływania pośredniego, zaprojektowaną lub wykorzystywaną w sposób, który uprzywilejowuje konkretne cele nadawców, kierując np. uwagę użytkowników ku określonym obiektom, narracjom czy interakcjom. Można manipulację – która jest „moralnie nie do przyjęcia, ponieważ wykorzystuje podatności jednostek i kieruje ich zachowania w sposób, który prawdopodobnie przyniesie korzyść manipulatorowi" (Wang 2022) – traktować także jako formę psychologicznej agresji, mającą na celu zmuszenie osoby do myślenia lub działania w sposób, który służy interesom manipulatora, często kosztem własnych potrzeb lub dobra ofiary[20].

Zjawisku temu sprzyjają także mechanizmy personalizacji, które wpisują się w strategie manipulacji społecznej Naoma Chomsky'ego. W myśl zasady: poznaj ludzi lepiej niż oni samych siebie, algorytmy AI w oparciu o nasz ślad cyfrowy czytają nam w myślach. W ten sposób algorytmy uczą się podatności jednostki i dostosowują bodźce do jej profilu (przewidują, co przyciągnie jej uwagę).

---

[20] Jeśli przyjmiemy za J. Habermasem, że działania komunikacyjne (rozumiane jako dążenie do porozumienia i koordynacji działań) są normą, a działania strategiczne – wykroczeniem przeciwko niej, to manipulacja nie jest traktowana jako zło społeczne, a jedynie odstępstwo od normy społecznej komunikacji. Traktowana w ten sposób może w niektórych przypadkach stracić swoje pejoratywne zabarwienie. Manipulacja bywa więc w technicznej definicji oficerów śledczych definiowana jako ogół taktyk i trików perswazyjnych, które są skuteczne wyłącznie w odniesieniu do osób winnych i fakt ten stanowi, według nich, etyczne uzasadnienie ich stosowania. Cyt. za: J. Aksman, *Wpływ, perswazja, propaganda, manipulacja – próba uporządkowania pojęć*, [w:] *Manipulacja. Pedagogiczno-społeczne aspekty*, cz. I: *Interdyscyplinarne aspekty manipulacji*, J. Aksman (red.), Krakowska Akademia im. A. Frycza Modrzewskiego, Kraków 2010.

Na korzyść manipulacji wpływa brak transparentności w działaniu algorytmów, który oznacza, że użytkownicy, decydenci i społeczeństwo nie mają pełnego zrozumienia procesów podejmowania decyzji przez AI. Istnieje zatem ryzyko, że algorytmy mogą wprowadzać błędy (halucynacje) lub wykazywać uprzedzenia (bias), co może prowadzić do niesprawiedliwych osądów w kontekście różnych grup społecznych. Stąd w kręgach naukowców, profesjonalistów, regulatorów i aktywistów tak wysoko ceniona jest przejrzystość algorytmiczna (Estop 2014; Weller 2017). Jednak wielu badaczy zakwestionowało to stanowisko, rozważając praktyczne kwestie dotyczące przejrzystości algorytmów (Ananny, Crawford 2018; Diakopoulos 2020), bo np. niektóre dane dotyczące algorytmów bywają zbyt wrażliwe, by je ujawnić, mogą zaszkodzić przewadze konkurencyjnej danej firmy lub prowadzić do manipulowania systemem przez konsumentów (Diakopoulos 2020). Pojawia się pytanie: co, jeśli sama przejrzystość algorytmiczna jest formą manipulacji – techniką dyscyplinarną w erze Big Data? W rzeczywistości przejrzystość algorytmiczna[21] jest procesem społecznym powiązanym z relacjami władzy, który jest znacznie bardziej złożony niż wyłącznie ujawnienie informacji, określające, ile danych algorytm powinien ujawnić (Ananny, Crawford 2018; Weller 2017). Jak twierdzi Hao Wang (2022), przejrzystość algorytmiczna z perspektywy władzy może być techniką normalizowania zachowań ludzi (foucaultowskie ujęcie przejrzystości stanowiącej część dyscyplinarnej struktury władzy)[22]. Przykładem jest m.in. system punktacji FICO, który nie tylko

[21] W tym kontekście przejrzystość algorytmiczna to nie tylko informacyjne ujawnienie wewnętrznych mechanizmów algorytmu, błędnie postrzeganego wyłącznie jako „technicznego i samodzielnego obiektu", stosunkowo neutralnego i odizolowanego od władzy społecznej i politycznej. Istotnego znaczenia nabierają tu bowiem ukryte struktury władzy oraz sposób, w jaki ona działa w procesie ujawniania informacji. Nawet jeśli zostanie przedstawione wierne informacyjne wyjaśnienie algorytmów, może ono zostać starannie wybrane spośród szerokiego zestawu możliwych, aby służyć celom tzw. „wdrożeńców" (wdrożycieli – właścicieli algorytmów, np. Amazon), czyli 1 z 3 klas osób zazwyczaj zaangażowanych w proces ujawniania informacji algorytmicznej. Pozostałe to: deweloperzy – twórcy algorytmów, i użytkownicy systemów algorytmicznych – często dotknięci decyzjami algorytmicznymi.

[22] Działanie asymetrycznej władzy może manipulować zachowaniem ludzi poprzez przejrzystość algorytmiczną. Tego typu władza jest głęboko zakorzeniona w społeczeństwie

ma na celu obliczanie ryzyka użytkowników kredytów, ale również zachęcanie konsumentów do przestrzegania oczekiwanych norm (m.in. systemy punktacji często zawierają szereg kar, które mogą dyscyplinować zachowania poszczególnych osób). To właśnie dzięki temu pozornemu aktowi przejrzystości skutecznie działa dyscyplinarna siła FICO Score. Innymi słowy, sama przejrzystość algorytmiczna stała się kluczową częścią techniki dyscyplinarnej.

Wśród mechanizmów manipulacji algorytmicznej (narzędzi i strategii wywierania wpływu na użytkownika) możemy zatem zidentyfikować następujące elementy:

- wpływ ukryty – niejawna/ukryta moderacja i ograniczanie widoczności/zasięgu treści – niejawne, zakamuflowane oddziaływanie algorytmów w postaci precyzyjnie dobranych treści, bez świadomości, że zostały one wybrane strategicznie, lub ograniczanie zasięgu treści bez ich formalnego usunięcia (np. *shadow banning*) (Gillespie 2018);
- eksploatacja podatności – algorytm identyfikuje podatności psychologiczną, poznawczą i sytuacyjną użytkownika i wzmacnia treści wywołujące jego reakcje (radość, współczucie, gniew, oburzenie czy lęk);
- optymalizacja behawioralna (*behavioral shaping*) – algorytm wzmacnia treści, które zwiększają zaangażowanie użytkownika – szczególnie emocjonalne i kontrowersyjne – przez nagrody (lajki, rekomendacje, dopływ treści);
- kształtowanie środowiska informacyjnego – algorytm odsuwa treści alternatywne na dalszy plan, a użytkownik trafia do „bańki informacyjnej". Zjawisko to bywa opisywane w literaturze jako mechanizm zawężania pola percepcji, co ogranicza kontakt z alternatywnymi narracjami i osłabia zdolność krytycznego namysłu (Bozdag 2013);

algorytmicznym, gdzie potężne podmioty potrafią „zamieniać jednostki w obiekty rangi i oceny". Jak podkreśla S. Zuboff, luka we władzy między użytkownikami a kapitalistami inwigilacyjnymi jest ogromna: oni wiedzą o nas wszystko, ale my wiemy o nich niewiele. Przewidują naszą przyszłość, ale dla dobra innych (Zuboff, Laidler 2019).

– wzmocnienie i reprodukcja uprzedzeń algorytmicznych (*algorithmic bias*) –systematyczne odchylenia w działaniu algorytmów prowadzą do nierównego traktowania użytkowników lub treści. Uprzedzenia te są często konsekwencją stronniczych danych lub uproszczonych modeli rzeczywistości społecznej i mają charakter strukturalny, nawet jeśli nie są zamierzone (Mittelstadt et al. 2016).

Mechanizmy manipulacyjne bezpośrednio wpływają na użytkownika poprzez proces oddziaływania algorytmów (proces manipulacyjny algorytmów), na który składają się:

– percepcja – użytkownik doświadcza świata przez algorytm, nie widzi jego selekcji;
– internalizacja bodźców – system wzmacnia określone narracje, stopniowo kształtując emocje, przekonania i priorytety odbiorcy. Użytkownik internalizuje powtarzające się bodźce dopasowane do jego profilu podatności;
– zmiana stanu mentalnego – system modyfikuje przekonania, emocje, uwagę, motywacje. Następuje wzrost strachu, zaufania do określonych źródeł albo niechęci wobec innych;
– zmiana zachowań – użytkownik podejmuje decyzje wyborcze, które są w interesie podmiotu kontrolującego algorytm (np. reklamodawcy politycznego), a nie wynikają z pełnej informacji.

Efektami manipulacji ze strony algorytmów, które generuje proces manipulacyjny, są m.in.:

– osłabienie autonomii użytkownika: manipulacja narusza zdolność do samodzielnego podejmowania decyzji;
– polaryzacja i zniekształcenie opinii publicznej: hiperpersonalizacja i filtrowanie prowadzą do zamkniętych baniek informacyjnych;
– wzmacnianie nierówności politycznej i poznawczej: systemy premiują grupy z większym „kapitałem informacyjnym";
– spadek zaufania do mediów i instytucji: manipulowana przestrzeń informacyjna prowadzi do erozji zaufania społecznego.

Warto zauważyć, że skutki manipulacji algorytmicznej modulowane mogą być przez takie czynniki kontekstowe i indywidualne (regulujące, wzmacniające lub osłabiające intensywność algorytmów), jak:

- intencja projektanta – manipulacja może wystąpić nawet bez niej, ale intencjonalność zwiększa ryzyko;
- siła bodźca i częstotliwość ekspozycji – intensywność rekomendacji i kierowanie treści wzmacniają efekt manipulacji;
- kompetencje cyfrowe użytkownika – użytkownik o niskiej umiejętności krytycznej analizy informacji jest wyjątkowo podatny na manipulacje ze strony algorytmów.

Manipulacja algorytmiczna ma charakter socjotechniczny – łączy elementy konstrukcyjne algorytmów z kontekstami społecznymi, w których są użytkowane. Algorytmy nie działają w próżni – ich efekty są wynikiem złożonych interakcji między projektantami, użytkownikami, platformami i warunkami ekonomicznymi (np. modelami biznesowymi opartymi na reklamie). Ponadto użytkownicy nie są wyłącznie pasywnymi odbiorcami algorytmicznych rekomendacji – mogą świadomie manipulować algorytmami (ang. *algorithm manipulation behavior*), np. przez określone sekwencje interakcji, ukierunkowane kliknięcia czy strategiczne użycie treści, aby wpływać na to, co algorytm im rekomenduje. Tego typu zachowania ujawniają ambiwalentną naturę manipulacji algorytmicznej jako narzędzia wpływu zarówno systemu na użytkownika, jak i użytkownika na system.

Jednym z kluczowych, choć często niedostatecznie eksponowanych aspektów manipulacji algorytmicznej jest jej wpływ na autonomię poznawczą jednostki, która jest rozumiana jako zdolność do samodzielnego kształtowania opinii i decyzji na podstawie pluralistycznego dostępu do informacji oraz refleksyjnego namysłu (Floridi 2014; Mittelstadt et al. 2016). To właśnie ten wymiar czyni manipulację algorytmiczną problemem etycznym, a nie wyłącznie technologicznym. Warto zauważyć, że algorytmy, działając jako architekci wyboru, kształtują środowisko decyzyjne użytkownika w sposób, który może prowadzić do swego rodzaju algorytmicznego paternalizmu – „podpowiadania" określonych decyzji przy jednoczesnym ograniczaniu widoczności alternatyw. W tym sensie manipulacja algorytmiczna narusza autonomię nie poprzez przymus, lecz projekt środowiska informacyjnego.

Z perspektywy bezpieczeństwa i nie tylko manipulacja algorytmiczna może prowadzić do:

- erozji zaufania społecznego do mediów, instytucji i wiedzy eksperckiej;
- polaryzacji i fragmentacji sfery publicznej, utrudniającej deliberację demokratyczną;
- osłabienia autonomii decyzyjnej jednostek, których wybory są kształtowane przez niejawne mechanizmy selekcji;
- zwiększonej podatności na operacje wpływu, w tym działania państw i aktorów niepaństwowych w ramach wojen informacyjnych (NASK 2019; NASK 2024);
- zmęczenia poznawczego użytkowników – algorytmy wykorzystują ograniczoną zdolność uwagi;
- normalizacji manipulacji – użytkownicy adaptują się do bycia „prowadzonymi";
- braku sprawczości zbiorowej – jednostka nie ma realnego wpływu na algorytm;
- syndromu „długiego trwania" – manipulacja algorytmiczna działa kumulatywnie, nie incydentalnie.

Regulacja manipulacji algorytmicznej w Unii Europejskiej nie występuje jako jednolity akt prawny odnoszący się bezpośrednio do tego pojęcia, lecz jest rozproszona w kilku komplementarnych instrumentach prawnych, które razem tworzą ramy prewencji i odpowiedzialności algorytmicznej. Wśród regulacji systemowych odnajdujemy:

- Digital Services Act – rozporządzenie Parlamentu Europejskiego i Rady (UE), które wprowadza po raz pierwszy obowiązki systemowe wobec bardzo dużych platform internetowych (VLOPs), odnoszące się bezpośrednio do ryzyka wynikającego z algorytmicznej dystrybucji treści. DSA identyfikuje ryzyka systemowe wynikające z funkcjonowania algorytmów rekomendacyjnych (art. 34); nakłada obowiązek oceny i ograniczania zagrożeń takich jak manipulacja informacyjna i dezinformacja; wprowadza wymóg transparentności systemów rekomendacyjnych, w tym ujawniania głównych parametrów rankingowych. W kontekście manipulacji algorytmicznej DSA

uznaje algorytmy nie za neutralne narzędzia, lecz źródło zagrożeń dla debaty publicznej i procesów demokratycznych (European Commission 2022);
- Artificial Intelligence Act (2024) – rozporządzenie przyjęte w 2024 r., które wprowadza klasyfikację systemów AI według poziomu ryzyka, co ma kluczowe znaczenie dla manipulacji algorytmicznej. Szczególnie istotne są: zakaz systemów AI wykorzystujących podprogowe techniki manipulacyjne naruszające autonomię użytkownika; uznanie systemów wpływających na zachowania społeczne za systemy wysokiego ryzyka; obowiązek dokumentowania i audytowania algorytmów. AI Act po raz pierwszy w prawie UE *explicite* uznaje, że algorytm może być narzędziem manipulacji, nawet bez użycia fałszywej treści (European Parlament 2024).

Poza UE istotne znaczenie mają:
- OECD Principles on AI (2019) – zasada transparentności i odpowiedzialności;
- UNESCO Recommendation on the Ethics of AI (2021) – zakaz manipulacji poznawczej i emocjonalnej.

Istotne jest zatem postulowanie wielowarstwowego podejścia do przeciwdziałania negatywnym skutkom manipulacji algorytmicznej, w tym:
- transparentności algorytmicznej: ujawnienia kryteriów działania algorytmów, logiki rekomendowania treści publiczności oraz relacji władzy;
- audytu algorytmów i oceny skutków: niezależnych testów i oceny ich wpływu na różne grupy użytkowników i areny debaty publicznej;
- wzmocnienia kompetencji informacyjnej: edukacji społeczeństwa i ekspertów w zakresie rozumienia mechanizmów algorytmicznych i ich wpływu.

Emilia Musiał

E. Bozdag, *Bias in algorithmic filtering and personalization*, „Ethics and Information Technology" 2013, no. 15(3), https://doi.org/10.1007/s10676-013-9321-6; L. Floridi, *The fourth revolution: How the infosphere is reshaping human reality*,

Oxford University Press, Oxford 2014; T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, London 2018; T. Gillespie, *The relevance of algorithms*, [w:] *Media Technologies: Essays on Communication, Materiality, and Society*, T. Gillespie, P.J. Boczkowski, K.A. Foot (eds.), MIT Press, Oxford 2014; R. Kitchin, *Thinking critically about and researching algorithms*, „Information, Communication & Society" 2018, no. 20(1), https://doi.org/10.1080/1369118X.2016.1154087; H. Wang, *Transparency as Manipulation? Uncovering the Disciplinary Power of Algorithmic Transparency*, „Philosophy & Technology" 2022, no 35(35), https://doi.org/10.1007/s13347-022-00564-w; B.D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi, *The ethics of algorithms*, „Big Data & Society" 2016, no. 3(2), https://doi.org/10.1177/2053951716679679; C.R. Sunstein, *Nudging and Choice Architecture: Ethical Considerations*, „Yale Journal on Regulation" 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2551264.# (dostęp 16.12.2025); *Wojna informacyjna 2022–2023*, 2024, https://www.nask.pl/media/2024/10/Raport__wojna_informacyjna.pdf (dostęp 16.12.2025); *Zjawisko dezinformacji w dobie rewolucji cyfrowej*, 2019, https://rszarf.ips.uw.edu.pl/krytarg/raport-nask2019.pdf (dostęp 16.12.2025).

MIĘDZYNARODOWA ORGANIZACJA PRACY, MOP (ang. International Labour Organization, ILO) została ustanowiona w 1919 r. jako odpowiedź na potrzebę zinstytucjonalizowanej współpracy rządów, przedsiębiorców i związków zawodowych w celu realizacji sprawiedliwości społecznej oraz poprawy warunków życia i pracy w skali światowej. Pierwszym wyrazem tych dążeń było zorganizowanie w Berlinie w 1890 r. międzynarodowej konferencji z udziałem przedstawicieli 15 państw, na której nie podjęto konkretnych zobowiązań.

W 1900 r., na konferencji w Paryżu powołano Międzynarodowe Stowarzyszenie Legislacji Pracy z siedzibą w Bazylei, zajmujące się tłumaczeniem i publikowaniem krajowych regulacji prawa pracy. Rok później powstał Międzynarodowy Sekretariat Krajowych Związków Zawodowych, przemianowany w 1913 r. na Międzynarodową Federację Związków Zawodowych, która odegrała rolę kluczową w pierwszym okresie istnienia ILO. W 1906 r., na konferencji dyplomatycznej w Brnie przyjęto 2 pierwsze międzynarodowe konwencje pracy: ograniczającą stosowanie białego fosforu w produkcji zapałek oraz zakazującą nocnej pracy kobiet w przemyśle (z wyjątkiem małych przedsiębiorstw). Wydarzenie to zapoczątkowało nowy etap w stosunkach międzynarodowych w dziedzinie pracy. Kolejne

inicjatywy – dotyczące pracy nocnej młodocianych oraz maksymalnego dziesięciogodzinnego dnia pracy kobiet i młodzieży – zostały przerwane przez wybuch I wojny światowej.

W 1919 r. na wniosek związków zawodowych konferencja pokojowa w Paryżu powołała Komisję Pracy do opracowania konstytucji ILO (dokumentu opartego na projekcie brytyjskim), który 11 kwietnia 1919 r. stał się XIII rozdziałem traktatu wersalskiego i – po późniejszych poprawkach – pozostaje do dziś podstawą funkcjonowania organizacji. W okresie międzywojennym ILO działała jako agencja Ligi Narodów, koncentrując się na takich zagadnieniach, jak ośmiogodzinny dzień pracy, bezrobocie, ochrona macierzyństwa oraz warunki pracy kobiet i młodzieży. W 1920 r. mianowano pierwszego dyrektora, którym został Albert Thomas z Francji. W tym samym roku, po przeniesieniu sekretariatu ILO do tymczasowych siedzib w Paryżu i Londynie, Rada Administracyjna podjęła decyzję o stałym utworzeniu sekretariatu w Genewie.

W 1926 r. organizacja ustanowiła system nadzoru nad stosowaniem swoich standardów. W 1934 r. do ILO przystąpiły USA i ZSRR, który utracił członkostwo w 1939 r. w wyniku wykluczenia z Ligi Narodów i został ponownie przyjęty w 1954. Jednocześnie, w obliczu wzrostu nacjonalistycznych rządów w Europie, organizacja zaczęła się odsuwać od Starego Kontynentu i w 1936 r. zorganizowała pierwszą regionalną konferencję w Santiago w Chile.

W sierpniu 1940 r. biuro przeniosło się do Monrealu, gdzie 40 pracowników z 18 krajów gościł do 1947 r. Uniwersytet McGill. W 1944 r. w Filadelfii odbyła się Międzynarodowa Konferencja Pracy, która przyjęła deklarację filadelfijską, stanowiącą obecnie integralny aneks do konstytucji: rozszerzyła ona i pogłębiła cele i zadania organizacji, wskazując m.in. na prawo wszystkich ludzi do rozwoju w warunkach wolności, godności i bezpieczeństwa ekonomicznego oraz uznając ubóstwo za zagrożenie dla dobrobytu powszechnego. W 1946 r. ILO stała się pierwszą wyspecjalizowaną agencją Organizacji Narodów Zjednoczonych, wchodząc w system ścisłej współpracy międzynarodowej.

Wskutek zabiegów Indii o zwiększenie roli krajów rozwijających się w ILO w 1947 r. zorganizowano pierwszą przygotowawczą Azjatycką Konferencję Regionalną. W 1952 r. ILO uruchomiła Program dla społeczności

andyjskich – pierwszy na tak szeroką skalę program współpracy technicznej, ukierunkowany na poprawę warunków społecznych i ekonomicznych rdzennych mieszkańców Andów w 7 krajach Ameryki Łacińskiej. W 1960 r. zorganizowano pierwszą Afrykańską Konferencję Regionalną w Lagos, w Nigerii będącą następstwem przyjęcia do organizacji 16 nowo niepodległych państw afrykańskich.

W 1969 r. ILO została uhonorowana Pokojową Nagrodą Nobla. W 1977 r. Rada Administracyjna przyjęła deklarację w sprawie przedsiębiorstw wielonarodowych i polityki społecznej (zmieniona na jej sesjach: 279 – w listopadzie 2000 r., 295 – w marcu 2006 r., 329 – w marcu 2017 r.), której celem jest ukierunkowanie przedsiębiorstw wielonarodowych w obszarach zatrudnienia, szkolenia, warunków pracy, bezpieczeństwa i higieny pracy oraz stosunków przemysłowych. W 1998 r. przyjęto deklarację w sprawie podstawowych zasad i praw w pracy, która ustanawia 4 kategorie praw podstawowych, potwierdzając w ten sposób podejście ILO do praw człowieka w kontekście globalnej gospodarki. Są to: swobody zrzeszania się oraz efektywnego uznania prawa rokowań zbiorowych, likwidacji wszelkich form pracy przymusowej lub obowiązkowej, skutecznej likwidacji pracy dzieci oraz likwidacji dyskryminacji w zatrudnieniu i w zakresie wykonywania zawodu.

W 2004 r. ILO powołała Światową Komisję ds. Społecznego Wymiaru Globalizacji. W 2008 r. przyjęła deklarację w sprawie sprawiedliwości społecznej na rzecz sprawiedliwej globalizacji, w której określono 4 cele strategiczne ILO: zatrudnienie, ochrona socjalna, dialog społeczny i podstawowe prawa w pracy, traktowane jako „nierozłączne, wzajemnie powiązane i wspierające się". W 2009 r. Międzynarodowa Konferencja Pracy przyjęła Globalny Pakt na rzecz Zatrudnienia, odnoszący się do społecznych kosztów kryzysu i wzywający rządy do uczynienia tworzenia miejsc pracy centralnym elementem strategii odbudowy. W 2015 r. zorganizowano pierwsze spotkanie Globalnej Komisji ds. Przyszłości Pracy. W 2019 r. przyjęto deklarację z okazji stulecia istnienia ILO na rzecz przyszłości pracy. W czerwcu 2022 r. Międzynarodowa Konferencja Pracy na 110 sesji przyjęła rezolucję o implementacji bezpiecznego i zdrowego środowiska pracy do ram podstawowych zasad i praw w pracy ILO, co

skutkowało zmianami w deklaracji z 1998 r. w postaci włączenia 5 kategorii praw, tj. bezpiecznego i zdrowego środowiska pracy.

Misją ILO jest w szczególności tworzenie i upowszechnianie międzynarodowych standardów oraz podstawowych zasad i prawa pracy, poszerzanie możliwości kobiet i mężczyzn w zakresie uzyskiwania godnego zatrudnienia i stabilnych dochodów, zwiększanie zasięgu oraz efektywności systemów ochrony socjalnej dla wszystkich, a także umacnianie trójstronnej współpracy i dialogu społecznego.

W skład ILO wchodzą Międzynarodowa Konferencja Pracy, Rada Administracyjna, Międzynarodowe Biuro Pracy.

Międzynarodowa Konferencja Pracy stanowi organ najwyższy, złożony z trójstronnych delegacji państw członkowskich ILO, który m.in. formułuje i ustanawia międzynarodowe standardy pracy w formie konwencji i zaleceń, monitoruje ich implementację za pośrednictwem Komitetu ds. Stosowania Standardów, przyjmuje dwuletni program ILO, budżet oraz rezolucje określające kierunki ogólnej polityki oraz przyszłych działań organizacji, ustala zasady podziału kosztów między państwa członkowskie, wybiera członków Rady Administracyjnej, decyduje o przyjęciu do ILO nowych państw niebędących członkami ONZ, uchwala zmiany w konstytucji ILO, rozpatruje sprawozdania Dyrektora Generalnego oraz Przewodniczącego Rady Administracyjnej. Pracami Konferencji kieruje Prezydium wybierane na posiedzeniu otwierającym. W jego skład wchodzą przewodniczący (delegat rządowy lub minister) oraz 3 wiceprzewodniczący: delegat rządowy, delegat pracodawców i delegat pracowników. Większość kwestii merytorycznych realizują komitety, które składają sprawozdania plenarnemu posiedzeniu Konferencji. Ich rezultaty (rezolucje, konkluzje, instrumenty itp.) nabierają mocy wyłącznie po zatwierdzeniu przez plenum, co w niektórych przypadkach może wymagać przeprowadzenia głosowania. Wyróżnia się 2 rodzaje komitetów: stałe (ds. ogólnych, ds. mandatowych, redakcyjny, finansowy, ds. stosowania standardów) oraz techniczne (do ustanawiania standardów, dyskusji).

Rada Administracyjna stanowi organ wykonawczy, pełniący funkcje decyzyjne i nadzorcze, który m.in. wybiera Dyrektora Generalnego, określa i kształtuje politykę ILO, realizuje strategiczne wytyczne przyjęte przez Międzynarodową Konferencję Pracy, sprawuje kierownictwo nad

działalnością Biura oraz Dyrektora Generalnego, ustala porządek obrad Międzynarodowej Konferencji Pracy, zatwierdza projekt programu i budżetu przedkładany następnie Konferencji do ostatecznego przyjęcia, realizuje procedury konstytucyjne związane ze stosowaniem ratyfikowanych konwencji, zatwierdza porządek obrad oraz, w razie potrzeby, skład spotkań regionalnych, sektorowych i eksperckich. Posiedzenia Rady Administracyjnej odbywają się w trybie plenarnym, a jej prace są zorganizowane w 5 sekcjach podzielonych na segmenty, tj. 1) instytucjonalna, 2) rozwoju polityki, 3) zagadnień prawnych i międzynarodowych standardów pracy, 4) programowa, finansowa i administracyjna, 5) wysokiego szczebla, która obraduje w miarę potrzeb, w 1 z 2 trybów, tj. Segment Polityki Strategicznej zajmujący się kwestiami o strategicznym znaczeniu dla ILO (posiedzenia odbywają się w trybie zwykłego segmentu Rady Administracyjnej), Zespół Roboczy ds. Społecznego Wymiaru Globalizacji obradujący jako komitet plenarny, umożliwiający udział w debacie przedstawicielom rządów niebędącym członkami Rady Administracyjnej (z pracy zespołu nie wynikają decyzje, zalecenia ani sprawozdania). Rada może również powoływać komitet lub zespół roboczy celem rozpatrzenia określonych zagadnień; określa jego skład, mandat oraz czas trwania, np.

- Komitet ds. Wolności Związkowej – organ trójstronny utworzony w 1951 r. w celu badania naruszeń praw organizowania się pracowników i pracodawców;
- Trójstronna Grupa Robocza Mechanizmu Przeglądu Standardów utworzona w 2015 r. w celu przeglądu międzynarodowych standardów pracy pod kątem solidności i adekwatności do uwarunkowań świata pracy, z myślą o ochronie pracowników oraz uwzględnieniu potrzeb zrównoważonych przedsiębiorstw;
- Trójstronna Grupa Robocza ds. Demokratyzacji Zarządzania ILO utworzona w 2019 r.;
- Rada Międzynarodowego Centrum Szkoleniowego ILO.

Rada Administracyjna może także obradować jako Komitet Plenarny, zgodnie z art. 4.3 regulaminu wewnętrznego Rady Administracyjnej, z udziałem przedstawicieli rządów, które nie są w niej reprezentowane, w celu umożliwienia im przedstawienia stanowisk w sprawach dotyczących sytuacji w ich własnych krajach.

Międzynarodowe Biuro Pracy to stały sekretariat, odpowiedzialny za wdrażanie polityk i programów przyjętych przez organy zarządzające ILO, na czele którego stoi Dyrektor Generalny. Praca zorganizowana jest w 4 klastrach pozostających pod nadzorem asystenta Dyrektora Generalnego, tj. 1) zarządzanie, prawa i dialog, 2) zatrudnienie i ochrona socjalna, 3) relacje zewnętrzne i korporacyjne, 4) usługi korporacyjne. Zastępca Dyrektora Generalnego koordynuje działalność badawczą, statystyczną, publikacyjną, szkoleniową, a także 4 Programy Działań Priorytetowych, tj. 1) przejście z gospodarki nieformalnej do formalnej, 2) sprawiedliwe transformacje w kierunku zrównoważonych środowiskowo gospodarek i społeczeństw, 3) rezultaty w zakresie godnej pracy w łańcuchach dostaw, 4) godna praca w sytuacjach kryzysowych i pokryzysowych.

Biuro ILO ds. Działalności Pracowników (ang. Bureau for Workers' Activities, ACTRAV) stanowi główne ogniwo łączące Międzynarodowe Biuro Pracy ze światem pracy za pośrednictwem jednego z jej podmiotów konstytutywnych, tj. organizacji pracowniczych. Z kolei Biuro ILO ds. Działalności Pracodawców (ang. Bureau for Employers' Activities, ACT/EMP) pomaga organizacjom pracodawców i przedsiębiorstw w budowaniu silnych, niezależnych i reprezentatywnych organizacji.

Instrumenty prawne ILO opracowywane są przez przedstawicieli rządów, pracodawców i pracowników, a następnie przyjmowane na corocznej Międzynarodowej Konferencji Pracy. Konwencje i protokoły stanowią prawnie wiążące umowy międzynarodowe, które po ratyfikacji przez państwa członkowskie rodzą zobowiązania prawne, natomiast zalecenia to niewiążące akty o charakterze wytycznych, służące ukierunkowaniu polityk i praktyk krajowych. Konwencja zazwyczaj określa podstawowe zasady i ramowe zobowiązania, natomiast powiązane z nią zalecenie rozwijają ją, dostarczając szczegółowych wskazówek wdrożeniowych. Zalecenia mogą również funkcjonować samodzielnie, niezależnie od konwencji. Fundamentalne konwencje ILO to:

- nr 87 dotycząca wolności związkowej i ochrony praw związkowych z dnia 9 lipca 1948 r.;
- nr 98 dotycząca stosowania zasad prawa organizowania się i rokowań zbiorowych z dnia 1 lipca 1949 r.;

- nr 29 dotycząca pracy przymusowej lub obowiązkowej z dnia 28 czerwca 1930 r. i protokół z dnia 11 czerwca 2014 r.;
- nr 105 o zniesieniu pracy przymusowej z dnia 25 czerwca 1957 r.;
- nr 138 dotycząca najniższego wieku dopuszczenia do zatrudnienia z dnia 26 czerwca 1973 r.;
- nr 182 dotycząca zakazu i natychmiastowych działań na rzecz eliminowania najgorszych form pracy dzieci z dnia 17 czerwca 1999 r.;
- nr 100 dotycząca jednakowego wynagrodzenia dla pracujących mężczyzn i kobiet za pracę jednakowej wartości z dnia 29 czerwca 1951 r.;
- nr 111 dotycząca dyskryminacji w zakresie zatrudnienia i wykonywania zawodu z dnia 25 czerwca 1958 r.;
- *nr 155 dotycząca bezpieczeństwa*, zdrowia pracowników i środowiska *pracy* z dnia 3 czerwca *1981 r.;*
- nr 187 dotycząca struktur promujących bezpieczeństwo i higienę pracy z dnia 15 czerwca 2006 r.

W obszarze zarządzania najważniejszymi konwencjami ILO są:

- nr 81 dotycząca inspekcji pracy w przemyśle i handlu z dnia 11 lipca 1947 r.;
- nr 122 dotycząca polityki zatrudnienia z dnia 9 lipca 1964 r.;
- nr 129 dotycząca inspekcji pracy w rolnictwie z dnia 25 czerwca 1969 r.;
- nr 144 dotycząca trójstronnych konsultacji w zakresie wprowadzenia w życie międzynarodowych norm w sprawie pracy z dnia 21 czerwca 1976 r.

Integralną część polityki normalizacyjnej ILO stanowi mechanizm przeglądu standardów (ang. Standards Review Mechanism, SRM), w ramach którego Trójstronna Grupa Robocza SRM (powołana w 2015 r.) dokonuje przeglądu międzynarodowych standardów pracy celem przedstawienia Radzie Administracyjnej zaleceń dotyczących oceny stanu obowiązującego, braków w zakresie regulacyjnym, konkretnych i czasowo określonych działań następczych.

System nadzoru ILO nad stosowaniem konwencji i zaleceń w prawie i praktyce po przyjęciu przez Międzynarodową Konferencję Pracy i ratyfikacji przez państwa obejmuje 2 rodzaje mechanizmów:

– stały system nadzoru – polega na analizie cyklicznych sprawozdań przedkładanych przez państwa członkowskie dotyczących środków wdrożeniowych zastosowanych w celu realizacji postanowień ratyfikowanych konwencji, a także weryfikacji uwag w tym zakresie przesyłanych przez organizacje pracowników i pracodawców. Analizę przeprowadzają 2 organy:

- Komitet Ekspertów ds. Stosowania Konwencji i Zaleceń (ang. Committe of Experts on the Applications of Conventions and Recommendations, CEACR) – składający się z 20 międzynarodowych i krajowych ekspertów prawnych badających stosowanie konwencji, protokołów i zaleceń ILO przez państwa członkowskie;
- Komitet Konferencji ds. Stosowania Standardów (ang. Conference Committee on the Application of Standards, CAS) – będący komitetem stałym składającym się z delegatów rządu, pracowników i pracodawców, analizujący raporty w trybie trójstronnym (w niektórych przypadkach formułując wnioski i zalecenia dla rządów);

– procedury specjalne – obejmują mechanizmy reprezentacji oraz skarg o charakterze ogólnym, a także odrębną procedurę odnoszącą się do wolności zrzeszania się, tj.

- procedura składania oświadczeń w sprawie stosowania ratyfikowanych konwencji;
- procedura składania skarg dotyczących stosowania ratyfikowanych konwencji;
- specjalna procedura składania skarg dotyczących wolności zrzeszania się za pośrednictwem Komitetu ds. Wolności Związkowej.

Wydatki budżetu stałego pokrywają składki członkowskie ustalane zgodnie z podziałem zatwierdzonym przez Międzynarodową Konferencję Pracy. Wysokość składek przypadających na poszczególnych członków jest określana przez Radę Administracyjną, która przedkłada w tej sprawie

odpowiednie propozycje Komitetowi Finansowemu ILO. Ostateczną decyzję w zakresie podziału obciążeń finansowych podejmuje Konferencja, opierając się na sprawozdaniu przedstawionym przez Komitet Finansowy.

Członkami ILO jest 187 państw (stan na styczeń 2026). Organizacja współpracuje m.in. z Unią Europejską (w szczególności z Dyrekcją Generalną ds. Polityki Sąsiedztwa i Negocjacji, Dyrekcją Generalną ds. Partnerstw Międzynarodowych, Dyrekcją Generalną ds. Zatrudnienia, Spraw Społecznych i Włączenia Społecznego, a także wybranymi delegacjami UE w Azji w obszarze zasad i prawa pracy), Organizacją Narodów Zjednoczonych (organami, programami, funduszami, komisjami), agencjami wyspecjalizowanymi ONZ, licznymi organizacjami regionalnymi i międzynarodowymi, przedstawicielami sektora prywatnego, instytucjami finansowymi (Bankiem Światowym, Afrykańskim Bankiem Rozwoju, Międzynarodowym Funduszem Walutowym). Jest również partnerem Współpracy Południe-Południe odnoszącej się do współpracy rozwojowej między krajami rozwijającymi się na globalnym Południu, a także współpracy trójstronnej w sytuacji, gdy współpraca PP jest realizowana przy wsparciu partnera z północy. Angażuje się także w inne partnerstwa wielostronne, np. Globalną koalicję na rzecz sprawiedliwości społecznej, Międzynarodową sieć biznesu i osób niepełnosprawnych, Międzynarodową koalicję na rzecz równych płac, Globalny akcelerator do spraw zatrudnienia i ochrony socjalnej na rzecz sprawiedliwej transformacji, Globalną sieć biznesową do spraw zabezpieczenia społecznego, Sieć ochrony socjalnej, wolności i sprawiedliwości dla pracowników.

Projekty i programy współpracy rozwojowej ILO obejmują:

- Program partnerstwa na rzecz poprawy perspektyw osób przymusowo przesiedlonych i społeczności przyjmujących (PROSPECTS) w obszarze edukacji ochrony socjalnej i godnej pracy. Czas trwania: 1 stycznia 2019 – 31 grudnia 2027. Inicjatywie przewodzi rząd Holandii, a partnerami są ILO, Międzynarodowa Korporacja Finansowa, Wysoki Komisarz Narodów Zjednoczonych ds. Uchodźców, Fundusz Narodów Zjednoczonych na rzecz Dzieci i Bank Światowy;
- program Lepsza Praca (Better Work) łączący wszystkie szczeble przemysłu odzieżowego celem poprawy warunków pracy,

poszanowania praw pracowniczych, konkurencyjności przedsiębiorstw odzieżowych i obuwniczych, realizowany przy współpracy ILO i Międzynarodowej Korporacji Finansowej;
- projekt Vision Zero Fund (VZF) będący inicjatywą G7 mającą na celu zapobieganie zgonom, urazom i chorobom związanym z pracą w globalnych łańcuchach dostaw. Czas trwania: 1 czerwca 2016 – 1 czerwca 2020;
- Alliance 8.7 stanowiący globalne partnerstwo wspierające rządy w osiąganiu celu 8.7 Agendy 2030. Promuje ono: 1) przyspieszenie działań na rzecz wyeliminowania pracy przymusowej, współczesnego niewolnictwa, handlu ludźmi i pracy dzieci; 2) badania, gromadzenia danych i wymiany wiedzy na temat skali zjawiska i skutecznych rozwiązań; 3) stymulowanie innowacji i efektywne wykorzystanie zasobów.

Instrument programowy ILO na poziomie krajowym stanowią Krajowe programy na rzecz godnej pracy (ang. Decent Work Country Programmes, DWCPs), które identyfikują priorytety podmiotów organizacji w danym kraju i określają planowane wsparcie celem osiągania rezultatów w ramach tych priorytetów.

Klaudia Cenda-Miedzińska

International Labour Organization (ILO), *Constitution of the International Labour Organisation (ILO)*, 1.04.1919; International Labour Organization, https://www.ilo.org/about-ilo (dostęp 24.01.2026); International Labour Organization, *ILO Development Cooperation Strategy 2020–25*, GB.340/POL/6, 12.10.2020; International Labour Organization, *The ILO Governing Body at a glance*, ILO, 1.02.2023; International Labour Organization, *The ILO's Strategic Plan for 2026–29 – Delivering social justice through decent work in times of uncertainty*, GB.352/PFA/1, 30.09.2024; International Labour Organization, *The International Labour Conference at a glance*, ILO, 19.05.2023; D. Maul, *The International Labour Organization. 100 years of global social policy*, De Gruyter Oldenbourg, Berlin 2019.

MIĘDZYNARODOWE WIELOSTRONNE PARTNERSTWO PRZECIWKO ZAGROŻENIOM INTERNETOWYM (ang. International Multilateral Partnership Against Cyber Threats, IMPACT). Publiczno-prywatne przedsięwzięcie i organ wykonawczy ITU (Międzynarodowego Związku Telekomunikacyjnego,

International Telecommunication Union). Siedziba organizacji IMPACT znajdowała się w Cyberjaya, w Malezji, która była zarazem siedzibą GCA (Globalnej Agendy Cyberbezpieczeństwa, Global Cybersecurity Agenda).

Historia IMPACT rozpoczęła się w 2006 r., kiedy to podczas ceremonii zamknięcia 15 Światowego Kongresu Technologii Informacyjnych ogłoszono inicjatywę powstania organizacji. W 2008 r. ITU i IMPACT podpisały memorandum o porozumieniu i właśnie wtedy organizacja została wybrana na siedzibę Globalnej Agendy Cyberbezpieczeństwa (GCA) ITU. Początkowo organizacja była znana jako Międzynarodowe Wielostronne Partnerstwo Przeciwko Cyberterroryzmowi (ang. International Multilateral Partnership Against Cyber-Terrorism), jednak w 2008 r. zmieniono nazwę na Międzynarodowe Wielostronne Partnerstwo Przeciwko Zagrożeniom Internetowym. W 2011 r., podczas Forum Szczytu Światowego Społeczeństwa Informacyjnego 2011 w Genewie IMPACT formalnie stał się organem wykonawczym ds. cyberbezpieczeństwa wyspecjalizowanej agencji ONZ – ITU. Organizacja została wtedy zobowiązana przez ITU do świadczenia pomocy w zakresie cyberbezpieczeństwa państwom członkowskim ITU, a także innym organizacjom w ramach systemu ONZ. Wszystkie działania w ramach partnerstwa ITU z Międzynarodowym Wielostronnym Partnerstwem Przeciwko Zagrożeniom Internetowym zakończyły się w 2016 r. IMPACT ogłosił formalne rozwiązanie na początku 2018 r., co oznaczało natychmiastowe wypowiedzenie porozumienia i umowy o współpracy podpisanej między stronami.

Jako pierwszy na świecie kompleksowy sojusz na rzecz walki z cyberzagrożeniami IMPACT zrzeszał rządy, środowisko akademickie i ekspertów branżowych, aby zwiększyć możliwości globalnej społeczności w zakresie radzenia sobie z cyberzagrożeniami. IMPACT oferował państwom członkowskim ITU dostęp do wiedzy specjalistycznej, infrastruktury i zasobów, aby skutecznie przeciwdziałać cyberzagrożeniom, a także wspierał agencje Organizacji Narodów Zjednoczonych w ochronie infrastruktury ICT. IMPACT wspierał kraje partnerskie w budowaniu i rozwijaniu zdolności związanych z funkcjonowaniem narodowych zespołów reagowania na incydenty komputerowe (CIRT), które obejmowały 3 główne obszary:

- ocena zdolności CIRT – IMPACT analizował, jak krajowy CIRT radzi sobie z identyfikacją, zarządzaniem i reagowaniem na

cyberzagrożenia. Oceniał także efektywność i strukturę zespołu w celu upewnienia się, że wszelkie incydenty są obsługiwane zgodnie z najlepszymi praktykami;
- ocena gotowości do utworzenia CIRT – IMPACT oceniał gotowość kraju do powołania tego zespołu, o ile jeszcze go nie posiadał. W tym celu analizował stan cyberbezpieczeństwa, określał potrzeby kraju, wskazywał wymagania organizacyjne i instytucjonalne potrzebne do ustanowienia CIRT, a także przygotowywał zalecenia dotyczące wzmocnienia bezpieczeństwa w danym kraju;
- wdrożenie CIRT – IMPACT przeprowadzał proces wdrożeniowy, a w jego ramach tworzył i uruchamiał narodowy CIRT z podstawowym zestawem usług, zapewniał szkolenia dla urzędników do obsługi CIRT oraz przygotowywał i testował procedury operacyjne.

Oprócz tego dla krajów partnerskich IMPACT przeprowadzał wewnętrzne i zewnętrzne oceny podatności w celu wykrycia luk w zabezpieczeniach, a także ich szybkiego usunięcia. Dzięki takim ocenom partnerzy mogli zidentyfikować zagrożenia w swojej infrastrukturze, uzyskać wsparcie w minimalizowaniu szkód i utracie danych czy zaplanować działania naprawcze. Dodatkowo IMPACT oferował swoim klientom 2 rodzaje testów penetracyjnych: wewnętrzne (kompleksowe testy bezpieczeństwa wszystkich systemów bezpośrednio i pośrednio powiązanych z firmą) i zewnętrzne (koncentrujące się na identyfikacji i weryfikacji luk w zabezpieczeniach wszystkich usług dostępnych w internecie w ramach krytycznej infrastruktury IT organizacji). Testy penetracyjne polegają na testowaniu systemów komputerowych lub sieci w celu wykrycia słabych punktów w zabezpieczeniach, które później mógłby wykorzystać atakujący.

Będąc partnerem ITU-IMPACT, kraje posiadały bezpłatny dostęp do specjalistycznych narzędzi i systemów GRC, takich jak NEWS (ang. Network Early Warning System) i ESCAPE (ang. Electronically Secured Collaborative Application Platform for Experts), które pomagały im zwalczać nowe i rozwijające się zagrożenia cybernetyczne.

NEWS to platforma łącząca informacje pochodzące od wielu sojuszy i dostawców rozwiązań cyberbezpieczeństwa, której celem jest terminowe

dostarczanie właściwych informacji odpowiednim władzom, umożliwiając im skuteczne reagowanie na cyberzagrożenia. Dodatkowo NEWS zarządza uprawnieniami i bezpieczeństwem informacji w zakresie gromadzonych danych.

ESCAPE to narzędzie, które umożliwia ekspertom ds. cyberbezpieczeństwa z różnych krajów dzielenie się specjalistyczną wiedzą, łączenie zasobów i zdalną współpracę. Platforma ESCAPE umożliwia GRC pełnienie funkcji kompleksowego centrum koordynacji i reagowania dla krajów w czasach kryzysu, umożliwiając szybką identyfikację i udostępnianie zasobów. Przyspiesza ona reagowanie ITU-IMPACT na cyberzagrożenia.

Istnieje kilka inicjatyw, których twórcą był IMPACT, m.in.

- Centrum Zapewnienia Bezpieczeństwa i Badań (ang. Centre for Security Assurance & Research),
- Centrum Szkoleń i Rozwoju Umiejętności (ang. Centre for Training & Skills Developments),
- GRC – Globalne Centrum Reagowania (ang. Global Response Centre).

W obliczu rosnącej liczby zagrożeń cybernetycznych współpraca międzynarodowa stała się istotnym elementem budowania bezpieczeństwa. Ważną rolę odegrał tutaj IMPACT, nawiązując partnerstwa z wiodącymi organizacjami czy instytucjami zajmującymi się cyberbezpieczeństwem. Warto przywołać również dokument zatytułowany Draft Cooperation Agreement between the International Criminal Police Organization – INTERPOL and the International Multilateral Partnership Against Cyber Threats (IMPACT), który zatwierdzony został w dniach 5–8 listopada 2012 r., podczas Zgromadzenia Ogólnego Interpolu w Rzymie, we Włoszech, a także umowę o współpracy między Interpolem a IMPACTEM podpisaną 8 listopada 2012 r. w Rzymie. Zgodnie z umową strony w stosownych przypadkach i zgodnie z jej celem mogły korzystać ze specjalistycznej wiedzy w dziedzinie cyberbezpieczeństwa. Dążyły one w szczególności do:

- wyznaczenia i utrzymywania właściwych punktów kontaktowych w celu rozwijania i koordynowania komunikacji między stronami;
- wymiany informacji na temat informatyki śledczej i analizy złośliwego oprogramowania, a także innych informacji

analitycznych istotnych z punktu widzenia cyberbezpieczeństwa, z wyłączeniem danych osobowych;
- promowania budowania potencjału poprzez wzajemną pomoc i udział w sesjach szkoleniowych i konferencjach;
- regularnych konsultacji za pośrednictwem wyznaczonych punktów kontaktowych w kwestiach objętych umową, jak i w sprawach stanowiących przedmiot wspólnego zainteresowania związanych z obszarem cyberbezpieczeństwa.

W ramach umowy strony zobowiązały się do zapewnienia bezpieczeństwa i poufności wszelkich dokumentów i informacji wymienianych pomiędzy nimi: przekazywanie danych do Interpolu podlegało zasadom i regulaminom IMPACT, a do IMPACT – zasadom i regulaminom Interpolu. Istotne było także nawiązanie współpracy Kaspersky Lab z Międzynarodowym Związkiem Telekomunikacyjnym oraz Międzynarodowym Wielostronnym Partnerstwem Przeciwko Cyberzagrożeniom. Firma miała uczestniczyć w dyskusjach na wysokim szczeblu na temat cyberbezpieczeństwa podczas szczytu liderów na konferencji ITU Telecom World 2012, kiedy to poruszane były kwestie związane z ograniczaniem ryzyka związanego z dużymi skoordynowanymi cyberatakami oraz zacieśnianiem współpracy międzynarodowej.

W ramach swojej misji wzmocnienia globalnego bezpieczeństwa cyfrowego Międzynarodowe Wielostronne Partnerstwo Przeciwko Zagrożeniom Internetowym angażowało się w międzynarodowe inicjatywy i projekty, które podnosiły poziom przygotowania państw na zagrożenia cybernetyczne. Jedną z nich były ćwiczenia, które zorganizowano w grudniu 2011 r. w Azji Południowo-Wschodniej i były to pierwsze na świecie transgraniczne ćwiczenia wojskowe zorganizowane przez organizację międzynarodową i agencję Organizacji Narodów Zjednoczonych. Ćwiczenia zostały zainicjowane przez ITU-IMPACT ALERT (ang. Applied Learning for Emergency Response Team) i obejmowały symulację reakcji na cyberataki, w której uczestniczyły zespoły reagowania na incydenty komputerowe (CERT/CIRT) m.in. z Wietnamu, Kambodży i Laosu, a także eksperci z ITU-IMPACT.

Kolejne były ćwiczenia z zakresu cyberbezpieczeństwa, które zorganizowane zostały przez Międzynarodowy Związek Telekomunikacyjny

i Międzynarodowe Wielostronne Partnerstwo Przeciwko Zagrożeniom Cybernetycznym (ITU-IMPACT), a także Ministerstwo Transportu, Gospodarki Morskiej i Łączności Turcji oraz Urząd ds. Technologii Informacyjnych i Komunikacyjnych (ICTA) w dniach 15–16 maja 2014 r. w Stambule, w Turcji. Miały na celu wzmocnienie międzynarodowego bezpieczeństwa cybernetycznego i przyciągnęły 17 krajów, takich jak Turcja, Albania, Angola, Ukraina, Rumunia, Azerbejdżan, Sudan, Bośnia i Hercegowina, Bułgaria, Hiszpania, Gruzja, Włochy, Jordania, Litwa, Malezja, Senegal i Sri Lanka. Podczas ćwiczeń odbyły się prezentacje ekspertów w dziedzinie cyberbezpieczeństwa, warsztaty poświęcone kryminalistyce, bezpieczeństwu mobilnemu i standaryzacji w cyberbezpieczeństwie, a także ochronie dzieci w internecie. Krajowe zespoły CIRT wzięły z kolei udział w serii symulacji rzeczywistych zagrożeń cybernetycznych w celu ocenienia swoich możliwości radzenia sobie z incydentami.

W dniach 22–24 września 2014 r. w Port Vila, na Vanuatu przeprowadzono również Warsztaty na Rzecz Budowania Potencjału Wysp Pacyfiku w zakresie Ochrony Dzieci w Internecie, które zorganizowały Międzynarodowy Związek Telekomunikacyjny i Organizacja Telekomunikacyjna Wspólnoty Narodów (CTO), we współpracy z IMPACT oraz Regulatorem Telekomunikacji i Radiokomunikacji Vanuatu (TRR), Biurem Głównego Dyrektora ds. Informacji Rządowej Vanuatu (OGCIO) oraz przy wsparciu Departamentu Łączności Australii. Głównym celem warsztatów było podniesienie świadomości na temat problemów związanych z bezpieczeństwem dzieci w internecie – obejmowały 5 filarów Inicjatywy na rzecz Ochrony Dzieci w Internecie:

- budowanie potencjału;
- środki prawne;
- współpraca międzynarodowa;
- środki techniczne i proceduralne;
- struktura organizacyjna.

Uczestnicząc w licznych inicjatywach i wydarzeniach na całym świecie, IMPACT zyskał uznanie jako wiarygodna organizacja w dziedzinie cyberbezpieczeństwa dla agencji medialnych na całym świecie. IMPACT był prezentowany w wielu agencjach medialnych, m.in. Al Jazeera, CNN, SC Magazine, CNBC, UNTV czy FutureGov TV. Dodatkowo za wkład

w globalną operacjonalizację GCA ITU otrzymał podwójne wyróżnienie podczas programu Asia Pacific Information Security Leadership Achievements (ISLA) 2010 zorganizowanego przez (ISC)2 w Singapurze.

Od 2009 do 2013 r. IMPACT ocenił i wdrożył CIRT w ponad 45 krajach, ufundował ponad 300 stypendiów w blisko 40 krajach, przeszkolił około 1600 praktyków i specjalistów ds. cyberbezpieczeństwa w niemal 80 krajach i przeprowadził ćwiczenia cybernetyczne dla CIRT/CERT w 70 krajach w 4 regionach.

Lucyna Łowisz

N. Choucri, S. Madnick, J. Ferwerda, *Institutions for Cyber Security: International Responses and Global Imperatives*, „Information Technology for Development" 2014, no. 20(2), https://doi.org/10.1080/02681102.2013.836699; *First Pacific Islands Capacity Building Workshop on Child Online Protection and Commonwealth National Cybersecurity Framework Regional Workshop, 22–24 September 2014, Port Vila, Vanuatu*, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2014/September-COP/home.aspx (dostęp 8.12.2025); *IMPACT (International Multilateral Partnership Against Cyber Threats)*, https://www.linkedin.com/company/international-multilateral-partnership-against-cyber-threats-impact- (dostęp 7.12.2025); *IMPACT Annual Book*, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT_AnnualBook.pdf (dostęp 8.12.2025); International Criminal Police Organization – INTERPOL and the International Multilateral Partnership Against Cyber Threats (IMPACT), *International Criminal Police Organization – INTERPOL and the International Multilateral Partnership Against Cyber Threats (IMPACT) on cooperation in the field of cyber security*; International Criminal Police Organization – INTERPOL, *81st INTERPOL General Assembly*, https://www.interpol.int/News-and-Events/Events/2012/81st-INTERPOL-General-Assembly (dostęp 8.12.2025); *International Cyber Shield Exercise 2014, 15–16 May 2014*, Istanbul, Turkey, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Turkey_cyberdrill_2014.aspx (dostęp 8.12.2025); *International Multilateral Partnership Against Cyber Threats*, https://dig.watch/actor/international-multilateral-partnership-against-cyber-threats (dostęp 9.12.2025); *International Multilateral Partnership Against Cyber Threats*, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_IMPACT_infopack_.pdf (dostęp 8.12.2025); *International Multilateral Partnership Against Cyber Threats, Overview*, https://www.itu.int/ITU-D/conferences/rpm/2009/asp/documents/IMPACTOverview.pdf (dostęp 8.12.2025); INTERPOL, Draft Cooperation Agreement between the International Criminal

Police Organization – INTERPOL and the International Multilateral Partnership Against Cyber Threats (IMPACT), AG-2012-RES-07; *ITU-D ICT Applications and Cybersecurity Division Publications*, https://www.itu.int/ITU-D/cyb/publications/ (dostęp 9.12.2025); *ITU-IMPACT establishes first Cybersecurity Innovation Centre for Arab region*, „Telecom Standards" 2013, no. 22(12); J.A. Lewis, *National Perceptions of Cyber Threats*, „Strategic Analysis" 2014, no. 38(4), https://doi.org/10.1080/09700161.2014.918445; The NATO Cooperative Cyber Defence Centre of Excellence, *ITU-IMPACT's First Regional Cyber Security Centre in the Arab World*, https://ccdcoe.org/incyder-articles/itu-impacts-first-regional-cyber-security-centre-in-the-arab-world/ (dostęp 9.12.2025); A. Ntoko, *Global Cybersecurity Agenda (GCA) A framework for international cooperation, Presentation*, https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf (dostęp 9.12.2025); V. Philip, *ITU-IMPACT, Regional Cybersecurity Forum – CLMV*, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2013/ITU%20Cybersecurity%20Workshop%20and%20Cyberdrill_Vientiane_Lao_PDR/Presentation/CLMV-ALERT-2013-ITU-IMPACT-Case-Studies-Philip.pdf (dostęp 8.12.2025); *Press Release "ITU teams up with Kaspersky Lab for ITU Telecom World 2012"*, https://www.itu.int/net/pressoffice/press_releases/2012/30.aspx (dostęp 9.12.2025); *Press Release 2011 ITU-IMPACT ALERT*, https://www.itu.int/net/pressoffice/press_releases/2011/50.aspx (dostęp 8.12.2025); J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy* [rozprawa doktorska], Białystok 2017.

MIĘKKA SIŁA (ang. *soft power*) – zdolność państwa do osiągnięcia swoich celów, pozyskiwania sojuszników, zdobywania i wywierania wpływów na inne państwa dzięki atrakcyjności własnej kultury, wartości społecznych i politycznych, instytucji, a nie na drodze zastraszania czy przymusu, dominacji zbrojnej, twardej siły (*hard power*), podstawą której jest nacisk wojskowy i ekonomiczny.

Soft power charakteryzuje pozycję państwa na arenie międzynarodowej i jest połączeniem potencjału gospodarczego i taktyki działań. Koncepcja ta została po raz pierwszy sformułowana przez amerykańskiego politologa, profesora Uniwersytetu w Harvardzie Josepha Nye'a Jr. w 2004 r., który podkreślał, że *soft power* to możliwość otrzymania tego, czego się chce, za pośrednictwem atrakcji, a nie przymusu lub płatności. W swojej koncepcji „miękkiej siły" Nye pokazał, że jej realizacja pozwala państwom

wpływać na świat zewnętrzny znacznie bardziej efektywnie niż przy użyciu środków wojskowych lub ekonomicznych.

„Państwo może osiągnąć pożądane rezultaty dla siebie w polityce światowej, ponieważ inne kraje – podziwiając jego wartości, naśladując jego przykład, aspirujących do poziomu dobrobytu i otwartości – chcą iść za nim", napisał Nye w swojej książce *Miękka siła: środek do osiągnięcia sukcesu w polityce światowej*. Miękka siła jest oparta na tradycjach i kulturze narodu, nie stanowi wytworu propagandy, ale powstaje na skutek atrakcyjnego rozwoju, i właśnie tak rozumieją miękką siłę państwa zachodnio-demokratyczne. Istnieją 3 główne sposoby dla osiągnięcia celu: przymus (kij), wynagrodzenie (marchewka) i atrakcyjność (miękka siła).

Nye określił pojęcie *soft power* jako zdolność kształtowania preferencji innych dzięki atrakcyjności i przyciągania za pomocą posiadanych zasobów, do których zaliczył kulturę, wartości i styl uprawiania polityki zagranicznej, chociaż są trudności z określeniem uniwersalnych zasad, metod i weryfikowalnych wyników badań.

Koncepcja ponad dziesięciolecie blisko dekadę temu zaczęła być postrzegana jako strategia informacyjnego wpływu na zagraniczną publiczność medialną poprzez informacje o kulturze, sztuce, tradycjach narodów.

Pojęcie to ma głębokie korzenie filozoficzne; idea atrakcyjności i przyciągania jako forma władzy pochodzi od starożytnych chińskich filozofów takich jak Lao Tzu (VII w. p.n.e.). Miękką siłę mogą posiadać nie tylko państwa, ale wszystkie podmioty polityki międzynarodowej, takie jak organizacje pozarządowe lub agencje międzynarodowe. Celem *soft power* państwa jest taka polityka w stosunkach międzynarodowych, z którą inne rządy będą się utożsamiać, dla której będą wykazywać zrozumienie i której wartości będą podzielać.

W ostatnich latach powstaje coraz więcej wskaźników tego pojęcia. Podczas gdy *hard power* służy raczej celom odstraszania i przymuszania, miękka siła to przyciąganie; będąc z natury nieprzymusową, pozwala na perswazję oraz stymulowanie innych do współpracy.

Komponenty miękkiej siły państwa to:

– wizerunek kraju w świecie: eksport filmów, muzyki, książek, kultury państwa, która przyciąga innych, dyplomacja, aktywna obecność reprezentantów kraju na forach organizacji

międzynarodowych, pomoc o charakterze materialno-techniczno-finansowym dla krajów rozwijających się, publiczna dyplomacja, zainteresowanie językiem w innych krajach, sukcesy sportowe;
- wartości w polityce wewnętrznej i zagranicznej: wolność, równość i sprawiedliwość; praworządność, uczciwość, porządek społeczny, jakość instytucji państwowych, poziom wolności osobistej, procent elektoratu uczestniczący w wyborach, stosunek do środowiska naturalnego;
- stopień integracji ze światem: stosunki zewnętrzne, rozwój bezpośrednich kontaktów z zagranicznymi odbiorcami poprzez system wymiany i programy stypendiów naukowych dla cudzoziemców; udział w instytucjach światowych, inwestycje zagraniczne, liczba imigrantów urodzonych za granicą, poziom rozwoju turystyki; pozycja wyższych uczelni w publikowanych rankingach, poziom płynnego komunikowania się w obcych językach.

W raporcie Index Mocy Państw 2018 Piotr Arak i Grzegorz Lewicki podkreślają, że siła miękka to umiejętność wpływania na innych poprzez przyciąganie, perswazję i sympatię, a nie twardą politykę przymusu i pieniędzy. Źródłem „miękkiej siły" jest często dobrze opowiedziana historia.

Ponieważ miękka siła wyłoniła się jako alternatywa dla twardej polityki, bardziej pasuje do etycznie myślących naukowców i polityków, jednak ma charakter opisowy, a nie normatywny. Jak każda forma siły, może być wykorzystywana w różnych celach. Po II wojnie światowej Związek Radziecki wykorzystywał „miękkie" środki oddziaływania, takie jak ideologia komunistyczna, „mit nieuchronności" (*the myth of inevitability*) i ponadnarodowe instytucje komunistyczne. Ponieważ użycie siły stało się bardziej kosztowne, jej mniej „groźne" formy zyskały na atrakcyjności.

Wszechstronność procesu globalizacji zmniejszyła przestrzeń dla wykorzystania tradycyjnych mechanizmów władzy przez państwa i doprowadziła do zmiany wzorców globalnej konkurencji. W nowej erze sukces ekonomiczny, przekonanie ideologiczne i atrakcyjność kulturowa kraju stały się ważniejszym czynnikiem wpływu niż potęga militarna i posiadanie broni jądrowej.

„Miękka siła" była odpowiedzią na zmiany, które zaszły w systemie międzynarodowym na przełomie wieków XX i XXI, i zaczęła funkcjonować jako ważne narzędzie polityki zagranicznej. Eksperci twierdzą, że „miękka siła" stała się centralną koncepcją rozumienia współczesnych stosunków międzynarodowych – jest mocno zakorzeniona w praktyce polityki zagranicznej wielu krajów świata, a dzięki tej popularności rządy zaczęły aktywnie wdrażać strategie komunikacyjne w polityce zagranicznej: zdobywać zaufanie partnerów, kształtować wizerunek swojego kraju w mediach i nawiązywać bliskie więzi z zagraniczną publicznością. Państwo, które nie uwzględnia koncepcji „miękkiej siły" w swojej strategii polityki zagranicznej, jest raczej wyjątkiem – daje to możliwość zintensyfikowania zasobów wpływów zewnętrznych, które mogą być bardziej skuteczne we współczesnym świecie w kontekście globalizacji.

Pojęcie „miękkiej siły" w Federacji Rosyjskiej zyskało popularność i zostało wprowadzone w oficjalnych dokumentach polityki zagranicznej; ponadto utworzono instytucje, które miały za zadanie koordynować stosowanie tego rodzaju narzędzi w polityce międzynarodowej – są to programy w dziedzinie upowszechniania i wzmacniania pozycji języka rosyjskiego na świecie, projekty kulturalne, wymiana młodzieży, współpraca w nauce, edukacja zagranicznych studentów na rosyjskich uniwersytetach, rosyjskie serwisy eksperckie i think tanki.

Rosyjska interpretacja *soft power* charakteryzuje się negatywną i nieufną postawą, zrównując tę koncepcję z metodami manipulowania świadomością, propagandą, wojną psychologiczną i kontrolowanym chaosem. Rosyjskie kierownictwo stworzyło wiele instytucji, których zadaniem było zintegrowane wykorzystanie narzędzi miękkiej siły w polityce zagranicznej – należą do nich agencja Rossotrudnichestvo, Fundacja Russki Mir, Fundacja Rozwoju Dyplomacji Publicznej im. A. Gorczakowa (ros. *Фонд развития публичной дипломатии им. А.Г. Горчакова*), a także wiele ośrodków analitycznych i serwisów eksperckich. Utworzono kanały informacyjne, takie jak RT, MIA Russia Today, Sputnik, które jako narzędzia „miękkiej siły" mają prezentować światu wydarzenia międzynarodowe zgodne z interesami polityki zagranicznej Rosji. W latach 2012–2021 Federacja Rosyjska przeprowadziła udane prace nad zwiększeniem obecności oficjalnych struktur polityki zagranicznej w międzynarodowej przestrzeni

informacyjnej, w szczególności w sieciach społecznościowych: konta MSZ, jego departamentów i kierownictwa pojawiły się w głównych sieciach społecznościowych – pozwoliło to przedstawić rosyjski punkt widzenia na wydarzenia światowe, na szeroką skalę. Głównymi elementami rosyjskiego mechanizmu wykorzystywania narzędzi *soft power* są instytucje rządowe, fundusze prorządowe i organizacje publiczne, a także kanały informacyjne; konserwatywne wartości tradycyjnej rodziny i tradycyjnego społeczeństwa z wyraźną rolą religii.

Jeżeli *soft power* w sensie klasycznym oznacza przyciąganie i perswazję, to w przypadku Rosji granica między „miękką siłą" a dezinformacją jest często płynna i łączy się z elementami propagandy, narracji historycznych, mediów państwowych oraz inwestycji kulturowych i edukacyjnych. Po pełnoskalowej inwazji na Ukrainę, w lutym 2022 r. reputacja Rosji na świecie znacząco osłabła; jej *soft power* zmniejszyła się w rankingach międzynarodowych – według indeksów z 6,4 (2022) do 5,6 (2025). Wielu analityków podkreśla, że agresja podważyła klasyczne instrumenty przyciągania Rosji – ludzie i państwa zrezygnowali z pozytywnych skojarzeń z Moskwą, co osłabiło tradycyjny *soft power*.

Główne narzędzia rosyjskiej miękkiej siły w latach 2022–2025:

- rosyjskie instytucje, media państwowe i elity polityczne odwołują się do historii, religii i tożsamości jako narzędzi miękkiej siły, aby legitymizować swoje działania wobec Ukrainy i krajów postsowieckich oraz utrwalać wizerunek Rosji jako „obrońcy wspólnej cywilizacji". Ta narracja łączy elementy historyczne z imperialnymi o „jedności cywilizacyjnej", wykorzystując takie techniki, jak odwołania do wspólnej historii i kultury, narracje religijne i moralne uzasadniające działania polityczne, wykorzystanie literatury, sztuki i filmu do szerzenia symbolicznych przekazów;
- rosyjskie propagandowe media państwowe (np. RT, Sputnik) próbują utrzymać i rozszerzać wpływ w różnych częściach świata, ponieważ po 2022 r. wiele krajów zablokowało oficjalne nadawanie tych mediów, co ograniczyło ich wpływ; mimo to kanały te próbują omijać zakazy np. poprzez wykup czasu antenowego lub przekazy online. W praktyce media stają się

instrumentem propagandy państwowej, a nie klasycznym narzędziem *soft power*, co wiąże się z ograniczeniem ich atrakcyjności dla niezależnych odbiorców;
- jednym z celów rosyjskiej strategii jest budowanie wpływów poprzez edukację i studia zagraniczne: oferowanie stypendiów dla studentów z Afryki i Bliskiego Wschodu – narzędzie mające kształtować przychylne elity przyszłości. Takie programy są postrzegane jako próba długofalowego wpływu międzynarodowego;
- Rosja prowadzi intensywne kampanie informacyjne, które łączą klasyczne techniki *soft power* (kultura, narracje) z elementami dezinformacji i *sharp power* – agresywnych, manipulacyjnych działań mających na celu wpływanie na opinię publiczną innych państw. Przykładem jest operacja Doppelgänger – rosyjska kampania dezinformacyjna mająca na celu osłabienie poparcia dla Ukrainy w Europie i USA poprzez fałszywe narracje i media podszywające się pod zachodnie portale;
- rosyjskie służby i powiązane podmioty stosują techniki psychologicznego oddziaływania w mediach społecznościowych, m.in. rozsyłanie ustrukturyzowanych narracji przez boty i prorosyjskie konta, nacisk na lokalne społeczności poprzez dedykowane kampanie. Przykładowo w okupowanych częściach Ukrainy tysiące automatycznych wiadomości miały na celu wpływać na postawy lokalnej ludności i podważać ukraińską tożsamość.

Cele rosyjskiej miękkiej siły 2022–2025:
- utrwalenie i legitymizacja narracji Kremla przedstawiających Rosję jako obrończynię wartości i historii, a nie agresorkę;
- osłabianie solidarności międzynarodowej wobec Ukrainy, wpływając na nastroje społeczne w UE i USA w celu zmniejszenia poparcia dla sankcji i pomocy militarnej;
- kreowanie alternatywnych elit w krajach globalnego Południa poprzez programy edukacyjne i współpracę naukową (np. w Afryce).

Atak na Ukrainę obniżył potencjał *soft power* Rosji i doprowadził do jej spadku w rankingach międzynarodowych. Wiele krajów zakazało

nadawania rosyjskich mediów państwowych, co ograniczyło zasięg narracji i wymusiło stosowanie alternatywnych technik omijających.

Rosyjska miękka siła po 2022 r. stała się bardziej narzędziem hybrydowym, łączącym klasyczne narracje z agresywną propagandą i dezinformacją. *Soft power* musiała ustąpić miejsca *sharp power* (bardziej konfrontacyjnym narzędziom wpływu), gdy tradycyjne metody zawiodły w obliczu światowego sprzeciwu wobec inwazji. Rosyjskie działania miękkiej siły są skierowane zarówno do państw globalnego Południa (edukacja, młode elity), jak i społeczeństw zachodnich.

Aktualne wydarzenia pokazują, że działania w ramach miękkiej siły mogą przyczyniać się do destabilizacji sytuacji, obejmować faktyczną aneksję terytorium lub niszczenie infrastruktury, ale jednocześnie narażają państwo stosujące te środki na utratę wsparcia i solidarności międzynarodowej. Rosja w Ukrainie próbowała – i próbuje! – naruszyć spokój społeczny w regionach, suwerenność państwa i legalne zarządzanie w miastach za pośrednictwem masowych akcji społecznych i prorosyjskich haseł. Agresor nie ogłosił początku wojny, a zamieszki miały wyglądać jak naturalne wewnętrzne procesy polityczne, które wywołała rewolucja godności. W ten sposób wprowadzał swoje technologię społeczne w tych jednostkach administracyjnych, które miały być polem walki, wykorzystując miękką siłę jako instrument nacisku na suwerenne państwo: konfrontacje ideologiczne (w tym dyskursy historyczne, religijne i światopoglądowe), ataki propagandowe, wojny gospodarczo-energetyczne, działalność na rzecz agresora wtajemniczonych osób. Rosyjska „miękka siła" jest taktycznym i cynicznym narzędziem stosowanym w celu osiągnięcia specyficznej geostrategicznej ambicji – to najczęściej władza, potęga bądź elastyczna siła.

Soft power Rosji w latach 2022–2025 została zredefiniowana przez presję wojny i konieczność walki o narrację. Tradycyjne instrumenty przyciągania kulturowego zmieniły się w narzędzia narracyjne i propagandowe. Rosyjska miękka siła jest dziś bardziej wskaźnikiem wojny informacyjnej niż klasycznym narzędziem perswazji.

Wsparciem dla *soft power* są media, szczególnie sieci społecznościowe, za pomocą których można tworzyć pozytywny wizerunek państwa przez kulturę, edukację, naukę, religię, sport. Jak podkreśla Robert Łoś, media są ważnym narzędziem umożliwiającym użycie *soft power* przez Rosję

– stacje telewizyjne i radiowe, prasa, portale internetowe odgrywają istotną rolę w rozpowszechnianiu informacji w środowiskach, które głównie nastawiają się na kulturę rosyjską.

Natomiast Chiny proponują bardziej rozbudowaną, azjatycką wersję *soft power*, do której zalicza się wszystkie atrybuty państwowości, z wyjątkiem sfery bezpieczeństwa, włączając inwestycje i działania pomocowe. Do tak rozbudowanego modelu dochodzą jeszcze 2 warianty: „wysoka miękka siła" (*high soft power*) – skierowana do elit, oraz „niska miękka siła" (*low soft power*) – dedykowana szerszej publiczności. Najważniejsze elementy chińskiej *soft power* to wzrost i potencjał gospodarczy; promocja w świecie chińskich wartości, kultury i języka; poparcie dla wielobiegunowego systemu międzynarodowego, w którym państwa nie ingerują w sprawy wewnętrzne innych krajów; Chińskie Radio Międzynarodowe nadające przez 24 godziny do państw południowo-azjatyckich; wzrost wsparcia finansowego dla państw Azji Południowo-Wschodniej; organizowanie podróży studyjnych (*study trips*) do ChRL i wymian studenckich; promocja turystyki (zarówno przyjazdowej, jak i wyjazdowej). Zachodni autorzy często podkreślają ukryte niebezpieczeństwo rosnącej „miękkiej siły" Chin, określając ją jako ofensywną taktykę potęgi wschodniej.

Obecnie możemy wyróżnić 5 głównych sposobów przekazywania miękkiej siły, które w taki czy inny sposób są używane na całym świecie i wymagają dużego potencjału wszystkich zasobów państwa: polityka zagraniczna (dyplomacja kulturalna, dyplomacja publiczna itp.); mass-media; instytucje, struktury sieciowe; internet i sieci społecznościowe; religia.

Miękka siła stała się integralnym elementem współczesnej polityki międzynarodowej, stanowiąc wszechstronny zestaw narzędzi umożliwiających realizację celów polityki zagranicznej poprzez wykorzystanie potencjału społeczeństwa obywatelskiego, mediów i technologii komunikacyjnych, działań humanitarnych oraz innych uzupełniających metod i instrumentów dyplomacji. Współcześnie na arenie międzynarodowej państwo dostosowuje się do nowoczesnych strategii rozwoju technologii, co sprawia, że rozwija się *soft power*, zmieniając sferę medialną w bezkonkurencyjny globalny zasób oddziaływania na umysły i aspiracje milionów ludzi. Właśnie informacja i rozpowszechnienie sieci społecznościowych pozwoliły na zdobycie nowych efektów wpływu „miękkiej siły".

O ostatecznej klasyfikacji decydują punkty przyznawane na podstawie danych instytucji oraz opinii respondentów z poszczególnych państw. Na ocenę składa się 6 kategorii: rząd (w tym jego efektywność i dyplomacja), kultura, zaangażowanie na arenie międzynarodowej, edukacja, rozwój cyfrowy, przedsiębiorczość. Pod uwagę bierze się również takie aspekty, jak np. wyniki państwa w sporcie czy liczba restauracji z gwiazdkami Michelin.

Oprócz siły miękkiej i twardej coraz bardziej zaczyna liczyć się tzw. siła ostra (inaczej *sharp power*), służąca do niejawnego wpływania na opinie publiczne krajów poprzez informację i dezinformację. W użyciu tego typu siły przodują globalne potęgi autorytarne, takie jak Rosja czy Chiny. Dla jej zwolenników nie liczy się prawda, czyli zgodność przekazywanej treści z rzeczywistością, ale wpływ na realizację interesów kraju.

W 2024 r. Stany Zjednoczone umocniły pozycję lidera w rankingu Global Soft Power Index firmy Brand Finance, osiągając rekordowy wynik i zajmując pierwsze miejsca w kategoriach znajomości i reputacji, podczas gdy Wielka Brytania pozostała na czele w obszarze kultury i edukacji, Chiny utrzymały trzecie miejsce, a kluczowym trendem stało się znaczenie gospodarki i handlu dla postrzegania siły narodu. Badanie wskazuje na wzrost znaczenia „miękkiej siły" w kontekście gospodarczym, podkreślając wpływ stabilności ekonomicznej, silnych marek i łatwości prowadzenia biznesu, oraz na większe powiązanie polityki miękkiej siły z narodowymi priorytetami, co widać w działaniach takich jak promowanie tożsamości narodowej.

Ogólne trendy wykorzystania miękkiej siły w 2024 r.:

- większa spójność polityki miękkiej siły z priorytetami gospodarczymi i politycznymi;
- zwiększone wykorzystanie miękkiej siły do promowania tożsamości narodowej.

Badaniami zostały objęte 193 państwa członkowskie ONZ: kraje wykorzystujące *soft power wydają się bardziej atrakcyjne dla inwestycji, turystyki i talentów. W zmieniającym się świecie, gdzie dominują wyzwania ekonomiczne i polityczne, postrzeganie stabilności gospodarczej staje się kluczowe dla reputacji i wpływu narodów.*

Global Soft Power Index 2025, jedno z najważniejszych zestawień oceniających siłę państw poprzez ich wpływ, wizerunek i skuteczność dyplomatyczną, umieścił Polskę na 32 miejscu w zestawieniu. Choć oznacza to

minimalny awans (o 1 pozycję względem ubiegłego roku), to – jak zauważają eksperci – nie jest to efekt poprawy działań Polski, lecz osłabienia pozycji Izraela. Wśród największych problemów Polski w kontekście *soft power* można wyróżnić zwiększanie wpływu rządu na media publiczne i odmowę przyjęcia uchodźców. Według autorów raportu osłabienie miękkiej siły wynika także z krytyki polskiego rządu przez Unię Europejską, chociaż Polska jest liczącym się podmiotem w regionie i ma dobrze rozwiniętą kulturę. Największym atutem jest z kolei branża turystyczna, za którą kryje się bogata historia i kultura. Autorzy raportu rekomendują, aby Polska, jako lider tej części Europy, zrównoważyła swoje stosunki z Brukselą, Waszyngtonem i państwami regionu, ponieważ z budowania tych relacji może osiągnąć wymierne korzyści.

Na szczycie rankingu Global Soft Power Index 2025 znalazły się Stany Zjednoczone, następnie Chiny (wysuwając się na drugą pozycję), Wielka Brytania i Japonia. To państwa, które nie tylko dysponują potężnymi gospodarkami i armiami, ale także prowadzą przemyślaną i jednolitą politykę zagraniczną. Indeks mierzy zdolność państwa do wywierania wpływu poprzez kulturę, politykę i wartości. Wyniki z 2025 r. wskazują na przesunięcie w kierunku wschodnich wpływów: Korea Południowa jest najszybciej awansującym krajem w rankingu G100, a Salwador poprawił swoją pozycję o 35 miejsc. Tymczasem państwa zaangażowane w konflikty zbrojne odnotowują spadek wskaźnika miękkiej siły.

Polityka zagraniczna wiodących państw świata jest nie do pomyślenia bez arsenałów „miękkiej siły" – totalnego przepływu informacji, który przełamuje granice wyobrażeń dotyczących niepolitycznego życia krajów i narodów. Pojęcie to jest uważane za strategię programowo-informacyjną polityki zagranicznej współczesnych państw. Zakres możliwości „miękkiej siły" i stopień jej udziału w kształtowaniu wpływu państw uważa się za pozycjonowanie ich statusu.

Znamiennym przykładem „miękkiej siły" jest polityka rozszerzenia i polityka rozwojowa Unii Europejskiej. Zastosowanie zestawu metod i instrumentów *soft power* UE poszerza stabilność i wzrost norm społecznych oraz gospodarczych.

Olga Wasiuta

G. Gallarotti, *Soft Power: What it is, Why it's Important, and the Conditions Under Which it Can Be Effectively Used*, „Journal of Political Power" 2011, vol. 4(1); *Global Soft Power Index 2025*, https://www.ucg.ac.me/skladiste/blog_45671/objava_195259/fajlovi/Global%20Soft%20Power%20Index%202025.pdf (dostęp 8.01.2026); R. Łoś, *Soft power Rosji*, „Przegląd Strategiczny" 2017, nr 10; R. Łoś, *Soft power we współczesnych stosunkach międzynarodowych*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2017; J. Nye, *The Powers to Lead*, NY Oxford University Press, Oxford 2008; J.S. Nye, *Bound to Lead: The Changing Nature of American Power*, Basic Books, New York 1990; J.S. Nye, *Przyszłość sił*, Wydawnictwo Naukowe PWN, Warszawa 2012; J.S. Nye, *Soft Power. Jak osiągnąć sukces w polityce światowej*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2007; J.S. Nye, *Soft Power. The Means to Success in World Politics*, Public Affairs, New York 2004; J.S. Nye, *What China and Russia Don't Get About Soft Power*, „Foreign Policy" 29.04.2013, http://www.foreignpolicy.com/articles/2013/04/29/what_china_and_russia_don_t_get_about_soft_power (dostęp 12.12.2025); B. Ociepka, *Miękka siła i dyplomacja publiczna Polski*, Wydawnictwo Naukowe Scholar, Warszawa 2013; M. Pławski, *„Brak strategii, niespójna dyplomacja". Polska dopiero na 32. miejscu w Global Soft Power Index 2025*, 4.10.2025, https://kresy.pl/wydarzenia/brak-strategii-niespojna-dyplomacja-polska-dopiero-na-32-miejscu-w-global-soft-power-index-2025/#goog_rewarded (dostęp 8.01.2026); *Rosja 2025: Globalne ambicje, ograniczone zasoby. Stan rosyjskiej ekonomii i polityki* [raport], https://ine.org.pl/rosja-2025-globalne-ambicje-ograniczone-zasoby-stan-rosyjskiej-ekonomii-i-polityki-raport/ (dostęp 8.01.2026); M. Sułek, E. Szymala, *Potęga Państw 2025* [raport], 28.12.2024, https://ine.org.pl/potega-panstw-2025-raport/ (dostęp 8.01.2026); R. Szczepaniak, *Soft power („miękka siła") w relacjach międzynarodowych. Dyplomacja kulturalna - redefinicja pojęcia*, „Horyzonty Polityki" 2011, nr 2; J. Trzcińska, *Miękka siła jako narzędzie polityki zagranicznej Chińskiej Republiki Ludowej i Republiki Korei*, „Gdańskie Studia Azji Wschodniej" 2016, nr 9; O. Wasiuta, *Miękka siła („soft power")*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo ARCANA, Kraków 2017.

MILITARYZACJA NARODU – samo pojęcie militaryzacji nastręcza nie lada problemów natury semantycznej, wynikających często z wielowektorowego ujęcia tego terminu. Postulaty militaryzujące, które w kontekście obrony narodowej państwa jawią się jako jednoznacznie pozytywne – uzupełniające i wspierające działalność regularnych sił wojskowych, nierzadko utożsamiane są z postulatami militarystycznymi, które kojarzyć

się mogą z negatywną działalnością państwa – militaryzmem ograniczającym swobody obywatelskie celem wzmocnienia kontroli wojskowej nad wszystkimi płaszczyznami życia publicznego. Według *Słownika politologii* terminem „militaryzm" (*militarism*) określa się „stan, w którym państwo przyznaje sprawom wojny i groźbie użycia siły najwyższy priorytet spośród swych politycznych celów. Ewentualnie [jest to – przyp. PŁ] sytuacja, gdy wartości wiązane z wojną (patriotyzm, jedność, hierarchia, dyscyplina) przenikają społeczeństwo obywatelskie. W praktyce oba zastosowania terminu nachodzą na siebie. Termin ma źródło w XIX-wiecznym niepokoju wywołanym zagrożeniem rządów cywilnych przez wojskowych i strachem przed ograniczeniem liberalnych wartości i swobód". Biorąc pod uwagę zaprezentowaną definicję, pojęcie militaryzacji winno wiązać się przede wszystkim ze wspomnianym aspektem podkreślania istoty i znaczenia wartości patriotyzmu, jedności, hierarchii i dyscypliny w (samo) organizującym się społeczeństwie obywatelskim, jednakże nie w obliczu trwającej wojny, ale zapobiegawczo – w warunkach pokoju. Zatem militaryzacja będąca postulatem polityki obronnej państwa jawi się tu jako działanie o charakterze prewencyjnym, nie zaś reakcyjnym. Choć, jak wcześniej zaznaczono, militaryzm nierzadko w powszechnym odbiorze kojarzy się z ograniczeniem pewnych swobód, to wziąwszy pod uwagę jego walor wychowawczy (w sensie moralnego i obywatelskiego wychowania żołnierza), będzie on nieodłącznym elementem cnoty obywatelskiej oraz polem do ukształtowania, szczególnie u ludzi młodych, postawy karności, dyscypliny i hierarchii, które, zdaniem Tomasza Szczepańskiego, czynią wychowanie militarne wspólnotowym, ściśle związanym z procesem militaryzacji narodu.

W internetowym wydaniu *Słownika języka polskiego* militaryzacja to „podporządkowanie życia gospodarczego, społecznego, politycznego celom wojskowym". O ile to podporządkowanie, które było wynikiem sytuacji w państwie wywołanej mobilizacją do zbliżającej się wojny lub nagłym jej wybuchem i zostało wprowadzone odgórnie, jest powszechnie uznawane za ograniczenie swobód jednostki w wymiarach wskazanych w przytoczonej definicji, o tyle podporządkowanie się celom wojskowym (mające charakter czynu zapobiegawczego w czasie pokoju i będące wyrazem oddolnej działalności społeczeństwa) można traktować jako pewien

przywilej, uprawnienie jednostek, oraz nazywać militaryzacją narodu, szczególnie kiedy mowa o edukacji dla bezpieczeństwa i obronności konkretnego narodu w konkretnym państwie. Militaryzację narodu w tym kontekście należy wiązać z szeroko pojętym wychowaniem narodowym, patriotycznym oraz przebiegającym równolegle samokształceniem na polu cywilnym i wojskowym, teoretycznym i praktycznym, amatorskim i profesjonalnym. Biorąc pod uwagę geopolityczną i geostrategiczną płaszczyznę zagrożeń militarnych i niemilitarnych pierwszych dekad XXI w., komplementarność w powyższym zakresie wydaje się szczególnie istotną kwestią dla bezpieczeństwa i suwerenności państwa.

Problematyka militaryzacji wiąże się także z przeniesieniem lub wprost przerzuceniem części odpowiedzialności za obronę państwa na podmioty zajmujące się zabezpieczeniem sprawnego funkcjonowania kraju, nie tylko pod względem przygotowania *stricte* wojskowego. Oczywiście w sytuacji odejścia od obowiązkowej służby wojskowej i tworzenia armii zawodowej konieczna wydaje się delegacja wspomnianej odpowiedzialności na inne podmioty, gdyż, jak pisze Radosław Sitek, głównym zadaniem armii zawodowej jest przede wszystkim neutralizowanie działań potencjalnego agresora, by stworzyć możliwość uruchomienia osobowych, rzeczowych i materiałowych rezerw na wypadek sytuacji kryzysowych, mobilizacji i wojny oraz umożliwić przestawienie gospodarki na produkcję w celach wojennych.

Obok regularnych sił zbrojnych jednostki przeznaczone do militaryzacji w świetle ustawy z 11 marca 2022 r. o obronie ojczyzny stanowią ważny element obrony narodowej państwa wspieranej w dyskursie publicznym (ale i specjalistycznym) postulatami rozwijania Wojsk Obrony Terytorialnej czy liberalizacji prawa do posiadania broni. Współcześnie rozwijane są koncepcje przygotowania obronnego obywateli oraz budowania odporności państwa na zagrożenia dla funkcjonowania systemu bezpieczeństwa narodowego o charakterze militarnymi i niemilitarnym. Mowa tu choćby o dążeniu do wprowadzania nowej koncepcji przygotowania obronnego, obejmującego nie tylko Siły Zbrojne Rzeczypospolitej Polskiej, ale – jak wskazuje Marta Adamczewska – również szeroko rozumiany komponent społeczny, co znajduje wyraz m.in. w regulacjach dotyczących tworzenia

aktywnej rezerwy, działalności organizacji proobronnych czy promowania idei powszechnej gotowości obronnej społeczeństwa.

Militaryzacja narodu, będąca przedmiotem niniejszej analizy, łączy nierozerwalnie pojęcie swoistego uposażenia, dozbrojenia, zaopatrzenia reprezentantów danego narodu w wiedzę i środki mające zapewnić zabezpieczenie żywotnych interesów narodowych państwa z koncepcją wychowania narodowego mającego zaktywizować społeczeństwo w obszarze obrony zwłaszcza przed militarnymi zagrożeniami dla niepodległości państwa, gdyż – jak wskazuje Jerzy Konieczny – w przypadku „bezpieczeństwa militarnego zagrożeniem jest groźba użycia siły w celu opanowania terytorium i ograniczenie suwerenności innych państw, w tym również wymuszenie pożądanych zachowań". Dlatego też ważne w koncepcji militaryzacji narodu jest: po pierwsze, wychowanie w duchu jedności narodowej i realizacji wspólnego celu, jakim jest obrona narodowego i państwowego interesu; po drugie, realna chęć realizacji obowiązku służby ojczyźnie wynikająca ze świadomości znaczenia stanu bezpieczeństwa oraz zagrożeń wewnętrznych i zewnętrznych; po trzecie, wyszkolenie i przysposobienie obronne prowadzone permanentnie w duchu edukacji dla bezpieczeństwa wynikającej z wewnętrznej potrzeby, a nie nakazu pochodzącego z zewnątrz; po czwarte, zaangażowanie, twórcza postawa i samodzielność jednostek będące podstawami narodowego aktywizmu.

Te wytyczne zbieżne są w zasadniczej ich części z postulatami wychowania moralnego oraz obywatelsko-wojskowego charakterystycznymi w czasie wojny dla takich struktur, jak choćby Grupa Szańca czy Narodowe Siły Zbrojne – narodowych formacji utworzonych do walki z okupantem w czasie wojny.

Koncepcja militaryzacji narodu idzie w parze z podkreślanym w wielu środowiskach narodowych w Polsce (w gruncie rzeczy elitarnym) postulatem aktywizmu narodowego, mającego przeciwdziałać bierności poprzez realne i wielopłaszczyznowe zaangażowanie obywateli w pracę na rzecz dobra narodowej wspólnoty oraz oddolną inicjatywność prowadzoną w kierunku realizacji interesu narodowego głównie w aspekcie praktycznym i utylitarystycznym. Ten swoisty elitaryzm aktywizmu na rzecz dobra ogółu trafnie oddał Marek Jan Chodakiewicz: „Polskość aktywna to świadome poczucie wspólnoty narodowej, wyrażające się

działalnością na rzecz ogółu […]. Polskość pasywną reprezentują masy narodowe, aktywną – elity narodowe […]. Przynależność do masy czy elity narodowej nie zależy bowiem od wykonywanego zawodu lub pochodzenia, ale od stopnia świadomości narodowej, stopnia identyfikacji z polskością, a więc stopnia aktywności w wypełnianiu obowiązków wynikających z przynależności do społeczeństwa polskiego. O aktywności bądź pasywności narodowej decyduje świadomy stosunek do obowiązku wypływającego z poczucia polskości". Podobnie militaryzacja narodu w przekonaniu środowisk pronarodowych winna być odzwierciedleniem pragnienia wypełnienia obowiązku wynikającego z przynależności do określonej wspólnoty, poczucia jedności i potrzeby zapewnienia państwu i jego obywatelom bezpieczeństwa.

Obrona państwa (w sensie militarnym i niemilitarnym) łączy się nieodzownie z polityką bezpieczeństwa, która względy interdyscyplinarne i hybrydyczne w kontekście współpracy reprezentantów nauk o bezpieczeństwie, nauk o polityce i administracji, ekonomii, pedagogiki, historii itd. traktuje priorytetowo. W przekonaniu autora podejście interdyscyplinarne i wieloaspektowe należy stosować również w przypadku analizy polityki obronnej państwa jako całości oraz poszczególnych jej elementów. Kwestia obronności zawiera w sobie wiele elementów, które mają charakter reagujący na wiele zagrożeń dla bezpieczeństwa związanych ze skokiem technologicznym i cywilizacyjnym, degradacją środowiska naturalnego, słabnącymi więziami międzyludzkimi, radykalizmem, terroryzmem itd. Dlatego też w ramach polityki bezpieczeństwa, będącej ważnym problemem badawczym, istotne jest to, aby elementem prowadzonych badań uczynić sprawę przeciwstawienia się społeczeństwa wyartykułowanym zagrożeniom, czyli również kwestię militaryzacji narodu jako kluczowego czynnika wspierającego obronę narodową. Narodowa polityka obronna państwa, która w założeniu ma odzwierciedlać uczestnictwo suwerennego narodu w działaniu na rzecz bezpieczeństwa wspólnoty, powinna wypełniać 2 podstawowe funkcje charakterystyczne dla działalności państwa, mianowicie: wewnętrzną (utrzymanie ładu i porządku społecznego, bezpieczeństwa wewnętrznego) i zewnętrzną (ochrona żywotnych interesów państwa, realizacja racji stanu, tworzenie bezpiecznej przestrzeni życiowej dla narodu, unikanie i rozwiązywanie konfliktów na szczeblu

międzynarodowym). Militaryzacja narodu, rozpatrywana również jako koncepcja polityczna wielu środowisk narodowych w Polsce na przestrzeni lat, bywa postulatem wynikającym z uznania, iż konstytutywnymi czynnikami obronności kraju są: obowiązek obrony państwa, który spoczywa na barkach każdego jego obywatela; fakt, iż obrona państwa spoczywa przede wszystkim na jego narodzie, a nie na innych państwach czy organizacjach międzynarodowych, które miałyby go w tym celu wyręczyć; uznanie za najwyższy przejaw racji stanu przetrwania i ciągłości istnienia państwa.

Paweł Łubiński

M. Adamczewska, *Świadomość obywatelska i przygotowanie społeczne jako element wzmacniania odporności państwa w warunkach zagrożenia bezpieczeństwa*, „Wiedza Obronna" 2025, t. 292, nr 3; M.J. Chodakiewicz, *O prawicy i lewicy*, Wydawnictwo Glaukopis, Warszawa–Gdańsk 2013; M.J. Chodakiewicz, J. Mysiakowska-Muszyńska, W.J. Muszyński, *Polska dla Polakow! Kim byli i są polscy narodowcy*, Wydawnictwo Zysk i S-ka, Poznań 2015; J. Konieczny, *Polityka bezpieczeństwa*, [w:] *Podstawowe kategorie polityki*, S. Opara, D. Radziszewska-Szczepaniak, A. Żukowski (red.), Instytut Nauk Politycznych UWM, Olsztyn 2005; P. Kornobis, *Militaryzm [militarism]*, [w:] *Słownik politologii*, B. Walicka (red.), Wydawnictwo Naukowe PWN, Warszawa 2008; A. Korybski, *Funkcje państwa*, [w:] *Wprowadzenie do nauki o państwie i polityce*, B. Szmulik, M. Żmigrodzki (red.), Uniwersytet Marii Curie-Skłodowskiej, Lublin 2007; *Militaryzacja*, http://sjp.pwn.pl/szukaj/militaryzacja.html (dostęp 8.01.2026); E. Ponczek, *Aksjologia polityczna Polskiego Ruchu Narodowego (1939–1945). Interes narodowy – geopolityka – wychowanie narodowe*, [w:] *Narodowa Demokracja XIX–XXI wiek: Dzieje ruchu politycznego. Księga pamiątkowa poświęcona pamięci profesora Romana Wapińskiego (1931–2008)*, t. 1: *Koncepcje – ludzie*, T. Sikorski, A. Wątor (red.), Wydawnictwo Adam Marszałek, Toruń 2012; R. Sitek, *Militaryzacja*, „Przegląd Logistyczny" 2011, nr 2; T. Szczepański, *Nacjonalizm, militaryzm, etatyzm. Podstawy wychowania narodowego*, „Polityka Narodowa" 2013, nr 13; W. Żebrowski, *Badanie polityki. Ogniwa procesu badawczego na studiach politologicznych*, Instytut Nauk Politycznych UWM, Olsztyn 2012.

MIMIKRA SPOŁECZNA PRZESTĘPCÓW (ang. *criminal social mimicry)* – zjawisko, w którym osoby o skłonnościach przestępczych celowo lub nieświadomie upodabniają się do otoczenia społecznego, maskując swoją

prawdziwą tożsamość, intencje i działania przestępcze, aby uniknąć ich wykrycia i dostosować się do określonej grupy społecznej.

Przestępca stosujący mimikrę stara się przystosować do środowiska, przyjmując jego:

- normy zachowań;
- sposoby komunikacji;
- wygląd zewnętrzny;
- wartości i rytuały społeczne.

W ten sposób staje się niedostrzegalny dla organów ścigania i otoczenia, co znacznie utrudnia jego zdemaskowanie lub wzbudzenie podejrzeń.

Mimikra jest formą adaptacyjnego przystosowania ochronnego polegającą na upodabnianiu się organizmu do innych jednostek lub elementów środowiska w celu wprowadzenia w błąd potencjalnego przeciwnika funkcjonującego w tym samym otoczeniu. Mechanizm ten nie zmierza do całkowitego zaniku różnicy, lecz wytworzenia pozornego podobieństwa, które jednocześnie maskuje i częściowo ujawnia odmienność, umożliwiając podmiotowi zajęcie pozycji trudnej do rozpoznania w polu percepcyjnym zagrożenia. Istotą mimikry jest naśladowanie rozumiane nie jako proste kopiowanie formy, lecz proces działania, w którym podobieństwo staje się narzędziem oszustwa i ochrony.

Mimikra społeczna jest sytuacyjnie modyfikowanym mechanizmem adaptacyjnym funkcjonowania podmiotów społecznych, m.in. jednostek, grup i wspólnot, polegającym na naśladowaniu i upodabnianiu się do obowiązujących wzorców zachowań, ról, norm i stylów komunikacji w celu minimalizacji zagrożenia lub zwiększenia szans osiągnięcia sukcesu w warunkach społecznej niepewności. Mechanizm ten łączy nieświadome formy naśladownictwa ze strategiczną zdolnością adaptacyjną podmiotu, przejawiającą się w świadomym zniekształcaniu własnych postaw, odwoływaniu się do ambiwalencji i podwójnej moralności oraz realizowaniu zamaskowanych ról społecznych zgodnych z oczekiwaniami otoczenia i zinstytucjonalizowanymi normami. Zdolność do mimikry społecznej nie ma charakteru biologicznie wrodzonego, lecz kształtuje się w procesie socjalizacji i rozwoju społecznego, stanowiąc wytwór historyczno-kulturowych i sytuacyjnych uwarunkowań działania podmiotu.

W kontekście kryminologicznym mimikra społeczna opisuje mechanizmy adaptacyjne jednostek działających w społeczeństwie w sposób przestępczy, które poprzez planowe, świadome upodabnianie się do norm i ról społecznych potrafią maskować swoją prawdziwą tożsamość i intencje, umożliwiając długotrwałe, zorganizowane i skuteczne funkcjonowanie w środowisku społecznym, minimalizując ryzyko identyfikacji.

W analizie mimikry społecznej istotne jest rozpoznanie różnych wymiarów funkcjonowania jednostki, które obejmują strategie adaptacyjne i mechanizmy przystosowawcze w relacjach społecznych, w tym formy:

- behawioralne;
- zawodowe;
- emocjonalne;
- tożsamościowe;
- środowiskowe.

Mimikra behawioralna jest adaptacyjnym mechanizmem społecznym polegającym na świadomym lub nieświadomym naśladowaniu stylu życia, manier, języka, gestów oraz innych zachowań społecznie akceptowanych, który umożliwia jednostce skuteczne funkcjonowanie w grupie, zwiększa akceptację społeczną oraz sprzyja synchronizacji interakcji międzyludzkich. W psychologii społecznej mechanizm ten bywa interpretowany jako forma efektu kameleona, czyli automatycznego lub celowego dopasowywania się do zachowań innych, co ułatwia budowanie relacji i redukuje napięcie w interakcjach. W kontekście kryminologicznym mimikra behawioralna pełni funkcję strategiczną, pozwalając jednostkom działającym przestępczo, np. przestępcom gospodarczym, przyjmować pozory zachowań zgodnych z normami społecznymi, takich jak postawa przedsiębiorcy, filantropa czy osoby o wysokim statusie społecznym, co umożliwia maskowanie rzeczywistych intencji, minimalizowanie ryzyka ujawnienia przestępczej działalności i długotrwałe funkcjonowanie w środowisku społecznym.

Mimikra zawodowa oznacza strategiczne wykorzystanie wykonywanego zawodu, pełnionej funkcji społecznej lub pozycji instytucjonalnej jako społecznie akceptowanej osłony dla działalności przestępczej, umożliwiającej ukrywanie rzeczywistych intencji oraz charakteru podejmowanych działań. Mechanizm ten polega na świadomym odtwarzaniu ról

zawodowych, norm etycznych i standardów kompetencyjnych właściwych danej profesji, co sprzyja budowaniu wiarygodności, zaufania i społecznej legitymizacji podmiotu. W ujęciu kryminologicznym mimikra zawodowa stanowi istotny element długotrwałych i planowych strategii przestępczych, pozwalając na funkcjonowanie w ramach legalnych struktur organizacyjnych, jak ma to miejsce np. w przypadku księgowych, doradców finansowych czy menedżerów wykorzystujących swoją pozycję do procederu prania pieniędzy.

Mimikra emocjonalna polega na symulowaniu, modulowaniu lub selektywnym odtwarzaniu ekspresji emocjonalnej oraz reakcji empatycznych w celu dostosowania się do oczekiwań interakcyjnych otoczenia i wywarcia pożądanego wpływu na innych uczestników relacji społecznej. Mechanizm ten obejmuje naśladowanie stanów afektywnych, tonu emocjonalnego wypowiedzi oraz zachowań interpretowanych jako empatyczne, co sprzyja budowaniu więzi, wzbudzaniu zaufania i obniżaniu czujności interpersonalnej. W perspektywie kryminologicznej mimikra emocjonalna stanowi istotną strategię manipulacyjną, wykorzystywaną przez sprawców do pozyskiwania współpracowników lub ofiar poprzez pozorne okazywanie empatii, troski lub zaangażowania emocjonalnego, co umożliwia długotrwałe utrzymanie relacji instrumentalnych oraz skuteczne maskowanie rzeczywistych intencji.

Mimikra tożsamościowa odnosi się do konstruowania i podtrzymywania nowej, społecznie akceptowanej lub pozornie nieskazitelnej tożsamości, która zastępuje lub maskuje tożsamość rzeczywistą jednostki w celu umożliwienia jej funkcjonowania w strukturach społecznych bez wzbudzania podejrzeń. Zjawisko to obejmuje zarówno tworzenie fałszywych biografii, dokumentów i ról społecznych, jak i prowadzenie podwójnego życia, w którym prezentowana tożsamość pozostaje spójna z obowiązującymi normami i oczekiwaniami społecznymi. W ujęciu kryminologicznym mimikra tożsamościowa stanowi zaawansowaną strategię adaptacyjną, wykorzystywaną przez sprawców do długotrwałego ukrywania przestępczej działalności, unikania odpowiedzialności oraz utrzymywania stabilnych relacji społecznych opartych na fałszywych podstawach, co znacząco utrudnia procesy identyfikacji i zdemaskowania.

Mimikra środowiskowa polega na świadomym dostosowaniu zachowań, symboliki, języka, norm interakcyjnych oraz stylu funkcjonowania do specyfiki określonego środowiska społecznego w celu uzyskania akceptacji, niewidoczności i możliwości swobodnego działania w jego obrębie. Praktyka ta obejmuje proces integracji z istniejącymi strukturami formalnymi i nieformalnymi, takimi jak grupy przestępcze, gangi, wspólnoty religijne czy organizacje społeczne, poprzez internalizację ich reguł, rytuałów i wzorców komunikacji. W perspektywie kryminologicznej mimikra środowiskowa stanowi istotną strategię kamuflażu umożliwiającą ukrywanie rzeczywistego charakteru działań, pozyskiwanie zasobów i informacji oraz długotrwałe funkcjonowanie w danym środowisku bez wzbudzania podejrzeń, co znacząco utrudnia rozpoznanie i neutralizację aktywności przestępczej.

Wyróżnienie poszczególnych form mimikry społecznej pozwala na dalsze rozważania dotyczące uwarunkowań indywidualnych sprzyjających jej stosowaniu. Mimikra społeczna przestępców opiera się na zdolności jednostki do świadomego dopasowywania własnego zachowania i autoprezentacji do oczekiwań otoczenia w celu ukrycia swoich prawdziwych zamiarów i uniknięcia wykrycia. Osoby stosujące tę strategię wykorzystują zarówno cechy osobowościowe, jak i umiejętności społeczne, które zwiększają skuteczność ich maskowania w kontaktach społecznych. W szczególności do najważniejszych predyspozycji sprzyjających stosowaniu strategii mimikry społecznej należą:

- psychopatia społeczna;
- cechy narcystyczne;
- inteligencja emocjonalna instrumentalna.

Jednostki o cechach psychopatii społecznej charakteryzują się zimną kalkulacją, powierzchownym urokiem i ograniczoną empatią emocjonalną. Potrafią manipulować innymi dla własnej korzyści, często bez odczuwania poczucia winy lub wyrzutów sumienia. Ich zdolność do maskowania emocji oraz kontrolowania impulsów umożliwia funkcjonowanie w społeczeństwie bez ujawniania skłonności przestępczych, co stanowi fundament strategii mimikry społecznej.

Osoby o cechach narcystycznych wykazują silne poczucie własnej wartości, potrzebę podziwu i tendencję do autoprezentacji w korzystnym

świetle. Narcystyczna pewność siebie oraz zdolność do kreowania atrakcyjnego wizerunku społecznego zwiększają skuteczność mimikry, pozwalając im zdobywać zaufanie i akceptację otoczenia. W połączeniu z manipulacyjnymi strategiami psychopatycznymi, cechy narcystyczne wspierają utrzymanie pozornej normalności w kontaktach społecznych.

Inteligencja emocjonalna instrumentalna odnosi się do umiejętności rozpoznawania i wykorzystywania emocji innych w sposób strategiczny. Jednostki z wysokim poziomem tej zdolności potrafią przewidywać reakcje otoczenia, kontrolować własne wyrażanie emocji i selektywnie dostosowywać zachowania w zależności od kontekstu. W praktyce pozwala to na subtelną manipulację społeczną i skuteczne ukrywanie prawdziwych intencji, co jest ważnym elementem mimikry społecznej.

Jednostki stosujące mimikrę społeczną charakteryzują się zazwyczaj wysokim poziomem samokontroli, charyzmą oraz zdolnościami organizacyjnymi, co w połączeniu z cechami psychopatii społecznej, narcystycznymi oraz instrumentalną inteligencją emocjonalną znacząco utrudnia ich wykrycie i zidentyfikowanie w ramach systemów nadzoru społecznego i kryminalnego.

W celu zobrazowania mechanizmów mimikry społecznej w praktyce warto odwołać się do historycznych i współczesnych przypadków osób, które dzięki wcześniej opisanym cechom osobowościowym i umiejętnościom społecznym potrafiły skutecznie maskować swoje przestępcze zamiary, co ilustruje, jak te predyspozycje umożliwiają utrzymanie pozornej normalności w kontaktach z otoczeniem i utrudniają rozpoznanie i ujawnienie jednostek stosujących mimikrę społeczną. Analizowane przykłady obejmują:

- mimikrę przestępczości agresywnej;
- mimikrę finansową;
- mimikrę instytucjonalną;
- mimikrę cyfrową.

Ted Bundy, seryjny morderca działający w Stanach Zjednoczonych w latach 70., stanowi klasyczny przykład jednostki wykorzystującej mimikrę społeczną. Potrafił wzbudzać zaufanie i sympatię, funkcjonując w społeczeństwie jako wolontariusz i student prawa, co tworzyło obraz wręcz wzorowego obywatela. Dzięki wysokiej kontroli impulsów, zdolności

do manipulacji oraz powierzchownemu urokowi skutecznie maskował swoje przestępcze zamiary, pozostając trudnym sprawcą do wykrycia. Bundy ilustruje, jak wcześniej opisane cechy osobowościowe i umiejętności społeczne pozwalają na skuteczne utrzymanie pozornej normalności w kontaktach z otoczeniem.

Bernard Madoff, twórca największej piramidy finansowej w historii Stanów Zjednoczonych, stanowi przykład przestępcy stosującego mimikrę społeczną w sferze ekonomicznej. Madoff cieszył się reputacją szanowanego inwestora, co pozwalało mu maskować prawdziwe intencje i budować zaufanie wśród klientów oraz współpracowników. Jego działania wymagały wysokiego poziomu planowania, cierpliwości oraz kontroli impulsów, a także zdolności do strategicznej manipulacji percepcją innych. Madoff doskonale ilustruje, jak opisane predyspozycje umożliwiają utrzymanie pozornej normalności i społecznej wiarygodności w kontekście przestępczości finansowej, czyniąc jego działania trudnymi do wykrycia przez otoczenie i instytucje nadzoru.

Członkowie zorganizowanych grup przestępczych często wykorzystują mechanizmy mimikry społecznej, wchodząc w struktury legalnych instytucji, aby zdobyć wpływy i ochronę dla swojej działalności. Przykłady obejmują infiltrację biznesu, polityki lokalnej oraz instytucji publicznych, gdzie przestępcy mogą wpływać na decyzje, unikać odpowiedzialności i zwiększać zasięg swoich operacji, zachowując jednocześnie pozorną legalność działań. Tego typu działania wymagają umiejętności strategicznej autoprezentacji, kontrolowania percepcji otoczenia i stopniowego budowania zaufania w legalnych strukturach, co pozwala na skuteczne maskowanie przestępczych zamiarów. Infiltracja mafii w instytucje legalne stanowi przykład mimikry społecznej, w której przestępcze cele realizowane są poprzez pozornie normalne, formalne interakcje społeczne, czyniąc wykrycie sprawców wyjątkowo trudnym.

Cyberprzestępcy coraz częściej stosują mimikrę społeczną, podszywając się pod specjalistów IT, administratorów systemów lub konsultantów technicznych, aby uzyskać dostęp do zasobów informatycznych organizacji. Wykorzystując wiedzę branżową, profesjonalny język oraz pozory kompetencji, budują zaufanie wśród pracowników i użytkowników systemów, co umożliwia im przeprowadzanie ataków bez konieczności

stosowania otwartej siły czy technicznych włamań. Tego rodzaju działania opierają się na manipulacji relacjami zawodowymi i strukturami autorytetu, gdzie przestępcze intencje są skutecznie maskowane przez pozorną legalność i umiejętności informatyczne. Przypadek cyberprzestępców ilustruje, że mimikra społeczna stanowi decydujący mechanizm także w środowisku cyfrowym, gdzie granica między legalną rolą zawodową a działalnością przestępczą bywa szczególnie trudna do rozpoznania.

Ustalenie predyspozycji sprzyjających mimikrze społecznej pozwala na określenie zakresu, w jakim zjawisko to funkcjonuje w różnych obszarach nauki i praktyki, m.in. w:

- profilowaniu kryminalnym;
- psychologii sądowej;
- analizie zachowań przestępczych;
- socjologii dewiacji;
- bezpieczeństwie wewnętrznym.

Jako konstrukt teoretyczny mimikra społeczna umożliwia identyfikację mechanizmów maskowania przestępczych zamiarów oraz strategii manipulacji w kontaktach społecznych. W praktyce rozpoznanie tego typu zachowań wymaga analizy długofalowych wzorców, a nie pojedynczych incydentów, gdyż jednostki stosujące mimikrę społeczną często funkcjonują przez lata jako pozornie wzorowi obywatele, skutecznie ukrywając swoją aktywność przestępczą. W konsekwencji pojęcie to pełni podwójną funkcję: dostarcza ram analitycznych dla badań nad dynamiką zachowań przestępczych oraz stanowi praktyczne narzędzie w projektowaniu strategii wykrywania, prewencji i interwencji w środowiskach społecznych jak i cyfrowych.

Dariusz Hybś

T. Dobrogoszcz, *Przeciw stereotypom: mimikra a hybrydyczność. Współczesna proza polska na tropie tożsamości polskich migrantów w Wielkiej Brytanii*, „Teksty Drugie. Literatura Migracyjna" 2016, nr 3; K. Drat-Ruszczak, *Osobowość narcystyczna: kiedy i jak motywuje rozbieżność Ja?*, [w:] *Osobowość a procesy psychiczne i zachowanie*, B. Wojciszke, M. Plopa (red.), Oficyna Wydawnicza Impuls, Kraków 2003; B. Hołyst, *Psychologia kryminalistyczna. Diagnoza i praktyka*, Wydawnictwo Difin SA, Warszawa 2018; W. Kulesza, *Efekt kameleona. Psychologia naśladownictwa*,

Wydawnictwo Naukowe Scholar, Warszawa 2017; A. Lobanova, *Mimikra społeczna w sferze nauki: treść i formy jej przejawiania się*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie" 2014, nr 68; J. Maciuszek, *Wpływ społeczny a procesy automatyczne i bezrefleksyjność*, [w:] *Wokół wpływu społecznego*, R. Polczyk, J. Maciuszek, D. Doliński (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012; P. Motylińska, *Inżynieria społeczna*, [w:] *Encyklopedia bezpieczeństwa*, t. 2: *D–K*, O. Wasiuta, S. Wasiuta (red.), Wydawnictwo Libron, Kraków 2021; K. Musiał, P. Manning, *Madoff's Ponzi investment fraud: a social capital analysis*, „Journal of Financial Crime" 2018, vol. 25(2); W. Musiał, *Mimikra jako przykład decepcji w przyrodzie a przejawy oszustwa w ekonomii – wybrane problemy*, „Zeszyty Naukowe SGGW, Polityki Europejskie, Finanse i Marketing" 2018, nr 20(69); P.K. Oleś, *Wprowadzenie do psychologii osobowości*, Wydawnictwo Naukowe Scholar, Warszawa 2009; E. Piórecka, *Przestępczość zorganizowana na terenie Włoch oraz jej wpływ na przestępczość zorganizowaną w niektórych państwach Europy*, „Świat Idei i Polityki" 2018, t. 17; A. Smelkowska-Zdziabek, *Narcystyczne zaburzenia osobowości*, [w:] *Psychologia zaburzeń osobowości. Wybrane zagadnienia*, L. Cierpiałkowska (red.), Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 2004; B. Wojciszke, *Psychologia społeczna*, Wydawnictwo Naukowe Scholar, Warszawa 2011; Ł. Wroński, *Seryjni i wielokrotni mordercy Profilowanie psychologiczne i psychogeograficzne*, Wydawnictwo Centrum Psychologii Kryminalnej, Warszawa 2016.

N

NARODOWA STRATEGIA WOJSKOWA WĘGIER Z 2021 R. (węg. Magyarország Nemzeti Katonai Stratégiája, MNKS) – dokument przyjęty uchwałą rządu Węgier nr 1393/2021 z dnia 24 czerwca 2021 r. stanowiący długoterminową wizję rozwoju obronności państwa węgierskiego. MNKS analizuje środowisko węgierskiego bezpieczeństwa, wskazuje kierunki modernizacji sił zbrojnych, przemysłu obronnego oraz systemów finansowania. Struktura strategii obejmuje wstęp, 7 rozdziałów oraz postanowienia końcowe. Ponadto dokument określa sposoby wdrażania, a także obowiązki Ministerstwa Obrony i Dowództwa Sił Zbrojnych w zakresie opracowywania szczegółowych regulacji, doktryn oraz planów wykonawczych. Uwzględniając wymieniony podział, przytoczyć można następujące zapisy Narodowej Strategii Wojskowej Węgier z 2021 r.:

1. Wprowadzenie zawiera najważniejsze potrzeby wdrożenia MNKS. Podkreślono, że obrona Węgier jest wspólnym zadaniem państwa i społeczeństwa, które wymaga silnych sił zbrojnych, sprawnej międzyinstytucjonalnej (w ramach NATO i UE) oraz międzynarodowej

współpracy, a także rozwoju krajowego przemysłu obronnego – przede wszystkim za pośrednictwem programu Zrínyi 2026. Wprowadzenie ujmuje bezpieczeństwo w sposób wielowymiarowy, wskazując na konieczność skoordynowanego, całościowego podejścia do budowy odporności oraz zdolności obronnych państwa.

2. *Środowisko operacyjne XXI w.* to tytuł rozdziału 2, gdzie wskazano na złożone, zmienne i trudne do przewidzenia, globalne środowisko bezpieczeństwa, w którym rośnie znaczenie rywalizacji mocarstw i technologii przełomowych, takich jak sztuczna inteligencja, drony, systemy autonomiczne, cyberprzestrzeń oraz technologie kosmiczne. W rozdziale tym zaznaczono, że konflikty mają charakter wielodomenowy, łącząc działania lądowe, powietrzne, cybernetyczne, informacyjne i kosmiczne, gdzie granica między pokojem a wojną zanika na skutek działań hybrydowych i operacji poniżej progu konwencjonalnego ataku. Nadmieniono także, iż presja migracyjna i niestabilność na peryferiach Europy dodatkowo wpływają na bezpieczeństwo regionu, co wymaga adaptacji oraz gotowości do reagowania przez państwa takie jak Węgry.
3. W kolejnej części omówiono zagrożenia i wyzwania wymagające udziału sił zbrojnych, wskazując na szerokie spektrum zagrożeń – od potencjalnego ataku konwencjonalnego państwa, przez działania hybrydowo-cybernetyczne, po terroryzm oraz nielegalną migrację. Dokument zwraca uwagę również na rosnącą rolę cyberoperacji, które mogą dezorganizować funkcjonowanie państwa na równi z atakami kinetycznymi. W rozdziale 3 znajdują się także odwołania do zagrożeń związanych z pandemią i jej wtórnymi skutkami, a także katastrofami naturalnymi oraz przemysłowymi. Zgodnie z wnioskami podsumowującymi tę część w większości scenariuszy reagowanie wymaga aktywnego udziału węgierskich sił zbrojnych – samodzielnie lub w ramach międzyinstytucjonalnych struktur, takich jak NATO czy UE.
4. Najobszerniejszy rozdział strategii zatytułowany *Obrona przyszłości* przedstawia kierunkową wizję rozwoju węgierskiego systemu obronnego obejmującego zdolności odstraszania, sprawności reagowania oraz przygotowania państwa na wszelkie zagrożenia.

Został on podzielony na 5 podrozdziałów. Zgodnie z pierwszym, węgierska armia powinna być zdolna do szybkiej interwencji, udziału w operacjach kryzysowych, a także utrzymania gotowości udzielenia wsparcia sojuszniczego. Następny podrozdział omawia potencjał zdolności współpracy narodowej, który w sytuacjach nadzwyczajnych byłby efektywny dzięki budowie systemu łączącego cywilne i wojskowe zasoby. Byłoby to możliwe m.in. dzięki podnoszeniu świadomości obronnej obywateli, przygotowaniu społeczeństwa na zagrożenia, rozwojowi współpracy naukowej umożliwiającej wdrażanie innowacyjnych rozwiązań w sektorze wojskowym. Kolejny podrozdział przedstawia współpracę cywilno-wojskową jako kluczowy element bezpieczeństwa, wskazując na konieczność rozwijania krajowej gospodarki i przemysłu obronnego, a także roli państwa w budowie odporności narodowej, która umożliwia przetrwanie oraz szybkie odtworzenie funkcjonowania państwa. Przedostatni podrozdział ilustruje możliwość rozwoju interoperacyjności międzynarodowej na 3 poziomach: wzajemne planowanie, wspólne szkolenia oraz udział w siłach gotowości i wielonarodowych formacjach. W ostatniej części rozdziału 4 można znaleźć rekomendacje dotyczące polityki kadrowej w węgierskiej armii, która powinna koncentrować się na rozwoju zawodowym, zdrowiu psychicznym, wsparciu rodzin, edukacji patriotycznej oraz wzmocnieniu prestiżu służby wojskowej. Powstałe wnioski wskazują, że węgierska obrona narodowa wymaga współdziałania administracyjnego, gospodarczego, społecznego oraz sił zbrojnych. Z kolei według autorów strategii coraz większą rolę w systemie obronnym będzie odgrywała ochrona infrastruktury krytycznej, cyberbezpieczeństwo, stabilność energetyczną oraz przygotowanie społeczne.

5. Wizja odnowienia węgierskich sił zbrojnych została przedstawiona w rozdziale 5, co w ocenie autorów dokumentu byłoby najbardziej efektywne m.in. dzięki przeprowadzeniu modernizacji oraz unowocześnieniu systemów dowodzenia, łączności, a także za pośrednictwem wdrożenia programów rozwojowych brygad lądowych, lotniczych oraz zwiększenia zdolności rozpoznania.

Zwrócono również uwagę na element technologiczny związany z dynamicznym rozwojem systemów autonomicznych, bezzałogowych, a także ewolucję sposobu prowadzonych operacji cybernetycznych i dezinformacyjnych. Zalecono, aby węgierskie siły zbrojne w procesie odnowienia dążyły do poziomu osiągnięcia zdolności do prowadzenia działań o wysokiej intensywności, które byłyby wspierane przez odpowiednią logistykę, medycynę wojskową oraz rozbudowaną strukturę rezerw.

6. Zgodnie z rozdziałem 6 odbudowa i rozwój krajowego przemysłu obronnego stanowią fundament suwerenności technologicznej oraz wsparcia armii. Zwiększenie produkcji sprzętu wojskowego w kraju może przyczynić się do wzmocnienia militarnego zaplecza badawczo-rozwojowego, a także innowacyjności gospodarki. W ocenie autorów strategii współpraca z partnerami europejskimi i transatlantyckimi w sektorze przemysłu obronnego może w przyszłości stać się jednym z filarów gospodarczych oraz narzędziem wzmacniania regionalnej pozycji kraju.
7. Modernizacja krajowego przemysłu zbrojeniowego ma stanowić 20% węgierskiego budżetu obronnego, który zgodnie z długofalowym finansowaniem obronności będzie utrzymany na poziomie co najmniej 2% PKB. Wśród najważniejszych zakupów, które obejmą finansowanie, wymienia się nowoczesny sprzęt, rozwój infrastruktury wojskowej, systemy szkoleniowe oraz badania. Jak zaznaczono w rozdziale 7, wydatki są postrzegane jako inwestycja w bezpieczeństwo oraz niezależność państwową. Podkreślono także, iż budżet obronny w sytuacji strategicznej może zostać w przyszłości zwiększony.
8. Ostatni rozdział przedstawia postanowienia końcowe, zgodnie z którymi zaleca się, aby Ministerstwo Obrony Węgier opracowało szczegółowe regulacje, doktryny oraz plany dla Dowództwa Węgierskich Sił Zbrojnych. Strategia co prawda ma charakter długoterminowy, lecz jej uaktualnianie powinno następować w przypadku istotnych zmian w środowisku bezpieczeństwa lub systemie zarządzania obroną nie rzadziej niż raz na 4 lata. Dokument ponadto stanowi ramę strategiczną, której istotnym zadaniem jest

kierowanie rozwojem sił zbrojnych, planowaniem obronnym oraz integracją wojskowych i cywilnych elementów bezpieczeństwa narodowego. Będzie to możliwe poprzez ciągłe zapewnianie elastyczności, a także zdolności adaptacji w warunkach dynamicznie zmieniających się zagrożeń XXI w.

Narodowa Strategia Wojskowa Węgier z 2021 r. podkreśla kluczową rolę czasu i przestrzeni w planowaniu obronnym, reagowaniu kryzysowym i prowadzeniu operacji. W centrum uwagi znajduje się środowisko operacyjne XXI w. z dominującą rolą wojny hybrydowej. To z kolei, w ocenie autorów, wymaga stałej obecności, mobilności oraz zdolności państwowej do szybkiego rozpoznania i reagowania. Dlatego też w dokumencie wskazano istotny czynnik, jakim w kolejnych latach powinno być skuteczne modernizowanie sił zbrojnych (m.in. w ramach przytoczonego wcześniej programu Zrínyi 2026), które przyczyni się do zwiększenia potencjału odstraszania państwa. Posiadanie zmodernizowanej armii, rozwiniętej infrastruktury oraz zdolności bojowej umożliwi planowanie budżetowe na poziomie 2% PKB. Jak podkreślają autorzy strategii, rozwój ten powinien obejmować również węgierski wywiad i kontrwywiad wojskowy, odpowiedzialne za pozyskiwanie i analizę informacji, które przyczyniają się do zwiększenia skuteczności decyzyjnej organów państwowych. To w wielu przypadkach może pomóc w zdobyciu przestrzeni czasowej w sytuacji zagrożenia zewnętrznego. Co prawda, w treści MNKS zaznaczono, iż Węgry nie wskazują żadnego państwa jako wroga, niemniej w obliczu dynamicznych oraz trudnych do przewidzenia rodzajów oraz skali zagrożeń za rzecz istotną uznano potrzebę regularnego wzmacniania własnego potencjału obronnego. Uwzględniono również czynnik współpracy międzynarodowej, który powinien objawiać się poprzez regularne wspieranie działań wewnątrz sektora bezpieczeństwa w wymiarze regionalnym, europejskim oraz transatlantyckim. Wymieniono ponadto, iż fundamentem węgierskiego bezpieczeństwa pozostaje NATO, a także system kolektywnej obrony uzupełniony współpracą w ramach UE, ONZ i OBWE. Wśród rodzajów zagrożeń, na jakie MNKS zwraca szczególną uwagę, wymienić można technologię informacyjną, tj. AI, robotyka, cyberprzestrzeń, energia, druk 3D czy technologie kosmiczne, których wykorzystanie może mieć istotne znaczenie w potencjalnym konflikcie zbrojnym. Z tego względu autorzy

strategii rekomendują wzmożenie inwestycji w węgierską cyberobronę, szybkie rozpoczęcie wdrażania innowacyjnych procesów adaptacyjnych w węgierskim przemyśle obronnym, a także zastosowanie efektywnych rozwiązań w sektorze cywilnym.

Artur Jach-Chrząszcz, Karol Kochnowski

1393/2021 (VI. 24) *Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról*, https://njt.hu/jogszabaly/2021-1393-30-22 (dostęp 25.11.2025); P. Bak, G. Németh, D. Szőke, *Foundations of Hungarian defence policy*, „Honvédségi Szemle" 2020, no. 148(2), 10.35926/hdr.2020.2.1; B. Faragó, *Hungary's evolving defence policy: from security consumer to strategic autonomy within NATO*, „Strategies XXI: The Complex and Dynamic Nature of the Security Environment" 2025, 10.53477/3045-2309-25-03; A. Hugyik, *Best practices in the application of the concept of resilience: building hybrid warfare and cybersecurity capabilities in the Hungarian Defense Forces, Connections*, „The Quarterly Journal" 2020, no. 19(4), 10.11610/connections.19.4.02; I. Resperger, *Az új nemzeti katonai stratégiáról*, „Hadtudomány" 2021, no. 31(E-szám), 10.17047/hadtud.2021.31.e.203; I. Todorov, *Hungarian and Slovak national security vision in the context of the Russian-Ukrainian war*, „Wschód Europy. Studia Humanistyczno-Społeczne" 2024, no. 10(1), 10.17951/we.2024.10.1.165-175; P. Zentay, E. Hegedűs, *A 3D-s nyomtatás és katonai alkalmazásának lehetőségei. 2. rész*, „Haditechnika" 2023, no. 57(1), 10.23713/ht.57.1.

NARODOWE CENTRUM BEZPIECZEŃSTWA CYBERPRZESTRZENI (NCBC) – państwowa jednostka budżetowa podległa ministrowi obrony narodowej funkcjonująca pod tą nazwą od marca 2019 r. na mocy Zarządzenia nr 6/MON z dnia 5 marca 2019 r. w sprawie zmiany nazwy państwowej jednostki budżetowej – Narodowe Centrum Kryptologii na Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni oraz nadania statutu Narodowemu Centrum Bezpieczeństwa Cyberprzestrzeni, odpowiedzialna za konsolidację kompetencji i zasobów Ministerstwa Obrony Narodowej w zakresie kryptologii, cyberbezpieczeństwa i systemów teleinformatycznych. Wcześniej jednostka funkcjonowała jako Narodowe Centrum Kryptologii (NCK). Centrum było odpowiedzialne za kluczowe obszary związane z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów IT.

Narodowe Centrum Kryptologii zostało utworzone w 2013 r. na mocy Zarządzenia Nr 10/MON Ministra Obrony Narodowej z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii. Narodowe Centrum Kryptologii realizowało zadania w ramach działalności naukowo-edukacyjnej, badawczo-rozwojowej, wdrożeniowej i opiniodawczej. Na czele Centrum stał Dyrektor. W 2014 r. zapowiadano, że w ramach reformy systemu kierowania i dowodzenia SZ RP planuje się utworzenie Centrum Operacji Cybernetycznych w ramach NCK.

Podstawy prawne funkcjonowania Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni stanowiły:

- Zarządzenie Nr 6/MON z dnia 5 marca 2019 r. w sprawie zmiany nazwy państwowej jednostki budżetowej – Narodowe Centrum Kryptologii na Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni oraz nadania statutu Narodowemu Centrum Bezpieczeństwa Cyberprzestrzeni;
- Decyzja Nr 57/MON z dnia 23 kwietnia 2020 r. zmieniająca decyzję w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych wraz z ich podporządkowaniem.

Narodowe Centrum Bezpieczeństwa w Cyberprzestrzeni pełniło także funkcję CISIRT MON (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego), monitorując sieci RON 24/7. Jako jednostka ekspercka Ministerstwa Obrony Narodowej zapewniać miała bezpieczeństwo teleinformatyczne całego resortu.

Statut Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni nadawał jednostce konkretne zadania, takie jak konsolidacja kompetencji i zasobów resortu obrony narodowej w obszarze kryptologii, w szczególności:

1. Realizacja zadań związanych z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych.
2. Wytwarzanie nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych.
3. Osiągnięcie oraz utrzymanie potencjału i kompetencji w zakresie:

- budowy urządzeń i narzędzi kryptograficznych służących do przetwarzania informacji niejawnych oraz innych posiadających zdolności kryptograficzne;
- wytworzenia rozwiązań do pełnej ochrony i zabezpieczenia informacji i przekazu wraz z możliwością przygotowania zasad wdrożenia i produkcji;
- wypracowania metodologii i rozwiązań naukowo-technicznych w obszarze badania odporności rozwiązań kryptograficznych na kompromitację;
- zapewnienia warunków do prowadzenia badań, także we współpracy z jednostkami organizacyjnymi posiadającymi uprawnienia do nadawania stopnia naukowego doktora w dziedzinach nauki związanych w sposób bezpośredni lub pośredni z kryptologią;
- organizacji biblioteki i zbioru opracowań, w tym zawierających informacje niejawne, dotyczących zaawansowanej kryptologii.

4. Realizacja zadań w zakresie kryptologii zleconych, za pośrednictwem ministra obrony narodowej, przez inne organy państwa lub administracji publicznej.
5. Realizacja innych zadań zleconych przez ministra obrony narodowej.
6. Realizacja zadań związanych z pełnieniem funkcji gestora sprzętu wojskowego stanowiącego urządzenia i narzędzia kryptograficzne.
7. Przygotowywanie i przeprowadzanie postepowań o zamówienie publiczne w projektach naukowo-badawczych w obszarze związanym z kryptologią i cyberobroną, we współpracy z jednostkami inicjującymi oraz zawierania umów w tym zakresie.

Statut głosił, że centrum realizuje zadania w ramach działalności:

- naukowo-edukacyjnej przez konsolidację środowisk naukowych reprezentujących dziedziny nauki związane w sposób bezpośredni lub pośredni z kryptologią, opracowanie oraz aktualizację, zgodnie z najnowszym stanem wiedzy, efektów kształcenia w zakresie podstaw kryptologii i upowszechnianie ich w środowisku akademickim, a także promowanie ich wdrożenia

w polskich uczelniach, prowadzenie działalności naukowej w zakresie wymagającym dostępu do informacji niejawnych;
- badawczo-rozwojowej przez koordynację prac badawczych w resorcie obrony narodowej i prowadzenie we współpracy z podmiotami naukowymi i przemysłowymi innowacyjnych badań naukowych i prac rozwojowych, budowanie demonstratorów technologii, prototypów i rozwiązań pilotażowych, w zakresie technologii kryptologicznych oraz zapewnianie laboratoriów na potrzeby specjalistycznych badań i analiz związanych z kryptologią, w szczególności na potrzeby ministra obrony narodowej i polskich służb specjalnych;
- wdrożeniowej w zakresie technologii kryptologicznych urządzeń i technologii, będących m.in. produktami centrum lub badanymi przez centrum, w urządzeniach produkowanych przez polski przemysł oraz stworzenie potencjału umożliwiającego wsparcie pracami laboratoryjnymi i analitycznymi procesu akredytacji i certyfikacji rozwiązań kryptograficznych;
- opiniodawczej w zakresie realizacji zadań związanych z wymogami opracowywania i opiniowania dokumentów dotyczących pozyskiwania, funkcjonowania, zakupu, wytwarzania, użytkowania systemów, technologii i dokumentów oraz urządzeń kryptograficznych w Siłach Zbrojnych Rzeczypospolitej Polskiej.

Działalnością NCBC kierował dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, reprezentując także jednostkę na zewnątrz. Od 2019 r. na czele Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni stał gen. bryg. Karol Molenda, będąc także pełnomocnikiem MON ds. utworzenia wojsk obrony cyberprzestrzeni. Statut określał powołanie dyrektora Centrum oraz jego zastępców na 3-letnią kadencję przez ministra obrony narodowej. Dyrektor NCBC miał wykonywać zadania statutowe przy pomocy zastępców dyrektora, głównego księgowego, szefów komórek wewnętrznych.

W lutym 2019 r. Mariusz Błaszczak, ówczesny minister obrony narodowej, zatwierdzając Koncepcję organizacji i funkcjonowania Wojsk Obrony Cyberprzestrzeni, rozpoczął proces tworzenia nowego komponentu

sił zbrojnych. W strukturach Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni formalnie utworzono Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni.

Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni otrzymało imię Jerzego Witolda Różyckiego Decyzją nr 11/MON Ministra Obrony Narodowej Mariusza Błaszczaka z dnia 4 lutego 2020 r.

Decyzja Nr 4/MON Ministra Obrony Narodowej z dnia 14 stycznia 2022 r. wprowadzała zmianę i na jej mocy przemianowano Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni w Legionowie na Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni w Legionowie, a następnie na mocy Decyzji MON Nr 117/MON Ministra Obrony Narodowej z dnia 22 sierpnia 2022 r. – na Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni w Legionowie. Decyzją Nr 15/MON z 15 lutego 2022 r. w sprawie organizatora wojskowego systemu telekomunikacyjnego Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni zostało wyznaczone jako organizator wojskowego systemu telekomunikacyjnego.

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni funkcjonuje na mocy ustawy z dnia 11 marca 2022 r. o obronie ojczyzny, która weszła w życie 23 kwietnia 2022 r. Na bazie Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni i jednostek bezpośrednio podporządkowanych powstało Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC), którym kieruje gen. bryg. Karol Molenda.

Decyzją Nr 66/MON Ministra Obrony Narodowej z dnia 19 czerwca 2024 r. w sprawie przejęcia dziedzictwa tradycji oraz nadania imienia patrona Dowództwu Komponentu Wojsk Obrony Cyberprzestrzeni Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni przejęło dziedzictwo tradycji Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni.

Agnieszka Warchoł

Decyzja Nr 117/MON Ministra Obrony Narodowej z dnia 22 sierpnia 2022 r. zmieniająca decyzję w sprawie podporządkowania jednostek organizacyjnych osobom zajmującym kierownicze stanowiska Ministerstwa Obrony Narodowej albo kierownikom komórek organizacyjnych; Decyzja Nr 15/MON Ministra Obrony

Narodowej z dnia 15 lutego 2022 r. w sprawie organizatora wojskowego systemu telekomunikacyjnego; Decyzja Nr 168/MON Ministra Obrony Narodowej z dnia 26 listopada 2021 r. w sprawie podporządkowania jednostek organizacyjnych osobom zajmującym kierownicze stanowiska Ministerstwa Obrony Narodowej albo kierownikom komórek organizacyjnych; Decyzja Nr 4/MON Ministra Obrony Narodowej z dnia 14 stycznia 2022 r. zmieniająca decyzję w sprawie podporządkowania jednostek organizacyjnych osobom zajmującym kierownicze stanowiska Ministerstwa Obrony Narodowej albo kierownikom komórek organizacyjnych; Decyzja Nr 57/MON z dnia 23 kwietnia 2020 r. zmieniająca decyzję w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych wraz z ich podporządkowaniem; Decyzja Nr 66/MON Ministra Obrony Narodowej z dnia 19 czerwca 2024 r. w sprawie przejęcia dziedzictwa tradycji oraz nadania imienia patrona Dowództwu Komponentu Wojsk Obrony Cyberprzestrzeni; A. Warchoł, *Wojska Obrony Cyberprzestrzeni*, [w:] *Encyklopedia bezpieczeństwa*, t. 6, O. Wasiuta, S. Wasiuta (red.), Wydawnictwo Libron, Kraków 2023; *Wojska Obrony Cyberprzestrzeni rozpoczynają działalność*, https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni-rozpoczynaja-dzialalnosc (dostep 11.12.2025); Zarządzenie Nr 10/MON Ministra Obrony Narodowej z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii; Zarządzenie Nr 6/MON Ministra Obrony Narodowej z dnia 5 marca 2019 r. w sprawie zmiany nazwy państwowej jednostki budżetowej – Narodowe Centrum Kryptologii na Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni oraz nadania statutu Narodowemu Centrum Bezpieczeństwa Cyberprzestrzeni; Zarządzenie nr 6/MON z dnia 5 marca 2019 r. w sprawie zmiany nazwy państwowej jednostki budżetowej – Narodowe Centrum Kryptologii na Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni oraz nadania statutu Narodowemu Centrum Bezpieczeństwa Cyberprzestrzeni.

NISZCZYCIEL był pierwotnie małym i szybkim okrętem wojennym przeznaczonym do obrony przed torpedowcami, dlatego ten typ okrętu nazywano początkowo niszczycielem torpedowców. Wraz z końcem ery pancerników niszczyciele stały się jednymi z większych (obok krążowników) jednostek. Co więcej, niszczyciel jest najmniejszym typem okrętu wojennego zdolnym do pełnienia roli uniwersalnej, dzięki czemu może samodzielnie wykonywać misje operacyjne w wojnie morskiej, bez dodatkowego wsparcia.

Pojawienie się torpedy jako nowego elementu morskiego uzbrojenia pod koniec ósmej dekady XIX stulecia szybko doprowadziło do powstania nowego typu okrętu – torpedowca. W założeniu doktrynalnym francuskiej młodej szkoły (fr. *jeune école*) lansowanej przez admirała Théophile Aube, eskadry torpedowców miały zrównoważyć przewagę Royal Navy nad flotą francuską, zwłaszcza na wodach kanału La Manche. Termin „niszczyciel" jest – jak już wspomniano – dosłownym tłumaczeniem angielskiego słowa *destroyer*, ponieważ ta klasa okrętu została zaprojektowana w Wielkiej Brytanii w odpowiedzi na rozwój torped i kutrów torpedowych. Ówczesna wiodąca brytyjska marynarka wojenna opierała się na dużych pancernikach, które ze swymi wielkokalibrowymi bateriami dział były słabo przygotowane do obrony przed szybko zbliżającymi się torpedowcami. Aby je chronić, budowano nieco większe i szybsze okręty, zaprojektowane do skutecznego zwalczania atakujących torpedowców za pomocą ich szybkostrzelnych dział. Ten typ nazywano myśliwym torpedowców lub niszczycielem kutrów torpedowych (we Francji Contretorpilleur, we Włoszech Cacciatorpediniere). Nieporęczny termin „niszczyciel torpedowców" wkrótce skrócono do terminu „niszczyciel". Posiadały one również uzbrojenie torpedowe do kontrataków, dlatego też rozróżnienie między torpedowcem a niszczycielem jest płynne, zwłaszcza w przypadku wczesnych okrętów tego typu. Pierwszymi klasami okrętów noszącymi formalną nazwę niszczyciela torpedowców (*torpedo boat destroyer*) były 2 klasy okrętów: Daring i Havock, zbudowane dla Royal Navy. Okręty te wypierały ok 300 t, mając za uzbrojenie główne działo kalibru 76 mm i 2 wyrzutnie torpedowe. Wynalezienie napędu turbinowego pozwoliło na zwiększenie prędkość nowych niszczycieli do 34–35 w., ale też wzrosła ich wyporność, osiągając u progu I wojny światowej 1000 t. Przykładowo typ K budowany w latach 1912–1913 miał wyporność 996 t, a uzbrojony był w 3 działa kalibru 102 mm i 2 wyrzutnie torpedowe kalibru 533 mm. Niemieckie okręty o zbliżonej charakterystyce nadal nazywano torpedowcami (niem. Torpedoboote). Typ V 25, oddany do służby tuż przed wybuchem pierwszego światowego konfliktu, wypierał 812 t. Jego uzbrojenie podstawowe składało się z 3 dział kalibru 88 mm i 6 wyrzutni torped kalibru 500 mm. Skonstruowane pod koniec wojny duże jednostki typu S 113 wypierające ponad 2000 t i uzbrojone w 4 działa kalibru 150 mm

Niemcy nadal konsekwentnie nazywali torpedowcami, dodając jedynie predykat „wielkie" (niem. Grosse Torpedoboote).

Podczas I wojny światowej niszczyciele były wykorzystywane do wielu zadań, od tych, dla których zostały stworzone – eskorta dużych okrętów, po działania rozpoznawcze i konwojowanie statków handlowych. Dowiodły też, że są okrętami bardziej uniwersalnymi, niż początkowo przypuszczano. Ich uzbrojenie wzbogacono w świetle doświadczeń wojennych o broń przeciw okrętom podwodnym oraz artylerię przeciwlotniczą. Okazało się również, że nadają się doskonale do stawiania zagród minowych. Pod koniec I wojny światowej niszczyciele mogły zabierać na swe pokłady do 50–60 min morskich.

Po I wojnie światowej zarówno wyporność, jak i uzbrojenie niszczycieli zaczęły znacząco wzrastać. Wzorcem takich zmian był japoński niszczyciel typu Fubuki, wypierający ponad 2000 t, uzbrojony w 6 dział kalibru 127 mm w zamkniętych wieżach (absolutne *novum* na niszczycielach) przy prędkości 38 w., 9 wyrzutni torpedowych kalibru 610 mm. Okręt ten zdecydowanie górował w momencie wcielenia go do służby (1928) nad każdym niszczycielem innych mocarstw morskich. Konstrukcja ta zmusiła inne państwa do budowy okrętów o podobnej charakterystyce. Do momentu wybuchu II wojny światowej powstały superniszczyciele brytyjskie typu Tribal, amerykańskie Porter czy francuskie Mogador. W niemieckiej Kriegsmarine duże okręty tej klasy (typ 1934 A) wreszcie zaczęto określać mianem niszczycieli (niem. *Zerstörer*). Niemcy wybudowali zresztą (stępki położono już w 1938 r.) prawdziwe superniszczyciele (typ 1936 A określany później jako Narvik). Ich pełna wyporność bojowa sięgała 3500 t, a uzbrojenie główne złożone było z 5 dział kalibru 150 mm. Pomimo znaczącego potencjału bojowego okręty nie były pozbawione wad: pojawiły się problemy z niezawodnością wysokociśnieniowych kotłów parowych i dzielnością morską na wzburzonym morzu ze względu na nowo zaprojektowaną konstrukcję dziobu i ciężką artylerię dziobową. Duże niszczyciele zamówiono w Wielkiej Brytanii także dla polskiej marynarki wojennej. Chodzi o 2 okręty typu Grom (Grom i Błyskawica) o wyporności przekraczającej 2 tys. t, uzbrojonych w 7 dział kalibru 120 mm. Budowę 2 kolejnych tego typu (domniemane nazwy Huragan i Orkan) przerwała agresja Niemiec w 1939 r. W ZSRR wybudowano kilkadziesiąt niezbyt

udanych jednostek typu 7 i 7U, natomiast tuż przed wybuchem wojny ZSRR zamówił we Włoszech zupełnie nowy typ niszczyciela (Taszkient) o wyporności przekraczającej 3 tys. t, silnym uzbrojeniu (6 dział kalibru 130 mm) i fenomenalnej prędkości sięgającej 42 w. Kolejne jednostki tego typu z racji wybuchu wojny nie zostały zbudowane.

Niszczyciele budowane przed II wojną światową powstawały z myślą o walce z podobnymi jednostkami nawodnymi przeciwnika, stąd też kładziono nacisk na uzbrojenie ofensywne – artyleria główna oraz broń torpedowa. W mniejszym stopniu zwracano uwagę na uzbrojenie przeciw okrętom podwodnym oraz przeciwlotnicze. Działania na morzu od pierwszych dni II wojny światowej boleśnie te przewidywania zweryfikowały. Okazało się, że najważniejsze zadanie stawiane przed niszczycielami to eskorta zarówno konwojów statków handlowych, jak i zespołów uderzeniowych floty. Taki stan rzeczy prowadził do częstego przezbrajania jednostek tej klasy, przy czym zazwyczaj dokonywało się ono na rzecz wzmocnienia potencjału obronnego niszczycieli. Przykładem może być zmiana artylerii głównej na ORP Błyskawica z 7 dział kalibru 120 mm na 8 kalibru 102 mm, mających uniwersalne zastosowanie (dotychczasowa artyleria główna niszczyciela nie nadawała się do walki z samolotami). Wszystkie nowe niszczyciele budowane w USA czy Wielkiej Brytanii podczas wojny wyposażano w uniwersalną artylerie główną. Podobnie w Japonii (np. niszczyciel typu Akizuki) – nowo budowane niszczyciele konstruowano z myślą o walce z okrętami podwodnymi i lotnictwem. Tylko Kriegsmarine, dla której budowano niszczyciele typu Narvik, nie uległa do końca temu trendowi; rosła też wyporność jednostki tej klasy. Przykładowo brytyjskie okręty typu Battle budowane w długiej serii od 1942 r. miały wyporność pełną bojową przekraczającą 3 tys. t. Doświadczenia wojenne wykorzystywano także w krajach neutralnych, np. w Szwecji jeszcze podczas wojny (1943) rozpoczęto budowę niszczycieli typu Öland – choć relatywnie nieduże (2250 t), przenosiły silne uzbrojenie, co więcej skonstruowano je tak, by można było dokonywać na nich modernizacji. Ich służba trwała ponad 40 lat, do 1979 r. Zapotrzebowanie na dużą liczbę jednostek eskortowych sprawiło, że podczas wojny (głownie w USA i Wielkiej Brytanii) pojawiły się tzw. niszczyciele eskortowe, np. amerykański typ Evarts czy brytyjski Hunt III. Były one mniejsze od niszczycieli floty

(około 1000 t wyporności), a ich uzbrojenie miało zasadniczo przeciwlotniczy i przeciwpodwodny charakter.

Bezpośrednio po II wojnie światowej mocarstwa zachodnie korzystały z licznych budowanych w latach 1939–1945 niszczycieli, np. brytyjski typ Battle czy amerykański Fletcher. Ten drugi liczył aż 175 jednostek i od lat 50. minionego stulecia zasilał marynarki wojenne państw NATO (m.in. RFN, Grecja i Turcja). Już tylko nieliczne państwa budowały po II wojnie światowej niszczyciele artyleryjskie (np. RFN, typ Hamburg); wyjątkiem był ZSRR, którego niszczyciele przedwojennej budowy były zdecydowanie przestarzałe, dlatego też flota sowiecka wcieliła do służby w latach 40. i 50. XX stulecia długie serie m.in. 2 typów (30 bis oraz typ 56). Podjęto też pierwsze próby przezbrajania istniejących niszczycieli z klasycznym uzbrojeniem artyleryjskim na jednostki rakietowe. Typowym przykładem są jednostki sowieckie typu 56, na których rufową dwulufową wieżę dział kalibru 130 mm zastąpiono wyrzutniami rakiet przeciwlotniczych (projekt 56 A). Do tego typu należał przekazany marynarce wojennej PRL ORP Warszawa. Pojawienie się pocisków ziemia–powietrze i ziemia–ziemia, takich jak Exocet, na początku lat 60. XX w. zmieniło sposób prowadzenia wojny na morzu. Niszczyciele rakietowe zostały opracowane w celu przenoszenia tej broni i ochrony floty przed zagrożeniami z powietrza, okrętów podwodnych i nawodnych. Przykładami są radzieckie okręty klasy Kashin, brytyjskie – County, i amerykańskie – Charles F. Adams. Wraz z nowym rakietowym uzbrojeniem rosła wyporność okrętów tej klasy. Przykładowo niszczyciele brytyjskiego typu County z lat 60. ubiegłego stulecia wypierały ponad 6 tys. t, niemal tyle co lekkie krążowniki z lat II wojny światowej. Choć uznane za okręty uniwersalne, były stosunkowo drogie w eksploatacji, dlatego też kolejna seria brytyjskich okrętów tej klasy (typ 42) była mniejsza i zdecydowanie mniej uniwersalna od poprzedników. Te oszczędności zemściły się podczas wojny falklandzkiej: brytyjska Royal Navy straciła 2 niszczyciele tego typu (Sheffield i Coventry). Co ciekawe, pierwszy z nich zatonął w wyniku trafienia rakiety Exocet, a takim samym pociskiem (choć wersji ziemia–woda) trafiono niszczyciela Glamorgan. Okręt ten, choć trafiony i uszkodzony, pozostał w linii, a doświadczenia te wywołały gorące dyskusje co do przyszłości, wielkości i uzbrojenia okrętów tej klasy. Obecnie niszczyciele są na wyposażeniu nielicznych

marynarek, a ich wielkość jest zróżnicowana: waha się od 3 tys. t w przypadku argentyńskich jednostek typu Almirante Brown (niemiecki typ MEKO 360H2) do ponad 10 tys. t u chińskiego niszczyciela typu 055. Ten ostatni okręt, według amerykańskich ekspertów, powinien być klasyfikowany jako krążownik rakietowy. Dodać w tym miejscu należy, że w japońskich siłach morskich samoobrony wszystkie większe jednostki nawodne klasyfikowane są jako niszczyciele, również okręty lotnicze typu Izumo nazywane są „niszczycielami helikopterowymi", choć wypierają prawie 30 tys. t i *de facto* są lotniskowcami. Nie ulega jednak wątpliwości, że niszczyciele na długo będą pełnić istotną rolę we flotach oceanicznych głównych mocarstw morskich.

Roman Kochnowski

R. Jackson, *Zerstörer, Fregatten und Korvetten*, Gondrom Verlag, Bindlach 2001; W. Koszela, *Niszczyciele Polskiej Marynarki Wojennej*, Alma Press, Warszawa 2013; D. Lyon, *The First Destroyers*, Chatham Publishing, 1 & 2 Faulkner's Alley, Cowcross St. London 1996; M.S. Sobański, *Niszczyciele Typu Narvik*, „Okręty Wojenne" 2025; S. Terzibaschitsch, *Zerstörer der U.S. Navy von der Farragut-Klasse bis zur Forrest-Sherman-Klasse*, Bechtermünz Verlag, Augsburg 1997; M.J. Whitley, *Zerstörer im Zweiten Weltkrieg. Technik – Klassen – Typen*, 2. Auflage, Motorbuch Verlag, Stuttgart 1997.

O

OCHRONA NAJWAŻNIEJSZYCH ORGANÓW PAŃSTWA POLSKIEGO W OKRESIE MIĘDZYWOJENNYM. Zamachy na przedstawicieli władzy są trwałym elementem historii świata i doprowadzały do poważnych w skutkach konsekwencji politycznych. Przed wybuchem I wojny światowej tylko w Polsce miało miejsce kilka zamachów na przedstawicieli ówczesnej władzy.

Pierwszy z zamachów został przeprowadzony 2 sierpnia 1906 r. przez Oddział Bojowy Organizację Bojową Polskiej Partii Socjalistycznej (OB PPS) na szefa żandarmów Królestwa Polskiego, generała Andrieja Markgrafskiego. Kolejny zamach miał miejsce 18 sierpnia 1906 r. i dokonała go ta sama organizacja, a ofiarą był generał-gubernator warszawski Gieorgij Skałon. W dniu 27 sierpnia 1906 r. zamachowcy z PPS zabili Nikołaja Wonlarlskiego, tymczasowego generała-gubernatora Warszawy i guberni warszawskiej.

Z kolei 28 czerwca 1914 r. w Sarajewie miał miejsce zamach na arcyksięcia Franciszka Ferdynanda. Wydarzenia światowe, nieuregulowana sprawa granic państwa oraz konflikty na wszystkich rubieżach, łącznie z rewolucją w Rosji, wymuszały powołanie służb odpowiedzialnych za bezpieczeństwo najważniejszych osób w Polsce. W listopadzie 1918 r. funkcję

naczelnego wodza odpowiedzialnego za organizowanie Wojska Polskiego oraz funkcję naczelnika państwa objął Józef Piłsudski. Postanowiono więc powołać oddziały odpowiedzialne za bezpieczeństwo naczelnika państwa oraz nowo powstałych organów państwowych. Wchodziły one w skład utworzonej wówczas kwatery wojskowej i składały się z oddziałów przybocznych naczelnika państwa, kompanii piechoty oraz Szwadronu Przybocznego Naczelnika Państwa i Naczelnego Wodza.

Z uwagi na konieczność zapewnienia bezpieczeństwa podczas wyprawy wileńskiej głównodowodzącemu Józefowi Piłsudskiemu 15 kwietnia 1919 r. zorganizowano Pluton Osłony Jazdy Naczelnego Wodza, który stanowił zalążek Szwadronu Przybocznego. Walki o Wilno były doskonałym sprawdzianem weryfikującym przydatność Plutonu Osłony Jazdy Naczelnego Wodza, stąd też powstała idea stworzenia podobnego oddziału, jako wyodrębnionej jednostki, której głównym zadaniem była służba na rzecz bezpieczeństwa naczelnika państwa i naczelnego wodza.

Latem 1919 r. por. Tadeusz Kobylański i ppor. Adam Jan Bolesław Michalewski otrzymali rozkaz zorganizowania Szwadronu Przybocznego składającego się z 4 plutonów, z prawem swobodnego doboru oficerów i podoficerów. We wrześniu 1919 r. jednostka rozpoczęła swoją działalność z pełnym stanem jednolicie umundurowanych żołnierzy; w jej skład wchodzili: dowódca szwadronu, 4 dowódców plutonów i 4 plutony liniowe. 26 kwietnia 1920 r. został zatwierdzony przez władze wojskowe etat Generalnej Adiutantury Naczelnego Wodza, która funkcjonowała już wcześniej. Zgodnie z tym postanowieniem Szwadron Przyboczny należał pod względem ewidencyjnym, szkolenia i uzupełnienia do szwadronu zapasowego 1 Pułku Szwoleżerów jako tzw. szwadron nadetatowy. Liczył 143 żołnierzy: 6 oficerów (dowódca, zastępca dowódcy, 4 dowódców plutonów), 29 podoficerów, 107 szeregowców, w tym 4 trębaczy i 1 majstra wojskowego. Na wyposażeniu szwadronu pozostawały 124 konie wierzchowe i 14 pociągowych. Poziom wyszkolenia Szwadronu Przybocznego stał na wysokim poziomie, a jego charakterystyczną cechą był wręcz wzorowy porządek. Przy starannej rekrutacji odwoływano się do zasobów kadrowych mającego legionowe korzenie 1 Pułku Szwoleżerów. W okresie pokojowym Szwadron Przyboczny poza zadaniami ochronnymi pełnił dodatkowo funkcje reprezentacyjne i ogólnowojskowe. Realizował zadania

związane z eskortowaniem naczelnika państwa, nuncjusza papieskiego i ambasadorów oraz posłów państw obcych udających się do Belwederu w celu złożenia listów uwierzytelniających.

W dniu 9 grudnia 1922 r. Zgromadzenie Narodowe spośród 5 kandydatów wybrało na urząd prezydenta Rzeczypospolitej prof. Gabriela Narutowicza, co wywołało manifestacje niezadowolenia, inspirowane głównie przez endecję. 11 grudnia 1922 r. protestujący tłum usiłował uniemożliwić dotarcie prezydentowi elektowi do gmachu sejmu i objęcie władzy. Wzburzeni protestujący zablokowali trasę przejazdu ławkami, a powóz prezydenta został obrzucony grudami śniegu. Zabezpieczający przejazd prezydenta 1 szwadron 1 Pułku Szwoleżerów Józefa Piłsudskiego sam nie był w stanie zapobiec atakom i został wsparty przez 2 szwadron rotmistrza Kazimierza Mastalerza (późniejszego bohatera kampanii 1939 r.). To umożliwiło bezpieczne przeprowadzenie prezydenta do Łazienek, a następnie – Belwederu. Akty nieprzyjazne wobec prezydenta powtarzały się jeszcze, z różnym nasileniem, w kolejnych dniach. Dotyczyły one także posłów ze środowisk, które swymi głosami doprowadziły do wyboru Narutowicza. Sytuacja ta zwróciła uwagę na braki w ochronie najwyższego przedstawiciela Rzeczypospolitej. W Belwederze odbyła się oficjalna uroczystość, podczas której naczelnik państwa przekazał prezydentowi Szwadron Przyboczny.

Po przejęciu władzy przez nowo wybranego prezydenta w Dodatku Tajnym Nr 30 do Dziennika Rozkazów Nr 50 ukazał się rozkaz, na mocy którego dotychczasowy Szwadron Przyboczny Naczelnika Państwa otrzymał nazwę Szwadron Przyboczny Prezydenta Rzeczypospolitej. 2 dni po zaprzysiężeniu, podczas otwarcia przez prezydenta wystawy w warszawskim Towarzystwie Zachęty Sztuk Pięknych doszło do zamachu na jego życie. Narutowicz został zamordowany 16 grudnia 1922 r. o godzinie 12.20 przez malarza i krytyka sztuki Eligiusza Niewiadomskiego, związanego ideowo z obozem narodowym. Przed 1914 r. uczestniczył on w konspiracji i był więziony w Cytadeli, brał również udział, jako ochotnik, w wojnie 1920 r. Pomimo takiej patriotycznej życiowej karty zdecydował się na zamach i nie uchylał się od poniesienia odpowiedzialności; wyznawał zasadę romantycznego terroryzmu, że odbierając komuś życie, w zamian należy złożyć w ofierze własne. Podczas późniejszego procesu nie poprosił

o łagodny wyrok, a gdy skazany został na śmierć, odmówił wystąpienia o łaskę. Wówczas obowiązek zapewnienia bezpieczeństwa prezydentowi spoczywał również na policji politycznej. Przeprowadzenie zamachu ujawniło nieudolność ówczesnych służb odpowiedzialnych za ochronę i zapewnienie bezpieczeństwa głowie państwa.

Zamach ten, a także nieudany atak na Józefa Piłsudskiego uświadomiły decydentom potrzebę powołania wyspecjalizowanej jednostki odpowiedzialnej za zapewnienie bezpieczeństwa kierowniczym organom w Polsce. Konsekwencją tego był rozkaz ministra spraw wewnętrznych Zygmunta Hübnera z dnia 12 czerwca 1924 r. o powołaniu brygady ochronnej, do zadań której należało zapewnienie bezpieczeństwa prezydentowi Rzeczypospolitej Polskiej, a działania prowadzono w oparciu o Instrukcję o prowadzeniu służby ochronnej. Dokument regulował formy prowadzenia działań ochronnych oraz sam zakres ochrony. Instrukcja uwzględniała 4 stopnie zabezpieczeń stosowanych wobec głowy państwa, a także prezydentów obcych państw i innych dygnitarzy polskich. Odbywało się to w formie ochrony osobistej, zabezpieczenia obiektów oraz tras i dworców kolejowych.

Ochrona I stopnia zawarta w Instrukcji o prowadzeniu służby ochronnej obowiązywała podczas najwyższego stopnia zagrożenia i uwzględniała wykorzystanie wszelkich możliwych i dostępnych środków, będących w dyspozycji brygady ochronnej. Podczas prowadzonych działań sprawdzano trasę przejazdu osoby ochranianej wraz z przyległymi terenami; w przypadku podróży koleją służby kontrolowały linie na 6 godzin przed przejazdem pociągu wiozącego osobę ochranianą. Kontrole przeprowadzała policja mundurowa przy pomocy wojska, rozmieszczając posterunki stałe, patrole piesze i konne. Zgodnie z obowiązującymi przepisami odległość pomiędzy wystawionymi patrolami nie mogła przekraczać kilometra, natomiast w terenach górskich, kiedy linia kolejowa była kręta, odległość tę zmniejszano. Ponadto zabezpieczeniu podlegały trasy i dworce kolejowe, mosty, zwrotnice, składy opałowe, z których brany był opał do lokomotywy. W miastach trasy przejazdu kontrolowały policja oraz żandarmeria: dzielono je na odcinki, które były podporządkowane wskazanym funkcjonariuszom, a za kilka takich odcinków odpowiadał oficer – komendant rejonu ochronnego. Podczas przejazdu osoby ochranianej obserwowano

okna domów, bramy i ulice. Przed przyjazdem osoby ochranianej do innych miejscowości przeprowadzano kontrolę hoteli, pensjonatów, pokoi gościnnych. Przy skrzyżowaniach umieszczano funkcjonariuszy, którzy w wypadku zaistnienia takiej konieczności zarządzali zamknięcie odcinka ulicy. Na terenach wiejskich ochrona składała się z posterunków policyjnych, ustawionych przy większych skupiskach ludności, patroli konnych i wywiadowczych. Przejazd osoby ochranianej samochodem zabezpieczany był przez pojazd jadący z przodu, w którym znajdował się przedstawiciel miejscowych władz z policjantem, natomiast za pojazdem ochranianym przemieszczały się 2 samochody z funkcjonariuszami brygady ochronnej. Miejsce zamieszkania osoby ochranianej było zabezpieczone 3 kordonami służb. Pierwszy stanowili funkcjonariusze brygady ochronnej, drugi formowali wywiadowcy, natomiast trzeci tworzyli policjanci mundurowi oraz żandarmi.

Ochrona II stopnia realizowana była w ograniczony sposób i swym zakresem obejmowała zabezpieczenie tras przejazdów i terenów przyległych przez policję, oraz zapewnienie ochrony bezpośredniej przez funkcjonariuszy brygady ochronnej.

Ochrona III stopnia swym zakresem obejmowała zabezpieczenie wyłącznie mostów i stacji kolejowych, na których zatrzymywał się pociąg z osobą ochranianą oraz ochroną bezpośrednią.

Natomiast ochrona IV stopnia swym zakresem obejmowała wyłącznie ochronę osobistą. O zastosowaniu konkretnego stopnia ochrony decyzję podejmował Departament Bezpieczeństwa i Prasy Ministerstwa Spraw Wewnętrznych, na wniosek naczelnika Wydziału V Komendy Głównej Policji Państwowej. Na czele brygady stał kierownik, któremu podlegali wszyscy żołnierze wchodzący w jej skład. Był on odpowiedzialny za precyzyjne i sprawne wykonywanie działań ochronnych związanych z zapewnieniem bezpieczeństwa prezydenta Rzeczypospolitej; podczas jego przejazdów kolejowymi środkami transportu kierownik brygady ochronnej stosował metody zabezpieczenia zawarte w instrukcji T.B.12251/24 z dnia 12 czerwca 1924 r. W przypadku wyjazdu prezydenta poza teren miasta brygada ochronna podlegała naczelnikowi Okręgowego Urzędu Policji Politycznej terenu, na którym znajdowała się osoba ochraniana. Po przewrocie majowym w 1926 r. w wielu instytucjach przeprowadzono

wiele zmian organizacyjnych oraz personalnych – w znacznym stopniu dotyczyły one również Gabinetu Wojskowego.

W 1926 r., po wybraniu na urząd prezydenta Ignacego Mościckiego, zapadła decyzja dotycząca likwidacji szwadronu. Na mocy zapisów zawartych w Dodatku Tajnym Nr 5 do Dziennika Rozkazów Nr 17 z dnia 30 czerwca żołnierze Szwadronu Przybocznego zostali przeniesieniu do 1 Pułku Szwoleżerów Józefa Piłsudskiego, w miejsce 2 szwadronu, który został podzielony między pozostałe jednostki. Pełnił funkcje reprezentacyjne i ogólnowojskowe, do których zaliczano eskortowanie ambasadorów i posłów obcych państw. Ponadto szwadron pełnił kilka razy w tygodniu służbę wartowniczą przy Belwederze. W wyniku przeprowadzonej likwidacji podjęto decyzję, iż służbę wartowniczą w rezydencji prezydenta Rzeczypospolitej, aż do dalszych rozkazów, obejmą jednostki garnizonu według zarządzeń komendanta miasta. Komendant miasta Warszawy w porozumieniu z generalnym adiutantem prezydenta Rzeczypospolitej decydował o zniesieniu służby wartowniczej w Belwederze. W ten sposób zatwierdzono tymczasowe pełnienie służby wartowniczej przez 22 Pułk Piechoty. Tym samym został unieważniony rozkaz ministra spraw wojskowych mówiący o podporządkowaniu Oddziału Przybocznego.

Na podstawie rozkazu ministra spraw wojskowych, opublikowanego w Dodatku Tajnym nr 6 do Dziennika Rozkazów nr 19 z dnia 20 lipca 1926 r., zlikwidowano Kwaterę Wojskową Prezydenta RP, powołując w jej miejsce Gabinet Wojskowy Prezydenta Rzeczypospolitej. W 1928 r. w wyniku przeprowadzonych zmian pododdziały przekształcono w Oddział Zamkowy, który z drobnymi zmianami funkcjonował do 1939 r. Ważne stanowiska, z punktu widzenia bezpieczeństwa i koordynacji prowadzonych czynności, zajmowali adiutanci przyboczni; oficerów na to stanowisko dobierano bardzo starannie i wywodzili się oni wyłącznie z elitarnych pułków II Rzeczypospolitej. Do 1928 r. stanowiska adiutantów przybocznych piastowali 2 oficerowie, następnie – z uwagi na specyfikę służby – liczbę te zwiększono do 3. Specyfika ta polegała na współdziałaniu przy realizowaniu codziennych obowiązków prezydenta, z uwzględnieniem aspektów bezpieczeństwa. Do takich obowiązków zaliczało się m.in. sprawdzenie samochodów pod względem gotowości do wyjazdu i kierowców, a także rzeczy osobistych prezydenta i towarzyszących mu

przedstawicieli urzędów. Ochronę miejsca zamieszkania prezydenta Ignacego Mościckiego, którym był Zamek Królewski, powierzono doskonale wyszkolonej, o nienagannej prezencji, kompanii zamkowej, która obok codziennej służby pełniła funkcje reprezentacyjną, asystując przy wizytach przedstawicieli państw obcych przebywających na terytorium Rzeczypospolitej Polskiej. W ramach struktur Gabinetu Wojskowego powołano do życia zamkową kolumnę samochodową. Pojazdy, które znajdowały się na wyposażeniu zamkowej kolumny samochodowej, wykorzystywane były do transportu prezydenta, jak również przedstawicieli państw obcych przebywających w Polsce.

W wyniku dalszych reform Gabinetu Wojskowego stworzono nową strukturę, która decydowała o podporządkowaniu szefa Gabinetu Wojskowego bezpośrednio prezydentowi, jednak w sprawach personalnych w dalszym ciągu podlegał on ministrowi spraw wojny. Szef Gabinetu Wojskowego w ramach swoich obowiązków odpowiadał za planowanie i przygotowanie krajowych oraz zagranicznych wyjazdów prezydenta, z uwzględnieniem terminu i składu delegacji towarzyszącej (m.in. trasy w przypadku przejazdu kolumną samochodową, aktualny rozkłady jazdy w przypadku podróży pociągiem oraz miejsca zakwaterowania dla prezydenta i członków delegacji).

W ramach realizacji czynności związanych z przygotowaniem zabezpieczenia szef Gabinetu Wojskowego współpracował z naczelnikiem wydziału V Komendy Głównej Policji Państwowej. Za prawidłowe współdziałanie funkcjonariuszy, żołnierzy i przedstawicieli administracji terenowej podczas zabezpieczenia tras przejazdu odpowiadał dowódca plutonu żandarmów.

Zgodnie z obowiązującą wówczas Instrukcją o prowadzeniu służby ochronnej trasy przejazdu podlegały szczególnemu „zadbaniu". Pod tym pojęciem mieści się obecnie stosowana kontrola pirotechniczna tras przejazdu prezydenckiej kolumny samochodowej, ponadto trasy przejazdu zabezpieczano przy użyciu patroli policji konnej oraz poprzez wystawienie posterunków policyjnych rozmieszczanych przy dużych skupiskach ludności. Natomiast mosty zabezpieczano za pomocą dwuosobowych posterunków policyjnych.

Do zadań funkcjonariuszy realizujących działania związane z zabezpieczeniem przeprawy należały obserwacja mostu oraz niedopuszczenie do przebywania w terenie przyległym osób niepowołanych podczas przejazdu osoby ochranianej. Instrukcja o prowadzeniu służby ochronnej przewidywała 4 stopnie zabezpieczenia prezydenta podczas przejazdu pojazdami kolumny samochodowej. Pierwszy uwzględniał zabezpieczenie pojazdu prezydenckiego przez 3 pojazdy ochronne: 1 poruszał się przed pojazdem głównym i zajmowali w nim miejsca przedstawiciele administracji terenowej oraz funkcjonariusz bezpieczeństwa, zaś pozostałe 2 – za pojazdem głównym. Drugi stopień uwzględniał użycie 2 pojazdów ochronnych do zabezpieczenia pojazdu głównego: 1 pojazd ochronny poruszał się przed pojazdem głównym, kolejny natomiast – za nim. Trzeci stopień zakładał udział w kolumnie 1 pojazdu ochronnego, co wpływało na zmniejszenie ilości żołnierzy ochrony osobistej.

Szczegółowego podziału zadań dokonał minister spraw wewnętrznych Marian Zyndram-Kościałkowski, wydając 19 grudnia 1934 r. Instrukcję ochronną, której druga część była zatytułowana: *Ochrona Prezydenta Rzeczypospolitej*. Przedmiotowy dokument określał zadania i podział kompetencji służb odpowiedzialnych za zapewnienie bezpieczeństwa prezydentowi Rzeczypospolitej Polskiej. Wprawdzie instrukcja nie dawała żołnierzom realizującym czynności ochronne uprawnień do prowadzenia dochodzeń i ścigania przestępców, jednak stwarzała możliwości podejmowania zdecydowanych działań ochronnych polegających na prowadzeniu stałej ochrony bezpośredniej wobec osoby uprawnionej, zabezpieczeniu miejsca zamieszkania oraz tras przejścia i przejazdu, jak również decydowaniu o doborze pracowników obsługi i służby. Zasadniczym rodzajem ochrony jest ochrona zwykła, która bez krępowania swobody osoby ochranianej winna być prowadzona dyskretnie, na podstawie stałych planów ochronnych, i uwzględniać przepisy protokołu dyplomatycznego oraz przyjęte zwyczaje. Przez ochronę obostrzoną należy rozumieć środki nadzwyczajne, zmierzające – zależnie od sytuacji – do zapewnienia ochrony w wytworzonych lub spodziewanych warunkach, szczególnie niebezpiecznych. Zgodnie z wytycznymi zawartymi w instrukcji ochrona bezpośrednia realizowana była w strefie wewnętrznej jako służba stała. Oficerowie realizujący czynności ochronne w strefie wewnętrznej mieli

obowiązek m.in. stałego przebywania w bezpośredniej bliskości osoby ochranianej. Ponadto do ich zadań należało znajdowanie się w składzie oficjalnej świty oraz kontrola miejsc pracy i wypoczynku osoby ochranianej.

Andrzej Czop

S. Zalewski, *Polityczny aspekt działania Biura Ochrony Rządu*, [w:] *Bezpieczeństwo osób podlegających ustawowo ochronie wobec zagrożeń XXI wieku*, P. Bogdalski, J. Cymerski, K. Jałoszyński (red.), Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji, Szczytno 2014; P.K. Marszałek, *Prawne podstawy organizacji ochrony VIP-ów w II Rzeczypospolitej*, „Studia Lubuskie" 2009, t. 5; K. Jałoszyński, J. Cymerski, *Organy administracji rządowej wobec zagrożeń terrorystycznych. Biuro Ochrony Rządu wobec terroryzmu*, Wyższa Szkoła Administracji, Bielsko-Biała 2013; K. Karolczak, *Encyklopedia terroryzmu*, Wydawnictwo Spar, Warszawa 1995; Z. Gnat-Wieteska, *Szwadrony Przyboczne i Szwadron Reprezentacyjny Wojska Polskiego w latach 1919–1948*, Ajaks, Pruszków 1992; E.J. Czerniawski, *Z mojej służby w Belwederze*, „Zeszyty Historyczne" 1975, nr 33; R. Litwiński, *Ochrona dostojników państwowych przez policję w II Rzeczypospolitej*, „Niepodległość" 2005, t. LV; E. Szumiec-Zielińska, *Kompania Zamkowa*, „Przegląd Historyczno-Wojskowy" 2002, t. 3, nr 2; J. Cymerski, A. Czop, *Służba Ochrony Państwa i Specjalistyczne Uzbrojone Formacje Ochronne wobec współczesnych zagrożeń*, Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2019.

ODPORNOŚĆ EKOLOGICZNA (ang. *ecological resilience*) stanowi jedno z fundamentalnych pojęć współczesnych nauk o środowisku i zrównoważonym rozwoju. Pojęcie to definiuje zdolność ekosystemów oraz systemów społeczno-ekologicznych do absorpcji zaburzeń, adaptacji do zmiennych warunków oraz utrzymania kluczowych funkcji, struktur i tożsamości mimo presji środowiskowych. Odporność ekologiczna odnosi się zarówno do procesów biotycznych i abiotycznych, jak i interakcji między komponentami przyrody oraz działalnością człowieka, stanowiąc ramy analityczne umożliwiające ocenę trwałości i stabilności systemów przyrodniczych w warunkach narastającej presji antropogenicznej. Szczególne znaczenie pojęcie to zyskało w kontekście globalnych zmian klimatu, degradacji siedlisk, fragmentacji krajobrazu, utraty bioróżnorodności oraz intensyfikacji użytkowania zasobów naturalnych.

Odporność ekologiczna oznacza zdolność systemu do utrzymania stabilnych relacji wewnętrznych oraz przystosowania się do zmian w warunkach środowiskowych w taki sposób, aby zapewnić swoje przetrwanie i dalsze funkcjonowanie. W odróżnieniu od klasycznego ujęcia stabilności opartego na założeniu pojedynczego punktu równowagi, odporność ekologiczna dopuszcza istnienie wielu alternatywnych stanów stabilnych, pomiędzy którymi system może się przemieszczać pod wpływem zaburzeń o różnej intensywności i częstotliwości. Ekosystem w tym ujęciu traktowany jest jako układ dynamiczny, zdolny do reorganizacji, rekombinacji struktur oraz zmian konfiguracji funkcjonalnych bez konieczności utraty swojej tożsamości.

W literaturze przedmiotu podkreśla się ścisły związek odporności z pojęciami złożoności struktur troficznych, sieci interakcji ekologicznych oraz nieliniowej dynamiki systemów. Stabilność nie jest rozumiana jako statyczny brak zmian, lecz zdolność do utrzymania funkcjonalnej integralności w warunkach zmienności i niepewności. Rozróżnia się przy tym pojęcia odporności (*resilience*) i oporności (*resistance*) jako odrębne, choć powiązane komponenty reakcji systemów ekologicznych. Oporność oznacza zdolność do przeciwstawiania się zaburzeniom bez istotnych zmian strukturalnych, natomiast odporność obejmuje zdolność do absorpcji zakłóceń i reorganizacji bez utraty zasadniczych funkcji systemu.

Współczesne ujęcia teoretyczne wprowadzają dodatkowe kategorie opisowe, w tym adaptowalność (*adaptability*) i transformowalność (*transformability*). Adaptowalność definiowana jest jako zdolność podmiotów funkcjonujących w systemie do wpływania na jego odporność poprzez modyfikację strategii, procesów i struktur w odpowiedzi na zmieniające się warunki zewnętrzne, obejmując uczenie się, elastyczność instytucjonalną oraz eksperymentowanie w ramach istniejących ograniczeń. Transformowalność odnosi się natomiast do zdolności tworzenia zasadniczo nowego systemu w sytuacji, gdy dotychczasowy układ staje się niefunkcjonalny z przyczyn ekologicznych, ekonomicznych lub społecznych, umożliwiając fundamentalną zmianę kierunku rozwojowego.

W literaturze naukowej wyróżnia się 3 podstawowe typy odporności, różniące się założeniami ontologicznymi oraz implikacjami praktycznymi. Odporność inżynieryjna (*engineering resilience*) opiera się na założeniu

istnienia pojedynczego stanu równowagi i koncentruje się na szybkości powrotu systemu do stanu wyjściowego po zakłóceniu, akcentując efektywność, stabilność operacyjną oraz przewidywalność zachowania układu. Odporność ekologiczna (*ecological resilience*) uznaje możliwość istnienia wielu stanów stabilnych i mierzy się wielkością zaburzenia, jakie może zostać zaabsorbowane bez trwałej zmiany reżimu funkcjonowania systemu, podkreślając znaczenie trwałości, zmienności i nieliniowości procesów. Odporność społeczno-ekologiczna (*social-ecological resilience*) odnosi się do systemów złożonych z komponentów przyrodniczych i społecznych, definiując ich zdolność do absorpcji stresorów, samoorganizacji, uczenia się oraz adaptacji przy zachowaniu podstawowych funkcji i struktur, a także zdolność do modyfikacji reguł funkcjonowania w odpowiedzi na zmiany długookresowe.

Istotnym elementem współczesnej teorii odporności jest Model Cyklu Adaptacyjnego (Adaptive Cycle Model), opisujący dynamikę systemów złożonych poprzez 4 fazy: eksploatacji (r) charakteryzującej się szybkim wzrostem i akumulacją zasobów; konserwacji (K) obejmującej stopniowe zwiększanie powiązań i stabilizacji struktur przy jednoczesnym narastaniu sztywności; uwolnienia (Ω) polegającej na gwałtownym rozpadzie dotychczasowych powiązań i uwolnieniu zasobów wskutek zaburzeń; oraz reorganizacji (α) umożliwiającej powstawanie nowych konfiguracji strukturalnych i funkcjonalnych. Rozszerzeniem tego modelu jest koncepcja panarchii opisująca hierarchiczną organizację cykli adaptacyjnych funkcjonujących na różnych skalach czasowych i przestrzennych, w ramach której wyróżnia się mechanizmy interakcji między poziomami, takie jak oddziaływania wstępujące oraz mechanizmy pamięci systemowej, a także zjawiska pułapek ubóstwa i sztywności jako stanów ograniczających zdolność do adaptacji.

Empiryczne badania funkcjonowania odporności ekologicznej wskazują na zróżnicowane trajektorie zmian w zależności od typu ekosystemu. W ekosystemach leśnych obserwuje się istotne tendencje spadku odporności lasów tropikalnych i umiarkowanych, mierzone wzrostem autokorelacji czasowej wskaźników produktywności. Lasy borealne wykazują lokalnie przejściowy wzrost odporności, interpretowany jako efekt wyższych temperatur i zwiększonej koncentracji dwutlenku węgla, jednak

proces ten nie eliminuje ryzyka długoterminowej destabilizacji. Szacuje się, że znaczna część nienaruszonych lasów osiągnęła już poziomy bliskie progom krytycznym, przy których prawdopodobieństwo gwałtownych zmian reżimu ekologicznego istotnie wzrasta.

Szczególne znaczenie przypisuje się ekosystemom Amazonii, w których identyfikuje się krytyczne wartości rocznych sum opadów, długości pory suchej, skumulowanego deficytu wodnego oraz udziału powierzchni podlegającej wylesianiu, po przekroczeniu których możliwa jest nieodwracalna transformacja funkcjonalna. Wskazuje się, że przy utrzymaniu obecnych trendów presji antropogenicznej punkt krytyczny może zostać osiągnięty w perspektywie najbliższych dekad, co oznaczałoby przejście od systemu lasów deszczowych do formacji bardziej sucholubnych i mniej produktywnych biologicznie.

Ekosystemy morskie, w szczególności rafy koralowe, charakteryzują się wrażliwością na wahania temperatury wody oraz zakwaszenie oceanów. Identyfikuje się krytyczne progi częstości zjawisk bielenia, po przekroczeniu których dochodzi do gwałtownej degradacji struktury raf i utraty bioróżnorodności. Pomimo obserwowanej stopniowej adaptacji termicznej koralowców tempo zmian klimatycznych przewyższa zdolności dostosowawcze wielu gatunków. Zakwaszenie oceanów, związane ze wzrostem koncentracji dwutlenku węgla, prowadzi do spadku pH wód i osłabienia procesów kalcyfikacji, co wpływa negatywnie na przeżywalność i wzrost organizmów o szkieletach wapiennych. Prognozy wskazują na istotne zmniejszenie globalnego potencjału połowowego w scenariuszach wysokich emisji.

Torfowiska stanowią jeden z kluczowych magazynów węgla w biosferze, pomimo relatywnie niewielkiego udziału w powierzchni lądowej globu. Akumulują one znaczące ilości węgla organicznego w warunkach ograniczonej dostępności tlenu i niskiego tempa rozkładu materii organicznej. Odwodnienie torfowisk prowadzi do gwałtownego wzrostu emisji gazów cieplarnianych oraz zwiększa podatność na pożary o dużej intensywności. Pożary torfowisk generują skrajnie wysokie emisje dwutlenku węgla i aerozoli, wywierając wpływ na bilans radiacyjny atmosfery oraz jakość powietrza w skali regionalnej i globalnej.

Ekosystemy przybrzeżne, w tym lasy namorzynowe i solniska, wykazują ograniczoną zdolność adaptacji do wzrostu poziomu morza. Zdolność ta zależy od tempa depozycji osadów mineralnych, akumulacji materii organicznej w glebie oraz odporności struktur korzeniowych na erozję i zagęszczanie. Przekroczenie określonych progów tempa wzrostu poziomu morza prowadzi do utraty siedlisk, degradacji usług ekosystemowych oraz zwiększenia podatności obszarów lądowych na zalewanie i sztormy.

Odporność miejska (*urban resilience*) stanowi odrębną kategorię analityczną, opisującą zdolność systemów miejskich do utrzymania lub szybkiego odzyskiwania pożądanych funkcji w warunkach zaburzeń, w tym katastrof naturalnych, kryzysów infrastrukturalnych oraz długoterminowych zmian klimatycznych. Ujęcia systemowe integrują komponenty społeczne, ekologiczne i technologiczne, traktując miasto jako system złożony, w którym kluczowe znaczenie mają: zdolność do uczenia się, elastyczność struktur zarządzania, redundancja infrastrukturalna, sprawiedliwość społeczna, różnorodność funkcjonalna, przewidywalność zagrożeń oraz zdolność do transformacji w odpowiedzi na ograniczenia rozwojowe. Dominujące podejścia analityczne wskazują, że wysoki poziom odporności miejskiej wymaga równoległego wzmacniania kapitału społecznego, jakości środowiska przyrodniczego oraz niezawodności systemów technicznych.

Miejska wyspa ciepła (Urban Heat Island, UHI) stanowi zjawisko klimatyczne polegające na podwyższonej temperaturze powietrza na obszarach zurbanizowanych względem terenów niezurbanizowanych, zwykle w zakresie 1–7°C. Zjawisko to wynika z dominacji powierzchni nieprzepuszczalnych, zwiększonej pojemności cieplnej materiałów budowlanych, ograniczonej ewapotranspiracji, zmodyfikowanej cyrkulacji powietrza w tzw. kanionach ulicznych oraz emisji ciepła antropogenicznego. Strategie mitygacyjne obejmują rozwój parków miejskich, drzew ulicznych, zielonych dachów oraz niebiesko-zielonej infrastruktury (zintegrowany system terenów zielonych i elementów wodnych w miastach mający na celu gospodarowanie wodą opadową, łagodzenie skutków zmian klimatu (powodzie, susze) i poprawę jakości życia, integrujący rozwiązania oparte na przyrodzie, takie jak ogrody deszczowe, zielone dachy, stawy retencyjne czy przepuszczalne nawierzchnie zamiast tradycyjnej betonowej

infrastruktury), przy czym efekt wyspy chłodu generowany przez duże obszary zieleni miejskiej może obniżać temperaturę lokalną o wartości porównywalne z intensywnością samego efektu UHI. Rozwiązania oparte na przyrodzie są oceniane jako wysoce efektywne ekonomicznie, wykazując przeciętnie istotnie korzystniejszy stosunek kosztów do korzyści niż klasyczne interwencje inżynieryjne, a także dostarczając dodatkowych korzyści ekosystemowych w porównaniu z infrastrukturą szarą.

Koncepcja miast-gąbek (*sponge cities*) funkcjonuje jako podejście planistyczne oparte na infrastrukturze hydroekologicznej, której celem jest zwiększenie zdolności obszarów miejskich do infiltracji, retencji, magazynowania i samooczyszczania wód opadowych. Model ten zakłada szerokie zastosowanie rozwiązań opartych na przyrodzie, takich jak ogrody deszczowe, nawierzchnie przepuszczalne, mokradła miejskie i systemy retencyjne oparte na procesach biologicznych i fizycznych. W praktyce wdrożeniowej programy typu „miasto-gąbka" obejmują dziesiątki ośrodków miejskich i formułują długoterminowe cele dotyczące udziału powierzchni miejskiej wyposażonej w elementy retencyjne, przy czym założenia te odnoszą się do reorganizacji hydrologii miejskiej w skali całych zlewni zurbanizowanych.

Odporność klimatyczna w ujęciu międzynarodowych ocen naukowych definiowana jest jako zdolność złożonych systemów społecznych, ekonomicznych i ekologicznych do radzenia sobie z zagrożeniami klimatycznymi poprzez absorpcję zakłóceń, adaptację struktur i funkcji oraz reorganizację w sposób pozwalający zachować podstawową tożsamość i zdolność do dalszego rozwoju. Wyróżnia się 3 komplementarne komponenty odporności: zdolność adaptacyjną obejmującą stopniowe dostosowywanie się do zmian; zdolność antycypacyjną odnoszącą się do prognozowania i przygotowania na przyszłe zagrożenia; oraz zdolność absorpcyjną polegającą na ograniczaniu behawioralnych i strukturalnych skutków nagłych zdarzeń. Wskazuje się, że znaczna część populacji świata funkcjonuje w kontekstach wysokiej podatności na zmiany klimatu, a możliwość pogodzenia rozwoju społeczno-gospodarczego z odpornością klimatyczną ulega istotnemu ograniczeniu wraz ze wzrostem globalnej temperatury powyżej progów uznawanych za krytyczne dla stabilności systemu klimatycznego.

Bioróżnorodność uznawana jest za fundamentalny czynnik stabilności procesów ekosystemowych, wpływający zarówno na poziom produktywności, jak i na jej zmienność w czasie. Wskazuje się na silne uzależnienie globalnej aktywności ekonomicznej od usług ekosystemowych, obejmujących regulację klimatu, zapylanie, dostęp do wody oraz stabilność systemów żywnościowych. Redundancja funkcjonalna rozumiana jest jako stopień, w jakim wiele gatunków pełni podobne role ekologiczne, tworząc efekt portfelowy stabilizujący ogólną dynamikę systemu. Zależność pomiędzy redundancją a stabilnością cechuje się jednak wysoką zmiennością, co wskazuje na kontekstową specyfikę relacji między strukturą zespołów biologicznych a odpornością.

Hipotezy teoretyczne dotyczące stabilności ekosystemów obejmują koncepcję efektu ubezpieczeniowego, zgodnie z którą bogactwo gatunkowe zmniejsza fluktuacje czasowe produktywności i zwiększa jej długookresowe średnie wartości. Uzupełnieniem tego ujęcia jest pojęcie różnorodności odpowiedzi, opisujące zróżnicowanie reakcji gatunków na stresory środowiskowe w obrębie tej samej grupy funkcjonalnej, co traktowane jest jako kluczowy mechanizm zabezpieczający systemy przyrodnicze przed niepewnością i zmiennością warunków zewnętrznych.

Łączność ekologiczna stanowi podstawę funkcjonowania metapopulacji i procesów krajobrazowych, umożliwiając przepływ osobników, genów i propagul oraz ograniczając negatywne skutki fragmentacji siedlisk. Systemy przestrzennie rozdzielonych populacji, połączonych okresową dyspersją, zapewniają długookresowe przetrwanie gatunków poprzez mechanizmy kolonizacji i rekolonizacji. Empiryczne i modelowe analizy wskazują, że dobrze zaprojektowane korytarze ekologiczne zmniejszają zróżnicowanie genetyczne między płatami siedlisk i zwiększają zmienność genetyczną wewnątrz populacji, co przekłada się na podwyższoną zdolność adaptacyjną.

Progi ekologiczne definiowane są jako nieciągłe przejścia między stanami systemu, w których relatywnie niewielka zmiana czynnika sprawczego może wywołać gwałtowną reorganizację struktury i funkcji. Przejścia reżimowe obejmują szybkie transformacje systemów między alternatywnymi stanami stabilnymi, często związane z utratą kluczowych sprzężeń zwrotnych. Punkty krytyczne rozumiane są jako wartości

progowe, po których przekroczeniu reorganizacja ma charakter nagły i w wielu przypadkach nieodwracalny w skali czasowej istotnej z punktu widzenia zarządzania środowiskowego. Zjawisko histerezy opisuje zależność aktualnego stanu systemu od jego trajektorii historycznej, skutkującą asymetrią pomiędzy warunkami degradacji i odbudowy.

Wczesne sygnały ostrzegawcze nadchodzących przejść krytycznych obejmują wzrost autokorelacji i wariancji zmiennych stanu, zmiany rozkładów statystycznych, zjawiska migotania (*flickering*) między stanami alternatywnymi oraz charakterystyczne wzorce przestrzenne. Modele predykcyjne oraz eksperymenty w skali ekosystemowej potwierdzają użyteczność tych wskaźników, choć ich skuteczność zależy od jakości i długości szeregów danych oraz specyfiki analizowanego systemu.

Koncepcja granic planetarnych identyfikuje zestaw procesów biofizycznych regulujących stabilność systemu Ziemi, w ramach których wyróżnia się zmiany klimatu, integralność biosfery, obiegi biogeochemiczne azotu i fosforu, zmianę użytkowania gruntów, stan wód słodkich, obecność nowych substancji antropogenicznych, zakwaszenie oceanów, obciążenie aerozolami atmosferycznymi oraz stan warstwy ozonowej. Aktualne oceny wskazują na przekroczenie większości zidentyfikowanych granic, co zwiększa ryzyko destabilizacji powiązanych procesów i kaskadowych efektów w skali globalnej.

Systemy społeczno-ekologiczne (SES) rozumiane są jako trwale sprzężone układy procesów biofizycznych i społecznych, funkcjonujące poprzez regularne interakcje między komponentami przyrodniczymi i instytucjonalnymi. Analizy systemowe wskazują na znaczenie struktur zarządzania, reguł dostępu do zasobów oraz zdolności do samoorganizacji jako kluczowych determinant trwałości takich systemów. Złożoność SES wymaga podejść policentrycznych i adaptacyjnych, uwzględniających wielopoziomowe sprzężenia zwrotne i lokalne uwarunkowania.

Zasady budowania odporności w systemach społeczno-ekologicznych obejmują utrzymywanie różnorodności i redundancji, świadome zarządzanie łącznością, koncentrację na zmiennych wolnozmiennych i sprzężeniach zwrotnych, rozwijanie kompetencji w zakresie myślenia systemowego, promowanie uczenia się iteracyjnego, poszerzanie partycypacji interesariuszy oraz wzmacnianie policentrycznych struktur zarządzania.

Analizy literatury wskazują jednak na ograniczoną skalę ich praktycznej operacjonalizacji, co ujawnia znaczącą lukę pomiędzy rozwojem teorii a implementacją.

Ramy rozwoju odpornego klimatycznie odnoszą się do integracji działań adaptacyjnych i mitygacyjnych w celu równoczesnego ograniczania ryzyka klimatycznego i wspierania zrównoważonego rozwoju. W tym ujęciu globalne porozumienia środowiskowe formułują cele adaptacyjne i zobowiązania finansowe mające na celu ograniczanie podatności systemów społeczno-ekologicznych oraz wzmacnianie ich zdolności do reagowania na zmiany klimatu. Znaczenie mają również międzynarodowe ramy ochrony bioróżnorodności, ukierunkowane na zwiększanie powierzchni obszarów chronionych, odbudowę ekosystemów zdegradowanych i mobilizację zasobów finansowych.

Zarządzanie adaptacyjne stanowi podejście iteracyjne, w którym strategie traktowane są jako hipotezy robocze, a interwencje – jako kontrolowane eksperymenty sprzyjające akumulacji wiedzy i redukcji niepewności decyzyjnej. Wyróżnia się podejście aktywne, oparte na równoległym testowaniu alternatywnych modeli decyzyjnych, oraz pasywne, w którym uczenie się następuje jako efekt uboczny wdrażanych działań. Proces ten obejmuje cykliczne fazy diagnozy problemu, projektowania interwencji, implementacji, monitoringu, ewaluacji i korekty działań.

Rozwiązania oparte na przyrodzie (Nature-based Solutions, NbS) definiowane są jako działania ukierunkowane na ochronę, zrównoważone zarządzanie i odbudowę ekosystemów w sposób umożliwiający równoczesne osiąganie celów społecznych, ekonomicznych i przyrodniczych. Uzupełnieniem jest adaptacja oparta na ekosystemach (EbA), skoncentrowana na zmniejszaniu podatności na skutki zmian klimatu poprzez wzmacnianie funkcji regulacyjnych ekosystemów. Analizy wskazują na znaczący potencjał tych rozwiązań w zakresie mitygacji i adaptacji, przy jednoczesnym dostarczaniu współkorzyści dotyczących jakości życia i ochrony bioróżnorodności.

Pomiar odporności ekologicznej pozostaje obszarem intensywnego rozwoju metodologicznego. Wykorzystywane są metody analizy wczesnych sygnałów ostrzegawczych, identyfikacji punktów przerwania oraz analizy szeregów czasowych wskaźników funkcjonowania ekosystemów.

Teledetekcja satelitarna, indeksy wegetacyjne oraz zintegrowane wskaźniki syntetyczne umożliwiają monitorowanie zmian w czasie i przestrzeni, przy czym ograniczeniem pozostają brak uniwersalnych miar oraz wysoka zależność wyników od kontekstu lokalnego.

Fragmentacja siedlisk identyfikowana jest jako jeden z głównych czynników ograniczających odporność systemów przyrodniczych, prowadząc do spadku bioróżnorodności oraz degradacji funkcji regulacyjnych. Skutki brzegowe, izolacja płatów siedlisk i dług czasowy wymierania pogłębiają długofalową degradację systemów. Równolegle zanieczyszczenie mikroplastikiem stanowi czynnik presji na ekosystemy wodne i lądowe, wpływając negatywnie na procesy glebowe, aktywność mikroorganizmów oraz wydajność fotosyntetyczną roślin.

Postępujące zmiany w ekosystemach słodkowodnych przejawiają się spadkiem odporności jezior w skali globalnej, powiązanym z presją demograficzną i eutrofizacją. Ryzyko kaskadowych punktów krytycznych wzrasta wraz z intensyfikacją interakcji pomiędzy elementami systemu klimatycznego i biosfery, prowadząc do obniżania progów wyzwalających przejścia fazowe.

Luki badawcze obejmują brak standaryzacji metodologii, niedostateczne dane długoterminowe, niepełne rozpoznanie sprzężeń zwrotnych oraz ograniczoną zdolność do integracji danych pochodzących z różnych skał. Rozwój metod opartych na środowiskowym eDNA, sztucznej inteligencji oraz zaawansowanej teledetekcji umożliwia coraz dokładniejsze monitorowanie procesów ekologicznych, jednak skuteczność tych podejść zależy od dostępności infrastruktury danych oraz koordynacji działań badawczych.

Odporność ekologiczna traktowana jest obecnie jako kategoria centralna dla polityki środowiskowej i klimatycznej, stanowiąc podstawę projektowania strategii adaptacyjnych, restauracyjnych i transformacyjnych. Integracja wiedzy naukowej z praktyką zarządczą pozostaje kluczowym wyzwaniem wymagającym przejścia od deklaratywnych ram normatywnych do operacyjnych modeli wdrożeniowych, zdolnych do ograniczania ryzyka systemowego i zwiększania trwałości relacji człowieka z biosferą.

Aleksander Wasiuta

Ch.R. Biggs, *Does functional redundancy affect ecological stability and resilience? A review and meta-analysis*, „Ecosphere" 2020, vol. 11, no. 7; D.F. Boesch, *Diversity, stability and response to human disturbance in estuarine ecosystems*, „Proceedings of the First International Congress of Ecology" 1974, vol. 1; C.A. Boulton, T.M. Lenton, N. Boers, *Pronounced loss of Amazon rainforest resilience since the early 2000s*, „Nature Climate Change" 2022, vol. 12, no. 3; S.R. Carpenter, *Early warnings of regime shifts: a whole-ecosystem experiment*, „Science" 2011, vol. 332, no. 6033; S.R. Carpenter, W.A. Brock, *Rising variance: a leading indicator of ecological transition*, „Ecology Letters" 2006, vol. 9, no. 3; *Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report*, Cambridge University Press, Cambridge 2022; T. Elmqvist, *Response diversity, ecosystem change, and resilience*, „Frontiers in Ecology and the Environment" 2003, vol. 1, no. 9; B.M. Flores, *Critical transitions in the Amazon forest system*, „Nature" 2024, vol. 626, no. 7999; C. Folke, *Resilience: The emergence of a perspective for social-ecological systems analyses*, „Global Environmental Change" 2006, vol. 16, no. 3; G. Forzieri, *Emerging signals of declining forest resilience under climate change*, „Nature" 2022, vol. 608, no. 7923; R. Le Gouvello, *The IUCN Global Standard for Nature-based Solutions™ as a tool for enhancing the sustainable development of marine aquaculture*, „Frontiers in Marine Science" 2023, vol. 10; P.M. Groffman, *Ecological thresholds: the key to successful environmental management or an important concept with no practical application?*, „Ecosystems" 2006, vol. 9, no. 1; L.H. Gunderson, *Ecological resilience – in theory and application*, „Annual Review of Ecology and Systematics" 2000, vol. 31, no. 1; N.M. Haddad, *Habitat fragmentation and its lasting impact on Earth's ecosystems*, „Science Advances" 2015, vol. 1, no. 2; B.T. Hart, *Ecological risk to aquatic systems from salinity increases*, „Australian Journal of Botany" 2003, vol. 51, no. 6; *Human-nature interactions in the Anthropocene: potentials of social-ecological systems analysis*, M.Glaser (ed.), Routledge, London 2012; R.T. Kingsford, *Ramsar wetlands of international importance–improving conservation outcomes*, „Frontiers in Environmental Science" 2021, vol. 9; K.J. Kroeker, *Impacts of ocean acidification on marine organisms: quantifying sensitivities and interaction with warming*, „Global Change Biology" 2013, vol. 19, no. 6; R. MacArthur, *Fluctuations of animal populations and a measure of community stability*, „Ecology" 1955, vol. 36, no. 3; M.D. McGinnis, E. Ostrom, *Social-ecological system framework: initial changes and continuing challenges*, „Ecology and Society" 2014, vol. 19, no. 2; T. McPhearson, *A social-ecological-technological systems framework for urban ecosystem services*, „One Earth" 2022, vol. 5, no. 5; S. Meerow, J.P. Newell, M. Stults, *Defining urban resilience: A review*, „Landscape and Urban Planning" 2016, vol. 147; E. Ostrom, *A diagnostic approach for going beyond panaceas*, „Proceedings of the National Academy of Sciences" 2007, vol. 104, no.

39; E. Ostrom, *A general framework for analyzing sustainability of social-ecological systems*, „Science" 2009, vol. 325, no. 5939; J. Rockström, *A safe operating space for humanity*, „Nature" 2009, vol. 461, no. 7263; J. Rockström, *Planetary boundaries: exploring the safe operating space for humanity*, „Ecology and Society" 2009, vol. 14, no. 2; N. Saintilan, *Thresholds of mangrove survival under rapid sea level rise*, „Science" 2020, vol. 368, no. 6495; M. Scheffer, *Catastrophic shifts in ecosystems*, „Nature" 2001, vol. 413, no. 6856; M. Scheffer, *Early-warning signals for critical transitions*, „Nature" 2009, vol. 461, no. 7260; W. Steffen, *Planetary boundaries: Guiding human development on a changing planet*, „Science" 2015, vol. 347, no. 6223; B. Walker, *Resilience, adaptability and transformability in social-ecological systems*, „Ecology and Society" 2004, vol. 9, no. 2; N. Wunderling, A. von der Heydt, *Climate tipping point interactions and cascades*, The Global Tipping Points: Report 2023, 2023; S. Yachi, M. Loreau, *Biodiversity and ecosystem productivity in a fluctuating environment: the insurance hypothesis*, „Proceedings of the National Academy of Sciences" 1999, vol. 96, no. 4.

ODPORNOŚĆ ENERGETYCZNA (ang. *energy resilience*) stanowi jedno z fundamentalnych pojęć współczesnej polityki energetycznej oraz nauk o infrastrukturze krytycznej, opisując zdolność systemów energetycznych do antycypowania zaburzeń, absorpcji ich skutków, szybkiej odbudowy funkcjonalności oraz adaptacji do zmiennych warunków operacyjnych przy jednoczesnym zachowaniu ciągłości dostaw energii dla odbiorców końcowych. Pojęcie to, intensywnie rozwijane od początku XXI w. w odpowiedzi na narastające zagrożenia klimatyczne, geopolityczne i cybernetyczne, zyskało szczególne znaczenie w kontekście transformacji energetycznej, postępującej elektryfikacji gospodarki oraz rosnącej zależności społeczeństw od stabilnych i niezakłóconych dostaw energii elektrycznej, gazu ziemnego i paliw płynnych. W odróżnieniu od klasycznie rozumianej niezawodności energetycznej, koncentrującej się na minimalizowaniu prawdopodobieństwa awarii w warunkach standardowej eksploatacji, odporność energetyczna obejmuje znacznie szersze spektrum zagadnień, uwzględniając zdolność systemu do funkcjonowania w warunkach ekstremalnych zdarzeń o niskim prawdopodobieństwie wystąpienia, lecz potencjalnie katastrofalnych konsekwencjach, określanych w literaturze jako *high-impact low-probability events* (HILP). Analizy Międzynarodowej Agencji Energetycznej jednoznacznie wskazują, że sektor energetyczny

stanowi kręgosłup funkcjonowania pozostałej infrastruktury krytycznej – telekomunikacji, transportu, systemów wodociągowych oraz rynków finansowych – przez co zakłócenia w dostawach energii mogą generować kaskadowe awarie o zasięgu znacząco wykraczającym poza sam sektor elektroenergetyczny.

Geneza współczesnego ujęcia odporności systemów sięga prac Crawforda Stanleya Hollinga z lat 70. XX w., poświęconych odporności systemów ekologicznych, które następnie zostały zaadaptowane do analizy systemów inżynieryjnych oraz infrastruktury krytycznej. Przełomowy charakter miała publikacja Michela Bruneau z 2003 r., w której zaproponowano czterowymiarowe ujęcie odporności społeczności na zagrożenia obejmujące wymiary techniczny, organizacyjny, społeczny i ekonomiczny. W kolejnych latach koncepcja ta została przeniesiona na grunt systemów energetycznych, przy czym istotny wkład wnieśli m.in. Thomas P. Hughes, analizujący znaczenie czasu trwania zdarzeń zakłócających dla zdolności adaptacyjnych systemów, oraz Holger Gasser i jego współpracownicy, którzy w 2021 r. w *Sustainable and Resilient Infrastructure* przedstawili kompleksowy przegląd metod oceny odporności systemów energetycznych. W literaturze funkcjonuje wiele definicji odporności energetycznej różniących się zakresem oraz akcentami metodologicznymi. Według Resilience Alliance odporność interpretowana jest jako zdolność systemu do absorpcji zaburzeń przy jednoczesnym zachowaniu podstawowych funkcji, struktury i tożsamości. Raport Szóstego Raportu Oceny (AR6) ujmuje odporność jako zdolność wzajemnie powiązanych systemów społecznych, ekonomicznych i ekologicznych do reagowania na niebezpieczne zdarzenia, trendy lub zaburzenia poprzez reorganizację umożliwiającą zachowanie ich fundamentalnych funkcji. Z kolei inne publikacje proponują definicję odporności systemu energetycznego jako jego zdolności do „odbicia się naprzód" (*bounce forward*) w obliczu zagrożeń, integrującej cechy techniczne, komponenty społeczno-techniczne oraz normatywny cel zapewnienia bezpiecznego, zrównoważonego, konkurencyjnego i dostępnego cenowo zaopatrzenia w energię.

Współczesna literatura rozróżnia kilka typów odporności energetycznej w zależności od przyjętej perspektywy teoretycznej i praktycznej. Odporność inżynieryjna koncentruje się na szybkości powrotu systemu

do stanu równowagi po wystąpieniu zakłócenia, kładąc nacisk na efektywność, przewidywalność oraz możliwość precyzyjnej kontroli parametrów technicznych. Odporność ekologiczna zakłada istnienie wielu stanów stabilnych i definiowana jest poprzez zdolność systemu do pochłaniania zakłóceń bez utraty kluczowych funkcji i struktury. Trzecią kategorię stanowi odporność społeczno-ekologiczna, która integruje aspekty techniczne z procesami społecznymi, instytucjonalnymi i zarządczymi, co ma szczególne znaczenie w odniesieniu do systemów energetycznych jako złożonych systemów społeczno-technicznych, osadzonych w określonych uwarunkowaniach politycznych, ekonomicznych i kulturowych. Ramy operacyjne oceny odporności energetycznej najczęściej opierają się na koncepcji krzywej odporności, opisującej zmianę poziomu wydajności systemu w czasie przed, w trakcie i po wystąpieniu zdarzenia zakłócającego. W modelu tym wyróżnia się cztery podstawowe funkcje odporności: opór (*resist*), restabilizację (*restabilize*), odbudowę (*rebuild*) oraz rekonfigurację (*reconfigure*). Funkcja oporu odnosi się do zdolności systemu do minimalizowania początkowej degradacji wydajności w odpowiedzi na zakłócenie. Restabilizacja obejmuje proces zatrzymywania dalszej degradacji parametrów pracy bezpośrednio po zdarzeniu. Odbudowa dotyczy działań zmierzających do przywrócenia funkcjonowania systemu do poziomu sprzed zakłócenia lub do stanu funkcjonalnie równoważnego. Rekonfiguracja natomiast opisuje zdolność systemu do adaptacji i transformacji strukturalnej w odpowiedzi na zmieniające się warunki, w tym potencjał przejścia do nowego, bardziej odpornego stanu funkcjonowania.

Zagrożenia dla odporności systemów energetycznych można klasyfikować w kilku głównych kategoriach, przy czym każda z nich wymaga odmiennych strategii prewencyjnych i adaptacyjnych. Pierwszą, historycznie najistotniejszą grupę stanowią zagrożenia pogodowe i klimatyczne, które odpowiadają za znaczną część zakłóceń w dostawach energii na świecie. Dane Swiss Re Institute wskazują, że ponad 1/3 przerw w dostawach energii elektrycznej w Stanach Zjednoczonych w latach 2012–2023 była związana z ekstremalnymi zjawiskami pogodowymi. Huragany, burze lodowe, fale upałów, długotrwałe susze oraz pożary lasów prowadzą do uszkodzeń linii przesyłowych i dystrybucyjnych, stacji transformatorowych oraz jednostek wytwórczych, a intensyfikacja tych zjawisk pozostaje w silnym związku ze

zmianami klimatu. Do najbardziej dotkliwych przykładów należy burza śnieżna Uri w Teksasie w lutym 2021 r., która doprowadziła do utraty niemal połowy dostępnych mocy wytwórczych stanu, pozostawiając ponad 4,5 mln gospodarstw domowych bez prądu i generując ogromne straty ekonomiczne. Systemowi elektroenergetycznemu Teksasu, zarządzanemu przez ERCOT, zabrakło zaledwie 4 minut i 37 sekund do całkowitego kolapsu, którego skutki usuwano by tygodniami. Analogiczne zdarzenia miały miejsce w innych stanach oraz częściach świata – na przykład huragan Ian w 2022 r. pozbawił energii elektrycznej 2,6 mln mieszkańców Florydy, natomiast huragan Ida w 2021 r. spowodował wielodniowe przerwy w dostawach energii dla około miliona odbiorców w Luizjanie. W Europie silne wiatry w października 2018 r. doprowadziły do rozległych uszkodzeń infrastruktury przesyłowej we Włoszech, powodując serię poważnych awarii i ubytek mocy rzędu 5 tys. MW.

Drugą istotną kategorię stanowią zagrożenia cybernetyczne, których znaczenie dynamicznie rośnie wraz z postępującą cyfryzacją i automatyzacją systemów energetycznych. Raport *Thales Data Threat Report* z 2024 r. wskazuje, że 93% organizacji zarządzających infrastrukturą krytyczną odnotowało wzrost liczby cyberataków, a 42% doświadczyło incydentów naruszenia bezpieczeństwa danych. Pierwszym udokumentowanym cyberatakiem bezpośrednio wpływającym na dostępność systemu elektroenergetycznego był atak na zachodnią Ukrainę w grudniu 2015 r., w ramach którego napastnicy przejęli kontrolę nad systemami sterowania i ręcznie wyłączyli 30 podstacji, pozbawiając zasilania około 225 tys. odbiorców. Incydent z rurociągiem Colonial Pipeline w 2021 r. unaocznił, w jaki sposób cyberataki mogą przekładać się na realne zakłócenia infrastruktury fizycznej i funkcjonowania gospodarki – wstrzymanie operacji na okres tygodnia wynikało nie tylko z samego ataku, lecz z niemożności szybkiego oszacowania jego zakresu i skutków. Systemy energetyczne wykazują szczególną podatność na zagrożenia cybernetyczne ze względu na rosnącą integrację technologii operacyjnych z systemami informatycznymi, wykorzystywanie przestarzałych systemów ICS i SCADA projektowanych w czasach, gdy bezpieczeństwo cybernetyczne nie stanowiło priorytetu, a także szybkie rozpowszechnianie urządzeń internetu rzeczy i inteligentnych liczników, które znacząco rozszerzają powierzchnię

potencjalnego ataku. Międzynarodowa Agencja Energetyczna podkreśla, że pełna eliminacja ryzyka cyberataków nie jest możliwa, jednak systemy mogą być projektowane w taki sposób, aby charakteryzowały się podwyższoną zdolnością do przetrwania, adaptacji oraz szybkiego odzyskiwania sprawności operacyjnej po incydentach, przy jednoczesnym utrzymaniu krytycznych funkcji.

Trzecią grupę zagrożeń tworzą czynniki geopolityczne oraz zakłócenia w łańcuchach dostaw, których znaczenie uległo gwałtownemu wzrostowi po agresji Rosji na Ukrainę w 2022 r. Badania opublikowane w 2025 r. wskazują, że ryzyko geopolityczne systematycznie hamuje tempo transformacji energetycznej poprzez nasilenie zmienności cen surowców, destabilizację łańcuchów dostaw oraz przesuwanie priorytetów politycznych państw. Uzależnienie od importu paliw kopalnych, a coraz częściej również krytycznych minerałów i komponentów niezbędnych do produkcji technologii odnawialnych, zwiększa podatność państw na szoki zewnętrzne pozostające poza ich bezpośrednią kontrolą. Ilustratywnym przykładem był kryzys energetyczny w północnym Meksyku w lutym 2021 r., kiedy ekstremalne warunki pogodowe w Teksasie doprowadziły do wstrzymania eksportu gazu ziemnego, powodując niedobory paliwa w elektrowniach gazowych i wymuszając rotacyjne wyłączenia w 26 stanach Meksyku.

W odpowiedzi na zidentyfikowane zagrożenia rozwinięto szerokie spektrum strategii wzmacniania odporności energetycznej, obejmujących zarówno rozwiązania techniczne, jak i instrumenty instytucjonalno-regulacyjne. Jednym z kluczowych kierunków jest decentralizacja wytwarzania energii poprzez rozwój rozproszonych zasobów energetycznych, obejmujących instalacje fotowoltaiczne, małe turbiny wiatrowe, magazyny energii oraz układy kogeneracyjne. Zasoby te mogą zabezpieczać ciągłość dostaw energii dla odbiorców lokalnych nawet w warunkach awarii sieci przesyłowej, co określane jest mianem „pracy wyspowej". Szczególną rolę odgrywają mikrosieci, rozumiane jako lokalne, sterowalne systemy energetyczne zdolne do pracy zarówno w trybie synchronicznym z siecią krajową, jak i autonomicznym. Mikrosieci znacząco zwiększają odporność systemu elektroenergetycznego poprzez umożliwienie nieprzerwanego zasilania obiektów krytycznych – szpitali, instalacji wojskowych, centrów przetwarzania danych oraz kluczowych węzłów telekomunikacyjnych

– w sytuacjach awarii infrastruktury nadrzędnej. Przykładowo projekty wdrażane w Portoryko po zniszczeniach spowodowanych huraganem Maria w 2017 r. wykazały, że mikrosieci oparte na odnawialnych źródłach energii i magazynach bateryjnych są w stanie podtrzymywać funkcjonowanie odizolowanych społeczności nawet w warunkach długotrwałego odłączenia od głównej sieci.

Magazynowanie energii stanowi jeden z fundamentalnych filarów wzmacniania odporności systemów energetycznych. Bateryjne systemy magazynowania energii umożliwiają czasowe i przestrzenne rozdzielenie procesu wytwarzania energii od jej zużycia, co pozwala na dostarczanie energii w miejscu i czasie największego zapotrzebowania. Z punktu widzenia odporności systemowej magazyny energii mogą w bardzo krótkim czasie przechodzić w tryb zasilania obciążeń krytycznych w sytuacji awarii sieci lub nagłego spadku generacji. Czas reakcji liczony w sekundach znacząco przewyższa możliwości klasycznych agregatów dieslowskich oraz turbin gazowych, co zwiększa zdolność systemu do podtrzymania ciągłości zasilania.

Agregacja rozproszonych zasobów magazynowania, rozmieszczonych w obrębie wielu mikrosieci, umożliwia tworzenie tzw. wirtualnych elektrowni (*virtual power plants*, VPP), które pełnią funkcje stabilizujące na poziomie systemowym. Mechanizmy te pozwalają na wygładzanie profilu obciążenia, redukcję pików zapotrzebowania oraz dynamiczne bilansowanie podaży i popytu w czasie rzeczywistym, co ogranicza ryzyko przeciążeń i awarii kaskadowych.

Inteligentne sieci elektroenergetyczne oraz zaawansowane systemy automatyzacji dystrybucji stanowią kolejny kluczowy element zwiększania odporności systemów przesyłowych i dystrybucyjnych. Systemy automatycznej lokalizacji, izolacji i przywracania zasilania (*fault location, isolation and service restoration*, FLISR) umożliwiają skracanie czasu trwania przerw poprzez automatyczne wykrywanie uszkodzeń, separację uszkodzonych odcinków oraz rekonfigurację topologii sieci w celu zasilania obszarów nieobjętych awarią. Cyfryzacja sieci, mimo wprowadzania nowych wektorów ryzyka w obszarze cyberbezpieczeństwa, umożliwia bardziej precyzyjny monitoring stanu infrastruktury, rozwój utrzymania predykcyjnego oraz szybsze i bardziej skoordynowane reagowanie na zdarzenia zakłócające.

Integracja infrastruktury energetycznej z rozwiązaniami z zakresu zarządzania wodami opadowymi i adaptacji do zmian klimatu znajduje odzwierciedlenie w koncepcjach urbanistycznych opartych na zwiększaniu zdolności retencyjnych obszarów zurbanizowanych. Systemy tego typu wzmacniają odporność miast na powodzie i ekstremalne opady, a pośrednio ograniczają ryzyko uszkodzeń infrastruktury energetycznej zlokalizowanej w obszarach zalewowych.

Pomiar i ocena odporności energetycznej pozostają istotnym wyzwaniem metodologicznym, ponieważ odporność odnosi się do zdarzeń rzadkich, niepewnych i trudnych do jednoznacznej kwantyfikacji. Klasyczne wskaźniki niezawodności systemów elektroenergetycznych obejmują SAIDI (System Average Interruption Duration Index), który jest wskaźnikiem przeciętnego systemowego czasu trwania przerwy długiej w dostawach energii elektrycznej, wyznaczony w minutach na odbiorcę, SAIFI (System Average Interruption Frequency Index) – wskaźnik przeciętnej systemowej częstości przerw długich w dostawie energii, oraz CAIDI (Customer Average Interruption Duration Index), odnoszący się do średniego czasu przywracania zasilania po przerwie, w przypadku wystąpienia awarii. Wskaźniki te są powszechnie stosowane w praktyce regulacyjnej i operacyjnej, jednak w ograniczonym zakresie odzwierciedlają zachowanie systemów w warunkach zdarzeń ekstremalnych.

W celu lepszego uchwycenia odporności na zdarzenia o dużej skali coraz częściej stosuje się podejścia uwzględniające odrębne raportowanie danych z dni o charakterze nadzwyczajnym (Major Event Days, MED), w których poziom zakłóceń przekracza przyjęte progi. Rozwijane są również wskaźniki uzupełniające, takie jak liczba odbiorców doświadczających wielokrotnych przerw (Customers Experiencing Multiple Interruptions, CEMI) oraz liczba odbiorców dotkniętych długotrwałymi przerwami (Customers Experiencing Long Interruption Duration, CELID), a także miary czasu i kosztu odbudowy systemu po zdarzeniach ekstremalnych. Jednocześnie należy podkreślić, że nakłady na zwiększanie odporności klimatycznej i cybernetycznej trudno poddają się klasycznej analizie kosztów i korzyści, gdyż ich efektywność przejawia się przede wszystkim w postaci zdarzeń, które nie wystąpiły, a których skali nie można bezpośrednio obserwować.

Ramy regulacyjne i polityczne w obszarze odporności energetycznej podlegają dynamicznej ewolucji na poziomie krajowym i ponadnarodowym. W obrębie Unii Europejskiej wprowadzono wymogi dotyczące cyberbezpieczeństwa operatorów usług kluczowych oraz obowiązki wdrażania systemów zarządzania ryzykiem i raportowania incydentów. Wymogi te zostały wprowadzone przede wszystkim przez dyrektywę NIS (2016/1148/UE), a obecnie są zaostrzane przez nową – NIS 2. Energetyka jest jednym z kluczowych sektorów objętych tymi przepisami. Ustanowiono również obowiązek uwzględniania zagrożeń o charakterze celowym w podstawowych ocenach ryzyka oraz ramy współpracy między państwami członkowskimi na rzecz ochrony infrastruktury krytycznej. Podmioty z sektora energetycznego mają obowiązek wdrażania środków zarządzania ryzykiem (zarówno technicznym, jak i organizacyjnym) oraz terminowego zgłaszania poważnych incydentów właściwym organom krajowym. Dyrektywa NIS 2 dodatkowo zaostrza te wymogi dotyczące zarządzania ryzykiem i skraca ramy czasowe na zgłaszanie incydentów. Ramy współpracy są realizowane m.in. poprzez dyrektywę o odporności podmiotów krytycznych (CER), która zastąpiła wcześniejsze regulacje. Obejmuje ona obowiązek uwzględniania zagrożeń o charakterze celowym (np. ataki terrorystyczne, sabotaż, zagrożenia hybrydowe) w podstawowych ocenach ryzyka oraz ustanawia mechanizmy współpracy między państwami członkowskimi w zakresie ochrony infrastruktury krytycznej o znaczeniu transgranicznym. W Stanach Zjednoczonych funkcjonują programy ukierunkowane na wzmacnianie zdolności sektora energetycznego w zakresie wymiany informacji o zagrożeniach, podnoszenia poziomu cyberbezpieczeństwa organizacji oraz koordynacji działań reagowania kryzysowego: rząd USA (przede wszystkim Departament Energii – DoE, oraz Agencja ds. Cyberbezpieczeństwa i Infrastruktury – CISA) prowadzi aktywne programy wspierające odporność sektora energetycznego, co potwierdza ostatnie wzmożone działania w tym obszarze. Działania te koncentrują się na wymianie informacji o zagrożeniach poprzez funkcjonowanie mechanizmów i centrów wymiany danych, które ułatwiają sektorowi energetycznemu (zarówno prywatnym, jak i publicznym podmiotom) szybkie otrzymywanie i udostępnianie informacji o aktualnych zagrożeniach i podatnościach; podnoszeniu cyberbezpieczeństwa: realizowane

są programy wspierające operatorów w zakresie wzmacniania systemów sterowania przemysłowego (ICS/OT), w tym audyty, wsparcie techniczne i fundusze; koordynacji reagowania kryzysowego: rząd federalny pracuje nad aktualizacją planów reagowania na incydenty oraz ustanawia wspólne grupy zadaniowe z sektorem prywatnym w celu koordynacji działań w przypadku poważnych zakłóceń w dostawach energii.

Strategiczne rezerwy paliw stanowią klasyczny instrument wzmacniania odporności na poziomie państwowym. Utrzymywanie zapasów surowców energetycznych pozwala na amortyzowanie skutków krótkoterminowych zakłóceń podaży i stabilizację rynków wewnętrznych. W ostatnich latach zwiększeniu uległy również wymagania dotyczące minimalnego poziomu zapełnienia magazynów gazu ziemnego przed sezonami o podwyższonym zapotrzebowaniu. Jednocześnie transformacja energetyczna prowadzi do zmiany struktury zależności importowych, przesuwając punkt ciężkości z paliw kopalnych na surowce krytyczne i komponenty technologiczne wykorzystywane w systemach odnawialnych źródeł energii.

Odporność energetyczna budynków stanowi wyodrębniony obszar analizy, odnoszący się do zdolności obiektów do utrzymania podstawowych funkcji użytkowych w warunkach długotrwałych przerw w dostawach energii. Obejmuje ona zarówno pasywne cechy konstrukcyjne, takie jak wysoka izolacyjność przegród, akumulacyjność cieplna oraz odpowiednia orientacja względem nasłonecznienia, jak i aktywne systemy wytwórcze i magazynujące, w tym instalacje fotowoltaiczne, pompy ciepła oraz lokalne magazyny energii. Szczególne znaczenie przypisuje się elastyczności energetycznej budynków, rozumianej jako zdolność do przesuwania zużycia energii w czasie w odpowiedzi na warunki systemowe.

Koszty nieodporności systemów energetycznych mają wymiar makroekonomiczny i społeczny, a ich skala rośnie wraz z intensyfikacją zjawisk ekstremalnych oraz postępującą elektryfikacją gospodarek. Straty ekonomiczne związane z katastrofami naturalnymi osiągają wartości liczone w setkach miliardów jednostek walutowych rocznie, przy czym znaczna ich część wiąże się bezpośrednio lub pośrednio z infrastrukturą energetyczną. Analizy efektywności ekonomicznej wskazują na wysoką stopę zwrotu z inwestycji ukierunkowanych na działania prewencyjne

i adaptacyjne. Jednocześnie tempo modernizacji sieci elektroenergetycznych pozostaje niewystarczające w stosunku do potrzeb wynikających z transformacji energetycznej i wzrostu zapotrzebowania na energię.

W perspektywie długookresowej odporność energetyczna staje się zagadnieniem o rosnącej złożoności. Elektryfikacja transportu, ogrzewania oraz procesów przemysłowych zwiększa systemową wagę niezakłóconych dostaw energii elektrycznej, czyniąc awarie sieci potencjalnie krytycznymi dla funkcjonowania całych gospodarek. Rosnący udział zmiennych źródeł energii odnawialnej wymusza rozwój nowych mechanizmów bilansowania i stabilizacji systemu. Postępująca decentralizacja wytwarzania z kolei komplikuje zarządzanie siecią, równocześnie tworząc nowe możliwości zwiększania odporności dzięki redundancji i modularności.

Wydarzenia polegające na rozległych awariach systemów elektroenergetycznych unaoczniły praktyczne znaczenie odporności systemowej oraz potrzebę przyspieszonej modernizacji infrastruktury. Zdarzenia tego typu stanowią impuls do intensyfikacji inwestycji w inteligentne sieci, magazyny energii i mechanizmy koordynacji transgranicznej, a także pogłębionych badań nad architekturą przyszłych systemów elektroenergetycznych.

Podsumowując, odporność energetyczna stanowi kompleksową właściwość systemów energetycznych obejmującą zdolność do przewidywania zagrożeń, absorbowania ich skutków, adaptacji strukturalnej oraz szybkiego przywracania funkcjonalności. W realiach transformacji energetycznej i eskalacji różnego rodzaju zagrożeń klimatycznych odporność przestaje być wyłącznie parametrem technicznym, a staje się kategorią strategiczną, determinującą bezpieczeństwo państw, stabilność gospodarczą i dobrostan społeczny.

Aleksander Wasiuta

F. Amini, S. Ghassemzadeh, N. Rostami, V.S. Tabar, *Electrical energy systems resilience: A comprehensive review on definitions, challenges, enhancements and future proceedings*, „IET Renewable Power Generation" 2023, vol. 17, https://doi.org/10.1049/rpg2.12705; *Assessing Energy System Resilience in the UK to 2050*, NPC, London 2025, https://nationalpreparednesscommission.uk/publications/assessing-energy-system-resilience-in-the-uk-to-2050/ (dostęp 12.12.2025); M. Bruneau, S.E. Chang, R.T. Eguchi, G.C. Lee, T.D. O'Rourke, A.M. Reinhorn, *A Framework to*

Quantitatively Assess and Enhance the Seismic Resilience of Communities, „Earthquake Spectra" 2003, vol. 19, https://doi.org/10.1193/1.1623497; L. Carlson, G. Basset, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Philips, D. Verner, R. Whitfield, *Resilience: Theory and Applications, Argonne National Laboratory, Decision and Information Sciences Division*, ANL/DIS-12-1, Argonne 2012; *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, DOE, Washington 2017, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf (dostęp 21.11.2025); Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union…, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (dostęp 25.11.2025); *Electricity Grids and Secure Energy Transitions*, International Energy Agency, Paris 2023, https://www.iea.org/reports/electricity-grids-and-secure-energy-transitions (dostęp 25.11.2025); *Enhancing Cyber Resilience in Electricity Systems*, International Energy Agency, Paris 2021, https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (dostęp 23.11.2025); P. Gasser, P. Lustenberger, M. Cinelli, W. Kim, M. Spada, P. Burgherr, T.Y. Sun, *A review on resilience assessment of energy systems*, „Sustainable and Resilient Infrastructure" 2021, vol. 6, no. 5, https://doi.org/10.1080/23789689.2019.1610600; C.S. Holling, *Resilience and Stability of Ecological Systems*, „Annual Review of Ecology, Evolution, and Systematics" 1973, vol. 4, http://dx.doi.org/10.1146/annurev.es.04.110173.000245 (dostęp 25.11.2025); L. Hughes, *The effects of event occurrence and duration on resilience and adaptation in energy systems*, „Energy" 2015, vol. 84, https://doi.org/10.1016/j.energy.2015.03.010; IEEE 1366:2022, *IEEE Guide for Electric Power Distribution Reliability Indices*, https://www.bsbedge.com/standard/ieee-guide-for-electric-power-distribution-reliability-indices/IEEE1366 (dostęp 25.11.2025); G. Kostenko, A. Zaporozhets, *Enhancing the Power System Resilience Through the Application of Micro Power Systems (microgrid) with Renewable Distributed Generation*, „System Research in Energy" 2023, no. 3(74), https://doi.org/10.15407/srenergy2023.03.025; Y. Lin, Z. Bie, A. Qiu, *A review of key strategies in realizing power system resilience*, „Global Energy Interconnection" 2018, vol. 1, no. 1, https://doi.org/10.14171/j.2096-5117.gei.2018.01.009; T. McPhearson, E.M. Cook, M. Berbés-Blázquez, *A social-ecological-technological systems framework for urban ecosystem services*, „One Earth" 2022, vol. 5, no. 5, https://doi.org/10.1016/j.oneear.2022.04.007; S. Meerow, J.P. Newell, M. Stults, *Defining urban resilience: A review*, „Landscape and Urban Planning" 2016, vol. 147, https://doi.org/10.1016/j.landurbplan.2015.11.011; M. Ouyang, L. Dueñas-Osorio, *Multi-dimensional hurricane resilience assessment of electric power systems*, „Structural Safety" 2014, vol. 48, https://doi.org/10.1016/j.strusafe.2014.01.001; P.E. Roege, Z.A. Collier, J.

Mancillas, J.A. McDonagh, I. Linkov, *Metrics for energy resilience*, „Energy Policy" 2014, vol. 72, https://doi.org/10.1016/j.enpol.2014.04.012 (dostęp 23.11.2025); *Panarchy: Understanding Transformations in Human and Natural Systems*, L.H. Gunderson, C.S. Holling (eds.), Island Press, Washington, DC 2002; *Power Systems in Transition*, International Energy Agency, Paris 2024, https://www.iea.org/reports/power-systems-in-transition (dostęp 23.11.2025); M. Scheffer, S. Carpenter, J.A. Foley, C. Folke, B. Walker, *Catastrophic shifts in ecosystems*, „Nature" 2001, vol. 413, no. 6856, 10.1038/35098000; *State Energy Resilience Framework*, Argonne National Laboratory, ANL/GSS-16/4, Argonne 2016, https://publications.anl.gov/anlpubs/2017/02/133591.pdf (dostęp 25.11.2025); *Thales, 2024 Data Threat Report*, Thales Group, Paris 2024, https://cpl.thalesgroup.com/2024/data-threat-report (dostęp 12.12.2025).

ODPORNOŚĆ FINANSOWA (ang. *financial resilience*) stanowi jedno z fundamentalnych pojęć współczesnej ekonomii oraz nauk o zarządzaniu definiujących zdolność podmiotów gospodarczych – zarówno gospodarstw domowych, jak i przedsiębiorstw oraz instytucji finansowych – do antycypowania szoków ekonomicznych, absorpcji ich skutków, szybkiego przywracania równowagi finansowej oraz adaptowania się do zmieniających się warunków otoczenia przy jednoczesnym zachowaniu podstawowych funkcji ekonomicznych i społecznych. Koncepcja ta, intensywnie rozwijana od czasu globalnego kryzysu finansowego lat 2007–2009, a następnie pandemii COVID-19, zyskała szczególne znaczenie w kontekście rosnącej zmienności rynków finansowych, narastających zagrożeń geopolitycznych oraz postępującej cyfryzacji usług finansowych, które w sposób istotny przekształcają tradycyjne wzorce zarządzania finansami osobistymi i korporacyjnymi.

W odróżnieniu od pojęcia stabilności finansowej, które koncentruje się na stanie równowagi systemu w danym momencie, odporność finansowa obejmuje znacznie szerszy zakres zagadnień, w tym zdolność do absorpcji nieoczekiwanych zaburzeń, mechanizmy adaptacji do nowych warunków oraz procesy odbudowy po wystąpieniu szoków. Odporność i podatność finansowa to 2 strony tej samej monety – budowanie odporności rozpoczyna się od zrozumienia podatności wynikających z ekspozycji na ryzyko oraz braku dostępu do odpowiednich zasobów i instrumentów ochronnych, więc jest to zdolność jednostek lub gospodarstw domowych

do stawiania oporu, radzenia sobie oraz powrotu do równowagi po negatywnych zdarzeniach finansowych, przy wykorzystaniu dostępnych zasobów i sieci wsparcia.

Geneza współczesnego rozumienia odporności finansowej sięga badań nad odpornością systemów ekologicznych i społecznych, które następnie zostały zaadaptowane do analizy zachowań ekonomicznych jednostek i organizacji. Przełomowe znaczenie miało pojęcia kruchości finansowej (*financial fragility*) jako niezdolności do zgromadzenia środków na pokrycie nieoczekiwanych wydatków w rozsądnym czasie. W kolejnych latach koncepcja ta została rozszerzona analizą determinant odporności finansowej w kontekście inkluzji finansowej i alfabetyzacji cyfrowej.

W literaturze naukowej funkcjonuje wiele definicji i ram koncepcyjnych odporności finansowej, różniących się poziomem analizy i zakresem przedmiotowym. Na poziomie gospodarstw domowych Organizacja Współpracy Gospodarczej i Rozwoju (OECD) w ramach Międzynarodowej Sieci Edukacji Finansowej (INFE) wyróżnia 5 komponentów odporności finansowej: kontrolę nad pieniędzmi, dbałość o wydatki, posiadanie poduszki finansowej, radzenie sobie z niedoborami lub stresem finansowym oraz planowanie finansowe. Na poziomie instytucji finansowych odporność definiowana jest poprzez zdolność do absorpcji strat przy zachowaniu wypłacalności i płynności, co znajduje odzwierciedlenie w wymogach regulacyjnych określonych przez Bazylejski Komitet Nadzoru Bankowego. Z kolei na poziomie makroekonomicznym odporność systemu finansowego oznacza zdolność do wytrzymywania szoków bez generowania efektów kaskadowych zagrażających stabilności całej gospodarki.

Współczesna literatura wyróżnia kilka kluczowych wymiarów odporności finansowej w zależności od przyjętej perspektywy analitycznej oraz poziomu agregacji. Pierwszym jest odporność strukturalna obejmująca zasoby materialne i finansowe podmiotu, takie jak oszczędności, aktywa płynne, dostęp do kredytu i ubezpieczeń oraz dywersyfikacja źródeł dochodu.

Drugi wymiar to odporność behawioralna odnosząca się do zachowań i praktyk finansowych jednostek, w tym planowania budżetu, systematycznego oszczędzania, zarządzania długiem oraz podejmowania świadomych decyzji finansowych. Badania OECD/INFE *International*

Survey of Adult Financial Literacy z 2023 r. wskazują, że zaledwie 54% dorosłych w badanych krajach deklarowało zdolność do pokrycia większego wydatku odpowiadającego jednomiesięcznemu dochodowi bez zaciągania pożyczek lub zwracania się o pomoc do rodziny i znajomych. Co istotne, jedynie 43% respondentów było w stanie pokryć wydatki na życie przez co najmniej 3 miesiące w przypadku utraty głównego źródła dochodu, co wskazuje na istotne deficyty w zakresie tworzenia rezerw finansowych.

Trzecim wymiarem jest odporność poznawcza obejmująca wiedzę finansową oraz kompetencje cyfrowe niezbędne do efektywnego funkcjonowania we współczesnym systemie finansowym. Zgodnie z definicją OECD alfabetyzacja finansowa stanowi kombinację świadomości finansowej, wiedzy, umiejętności, postaw i zachowań niezbędnych do podejmowania racjonalnych decyzji finansowych. Badania prowadzone na danych z *China Household Finance Survey* wykazały, że alfabetyzacja finansowa istotnie zwiększa odporność gospodarstw domowych poprzez zwiększenie bogactwa (wyższe dochody z majątku i działalności gospodarczej) oraz efekt mitygacji ryzyka (szersze pokrycie ubezpieczeniowe i wyższe oszczędności).

Czwartym wymiarem jest odporność relacyjna odnosząca się do kapitału społecznego i sieci wsparcia, na które jednostka może liczyć w sytuacji kryzysu finansowego. Do kluczowych komponentów odporności finansowej należą nie tylko zasoby ekonomiczne i wiedza finansowa, lecz również kapitał społeczny umożliwiający mobilizację pomocy ze strony rodziny, przyjaciół i społeczności lokalnej. Strategie wzmacniania odporności obejmują m.in. dywersyfikację dochodów, oszczędzanie, zaciąganie pożyczek, redukcję wydatków oraz wykorzystywanie sieci społecznych.

Na poziomie przedsiębiorstw, w szczególności małych i średnich (MŚP), odporność finansowa definiowana jest jako zdolność firmy do przetrwania okresów trudności finansowych i uniknięcia niewypłacalności. Pandemia COVID-19 istotnie zwiększyła ryzyko niewypłacalności wśród MŚP w krajach europejskich. Udział przedsiębiorstw z ujemnym kapitałem własnym – jednej z definicji niewypłacalności – wzrósł średnio o 21% w tym okresie. Jednocześnie przedsiębiorstwa innowacyjne okazały się bardziej odporne, utrzymując lepszy dostęp do finansowania bankowego.

W kontekście przedsiębiorstw kluczowe determinanty odporności finansowej obejmują strukturę finansowania, wskaźniki płynności i rentowności, poziom zadłużenia oraz zdolność do generowania przepływów pieniężnych. Jak wynika z badań z 2021 r. na próbie hiszpańskich MŚP w postępowaniach upadłościowych, jedynie redukcja zadłużenia była istotnie powiązana z przetrwaniem firmy, podczas gdy redukcja zapasów i zatrudnienia zwiększała prawdopodobieństwo likwidacji. Wyniki te podważają konwencjonalne podejście dotyczące strategii restrukturyzacyjnych i sugerują, że menedżerowie niewypłacalnych firm powinni koncentrować się na poprawie płynności i efektywności operacyjnej prowadzących do redukcji długu, a nie automatycznej, przekrojowej redukcji kosztów.

Na poziomie instytucji finansowych i systemu bankowego odporność definiowana jest przede wszystkim poprzez zdolność do absorpcji strat przy zachowaniu stabilności kapitałowej i płynności. Ramy regulacyjne Bazylea III, opracowane przez Bazylejski Komitet Nadzoru Bankowego w odpowiedzi na globalny kryzys finansowy lat 2007–2009, ustanowiły globalne standardy regulacyjne mające na celu wzmocnienie odporności banków i systemu bankowego jako całości. Zgodnie z dokumentem programowym z 2010 r. ramy te obejmują wyższe wymogi kapitałowe, większe pokrycie ryzyka, wprowadzenie wskaźnika dźwigni jako zabezpieczenia dla wymogów opartych na ryzyku, środki promujące budowanie buforów kapitałowych oraz globalne standardy płynności.

Kluczowym elementem regulacji jest test warunków skrajnych (*stress testing)*, stanowiący podejście oceniające wpływ poważnych, groźnych, lecz prawdopodobnych scenariuszy mogących wpłynąć na odporność instytucji finansowych. Testy te wykorzystują modele i dane na poziomie pojedynczej instytucji lub całego systemu i mogą opierać się na scenariuszach historycznych lub hipotetycznych. Celem testów warunków skrajnych jest ocena, czy bank posiada wystarczający kapitał, by wytrzymać dany szok lub jak poważny musi być szok, aby wyczerpać kapitał banku. Przykładowo Federalna Rezerwa Stanów Zjednoczonych prowadzi coroczne testy warunków skrajnych, których celem jest zapewnienie, że duże instytucje finansowe dysponują solidnymi procesami planowania kapitałowego.

System regulacji bazylejskich wprowadza zarówno wymogi mikro-, dotyczące kondycji i stabilności pojedynczych instytucji finansowych, jak

i makroostrożnościowe, odnoszące się do stabilności systemu finansowego jako całości. Nadzór mikroostrożnościowy koncentruje się na odpowiednim poziomie kapitału, zarządzaniu płynnością, kontroli ryzyka oraz strukturach ładu korporacyjnego, mając na celu ochronę deponentów, inwestorów i innych interesariuszy przed stratami wynikającymi z nieodpowiedzialnych praktyk lub nadmiernego podejmowania ryzyka; z kolei makroostrożnościowy uwzględnia współzależności między instytucjami finansowymi, wspólne ekspozycje oraz wzmacnianie ryzyka przez procykliczne zachowania, wykorzystując takie narzędzia, jak antycykliczny bufor kapitałowy oraz sektorowe wymogi kapitałowe, w celu ograniczania narastania ryzyka systemowego.

W kontekście odporności systemowej szczególne znaczenie mają banki o znaczeniu systemowym G-SIBs (Global Systemically Important Banks) i D-SIBs (Domestic Systemically Important Banks), które podlegają dodatkowym wymogom kapitałowym ze względu na ryzyko, jakie ich ewentualna niewypłacalność stanowiłaby dla całego systemu finansowego. Zgodnie z ramami Bazylea III globalnie systemowo ważne banki zobowiązane są do utrzymywania dodatkowego bufora kapitałowego w wysokości od 1% do 3,5% aktywów ważonych ryzykiem, w zależności od oceny ich znaczenia systemowego. Jak wskazuje analiza Bazylejskiego Komitetu Nadzoru Bankowego, oceniająca wpływ reform bazylejskich, wymogi te przyczyniły się do istotnego wzrostu wskaźników kapitałowych banków oraz poprawy rynkowych miar odporności instytucji finansowych.

Pandemia COVID-19 stanowiła bezprecedensowy test odporności finansowej na wszystkich poziomach – od gospodarstw domowych, przez przedsiębiorstwa, po system finansowy jako całość, i wywołała największy globalny kryzys gospodarczy od ponad 100 lat, prowadząc do dramatycznego wzrostu nierówności wewnątrz krajów i między nimi. Skutki gospodarcze były szczególnie dotkliwe w gospodarkach wschodzących, gdzie straty dochodowe ujawniły i pogłębiły wcześniejsze słabości strukturalne. Jednocześnie ogromna reakcja polityczna – obejmująca środki fiskalne, monetarne i regulacyjne – okazała się zasadniczo skuteczna w łagodzeniu najpoważniejszych krótkoterminowych konsekwencji kryzysu dla ludności, choć jednocześnie wygenerowała nowe ryzyka w postaci gwałtownego wzrostu poziomów zadłużenia prywatnego i publicznego.

Przykładowo w Stanach Zjednoczonych odpowiedź na kryzys pandemiczny obejmowała 5 ustaw pomocowych uchwalonych w 2020 r. oraz *American Rescue Plan* z 2021 r., co przyczyniło się do uczynienia recesji COVID-19 najkrótszą w nowożytnej historii Stanów Zjednoczonych i wywołania dynamicznego ożywienia gospodarczego, które obniżyło stopę bezrobocia z rekordowego poziomu 14,8% w kwietniu 2020 r. do poniżej 3,9% już w styczniu 2022 r. Tymczasowe zmiany w polityce społecznej – obejmujące rozszerzenie ulgi podatkowej na dzieci, zwiększenie zasiłków dla bezrobotnych oraz programów pomocy żywnościowej, mieszkaniowej i zdrowotnej – istotnie ograniczyły ubóstwo, brak ubezpieczenia zdrowotnego oraz trudności materialne milionów Amerykanów.

W wymiarze makroekonomicznym odporność finansowa gospodarstw domowych przekłada się bezpośrednio na stabilność całej gospodarki. Gdy gospodarstwa domowe są w stanie absorbować szoki dochodowe i płynnościowe, ich zbiorcza zdolność do utrzymania konsumpcji i obsługi zobowiązań finansowych może decydować o różnicy między głęboką recesją a jedynie przejściowym spowolnieniem gospodarczym. Pandemia COVID-19 dostarcza empirycznych dowodów na istnienie tej zależności – w porównaniu z innymi dużymi gospodarkami ożywienie gospodarcze Stanów Zjednoczonych po początkowej recesji było relatywnie silne, co można przypisać przede wszystkim utrzymaniu poziomu wydatków konsumpcyjnych i inwestycji, wspieranych przez ekspansywną politykę fiskalną obejmującą płatności stymulacyjne, podwyższone zasiłki dla bezrobotnych oraz moratoria na spłatę zobowiązań.

Budowanie odporności finansowej gospodarstw domowych wymaga zintegrowanego podejścia łączącego edukację finansową z inkluzją finansową, a planowanie i oszczędzanie stanowią niezbędne elementy tworzenia buforów zarówno na wypadek nagłych potrzeb, jak i w perspektywie długoterminowej. Typowe przykłady edukacji finansowej ukierunkowanej na promowanie oszczędzania obejmują spersonalizowane komunikaty i przypomnienia dotyczące odkładania środków na konkretne cele, internetowe kalkulatory dochodów emerytalnych ułatwiające złożone obliczenia związane z długookresowymi decyzjami oszczędnościowymi, a także kursy oraz interaktywne aplikacje edukacyjne.

Inkluzja finansowa stanowi warunek sprzyjający budowaniu odporności finansowej, gdyż umożliwia jednostkom bezpieczne gromadzenie i zarządzanie zasobami finansowymi w ramach regulowanych instytucji, zamiast korzystania z nieformalnych i nieregulowanych kanałów. Zarówno alfabetyzacja finansowa, jak i cyfrowa są istotnie powiązane z odpornością finansową gospodarstw domowych, co podkreśla potrzebę redefinicji tradycyjnej koncepcji alfabetyzacji finansowej w kierunku jej rozszerzenia o kompetencje cyfrowe, co ma istotne implikacje dla krajów rozważających oba podejścia jako zintegrowaną strategię poprawy długoterminowej odporności finansowej gospodarstw domowych.

Pomiar odporności finansowej pozostaje istotnym wyzwaniem metodologicznym ze względu na wielowymiarowy charakter oraz zróżnicowanie sposobów przeprowadzenia badań empirycznych. Literatura przedmiotu wyróżnia 2 główne podejścia do pomiaru odporności finansowej gospodarstw domowych. Pierwsze opiera się na wskaźnikach jakościowych, odzwierciedlających subiektywne oceny zdolności do pozyskania środków awaryjnych lub postrzeganej intersubiektywnej kontrolowalności poziomu zadłużenia. Drugie wykorzystuje miary obiektywne, bazujące na rzeczywistych wartościach, takich jak poziom oszczędności i zadłużenia. Oba podejścia obarczone są istotnymi ograniczeniami: wskaźniki jakościowe mogą być podatne na błędy percepcyjne i czynniki psychologiczne, natomiast miary obiektywne napotykają problemy endogeniczności w analizach ekonometrycznych ze względu na złożoność mechanizmów kształtujących zmienne wynikowe.

W kontekście instytucji finansowych pomiar odporności opiera się na zestawie wskaźników regulacyjnych obejmujących współczynniki kapitałowe (*Common Equity Tier 1*, *Tier 1 Capital Ratio*, *Total Capital Ratio*), wskaźniki płynności (*Liquidity Coverage Ratio*, *Net Stable Funding Ratio*) oraz wskaźnik dźwigni finansowej. Wyniki testów warunków skrajnych stanowią dodatkowy wymiar oceny odporności, symulujący zachowanie instytucji w hipotetycznych scenariuszach niekorzystnych, celem tych działań jest zapewnienie, że instytucje finansowe dysponują solidnymi procesami planowania kapitałowego, uwzględniającymi ich specyficzne profile ryzyka, oraz wystarczającym buforem kapitałowym

umożliwiającym kontynuację działalności w okresach nasilonego stresu gospodarczego i finansowego.

Ramy regulacyjne dotyczące odporności finansowej ewoluują zarówno na poziomie krajowym, jak i międzynarodowym. W kontekście gospodarstw domowych OECD opracowuje rekomendacje oraz narzędzia pomiarowe w ramach *Recommendation of the Council on Financial Literacy* oraz cyklicznych międzynarodowych badań alfabetyzacji finansowej dorosłych, obejmujących kilkadziesiąt krajów. Na poziomie instytucji finansowych Bazylejski Komitet Nadzoru Bankowego kontynuuje prace nad udoskonalaniem standardów bazylejskich, przy czym reformy tzw. *Basel III Endgame* podlegają stopniowej implementacji. W Unii Europejskiej dyrektywa CRD V oraz rozporządzenie CRR II transponują standardy bazylejskie do prawa wspólnotowego, uzupełniane przez ramy dotyczące restrukturyzacji i uporządkowanej likwidacji banków (BRRD).

Perspektywy przyszłościowe w zakresie odporności finansowej koncentrują się na kilku kluczowych obszarach. Po pierwsze, cyfryzacja usług finansowych stwarza jednocześnie istotne możliwości – poprzez rozszerzenie dostępu do produktów finansowych i narzędzi zarządzania finansami osobistymi – oraz poważne zagrożenia w postaci cyberprzestępczości, oszustw cyfrowych i wykluczenia osób pozbawionych kompetencji cyfrowych. Zgodnie z wynikami *OECD/INFE International Survey of Adult Financial Literacy* z 2023 r. około 60% dorosłych korzystających z produktów i usług finansowych online osiąga minimalny docelowy poziom cyfrowej alfabetyzacji finansowej, co wskazuje na znaczące luki w przygotowaniu populacji do bezpiecznego funkcjonowania w cyfrowym środowisku finansowym.

Po drugie, zmiany klimatyczne oraz transformacja energetyczna generują nowe kategorie ryzyka finansowego, które wymagają systematycznego uwzględniania w ramach oceny odporności. Europejski Bank Centralny oraz inne organy nadzoru prowadzą klimatyczne testy warunków skrajnych, badające ekspozycję instytucji finansowych na ryzyko fizyczne związane z ekstremalnymi zjawiskami pogodowymi i długoterminowymi zmianami klimatu oraz ryzyko transformacji wynikające z przejścia do gospodarki niskoemisyjnej. Po trzecie, rosnąca złożoność globalnego systemu finansowego oraz wzajemne powiązania między

instytucjami wymagają dalszego doskonalenia narzędzi analitycznych zdolnych do wczesnej identyfikacji ryzyka systemowego i potencjalnych efektów zarażania.

Podsumowując, odporność finansowa stanowi wielowymiarową koncepcję obejmującą zdolność podmiotów gospodarczych na różnych poziomach agregacji do antycypowania, absorpcji, adaptacji oraz powrotu do równowagi po negatywnych zdarzeniach i szokach finansowych. Budowanie odporności wymaga spójnego, zintegrowanego podejścia łączącego zasoby materialne i finansowe, kompetencje poznawcze i behawioralne, sieci wsparcia społecznego oraz odpowiednie ramy regulacyjne i instytucjonalne. W warunkach narastającej zmienności i niepewności w globalnym systemie ekonomiczno-finansowym odporność finansowa przestaje być wyłącznie pożądanym atrybutem racjonalnego zarządzania, a staje się strategicznym imperatywem warunkującym stabilność gospodarstw domowych, przetrwanie przedsiębiorstw, bezpieczeństwo systemu finansowego oraz długookresowy, zrównoważony wzrost gospodarczy.

Aleksander Wasiuta

S. Ansar, A. Demirgüç-Kunt, L. Klapper, D. Singer, *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*, World Bank Group, Washington, DC 2021, http://documents.worldbank.org/curated/en/099818107072234182 (dostęp 27.11.2025); *Basel Committee on Banking Supervision, Evaluation of the Impact and Efficacy of the Basel III Reforms*, Bank for International Settlements, Basel 2022, https://www.bis.org/bcbs/publ/d544.htm (dostęp 27.11.2025); *Basel Committee on Banking Supervision, Stress-testing Principles*, Bank for International Settlements, Basel 2018, https://www.bis.org/bcbs/publ/d450.htm (dostęp 30.11.2025); *The Basel framework: the global regulatory standards for banks, European Banking Authority*, https://www.eba.europa.eu/activities/basel-framework-global-regulatory-standards-banks (dostęp 27.11.2025); *Board of Governors of the Federal Reserve System*, 2023 Stress Test Scenarios, Federal Reserve Board, Washington 2023, https://www.federalreserve.gov/publications/2023-Stress-Test-Scenarios.htm (dostęp 7.12.2025); P. Białowolski, D. Węziak-Białowolska, M.T. Lee, Y. Chen, T.J. VanderWeele, E. McNeely, *The role of financial conditions for physical and mental health. Evidence from a longitudinal survey and insurance claims data*, „Social Science &

Medicine" 2021, vol. 281; R.L. Clark, A. Lusardi, O.S. Mitchell, *Financial Fragility During the COVID-19 Pandemic*, „NBER Working Paper" 2020, https://ssrn.com/abstract=3753115 (dostęp 28.11.2025); R.L. Clark, O.S. Mitchell, *Americans' Financial Resilience During the Pandemic*, „Financial Planning Review" 2022, vol. 5, no. 2–3, https://ssrn.com/abstract=4133696 (dostęp 28.11.2025); *G20/OECD-INFE Report on Supporting Financial Resilience and Transformation through Digital Financial Literacy*, OECD Publishing, Paris 2021, https://www.oecd.org/en/publications/g20-oecd-infe-report-on-supporting-financial-resilience-and-transformation-through-digital-financial-literacy_0132c06d-en.html (dostęp 28.11.2025); M.J. Gruenberg, *Basel III Endgame*, FDIC 2023, https://www.fdic.gov/news/speeches/2023/spjun2223.html (dostęp 12.12.2025); A. Hasler, A. Lusardi, N. Oggero, *Financial Fragility in the US: Evidence and Implications*, GFLEC Working Paper, The George Washington University 2018, https://gflec.org/wp-content/uploads/2018/04/Financial-Fragility-Research-Paper-04-16-2018-Final.pdf (dostęp 2.12.2025); J. Kass-Hanna, A.C. Lyons, F. Liu, *Building Financial Resilience through Financial and Digital Literacy in South Asia and Sub-Saharan Africa*, „Emerging Markets Review" 2022, vol. 51; O. Kaya, *Determinants and Consequences of SME Insolvency Risk during the Pandemic*, „Economic Modelling" 2022, vol. 115; A. Lusardi, D.J. Schneider, P. Tufano, *Financially Fragile Households: Evidence and Implications*, „Brookings Papers on Economic Activity" 2011; A. Lusardi, O.S. Mitchell, *The Economic Importance of Financial Literacy: Theory and Evidence*, „Journal of Economic Literature" 2014, vol. 52, no. 1; *OECD/INFE 2023 International Survey of Adult Financial Literacy*, OECD Publishing, Paris 2023, https://www.oecd.org/en/publications/oecd-infe-2023-international-survey-of-adult-financial-literacy_56003a32-en.html (dostęp 28.11.2025); *OECD/INFE Toolkit for Measuring Financial Literacy and Financial Inclusion 2022*, OECD Publishing, Paris 2022, https://www.oecd.org/en/publications/oecd-infe-toolkit-for-measuring-financial-literacy-and-financial-inclusion-2022_cbc4114f-en.html (dostęp 28.11.2025); M. Rico, N.R. Pandit, F. Puig, *SME insolvency, bankruptcy, and survival: an examination of retrenchment strategies*, „Small Business Economics" 2021, vol. 57, no. 1; *The Road to Resilience: Bridging Relief and Development for a More Sustainable Future*, IFRC, Geneva 2012, https://www.ifrc.org/sites/default/files/1224500-Road-to-resilience-EN-LowRes-2.pdf (dostęp 10.12.2025); F. Salignac, A. Marjolin, R. Reeve, *Conceptualizing and Measuring Financial Resilience: A Multidimensional Framework*, „Social Indicators Research" 2019, vol. 145; *Stress Testing – Executive Summary*, Bank for International Settlements, https://www.bis.org/fsi/fsisummaries/

stress_testing.pdf (dostęp 6.12.2025); *World Development Report 2022: Finance for an Equitable Recovery*, World Bank, Washington 2022, https://www.worldbank.org/en/publication/wdr2022 (dostęp 28.11.2025); J.J. Xiao, P. Białowolski, *Consumer financial capability and quality of life: A global perspective*, „Applied Research in Quality of Life" 2023, vol. 18, no. 1, https://doi.org/10.1007/s11482-022-10087-3.

ODSTRASZANIE PRZEZ KARĘ (ang. *deterrence by punishment*) – klasyczny sposób kształtowania bezpieczeństwa opierający się na groźbie zadania agresorowi wysokich kosztów w odpowiedzi na potencjalny atak. Logika tej strategii jest prosta: przeciwnik ma zrezygnować z agresji nie dlatego, że nie będzie w stanie jej przeprowadzić, lecz z tego względu, że skutki odwetu będą dla niego nie do zaakceptowania politycznie, militarnie, gospodarczo czy społecznie.

W modelu odstraszania przez karę można wyróżnić następujące elementy:

- główna logika – grożenie wysokimi kosztami odwetu;
- mechanizm – eskalacja, siły odstraszania, broń strategiczna;
- skutki dla agresora – pewność bolesnego odwetu;
- charakter – psychologiczny, strategiczny;
- przykład – broń nuklearna, sankcje, uderzenia odwetowe.

W XX w. koncepcja ta nierozerwalnie związała się z rozwojem broni jądrowej i polityką odstraszania w warunkach zimnej wojny, ale w rzeczywistości ma szerszy zakres. Odstraszanie przez karę może mieć postać zarówno militarnej odpowiedzi zbrojnej, jak i sankcji gospodarczych, blokad, izolacji dyplomatycznej czy działań prawnych. Wspólnym mianownikiem jest zawsze groźba spowodowania strat na poziomie, który czyni agresję przedsięwzięciem zbyt ryzykownym.

Odstraszanie przez karę można zdefiniować jako strategię zapobiegania agresji poprzez wiarygodne zapowiedzenie, że każde naruszenie określonych „czerwonych linii" spotka się z dotkliwą odpowiedzią. Odwet może być symetryczny (odpowiedź tego samego rodzaju, np. uderzenie zbrojne za uderzenie zbrojne) lub asymetryczny (np. sankcje gospodarcze za działania militarne).

W centrum tej logiki znajdują się 3 elementy:

1. Zdolność do zadania ciosu odwetowego – państwo musi realnie dysponować środkami, które mogą wyrządzić przeciwnikowi duże szkody.
2. Wiarygodność zamiaru użycia tych środków – przeciwnik musi wierzyć, że odwet będzie rzeczywiście zastosowany.
3. Komunikacja – groźba musi być jasno zakomunikowana i zrozumiała, tak by potencjalny agresor znał konsekwencje swoich działań.

Strategia ta silnie opiera się na założeniu racjonalności przeciwnika. Agresor ma zachowywać się jak aktor kalkulujący zyski i straty: jeśli straty przewidywane w wyniku odwetu przewyższają potencjalne korzyści, powinien powstrzymać się od agresji.

Wczesne formy odwetu – idea odstraszania przez karę wyprzedza rozwój nowoczesnej teorii strategicznej. Od starożytności w polityce i prawie pojawia się logika: „Jeżeli mnie zaatakujesz, odpłacę ci w sposób dla ciebie bolesny". Systemy kar zbiorowych, represji wobec agresorów, odwetowe kampanie wojskowe – wszystko to można uznać za historyczne przejawy myślenia odstraszającego.

Zimna wojna i broń jądrowa – nowoczesna doktryna odstraszania przez karę rozwinęła się podczas zimnej wojny. Pojawienie się broni nuklearnej sprawiło, że odwet mógł oznaczać katastrofalne zniszczenia, niewspółmierne do jakichkolwiek konwencjonalnych zdobyczy. Koncepcje takie jak „wzajemnie gwarantowane zniszczenie" (MAD) zakładały, że każda ze stron dysponuje zdolnością do zadania drugiego niszczącego ciosu nawet po pierwszym ataku przeciwnika. W takiej sytuacji wojna nuklearna staje się aktem samobójczym – właśnie to ma odstraszać. W tym okresie rozwijano złożone koncepcje eskalacji, sygnalizowania i „kontrolowania" groźby użycia broni jądrowej, a odstraszanie przez karę stało się centralnym elementem strategii mocarstw. Z czasem zaczęto jednak zastanawiać się także nad zastosowaniem podobnej logiki w sferze konwencjonalnej, ekonomicznej czy politycznej.

Odstraszanie przez karę może przybierać różne postaci i zdecydowanie nie ogranicza się tylko do groźby użycia broni masowego rażenia. W praktyce obejmuje przede wszystkim zapowiedź odwetu militarnego, zastosowanie środków gospodarczych, izolację polityczno-prawną oraz

reakcję w innych domenach niż ta, w której nastąpił atak. Odwet zbrojny jest tu najbardziej oczywistym narzędziem: państwo z góry komunikuje, że agresja spotka się z użyciem sił zbrojnych. W grę wchodzą zarówno klasyczne uderzenia konwencjonalne na cele wojskowe czy newralgiczną infrastrukturę, jak i operacje o mniejszej skali, ale dużym znaczeniu demonstracyjnym, które mają pokazać, że strona atakowana jest gotowa eskalować konflikt. W skrajnych scenariuszach do katalogu możliwych środków włącza się także użycie broni jądrowej. Chodzi nie tylko o zadanie strat materialnych, ale podważenie sensu militarnego i politycznego pierwotnego ataku, tak aby dalsze działania, z punktu widzenia napastnika, traciły logikę.

Kara może mieć również charakter ekonomiczny. Groźba sankcji gospodarczych obejmujących embargo, ograniczenia w handlu, zamrożenie aktywów, odcięcie od technologii czy rynków finansowych stała się jednym z najczęściej stosowanych narzędzi nacisku. Taki przekaz sprowadza się do obietnicy poważnego uszczerbku dla gospodarki państwa, które naruszy określone normy lub podejmie działania uznane za niedopuszczalne. Jest to szczególnie atrakcyjny instrument wobec tych podmiotów, wobec których bezpośrednia konfrontacja militarna byłaby zbyt ryzykowna albo postrzegana jako nieproporcjonalna.

Wymiar polityczno-prawny odstraszania przez karę wiąże się z groźbą utraty pozycji w systemie międzynarodowym. Potępienie na forach organizacji międzynarodowych, wykluczenie z ważnych formatów współpracy, ściganie odpowiedzialnych za zbrodnie w trybie międzynarodowym, zakazy podróży dla przedstawicieli elit czy ograniczanie udziału w instytucjach i procesach decyzyjnych. Wszystkie te działania mogą działać zniechęcająco. Uderzają one nie tylko w samo państwo, ale w osoby, które sprawują władzę i często opierają swoją legitymizację na kontaktach zewnętrznych oraz prestiżu międzynarodowym.

Coraz większą rolę odgrywa także odpowiedź w innych domenach niż ta, w której doszło do pierwotnego naruszenia. W debacie strategicznej mówi się o odstraszaniu krzyżowym, polegającym na tym, że państwo zapowiada reakcję np. na cyberatak poprzez środki finansowe, informacyjne lub ograniczone działania zbrojne. Taki zabieg utrudnia przeciwnikowi

kalkulację opłacalności agresji, ponieważ nie może on z góry przewidzieć, w jakiej sferze poniesie koszty i jak bardzo dotkliwe one będą.

Sama deklaracja gotowości do ukarania agresora nie wystarcza jednak do tego, aby odstraszanie zadziałało; potrzebne są pewne warunki brzegowe. Po pierwsze, liczy się realny potencjał, bo bez zdolności do przeprowadzenia odwetu groźby są pustymi słowami. Dotyczy to zarówno możliwości militarnych, jak i zasobów gospodarczych czy instrumentów politycznych. Potencjalny przeciwnik musi mieć świadomość, że zapowiadane środki są faktycznie dostępne i mogą zostać użyte.

Równie ważna jest wiarygodność zamiaru. Nawet jeśli środki odwetu istnieją, agresor może uznać, że druga strona nie odważy się z nich skorzystać z obawy przed eskalacją, kosztem politycznym na arenie wewnętrznej czy sprzeciwem opinii publicznej. Właśnie dlatego państwa starają się podtrzymywać wrażenie determinacji poprzez ćwiczenia wojskowe, pokazy siły, publikowanie doktryn użycia siły czy konsekwentne stosowanie wcześniej zapowiadanych sankcji. To wszystko ma dowodzić, że zapowiedzi nie są czystą retoryką.

Istotny jest również sposób komunikowania groźby. Odstraszanie może funkcjonować tylko wtedy, gdy przekaz jest zrozumiały dla odbiorcy. Granice, których przekroczenie spowoduje nałożenie kary, często określane jako „czerwone linie", powinny być możliwie jasno zarysowane. Nieprecyzyjne lub sprzeczne sygnały zwiększają ryzyko błędnej kalkulacji po stronie potencjalnego agresora, który może uznać, że jego działania pozostaną poniżej progu reakcji albo że druga strona blefuje.

W tle tego wszystkiego znajduje się założenie o racjonalności odbiorcy. Koncepcja odstraszania przez karę opiera się na przekonaniu, że decydenci polityczni i wojskowi dokonują kalkulacji zysków i strat. W praktyce motywacje mogą być inne: ideologiczne, związane z utrzymaniem władzy, potrzebą demonstracji siły, presją wewnętrznych grup poparcia. W takich okolicznościach groźba kary może zostać zignorowana lub zinterpretowana w sposób nieprzewidziany przez stronę odstraszającą.

W historii najpełniej rozwiniętym przykładem zastosowania odstraszania przez karę była rywalizacja nuklearna między Stanami Zjednoczonymi a Związkiem Radzieckim w okresie zimnej wojny. Obie strony utrzymywały rozbudowane arsenały broni jądrowej, zdolne do zadania

przeciwnikowi zniszczeń o skali niewyobrażalnej w kategoriach konwencjonalnych. Układ ten, określany jako wzajemnie gwarantowane zniszczenie, miał paradoksalnie działać stabilizująco: pełnoskalowa wojna stawała się równoznaczna z katastrofą dla wszystkich uczestników, a więc przestawała być racjonalnym narzędziem polityki.

Zapowiedź, że atak na jedno państwo spotka się z reakcją całego układu sojuszniczego, ma zniechęcać potencjalnego agresora do podejmowania działań przeciw państwom formalnie słabszym militarnie. W tym sensie odstraszanie przez karę zostaje „udostępnione" mniejszym państwom, które otrzymują wsparcie w postaci groźby reakcji ze strony silniejszego partnera.

Artykuł 5 traktatu waszyngtońskiego jest klasycznym przykładem odstraszania przez karę w wydaniu sojuszniczym. Zapis, że zbrojny atak na jedno państwo członkowskie jest traktowany jako atak na wszystkie, oznacza dla potencjalnego agresora konieczność liczenia się nie z reakcją pojedynczego kraju, lecz całego NATO, z jego potencjałem militarnym, gospodarczym i politycznym. Groźba „zbiorowej odpowiedzi", łącznie z użyciem siły zbrojnej, ma odstraszać właśnie przez perspektywę bardzo wysokich kosztów ewentualnej agresji. W tym sensie artykuł 5 tworzy mechanizm rozszerzonego odstraszania przez karę: bezpieczeństwo państw słabszych militarnie zostaje „podparte" możliwościami mocarstw, w tym nuklearnych. Agresor, rozważając atak na któregokolwiek członka NATO, musi brać pod uwagę nie tylko lokalną obronę, ale także odwet całego sojuszu w formie operacji wojskowej, sankcji, izolacji politycznej czy połączonych działań w różnych domenach. Niepewność co do skali i dokładnej formy tej odpowiedzi dodatkowo komplikuje jego kalkulację. Fakt, że artykuł 5 został faktycznie uruchomiony po zamachach z 11 września 2001 r., pokazał, iż zobowiązanie to nie jest wyłącznie deklaracją polityczną, lecz może zostać wprowadzone w życie. Od tego czasu wszystkie dyskusje o wzmocnieniu wschodniej flanki, rozmieszczeniu wojsk sojuszniczych czy zwiększaniu wydatków obronnych krążą wokół jednego pytania: na ile groźba wspólnej odpowiedzi pozostaje wiarygodna. To właśnie wiara w realność tej kary, a nie fizyczne uniemożliwienie ataku ma powstrzymywać przeciwnika przed uderzeniem na terytorium któregokolwiek z członków NATO.

W praktyce instrumentem karnym bardzo często stają się również sankcje, stosowane wobec państw rozwijających programy nuklearne, prowadzących agresywną politykę regionalną lub rażąco naruszających prawa człowieka. W wielu przypadkach sama zapowiedź ich wprowadzenia ma działać prewencyjnie, wpływając na kalkulacje potencjalnego sprawcy jeszcze przed podjęciem kroków, które trudno byłoby odwrócić.

Nie brakuje jednak zastrzeżeń wobec tego sposobu kształtowania bezpieczeństwa. Groźba zadania poważnych strat zawsze niesie ze sobą ryzyko eskalacji. Strona ukarana może zareagować własnym odwetem, uruchamiając spiralę narastających działań. Szczególnie niebezpieczne jest to tam, gdzie w grę wchodzą środki o bardzo dużej sile rażenia, których użycie trudno kontrolować zarówno technicznie, jak i politycznie.

Do tego dochodzą koszty moralne i polityczne. Odstraszanie przez karę często zakłada gotowość do użycia środków, które mogą prowadzić do śmierci ludności cywilnej, zniszczenia infrastruktury czy długotrwałych kryzysów humanitarnych. W państwach demokratycznych, gdzie opinia publiczna jest wrażliwa na takie skutki, utrzymanie wiarygodnej groźby bywa trudne, zwłaszcza w dłuższej perspektywie.

Znaczącym ograniczeniem jest też niższa skuteczność wobec aktorów niestandardowych. Organizacje terrorystyczne czy zbrojne grupy niepaństwowe nie dysponują klasycznym terytorium, gospodarką czy rozpoznawalnymi elitami, które można „ukarać" w tradycyjny sposób. Często świadomie dążą do konfrontacji, a straty własne nie są dla nich czynnikiem zniechęcającym. Groźba kary traci w takich warunkach część swojego potencjału.

Wreszcie, zbyt silne akcentowanie groźby odwetu może zostać odczytane jako przejaw agresywnej postawy, co sprzyja wyścigowi zbrojeń i poszukiwaniu przez drugą stronę środków przeciwdziałania. Państwo, które czuje się stale zagrożone cudzym odstraszaniem, może dążyć do uprzedzającego działania lub rozwijać własne środki eskalacji, co zamiast stabilizować sytuację, prowadzi do jej dalszego zaostrzenia.

W zmieniającym się środowisku bezpieczeństwa odstraszanie przez karę pozostaje ważnym narzędziem, ale coraz rzadziej występuje w czystej postaci. Traktuje się je raczej jako element szerszej strategii, łączony z budowaniem odporności państwa, wzmacnianiem obrony i działaniami prewencyjnymi. Groźba kary nadal może powstrzymywać przed agresją,

jednak sama w sobie nie wystarcza, aby zapewnić stabilność w świecie pełnym złożonych, rozproszonych i trudnych do przewidzenia zagrożeń.

W XXI w. zmienia się środowisko bezpieczeństwa, co wpływa także na możliwości używania kary jako podstawowego narzędzia odstraszania. Po pierwsze, rośnie znaczenie cyberprzestrzeni i informacji; trudniej jest ustalić sprawcę ataku, a więc również zastosować karę i wiarygodnie ją zapowiedzieć. Po drugie, rośnie rola aktorów niepaństwowych, dla których tradycyjne środki odwetu mają ograniczony sens. Po trzecie, opinia publiczna w wielu państwach jest coraz mniej skłonna akceptować działania odwetowe o dużej skali, co wpływa na wiarygodność groźby.

Jednocześnie narasta dyskusja o tym, jak łączyć odstraszanie przez karę z innymi środkami – militarnymi, gospodarczymi, informacyjnymi – oraz jak budować strategie, które nie opierają się wyłącznie na groźbie zadawania strat, ale też na wzmacnianiu odporności i stabilności własnego państwa.

Odstraszanie przez karę pozostaje jednym z głównych sposobów kształtowania strategii bezpieczeństwa. Jest atrakcyjne, bo – przynajmniej w teorii – pozwala zapobiec wojnie bez konieczności prowadzenia dużych działań obronnych z wyprzedzeniem. Kalkulacja jest prosta: „Nie atakuj, bo zapłacisz zbyt wysoką cenę". Model ten ma jednak wyraźne ograniczenia. Wymaga wiarygodności, zdolności, jasno zakomunikowanych czerwonych linii i założenia, że przeciwnik kalkuluje w logiczny sposób. W świecie pełnym niepaństwowych aktorów, kampanii informacyjnych, cyberataków i złożonych zależności politycznych sama groźba kary bywa niewystarczająca, dlatego coraz częściej traktuje się ją jako jeden z elementów szerszej strategii, a nie jako jedyny filar bezpieczeństwa.

Fabian Kobalczyk-Gruda

J. Abramovaite, *Classical Deterrence Theory Revisited: Empirical Tests of Severity, Certainty and Celerity*, „European Journal of Criminology" 2022, https://pure-oai.bham.ac.uk/ws/portalfiles/portal/169658586/abramovaitej2022classical.pdf (dostęp 29.11.2025); *Collective defence and Article 5*, „NATO Topics" 2025, https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5 (dostęp 29.11.2025); *Collective Defence in NATO: A Legal and Strategic Analysis of Article 5 in Light of the War in Ukraine*, 2025, https://www.schumannetwork.eu/2025/03/03/collective-defence-in-nato-a-legal-and-strategic-analysis-of-article-5-in-light-of-

the-war-in-ukraine/ (dostęp 29.11.2025); *Deterrence and defence*, „NATO Topics" 26.06.2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence (dostęp 29.11.2025); L. Forrester, *Classical Theories of Criminology: Deterrence*, [w:] *Criminology and Criminal Justice*, OER Collective, 2024, https://oercollective.caul.edu.au/criminology-criminal-justice/chapter/classical-theories-deterrence/ (dostęp 29.11.2025); A. Kacprzyk, *Keeping Collective Defence the Main Priority in NATO's New Strategy*, „PISM Strategic File" 2021, no. 10(116), https://pism.pl/publications/keeping-collective-defence-the-main-priority-in-natos-new-strategy (dostęp 29.11.2025); A. Kacprzyk, *Odstraszanie. Strategia i polityka*, Polski Instytut Spraw Międzynarodowych, Warszawa 2021; R. Kopeć, *Strategie nuklearne w okresie pozimnowojennym*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2014; R. Kopeć, P. Mazur, *Odstraszanie militarne w XXI wieku. Polska – NATO – Rosja*, Uniwersytet Pedagogiczny w Krakowie, Kraków 2017; K. Kubiak, *Po co w Europie amerykańska broń nuklearna? Odstraszanie nuklearne NATO w XXI wieku*, „International Relations/Internationalne Stosunki" 2019, t. 59, nr 2, https://www.irjournal.pl/pdf-124660-52725 (dostęp 29.11.2025); U. Kühn, L. Mengelkamp, F. Stärk, *From Nuclear Deterrence to Democratic Resilience: Towards a 21st Century Security Paradigm*, LSE IDEAS, London 2025, https://www.lse.ac.uk/ideas/projects/conflict-and-civicness-research-group/assets/Assets/Publications/Research-Reports/Non-Nuclear-Deterrence-Report-Final.pdf (dostęp 29.11.2025); M.J. Mazarr, *Understanding Deterrence*, RAND Corporation, Santa Monica 2018, PE-295, https://www.rand.org/pubs/perspectives/PE295.html (dostęp 29.11.2025); M. Paszyn, *Problem odstraszania konwencjonalnego NATO – aspekt polityczny*, „Studia Bezpieczeństwa Narodowego" 2019, nr 15, https://sbn.wat.edu.pl/pdf-135296-63616 (dostęp 29.11.2025); T. Preskiewicz, *Odstraszanie w strategii bezpieczeństwa państwa* [rozprawa doktorska], Wojskowa Akademia Techniczna, Warszawa 2023, https://bip.wat.edu.pl/.../doktrat_2023_final_drukowanie_2_0.pdf (dostęp 29.11.2025); *Sanctions, Peacemaking and Enforcement: International Responses to Coercive Diplomacy*, P. Wallensteen, C. Portela (eds.), Brill, Leiden–Boston 2015; T.S. Sechser, M. Fuhrmann, *Nuclear Weapons and Coercive Diplomacy*, Cambridge University Press, Cambridge 2017; M. Terlikowski, *Wysunięta obrona – nowe podejście do polityki obrony i odstraszania NATO*, „Komentarz PISM" 2022, https://pism.pl/publikacje/wysunieta-obrona-nowe-podejscie-do-polityki-obrony-i-odstraszania-nato (dostęp 29.11.2025); A. Wilner, *The Dark Side of Extended Deterrence*, „Journal of Strategic Studies" 2018, vol. 41, no. 5; R. Wilson, *The Myth of Nuclear Deterrence*, „Nonproliferation Review" 2008, vol. 15, no. 3; *Zagadnienie odstraszania*, „Przegląd NATO" 5.08.2016, https://www.nato.int/docu/review/pl/articles/2016/08/05/zagadnienie-odstraszania/index.html (dostęp 29.11.2025).

ODSTRASZANIE PRZEZ UNIEMOŻLIWIENIE/ODMOWĘ (ang. *deterrence by denial*) – jeden z dwóch klasycznych filarów teorii odstraszania. Główną jego ideą jest sprawienie, by potencjalny agresor uznał atak za nieskuteczny lub zbyt trudny, a więc nieopłacalny z militarnego, politycznego czy strategicznego punktu widzenia. Innymi słowy, kluczowym mechanizmem jest odjęcie przeciwnikowi pewności sukcesu, a nie grożenie mu kosztami odwetu. Strategia ta koncentruje się na fizycznych, logistycznych, operacyjnych i strukturalnych przeszkodach, które mają zniechęcić do ataku, obniżyć jego prawdopodobieństwo i zminimalizować szanse na powodzenie.

W historii bezpieczeństwa międzynarodowego koncepcja ta odgrywała rolę w różnych epokach – od obrony warownej i fortów, przez doktryny zimnowojenne, aż po współczesne strategie NATO, obronę cybernetyczną czy koncepcje wojny hybrydowej. Obecnie, w warunkach erozji stabilności międzynarodowej i wzrostu zagrożeń asymetrycznych, dyskusja o odstraszaniu przez uniemożliwienie powraca ze szczególną intensywnością, zwłaszcza w kontekście wschodniej flanki NATO i dynamicznego rozwoju technologii militarnych.

Model odstraszanie przez uniemożliwienie:

- główna logika – utrudnienie lub uniemożliwienie agresji;
- mechanizm – obrona, fortyfikacja, dyspozycyjność sił;
- skutki dla agresora – brak szans na sukces;
- charakter – reaktywny, fizyczny, operacyjny;
- przykład – umocnienia, mobilne jednostki, cyberzabezpieczenia.

W praktyce państwa rzadko stosują tylko jeden model odstraszania. Strategia mieszana jest bardziej realna, ale ich równowaga i proporcje zależą od kontekstu politycznego, kultury strategicznej, geopolityki oraz zasobów militarno-ekonomicznych.

Choć nowoczesna teoria ukształtowała się dopiero w XX w., logika odstraszania przez uniemożliwienie jest znacznie starsza. Można wyróżnić kilka etapów jej rozwoju.

1. Od starożytności do XIX w. – środki odstraszania przez uniemożliwienie były powszechnie stosowane w dawnych systemach obronnych. Budowa murów miejskich, fos, fortów, bastionów czy

naturalnych przeszkód stanowiła sposób na utrudnienie agresji. Przykłady:
- Wielki Mur Chiński;
- twierdze Rzeczypospolitej, np. Zamość czy Kamieniec Podolski;
- rzymski limes;
- średniowieczne grody obronne.

Wszystkie te rozwiązania odwoływały się do założenia, że napastnik zrezygnuje, jeśli koszt przełamania obrony okaże się zbyt wysoki.

2. XX w. i zimna wojna – w okresie zimnej wojny teoria odstraszania nabrała naukowego charakteru dzięki takim badaczom, jak:
   - Bernard Brodie;
   - Thomas Schelling;
   - Glenn Snyder.

W dyskusjach nad odstraszaniem jądrowym dominowała logika „kary", ale równolegle rozwijano koncepcję uniemożliwienia – szczególnie w kontekście konwencjonalnej obrony NATO w Europie.

3. XXI w. – współcześnie odstraszanie przez uniemożliwienie zyskuje na znaczeniu w związku z:
   - agresywną polityką Rosji;
   - rozwojem technologii precyzyjnych;
   - zagrożeniami cybernetycznymi;
   - wojną hybrydową i szarą strefą;
   - rywalizacją mocarstw w Azji;
   - potrzebą ochrony infrastruktury krytycznej.

W efekcie koncepcja ta ewoluowała od tradycyjnego pojmowania obrony do wielowymiarowej strategii obejmującej również przestrzeń cybernetyczną, energetyczną, kosmiczną oraz informacyjną.

Odstraszanie przez uniemożliwienie pełni w systemie bezpieczeństwa międzynarodowego wiele funkcji wynikających z jego podstawowej logiki, którą jest pozbawienie potencjalnego agresora wiary w możliwość osiągnięcia zamierzonych celów politycznych i militarnych. Jedną z najważniejszych funkcji tej strategii jest odebranie przeciwnikowi nadziei na szybkie zwycięstwo. W realiach współczesnych konfliktów zbrojnych tempo działań oraz zdolność uzyskania przewagi w pierwszych godzinach lub dniach operacji mają fundamentalne znaczenie.

Państwo, które jest przygotowane obronnie i posiada rozwinięte mechanizmy uniemożliwienia, sprawia, że przeciwnik nie może liczyć na łatwe, błyskawiczne przełamanie, co obniża atrakcyjność agresji jako środka realizacji celów strategicznych.

Innym aspektem jest podnoszenie kosztów operacyjnych, jakie musi ponieść potencjalny napastnik. Dobrze zaprojektowana, wielowarstwowa obrona obejmująca mobilne i elastyczne jednostki, obronę terenową, systemy fortyfikacji oraz rozwiązania inżynieryjne powoduje, że agresor musi angażować znacznie większe siły, liczyć się z potencjalnie wysokimi stratami oraz wydłużeniem czasu trwania operacji. Wzrost kosztów obejmuje również ryzyko polityczne i dyplomatyczne, ponieważ dłuższy konflikt daje społeczności międzynarodowej więcej czasu na reakcję, a to może prowadzić do sankcji, izolacji lub wsparcia dla strony broniącej się. W konsekwencji nawet potęgi dysponujące przewagą konwencjonalną muszą dokładnie kalkulować opłacalność ewentualnej agresji.

Trzecią funkcją odstraszania przez uniemożliwienie jest wzmacnianie wiarygodności politycznej państwa. Inwestowanie w obronę, rozwijanie infrastruktury obronnej, utrzymywanie gotowości oraz eksponowanie zdolności uniemożliwiających szybki sukces przeciwnika są komunikatami świadczącymi o determinacji do obrony terytorium i integralności państwowej. Wiarygodność ta ma znaczenie zarówno wewnętrzne, jak i zewnętrzne: wzmacnia morale społeczeństwa oraz zaufanie sojuszników, a zarazem utrudnia przeciwnikowi budowanie narracji o słabości czy braku woli obrony.

Odstraszanie przez uniemożliwienie pełni także funkcję stabilizującą w skali regionalnej. Państwa, które są w stanie utrudnić agresję już na samym początku konfliktu, wysyłają wyraźny sygnał, że nie są „łatwym celem". Taki komunikat znacząco zmniejsza ryzyko prowokacji lub prób zastraszenia, a stabilność w regionie wzrasta, ponieważ potencjalni agresorzy są świadomi trudności związanych z przeprowadzeniem skutecznej operacji. Stabilizacyjna funkcja odstraszania przez uniemożliwienie jest szczególnie ważna w regionach o dużej liczbie napięć, jak Europa Wschodnia, Azja Wschodnia czy Bliski Wschód.

Ostatnim z głównych atutów tej strategii jest jej relatywnie wysoka akceptowalność polityczna. W przeciwieństwie do odstraszania opartego

na groźbie odwetu, które często zakłada możliwość zadawania przeciwnikowi poważnych strat – włącznie z użyciem broni masowego rażenia, odstraszanie przez uniemożliwienie nie wymaga formułowania dramatycznych gróźb. Bazuje na defensywnych środkach zwiększających odporność państwa, przez co łatwiej je uzasadnić w debacie publicznej i na forum międzynarodowym. Jest to szczególnie istotne w zachodnich demokracjach, gdzie opinia publiczna i koszt polityczny ewentualnej eskalacji mają duże znaczenie.

Mechanizmy działania odstraszania przez uniemożliwienie obejmują szeroką gamę narzędzi i rozwiązań, z których wiele ma charakter zarówno militarny, jak i cywilny. Jednym z najstarszych i najbardziej intuicyjnych mechanizmów są fizyczne bariery oraz fortyfikacje. Do kategorii tej zalicza się zarówno nowoczesne umocnienia terenowe, jak i tradycyjne fortyfikacje wojskowe, przeszkody inżynieryjne czy stałe punkty oporu. Współczesna praktyka pokazuje, że takie struktury nie są reliktem przeszłości. Przykłady Korei Południowej czy Izraela dowodzą, że rozbudowane systemy umocnień nadal skutecznie ograniczają przestrzeń operacyjną przeciwnika i utrudniają szybkie przełamanie obrony, choć nie bazują tylko i wyłącznie na jednym modelu odstraszania.

Kolejnym mechanizmem jest rozproszona i elastyczna obrona, charakterystyczna dla nowoczesnych sił zbrojnych. Zakłada ona mobilność jednostek, decentralizację struktur dowodzenia, wykorzystanie systemów sieciocentrycznych oraz zdolność szybkiego reagowania na zmieniające się warunki pola walki. Rozproszona obrona utrudnia przeciwnikowi zadanie jednego decydującego uderzenia, niszczy jego nadzieję na błyskawiczne zwycięstwo i zmusza do rozciągania linii logistycznych, co zwiększa podatność agresora na kontratak.

Współczesnym i coraz ważniejszym obszarem odstraszania przez uniemożliwienie jest obrona cybernetyczna. W cyberprzestrzeni logika uniemożliwienia opiera się na redundancji systemów, segmentacji sieci, szybkim wykrywaniu intruzji oraz wdrażaniu wielowarstwowych środków ochrony. Celem jest takie zwiększenie trudności przeprowadzenia skutecznego cyberataku, by stał się on nieopłacalny, czasochłonny i podatny na neutralizację. W świecie, w którym infrastruktura państw zależy od

systemów cyfrowych, odporność cybernetyczna staje się jednym z najważniejszych elementów odstraszania.

Ostatnim mechanizmem w ramach odstraszania przez uniemożliwienie jest rozwój obrony terytorialnej oraz budowa odpornego społeczeństwa. Obejmuje to tworzenie wojsk obrony terytorialnej, efektywnych systemów rezerw, edukację obronną, odporność społeczeństwa na dezinformację i wojnę psychologiczną, a także zabezpieczenie infrastruktury krytycznej. Kraje zagrożone agresją hybrydową, m.in. państwa bałtyckie czy Finlandia, rozwijają te zdolności w sposób szczególnie intensywny, traktując je jako niezbędny element zniechęcania przeciwnika do działań destabilizacyjnych.

W praktyce państwa stosują różne warianty odstraszania przez uniemożliwienie, zależnie od warunków geograficznych, potencjału militarnego, zagrożeń oraz kultury strategicznej. Jednym z najczęściej spotykanych modeli jest obrona warstwowa, zakładająca stopniowe spowalnianie i rozbijanie ataku przeciwnika poprzez wiele kolejnych linii oporu. Tego typu rozwiązania były testowane jeszcze w XX w., lecz w kolejnym stuleciu zyskują na znaczeniu, ponieważ wysokomobilne systemy walki oraz technologia precyzyjna sprawiają, że rozproszone modułowe podejście zwiększa szanse utrzymania ciągłości obrony nawet po utracie części infrastruktury.

Drugim modelem jest obrona rozproszona obejmująca użycie małych, autonomicznych jednostek operujących na dużym obszarze. Taka strategia znacząco zmniejsza podatność obrony na jeden uderzeniowy manewr przeciwnika, a jednocześnie zwiększa niepewność operacyjną napastnika. Model ten często łączy się z doktryną „jeża", zakładającą, że terytorium państwa staje się trudne do opanowania, a kontrola nad nim – kosztowna i czasochłonna.

Trzecim podejściem jest budowanie odporności strukturalnej państwa, czyli rozwijanie rozwiązań zapewniających funkcjonowanie kluczowych sektorów nawet w warunkach zakłóceń. Dotyczy to przede wszystkim infrastruktury energetycznej, transportowej, telekomunikacyjnej i cybernetycznej. Przygotowanie redundancji systemów, magazynów rezerwowych oraz planów awaryjnych sprawia, że agresor nie może liczyć

na sparaliżowanie państwa jednym uderzeniem, co zmniejsza atrakcyjność działań destabilizacyjnych.

W ostatniej dekadzie NATO w coraz większym stopniu uwzględnia odstraszanie przez uniemożliwienie w swoich planach obronnych. Dotyczy to szczególnie państw bałtyckich i Polski, które ze względu na położenie geograficzne są narażone na szybkie operacje ofensywne. Wzmacnianie tzw. odporności narodowej, uprzednie rozmieszczenie uzbrojenia i wyposażenia, rozwijanie sił szybkiego reagowania, integracja obrony terytorialnej oraz budowa wielowarstwowych systemów obrony przeciwlotniczej tworzą środowisko, w którym agresor musiałby liczyć się z długotrwałą i kosztowną kampanią. To właśnie ta niepewność co do możliwości przeprowadzenia skutecznej operacji ogranicza prawdopodobieństwo agresji.

Finlandia od dziesięcioleci stanowi klasyczny przykład państwa, które swoją strategię obronną buduje w oparciu o koncepcję uniemożliwienia przeciwnikowi osiągnięcia celów. System bezpieczeństwa opiera się tam na powszechnym obowiązku obrony i rozbudowanym systemie rezerw, co pozwala na szybkie rozwinięcie dużej liczby przeszkolonych żołnierzy w razie kryzysu. Jednocześnie kładzie się duży nacisk na odporność społeczną: przygotowanie ludności do funkcjonowania w warunkach zakłóceń, wysoki poziom zaufania do instytucji publicznych oraz spójność państwa i społeczeństwa. Ważnym elementem fińskiego podejścia jest także rozległa obrona terenowa, wykorzystująca uwarunkowania geograficzne kraju, w tym lasy, jeziora i trudną sieć komunikacyjną, oraz infrastruktura projektowana z myślą o możliwości prowadzenia działań zbrojnych z licznymi obiektami przystosowanymi do funkcji obronnych i ochrony ludności. Fińska doktryna zakłada, że potencjalny przeciwnik nie będzie w stanie osiągnąć szybkiego zwycięstwa, a okupacja kraju stanie się przedsięwzięciem niezwykle wymagającym, długotrwałym i obciążonym dużym ryzykiem strat. W efekcie stanowi to jeden z najbardziej rozpoznawalnych modeli odstraszania pozbawionego komponentu broni masowego rażenia.

Izrael łączy w swojej strategii 2 podstawowe mechanizmy odstraszania: groźbę odwetu oraz systemy, które mają uniemożliwić przeciwnikowi zadanie decydującego ciosu. Z jednej strony, państwo dysponuje znacznym potencjałem ofensywnym i możliwością odpowiedzi na atak w sposób

dotkliwy dla przeciwnika; z drugiej – od wielu lat rozwijane są rozbudowane środki obrony obejmujące wielowarstwowe systemy antyrakietowe, zdolne do przechwytywania różnego typu pocisków, dobrze zorganizowaną obronę cywilną, utrzymywanie wysokiego poziomu gotowości społeczeństwa na wypadek kryzysu oraz dużą mobilność sił zbrojnych, które mogą szybko reagować na zagrożenia na różnych kierunkach. Taka kombinacja sprawia, że potencjalny agresor musi brać pod uwagę zarówno perspektywę doznania bolesnego odwetu, jak i trudność osiągnięcia celów militarnych w krótkim czasie. Synergia obu modeli powoduje, że planowanie skutecznej operacji przeciwko Izraelowi staje się wyjątkowo złożone i obarczone poważnym ryzykiem niepowodzenia.

Tajwan rozwija strategię odstraszania przez uniemożliwienie przede wszystkim jako odpowiedź na zagrożenie ewentualnym atakiem ze strony Chińskiej Republiki Ludowej. Koncepcja ta, często określana mianem obrony „jeża", zakłada takie przygotowanie państwa, aby potencjalny przeciwnik napotkał maksymalne trudności już na etapie prób desantu i przejęcia kontroli nad terytorium. W praktyce oznacza to tworzenie rozwiązań utrudniających prowadzenie operacji morskich i powietrznych, systematyczne rozwijanie środków ukierunkowanych na niszczenie zdolności logistycznych przeciwnika, rozproszenie sił obronnych na całym obszarze wyspy oraz oparcie planów obronnych na wykorzystaniu trudnego terenu i gęstej infrastruktury miejskiej. Celem jest doprowadzenie do sytuacji, w której przejęcie Tajwanu staje się procesem powolnym, kosztownym i obarczonym dużą niepewnością co do ostatecznego wyniku, co ma zniechęcać do podjęcia decyzji o agresji.

Polska, zwłaszcza po 2014 r., rozwija rozwiązania mające utrudnić potencjalnej agresji osiągnięcie efektu zaskoczenia i szybkiego przełamania. W centrum tego podejścia znajdują się m.in. Wojska Obrony Terytorialnej, system rezerw oraz ćwiczenia o charakterze kryzysowym i obronnym, a także coraz ściślejsza integracja wojsk operacyjnych z lokalnymi strukturami administracyjnymi. Równolegle wzmacniana jest odporność na działania hybrydowe – w tym na presję informacyjną, cyberataki i sabotaż – oraz ochrona infrastruktury krytycznej obejmującej sektor energetyczny, łączność, transport i systemy zaopatrzenia. Szczególna rola przypada WOT, które dzięki lokalnemu zakorzenieniu,

znajomości terenu oraz elastycznej strukturze organizacyjnej utrudniają przeprowadzenie operacji nastawionych na szybkie wywołanie chaosu i destabilizację instytucji państwowych. Obecność formacji terytorialnej w różnych regionach kraju zmniejsza szanse przeciwnika na osiągnięcie strategicznego zaskoczenia i tworzy warunki, w których objęcie trwałą kontrolą nad terytorium byłoby procesem wyjątkowo wymagającym.

Mimo wielu zalet koncepcja ta nie jest pozbawiona słabych stron. Jednym z najczęściej podnoszonych argumentów jest kosztowność utrzymywania rozbudowanego systemu obronnego, który wymaga stałych nakładów finansowych, szkoleń, modernizacji infrastruktury i zaangażowania społecznego. Państwa o ograniczonych zasobach mogą mieć trudności z utrzymaniem takiej strategii na poziomie zapewniającym realny efekt odstraszający.

Kolejnym problemem jest fakt, że odstraszanie przez uniemożliwienie działa głównie wtedy, gdy agresor racjonalnie kalkuluje swoje możliwości. W przypadku państw autorytarnych, kierujących się logiką polityki wewnętrznej, prestiżu lub ideologii, perspektywa poniesienia kosztów może nie mieć wystarczającej siły oddziaływania. Podobnie w sytuacjach, gdy agresor zakłada krótkotrwałe działania poniżej progu wojny, środki uniemożliwienia mogą okazać się niewystarczające.

Część badaczy zwraca również uwagę, że strategia ta, skupiając się na defensywie, może być interpretowana przez przeciwnika jako oznaka braku ofensywnej determinacji. W związku z tym państwa często decydują się na łączenie obu modeli odstraszania, tworząc mieszane strategie, które mają zarówno osłabić szanse na sukces agresji, jak i podnieść potencjalne koszty odwetowe.

W XXI w. zmienia się charakter zagrożeń, co wymusza adaptację tej strategii. Coraz większą rolę odgrywają:

- cyberataki;
- dezinformacja;
- presja ekonomiczna;
- operacje hybrydowe;
- działania paramilitarne i najemnicy;
- ataki na infrastrukturę energetyczną;
- zagrożenia w przestrzeni kosmicznej.

W tych warunkach uniemożliwienie wymaga połączenia tradycyjnych środków wojskowych z cyfrowymi systemami bezpieczeństwa, odpornością społeczną oraz strategiczną komunikacją państwa. Obronność staje się procesem obejmującym całe państwo, nie tylko siły zbrojne.

Fabian Kobalczyk-Gruda

Boundless Israel, Israeli Deterrence and the October 7 Attack, policy paper, Boundless Israel, 2024, https://boundlessisrael.org/paper/485/details (dostęp 27.11.2025); *Deterrence and defence*, „NATO Topics" 26.06.2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence (dostęp 27.11.2025); J. Grzela, *Finland's readiness for comprehensive national defence*, „Bezpieczeństwo. Teoria i Praktyka" 2022, t. XLVIII, nr 3; A. Kacprzyk, *Perspectives on NATO's Deterrence and Defence on the Eastern Flank*, Polish Institute of International Affairs (PISM), Warszawa 2018; C.P. Kirchofer, *Managing Non-State Threats with Cumulative Deterrence-by-Denial*, „Perspectives on Terrorism" 2017, vol. 11, no. 2, https://www.jstor.org/stable/26297836 (dostęp 27.11.2025); R. Kopeć, P. Mazur, *Odstraszanie militarne w XXI wieku. Polska – NATO – Rosja*, Wydawnictwo Uniwersytetu Pedagogicznego im. KEN, Kraków 2017; U. Kühn, L. Mengelkamp, F. Stärk, *From Nuclear Deterrence to Democratic Resilience: Towards a 21st Century Security Paradigm, Conflict and Civicness Research Group*, LSE IDEAS, London 2025, https://www.lse.ac.uk/ideas/projects/conflict-and-civicness-research-group/assets/Assets/Publications/Research-Reports/Non-Nuclear-Deterrence-Report-Final.pdf (dostęp 27.11.2025); C. Kunadu, *Doubting Deterrence by Denial,* „Emerging Threats Group Journal" 24.02.2025, https://emergingthreats.co.uk/doubting-deterrence-by-denial/ (dostęp 27.11.2025); M.J. Mazarr, *Understanding Deterrence, RAND Corporation*, Santa Monica 2018, RAND Perspective PE-295, https://www.rand.org/pubs/perspectives/PE295.html (dostęp 27.11.2025); A. Michalak, *Działania taktyczne wojsk obrony terytorialnej*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2020; A. Michalak, *Działania w obszarze zajętym przez przeciwnika – rola, możliwości i ograniczenia w wykorzystaniu Wojsk Obrony Terytorialnej*, „Wiedza Obronna" 2022, t. 279, nr 2, https://wiedzaobronna.edu.pl/index.php/wo/article/view/163 (dostęp 27.11.2025); *Odstraszanie militarne w XXI wieku. Polska – NATO – Rosja*, S. Koziej (red.), Wydawnictwo Akademii Obrony Narodowej, Warszawa, https://www.wojsko-polskie.pl/awl/u/aa/7a/aa7a0af7-a068-4021-b606-1abc3a8cc838/odstraszanie_militarne.pdf (dostęp 27.11.2025); D. Remžová, D. Urhová, *The Porcupine Strategy: Taiwan's Road to Self-Defense*, „China Observers in Central and Eastern Europe (CHOICE)" 17.10.2024, https://chinaobservers.eu/the-porcupine-strategy-taiwans-road-to-self-defense/ (dostęp

27.11.2025); R. Rushby, *An Introduction to Deterrence by Denial, Sea Power Centre – Australia*, Canberra 2025, https://seapower.navy.gov.au/sites/default/files/2025-03/Deterrence%20by%20Denial.pdf (dostęp 27.11.2025); J. Sawyer, *Dissuasion by Denial in Counterterrorism*, [w:] *Deterrence by Denial: Theory and Practice*, A.S. Wilner, A. Wenger (eds.), Cambria Press, Amherst–New York 2021; V. Shalamanov, *Deterrence and Defense at the Eastern Flank of NATO and Beyond*, „Connections: The Quarterly Journal" 2019, vol. 18, no. 1–2; *Strengthening NATO's eastern flank*, „NATO Topics" 23.10.2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/strengthening-natos-eastern-flank (dostęp 27.11.2025); *Taiwan's Porcupine Strategy and U.S. Prioritization of Denial Defense to Deter China: An Interview with Rohith Narayan*, „World Geostrategic Insights (WGI)" 18.02.2024, https://www.wgi.world/taiwan-s-porcupine-strategy-and-u-s-prioritization-of-denial-defense-to-deter-china-an-interview-with-rohith-narayan/ (dostęp 27.11.2025); P. Woyke, *Strategie przetrwania. Potencjał odstraszania w politykach obronnych Finlandii i Izraela po 1991 roku* [praca doktorska], Uniwersytet Jagielloński, Kraków 2022.

OKRĘT PODWODNY – jednostka pływająca zdolna do poruszania się zarówno na powierzchni, jak i pod wodą. Tym samym odróżnia się od innych łodzi i statków, które poruszają się wyłącznie na powierzchni, oraz od batyskafów przemieszczających się głównie wzdłuż osi pionowej. To rodzaj okrętu, najczęściej wojskowego, który jest zdolny do zanurzenia się i pozostawania w zanurzeniu przez dłuższy czas. Obecnie okręty podwodne służą w marynarkach wojennych 40 krajów, w tym 6 posiadających okręty podwodne o napędzie atomowym.

Współczesne okręty podwodne to najbardziej zróżnicowane pod względem wielkości i przeznaczenia jednostki bojowe sił morskich. Do tej klasy zalicza się bowiem zarówno jednostki przybrzeżne, niewiele większe od batyskafów, jak i okręty oceaniczne napędzane paliwem jądrowym, których wyporność przekracza 20 tys. t. Warto dodać, że te ostatnie wyposażone są w pociski balistyczne z głowicami jądrowymi i mają znaczenie strategiczne.

Chociaż eksperymentalne okręty podwodne budowano wcześniej, projektowanie okrętów podwodnych nabrało rozpędu w XIX w., a okręty podwodne stały się stałą klasą wielu marynarek wojennych. Po raz pierwszy zostały szeroko użyte podczas I wojny światowej, a obecnie są wykorzystywane w wielu marynarkach wojennych, zarówno oceanicznych,

jak i przybrzeżnych. Ich zastosowania militarne obejmują: atakowanie wrogich okrętów nawodnych oraz statków handlowych lub innych okrętów podwodnych; ochronę lotniskowców; prowadzenie blokady; odstraszanie nuklearne; operacje specjalne na niedostępnych obszarach podczas gromadzenia informacji wywiadowczych i prowadzenia rozpoznania; uniemożliwianie lub wpływanie na ruchy wroga; konwencjonalne ataki lądowe (np. wystrzelenie pocisku manewrującego) oraz tajne wprowadzanie płetwonurków lub sił specjalnych. Ich zastosowania cywilne obejmują: nauki morskie; ratownictwo; eksplorację oraz inspekcję i konserwację obiektów. Okręty podwodne mogą być modyfikowane do specjalistycznych funkcji, takich jak misje poszukiwawczo-ratownicze i naprawa kabli podmorskich. Są również wykorzystywane w przemyśle turystycznym i archeologii podwodnej. Nowoczesne okręty przeznaczone do głębokiego nurkowania wywodzą się z batyskafu, który z kolei rozwinął się z tzw. dzwonu nurkowego.

Termin „okręt podwodny" oznacza „podwodny" lub „podmorski" (jak w rurociągu podwodnym), chociaż jako rzeczownik odnosi się ogólnie do statku, który może podróżować pod wodą. Termin ten jest skróconą wersją słowa *submarine boat* i występuje w takiej formie w kilku językach, np. francuskim (*sous-marin*) i hiszpańskim (*submarino*), chociaż inne zachowują oryginalny termin, np. holenderski (*Onderzeeboot*), niemiecki (*Unterseeboot*), szwedzki (*Undervattensbåt*) i rosyjski (*подводная лодка*: podvodnaya lodka), z których wszystkie oznaczają „łódź podwodną". W polskiej terminologii nautycznej do czasów II wojny światowej używano tego właśnie określenia. Obecnie termin „łódź podwodna" jest już archaizmem i powszechnie obowiązuje określenie „okręt podwodny".

Pierwsze próby z pojazdami podwodnymi podejmowano już w starożytności, a następnie w dobie renesansu. Jednakże debiut podwodnej jednostki bojowej miał miejsce dopiero w II połowie XIX stulecia. W 1864 r., pod koniec wojny secesyjnej należący do marynarki Konfederacji okręt podwodny CSS Hunley stał się pierwszym okrętem podwodnym, który zatopił wrogą jednostkę, slup wojenny Unii USS Housatonic, używając beczki wypełnionej prochem strzelniczym na maszcie jako swego rodzaju prymitywnego ładunku torpedowego. CSS Hunley również zatonął. Jednakże użycie okrętów podwodnych na pełną skalę nastąpiło dopiero

podczas I wojny światowej; było to związane z postępem techniki, przede wszystkim skonstruowaniem silnika elektrycznego mającego za źródło energii baterie akumulatorowe. Te z kolei były ładowane podczas marszu okrętu na powierzchni przy pracy spalinowej jednostki napędowej, którą były początkowo prymitywne silniki benzolowe (niezbyt bezpieczne w eksploatacji) zastąpione z czasem przez silniki Diesla. Jednak przed wybuchem pierwszego światowego konfliktu do okrętów podwodnych podchodzono z pewnym dystansem, traktując je raczej jako jednostki pomocnicze, przede wszystkim do zadań rozpoznawczych. Jak się wydaje, można wyrazić opinię, że przełomem w tym względzie był udany atak niemieckiego okrętu podwodnego U-9, który 22 września 1914 r. na Morzu Północnym, nieopodal Hoek van Holland zatopił w ciągu godziny 3 brytyjskie krążowniki pancerne. W latach 1914–1918 okręty podwodne, zarówno państw ententy, jak i mocarstw centralnych odniosły wiele spektakularnych sukcesów w atakach na jednostki przeciwnika. Niemiecka flota U-bootów – gdyby tylko prowadzono konsekwentnie nieograniczoną wojnę podwodną – mogła rozstrzygnąć światowy konflikt na korzyść II Rzeszy; po 1918 r. przyznawało to wiele autorytetów, z Winstonem Churchillem na czele.

W okresie międzywojennym okręty podwodne były przez większość czołowych flot mocarstw nadal traktowane jako jednostki drugorzędne. Pewnym wyjątkiem były Japonia i Włochy, natomiast ZSRR rozbudował swą podwodną flotę do monstrualnych rozmiarów. W przeddzień agresji III Rzeszy na ZSRR we flocie sowieckiej służyło prawie 300 okrętów podwodnych, z czego prawie 200 należało do typów pełnomorskich. Jednocześnie, mimo że traktaty międzynarodowe dotyczące wojny na morzu (zwłaszcza konwencja z 1936 r.) znacznie ograniczały swobodę ich działania wobec żeglugi handlowej, udoskonalano je technicznie. Pojawiły się też duże jednostki nazywane wręcz krążownikami podwodnymi, jak np. francuski Surcouf wypierający ponad 3 tys. t w położeniu nawodnym, a uzbrojony (oprócz torped) w 2 działa kalibru 203 mm. Z kolei Cesarska Marynarka Wojenna Japonii zbudowała w trakcie wojny podwodny krążownik lotniczy(!) I-400, wypierający ponad 5 tys. t w położeniu nawodnym, zabierający 3 wodnosamoloty. W trakcie tego konfliktu nieograniczoną wojnę podwodną prowadzili Niemcy na Atlantyku oraz

Amerykanie – na Pacyfiku. Flocie USA udało się niemal całkowicie odciąć japońskie wyspy macierzyste od dostaw drogą morską. Lata II wojny światowej przyniosły wiele udoskonaleń technicznych tej klasy okrętów; do najważniejszych zaliczyć można tzw. chrapy, urządzenie umożliwiające korzystanie z silników Diesla w zanurzeniu oraz nowy napęd (turbiny Waltera stosowane w okrętach typu XXII), który umożliwiał okrętom podwodnym rewelacyjną prędkość 20 w. zanurzeniu. Jednocześnie zrewolucjonizowano środki walki przeciw podwodnemu zagrożeniu; poczynając od lokalizacji zanurzonych okrętów podwodnych (ASDIC), a kończąc na samolotach, które stały się znaczącym zagrożeniem dla tej klasy okrętów.

Doświadczenia II wojny światowej przyczyniły się do znaczących zmian w budowie okrętów podwodnych i ich zastosowaniu, jednak prawdziwą rewolucją było zastosowanie technik jądrowej i rakietowej. Pierwsze wystrzelenie pocisku manewrującego (SSM-N-8 Regulus) z okrętu podwodnego miało miejsce w lipcu 1953 r. z pokładu USS Tunny, okrętu floty z czasów II wojny światowej zmodyfikowanego do przenoszenia pocisku z głowicą jądrową. Tunny i bliźniaczy Barbero były pierwszymi amerykańskimi okrętami podwodnymi patrolowymi z odstraszaniem nuklearnym. W latach 50. XX w. energia jądrowa częściowo zastąpiła napęd dieslowo-elektryczny; opracowano również sprzęt do wydobywania tlenu z wody morskiej. Te dwie innowacje dały okrętom podwodnym możliwość pozostawania w zanurzeniu przez tygodnie lub miesiące. Większość jednostek tego rodzaju marynarki wojennej zbudowanych od tego czasu w USA, Związku Sowieckim (obecnie Rosji), Wielkiej Brytanii i Francji jest napędzana reaktorem jądrowym. W latach 1959–1960 pierwsze okręty podwodne wyposażone w pociski balistyczne zostały oddane do służby przez Stany Zjednoczone (typ George Washington) i Związek Radziecki (typ projekt 629) w ramach strategii odstraszania nuklearnego z czasów zimnej wojny. Okręty z napędem nuklearnym były u progu swej działalności zawodne, co prowadziło do wielu wypadków i katastrof. Związek Radziecki stracił co najmniej 4 okręty podwodne w tym okresie: K-129 został utracony w 1968 r., K-8 – w 1970 r., K-219 – w 1986 r., i Komsomolec – w 1989 r. (który utrzymywał rekord głębokości wśród wojskowych okrętów podwodnych: 1000 m). Wiele innych sowieckich okrętów podwodnych, takich jak K-19 (pierwszy radziecki atomowy okręt podwodny i pierwszy

radziecki okręt podwodny, który dotarł do Bieguna Północnego), zostało poważnie uszkodzonych przez ogień lub wycieki promieniowania. USA straciły w tym czasie 2 atomowe okręty podwodne: USS Thresher (z powodu awarii sprzętu podczas nurkowania testowego, gdy był na granicy możliwości operacyjnych) i USS Scorpion (z nieznanych dotąd przyczyn).

Współcześnie okręty podwodne dzielą się zasadniczo na 4 podstawowe podklasy:

- okręty o napędzie nuklearnym przystosowane do przenoszenia pocisków balistycznych z głowicami nuklearnymi. Ich wyporność sięga 20 tys. t, a uzbrojone są w kilkanaście strategicznych pocisków balistycznych, z kilkoma głowicami jądrowymi każdy. Są zazwyczaj częścią strategicznych sił odstraszania nuklearnego, w wypadku Wielkiej Brytanii jedynym tego systemu elementem;
- okręty o napędzie nuklearnym uzbrojonym w konwencjonalne środki walki (np. rakiety samosterujące, torpedy). Ich wyporność wynosi około 4–6 tys. t. W chwili obecnej okręty te podobnie jak jednostki podwodne strategicznego przeznaczenia posiadają wyłącznie mocarstwa nuklearne;
- oceaniczne okręty podwodne o napędzie konwencjonalnym i konwencjonalnym uzbrojeniu. Ich wyporność waha się od około 1,5 tys. do 4 tys. t. W zasadzie wszystkie nowoczesne okręty tej podklasy zdolne są do rażenia nie tylko celów morskich, ale również (rakietami samosterującymi, a nawet pociskami balistycznymi) celów lądowych. Wyjątkowymi jednostkami w tej podklasie są okręty izraelskie typu Dolphin, które mają na swych pokładach rakietowe pociski samosterujące wyposażone w głowice nuklearne;
- przybrzeżne okręty podwodne, które mogą być używane zarówno do klasycznych działań morskich, jak i operacji o dywersyjnym charakterze.

Ze względu na zwiększone możliwości działań współczesnych okrętów podwodnych, a przede wszystkim rażenia celów lądowych (także ładunkami konwencjonalnymi dużej mocy) ich znacznie rośnie, co

skłania floty niekorzystające do tej pory z tych jednostek do podjęcia działań w celu ich pozyskania.

Roman Kochnowski

I. Ballantyne, *Podwodni myśliwi. Kulisy zimnej wojny pod wodą*, Rebis, Poznań 2015; T. Clancy, *Atomowe okręty podwodne*, Non stop press, Warszawa 1993; R. Jackson, *Okręty podwodne świata*, Rebis, Poznań 2001; L.M. Koldau, *Mythos U-Boot*, Steiner, Stuttgart 2010; *Los Angeles Class Submarine*, https://www.naval-technology.com/projects/la/ (dostęp 25.01.2025); J. Tall, *Unterseeboote und Tiefseefahrzeuge*, Kaiser, Klagenfurt 2002; I. Witkowski, *U-booty: historia niemieckich okrętów podwodnych*, WIS-2, Warszawa 2009.

OLIGARCHIA – forma rządów, w której władza polityczna skoncentrowana jest w rękach nielicznej, uprzywilejowanej oraz silnie powiązanej wewnętrznie grupy osób, zazwyczaj wywodzącej się ze środowisk arystokratycznych lub zamożnych elit ekonomicznych, w szczególności przedstawicieli wielkiego biznesu, dominujących w kluczowych sektorach gospodarki. Dysponując znacznymi zasobami finansowymi i kapitałem społecznym, oligarchowie uzyskują istotny wpływ na procesy decyzyjne w państwie i wywierają presję na osoby formalnie sprawujące władzę oraz instytucje publiczne. Elita rządząca w systemie oligarchicznym ma charakter zamknięty, a dostęp do najważniejszych stanowisk publicznych oraz rzeczywistej władzy jest ograniczony do jej członków. Decyzje polityczne podejmowane są przede wszystkim w celu ochrony i realizacji interesów tej grupy, często kosztem dobra wspólnego i interesów społecznych. Chociaż wewnątrz elity mogą występować konflikty i rywalizacja o wpływy, na zewnątrz oligarchia prezentuje spójny i jednolity front, skutecznie blokując możliwość udziału szerszych grup społecznych w sprawowaniu władzy.

Pojęcie „oligarchia" wywodzi się z języka greckiego, od wyrazów: *oligos* – „nieliczny", i *arche* – „władza", i oznacza rządy wąskich elit społecznych. Pierwszą definicję oligarchii jako systemu rządów stworzył Arystoteles i zawarł ją w swoim dziele *Polityka*. Rozumiał on oligarchię jako ustrój zwyrodniały, będący zdegradowaną formą arystokracji, w którym władza polityczna znajduje się w rękach nielicznej grupy osób posiadających majątek. Oligarcha rządzi zatem dla korzyści bogatych, a władza nie

służy dobru wspólnemu, ale interesom tej grupy. Arystoteles wyróżnił 4 typy oligarchii w zależności od stopnia koncentracji władzy ekonomiczno-politycznej:

1. Umiarkowana (instytucjonalna) – forma rządów, w której władzę sprawuje liczniejsza grupa zamożnych obywateli posiadająca majątek wystarczający do udziału w życiu publicznym, ale nie do całkowitej dominacji w państwie. W efekcie władza rozproszona jest w obrębie szerokiej grupy społecznej, a ponieważ uczestników życia publicznego jest wielu, muszą oni ustalić prawa, aby utrzymać władzę. Kluczową rolę w państwie odgrywają zatem instytucje i normy prawne, a nie arbitralne decyzje jednostek.
2. Węższa – oznacza rządy zamożnych, których jest stosunkowo niewielu, dlatego posiadają oni większą zdolność do artykulacji interesów i ich obrony w ramach instytucji politycznych. Bogata elita rządząca nie jest jednak na tyle potężna, aby sprawować władzę całkowicie poza regułami, dlatego dokonuje selektywnej modyfikacji prawa, tworząc rozwiązania ustrojowe, które zapewniają jej większą kontrolę nad procesem rekrutacji do urzędów (np. zwiększając cenzusy, komplikując procedury, narzucając dodatkowe kryteria).
3. Dziedziczna – rządy wąskiej grupy najbogatszych rodzin, które już nie tylko kontrolują procedury polityczne, ale je w pełni monopolizują; elita sama wyznacza siebie do pełnienia urzędów, wprowadzając prawne mechanizmy dziedziczenia funkcji publicznych, a prawo zostaje podporządkowane interesom dynastii politycznych. Aparat państwa zostaje zintegrowany z własnością prywatną elity, a mobilność polityczna jest w praktyce wykluczona.
4. Skrajna – najbardziej zdegenerowany wariant powstaje wtedy, gdy elita jest bardzo nieliczna, niezwykle bogata i dysponuje liczną siecią zwolenników. Władzę sprawują nie instytucje, lecz jednostki, a system zaczyna przypominać formę monarchii, w której potęga pojedynczych oligarchów staje się niemal absolutna. Dominacja elity staje się bezpośrednia, pozbawiona mechanizmów kontroli instytucjonalnej, a władza jest wykonywana w sposób arbitralny. Władza oligarchiczna ma często charakter nieformalny – oligarchowie nie muszą bezpośrednio pełnić funkcji publicznych, aby

skutecznie oddziaływać na procesy decyzyjne. Wystarczające jest posiadanie trwałego i znaczącego wpływu na kluczowe obszary życia politycznego i gospodarczego państwa.

Rządy oligarchiczne występowały w wielu epokach historycznych i przybierały zróżnicowane formy, w zależności od uwarunkowań społecznych, politycznych i gospodarczych. Już w starożytności charakter oligarchiczny posiadały niektóre greckie *polis*, rządy Sparty oraz starożytnego Rzymu. Występowały również w średniowiecznym państwie mameluków (Egipt – oligarchia wojskowa) oraz w Republice Weneckiej (oligarchia kupiecka). W czasach nowożytnych ustrój oligarchiczny istniał m.in. w XVII- i XVIII-wiecznej Rzeczypospolitej Obojga Narodów, w której dominującą pozycję polityczną uzyskała magnateria (oligarchia magnacka), a także w XVIII-wiecznej Wielkiej Brytanii, w której władza była skupiona w rękach arystokracji (oligarchia arystokratyczna). W XIX i XX w. cechy oligarchiczne dostrzegalne były również w Stanach Zjednoczonych, gdzie znaczący wpływ na politykę uzyskali przedstawiciele wielkiego kapitału i przemysłu (oligarchia przemysłowa). Współczesne przykłady oligarchii występują głównie w krajach byłego Związku Radzieckiego, np. w Rosji, Ukrainie czy Białorusi, w których kluczową rolę odgrywają tzw. oligarchowie paliwowi, często związani z sektorem surowcowym i energetycznym. Do państw wykazujących tendencje oligarchiczne zalicza się również Chiny, w których władza polityczna i gospodarcza skoncentrowana jest w rękach wąskiej elity partyjnej mającej decydujący wpływ na strategiczne sektory gospodarki oraz największe przedsiębiorstwa państwowe, a mechanizm przekazywania władzy odbywa się w obrębie zamkniętego, uprzywilejowanego kręgu, co sprzyja długotrwałemu utrzymywaniu wpływów przez te same grupy społeczne.

Systemy oligarchiczne najczęściej powstają w warunkach gwałtownych transformacji społeczno-politycznych, liberalizacji ustrojowej i gospodarczej oraz nieuporządkowanych procesów prywatyzacyjnych. Szczególnie sprzyja temu słabość instytucji państwowych, zwłaszcza brak realnej niezależności sądownictwa oraz niski poziom egzekwowania prawa. Oligarchia może wyłaniać się w systemach gospodarczych opartych na własności prywatnej i umożliwiających względnie swobodną akumulację kapitału, zwłaszcza gdy proces ten nie jest odpowiednio regulowany.

Państwa podatne na oligarchizację charakteryzują się zazwyczaj wysokim poziomem korupcji, selektywnym stosowaniem prawa oraz ograniczonym pluralizmem gospodarczym. Rynek w takich warunkach ulega silnej monopolizacji, a państwo nie sprawuje skutecznej kontroli nad strategicznymi sektorami gospodarki lub czyni to w sposób nieefektywny. Istotnym czynnikiem sprzyjającym rozwojowi tej formy rządzenia jest również uzależnienie polityki od prywatnego finansowania. W krajach, w których kampanie wyborcze generują wysokie koszty, partie polityczne pozostają zależne od sponsorów, a regulacje dotyczące lobbingu są niewystarczające lub nieobecne, dostęp do władzy uzyskują głównie te podmioty, które dysponują znacznymi zasobami finansowymi. Istotną rolę odgrywa również koncentracja mediów w rękach oligarchów, która umożliwia im kontrolowanie debaty publicznej, wywieranie presji na decydentów oraz kształtowanie poparcia społecznego dla sprzyjających im aktorów politycznych.

Główne cechy i uwarunkowania sprzyjające osobom zamożnym w uzyskaniu pozycji oligarchów to:

- ekstremalna, ponadprzeciętna koncentracja bogactwa – samo posiadanie znacznego majątku nie jest wystarczającym warunkiem uzyskania statusu oligarchy. Kluczowe znaczenie ma skala zasobów finansowych i kapitałowych, która umożliwia realne oddziaływanie na decyzje polityczne, społeczne i gospodarcze państwa. Oligarchowie często posiadają dominujący udział w strategicznych sektorach gospodarki, takich jak energetyka, sektor surowcowy i górniczy, telekomunikacja, bankowość, media, infrastruktura; dysponują ponadto zdolnością finansowania kampanii wyborczych, podmiotów medialnych oraz rozbudowanych sieci patronackich, co pozwala im trwale zabezpieczać i rozszerzać swoje wpływy w sferze publicznej;
- zdolność wykorzystywania zgromadzonego majątku do bezpośredniego oddziaływania na władzę polityczną – oligarcha pełni rolę swoistego pośrednika między sferą biznesu a aparatem państwowym, łącząc kapitał ekonomiczny z faktycznym wpływem politycznym m.in. poprzez tworzenie i utrzymywanie sieci zależnych polityków, lojalnych współpracowników oraz

protegowanych, a także w prowadzenie działań lobbingowych wykraczających poza standardowe, transparentne mechanizmy właściwe systemom demokratycznym. Ponadto oligarchowie posiadają możliwość wpływania na obsadę kluczowych stanowisk publicznych oraz kształt decyzji politycznych sprzyjających ich interesom gospodarczym, często bez konieczności zajmowania formalnych funkcji w strukturach władzy państwowej;

– zdolność do zabezpieczania i ochrony własnego majątku przy wykorzystaniu instrumentów władzy państwowej poprzez możliwość oddziaływania na kształt regulacji prawnych, w szczególności prawa podatkowego, a także na funkcjonowanie organów kontrolnych i nadzorczych. Dzięki temu oligarchowie są w stanie ograniczać lub neutralizować działania państwa wobec własnych interesów ekonomicznych, utrzymując swoisty „immunitet ekonomiczny", który chroni ich majątek przed skuteczną kontrolą czy sankcjami.

Oligarchia w państwach postsocjalistycznych narodziła się po 1989 r. i stanowi szczególny rodzaj oligarchii transformacyjnej. Jej powstaniu sprzyjały głębokie przemiany polityczne i gospodarcze następujące po upadku systemu komunistycznego, w szczególności liberalizacja gospodarek wcześniej centralnie planowanych oraz szeroko zakrojone procesy prywatyzacyjne. Zmiany te stworzyły warunki do szybkiej akumulacji kapitału, często w warunkach niepełnych regulacji prawnych oraz słabej kontroli instytucjonalnej, co umożliwiało praktyki nie zawsze zgodne z obowiązującym prawem. Na takim gruncie wyrosła elita biznesowa, którą tworzą przedstawiciele wielkiego prywatnego biznesu ściśle powiązanego i uzależnionego od władzy politycznej. Zależność ta miała często charakter wzajemny – biznes opierał swój rozwój na decyzjach politycznych i dostępie do zasobów publicznych, natomiast elity polityczne korzystały z finansowego i organizacyjnego wsparcia ze strony nowo powstałych grup ekonomicznych. W ten sposób ukształtował się trwały układ interesów stanowiący fundament systemów oligarchicznych w niektórych państwach postsocjalistycznych.

Współcześnie systemy oligarchiczne funkcjonują przede wszystkim w państwach byłego Związku Radzieckiego, takich jak Rosja, Ukraina, Białoruś, Mołdawia czy Kazachstan. Ich ukształtowanie i trwałość są rezultatem splotu pewnych uwarunkowań historycznych, politycznych i społeczno-gospodarczych. Do kluczowych czynników sprzyjających dominacji układów oligarchicznych w społeczeństwach poradzieckich należy zaliczyć: utrzymującą się pozycję dawnej elity radzieckiej, gwałtowny i słabo kontrolowany proces prywatyzacji majątku państwowego oraz mechanizm uwłaszczenia nomenklatury, prowadzący do podziału stref wpływów między wąskie grupy interesu. Istotną rolę odegrał również brak silnych i stabilnych instytucji państwowych w początkowej fazie transformacji ustrojowej, a także społeczne przyzwolenie na korupcję wynikające z niskiego poziomu kultury politycznej i słabego zakorzenienia norm demokratycznych. Szczególnie istotne znaczenie odegrała bardzo szybka i słabo nadzorowana prywatyzacja zasobów państwowych oraz majątku narodowego w latach 90. XX w., która doprowadziła do koncentracji ogromnych zasobów materialnych w rękach nielicznej grupy oligarchów. Ważnym podmiotem tego procesu była grupa tzw. „czerwonych dyrektorów", czyli dawnych menedżerów przedsiębiorstw państwowych, którzy – dążąc do zabezpieczenia własnej pozycji i zgromadzonego kapitału – rozpoczęli proces przekształcania zasobów ekonomicznych na wpływy polityczne. W ten sposób utrwalono mechanizm wzajemnego przenikania się władzy gospodarczej i politycznej, stanowiący fundament współczesnych systemów oligarchicznych w regionie poradzieckim.

Na terenie Rosji pierwsi oligarchowie pojawili się już w połowie lat 80. XX w., w okresie rządów Michaiła Gorbaczowa pełniącego funkcję sekretarza generalnego KC KPZR w latach 1985–1991. Proces liberalizacji gospodarczej realizowany w ramach pierestrojki ujawnił liczne luki prawne, które zostały szybko wykorzystane przez najbardziej przedsiębiorczych i najlepiej usytuowanych aktorów gospodarczych. Restrukturyzacja gospodarki ZSRR dopuściła ograniczoną działalność prywatną, umożliwiając m.in. import deficytowych i wysoko pożądanych towarów, takich jak komputery osobiste, sprzęt elektroniczny czy odzież (np. dżinsy). Ze względu na chroniczne niedobory na rynku radzieckim towary te były sprzedawane z bardzo wysokimi marżami, co pozwoliło na szybką

akumulację kapitału i stworzyło podstawy wyłonienia się nowej elity biznesowej. W Federacji Rosyjskiej właściwa oligarchia ukształtowała się jednak głównie w latach 90. XX w. Większość rosyjskich oligarchów to potentaci związani z sektorem paliwowo-energetycznym, którzy zgromadzili ogromne majątki w okresie prezydentury Borysa Jelcyna (1991–1999), a następnie umocnili swoją pozycję w czasie rządów Władimira Putina (od 1999). Po rozpadzie Związku Radzieckiego w 1991 r. oligarchowie wyłonili się jako przedsiębiorcy formalnie funkcjonujący na wolnym rynku, jednak ich sukces ekonomiczny był w znacznym stopniu uzależniony od powiązań z aparatem państwowym oraz relacji z elitami politycznymi. Dla rosyjskich oligarchów kluczowe wówczas znaczenie miała legalizacja zgromadzonego kapitału oraz zapewnienie bezpieczeństwa ekonomicznego i osobistego na terytorium własnego państwa. Z tego względu byli oni silnie zainteresowani utrzymaniem sprzyjającej im władzy politycznej, która gwarantowała możliwość legalnego prowadzenia działalności gospodarczej i spokojnego funkcjonowania w kraju. Zachowanie *status quo* miało również fundamentalne znaczenie dlatego, że znaczna część ich dochodów pochodziła z kontraktów państwowych, koncesji oraz bezpośrednich lub pośrednich związków z sektorem publicznym. W ten sposób utrwalił się model ścisłego powiązania wielkiego kapitału z władzą państwową, stanowiący rdzeń rosyjskiego systemu oligarchicznego.

Za jednego z pierwszych rosyjskich oligarchów uznaje się naukowca Borisa Bieriezowskiego, z wykształcenia matematyka i informatyka, który w późniejszym okresie zaangażował się również w działalność polityczną. Jego aktywność gospodarcza obejmowała m.in. sektor motoryzacyjny, energetyczny, finansowy oraz medialny, co pozwoliło mu na zbudowanie rozległego imperium ekonomicznego. Znaczną część swojego majątku zgromadził w latach 90. XX w., w okresie prezydentury Borysa Jelcyna, którego kampanie wyborcze wspierał finansowo, zyskując jednocześnie istotne wpływy polityczne. Jego stosunki z następcą Jelcyna – Władimirem Putinem – nie układały się jednak pomyślnie: oligarcha otwarcie krytykował kierunek polityki nowego prezydenta oraz wspierał finansowo środowiska opozycyjne, co doprowadziło do narastającego konfliktu z władzami rosyjskimi. W konsekwencji Bieriezowski opuścił Rosję i uzyskał azyl polityczny w Wielkiej Brytanii.

W 2013 r. został znaleziony martwy w swoim domu pod Londynem; wyniki śledztwa wykazały śmierć samobójczą.

Do grona najbardziej rozpoznawanych rosyjskich oligarchów zalicza się również Romana Abramowicza, którego działalność obejmuje przede wszystkim sektor naftowy i gazowy, a także rynek nieruchomości oraz sport zawodowy. Istotną pozycję w rosyjskiej oligarchii zajmował także Michaił Chodorkowski, związany głównie z przemysłem naftowo-gazowym, który w latach 90. XX w. zbudował jeden z największych prywatnych koncernów energetycznych w Rosji. Kolejną znaczącą postacią jest Aliszer Usmanow, aktywny w sektorach górniczym, metalurgicznym i telekomunikacyjnym, a także w obszarze metali szlachetnych i nowoczesnych technologii. Wśród innych znanych przedstawicieli rosyjskiej elity oligarchicznej wymienia się Michaiła Prochorowa, którego interesy obejmowały m.in. sektor surowcowy, nieruchomości, finanse oraz sport, a także Władimira Lisina, jednego z czołowych magnatów przemysłu metalurgicznego.

Również w Ukrainie ukształtował się system oligarchiczny, którego geneza sięga jeszcze okresu radzieckiego. Wówczas wykształciły się główne klany o charakterze terytorialno-branżowym, takie jak środowisko donieckie, dniepropietrowskie czy tzw. grupa kijowska. Po ogłoszeniu niepodległości Ukrainy w 1991 r. struktury te stały się podstawą instytucjonalizacji nowych grup oligarchicznych, które przejęły kontrolę nad kluczowymi sektorami gospodarki i stopniowo zaczęły odgrywać istotną rolę w życiu politycznym państwa. Proces kształtowania się dominujących grup oligarchicznych w Ukrainie odbywał się w 2 etapach; pierwszy obejmował gromadzenie kapitału na początku lat 90. XX w., gdy największym sojusznikiem oligarchii była zdominowana przez dawną partyjną nomenklaturę państwowa biurokracja. W drugim etapie ukształtowana już oligarchia zaczęła przekształcać kapitał ekonomiczny w polityczny. Środowiska oligarchów, powiązane z elitą władzy na poziomie ogólnokrajowym i regionalnym, zaczęły same tworzyć struktury biurokratyczne, na które mogły wywierać wpływ. Uformował się zatem system powiązań organów państwowych z oligarchami polegający na korupcji politycznej, która stała się niezbędnym elementem istnienia i funkcjonowania oligarchii.

W Ukrainie powstało kilkanaście wpływowych grup oligarchicznych, które w znacznym stopniu decydowały o rozwoju establishmentu politycznego. Do najważniejszych ośrodków należy zaliczyć grupę Rinata Achmetowa (m.in. branża metalurgiczna i górnicza, energetyka, bankowość, telekomunikacja, sport), która wywodziła się z klanu donieckiego i w różnych okresach odgrywała bardzo istotne role w kontekście kierunku rozwoju kraju. Z kręgu dniepropietrowskiego wywodzili się najbardziej wpływowi oligarchowie Ukrainy od początku transformacji ustrojowej, m.in. Ihor Kołomojski, aktywny biznesmen w sektorze finansowym, medialnym, energetycznym i transportowym, oraz Hennadij Boholubow, związany przede wszystkim z branżą metalurgiczną, finansową i energetyczną. Istotną cechą ukraińskiego systemu oligarchicznego jest bezpośrednie zaangażowanie najwyższych przedstawicieli władzy państwowej w działalność biznesową. Przykładem jest Wiktor Janukowycz, który w czasie swojej prezydentury (2010–2014) stworzył rozbudowany system powiązań polityczno-biznesowych określany mianem Familii. Układ ten opierał się na koncentracji wpływów gospodarczych wokół wąskiego kręgu osób lojalnych wobec prezydenta i stanowił jedną z najbardziej scentralizowanych form oligarchicznej kontroli państwa w historii Ukrainy. Po wydarzeniach Euromajdanu zaczęły umacniać się środowiska powiązane z Petrem Poroszenką, będącym jednocześnie przedsiębiorcą i politykiem (prezydent w latach 2014–2019). Jego zaplecze gospodarcze obejmowało m.in. przemysł cukierniczy, sektor medialny, branżę motoryzacyjną oraz przemysł ciężki, co wpisywało się w utrwalony w Ukrainie model łączenia władzy politycznej z kapitałem prywatnym. Do wpływowych oligarchów ukraińskich należą również m.in. Dmytro Firtasz (branża chemiczna i energetyczna), Wiktor Pinczuk – zięć byłego prezydenta Leonida Kuczmy (branża metalurgiczna, medialna, finansowa) oraz Serhij Tihipko (branża finansowa).

Na Białorusi uwarunkowania sprzyjające wyłonieniu się oligarchii wiązały się przede wszystkim z dezorganizacją funkcjonowania państwa po rozpadzie Związku Radzieckiego. Słabość instytucji publicznych i brak stabilnych ram prawnych stworzyły sprzyjające środowisko dla szybkiej akumulacji kapitału przez najbardziej przedsiębiorcze i najlepiej usytuowane jednostki. W tych warunkach na początku lat 90. XX w. pojawili się

pierwsi znaczący białoruscy przedsiębiorcy, określani mianem „oligarchów pierwszej fali". Rozpoczynali oni działalność od zakładania niewielkich firm prywatnych, które w krótkim czasie przekształcały się w przedsiębiorstwa o zasięgu ogólnokrajowym. Należeli do nich m.in. Siarhiej Bruekker działający w branży finansowej, budowlanej i metalurgicznej; Leanid Wouk będący pierwszym białoruskim przedsiębiorcą inwestującym w wydobycie metali szlachetnych czy Alaksander Pupiejko, często uważany za pierwszego prawdziwego oligarchę białoruskiego, który swój majątek zbudował w oparciu o inwestycje w przemysł samochodowy.

Proces oligarchizacji na Białorusi uległ wyraźnemu spowolnieniu po 1996 r., wraz z konsolidacją władzy Aleksandra Łukaszenki. Zatrzymano wówczas rozwijający się proces prywatyzacji, a państwo odzyskało bezpośrednią kontrolę nad kluczowymi sektorami gospodarki. Jednocześnie nowo wyłaniającym się elitom ekonomicznym przekazano jednoznaczny sygnał, że prowadzenie dochodowej działalności gospodarczej jest możliwe wyłącznie pod warunkiem lojalnej współpracy z obozem władzy, akceptacji silnej roli państwa w redystrybucji zysków oraz całkowitego wycofania się z niezależnej aktywności politycznej. W rezultacie ukształtował się specyficzny model relacji między biznesem a państwem, odmienny od klasycznej oligarchii znanej z Rosji czy Ukrainy. Białoruscy przedsiębiorcy zostali podporządkowani władzy politycznej i pozbawieni autonomii politycznej, a ich funkcjonowanie uzależniono od decyzji aparatu państwowego. Spowodowało to powstanie w latach 2007–2008 grupy tzw. „oligarchów nomenklaturowych", która działa na zasadzie klanu, kontrolując praktycznie cały prywatny sektor białoruskiej gospodarki, i była powiązana z prezydentem lub członkami jego rodziny relacjami na zasadzie patronatu. Trzon oligarchii nomenklaturowej składał się z kilkunastu wpływowych i powiązanych z elitą rządzącą przedsiębiorców; należeli do niej m.in. Juryj Czyż (branża spożywcza, nieruchomości, energetyka), Uładzimir Piefcijeu (handel bronią) czy Anatol Cierniauski (branża energetyczna i nieruchomości). Inni wpływowi białoruscy oligarchowie to m.in. właściciel centrów handlowych i potentat rynku tytoniowego Pawieł Tapuzidzis, działający w przemyśle ciężkim Alaksandr Szakucin czy związani z sektorem rolniczym Jauhien Baskin i Alaksandr Maszenski. Współczesny trzon białoruskiego klanu oligarchów tworzy grupa

kilkudziesięciu najbardziej wpływowych i najbogatszych biznesmenów. Jest to struktura zamknięta, z szerokimi powiązaniami polityczno-gospodarczymi w całym kraju, pośrednio lub bezpośrednio związana z elitami władzy, a przede wszystkim – z rodziną Łukaszenków.

Środowisko białoruskiej oligarchii charakteryzują 4 podstawowe cechy odróżniające je m.in. od oligarchii ukraińskiej czy rosyjskiej, ponieważ białoruski oligarcha:

- nie może angażować się w politykę, a jedynym wyjątkiem jest wspieranie władzy (np. Szakucin był senatorem i zasiadał we władzach największej proprezydenckiej organizacji Biała Ruś, a Tapuzidzis często pełnił funkcję przewodniczącego komisji wyborczych podczas wyborów prezydenckich);
- powinien wspierać inicjatywy sportowe i kulturalne – praktycznie każdy z wymienionych biznesmenów jest członkiem albo przewodniczącym federacji konkretnej dyscypliny sportowej, wspiera drużynę sportową, promuje białoruskich zawodników lub wspiera budowę pałaców lodowych czy stadionów;
- musi być lojalny i w razie potrzeby wspierać państwo, dzięki przychylności którego prowadzi biznes i posiada majątek; najczęściej wyraża się to we współfinansowaniu spektakularnych i dużych inwestycji państwowych albo poprzez wzięcie pod osobistą pieczę upadających przedsiębiorstw;
- musi liczyć się z tym, że przynależność do grupy nomenklaturowych oligarchów nie zapewnia mu bezpieczeństwa i stabilnej sytuacji finansowej.

Rozpad Związku Radzieckiego stworzył również w Mołdawii sprzyjające warunki do wykształcenia się struktur oligarchicznych. Podobnie jak w innych państwach postsowieckich, pozycję oligarchów uzyskiwały przede wszystkim osoby utrzymujące bliskie relacje z przedstawicielami aparatu władzy wywodzącymi się z dawnej elity politycznej ZSRR. Szybki wzrost ich zasobów materialnych był w dużej mierze efektem nieprzejrzystych procesów prywatyzacji majątku państwowego oraz przejmowania najbardziej dochodowych przedsiębiorstw prywatnych w warunkach słabej kontroli instytucjonalnej. Kolejnym etapem realizacji tego modelu było zaangażowanie oligarchów w działalność polityczną. Z jednej strony,

zgromadzony majątek zapewniał środki finansowe niezbędne do prowadzenia kampanii wyborczych i budowania zaplecza politycznego, z drugiej zaś – wymagał zabezpieczenia poprzez uzyskanie wpływu na procesy decyzyjne państwa. W efekcie powstał mechanizm wzajemnej zależności między wielkim kapitałem a władzą publiczną, w którym uczestnictwo w polityce stało się kluczowym narzędziem ochrony interesów ekonomicznych oraz utrwalania pozycji oligarchicznej. W taki sposób swoją pozycję zbudował m.in. Władimir Plahotniuc – biznesmen działający w branży rozrywkowej, energetycznej i bankowo-finansowej, a następnie polityk – przywódca Demokratycznej Partii Mołdawii (PDM). Jego osobisty majątek w pewnym czasie stanowił równowartość niemal 1/3 budżetu całego państwa. Do grona najbardziej wpływowych osób w państwie należał również biznesmen Igor Dodon – późniejszy prezydent i nieoficjalny lider prorosyjskiej Partii Socjalistów Republiki Mołdawii (PSRM). Kontakty z Rosją były również źródłem jego prywatnego majątku: pełniąc funkcję ministra gospodarki, miał się wzbogacić na wydawaniu specjalnych zezwoleń w obszarze prowadzonej z tym krajem wymiany handlowej, dotyczyło to m.in. grupy mołdawskich producentów żywności oraz eksportowania produktów alkoholowych na rosyjski rynek pomimo nałożonego przez Moskwę embarga. Inny biznesmen Ilan Sor prowadził aktywną działalność w sferze politycznej jako założyciel populistycznej partii SOR i późniejszy burmistrz Orgiejowa. Jednocześnie prowadził działalność biznesową m.in. w branży finansowej, transportowej i rozrywkowej.

Wszyscy 3 wspomniani oligarchowie mołdawscy wykazują wiele wspólnych cech charakterystycznych dla postsowieckiego modelu oligarchii: ich działalność gospodarcza opierała się w znacznym stopniu na dochodach pochodzących z niejasnych lub nieprzejrzystych źródeł, a oni sami byli wielokrotnie podejrzewani o udział w malwersacjach finansowych oraz praktykach korupcyjnych. Uzyskiwanie i utrwalanie wpływów politycznych następowało przede wszystkim poprzez bliskie relacje z przedstawicielami aparatu władzy, a następnie było rozszerzane dzięki budowaniu powiązań o charakterze klanowym oraz tworzeniu tzw. partii wodzowskich. Ugrupowania polityczne kontrolowane przez oligarchów miały zazwyczaj silnie scentralizowaną strukturę, podporządkowaną interesom lidera, a prywatne środki finansowe oligarchów stanowiły

podstawowe źródło ich funkcjonowania. Głównym celem tych formacji była ochrona zdobytych wpływów politycznych oraz zabezpieczenie źródeł dochodów, w tym również tych o wątpliwej legalności. Wspólne doświadczenia transformacyjne oraz podobne mechanizmy działania doprowadziły do zbieżności interesów poszczególnych oligarchów i wytworzenia między nimi trwałego układu wzajemnych zależności polityczno-biznesowych, który dodatkowo wzmacniał ich pozycję w systemie władzy.

W Kazachstanie, podobnie jak w innych państwach poradzieckich, struktury oligarchiczne zaczęły kształtować się po rozpadzie ZSRR w 1991 r. Kluczową rolę odegrał proces prywatyzacji, w wyniku którego wyłoniła się wąska grupa osób – często powiązanych bezpośrednio lub pośrednio z rodziną prezydenta Nursułtana Nazarbajewa – która przejęła kontrolę nad strategicznymi sektorami gospodarki. Szczególne znaczenie miały zasoby surowcowe, takie jak ropa naftowa, gaz ziemny oraz górnictwo, stanowiące podstawę kazachskiej gospodarki i źródło nadzwyczajnych zysków. W takich warunkach politycznych narodziła się fortuna m.in. córki prezydenta Nazarbajewa – Dinary – i jej męża Timura Kulibajewa, którzy przejęli branżę finansową oraz sektor surowcowo-energetyczny, a także Almasa Sultangazina prowadzącego biznesy w sektorze elektronicznym, nieruchomości oraz medialno-rozrywkowym. Do tego grona zaliczyć można również Daniyara Abulgazina (sektor paliwowy i energetyczny, transport, elektronika); Vyacheslava Kima działającego głównie w zakresie bankowości cyfrowej i usług finansowych oraz nowych technologii; Timura Turlova prowadzącego działalność w zakresie usług finansowych, bankowości, usług cyfrowych i ubezpieczeń; Vladimira Kima – biznesmena w obszarze wydobycia i produkcji metali, a także Bulata Utemuratova prowadzącego biznes w branży bankowej i inwestycyjnej oraz górnictwie złota i hotelarstwie.

W następstwie kryzysu politycznego oraz masowych protestów społecznych w 2022 r. w Kazachstanie zainicjowano politykę deoligarchizacji. Polegała ona głównie na ograniczaniu wpływów dawnych grup związanych z erą Nazarbajewa oraz odzyskiwaniu majątku uznanego za nielegalnie przejęty. Kluczowym jej instrumentem była ustawa z 12 lipca 2023 r. o zwrocie do państwa nielegalnie nabytych aktywów, która przewidywała dobrowolny i przymusowy (sądowy) tryb odzyskiwania aktywów oraz

mechanizmy zabezpieczania majątku. Proces ten nie doprowadził jednak do pełnej deoligarchizacji w sensie systemowym. Jego skuteczność była ograniczona przede wszystkim przez brak trwałych, transparentnych i instytucjonalnie zakorzenionych reguł, które w sposób konsekwentny redukowałyby wpływ wielkiego kapitału na władzę publiczną. W rezultacie działania deoligarchizacyjne miały w dużej mierze charakter pokazowy oraz wizerunkowo-symboliczny, nie prowadząc do zasadniczej przebudowy relacji między państwem a elitami ekonomicznymi.

System oligarchiczny, niezależnie od kontekstu geograficznego, wywiera zazwyczaj negatywny wpływ na procesy demokratyczne w państwie. Wynika to przede wszystkim z koncentracji znacznych zasobów majątkowych i politycznych w rękach wąskiej grupy osób, co prowadzi do nierównego dostępu do władzy oraz utrudnia realizację reform gospodarczych i instytucjonalnych. Oligarchizacja sprzyja rozwojowi takich zjawisk, jak korupcja, nepotyzm oraz erozja zasad równości, przejrzystości i odpowiedzialności w życiu publicznym. W praktyce oligarchowie często dążą do bezpośredniego lub pośredniego wpływania na system polityczny poprzez utrzymywanie bliskich relacji z decydentami, finansowanie kampanii wyborczych, a niekiedy także osobiste sprawowanie funkcji publicznych. Mechanizmy te prowadzą do wykształcenia swoistego „społeczeństwa oligarchicznego", w którym władza polityczna pozostaje w rękach dominujących podmiotów gospodarczych. Państwo w takim układzie koncentruje się na ochronie interesów i praw własności głównych producentów, jednocześnie tworząc istotne bariery wejścia na rynek dla nowych przedsiębiorców, co ogranicza konkurencję i hamuje rozwój gospodarczy oraz demokratyczny.

Sabina Olszyk

D. Acemoglu, *Oligarchic Versus Democratic Societies*, „Journal of the European Economic Association" 2008, vol. 6, no. 1, https://economics.mit.edu/sites/default/files/publications/oligarchic%20vs%20democratic%20societies.pdf (dostęp 17.12.2025); Aristoteles, *Polityka*, Wydawnictwo Naukowe PWN, Warszawa 2006; K. Bacewicz, *Oligarchia a wybory parlamentarne w Republice Mołdawii w 2019 r.*, „Sprawy Międzynarodowe" 2020, t. 73, nr 4, https://doi.org/10.35757/SM.2020.73.4.04 (dostęp 17.12.2025); *Oligarchia*, [w:] *Encyklopedia zarządzania*,

https://mfiles.pl/pl/index.php/Oligarchia (dostęp 17.12.2025); R. Kęsek, *Oligarchia w życiu politycznym i gospodarczym wybranych państw postsowieckich. Perspektywa porównawcza*, „Politeja” 2023, t. 20, nr 2, https://doi.org/10.12797/Politeja.20.2023.83.08 (dostęp 17.12.2025); M. Rust, *Poradziecka oligarchizacja Ukrainy i Białorusi: procesy, mechanizmy, perspektywy*, „Sprawy Międzynarodowe” 2020, t. 73, nr 4, https://doi.org/10.35757/SM.2020.73.4.03 (dostęp 17.12.2025); J.A. Winters, *Oligarchy*, Cambridge University Press, Cambridge 2011, https://assets.cambridge.org/97805211/82980/frontmatter/9780521182980_frontmatter.pdf (dostęp 17.12.2025).

OPERACJA „PAJĘCZYNA” (ukr. *операція «Павутина»*) – specjalna operacja sabotażowa Służby Bezpieczeństwa Ukrainy, jedna z największych, która została przeprowadzona 1 czerwca 2025 r. na terytorium Rosji.

Operacja miała na celu uderzenie w lotnictwo strategiczne Rosji tysiące mil od własnego terytorium podczas pełnoskalowej wojny rosyjsko-ukraińskiej. Skoordynowane ataki były wymierzone w zasoby lotnictwa dalekiego zasięgu rosyjskich sił powietrznych na 5 bazach lotniczych, na których stacjonowały rosyjskie samoloty strategicznego lotnictwa: Olenija w obwodzie murmańskim (2000 km), Biełaja w obwodzie irkuckim (4300 km), Diagilew w obwodzie riazańskim (700 km), Iwanowo w obwodzie iwanowskim (900 km) i Ukrainka w obwodzie amurskim. Atak na bazę lotniczą Biełaja był pierwszą ukraińską akcją we wschodniej Syberii od początku wojny rosyjsko-ukraińskiej, podczas której potwierdzono uszkodzenia samolotów. Szczególnie udany był atak na bazę strategicznych lotniskowców rakietowych Tu-95MS w bazie Olenija, gdzie drony celnie trafiały w zbiorniki paliwa, a znaczna liczba samolotów doszczętnie spłonęła.

W przeciwieństwie do innych celów, atak na bazę lotniczą Ukrainka w obwodzie amurskim nie powiódł się, ponieważ ciężarówka z dronami eksplodowała po drodze, na autostradzie Czyta-Chabarowsk, w pobliżu Seriszewa.

Operacja o takiej skali i o takim efekcie ekonomicznym i militarnym, na tak wysokim poziomie technologicznym, nie miała miejsca w praktyce światowej. Oprócz spowodowania zniszczeń materialnych stała ważnym sygnałem nie tylko dla Rosji, ale także zachodnich sojuszników Ukrainy.

Ukraińska operacja „Pajęczyna” była poważnym ciosem i doprowadziła do kosztownych konsekwencji dla Rosji. Obywatele tego państwa

uważali, że ich strategiczne lotnictwo jest bezpieczne, zaś po atakach ogłoszono stan wyjątkowy w odniesieniu do baz lotniczych Engels i Morozowsk z powodu możliwego zagrożenia powietrznego. Bombowce, które nie zostały zniszczone, zaczęto od razu przerzucać do najbardziej oddalonych baz lotniczych na Czukotce i Kamczatce. Oprócz tego zwrócono uwagę na potrzebę wzniesienia umocnień, zainstalowania naprowadzanych radarowo dział i zagłuszarek urządzeń elektronicznych, budowę schronów lub hangarów, aby osłonić możliwe wektory ataku.

Operacja „Pajęczyna” pokazała, że Ukraina jest w stanie zaatakować ważne cele w dowolnym miejscu w Rosji, upokarzając Kreml i zadając znaczne straty moskiewskiej machinie wojennej.

Według *World Air Forces na początku 2025 r. rosyjskie siły powietrzne i kosmiczne miały 57 samolotów Tu-22M3, 47 – Tu-95MS, oraz 15 – Tu-160. Military Balance również podawał, że rosyjskie lotnictwo dalekiego zasięgu miało 57 samolotów Tu-22M3, 58 – Tu-95MS, i 13 bombowców Tu-160. Wszystkie mogły przenosić broń jądrową. Bardzo ważne wydaje się również uwzględnienie faktu, że samoloty te nie są już produkowane, a zatem nie można ich zastąpić nowymi modelami.*

Operację osobiście nadzorował prezydent Ukrainy Wołodymyr Zełenski, a bezpośrednio realizowali ją szef SBU Wasyl Maluk i pracownicy służby.

Niektórzy specjaliści nazwali zuchwały atak na rosyjskie bombowce strategiczne z 1 czerwca 2025 r. operacją „Trojańska ciężarówka”, odnosząc się do zamaskowanych pojazdów, które dostarczały drony w pobliżu strategicznych baz lotniczych Rosji. Zniszczone bombowce były używane do bombardowania Ukrainy od 2022 r.

Głównym środkiem zniszczenia lotnictwa strategicznego FR były drony FPV Osa ukraińskiej firmy First Contact, z których ponad 100 zostało zdalnie wystrzelonych z ciężarówek znajdujących się blisko do lotnisk. Według charakterystyki Osa jest w stanie unieść do 3,3 kg ładunku bojowego, utrzymuje się w powietrzu do 15 minut i przyspiesza do 150 km/h, co pozwala jej precyzyjnie trafiać w cele nawet przy silnym wietrze. Niektóre źródła twierdzą, że drony miały wbudowane elementy sztucznej inteligencji – do wykrywania i namierzania wrażliwych części samolotów.

Była to jedna z najtrudniejszych i starannie zaplanowanych operacji specjalnych z logistycznego punktu widzenia, przygotowywano ją przez ponad półtora roku. W tym czasie drony były dostosowywane do rozpoznawania celów, wykorzystano m.in. egzemplarze Tu-22M3 zgromadzone w Muzeum Lotnictwa Dalekiego Zasięgu i Lotnictwa Strategicznego w Połtawie. Celem szkolenia było nauczenie sztucznej inteligencji prawidłowej identyfikacji określonych obiektów oraz trafienie samolotów w ich najbardziej wrażliwe miejsca.

Najpierw SBU nielegalnie przetransportowała do Federacji Rosyjskiej 150 małych dronów szturmowych i 300 sztuk amunicji, a potem przeładowano je do drewnianych kontenerów startowych, które zamontowano na ciężarówkach i przetransportowano do co najmniej 4 lokalizacji oddalonych od siebie o tysiące kilometrów. Ataki przeprowadzono z ciężarówek znajdujących się w pobliżu lotnisk wojskowych. Wraz z rozpoczęciem operacji dachy kontenerów zostały otwarte zdalnie, a drony kierowały się w stronę swoich celów – bombowców strategicznych na lotniskach wojskowych.

Kontrola odbywała się za pośrednictwem rosyjskich sieci telekomunikacyjnych, a kilka mobilnych punktów startowych na terytorium FR znajdowało się w pobliżu baz rosyjskiego lotnictwa strategicznego. Taki atak jest pierwszym w historii świata przypadkiem, kiedy główne siły lotnictwa strategicznego, nośniki broni jądrowej, zostały pokonane bezpośrednio w swoich bazach przez grupowy atak dronów.

Podczas operacji wykorzystano nowoczesną technologię sterowania bezzałogowymi statkami powietrznymi, która łączy autonomiczne algorytmy sztucznej inteligencji i ręczną interwencję operatora. W szczególności z powodu utraty sygnału część dronów przełączyła się na wykonywanie misji z wykorzystaniem AI wzdłuż zaplanowanej wcześniej trasy, a po zbliżeniu się i nawiązaniu kontaktu ze specjalnie wyznaczonym celem głowica bojowa została automatycznie wyzwolona.

Drony były sterowane przez wersję ArduPilot, oprogramowania typu open source, który jest bezpłatny i może być modyfikowany przez każdego w różnych celach. Oprogramowanie można sparować z domowym dronem, wyświetla mapę obszaru z dostępem do GPS, umożliwia tworzenie punktów orientacyjnych i wydaje polecenia bezzałogowemu statkowi

powietrznemu. Jeśli GPS i autopilot są niedostępne z powodu okoliczności, działają inne funkcje pomocnicze. Program może automatycznie stabilizować drona w powietrzu, podczas gdy pilot skupia się na poruszaniu się do następnego celu. Piloci mogą przełączyć drona w tryb krążący, a także są tryby bezpieczeństwa, które utrzymują go w powietrzu w przypadku utraty sygnału. Drony komunikowały się ze swoimi ukraińskimi opiekunami za pośrednictwem rosyjskich sieci komórkowych.

Kierowcy ciężarówek byli przekonani, że przewożą domy szkieletowe; otrzymali zamówienie od przedsiębiorcy z obwodu murmańskiego, załadowali towary i ruszyli w drogę. Podczas jazdy nieznana osoba skontaktowała się z nimi telefonicznie i udzieliła instrukcji, gdzie i kiedy mają się zatrzymać. Jednemu z kierowców kazano zaparkować ciężarówkę na stacji benzynowej Rosnieft, w pobliżu lotniska wojskowego, po czym stamtąd wystrzelono drony.

W trakcie operacji udało się uderzyć w wiele samolotów wroga naraz. Służba Bezpieczeństwa Ukrainy poinformowała, że w wyniku specjalnej operacji, która obejmowała jednoczesne ataki na 4 lotniska wojskowe w Rosji, zniszczono 41 rosyjskich samolotów strategicznych, w tym Tu -95MS, Tu-22M3 i Tu-160, a także poważnie uszkodzono albo zniszczono samoloty radarowe A-50, których Rosja używała do wystrzeliwania rakiet dalekiego zasięgu. Operacja wyróżniała się bezprecedensowym zasięgiem geograficznym, obejmującym 5 obwodów w 3 strefach czasowych, a szacunkowy koszt zniszczonych samolotów strategicznych i pocisków manewrujących wroga wynosi ponad 7 mld dolarów, przy użyciu dronów o wartości 2 tys. dolarów.

Zniszczono 34% strategicznych lotniskowców i pocisków manewrujących na głównych lotniskach Federacji Rosyjskiej. To nie była tylko eliminacja samolotów wroga, ale poważny cios dla kraju.

Zdjęcia satelitarne i nagrania z dronów potwierdziły zniszczenie lub uszkodzenie co najmniej 8 bombowców Tu-95MS (około 6 z nich uzbrojonych w pociski manewrujące Ch-101); 7–12 bombowców Tu-22M-3, 2 samolotów radarowych dalekiego zasięgu A-50, 1 samolotu transportowego An-12 i prawdopodobnie 1 samolotu tankującego Ił-78M. Według Toma Coopera – austriackiego analityka i dziennikarza śledczego specjalizującego się w lotnictwie wojskowym – zniszczeniu uległo 70–100% „w pełni

gotowej do walki” floty rosyjskich Tu-95MS i około 30% gotowej do walki floty Tu-22M3.

Już na 2 i 3 dzień po ataku Rosjanie próbowali zatuszować straty, transportując ocalałe bombowce w celu zastąpienia spalonych, aby uszkodzone samoloty nie były widoczne na zdjęciach satelitarnych: na tych z 2 czerwca 2025 r. na jednym z zaatakowanych lotnisk widać spalony Tu-95, zaś 4 czerwca w pełni sprawny samolot stoi już na swoim miejscu – dokładnie w takiej samej pozycji jak wcześniej, choć widać spalone lotnisko.

Rosjanie nie mogą zastąpić żadnego z tych samolotów, bo nie są produkowane od 25 lat (lub dłużej). W przypadku A-50 nie są w stanie nawet dokonać przeglądu i naprawy, zaś odbudowa Tu-95MS jest bardzo czasochłonna i droga. Oznacza to zniwelowanie zagrożenia dla Ukrainy na co najmniej miesiąc, a prawdopodobnie na dłużej.

Ponadto drony uszkodziły rosyjską bazę okrętów podwodnych z napędem atomowym w mieście Siewieromorsk.

Operacja „Pajęczyna” była uznana za historyczną i bezprecedensową pod względem skali i szkód wyrządzonych przeciwnikowi. Jak podkreślił Zełenski, punkt kontroli operacji znajdował się w pobliżu jednego z regionalnych oddziałów FSB, w jednym z regionów Federacji Rosyjskiej. Był to największy atak dronów na rosyjskie bazy lotnicze do tego momentu wojny, w którym wykorzystano 117 dronów i – odpowiednio – taką samą liczbę operatorów bezzałogowych statków powietrznych.

Według licznych źródeł ukraińskich i amerykańskich Stany Zjednoczone nie brały udziału w operacji „Pajęczyna” i nie miały informacji o planach Ukrainy dotyczących ataku na rosyjskie lotniska, a Ukraina zbierała informacje wywiadowcze niezależnie, bez wsparcia USA. Decyzja ta była podyktowana częściowo obawami o wyciek tajnych informacji.

Operacja „Pajęczyna” dowodzi, że innowacje i nowe technologie odgrywają decydującą rolę w tej wojnie i zmieniają sytuację na polu bitwy, a Ukraina jest zdolna do podejmowania skutecznych decyzji taktycznych w wojnie z Federacją Rosyjską i może zadać wrogowi znaczne straty. Podkreślił to prezydent Ukrainy podczas szczytu Bukaresztańskiej Dziewiątki i państw nordyckich w Wilnie 2 czerwca 2025 r.

Okupanci uważali, że bazy lotnicze położone głęboko w Federacji Rosyjskiej są bezpieczne. Działania Służby Bezpieczeństwa Ukrainy wywołały

gniew i niepokój Kremla, ujawniając słabości zabezpieczeń rosyjskiej „jądrowej” floty powietrznej. Bloomberg opisuje to, powołując się na osoby bliskie wysokim rangą urzędnikom Kremla.

Po szeroko zakrojonej operacji Służby Bezpieczeństwa Ukrainy, która doprowadziła do znacznych strat w rosyjskim lotnictwie strategicznym, oficjalna reakcja Kremla była powściągliwa. Rosyjskie media państwowe próbowały umniejszyć znaczenie ataku, nie podając szczegółowych informacji o skali zniszczeń. Ten szeroko zakrojony atak wywołał w Rosji krytykę wewnętrzną dotyczącą bezpieczeństwa obiektów wojskowych i skuteczności obrony powietrznej. Niektórzy rosyjscy eksperci wojskowi uznali potrzebę przeglądu strategii obronnych i modernizacji systemów obrony powietrznej. Ogólnie rzecz biorąc, operacja SBU stała się poważnym wyzwaniem dla rosyjskiej machiny wojskowej.

Kaja Kallas, Wysoki Przedstawiciel Unii Europejskiej do Spraw Zagranicznych i Polityki Bezpieczeństwa, na spotkaniu ministrów obrony NATO w Brukseli 5 czerwca 2025 r. stwierdziła, że ukraińskie ataki dronów na rosyjskie strategiczne lotnictwo wojskowe „przepisują historię wojskowości”. Podkreśliła, że specjalna operacja o kryptonimie „Pajęczyna” pokazała, jak stosunkowo niedrogie drony mogą niszczyć niezwykle kosztowne samoloty, zmieniając tym samym istotę współczesnej wojny.

Ukraińskie ataki mogą mieć również pośrednie konsekwencje: ujawniły one poważne niedociągnięcia w organizacji rozmieszczenia samolotów strategicznych na lotniskach. Najwyraźniej drony swobodnie przekazywały sygnały podczas lotu, co może oznaczać, że w rejonie lotnisk nie działały żadne systemy walki elektronicznej. Podczas nalotów nie pojawiły się w prasie i blogosferze żadne doniesienia o ostrzale celów powietrznych przez systemy obrony powietrznej, ani nawet po prostu z broni ręcznej. Tu-95MS stały bez osłony na otwartym terenie. Sądząc po zdjęciach satelitarnych, Tu-22M3b znajdowały się na chronionych parkingach, ale osłona obejmowała jedynie nasypy.

Głównym skutkiem operacji „Pajęczyna” było nie tylko zniszczenie rosyjskich bombowców strategicznych, ale całkowita utrata kontroli rosyjskich służb specjalnych nad sytuacją wewnątrz państwa, co może bardzo poważnie wpłynąć na przebieg i perspektywy wojny. Głównym szokiem dla Rosji było uświadomienie, że ukraińskie służby specjalne są w stanie

działać wewnątrz Rosji niezauważone i przez długi czas. To właśnie podważa skuteczność rosyjskich służb specjalnych.

Konsekwencje nalotu ukraińskich bezzałogowych statków powietrznych na rosyjskie bazy lotnicze to:

- zniszczenie sprzętu wojskowego wartego miliardy dolarów;
- zniszczenie samolotów strategicznych, których Rosja już nie produkuje;
- osłabienie zdolności uderzeniowych wroga, ponieważ samoloty te były ważnym elementem ciągłych ataków terrorystycznych na miasta ukraińskie;
- konieczność wzmocnienia obrony baz i obiektów wymagająca dużych nakładów finansowych.

Implikacje operacji „Pajęczyna” wykraczają daleko poza wojnę rosyjsko-ukraińską, podważając starą ideę, że tyły są bezpieczne. Stosunkowo tanie drony, wystrzelone z terytorium Rosji, zniszczyły samoloty, które kosztowały miliardy i stanowiły podstawę uderzenia dalekiego zasięgu Moskwy.

Poza fizycznymi i finansowymi stratami dla rosyjskiej floty operacja „Pajęczyna” ma również silne skutki psychologiczne. Sygnalizuje, że Ukraina, po ponad 3 latach wojny, jest w stanie przeprowadzić wyrafinowane operacje na terytorium wroga. Ukraiński atak w samo serce Rosji może również wywrócić do góry nogami tradycyjne zasady prowadzenia wojny, ukazując plan przeprowadzania nalotów z głębi linii frontu.

Olga Wasiuta

D. Cole, P. Sauer, A. Mazhulin, *Ukraine launches major drone attack on Russian bombers, security official says*, 1.06.2025, https://www.theguardian.com/world/2025/jun/01/ukraine-launches-major-drone-attack-on-russian-bombers-security-official-says (dostęp 3.06.2025); T. Cooper, *Bean-counting*, 5.06.2025, https://xxtomcooperxx.substack.com/p/bean-counting (dostęp 6.06.2025); *Deadly 'Spiderweb': How Ukraine destroyed 40 Russian jets in historic behind-the-lines op*, 1.06.2025, https://newsukraine.rbc.ua/news/deadly-spiderweb-how-ukraine-destroyed-40-1748792204.html (dostęp 5.06.2025); J. Marson, J. Lytvynenko, B.T. Smith, S. Bosak, *Inside the Ukrainian Drone Operation That Devastated Russia's Bomber Fleet*, 3.06.2025, https://www.wsj.com/world/

ukraine-russia-drone-attack-bombers-cc77e534?mod=hp_lead_pos2 (dostęp 4.06.2025); D. Michaels, J. Lytvynenko, *Ukraine's Stunning Assault Roils Russia's Global Military Strategy Surprise drone attack hits Moscow's capacity to threaten distant rivals such as U.S.*, 2.06.2025, https://www.wsj.com/world/ukraines-stunning-assault-upends-russias-global-military-strategy-094f8c1c?mod=article_inline (dostęp 5.06.2025); M. Varenikova, A. Kuznietsova, N. Vasilyeva, *Ukraine Drone Strike Targets Russian Air Bases in Large-Scale Attack*, „The New York Times" 1.06. 2025, https://www.nytimes.com/2025/06/01/world/europe/russia-ukraine-strikes.html (dostęp 2.06.2025); Y. Zoria, *Trojan truck op: Kyiv destroys "34%" of Russia's strategic bomber fleet within hours with truck-launched FPV drones (updated)*, 2.06.2025, https://euromaidanpress.com/2025/06/02/trojan-truck-attack-ukraine-used-ai-trained-fpv-drones-launched-from-trucks-to-destroy-34-of-russias-strategic-bomber-fleet-in-a-day/ (dostęp 3.06.2025); *117 дронів і три часові пояси. Спецоперація Павутина у цифрах і мапа ударів по аеродромах РФ – інфографіка NV*, 2.06.2025, https://nv.ua/ukr/ukraine/events/operaciya-pavutina-karta-infografika-ta-golovni-cifri-pro-udari-po-aerodromah-byelaya-olenya-50518861.html (dostęp 3.06.2025); А. Абрамова, *Операція «Павутина»: водії фур, у яких були українські дрони, думали, що везуть каркасні будинки*, 2.06.2025, https://hromadske.ua/svit/245744-operatsiia-pavutyna-vodiyi-fur-v-iakykh-buly-ukrayinski-drony-dumaly-shcho-vezut-karkasni-budynky (dostęp 5.06.2025); П. Аксьонов, *Операція СБУ «Павутина»: скільки бомбардувальників втратила Росія і настільки легше стане Україні*, 3.06.2025, https://www.bbc.com/ukrainian/articles/c8d15z4rne8o (dostęp 5.06.2025); Х. Бондарєва, *Глава дипломатії ЄС: Операція «Павутина» переписує військову історію*, 5.06.2025, https://www.pravda.com.ua/news/2025/06/5/7515796/ (dostęp 6.06.2025); Х. Бондарєва, *Зеленський розповів колегам у Вільнюсі, що показала операція «Павутина»*, 2.06.2025, https://www.eurointegration.com.ua/news/2025/06/2/7212890/ (dostęp 3.06.2025); I. Hirnyk, *Експерт про операцію «Павутина»: вона обов'язково увійде до підручників з військової історії*, 2.06.2025, https://www.pap.pl/ua/ukrainian/news/ekspert-pro-operaciyu-pavutina-vona-obovyazkovo-uviyde-do-pidruchnikiv-z-viyskovoi (dostęp 3.06.2025); *«Формує новий тип війни». Операція Павутина продемонструвала здатність України завдавати ударів майже по будь-якій точці РФ – NYT*, 3.06.2025, https://nv.ua/ukr/world/countries/operaciya-pavutina-chi-skorotit-moskva-svoji-nastupalni-operaciji-v-ukrajini-pislya-atak-na-aerodromi-50519054.html#goog_rewarded (dostęp 4.06.2025); О. Ян, *Водії вантажівок розповіли про свою роль в операції «Павутина»*, 2.06.2025, https://militarnyi.com/uk/news/vodiyi-vantazhivok-rozpovily-pro-svoyu-rol-v-operatsiyi-pavutyna/ (dostęp 5.06.2025).

OPERACJA SIŁ POŁĄCZONYCH (ang. *joint operations*) – tematyka tego rodzaju działań poruszana jest w wielu podręcznikach polowych i dokumentach doktrynalnych sił zbrojnych państw narodowych oraz organizacji obronnych (NATO), są to m.in. AJP-01 (B) Allied Joint Doctrine, AJP-3 Allied Joint Operations, AJP-3.2 Allied Joint Doctrine for Land Operations, ATP-3.2 Land Operations, ATP-3.2.1 Allied Land Tactics, AJP-3.2.2 Command and Control of Allied Land Forces, Joint Operation JP-3 Sił Zbrojnych USA czy Doktryna Narodowa – Operacje Połączone (OP/01), Doktryna Prowadzenia Operacji Połączonych DD/3, Regulamin Działań Wojsk Lądowych DD/3.2 oraz Planowanie Działań na Szczeblu Taktycznym w Wojskach Lądowych DD/3.2.5 Sił Zbrojnych RP. Używane są także takie pojęcia, jak operacje połączone (*joint operations*), operacje wielonarodowe (*multinational operations*), operacje sojusznicze (*allied operations*) czy operacje wielodomenowe (*multidomain operations*). Regulamin Wojsk Lądowych RP definiuje działania połączone jako „skoordynowane użycie sił i środków rodzajów sił zbrojnych dla osiągnięcia wspólnego celu, w którym biorą udział komponenty co najmniej 2 rodzajów sił zbrojnych kierowane przez 1 dowódcę". Amerykański podręcznik polowy Joint Operation Joint Publication 3-0 przedstawia z kolei definicję sił połączonych „jako wojska składającego się z 2 lub więcej rodzajów sił zbrojnych (departamentów wojskowych), działających pod nadzorem 1 dowódcy".

Cele działań połączonych to rozbicie, zniszczenie, rozcięcie, odcięcie, pozbawienie przeciwnika manewru lub zmuszenie go do zaniechania walki. Mogą być one prowadzone w układzie narodowym, sojuszniczym i wielonarodowym podczas pokoju, kryzysu i wojny. Powinny zapewnić opanowanie i utrzymanie obszaru mającego znaczenie polityczne, ekonomiczne, operacyjne lub taktyczne. Na szczeblu operacyjnym i taktycznym prowadzone są w celu wykrycia przeciwnika, blokowania (pozbawienia go swobody działania) oraz atakowania, aby doprowadzić do jego porażki. Polegają także na działaniach głębokich, bezpośrednich i tylnych, które tworzą nierozłączną całość i powinny być rozpatrywane razem. Celem głębokich jest dążenie do ograniczenia swobody działania przeciwnika poprzez rozproszenie potencjału bojowego, zakłócenie spoistości i tempa działań, utrzymanie go z dala od obiektów, które mogą być jego celem,

a przez to tworzenie sprzyjających warunków do działań bezpośrednich, rozumianych jako walka z przeciwnikiem, wiązanie jego sił i rozbicie ważnych elementów potencjału bojowego oraz pokonanie sił głównych. Obejmują one zazwyczaj obszar o mniejszej głębokości, mają szybki przebieg i widoczny efekt. Z kolei celem działań tylnych jest zapewnienie swobody działania wojskom własnym poprzez podtrzymywanie zdolności bojowej i stworzenie dogodnych warunków do prowadzenia działań taktycznych oraz zapewnienia swobody zabezpieczenia logistycznego wojsk.

Podręcznik NATO AJP-3 Allied Joint Doctrine for the Conduct of Operations podkreśla, że operacje połączone opierają się na wspólnym wysiłku, jednolitej strukturze dowodzenia i komponentach sił zbrojnych, do których zalicza się:

- wojska lądowe;
- siły powietrzne;
- marynarkę wojenną;
- siły specjalne;
- wsparcie sił kosmicznych.

Operacje morskie obejmują wszelkie działania podejmowane przez siły nawodne, podwodne lub morskie siły powietrzne w celu uzyskania przewagi na morzach, kontroli nad nimi lub uniemożliwienia dostępu do nich, jak również projekcji siły z morza. Do tej kontroli zalicza się współpraca między sojusznikami, kierowanie żeglugą, ochrona morskich szlaków komunikacyjnych, zorganizowanie blokady lub embarga na żeglugę gospodarczą lub wojskową oraz operacje przechwytywania na morzu. Dotyczy to także operacji lokalizowania, klasyfikowania i śledzenia jednostek nawodnych, okrętów podwodnych i statków powietrznych oraz – w razie potrzeby – stosowana siły przeciwko nim. Siły morskie bezpośrednio uczestniczą w operacjach desantowych oraz lądowych, prowadząc działania uderzeniowe, rzeczne, przemieszczając wojska lądowe, pełniąc funkcje platform dowodzenia oraz kontroli sił połączonych.

Komponent wojsk lądowych jest najbardziej różnicowany spośród wszystkich pozostałych; składa się na niego różnorodna liczba wojsk, osób cywilnych, przedstawicieli organizacji międzynarodowych, organizacji pozarządowych, obserwatorów, mediów, agencji rządowych, służb specjalnych, co wiąże się z większym ryzykiem spójności działania,

nieporozumieniami i błędami. Ta złożoność wymaga podejścia, które kładzie nacisk na zdecentralizowane dowodzenie, swobodę działania, tempa i inicjatywy. Rolą wojsk lądowych jest zazwyczaj zdobywanie i utrzymanie terenu, neutralizacja sił wroga, jak również odzyskiwanie utraconego terytorium. Są one w stanie prowadzić jednocześnie kilka różnych operacji, wykorzystując ogień i manewr, uzyskując w ten sposób przytłaczającą siłę oraz osiągając pożądane rezultaty. Wymagają też znacznego zaopatrywania materiałowego, które zapewniane jest za pomocą transportu lotniczego, morskiego i lądowego.

Komponent sił powietrznych zajmuję się realizowaniem 4 rodzajów operacji: przeciwdziałaniem wrogiej obecności w domenie powietrznej, przeprowadzaniem ataków, mobilnością powietrzną oraz realizowaniem operacji typu ISR (obserwacja, wywiad, łączność). Innymi słowy, zasadniczym zadaniem sił powietrznych jest uzyskanie kontroli w przestrzeni powietrznej, co jest warunkiem niezbędnym do przeprowadzenia operacji lądowych i morskich. Po jej zdobyciu jednostki powietrzne mają możliwość projekcji siły nieograniczonej ukształtowaniem terenu. Ich cechami wyróżniającymi są szybkość, zasięg, wszechobecność i elastyczność, dzięki czemu mają możliwość przejęcia inicjatywy już na początku konfliktu i wspierania innych rodzajów wojska. Wymagają jednak ciągłej dostępności bezpiecznych baz lotniczych blisko prowadzonej operacji i niezbędnego wsparcia logistycznego. W przypadku regionów, gdzie infrastruktura HNS (wsparcia państwa gospodarza) jest ograniczona, konieczne jest zapewnienie szerokich działań z zakresu inżynierii wojskowej, aby mogły prowadzić misje.

Wsparcie udzielane przez komponent kosmiczny jest najbardziej ograniczone w porównaniu z pozostałymi. Państwa dysponują bowiem ograniczonymi zasobami w przestrzeni kosmicznej, na które składają się m.in. różnego rodzaju satelity, stacje kosmiczne oraz broń antysatelitarna (ASAT). Wsparciem są podmioty komercyjne zapewniające szerokie możliwości w kontekście integracji i planowania na wszystkich poziomach operacji. Usługi kosmiczne obejmują globalną łączność satelitarną, pozycjonowanie, nawigację i pomiar czasu, monitorowanie środowiska naziemnego i kosmicznego, w tym budowanie świadomości sytuacyjnej, dane geologiczne, meteorologiczne i oceanograficzne, prowadzenie wywiadu,

nadzoru i rozpoznania, wczesne ostrzeganie, śledzenie sił własnych, sojuszniczych i wroga oraz śledzenie ruchu morskiego.

Komponent wojsk specjalnych koncentruje się na działaniach prowadzonych przez specjalnie wyznaczone, zorganizowane, wyselekcjonowane, wyszkolone i wyposażone pododdziały z wykorzystaniem specjalistycznych metod działania i technik. Operacje specjalne mogą przynosić rezultaty zarówno na poziomie strategicznym, jak również operacyjnym oraz mogą być osiągane pomimo występowania wysokiego ryzyka politycznego. Obejmują one pomoc wojskową, specjalne rozpoznanie lub akcje bezpośrednie. Mogą być prowadzone samodzielnie, w połączeniu z innymi rodzajami wojsk, jako operacje sojusznicze, lub we współpracy z lokalnymi milicjami. Przed wybuchem wojny, w okresie rywalizacji między państwami, mogą być rozmieszczone na terenie kraju sojuszniczego w celu zapewnienia wczesnej obecności wojskowej, nawiązania łączności, przeprowadzania oceny przyszłego teatru działań, zapewnienia wczesnego dowodzenia, doradztwa siłom sojuszniczym lub przygotowania działań dywersyjnych, gdyby miejsce to zajęte zostało przez przeciwnika.

Operacje połączone, podobnie jak inne rodzaje operacji wojskowych, opierają się na określonych zasadach. Amerykański podręcznik polowy Join Operation JP-3 podkreśla, że w przypadku Sił Zbrojnych USA jest to 9 tradycyjnych zasad wojny: cel, ofensywa, masa, manewr, ekonomia siły, jedność dowodzenia, bezpieczeństwo, zaskoczenie, prostota, uzupełnionych o 3 dodatkowe: powściągliwość, wytrwałość i legitymizacja. Cel jest ukierunkowaniem każdej operacji wojskowej; powinien być jasko określony, zdecydowany i osiągalny. Zazwyczaj wiąże się on ze zniszczeniem potencjału wroga i osłabieniem jego woli walki.

Dowództwo operacji połączonych powinno unikać działań, które nie przyczyniają się bezpośrednio do osiągnięcia celu. Zmiana lub korekta celów operacji może mieć miejsce pod wpływem zmieniającej się sytuacji i musi być podjęta na najwyższych szczeblach dowodzenia wojskowego i politycznego. Kontekst polityczny jest niezbędny, ponieważ realizacja celów wojskowych wynika bezpośrednio z narodowych (politycznych) państwa. Zasada ofensywy opiera się na przekonaniu, że jest to najskuteczniejszy i najbardziej zdecydowany sposób osiągnięcia jasno określonego celu. W operacjach ofensywnych siły połączone przejmują i utrzymują

inicjatywę, zachowując jednocześnie swobodę działania, osiągając decydujące rezultaty. Dowódcy powinni wybierać obronę jedynie jako tymczasową metodę walki i równocześnie szukać okazji, aby ponownie atakować i przejmować inicjatywę. Zasada masy podkreśla konieczność koncentracji siły bojowej w najkorzystniejszym miejscu i czasie, aby zwiększyć prawdopodobieństwo osiągnięcia celów operacji. Zgromadzenie wojsk i przeprowadzenie ataku w określonym miejscu może umożliwić nawet słabszym siłom osiągnięcie zakładanych rezultatów, minimalizując jednocześnie straty osobowe i materialne. Manewr polega na postawieniu wroga w niekorzystnej sytuacji poprzez elastyczne zastosowanie siły bojowej; burzy to poczucie równowagi, chroniąc jednocześnie własne siły, przyczynia się do zachowania swobody działania i zmniejszenia podatności na ataki. Ekonomia sił polega na przeznaczeniu minimalnych, niezbędnych środków na działania drugorzędne, aby maksymalne mogły być wykorzystane na działania podstawowe. Innymi słowy, to rozsądne użycie i dysponowanie dostępnymi wojskami pod dowództwem jednej jednostki odpowiedzialnej za realizację celu.

W przypadku operacji prowadzonej wraz z partnerami wielonarodowymi lub takiej, w którą zaangażowane są instytucje spoza struktur wojskowych, jedność dowodzenia może być utrudniona bądź wręcz niemożliwa, jednak utrzymany może być wymóg jedności wysiłków. Zasada bezpieczeństwa polega na uniemożliwieniu wrogowi uzyskania nieoczekiwanej przewagi poprzez wykorzystanie przez dowódców środków, jakie mają do dyspozycji. Pozwala to chronić własne siły, ludność cywilną lub inne kluczowe priorytety operacji. Zaskoczenie może pomóc dowódcy zmienić układ sił i tym samym osiągnąć sukces znacznie wykraczający poza początkowe założenia. Czynniki wpływające na zaskoczenie to m.in. szybkość podejmowania decyzji, udostępnienie informacji i przemieszczanie sił, skuteczny wywiad, wprowadzanie w błąd, wprowadzenie nieoczekiwanej siły bojowej czy stosowanie zróżnicowanych taktyk i metod działania. Prostota polega na zwiększeniu prawdopodobieństwa, że plany i operacje wykonane zostaną zgodnie z zamierzeniami poprzez przygotowanie jasnych, nieskomplikowanych planów oraz zwięzłych rozkazów. Pozwala to na lepsze zrozumienie i planowanie działań na wszystkich szczeblach dowodzenia. Jest pożądane w czasie prowadzenia operacji

wojskowych z uwagi na warunki stresu, zmęczenia i „mgły wojny". Powściągliwość polega na zapobieganiu niepotrzebnemu użyciu siły; jeden nieodpowiedni rozkaz może powodować znaczące konsekwencje polityczne i militarne, dlatego zasada ta podkreśla rozsądne używanie dostępnych wojsk w ramach prowadzonej operacji. Zasada wytrwałości podkreśla konieczność zaangażowania wojska w realizację operacji i osiągnięcie celów; obejmuje odpowiednie przygotowanie, szkolenia oraz krajowe i sojusznicze ćwiczenia wojskowe. Często zaliczają się do niej także działania dyplomatyczne, ekonomiczne i informacyjne, będące uzupełnieniem działań wojskowych. Legitymizacja jest z kolei utrzymaniem prawnego i moralnego autorytetu wojska w ramach prowadzonej operacji, może być niekiedy czynnikiem decydującym o zwycięstwie, ponieważ opiera się na takich przesłankach, jak legalność, moralność i słuszność prowadzonych działań. Dotyczy także legitymizacji rządu w państwie, na terenie którego prowadzona jest operacja wojskowa, postrzegania go przez ludność cywilną i społeczność międzynarodową. Amerykański podręcznik Joint Military Operations Historical Collection wydany przez Kolegium Połączonych Szefów Sztabów podaje liczne przykłady operacji połączonych, jakie prowadzone były przez Siły Zbrojne USA. Jedną z pierwszych była bitwa pod Vickburgiem w 1863 r. prowadzona w ramach szerszej kampanii wojsk Unii nad rzeką Missisipi. Innymi przykładami były operacje „Chromite" w 1950 r. (bitwa pod Inczon), „Urgent Fury" w 1983 r. (atak na Grenadę), „Just Case" w 1989 r. (atak na Panamę), „Desert Storm" w 1991 r. (atak na Irak), działania USA w Somalii w 1993 r. czy operacja „Uphold Democracy" w latach 1994–1995 (interwencja w Haiti).

Tomasz Wójtowicz

AJP-3.2 Allied Joint Doctrine for Land Operations, ATP-3.2 Land Operations; ATP-3.2.1 Allied Land Tactics, AJP-3.2.2 Command and Control of Allied Land Forces; *Joint Military Operations Historical Collection*, „The Joint Chiefs of Staff" 15.07.1997; NATO Standard AJP-3 Allied Joint Doctrine for the Conduct of Operations; Regulamin Wojsk Lądowych, Dowództwo Wojsk Lądowych Pion Szkolenia, Joint Operation JP-3; R.W. RisCassi, *Doctrine for Joint Operations in a Combined Environment: A Necessity*, „Military Review" 01–02.1997; T. Wójtowicz, *The*

American Multi-Domain Operation as a response to the Russian concept of New Generation Warfare, „Nowa Polityka Wschodnia" 2022, nr 3(34).

OPROGRAMOWANIE ANTYSZPIEGOWSKIE (ang. *anti-spyware*) – rodzaj narzędzia służącego do monitorowania, wykrywania, ale również usuwania oprogramowań czy też systemów szpiegujących. Programy antyszpiegowskie mają fundamentalne znaczenie dla ochrony prywatności użytkowników, bezpieczeństwa danych czy też integralności systemów operacyjnych. W kontekście bezpieczeństwa państwa dotyczy to rozwiązań w zakresie infrastruktury krytycznej, administracji, a także instytucji strategicznych.

W instytucjach wojskowych czy też administracji państwowej rozwiązania antyszpiegowskie umożliwiają nie tylko identyfikację grup przestępczych, ale również wykrywanie prób inwigilacji przez wrogie służby wywiadowcze. Rozwiązanie to może zostać też poddane działaniom wrogich służb wywiadowczych. Na poziomie państwowym ważnym aspektem jest wykrywanie narzędzi szpiegowskich stosowane przez agencje wywiadowcze oraz cyberprzestępców.

Rozwój programów szpiegowskich wymaga stosowania technologii antyszpiegowskich, które umożliwiają wykrywanie oraz neutralizowanie działań wywiadowczych. Program antyszpiegowski ma na celu skutecznie ochraniać system; należy również omówić, jakiego rodzaju zagrożenia są wykrywane. Ważnym aspektem jest fakt, że narzędzia te muszą zapobiegać tradycyjnym zagrożeniom, takim jak złośliwe oprogramowania, ale również zwalczać nowoczesne ich typy.

Do tradycyjnych zagrożeń należy *hot-dependent*, z rodzaju *malware*, bazujący na plikach zapisanych lokalnie na dysku. Obejmuje trojany i keyloggery. Zagrożenia te wymagają istniejącego pliku, tak aby szkodliwy kod mógł zostać wdrożony. Zostają one poddane analizie statycznej. Warto też zaznaczyć, że działania te bywają nieskuteczne, technika ma bowiem pewne ograniczenia – ze względu na to narzędzia, w tym oprogramowanie antyszpiegowskie, mogą być zredukowane. Kolejnym zagrożeniem są nowoczesne techniki, takie jak *fileless malware* – to rodzaj złośliwego oprogramowania, które działając, nie pozostawiają śladów na twardym dysku, bazując tylko na pamięci operacyjnej. Tego rodzaju zagrożenie

przenika system, unikając tradycyjnych zabezpieczeń oraz opierając się na wykrywaniu plików.

Złośliwe oprogramowanie może manipulować procesami systemowymi albo wprowadzić zagrażający kod. Inną techniką stosowaną przez *fileless malware* jest tworzenie kanałów komunikacyjnych wraz z serwerem kontroli i ukrywanie ich przed narzędziami monitorującymi. Złośliwe oprogramowanie wprowadza swój kod do legalnych procesów działających w pamięci, przez co trudno zidentyfikować ten rodzaj zagrożenia tradycyjnymi metodami. Oprogramowania antyszpiegowskie działają również na poziomie procesów systemowych, wykorzystując np. *process hollowing*. Inną metodą zagrażającą programowi antyszpiegującemu jest modyfikacja rejestrów systemowych; polega na zaciemnieniu fragmentu kodu w danym rejestrze, co sprawia, że nie jest wykrywalny przez tradycyjne narzędzia.

Główną funkcją oprogramowania antyszpiegowskiego jest skanowanie komputera w celu wyszukiwania znanych programów szpiegujących, monitorując zagrożenia w czasie rzeczywistym, i działania przypominające zachowania *spyware* (oprogramowanie szpiegujące). Kluczowym elementem nowoczesnych systemów antyszpiegowskich jest analiza ruchu sieciowego bazująca na dynamicznych wzorcu, ale również identyfikacji działania złośliwego oprogramowania. Oprogramowanie antyszpiegowskie ewoluowało w odpowiedzi na rozwój technik stosowanych w programach szpiegowskich.

W ostatnich latach systemy szpiegowskie stają się coraz bardziej skomplikowane i trudne do wykrycia – stosują skuteczne modyfikacje kodu czy też skomplikowane ukrywanie, natomiast narzędzia antyszpiegowskie rozwinęły użyteczność metod analitycznych z wykorzystaniem chociażby sztucznej inteligencji. Oprogramowanie antyszpiegowskie to niezbędny element budujący bezpieczeństwo państwa, a w szczególności – cyberprzestrzeni. Ze względu na istotność narzędzia informatycznego wymienia się takie funkcje, jak monitorowanie aktywności i ruchu w sieci, łączenie technik analizy w celu wzmocnienia ochrony, blokowanie złośliwego oprogramowania, wykrywanie i zapobieganie kradzieży danych.

Oprogramowania antyszpiegowskie stosują nowoczesne metody wykrywania, takie jak sygnaturowe, hybrydowe, behawioralne, heurystyczne, maszynowe, za pomocą sztucznej inteligencji. Wykrywanie sygnaturowe

jest kluczowe – polega na porównywaniu plików i procesów, a także rozpoznawaniu kodu bazy danych złośliwego oprogramowania; analiza wyników pozwala na oznaczanie tych, które wydają się niebezpieczne. Metoda przynosi wiele korzyści, m.in. skuteczność działań wobec oprogramowań szpiegowskich, niewielkie zużycie zasobów; jest skuteczna, dopóki oprogramowanie szpiegowskie nie zostanie zmodyfikowane. Technika behawioralna oparta jest na obserwacji zachowań systemów w czasie rzeczywistym z wyszczególnieniem interakcji z systemem operacyjnym, plikami, a także innymi zasobami danych. Kluczowe dla tej metody jest to, że o zagrożeniu pliku decydują podejmowane działania, a nie sama ich charakterystyka. Wobec tego sprawdza się próby modyfikacji wpisów czy dokonanych zmian na plikach lub innych bazach danych, próby ukrywania procesów. Metoda ta wyróżnia się przede wszystkim zdolnością do identyfikowania nowych i dotąd nieznanych zagrożeń oraz neutralizowania oprogramowania szpiegowskiego stosującego zaawansowane techniki przenikania. Technika często generuje jednak błędne analizy zagrożeń i wymaga znacznych zasobów obliczeniowych. Metoda heurystyczna polega na analizie struktury oprogramowania przy wykorzystaniu modeli, np. eksperckich, statystycznych. Dodatkowo wykorzystuje się techniki polegające na analizie funkcji systemowych czy też ciągów instrukcji; jej zaletami są zdolność wykrywania nowych możliwości ataku programem szpiegowskim wrogiego państwa, ale też brak konieczności uruchamiania niezbędnych kodów, które mają za zadanie wykrywanie działań szpiegowskich w cyberprzestrzeni. Poza znaczącymi zaletami analitycy mogą mierzyć się z fałszywymi alarmami.

Najskuteczniejsza wydaje się z kolei metoda maszynowa – to dogłębna analiza danych, której zadaniem jest wykrywanie i klasyfikowanie binarne (rozpoznanie złośliwego oprogramowania). Jest ceniona ze względu na wysoką skuteczność rozpoznawania nowych i nieznanych wcześniej zagrożeń, a także nowoczesne techniki zapobiegania atakom. Trudnością stosowanej metody jest konieczność posiadania dużych i zrównoważonych baz danych, ale także ryzyko błędnej klasyfikacji z przyczyn technicznych (niepoprawnie zbudowany model stosowany przy wykrywaniu działalności szpiegowskiej). Metoda hybrydowa jest techniką mieszaną, połączeniem analizy statycznej oraz dynamicznej (behawioralna oparta

na sztucznej inteligencji). Jest ceniona ze względu na elastyczne rozwiązania, ale również uważne dostosowanie techniczne, tzn. budzący wątpliwości plik najpierw poddawany jest statycznej ocenie, a w następnej kolejności uruchamiany w sposób kontrolowany. Inną cenioną techniką modelu hybrydowego jest obserwacja wraz z wykorzystaniem sposobu heurystycznego. Rozwiązanie to opiera się na obserwacji zachowania wybranego programu.

Zaletą metody hybrydowej jest przede wszystkim wysoka skuteczność działania – wykrywanie nowych, ale również znanych już zagrożeń. Nie jest jednak pozbawiona wad – bywa często opóźniona, w szczególności podczas przeprowadzania analizy wieloetapowej. Ocenia się jednak, że najefektywniej wykrywa oprogramowania szpiegowskie. Należy zaznaczyć, że działanie programów antyszpiegowskich jest ważne dla budowania bezpieczeństwa nie tylko systemu komputerowego, ale również cyberprzestrzeni. Oprogramowanie to spełnia swoje funkcje m.in. poprzez zapewnienie prywatności użytkownika (ochrona przed atakiem cybernetycznym lub nieautoryzowanym użyciem danych), współdziałanie z innymi rozwiązaniami technicznymi (pozwala to na uzyskanie solidnej ochrony chociażby przy współpracy z programem antywirusowym), ochronę infrastruktury krytycznej (możliwość wykrywania prób nieautoryzowanego dostępu np. do systemu – infrastruktura krytyczna to newralgiczny sektor ochrony, który coraz częściej jest celem ataków), wykrywanie i usuwanie zagrożeń wykradania danych użytkownika (wykradzione dane mogą stanowić źródło np. oszustw finansowych).

Należy również zaznaczyć, że oprogramowania antyszpiegowskie napotykają ograniczenia w działaniu ze względu na rozwój blokowania wykrycia; problemem jest możliwość omijania systemów ochronnych, m.in. zaciemnianie struktur binarnych, wykorzystanie packerów, przekształcanie kodu. Przy wykorzystaniu takich metod analiza jest znacznie utrudniona, a nawet blokowana. Nowoczesne *malware* są konstruowane w taki sposób, aby aktywnie wykrywały zabezpieczenia; dzięki temu mogą zmieniać charakter swoich działań i stawać się niewidzialne dla przeprowadzanych analiz antyszpiegowskich. Popularnym zagrożeniem staje się również bezplikowość (rodzaj *spyware*). Należy zaznaczyć, że zainstalowanie narzędzia, jakim jest oprogramowanie antyszpiegowskie, nie

stanowi gwarancji ochrony. Konieczna jest aktualizacja systemu, a także dostosowanie odpowiednich metod do dynamicznie zmieniających się technik stosowanych przez złośliwe oprogramowania.

Natalia Borodziuk

T. Arjunan, *Real-Time Detection of Network Traffic Anomalies in Big Data Environments Using Deep Learning Models*, „International Journal for Research in Applied Science and Engineering Technology" 2024, no. 12(III):9, https://www.researchgate.net/publication/379000723_Real-Time_Detection_of_Network_Traffic_Anomalies_in_Big_Data_Environments_Using_Deep_Learning_Models (dostęp 3.12.2025); I. Kara, *Fileless Malware Threats: Recent advances, analysis approach through memory forensics and resarch Challenges*, „Expert Systems with Applications" 2022, 214(6):119133, https://www.researchgate.net/publication/364769363_Fileless_malware_threats_Recent_advances_analysis_approach_through_memory_forensics_and_research_challenges (dostęp 3.12.2025); M.A. Mimi, H. Ng, T.T.V. Yap, *Directional Features and Rule-Based Labeling for Real-Time Network Traffic-Based Android Spyware Classification*, „Journal od Supercomputing" 2025, no. 81(8), https://www.researchgate.net/publication/392239054_Directional_features_and_rule-based_labeling_for_real-time_network_traffic-based_android_spyware_classification (dostęp 3.12.2025); M. Qabalin, M. Naser, M. Alkasassbeh, *Android Spyware Detection Using Machine Learning: A Novel Dataset*, „Sensors" 2022, no. 22(15), https://www.researchgate.net/publication/362678689_Android_Spyware_Detection_Using_Machine_Learning_A_Novel_Dataset (dostęp 3.12.2025); D. Samociuk*, Antivirus Evasion Methods in Modern Operating Systems*, „Applied Sciences" 2023, 13(8):5083, https://www.researchgate.net/publication/370168873_Antivirus_Evasion_Methods_in_Modern_Operating_Systems (dostęp 3.12.2025); S. Talukder, Z. Talukder, *A Survey on Malware Detection and Analysis Tools*, „International Journal of Network Security & Its Applications" 2020, vol. 12(2), https://www.researchgate.net/publication/339816480_A_Survey_on_Malware_Detection_and_Analysis_Tools (dostęp 3.12.2025).

OSOBOWOŚĆ PRZESTĘPCZA – zespół względnie trwałych cech psychicznych, moralnych i społecznych jednostki, kształtujących się w toku jej rozwoju pod wpływem określonych warunków środowiskowych, relacji społecznych oraz doświadczeń życiowych. Zawiera m.in. impulsywność, obniżoną empatię, skłonność do agresji oraz lekceważenie norm społecznych i prawnych. Cechy te same w sobie nie przesądzają o popełnieniu

przestępstwa, lecz w określonych sytuacjach mogą sprzyjać zachowaniom sprzecznym z prawem. Osobowość przestępcza nie odnosi się do pojedynczego czynu zabronionego, lecz do trwałych predyspozycji jednostki zwiększających ryzyko zachowań przestępczych. Pojęcie to znajduje zastosowanie w psychologii i kryminologii jako narzędzie analizy mechanizmów predysponujących jednostkę do łamania prawa, profilowania sprawców oraz opracowywania strategii prewencyjnych.

Podejście rozróżniające jest istotne zarówno w badaniach psychologicznych, jak i praktyce kryminologicznej, ponieważ pozwala oddzielić analizę indywidualnych predyspozycji od oceny konkretnych zachowań. Rozpoznanie tej różnicy umożliwia również skuteczniejsze identyfikowanie czynników ryzyka, które w określonych okolicznościach mogą zwiększać prawdopodobieństwo wystąpienia zachowań przestępczych, oraz czynników ochronnych, które mogą je osłabiać. W rezultacie, aby dokładnie poznać mechanizmy powstawania osobowości przestępczej, należy badać nie tylko pojedyncze czyny, ale przede wszystkim trwałe cechy psychiczne, moralne i społeczne jednostki. Istotna jest również analiza ich interakcji z warunkami środowiskowymi i sytuacyjnymi, które mogą ujawniać lub hamować potencjalne zachowania antyspołeczne.

Analiza osobowości przestępczej staje się możliwa dzięki przyjęciu szerszego ujęcia osobowości jako względnie trwałej, dynamicznej i zintegrowanej organizacji cech psychicznych oraz psychofizycznych jednostki. Osobowość obejmuje m.in. temperament, charakter, intelekt, uzdolnienia, postawy moralne i wzorce zachowania, które kształtują się w toku rozwoju człowieka pod wpływem czynników biologicznych i środowiskowych. Nadaje ona spójność i ciągłość myśleniu, emocjom i działaniom jednostki, determinując jej indywidualny sposób funkcjonowania oraz przystosowania do otoczenia społecznego i fizycznego. Osobowość odzwierciedla unikalność jednostki, integruje doświadczenia przeszłe, aktualne formy reagowania oraz oczekiwania wobec przyszłości, stanowiąc względnie stały wzorzec regulujący zachowanie człowieka w różnych sytuacjach życiowych.

Przy założeniu, że w psychologii i psychiatrii osobowość najczęściej analizuje się w płaszczyźnie biologicznej i psychologicznej, należy podkreślić znaczenie jej wymiaru społeczno-kulturowego. Warstwa społeczna jest

bardziej zmienna i powierzchowna w porównaniu z głębiej zakorzenionymi cechami biologicznymi, jak i psychologicznymi, nie oznacza to jednak, że jest ona bez znaczenia. Presja otoczenia, normy społeczne, instytucje czy wyznawane ideologie mogą w istotny sposób modelować osobowość jednostki, wpływając na jej postawy, decyzje i hierarchię wartości. W zależności od warunków społecznych i historycznych człowiek może ulegać przemianom, które czasem sprawiają, że jego zachowanie wydaje się niezgodne z wcześniejszymi cechami osobowości, np. osoba dotąd moralna i powściągliwa w okresie pokoju może pod wpływem wojny, rewolucji czy nacisku grupowego działać w sposób brutalny lub bezwzględny. Władza, akceptacja instytucji czy nacisk ideologiczny mogą zmieniać priorytety jednostki, kierując jej decyzje wbrew własnemu sądowi i osobistej hierarchii wartości. W ten sposób płaszczyzna społeczno-kulturowa staje się istotnym czynnikiem w procesie formowania i modulowania osobowości, w tym również jej wariantów przestępczych.

Osobowość jednostki kształtuje się i funkcjonuje w wyniku dynamicznej interakcji czynników:

- biologicznych;
- psychologicznych;
- społeczno-kulturowych.

Wymiary biologiczny i psychologiczny sięgają głębiej w strukturę jednostki i charakteryzują się względną trwałością, obejmując m.in. uwarunkowania genetyczne, temperament, cechy charakteru, mechanizmy poznawcze i emocjonalne oraz zdolność do samokontroli. Z kolei wymiar społeczno-kulturowy, choć bardziej zmienny i podatny na wpływy środowiskowe, takie jak rodzina, grupy rówieśnicze, normy społeczne czy oddziaływanie instytucji, odgrywa istotną rolę w kształtowaniu postaw, hierarchii wartości i wzorców zachowań jednostki. Żaden z tych wymiarów nie funkcjonuje niezależnie od pozostałych. Predyspozycje biologiczne i cechy psychologiczne pozostają w stałej relacji z oddziaływaniami społecznymi, które mogą je zarówno wzmacniać, jak i modyfikować. Analiza osobowości w perspektywie tych 3 wzajemnie powiązanych płaszczyzn pozwala na pogłębione zrozumienie mechanizmów funkcjonowania człowieka oraz czynników sprzyjających podejmowaniu zachowań przestępczych.

W kontekście tak rozumianej wielowymiarowej struktury osobowości zasadne staje się uwzględnienie roli czynników ryzyka oraz ochronnych, które w toku rozwoju jednostki mogą sprzyjać kształtowaniu się osobowości przestępczej bądź ograniczać prawdopodobieństwo podejmowania zachowań sprzecznych z normami prawnymi i społecznymi. Do czynników ryzyka należą m.in.

- impulsywność;
- obniżona empatia;
- skłonność do agresji;
- środowisko kryminogenne;
- presja grupowa.

Z kolei czynniki ochronne obejmują:

- więzi rodzinne;
- przywiązanie do norm moralnych;
- zdolność do samokontroli;
- edukację;
- wsparcie społeczne.

Równowaga między tymi czynnikami decyduje o stopniu predyspozycji jednostki do zachowań przestępczych i pozwala wyjaśnić, dlaczego osoby o podobnych cechach biologicznych i psychologicznych mogą reagować odmiennie w różnych kontekstach społecznych.

Mechanizmy powstawania osobowości przestępczej są analizowane w ramach różnych dyscyplin naukowych, co znajduje odzwierciedlenie w istnieniu 3 zasadniczych grup teorii wyjaśniających to zjawisko:

- biologicznych;
- psychologicznych;
- socjologicznych i społeczno-kulturowych.

Teorie biologiczne koncentrują się na wrodzonych uwarunkowaniach jednostki, takich jak predyspozycje genetyczne, cechy temperamentu czy neurobiologiczne podstawy agresji i impulsywności. Badania wskazują, że niektóre zaburzenia układu nerwowego lub równowagi neuroprzekaźników mogą zwiększać ryzyko zachowań antyspołecznych.

Teorie psychologiczne, które obejmują m.in. teorię cech oraz teorię osobowości antyspołecznej, koncentrują się na trwałych cechach jednostki, mechanizmach poznawczych, postawach moralnych i temperamencie.

W literaturze zwraca się również uwagę na rolę zaburzeń osobowości, w tym antyspołecznej, oraz cech związanych z psychopatią, takich jak brak empatii, impulsywność, manipulacyjność i skłonność do ryzyka. Choć te cechy nie determinują automatycznie popełnienia przestępstwa, w połączeniu z określonymi czynnikami środowiskowymi i społecznymi mogą zwiększać ryzyko zachowań antyspołecznych. Psychopatia jest szczególnie istotna w badaniach nad osobowością przestępczą, ponieważ predysponuje do poważnych przestępstw, w tym przemocy, oszustw czy działań naruszających prawa innych osób. Uwzględnienie tych cech w profilowaniu sprawców pozwala lepiej przewidywać potencjalnie agresywne lub niebezpieczne zachowania jednostki.

Teorie socjologiczne i społeczno-kulturowe akcentują znaczenie środowiska społecznego w kształtowaniu zachowań jednostki, w szczególności wpływu grup rówieśniczych, norm instytucjonalnych oraz procesów uczenia się społecznego. Współczesne ujęcia w tym nurcie podkreślają interakcyjny charakter relacji między cechami jednostki a czynnikami środowiskowymi, wskazując, że presja grupowa, społeczne mechanizmy aprobaty oraz modelowanie ról mogą zarówno wzmacniać, jak i ograniczać predyspozycje do podejmowania zachowań przestępczych.

Uwzględniając różnorodne teoretyczne ujęcia osobowości przestępczej, możliwe jest wyodrębnienie priorytetowych cech i mechanizmów zachowań jednostki, które pozwalają lepiej zrozumieć przyczyny przestępczości oraz opracowywać skuteczne strategie profilowania i działań prewencyjnych. Koncepcja osobowości przestępczej znajduje zastosowanie w praktyce kryminologicznej i penitencjarnej, w tym w profilowaniu sprawców, programach prewencyjnych oraz resocjalizacyjnych. Analiza cech i wzorców zachowań, takich jak impulsywność, agresja, manipulacja, skłonność do ryzyka czy lekceważenie norm społecznych, umożliwia pogłębione zrozumienie mechanizmów predysponujących jednostkę do naruszania prawa. Wiedza o czynnikach ryzyka i ochronnych pozwala w procesach prewencji i resocjalizacji wzmacniać samokontrolę, empatię oraz więzi społeczne. Jednocześnie umożliwia ograniczanie postaw sprzyjających zachowaniom przestępczym. Teoria osobowości przestępczej integruje wymiar poznawczy z praktycznym, dostarczając narzędzi do diagnozy, oceny ryzyka oraz planowania działań korygujących

i zapobiegawczych. Trwałe cechy jednostki, w połączeniu z niekorzystnym środowiskiem i presją grupy, zwiększają ryzyko powtarzalności zachowań przestępczych. Poznanie tych mechanizmów ma fundamentalne znaczenie zarówno w profilowaniu sprawców, jak i projektowaniu strategii prewencyjnych oraz programów resocjalizacyjnych, mających na celu ograniczenie recydywy.

Podsumowując, zrozumienie osobowości przestępczej pozwala wskazać trwałe predyspozycje zwiększające ryzyko popełnienia czynów zabronionych prawem, przy czym ich posiadanie nie determinuje odpowiedzialności karnej. Uwzględnienie mechanizmów biologicznych, psychologicznych i społecznych, a także zaburzeń osobowości i cech psychopatycznych wspiera profilowanie sprawców oraz projektowanie działań prewencyjnych i resocjalizacyjnych zgodnych z przepisami. Szczególne znaczenie przypisuje się rozróżnieniu między trwałymi predyspozycjami jednostki a pojedynczym czynem przestępczym, co umożliwia adekwatną ocenę odpowiedzialności, ograniczenie recydywy i efektywną reintegrację społeczną.

Dariusz Hybś

L. Cierpiałkowska, *Zaburzenia osobowości w modelach medycznych i psychologicznych*, [w:] *Psychologia zaburzeń osobowości. Wybrane zagadnienia*, L. Cierpiałkowska (red.), Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 2004; J. Gąsiorowski, *Osobowość sprawcy przestępstwa i jej wpływ na proces wykrywczy*, „Zeszyty Naukowe Pro Publico Bono" 2023, t. 1 nr 1; J. Groth, *Antyspołeczne zaburzenie osobowości*, [w:] *Psychologia zaburzeń osobowości. Wybrane zagadnienia*, L. Cierpiałkowska (red.), Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 2004; C.S. Hall, G. Lindzey, J.B. Campbell, *Teorie osobowości*, Wydawnictwo Naukowe PWN, Warszawa 2006; L. Hochberg, *Osobowość sprawcy przestępstwa*, Wydawnictwo Prawnicze, Warszawa 1978; B. Hołyst, *Psychologia kryminalistyczna. Diagnoza i praktyka*, Wydawnictwo Difin, Warszawa 2018; A. Jakubik, *Zaburzenia osobowości*, Wydawnictwo Lekarskie PZWL, Warszawa 1997; A. Kępiński, *Psychopatie*, Wydawnictwo Literackie, Warszawa 1977; A. Mościkier, *Natura ludzka i problem przestępczości*, Wydawnictwo Akademickie „Żak", Warszawa 2001; E. Nęcka, *Psychologia. Wprowadzenie*, Wydawnictwo Naukowe Scholar, Warszawa 2023; P.K. Oleś, *Wprowadzenie do psychologii osobowości*, Wydawnictwo Naukowe

Scholar, Warszawa 2009; P. Pawlak, *Zagubione Ja. Zaburzenia dysocjacyjne. Jak je rozpoznać, zrozumieć i leczyć*, Wydawnictwo Sensus, Gliwice 2024; M. Radochoński, *Osobowość antyspołeczna*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2009; S. Siek, *Formowanie osobowości*, Wydawnictwo Akademii Teologii Katolickiej, Warszawa 1986; M. Rode, *Style myślenia przestępczego. Podstawy teoretyczne i diagnostyczne*, Wydawnictwo Difin, Warszawa 2013.

P

PANCERNIK to w zasadzie nieformalna nazwa okrętu, rzadko używana poza Polską. Przykładem jest język rosyjski (*броненосец*) lub ukraiński (*броненосець*), co całkowicie odpowiada terminowi polskiemu. W językach angielskim oraz niemieckim używa się odpowiednio terminów *battleship* oraz *Schlachtschiff* oznaczających okręt liniowy. Tożsame określenie odnajdziemy w wielu terminologiach nautycznych świata (m.in. francuskiej, hiszpańskiej, włoskiej czy portugalskiej). Nazwa ta po części wywodzi się z czasów sir Waltera Raleigha (przełom XVI i XVII stulecia), który wprowadził taktykę walki liniowej do strategii morskiej, a główne okręty floty nazwał właśnie w taki sposób. Należy jednak pamiętać, że w angielskiej terminologii nautycznej *battleship* ma znaczenie także funkcjonalne w odniesieniu do epoki żagla i oznacza „główny okręt floty", nawet jeśli dotyczy on galery czy galeonu.

Za pierwszy pancernik *par excellence* uznać należy stosunkowo niewielki okręt USS Monitor. Służył on we flocie Unii w czasie wojny secesyjnej i zasłynął w pojedynku z pancerną fregatą CSS Virginia dnia 8 marca 1862 r. na Hampton Roads. W tym momencie rozpoczęła się historia okrętu określanego jako pancernik. Druga polowa XIX w. przyniosła

bardzo szybki rozwój techniki okrętowej. Na przełomie XIX i XX stulecia typowy pancernik wypierał od 13 tys. do 17 tys. t, uzbrojenie główne składało się z 4 dział kalibru 240–305 mm umieszczonych w 2 dwudziałowych wieżach na dziobie i rufie okrętu. Uzupełniała je artyleria drugiego głównego kalibru 170–203 mm. oraz kilkanaście dział szybkostrzelnych do walki z torpedowcami. Okręty te osiągały prędkość w granicach 15–18 w. Ostatnimi reprezentantami tego typu były m.in. brytyjski Lord Nelson czy niemiecki Deutschland.

Wojna japońsko-rosyjska z lat 1904–1905, a zwłaszcza bitwa pod Cuszimą, zweryfikowała dotychczasowe opinie o największych okrętach wojennych, jakimi były pancerniki. Okazało się bowiem, że w warunkach bojowych decydującą rolę odgrywa tylko artyleria głównego kalibru. Skłoniło to konstruktorów okrętowych czołowych mocarstw morskich do rozważenia budowy pancerników monokalibrowych, tj. z ujednoliconą artylerią główną. Choć rozważania takie prowadzono w kilku krajach, to jednak pionierami w tej dziedzinie okazali się Brytyjczycy – admirał John Fisher, ówczesny Pierwszy Lord Morski, został ojcem pancernika nowej generacji, a kolejne nazywano drednotami na cześć pierwszego – HMS Dreadnought. Okręt był uzbrojony w aż 10 dział kalibru 305 mm, z czego 8 mogło prowadzić ogień na jedną burtę. Nowy pancernik wyposażono w napęd turbinowy, co zapewniło prędkość prawie 22 w. Bez wątpienia ta nowatorska konstrukcja deklasowała wszystkie dotychczas zbudowane pancerniki, także brytyjskie. Dało to impuls do przyspieszenia wyścigu zbrojeń morskich między Niemcami a Wielką Brytanią. Jednocześnie rosły wyporność i kaliber dział oddawanych do służby okrętów. Tuż przed wybuchem I wojny światowej na nowo budowanych jednostkach kaliber dział wzrósł do 381 mm (brytyjski typ Queen Elizabeth).

Po I wojnie światowej wyścig zbrojeń morskich nie ustał, lecz narastał z nową mocą w trójkącie Japonia – USA – Wielka Brytania. Nowo budowane okręty miały wyporność ponad 40 tys. t, a kaliber dział przekroczył 400 mm. Traktat waszyngtoński ograniczył wyporność do 35 tys. t, a kaliber dział nie mógł przekraczać 406 mm (16 cali). To sprawiło, że niemal wszystkie mocarstwa zarzuciły budowę nowych okrętów aż do lat 30. XX stulecia. Dopiero wobec braku zgody na przedłużenie tzw. wakacji morskich w 1935 r. rozpoczął się nowy wyścig zbrojeń w dość krótkim

przedziale czasowym, bo po wybuchu II wojny światowej budowę nowych okrętów liniowych rozpoczęły tylko Stany Zjednoczone (typ Iowa) oraz Wielka Brytania, choć powstanie jedynego brytyjskiego pancernika (typ Vanguard) uznać należy za ewenement. Okręty liniowe, których budowę rozpoczęto tuż przed wojną i zakończono w czasie jej trwania, były większe, szybsze i potężniej uzbrojone niż wcześniejsze konstrukcje. W tym gronie wymienić można amerykański typ North Carolina i South Dakota, brytyjski King George V, francuski Richelieu, japoński Yamato, niemiecki Bismarck oraz włoski Vittorio Veneto. Były to jednostki stosunkowo nowoczesne, jak na owe czasy, na których dobrze zbilansowano kaliber dział, grubość pancerza oraz prędkość. W tym gronie absolutnym ewenementem był japoński pancernik Yamato. Pełna wyporność bojowa tego okrętu (i bliźniaczego Musashi) znacznie przekraczała 70 tys. t, a kaliber dział miał monstrualny wymiar 460 mm. Budowa tak dużych okrętów wynikała wprost z japońskiej doktryny wojny morskiej, tzw. decydującej bitwy.

Japońska admiralicja uważała, że w przyszłej wojnie da się powtórzyć sukces spod Cuszimy i rozbić US Navy w pobliżu japońskich wysp macierzystych, przy czym właśnie pancerniki typu Yamato miały odegrać decydująca rolę. Zaplanowano budowę 5 jednostek tego typu, ale ostatecznie ukończono tylko 2, a trzeci okręt będący w budowie przerobiono na lotniskowiec. Zdecydowana większość admirałów mocarstw morskich była nawet tuż przed wybuchem II wojny światowej przekonana, że okręty liniowe odegrają istotną rolę w przyszłej wojnie. Do grona nielicznych sceptyków w tej kwestii należał będący wiceministrem marynarki japoński admirał Yamamoto Isoroku. Jego opinia była druzgocąca: „Wojskowi zawsze noszą przy sobie pamiątki dawnych wojen, jak np. samurajskie miecze. Te okręty (liniowe) tak się przydadzą Japonii jak owe miecze". To stanowisko potwierdziły doświadczenia w zmaganiach morskich II wojny światowej. Pancerniki sprawdziły się doskonale w równorzędnej walce między nimi; bardzo rzadko zdarzały się zatopienia w bezpośredniej walce. Bismarck wprawdzie został dosłownie rozstrzelany przez brytyjskie liniowce Rodney i King George V, ale w sytuacji, gdy po uszkodzeniu steru torpedą lotniczą pozbawiony został manewrowości. Pojedynków Bismarck vs Hood, Washington vs Kirishima czy Duke of York vs Scharnhorst nie należy brać pod uwagę – w starciach tych z pancernikiem walczył krążownik liniowy,

w dodatku (z wyjątkiem Scharnhorsta) starszy od swego przeciwnika o całą epokę. Skądinąd przywołane tu epizody potwierdziły tezę (wbrew temu, czego oczekiwał admirał Fisher), że krążownik liniowy nie będzie równorzędnym przeciwnikiem dla klasycznego pancernika.

Decydujący cios panowaniu stalowym „władcom mórz" położyło lotnictwo. Brytyjski nalot 20 samolotów na Tarent 11 listopada 1940 r., które wystartowały z lotniskowca, doprowadził do ciężkiego uszkodzenia 3 włoskich pancerników, z których 1 (Conte di Cavour) już nigdy nie wrócił do służby. Uszkodzenie torpedą Bismarcka przez samoloty brytyjskie działające z lotniskowca Ark Royal odegrało decydującą rolę w jego zatopieniu. Oczywiście obrońcy pancerników początkowo nie dali się przekonać; włoskie okręty stojące na kotwicy nie miały możliwości manewru, a o losie Bismarcka przesądziło wyjątkowo pechowe dla tego okrętu trafienie. Sytuacja (i poglądy) zmieniła się po starciu pod Kuantan, na Morzu Południowochińskim; startujące z baz lądowych japońskie bombowce i samoloty torpedowe posłały na dno pancernik Prince of Wales oraz krążownik liniowy Repulse, mimo że brytyjskie okręty dysponowały pełną swobodą manewru oraz silną artylerią przeciwlotniczą. Bardzo szybko stało się oczywiste, że wobec zagrożeń z powietrza, przy braku własnej eskorty, pancerniki są *de facto* bezradne. Ostatecznym dowodem tego stanu rzeczy był ostatni rejs japońskiego Yamato w kierunku Okinawy w kwietniu 1945 r. Ostatecznie pancernik ten został zatopiony 7 kwietnia 1945 r. przy stratach amerykańskich wynoszących kilka samolotów i kilkunastu członków ich załóg

Wzrastająca rola lotniskowców sprawiła, że zaniechano w trakcie wojny budowy nowych pancerników na rzecz okrętów lotniczych. Wyjątkiem były Stany Zjednoczone, które ostatecznie ukończyły 4 z 6 planowanych – Iowa, Missouri, New Jersey i Wisconsin. Ze względu na znaczną prędkość maksymalną (33 w.) były używane głownie jako eskorta lotniskowcowych grup uderzeniowych.

Pod koniec II wojny światowej alianckie pancerniki używane były głównie jako okręty wsparcia artyleryjskiego zarówno podczas desantów w Europie, jak i na Dalekim Wschodzie. Należy podkreślić, że w tej roli okazały się nieocenione, odgrywając istotną rolę w sukcesie operacji desantowych. Po zakończeniu II wojny światowej do końca lat 50. minionego

stulecia prawie wszystkie państwa mające w służbie pancerniki wycofały je z linii, nawet stosunkowo nowoczesne jednostki jak francuski Jean Bart czy wspomniany brytyjski Vanguard. Patrząc z perspektywy czasu, był to błąd, gdyż okręty te jako dość stabilna platforma uzbrojenia mogły być nosicielami nowoczesnych systemów rakietowych. Co więcej, reaktywowane podczas wojny wietnamskiej w 1967 r. pancerniki typu Iowa i ponownie wcielane do linii w latach 1982–1984 doskonale sprawdziły się w roli okrętów wsparcia artyleryjskiego, a podczas wojny w Zatoce Perskiej (1991) – także jako jednostki mogące wystrzeliwać pociski samosterujące. Do dziś nie brakuje opinii, że ich wycofanie ze służby w ostatnich latach XX w. było błędem.

Specjalnym podtypem tej klasy okrętów były krążowniki liniowe – dorównujące uzbrojeniem typowym pancernikom były od nich znacznie szybsze. Osiągano to zazwyczaj kosztem opancerzenia. Według pomysłodawcy tego podtypu – admirała Fishera – miały one niszczyć krążowniki pancerne nieprzyjaciela (w tej roli się sprawdziły) oraz – w razie potrzeby – wspierać „normalne" pancerniki w starciu liniowym. Ta druga funkcja okazała się fatalnym błędem, czego dowiodła bitwa jutlandzka, w której Royal Navy stracili aż 3 krążowniki liniowe w starciu z lepiej opancerzonymi okrętami niemieckimi tej samej klasy. Jakkolwiek po I wojnie światowej zbudowano kilka okrętów mogących uchodzić za nowoczesne krążowniki liniowe – amerykański typ Alaska, francuski Dunkerque oraz niemiecki Scharnhorst, to lepszym określeniem ich klasy była amerykańska nomenklatura – krążowniki najcięższe, gdyż w istocie najbardziej odpowiednią dla nich rolą byłoby zwalczanie ciężkich krążowników przeciwnika z artylerią kalibru 203 mm. *Notabene* tak właśnie uważali konstruktorzy nigdy niezbudowanych holenderskich krążowników projektu 1047. W starciu bowiem z klasycznym pancernikiem okręty te (czego dowiódł pojedynek Duke of York vs Scharnhorst z 26 grudnia 1943 r.) były bez szans.

Roman Kochnowski

N. Friedman, *Naval Firepower: Battleship Guns and Gunnery in the Dreadnought Era*, Naval Institute Press, Annapolis, Maryland 2008; J. Jordan, *Schlachtschiffe und Schlachtkreuzer, die Einsätze und Lebensläufe der grössten Schiffe der Welt von 1939 bis heute*, Podzun-Pallas, Friedberg (Hessen) 1989; T. Klimczyk, *Pancerniki*,

Lampart, Warszawa 2002; R.K. Massie, *Dreadnought. Britain, Germany and the Coming of the Great War*, Cape, London 1992; A. Preston, *Battleships 1856–1977*, Chartwell Books, Secaucus 1977; B. Taylor, *The World of the Battleship: The Lives and Careers of Twenty-One Capital Ships of the World's Navies, 1880–1990*, Seaforth Publishing Barnsley 2018.

PATERNALIZM (z łac. *pater* – „ojciec") – termin, który powstał w europejskiej myśli politycznej i filozoficznej w XVII–XIX w. Pierwotnie oznaczał „rządy ojcowskie", czyli system władzy, w którym państwo lub władca sprawuje opiekę nad poddanymi, ograniczając ich wolność w celu zapewnienia im ich własnego dobra. Właśnie w takim rozumieniu chiński filozof i polityk Konfucjusz (551–479 p.n.e.) postrzegał państwo jako wielką rodzinę, w której władca jest „ojcem", a poddani – „dziećmi". To model polityczny paternalizmu, w którym władza ma charakter patriarchalny (państwo kieruje się zasadami relacji rodzinnych), a władca bierze na siebie odpowiedzialność za dobrobyt obywateli.

Ideologiczne korzenie koncepcji paternalizmu można prześledzić w filozofii antycznej, w szczególności w naukach Platona (424/423–348/347 p.n.e.) i Arystotelesa (384–322 p.n.e.), gdzie władca jest postrzegany jako mądry opiekun obywateli. Platon w swoim słynnym dziele *Państwo* podkreślał znaczenie paternalistycznych podstaw interakcji jako ważnej części życia społecznego. Opisał idealne państwo, w którym mądrzy władcy-filozofowie sprawują władzę nad obywatelami, ponieważ ci nie są w stanie sami zrozumieć, co jest dla nich dobre. Jest to klasyczny przykład paternalistycznego ustroju: władza działa „dla dobra poddanych", nawet jeśli oni nie są tego świadomi.

W dziele *Polityka* **A**rystoteles traktował władzę ojca nad dziećmi, męża nad żoną, pana nad niewolnikiem jako naturalną hierarchię. Porównywał władzę w państwie do patriarchalnej władzy w rodzinie: władca powinien troszczyć się o obywateli tak jak ojciec o dzieci. Jednocześnie Arystoteles podkreślał, że taka władza powinna być racjonalna i ukierunkowana na dobro podwładnych, a nie tyrańska. W filozofii rzymskiej (szczególnie u Cycerona, 106–43 p.n.e.) idea władzy ojcowskiej (*patria potestas*) przenoszona jest na państwo, które jest „wielką rodziną", a władca – „ojcem ojczyzny" (*pater patriae*)**.** Podkreśla on moralny obowiązek władcy

działania dla wspólnego dobra (*communis utilitas*), nawet jeśli ogranicza to wolność obywateli. Filozofia antyczna położyła teoretyczne podwaliny pod rozwój paternalizmu.

W późniejszej tradycji europejskiej władzę postrzegano jako opiekę nad mniej doświadczonymi, wolność – jako życie w zgodzie z rozumem i prawem, a ingerencję władzy – jako uzasadnioną, jeśli miała na celu dobro poddanych. Nicolo Machiavelli (1469–1527) w traktacie *Książę* (*Il Principe*, 1513) postrzegał władcę jako osobę, która ma dbać o stabilność państwa i dobrobyt poddanych, nawet jeśli wymaga to użycia siły, oszustwa lub surowości. Jego koncepcja władzy może być interpretowana jako prototyp autorytarnego lub politycznego paternalizmu, w którym władca działa „dla dobra państwa" bez uwzględnienia woli poddanych.

Francuski myśliciel Jean Bodin (1530–1596) w dziele *Sześć ksiąg o Rzeczypospolitej* (*Les Six Livres de la République*, 1576) opracował koncepcję suwerenności – absolutnej i niepodzielnej władzy monarchy. Państwo jest wielką rodziną, w której monarcha jest „ojcem" poddanych, odpowiedzialnym za porządek, sprawiedliwość i dobrobyt; poddani natomiast powinni okazywać posłuszeństwo i zaufanie, tak jak dzieci wobec ojca. W koncepcji Bodina można dostrzec początki idei rozdzielenia religijnego i państwowego paternalizmu. Uznawał on znaczenie religii dla moralnego wychowania obywateli, ale uważał, że władza państwowa powinna być nadrzędna wobec duchowej w kwestiach polityki i zarządzania. Oznacza to, że opieka moralna Kościoła i polityczna państwa mają różne obszary działania.

Thomas Hobbes (1588–1679) w dziele *Lewiatan, czyli materia, forma i władza państwa kościelnego i świeckiego* (*Leviathan or The Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil*, 1651) ujawnił specyfikę nowego paternalistycznego znaczenia państwa. Paternalizm w odniesieniu do społeczeństwa definiowano jako regulator działań subiektów procesów społecznych. Jego zdaniem ludzie rezygnują z części wolności, aby państwo mogło chronić ich przed chaosem i przemocą.

W epoce oświecenia model paternalizmu spotkał się z krytyką ze strony Johna Locka (1632–1704) w dziele *Dwa traktaty o rządzie* (*Two Treatises of Government*, 1689), Jeana-Jacques'a Rousseau (1712–1778) w *Umowie społecznej* (*Du contrat social ou Principes du droit politique*,

1762) i Immanuela Kanta (1724–1804) w *Metafizyce moralności* (*Die Metaphysik der Sitten*, 1797). Uważali oni paternalizm za rodzaj despotyzmu, sprzecznego z zasadami wolności i autonomii jednostki. Locke jako jeden z pierwszych oddzielił władzę polityczną od „opieki rodzicielskiej" i odrzucił paternalizm jako podstawową zasadę zarządzania państwem, kładąc podwaliny pod liberalną koncepcję ograniczonej władzy. Kant odrzucał paternalistyczny despotyzm, ale w jego koncepcji władzy obecna była idea regulacji i opieki w granicach prawa, co czasami interpretuje się jako „moralnie uzasadnioną opiekę".

Na różnych etapach rozwoju społecznego ujawniały się różne aspekty rozumienia paternalizmu w życiu społecznym, zmieniało się jego znaczenie funkcjonalne. Na wczesnym etapie rozwoju społecznego, opartego na stosunkach rodowych, paternalizm przybierał formę mechanizmu społecznego: zapewniał opiekę nad podporządkowaną społecznością, pełnił funkcję zewnętrznej ochrony przed zagrożeniami. W procesie ewolucji społecznej paternalizm rodowy stopniowo przekształcał się w paternalizm państwowy, gdy funkcje opieki, ochrony i zarządzania przechodziły ze starszyzny rodowej na instytucje polityczne i władców, którzy zaczynali występować w roli „ojców" swoich poddanych. Średniowiecze stało się impulsem do budowy systemu społeczno-gospodarczego o charakterze wasalnym, umacniając istotę paternalizmu jako zjawiska społecznego. W okresie renesansu i nowożytności nastąpiło odrzucenie istniejącego społeczno-religijnego paradygmatu rozwoju relacji paternalistycznych i kształtowanie się nowych form aktywności paternalistycznej. Przejawiały się one poprzez protekcjonizm wobec subiektów relacji paternalistycznych, zapewniając kontrolę i regulację ich zachowań.

XIX w. stał się okresem upowszechnienia paternalizmu w strukturach społecznych i gospodarczych, ale jednocześnie pojawiła się krytyka ograniczania wolności indywidualnych i kształtowania się idei antypaternalistycznych w tradycji liberalnej. John Stuart Mill (1806–1873) w dziele *O wolności* (*On Liberty*, 1859) podał klasyczną definicję paternalizmu w sensie etycznym i politycznym, określając dopuszczalne granice ingerencji państwa w wolność jednostki. Filozofia Milla położyła podwaliny pod współczesną liberalną krytykę paternalizmu i określiła kluczowe zasady, na których opiera się współczesne liberalne podejście do wolności

jednostki. Twierdził on, że ingerencja państwa lub społeczeństwa w życie jednostki jest dopuszczalna tylko w celu zapobiegania szkodom wyrządzanym innym, podczas gdy ograniczanie wolności jednostki „dla jej własnego dobra" jest niedopuszczalne: „Jednostka ma pełne prawo do swobodnego dysponowania sobą, własnym ciałem i umysłem". Takie podejście podkreśla priorytet autonomii jednostki, jej zdolności do samodzielnego podejmowania decyzji i ponoszenia odpowiedzialności za skutki własnych czynów, co leży u podstaw krytyki wszelkich paternalistycznych form władzy.

Osobnym przejawem paternalistycznego myślenia w XIX w. był tak zwany paternalizm kolonialny, który znalazł odzwierciedlenie w polityce państw europejskich wobec podbitych narodów. Idea „misji cywilizacyjnej" (imperium brytyjskie, francuskie itp.) usprawiedliwiała nierówność i dominację, przedstawiając podporządkowanie jako formę „opieki" nad mniej rozwiniętymi narodami. Warto tu wspomnieć o dyskusji wokół utworu angielskiego prozaika i poety Rudyarda Kiplinga (1865–1936) *Brzemię białego człowieka* (*The White Man's Burden*, 1899) napisanego po wojnie hiszpańsko-amerykańskiej, w wyniku której Stany Zjednoczone uzyskały kontrolę nad Filipinami. W utworze tym Kipling wzywa „białego człowieka" do podjęcia ciężaru misji cywilizacyjnej – „oświecania", „wychowywania" i „akulturacji" narodów kolonii, nawet jeśli nie są one wdzięczne lub stawiają opór. Po opublikowaniu poematu rozgorzała szeroka dyskusja międzynarodowa: zwolennicy teorii imperialnej odebrali utwór jako moralne usprawiedliwienie kolonializmu, rzekomo imperia przynosiły porządek, edukację i postęp; krytycy dostrzegli w tym przykrywkę dla wyzysku, rasizmu i kulturowej wyższości. Jednocześnie dyskusja wokół utworu zapoczątkowała szerszą krytykę imperialnego myślenia, stała się ideową granicą między kolonialnym paternalizmem XIX w. a krytyką paternalistycznej ideologii w XX stuleciu, kiedy opieka zaczęła być postrzegana nie jako moralny obowiązek, ale forma dominacji.

Procesy modernizacji i kształtowania państwa społecznego w XX w. nadały paternalizmowi nowe formy i treść; nabrał cech systemowej polityki społecznej, przejawiając się zarówno w działalności państwa, jak i relacjach między pracodawcą a obywatelem. W okresie międzywojennym paternalizm przybrał wiele form – od społeczno-ochronnej po

totalitarno-kontrolną. Jego wspólną cechą było postrzeganie państwa lub instytucji jako „opiekuna" obywateli, ale z różnym stopniem wolności i zależności. W latach międzywojennych można mówić o paternalizmie państwowym, społecznym i korporacyjnym.

Paternalizm państwowy był charakterystyczny dla reżimów autorytarnych i totalitarnych – faszystowskich Włoch (korporacyjne państwo Mussoliniego), nazistowskich Niemiec, ZSRR (radziecki model socjalistyczny). Państwo w tych krajach występowało jako „ojciec-żywiciel", który troszczył się o obywateli – praca, edukacja, mieszkanie, ale w zamian wymagał całkowitej lojalności politycznej. „Ojcowie narodów", tacy jak Włodzimierz Lenin, Józef Stalin, Adolf Hitler i inni, przejęli władzę, gdy życie społeczno-gospodarcze ich krajów znajdowało się w stanie kryzysu – naród potrzebował zjednoczenia wokół idei rozwoju państwa opartego na relacjach rodzinnych. W ten sposób paternalistyczna retoryka maskowała kontrolę, mobilizację i tłumienie wolności.

W demokratycznych krajach Europy Zachodniej, w odpowiedzi na niestabilność społeczną po I wojnie światowej, ukształtował się paternalizm socjalny. Przejawił się on w rozwoju systemów ubezpieczeń społecznych, ochrony pracy i wsparcia dla bezrobotnych. Taka troska państwa nie wiązała się z totalitarną kontrolą. Jednym z najwyraźniejszych przykładów pozytywnego, zorientowanego społecznie paternalizmu w okresie międzywojennym i powojennym jest szwedzki model państwa socjalnego. W latach 30. XX w., po wielkim kryzysie w Szwecji powstał rząd socjaldemokratyczny, który dążył do uniknięcia zarówno skrajności kapitalizmu, jak i totalitaryzmu. Koncepcję „domu ludowego" (*Folkhemmet*) przedstawił Per Albin Hansson (1885–1946) w 1928 r.; model ten jest metaforą państwa jako wspólnego domu, w którym wszyscy obywatele wnoszą swój wkład i mają równe prawa do opieki i ochrony (państwo powszechnego dobrobytu). Koncepcja ta jest używana do określenia długiego okresu między 1932 a 1976 r., kiedy to socjaldemokraci sprawowali władzę (z wyjątkiem krótkiego okresu w 1936 r.) i wcielali ją w życie. Model szwedzki nie wymagał politycznego posłuszeństwa w zamian za gwarancje socjalne. Ten typ paternalizmu stał się podstawą modelu „państwa społecznego" już po 1945 r.

Po II wojnie światowej w krajach o gospodarce rynkowej powstały różne modele państw socjalnych i – odpowiednio – odmienne mechanizmy realizacji polityki społecznej. W latach 50. i 60. XX w. nastąpił rozwój i rozkwit państwa socjalnego, znanego jako „państwo dobrobytu". W przeciwieństwie do paternalistycznych funkcji państwa, na pierwszy plan wysuwa się w nim zadanie kształcenia, szkolenia zawodowego i orientacji ludności na udział w pracy produkcyjnej. W powojennej Szwecji państwo aktywnie regulowało gospodarkę, redystrybuowało zasoby, zapewniało obywatelom gwarancje socjalne. To forma tak zwanego miękkiego (łagodnego) paternalizmu: państwo ingeruje w życie ludzi w celu zapewnienia równości i stabilności społecznej, ale jednocześnie szanuje prawa demokratyczne. Miękki lub libertariański paternalizm uznaje konieczność paternalizmu ze względu na istnienie anomalii behawioralnych, ale zamierza stosować tylko takie środki, które nie ograniczają swobody działania poszczególnych osób w podejmowaniu decyzji. W tym przypadku stosuje się wyłącznie „miękkie" (łagodne) metody: zachęcanie, przedstawianie informacji w taki sposób, aby pomóc ludziom w podejmowaniu decyzji leżących w ich długoterminowym interesie.

Paternalizm korporacyjny aktywnie rozwijał się w przemyśle: duże przedsiębiorstwa i korporacje zapewniały pracownikom mieszkania, opiekę medyczną, rozrywkę. Celem było zwiększenie ich lojalności i zapobieganie strajkom.

Współczesne użycie terminu paternalizm łączy idee opieki społecznej, kontroli moralnej i regulacji administracyjnej. Przejawia się on w różnych dziedzinach i często balansuje między ochroną jednostki a ograniczeniem jej wolności, łącząc historyczne tradycje opieki społecznej z najnowszymi wyzwaniami technologicznymi i moralnymi. Niektórzy badacze uważają, że można mówić o 3 wariantach paternalizmu: twardym, średnim i miękkim.

Model paternalizmu w sferze stosunków społeczno-państwowych opiera się na praktycznych wyobrażeniach o potrzebach ludności niezbędnych do harmonijnego funkcjonowania. Przykładami politycznego i państwowego paternalizmu mogą być przepisy prawne (np. dotyczące obowiązkowej edukacji lub pasów bezpieczeństwa), ulgi podatkowe lub dotacje mające na celu stymulowanie „pożytecznych" zachowań obywateli

(np. wsparcie dla „zielonych" technologii). Z drugiej strony, istnieje również aspekt państwowo-politycznego paternalizmu związany z lobbingiem, który we współczesnej przestrzeni społeczno-politycznej stanowi złożone zjawisko. Do czynników paternalizmu społecznego można zaliczyć programy pomocy społecznej mające na celu zaspokojenie podstawowych potrzeb, nawet jeśli jednostki same nie są w stanie skutecznie zadbać o siebie. Ekonomiczny i korporacyjny – programy korporacyjnego zabezpieczenia społecznego: ubezpieczenia, opieka medyczna, szkolenia dla pracowników; firmy technologiczne, które wprowadzają ograniczenia dla użytkowników (np. blokowanie szkodliwych treści, kontrola czasu korzystania z aplikacji). Bioetyczny lub medyczny – polityka dotycząca dawców organów lub środków kwarantannowych podczas epidemii. Cyfrowe/technologiczne – algorytmy i platformy, które ograniczają lub kierują użytkowników w celu zapewnienia im „bezpieczeństwa" (np. automatyczne blokowanie niebezpiecznych stron internetowych, rekomendacje „zdrowych" treści); zarządzanie prywatnością i danymi użytkowników w celu ochrony przed ryzykiem.

Dla współczesnych stosunków społecznych można zastosować formułę „paternalizm – partnerstwo", która nie narzuca decyzji, lecz łączy troskę, wsparcie i kontrolę z możliwością wyboru i uczestnictwa podmiotu. Jest to w istocie demokratyczna i nowoczesna odmiana paternalizmu, która zachowuje jego pozytywne funkcje (ochrona, pomoc) i minimalizuje ograniczenia wolności. W polityce państwowej może się to przejawiać poprzez udział obywateli w podejmowaniu decyzji za pośrednictwem konsultacji, wysłuchań publicznych, petycji elektronicznych (np. e-demokracja w Estonii); inicjatywy społeczne, kiedy państwo, zapewniając zasoby, pozwala społecznościom samodzielnie określać priorytety rozwoju (model samorządu lokalnego w krajach skandynawskich); programy edukacyjne, które zapewniają dostęp do wiedzy i wsparcia, lecz pozostawiają jednostce wybór kierunku kształcenia. W praktyce korporacyjnej przejawia się to w oferowaniu pracownikom kursów szkoleniowych, coachingu, świadczeń socjalnych, przy czym pracownicy sami decydują, jak z nich korzystać.

Jednym z głównych elementów współczesnego rozumienia paternalizmu jest postrzeganie go jako zjawiska międzynarodowego. Organizacje światowe występują jedynie jako narzędzie paternalistycznej interakcji na

mniej lub bardziej równoprawnych zasadach współistnienia w określonej przestrzeni. Ten typ relacji władzy działa jako środek osiągania harmonii i równowagi rozwoju światowego, ukierunkowany na budowanie partnerstwa i przeciwstawny z natury środkom przymusu w stosunkach między państwami. Głównym zagrożeniem paternalizmu w tej sferze relacji jest jego zewnętrzna aktywność, która może zagrażać suwerenności państwa i tożsamości narodowej w imię utrzymania ogólnego kierunku globalnego rozwoju społeczności międzynarodowej. Protekcjonizm gospodarczy pozostaje istotnym aspektem paternalistycznych relacji między państwem a społeczeństwem na poziomie międzynarodowym jako środek regulowania stosunków gospodarczych. Jedną z najczęściej stosowanych form takiego protekcjonizmu jest polityka państwa wobec importu towarów i usług. Idea takiego oddziaływania gospodarczego pozostaje popularna niezależnie od formy rządów i systemów politycznych, które mają wprowadzać ją w życie.

Zoya Baran

S. Aybar, O. Cark, *Paternalistic Leadership and Work Engagement in the Innovative Service Industry: The Mediating Role of Psychological Contract*, **„***Marketing and Management of Innovations***" 2023, no.** *14***(4),** https://doi.org/10.21272/mmi.2023.4-03**;** G. Kirchgässner, *Soft Paternalism, Merit Goods and Normative Individualism*, „European Journal of Law and Economics" 05.2015, https://www.researchgate.net/publication/277934117_Soft_Paternalism_Merit_Goods_and_Normative_Individualism (dostęp 12.10.2025); P. Łabieniec, *Paternalizm w prawie i etyce zawodowej*, „Filozofia Publiczna i Edukacja Demokratyczna" 2013, nr 2(2), https://doi.org/10.14746/fped.2013.2.2.22; L. Magnusson, *An economic History of Sweden*, Routledge, London 2000; О. Масюк, *Патерналізм як об'єкт соціально-філософської рефлексії*, Дисертація на здобуття наукового ступеня кандидата філософських наук, Запоріжжя 2006.

POLACY A SZTUCZNA INTELIGENCJA – relacja Polaków ze sztuczną inteligencją (SI) obejmuje zarówno poziom deklaratywny, związany z wiedzą o technologii, ocenami społecznymi, emocjami i przewidywaniami dotyczącymi jej rozwoju, jak i praktyczny, wyrażający się w rzeczywistym korzystaniu z narzędzi opartych na SI, kontakcie z treściami generowanymi algorytmicznie oraz sposobach oceny wiarygodności informacji.

W ostatnich latach, wraz z dynamicznym upowszechnieniem narzędzi generatywnych, zagadnienie to nabrało dodatkowego znaczenia: użytkownicy coraz częściej funkcjonują w środowisku informacyjnym, w którym część przekazów może mieć pochodzenie syntetyczne, a autorstwo treści (człowiek vs algorytm) nie zawsze jest możliwe do jednoznacznego ustalenia. Zjawisko to wpływa na sposoby budowania zaufania do informacji, strategie weryfikacji oraz poczucie kontroli nad własnym środowiskiem informacyjnym.

Badania dotyczące postaw Polaków wobec sztucznej inteligencji prowadzone są w wielu dyscyplinach i mają zróżnicowany charakter – od sondaży opinii publicznej, przez analizy informatologiczne, medioznawcze i socjologiczne, po opracowania koncentrujące się na konkretnych kontekstach zastosowań, takich jak rynek pracy, edukacja, usługi publiczne czy bezpieczeństwo. W ujęciu syntetycznym wyłania się obraz społeczeństwa, które w dużej mierze zna pojęcie sztucznej inteligencji i dostrzega jej obecność w przestrzeni medialnej, lecz równocześnie często przypisuje tej technologii znaczenia uproszczone, a wobec jej skutków przejawia postawy ambiwalentne: od ciekawości i pragmatycznej akceptacji po lęk, nieufność i obawy dotyczące bezpieczeństwa. Jak wynika z analiz prowadzonych przez Laboratorium Badań Medioznawczych Uniwersytetu Warszawskiego, postawy te mają charakter spolaryzowany i silnie zależny od kontekstu zastosowań SI: respondenci relatywnie chętnie aprobują konkretne rozwiązania wspierające codzienne funkcjonowanie, przy jednoczesnym sceptycyzmie wobec scenariuszy zakładających autonomiczne decyzje algorytmów.

Sam termin „sztuczna inteligencja" jest w Polsce szeroko rozpoznawalny społecznie i funkcjonuje zarówno w obiegu medialnym, jak i potocznym. Według danych CBOS większość respondentów deklaruje kontakt z tym pojęciem, jednocześnie nie potrafiąc go precyzyjnie zdefiniować. W narracjach użytkowników SI bywa utożsamiana przede wszystkim z automatyzacją procesów, robotyzacją, „inteligentnymi maszynami" lub ogólnie rozumianą nowoczesną technologią komputerową, rzadziej natomiast łączona jest z takimi kategoriami jak uczenie maszynowe, analiza dużych zbiorów danych czy modele statystyczne przetwarzające język naturalny. Zdaniem Marii Nowiny-Konopki powierzchowny charakter tej

wiedzy sprzyja dezorientacji poznawczej wynikającej z trudności w rozróżnianiu działań wykonywanych przez człowieka od tych realizowanych przez algorytmy, a także z rosnącej liczby interakcji z chatbotami, przypominających komunikację międzyludzką.

Brak pogłębionego rozumienia zasad funkcjonowania systemów SI prowadzi do występowania skrajnych ocen technologii – z jednej strony, postrzegania jej jako niemal autonomicznej i wszechmocnej, z drugiej – nieprzejrzystej i potencjalnie zagrażającej jednostce oraz społeczeństwu. Obie narracje mają wspólne źródło we fragmentarycznej wiedzy oraz dominacji medialnych uproszczeń. Jak podkreślają badacze, społeczne wyobrażenia SI częściej kształtowane są przez przekazy medialne niż przez rzeczywiste doświadczenia technologiczne.

Ekspozycja Polaków na sztuczną inteligencję w ostatnich latach systematycznie rośnie, przy czym ma ona charakter zróżnicowany i często pośredni. Dla wielu użytkowników kontakt z SI nie oznacza bezpośredniego korzystania z zaawansowanych narzędzi, lecz styczność z efektami ich działania, takimi jak zautomatyzowane rekomendacje treści, spersonalizowane reklamy, chatboty obsługi klienta czy materiały generowane algorytmicznie w przestrzeni medialnej. W tym sensie sztuczna inteligencja funkcjonuje w codziennym doświadczeniu Polaków jako element infrastruktury informacyjnej. Wysoki stopień ekspozycji Polaków na treści poruszające temat SI raportowali m.in. członkowie Laboratorium Badań Medioznawczych Uniwersytetu Warszawskiego w publikacji z 2024 r. *Polacy o sztucznej inteligencji*. W przeprowadzonym przez nich sondażu telefonicznym aż 71% respondentów deklarowało, że w ciągu ostatnich 12 miesięcy miało kontakt z mediami (artykułami, audycjami, programami) poruszającymi temat SI. Autorzy raportu podkreślili, że kontakt z treściami medialnymi na temat SI wyraźnie zwiększa szansę na społeczną akceptację tych rozwiązań, lecz niekoniecznie przekłada się na pogłębione zrozumienie mechanizmów właściwych tej technologii.

Wnioski te potwierdzają wyniki międzynarodowego badania *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025*. Wyodrębniono z niego dane dla Polski, co pozwoliło na nakreślenie obrazu postaw społecznych wobec SI i poziomu adaptacji tej technologii w wielu obszarach życia. Stwierdzono, że niemal 70% (dokładnie 69%) respondentów

z Polski deklaruje, że korzysta z SI co najmniej raz na kilka miesięcy, przy czym aż 90% badanych stwierdziło, że nie jest świadome istnienia żadnych regulacji dotyczących AI. Większość Polaków wykorzystujących AI korzysta z narzędzi dostępnych publicznie i bezpłatnie. Co ciekawe, aż 89% badanych z Polski uważa, że stosowanie SI zwiększa ryzyko cyberzagrożeń, a 44% stwierdza, że osobiście doświadczyło skutków takiego incydentu.

Szczególnym wymiarem współczesnej ekspozycji na SI jest rosnąca obecność treści generowanych przez duże modele językowe (tekstów, obrazów i materiałów audiowizualnych) w ogólnie pojętej przestrzeni informacyjnej. Użytkownicy coraz częściej spotykają się z przekazami, których pochodzenie nie jest jednoznacznie oznaczone, co utrudnia rozróżnienie materiałów stworzonych przez człowieka od tych wygenerowanych przez systemy sztucznej inteligencji. Badania prowadzone w Polsce wskazują, że świadomość istnienia treści syntetycznych jest relatywnie wysoka, jednak doświadczenia użytkowników w zakresie ich identyfikacji i krytycznej oceny pozostają zróżnicowane. Część respondentów deklaruje zdolność rozpoznawania materiałów generowanych przez SI, inni natomiast przyznają, że w praktyce rozróżnienie to bywa trudne lub niemożliwe.

Postawy Polaków wobec sztucznej inteligencji charakteryzują się wyraźną ambiwalencją. W badaniach opinii publicznej konsekwentnie pojawia się obraz społeczeństwa, w którym ciekawość, umiarkowany optymizm i akceptacja instrumentalna współistnieją z lękiem, nieufnością oraz poczuciem zagrożenia. Jednym z najczęściej identyfikowanych wzorców jest selektywna aprobata konkretnych zastosowań SI, zwłaszcza wtedy, gdy są one postrzegane jako usprawniające codzienne funkcjonowanie lub wspomagające pracę człowieka. Jednocześnie obawy budzą scenariusze, w których sztucznej inteligencji przypisywana jest zdolność autonomicznego podejmowania decyzji lub zastępowania człowieka w obszarach wymagających odpowiedzialności i zaufania społecznego.

W strukturze emocji towarzyszących postrzeganiu SI istotną rolę odgrywa lęk odnoszący się przede wszystkim do potencjalnych skutków społecznych, ekonomicznych i informacyjnych tej technologii. Według danych CBOS respondenci najczęściej wskazują obawy związane z utratą miejsc pracy, pogłębianiem nierówności społecznych, osłabieniem relacji międzyludzkich oraz nadużyciami związanymi z manipulacją informacją.

Równolegle obserwuje się jednak postawy świadczące o ciekawości i umiarkowanym optymizmie, częściej deklarowane przez osoby mające bezpośrednie doświadczenia z korzystaniem z narzędzi opartych na SI. Raport NASK i Międzynarodowej Organizacji Pracy wskazuje, że użytkownicy regularnie korzystający z SI częściej dostrzegają jej użyteczność i potencjał wspomagający, podczas gdy osoby unikające tej technologii częściej zgłaszają brak zaufania oraz poczucie utraty kontroli.

Jednym z kluczowych obszarów debaty społecznej pozostaje wpływ sztucznej inteligencji na rynek pracy i gospodarkę. Polacy postrzegają rozwój SI zarówno jako szansę na zwiększenie efektywności i innowacyjności, jak i zagrożenie dla stabilności zatrudnienia. W narracjach respondentów silnie obecne są obawy związane z automatyzacją pracy oraz niepewnością zawodową, szczególnie w odniesieniu do profesji postrzeganych jako podatne na zastąpienie przez algorytmy. Jednocześnie część badanych wskazuje na potencjał SI jako narzędzia wspomagającego pracę człowieka, redukującego obciążenia rutynowe i wspierającego procesy decyzyjne. Istotnym elementem tych ocen jest także ryzyko pogłębiania nierówności społecznych wynikających z różnic w poziomie kompetencji cyfrowych. Stosunek Polaków do SI w kontekście wykorzystania tej technologii w miejscu pracy badany był m.in. przez Ogólnopolski Panel Badawczy Ariadna dla ThinkTank w 2025 r. Jak wynika z tych analiz, ponad połowa (51%) Polaków widzi AI bardziej w kategoriach zagrożeń niż korzyści, jednak liczba osób dostrzegających więcej zalet systematycznie się zwiększa. Większość respondentów (58%) obawia się, że AI odbierze pracę wielu osobom, a wśród zawodów najbardziej zagrożonych przez AI respondenci wskazywali tłumaczy, telemarketerów i pracowników obsługi klienta. Zdaniem badanych najmniej zagrożeni w tym kontekście są lekarze, specjaliści PR oraz artyści.

Wraz z upowszechnieniem sztucznej inteligencji coraz wyraźniej artykułowane są też kwestie związane z bezpieczeństwem jednostki i społeczeństwa. Obejmują one zarówno zagrożenia techniczne, takie jak naruszenia prywatności i cyberataki, jak i problemy o charakterze informacyjnym i poznawczym, związane z jakością, wiarygodnością oraz kontrolą nad obiegiem informacji. Szczególnie istotne jest ryzyko informacyjne wynikające z powszechności treści generowanych przez SI, takie

jak dezinformacja, manipulacja oraz trudności w odróżnianiu materiałów prawdziwych od syntetycznych. Badania empiryczne prowadzone wśród polskich studentów wskazują, że świadomość powszechności treści generowanych przez SI obniża poczucie bezpieczeństwa informacyjnego użytkowników, nasilając odczucia nieufności, podatności na manipulację oraz trudności w ocenie wiarygodności przekazów. Bezpośredni kontakt z materiałami syntetycznymi wiąże się ponadto z poczuciem konieczności wzmożonej weryfikacji informacji, obciążeniem poznawczym oraz lękiem o własny i cudzy dobrostan informacyjny. W tym kontekście bezpieczeństwo informacyjne przestaje być wyłącznie kategorią techniczną, a staje się doświadczeniem subiektywnym, powiązanym z emocjami, zaufaniem i poczuciem kontroli nad własnym środowiskiem medialnym. Brak jednoznacznych oznaczeń treści generowanych przez SI dodatkowo pogłębia niepewność użytkowników i sprzyja postulatom wprowadzenia czytelnych standardów identyfikacji materiałów syntetycznych.

Dynamiczny rozwój sztucznej inteligencji unaocznił również rolę kompetencji związanych z krytycznym korzystaniem z tej technologii, określanych mianem *AI literacy*. Badania prowadzone w tym zakresie ukazują rozbieżność pomiędzy deklarowaną pewnością użytkowników w zakresie oceny wiarygodności informacji a rzeczywistymi umiejętnościami rozpoznawania i weryfikowania treści syntetycznych. Szczególnie problematyczne okazuje się identyfikowanie materiałów wysokiej jakości, pozbawionych oczywistych błędów formalnych. Brak powszechnej wiedzy o narzędziach detekcyjnych oraz rzadkie korzystanie z takich rozwiązań pogłębiają lukę kompetencyjną, a nadmierna pewność siebie użytkowników może prowadzić do obniżonej czujności poznawczej. Rozwijanie *AI literacy* wymaga zatem nie tylko przekazywania wiedzy technicznej, lecz także kształtowania postaw refleksyjnych wobec technicznych limitów AI oraz własnych ograniczeń poznawczych. Coraz częściej podkreśla się rolę instytucji edukacyjnych, bibliotek, mediów i administracji publicznej w budowaniu świadomego i odpowiedzialnego podejścia do sztucznej inteligencji.

Analiza dotychczasowych badań pozwala zatem stwierdzić, że sztuczna inteligencja stała się trwałym elementem społecznej i informacyjnej rzeczywistości Polaków, a kontakt z jej zastosowaniami ma dla wielu

użytkowników charakter codzienny, choć często pośredni i nie w pełni uświadomiony. Społeczna percepcja SI cechuje się ambiwalencją, w której akceptacja instrumentalna współistnieje z lękiem i nieufnością. Szczególnie istotnym obszarem napięć pozostaje problematyka bezpieczeństwa, odnoszona zarówno do ochrony danych i systemów technicznych, jak i poczucia bezpieczeństwa informacyjnego użytkowników. Upowszechnienie treści generowanych przez sztuczną inteligencję nadwyręża zaufanie odbiorców do jakości informacji, zwiększa obciążenie poznawcze oraz wymusza nowe strategie weryfikacji przekazów. W tym kontekście kompetencje informacyjne i *AI literacy* stają się kluczowym zasobem umożliwiającym adaptację do zmieniającego się środowiska medialnego. Relacja Polaków ze sztuczną inteligencją wydaje się procesem dynamicznym, kształtowanym przez doświadczenia użytkowe, przekazy medialne, regulacje instytucjonalne oraz poziom kompetencji informacyjnych społeczeństwa. Jej zrozumienie stanowi istotny warunek projektowania skutecznych działań edukacyjnych, komunikacyjnych i regulacyjnych, sprzyjających odpowiedzialnemu i bezpiecznemu wykorzystaniu potencjału sztucznej inteligencji.

Paulina Motylińska, Anna Pieczka-Węgorkiewicz

K. Brylska, *Polacy o sztucznej inteligencji. Raport z sondażu telefonicznego LBM UW*, Laboratorium Badań Medioznawczych UW, Warszawa 2024, https://www.lbm.uw.edu.pl/18-publikacje/raporty-empiryczne (dostęp 7.12.2025); T. Gackowski, *Między lękiem przed inteligentnymi maszynami a zaufaniem do nowych technologii. Postrzeganie sztucznej inteligencji w badaniach opinii publicznej*, [w:] *Wiedza – komunikacja – działanie. Praktyki medialne w zdigitalizowanym świecie*, A. Hess, M. Nowina Konopka, W. Świerczyńska-Głownia (red.), Instytut Dziennikarstwa, Mediów i Komunikacji Społecznej Uniwersytetu Jagiellońskiego, Kraków 2025; *Komunikat z badań: Sztuczna inteligencja w opiniach Polaków*, Fundacja Centrum Badania Opinii Społecznej, Warszawa 2024, https://www.cbos.pl/SPISKOM.POL/2024/K_093_24.PDF (dostęp 7.12.2025); R. Lange, *Raport z badań społecznych: Sztuczna inteligencja w społeczeństwie i gospodarce*, https://cyberprofilaktyka.pl/badania/RAPORT_AI_ONLINE.pdf (dostęp 15.12.2025); D. Maison, *Raport z badania: Polacy o sztucznej inteligencji w miejscu pracy*, https://think-tank.pl/wp-content/uploads/2025/11/raport_dmaison_ai_081025.pdf (dostęp 15.12.2025); *Między ciekawością a niepewnością. Pokolenia Polaków*

wobec sztucznej inteligencji – wiedza, doświadczenia, nastroje, 2025, https://pwr.edu.pl/uczelnia/aktualnosci/polacy-a-sztuczna-inteligencja--niepewni--ale-ciekawi-co-przyniesie-przyszlosc-13795.html (dostęp 7.12.2025); P. Motylińska, A. Pieczka-Węgorkiewicz, *Poczucie bezpieczeństwa informacyjnego w dobie rozwoju generatywnej sztucznej inteligencji: badanie wstępne*, [w:] *Horyzonty informacji 7*, P. Korycińska (red.), Uniwersytet Jagielloński, Kraków 2025; M. Nowina Konopka, *Każdy zna się na AI. Przegląd badań polskiej opinii publicznej na temat sztucznej inteligencji*, „Zeszyty Prasoznawcze" 2023, t. 66, nr 4(256); *Sztuczna inteligencja w Polsce: krajobraz pełen paradoksów*, 2025, https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2025/07/pl-Raport-KPMG-w-Polsce-KPMG-AI-Trust-2025-web.pdf (dostęp 15.12.2025); M. Troszyński, *Generatywna sztuczna inteligencja a polski rynek pracy. Raport badawczy*, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, Warszawa 2025, https://www.nask.pl/media/2025/06/Generatywna-sztuczna-inteligencja-a-polski-rynek-pracy.pdf (dostęp 7.12.2015).

POLSKIE FORMACJE POLICYJNE W OKRESIE II WOJNY ŚWIATOWEJ. Klęska Polski we wrześniu 1939 r., utrata niepodległości i podział ziem polskich na części okupowane przez III Rzeszę i ZSRR sprawiły, że całe ówczesne pokolenie Polaków znalazło się pod jedną bądź drugą okupacją. Te prawidłowości znalazły potwierdzenie w stosunku do funkcjonariuszy Policji Państwowej.

Formacja ta we wrześniu 1939 r. liczyła około 35 tys. osób. Zgodnie z przyjętymi planami siły te w razie konfliktu zbrojnego miały podlegać komendantowi głównemu PP na obszarze nieobjętym stanem wojennym, natomiast na pozostałym – naczelnemu wodzowi; działaniami policji miał kierować tam szef żandarmerii. Błyskawiczne tempo ofensywy wojsk niemieckich spowodowało, że plany te nie zostały zrealizowane. Jest rzeczą charakterystyczną, że we wszystkich anektowanych bądź podbitych przez III Rzeszę krajach na okupowanym terytorium powoływano do służby miejscową policję. Tak było i w Polsce.

Po krótkim okresie zarządu wojskowego i rozwiązaniu straży obywatelskich rozkazem Wyższego Dowódcy SS i Policji z dnia 30 października 1939 r. powołano do służby wszystkich funkcjonariuszy Policji Państwowej znajdujących się na obszarze Generalnego Gubernatorstwa, utworzonego 4 dni wcześniej. Źródłem uzupełnień byli policjanci wysiedleni z ziem wcielonych do Rzeszy lub tam aresztowani i deportowani do Generalnego

Gubernatorstwa. Była to tzw. Policja Polska lub granatowa (ze względu na kolor mundurów). Jako służba pomocnicza pozostawała w pionie niemieckiej policji porządkowej; była kontynuacją Policji Państwowej w sensie organizacyjnym (te same urzędy i budynki) oraz kadrowym, a także formalnoprawnym; obowiązywały ją przedwojenne regulaminy i przepisy służbowe. Nie istniało oczywiście żadne wyższe dowództwo na szczeblu dystryktu ani komendy głównej.

Formalnie Policja Polska została powołana w dniu 17 grudnia 1939 r. Niemcy nałożyli na nią obowiązek pełnej bieżącej ochrony bezpieczeństwa i porządku publicznego. Według zaleceń Heinricha Himmlera niemiecka policja miała wkraczać tylko wówczas, jeśli wymagał tego interes niemiecki. Do stałych czynności Policji Polskiej należały: patrole prewencyjno-interwencyjne, nadzór nad stanem sanitarnym, regulacja ruchu kołowego, służba na dworcach kolejowych, kontrola obowiązku meldunkowego. Dochodził do tego nadzór nad bierną obroną przeciwlotniczą oraz podstawowe szkolenie Żydowskiej Służby Porządkowej sprawującej wewnętrzną służbę w gettach. Ponadto polscy policjanci musieli uczestniczyć wraz z Niemcami w łapankach, eskortowaniu ludzi do obozów przejściowych, obławach, ochronie obozów pracy przymusowej. Zmuszeni byli asystować przy egzekucjach oraz brać udział w działaniach skierowanym przeciw partyzantom. Bardzo niewielkie uprawnienia Policja Polska miała natomiast w stosunku do umundurowanych i cywilnych Niemców – możliwe tylko w wypadku zabójstwa. Dopuszczały one interwencję w stanie wyższej konieczności oraz w przypadku braku policji niemieckiej na miejscu zdarzenia.

PP była jedyną polską służbą uzbrojoną. Wyposażenie funkcjonariusza stanowił najczęściej pistolet z 5–20 nabojami lub karabin z 10–60 sztukami amunicji. Dopełnieniem były pałka i bagnet. Bardzo ważne stało się objęcie PP sądownictwem SS i policji 5 maja 1942 r., a od 1944 r. rozciągnięto je na rodziny policjantów. W wypadku „samowolnego opuszczenia służby przez członków policji cudzoziemskiej w Generalnym Gubernatorstwie", utraty broni bądź munduru sprawa była traktowana jako przestępstwo polityczne i groziło to obozem koncentracyjnym lub karą śmierci. Najważniejszym źródłem zasilania PP była powołana 1 października 1941 r. w Nowym Sączu Szkoła Policyjna Policji Polskiej GG.

Przeszkoliła ona około 3 tys. kandydatów. Komendantem szkoły był mjr Wincenty Słoma – żandarm austriacki, potem polski, emerytowany w 1952 r., a jego zastępcą Polak – mjr Antoni Pikor.

Szczupłość policyjnych sił niemieckich i narastanie ruchu oporu były powodem wydania przez Himmlera rozkazu z dnia 6 grudnia 1943 r. o powołaniu jednostek do ochrony składów i obiektów wojskowych, ale także działań skierowanych przeciw partyzantom. Formacje te tworzono drogą dobrowolnego lub przymusowego zaciągu, a składały się w 2/5 z obywateli okupowanych krajów. W latach 1942–1945 w Polsce, Jugosławii i ZSRR sformowano 250 takich batalionów. Ochotników do tworzonego w Polsce 202 batalionu było 2 (!). W tej sytuacji pozostali zostali do niego odkomenderowani. Oddział kwaterował w Krakowie, a w czasie akcji występował w umundurowaniu niemieckim. Część jego funkcjonariusz zdezerterowała i zasiliła szeregi 27 Wołyńskiej Dywizji Piechoty AK.

W 1940 r. służba śledcza została wyłączona z Policji Polskiej i przekształcona w Policję Kryminalną (PK). W ramach niemieckich urzędów Policji Kryminalnej (Kripo) istniały odtąd oddziały polskiej PK, których dyrekcje znajdowały się w Warszawie, Krakowie, Lublinie, a od 1941 r. także we Lwowie. W dystrykcie Radom w każdym komisariacie PP istniały 2–3-osobowe agentury kryminalne. Polscy funkcjonariusze zyskiwali dzięki temu możliwości dotarcia do ważnych wiadomości, co niejednokrotnie okazywało się bardzo ważne w kontekście ich kontaktów z ruchem oporu. Kadra Policji Kryminalnej szkolona była w Szkole Policji Bezpieczeństwa i SD w Rabce Zdroju. Istnienie Policji Polskiej jako zwartej formacji uzyskało aprobatę zarówno władz emigracyjnych, jak i podziemnych w kraju. Uważano bowiem, że wprowadzenie w jej miejsce wyłącznie policji niemieckiej będzie szkodliwe dla społeczeństwa oraz dla dalszej walki z okupantem.

Oficjalne kierownictwo policji tworzyło jakby konspiracyjny sztab nadzorczy, tak by w odpowiednim momencie można było jej użyć. Chwili takiej spodziewano się już wiosną 1940 r. w nadziei na odmianę, jaką przyniosą działania frontu zachodniego. Koncepcja ta załamała się, kiedy w dniu 7 maja 1940 r. aresztowano wszystkich 69 oficerów warszawskiej PP. Wiązało się to z uderzeniem na Belgię, Holandię i Francję oraz rozpoczęciem akcji AB (likwidacja czołowych przedstawicieli inteligencji).

Aresztowani oficerowie byli wprawdzie zwalniani, ale nie wszyscy: jednych wywieziono do Oświęcimia, inni nie powrócili do służby, pozostali znowu się w niej znaleźli. W tej sytuacji aktualne stało się wykorzystanie kadry policyjnej przez różne ośrodki konspiracyjne.

Wyróżnić można 3 formy współpracy policji granatowej z ruchem oporu: odgórnie kierowana budowa struktur o charakterze konspiracyjnym wewnątrz oficjalnych komórek PP i PK; udział policjantów w działalności organizacji podziemnych; indywidualne zaangażowanie policjantów w różnych, nieraz niezorganizowanych formach oporu. Struktury podziemne, które opierały się na urzędach i funkcjonariuszach Polskiej Policji, to przede wszystkim Państwowy Korpus Bezpieczeństwa i referat Policyjny w Wydziale Bezpieczeństwa i Kontrwywiadu Oddziału II Komendy Głównej AK. Komendantem głównym PKB został ppłk Mieczysław Kozielewski, zastępcą – ppłk Stanisław Wasilewski, a szefem sztabu – mjr Bolesław Buyko.

Od końca 1942 r. rozpoczął się znaczny wzrost szeregów Państwowego Korpusu Bezpieczeństwa (PKB), co było konsekwencją decyzji władz Armii Krajowej o przejściu do PKB funkcjonariuszy PP związanych z konspiracją wojskową oraz z Ludowej Straży Bezpieczeństwa. Komendantem głównym został adwokat Stanisław Tabisz, ze Stronnictwa Ludowego. W październiku 1943 r. liczebność całego PKB (bez dystryktu lubelskiego) wynosiła 8400 funkcjonariuszy. Z PKB współpracował Wojskowy Korpus Służby Bezpieczeństwa (WKSB) – rodzaj policji wojskowej. Obie te formacje ujawniły się w trakcie powstania warszawskiego, przejmując komisariaty Policji Polskiej. Bardzo ważnym aspektem działalności PP była współpraca z ogniwami kontrwywiadu wszystkich szczebli Związku Walki Zbrojnej – Armii Krajowej. Powiązania z Policją Polską posiadały wszystkie liczące się organizacje wojskowe i polityczne: od Gwardii Ludowej – Armii Ludowej, poprzez Bataliony Chłopskie, po Narodowe Siły Zbrojne, jak również wywiad radziecki. Straty osobowe, jakie ponosiła PP, były relatywnie duże.

Przyjmuje się, że w 1942 r. na terenie Generalnego Gubernatorstwa co 4 dni ginął policjant. Śmierć dosięgała oczywiście tych, którzy jednoznacznie współpracowali z okupantem, jak osoby zaangażowane w podziemną walkę z nim. O tym, że zaufanie władz okupacyjnych do Policji

Polskiej było mocno ograniczone, świadczy fakt, że żaden z 3 stopni alarmu na wypadek powstania nie przewidywał użycia PP. Przeciwnie, w najwyższym zakładano aresztowanie i rozbrojenie całej PP, a nawet jej fizyczną likwidację.

W 2000 r. społeczność policyjna w Polsce obchodziła „okrągłą" 60 rocznicę zbrodni popełnionej przez sowieckie NKWD na policjantach II Rzeczypospolitej. Moralny obowiązek wobec ofiar oraz wspólnota munduru i wykonywanego zawodu każe współcześnie żyjącym policjantom pamiętać o tej zbrodni. Przeprowadzona została ekshumacja zwłok funkcjonariuszy pomordowanych i pochowanych w Miednoje, a 2 września 2000 r. uroczyście otwarto i poświęcono ich cmentarz. „Był policjantem, to wystarczy, by go rozstrzelać" – powiedział na jednym z przesłuchań szef kalinińskiego NKWD Dmitrij Stefanowicz Tokariew, później generał bezpieczeństwa państwowego w Kazaniu. Według danych szacunkowych we wrześniu 1939 r. internowano na Kresach Wschodnich 12 tys. funkcjonariuszy i pracowników policji. Sposób traktowania jeńców zmieniał się w zależności od tego, czy dana grupa walczyła z oddziałami Armii Czerwonej, czy też poddawała się bez walki. Dowódcy tej armii początkowo nie mieli jasnych dyrektyw, jak postępować z określonymi kategoriami jeńców. Potwierdzają to policjanci, którym udało się przeżyć wojnę: brano ich do niewoli kilkukrotnie i następnie zwalniano.

Jednakże już 19 września 1939 r. radziecki komisarz spraw wewnętrznych Ławrientij Beria podjął decyzję o utworzeniu Zarządu do spraw Jeńców Wojennych i Internowanych (rozkaz nr 0308), a następnego dnia wydał dyrektywę, w której nakazał organizowanie obozów przejściowych i rozdzielczych. Na jej mocy powstały obozy jenieckie, w których przetrzymywano ok. 15 tys. Polaków. Znajdowały się one w pomieszczeniach poklasztornych w Kozielsku, Starobielsku i Ostaszkowie. Tam właśnie, na przełomie października i listopada 1939 r., skierowano pierwsze transporty polskich jeńców. Policjanci byli przewożeni do Ostaszkowa, do obozu o zaostrzonym rygorze, gdzie poza policjantami umieszczono również funkcjonariuszy Służby Granicznej, Służby Więziennej, żołnierzy Korpusu Ochrony Pogranicza, Żandarmerii Wojskowej i Oddziału II Sztabu Głównego, sędziów i prokuratorów oraz osadników wojskowych (ze wschodniej części II RP) i duchownych. Obóz został zlokalizowany

kilkanaście kilometrów od Ostaszkowa, na jednej z wysp jeziora Seliger, w pomieszczeniach poklasztornych prawosławnego monastyru Niłowa Pustyń. W przeciwieństwie do obozu kozielskiego i staro-bielskiego, które w głównej mierze były obozami oficerskimi, w ostaszkowskim w grudniu 1939 r. przebywały 6364 osoby, w tym: 48 oficerów wojska, 240 oficerów policji i żandarmerii, 775 podoficerów i 4924 szeregowych policji, 189 funkcjonariuszy Służby Więziennej, 9 agentów służb wywiadowczych, 5 osób duchownych, 35 osadników, 4 kupców, 4 byłych więźniów polskich, 5 pracowników sądownictwa, 72 szeregowców i podoficerów WP oraz 54 innych jeńców. Byli oni zakwaterowani w 20 prawie nieogrzewanych budynkach. Normy żywnościowe obliczono tak, aby służyły wyłącznie podtrzymywaniu życia, ale nie zaspokajały głodu. Ponadto jeńcy zostali poddani oddziaływaniu propagandowemu, w trakcie którego m.in. wygłaszano pogadanki, prowadzono indywidualne rozmowy, pokazywano filmy propagujące „osiągnięcia" Związku Radzieckiego.

Pod koniec 1939 r. władze ZSRR rozpoczęły przygotowania do ostatecznego rozwiązania problemu polskich jeńców wojennych; w tym celu skierowano do Ostaszkowa grupę dochodzeniową Siergieja Biełopileckiego, która miała przygotować – do końca stycznia 1940 r. – „akta jeńców wojennych – policjantów byłej Polski" na specjalną naradę tzw. „trójki" w centrali NKWD w Moskwie, mającej „zaocznie skazać w trybie administracyjnym polskich jeńców na śmierć" (na podstawie kodeksu karnego SFRR z 1926 r., art. 58, par. 13 – „za aktywną działalność" lub „aktywną walkę […] przeciwko klasie robotniczej i ruchowi rewolucyjnemu"). Ostatecznie los policjantów z Ostaszkowa przesądzony został 5 marca 1940 r. na posiedzeniu Biura Politycznego KC WKP(b) w składzie: Józef Stalin, Kliment Woroszyłow, Wiaczesław Mołotow, Anastas Mikojan i Łazar Kaganowicz. Wówczas podjęto decyzję akceptującą wniosek Berii o rozpatrzeniu w trybie specjalnym, z zastosowaniem kary śmierci przez rozstrzelanie, spraw 14 736 polskich jeńców, w tym 1030 oficerów i podoficerów policji, ochrony pogranicza i żandarmerii oraz 5138 szeregowych policji, żandarmerii, więziennictwa i wywiadu. Wniosek swój Beria uzasadniał tym, iż „wszyscy oni są zatwardziałymi, nierokującymi poprawy wrogami władzy radzieckiej".

W oparciu o te materiały z narady specjalnej Zarząd do spraw Jeńców Wojennych i Internowanych sporządził zbiorowe imienne listy do rozstrzelania, które rozesłał do obozów w kwietniu i maju 1940 r., gdyż wtedy „ziemia była na tyle rozmarznięta, iż można było już kopać zbiorowe groby". Dla obozu ostaszkowskiego przygotowano 64 listy zbiorcze, z danymi o 6263 osobach. Jednocześnie wydano polecenie „wyprawienia" tych osób do Kalinina. Poczyniono też przygotowania w gmachu kalinińskiego zarządu obwodowego NKWD związane z „rozładowaniem" obozu w Ostaszkowie. W tym celu w podziemiach gmachu NKWD przygotowano dźwiękochłonną celę śmierci, a z Moskwy sprowadzono mechaniczną koparkę do wykopywania dołów na zwłoki zamordowanych ofiar. Akcję likwidacyjną obozu w Ostaszkowie rozpoczęto 4 kwietnia 1940 r. Stan osobowy obozu wynosił w tym czasie 6364 osoby, w tym m.in. 5938 policjantów i żandarmów (ci ostatni stanowili niewielki odsetek tej liczby). Skazani na uśmiercenie funkcjonariusze polscy pędzeni byli z monastyru do przystanku kolejowego Soroga, a stamtąd – przez Lichosław – transportowano ich do Kalinina. Następnie ze stacji przewożeni byli karetkami więziennymi – *cziornymi woronomi* – do zarządu obwodowego NKWD przy ulicy Sowieckiej, gdzie umieszczano ich w podziemnych celach budynku. Po zapadnięciu zmroku przystępowano do egzekucji.

Wyglądało to następująco: „W jednym z obszernych pomieszczeń piwnicznych, tzw. czerwonym kąciku […] sprawdzono personalia skazanego, następnie skuwano go i przeprowadzano do znajdującej się tuż obok celi śmierci, o drzwiach zaopatrzonych w tkaninę wojłokowa. […] Po zaciągnięciu do celi śmierci ofiara była od razu mordowana strzałem w tył głowy. Zwłoki wynoszono na zewnątrz i układano na jednym z 5–6 oczekujących samochodów ciężarowych", po czym o świcie przewożono je do miejscowości Miednoje, nad rzeką Twiercą. Tam, na terenie rekreacyjnym kalinińskiego NKWD, grzebano zwłoki zamordowanych w uprzednio przygotowanych przez koparki dołach o głębokości 4 m, a każdy z nich mógł pomieścić „plon" jednej nocy, tj. 250–300 zamordowanych. Dołów takich w Miednoje znajduje się 25; pogrzebano w nich 6288 jeńców z obozu z Ostaszkowa.

Akcję „rozładowania" (mordowania) jeńców z Ostaszkowa zakończono 13 maja 1940 r. Rolę katów spełniało prawie 30 osób, lecz najbardziej

w tym względzie „wyróżniał" się major bezpieczeństwa państwowego ZSRR Władimir Błochin. Pół roku później wszyscy oni otrzymali – rozkazem specjalnym Berii z 26 października 1940 r. – nagrody „za skuteczne wypełnianie zadań specjalnych". Wynosiły one około 800 rubli, tj. tyle, ile otrzymywali co miesiąc pensji. Podstawą zbrodni katyńskiej były dwa dokumenty. Pierwszy z nich – datowany na 5 marca 1940 r. – to propozycja Berii wymordowania polskich jeńców; drugi natomiast – z tą samą datą – decyzja Biura Politycznego WKP(b) akceptująca tę propozycję, tj. wymordowania polskich jeńców wojennych i więźniów.

Andrzej Czop

A. Czop, M. Sokołowski, *Historia polskich formacji policyjnych od II Wojny Światowej do czasów współczesnych*, „Kultura Bezpieczeństwa" 2013, t. 13; H. Ćwięk, *Polska Policja Generalnego Gubernatorstwa w okupacyjnym systemie bezpieczeństwa Trzeciej Rzeszy*, „Przegląd Policyjny" 2021, nr 3(143); J. Grabowski, *Na posterunku. Udział polskiej policji granatowej i kryminalnej w zagładzie Żydów*, Wydawnictwo Czarne, Warszawa 2020; W. Grabowski, *Policja w planach Delegatury Rządu RP na kraj*, Księgarnia Akademicka, Kraków 1995; A. Hempel, *Pogrobowcy klęski. Rzecz o policji „granatowej" w Generalnym Gubernatorstwie 1939–1945*, Państwowe Wydawnictwo Naukowe, Warszawa 1990; A. Hempel, *Policja granatowa w okupacyjnym systemie administracyjnym Generalnego Gubernatorstwa: 1939–1945*, Instytut Wydawniczy Związków Zawodowych, Warszawa 1987; A. Misiuk, *Historia Policji w Polsce – od X wieku do współczesności*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2012; W. Pobóg-Malinowski, *Katastrofa wrześniowa*, Wydawnictwo im. Olofa Palme, Warszawa 1987.

POMOC HUMANITARNA jest formą wsparcia materialnego, technicznego i logistycznego udzielanego ludności dotkniętej skutkami katastrof wywołanych przez czynniki naturalne lub działalność człowieka. Podejmowana jest w możliwie najkrótszym czasie po wystąpieniu zdarzenia, którego skutki przekraczają możliwości reagowania lokalnych struktur państwowych i społecznych, w sytuacjach, gdy władze publiczne lub inne podmioty lokalne są przeciążone, niezdolne bądź niechętne do skutecznego działania. Celem pomocy humanitarnej jest prowadzenie działań opartych na rzeczywistych potrzebach w sytuacjach kryzysowych, ukierunkowanych na ratowanie i ochronę życia, zapobieganie ludzkiemu

cierpieniu, jego łagodzenie, zachowanie godności osób poszkodowanych oraz przywracanie elementarnych, godnych warunków egzystencji.

Fundament pomocy humanitarnej stanowią zasady humanitaryzmu, neutralności, bezstronności, niezależności. Ponadto jej świadczenie odbywa się na zasadach dobrej pomocy humanitarnej, ścisłej współpracy między wszystkimi podmiotami zaangażowanymi w jej niesienie, adekwatności, szybkości, możliwie niskich kosztów administracyjnych. Szczegółowy katalog 24 *Zasad i dobrych praktyk donatorstwa humanitarnego* (ang. *Principles and Good Practice of Humanitarian Donorship*) opracowano w ramach inicjatywy Dobre Donatorstwo Humanitarne (ang. Good Humanitarian Donorship, GHD) (zob. *Zasady świadczenia pomocy humanitarnej*).

Działania humanitarne obejmują zarówno udzielanie pilnego wsparcia ukierunkowanego na ochronę życia w czasie kryzysu humanitarnego lub bezpośrednio po jego wystąpieniu, jak również działania służące zapewnieniu dostępu do osób potrzebujących poprzez stworzenie warunków do bezpiecznego i niezakłóconego dostarczania pomocy oraz swobodnego przemieszczania się personelu humanitarnego.

Pomoc humanitarna nie stanowi narzędzia zarządzania kryzysowego państwa, nie jest też tożsama z interwencją humanitarną ani z pomocą rozwojową. Różnica między pomocą a interwencją humanitarną opiera się na kwestii zgody oraz użycia siły. Udzielenie pomocy humanitarnej wymaga zgody państwa-beneficjenta, a w sytuacji konfliktu zbrojnego – również stron konfliktu. Nie może być traktowana jako ingerencja w sam konflikt ani wrogie działanie, ale neutralna, bezstronna i niezależna odpowiedź na potrzeby ludności cywilnej. Z kolei interwencja humanitarna wiąże się z użyciem siły zbrojnej na terytorium innego państwa bez jego zgody, choć z reguły powołuje się na mandat Rady Bezpieczeństwa ONZ i deklarowany cel powstrzymania masowych, rażących naruszeń praw człowieka lub międzynarodowego prawa humanitarnego. Różnica między pomocą humanitarną a rozwojową dotyczy czasu, celu i zasad; ta pierwsza jest zazwyczaj krótkotrwała – stanowi natychmiastową odpowiedź na sytuacje kryzysowe pojawiające się w regionach niezależnie od poziomu ich rozwoju gospodarczego, które zagrażają życiu i zdrowiu ludzi. Ukierunkowana jest na ratowanie życia i łagodzenie cierpienia powstającego na skutek nagłych

wydarzeń. Opiera się na zasadach humanitaryzmu, neutralności, bezstronności i niezależności, które zapewniają jej apolityczny charakter. Z kolei pomoc rozwojowa jest długoterminowa i stanowi długofalową inwestycję w transformację społeczną i gospodarczą; jej celem jest wsparcie rozwoju gospodarczego, społecznego i politycznego w krajach rozwijających się, zwłaszcza w odpowiedzi na problemy systemowe. Odwołuje się do zasady solidarności, ale może być wykorzystywana przez państwa do osiągania swoich celów politycznych na arenie międzynarodowej, co oznacza, że nie zawsze przestrzega tych samych zasad apolityczności i neutralności.

Pomoc humanitarna realizowana jest na 3 wzajemnie powiązanych poziomach. Na międzynarodowym kształtowane są podstawowe zasady jej świadczenia, takie jak humanitaryzm, neutralność, bezstronność i niezależność, a także ustanawiane są fundamentalne prawa przysługujące osobom dotkniętym kryzysami humanitarnymi, w szczególności prawo do ochrony życia, dostępu do żywności, odzieży oraz schronienia. Poziom unijny polega na operacjonalizacji tych zasad i praw poprzez tworzenie konkretnych mechanizmów zarządzania pomocą humanitarną obejmujących instrumenty finansowe, ramy współpracy oraz systemy koordynacji działań pomiędzy państwami członkowskimi Unii Europejskiej. Natomiast na poziomie krajowym państwa implementują przyjęte normy i mechanizmy w drodze własnych regulacji prawnych, budowy odpowiednich struktur instytucjonalnych oraz stosowania procedur umożliwiających skuteczne udzielanie pomocy humanitarnej. Każdy z tych poziomów pełni komplementarną rolę: międzynarodowy nadaje ramy, regionalny buduje narzędzia, krajowy zapewnia wykonanie.

Międzynarodowe podstawy prawne świadczenia pomocy humanitarnej wynikają z prawa międzynarodowego publicznego, międzynarodowego prawa humanitarnego konfliktów zbrojnych, praw człowieka, rezolucji i praktyki organizacji międzynarodowych. Fundamentem jest Karta Narodów Zjednoczonych z 1945 r. (art. 1(3), art. 55 i 56), która nie definiuje pomocy humanitarnej, ale tworzy legitymację prawną dla działań humanitarnych ONZ i jej agend oraz współpracy państw w tym zakresie. Normatywnie wiążącą podstawę prawną pomocy humanitarnej w czasie konfliktów zbrojnych stanowią konwencje genewskie z 12 sierpnia 1949 r. wraz z protokołami dodatkowymi, w szczególności:

- artykuł 3 wspólny dla konwencji określający „minimum humanitarne" i przyznający Międzynarodowemu Komitetowi Czerwonego Krzyża prawo do inicjatywy humanitarnej;
- IV Konwencja genewska o ochronie osób cywilnych podczas wojny przewidująca m.in. pomoc osobom podlegającym ochronie, obowiązek dopuszczenia dostaw pomocy humanitarnej, ochronę personelu i środków pomocy (np. art. 30, 38(1), 59–61, 63, 108–110, 142);
- artykuł 70 protokołu dodatkowego I nt. działań pomocy o charakterze humanitarnym i bezstronnym w warunkach konfliktu międzynarodowego;
- artykuł 18 protokołu dodatkowego II regulujący prawo ludności cywilnej do otrzymywania pomocy humanitarnej oraz warunki jej świadczenia w konfliktach o charakterze niemiędzynarodowym;
- zasady prawa humanitarnego nr 31 (poszanowanie i ochrona personelu pomocy humanitarnej), nr 32 (poszanowanie i ochrona obiektów wykorzystywanych w operacjach pomocy humanitarnej).

Prawo międzynarodowe dotyczące praw człowieka nie reguluje bezpośrednio pomocy humanitarnej, ale tworzy normatywne uzasadnienie jej świadczenia. Kluczowe dokumenty stanowią:

- Międzynarodowy pakt praw obywatelskich i politycznych z 1966 r. chroniący prawo do życia (art. 6), wolność od tortur, nieludzkiego, poniżającego traktowania lub karania (art. 7);
- Międzynarodowy pakt praw gospodarczych, społecznych i kulturalnych z 1966 r. uznający prawo każdego do odpowiedniego poziomu życia dla niego samego i jego rodziny, włączając w to wyżywienie, odzież i mieszkanie oraz prawo do korzystania z najwyższego osiągalnego poziomu ochrony zdrowia fizycznego i psychicznego (art. 11, 12);
- Konwencja o prawach osób niepełnosprawnych z 2006 r. zobowiązująca państwa-strony do podejmowania wszelkich koniecznych działań służących zapewnieniu ochrony oraz bezpieczeństwa osób z niepełnosprawnościami w sytuacjach

zagrożenia, obejmujących konflikty zbrojne, kryzysy wymagające pomocy humanitarnej oraz klęski żywiołowe (art. 11).

Naruszenie tych praw w sytuacjach kryzysowych stanowi zatem materialną przesłankę uruchomienia pomocy humanitarnej.

Ramy systemowe pomocy humanitarnej wyznacza Rezolucja Zgromadzenia Ogólnego ONZ nr 46/182 (1991). Powołuje ona Koordynatora Pomocy w Sytuacjach Nadzwyczajnych (ang. Emergency Relief Coordinator, ERC), który w 1992 r. otrzymał status Podsekretarza Generalnego ds. Humanitarnych, będącego globalnym rzecznikiem osób dotkniętych kryzysami i głównym doradcą Sekretarza Generalnego ONZ we wszystkich kwestiach humanitarnych, Stały Komitet Międzyagencyjny (Inter-Agency Standing Committee, IASC), Skonsolidowany Proces Odwoławczy oraz Centralny Fundusz ds. Pomocy w Sytuacjach Kryzysowych jako kluczowe mechanizmy koordynacji i narzędzia Koordynatora. Z kolei konwencja z Tampere w sprawie zapewnienia zasobów telekomunikacyjnych dla łagodzenia skutków katastrof oraz na potrzeby operacji ratowniczych z dnia 18 czerwca 1998 r. reguluje zasady współpracy międzynarodowej w zakresie udostępniania infrastruktury telekomunikacyjnej podczas katastrof, znosząc bariery dotyczące korzystania z przydzielonych częstotliwości, ograniczeń importu sprzętu telekomunikacyjnego, a także dotyczących przemieszczania się ekip humanitarnych. Legalność, zakres i charakter działań pomocowych poszczególnych podmiotów świadczących pomoc humanitarną określają również mandaty i statuty organizacji, np. statut Międzynarodowego Komitetu Czerwonego Krzyża i jego mandat wynikający bezpośrednio z konwencji genewskich, statut Międzynarodowego Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca, mandaty agend wyspecjalizowanych ONZ (np. UNHCR, UNICEF, WFP, WHO). Znaczenie praktycznie, choć prawnie niewiążące, ma również Kodeks postępowania dla Międzynarodowego Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca i organizacji pozarządowych w przypadkach klęsk i katastrof z 1994 r. oraz Karta humanitarna przedstawiająca kontekst prawny i etyczny Zasad ochrony, Podstawowego standardu humanitarnego oraz Standardów minimalnych zawartych w podręczniku Sfery, tj. projektu utworzonego w 1997 r. przez grupę pozarządowych organizacji humanitarnych oraz Czerwony Krzyż i Ruch Czerwonego Półksiężyca, ukierunkowanego na

poprawę dostarczanej jakości pomocy humanitarnej oraz zwiększenie odpowiedzialności za podejmowane działania.

Unijne ramy pomocy humanitarnej wyznacza:

– prawo pierwotne:

- Traktat o Unii Europejskiej z 1992 r., art. 21, który nie reguluje pomocy humanitarnej wprost, ale wyznacza aksjologiczne ramy działań zewnętrznych UE, w tym ochronę praw człowieka, poszanowanie prawa międzynarodowego, współpracę i solidarność międzynarodową celem niesienia pomocy narodom, krajom i regionom dotkniętym klęskami żywiołowymi lub katastrofami spowodowanymi przez człowieka;
- Traktat o funkcjonowaniu Unii Europejskiej z 2007 r., art. 214 stanowiący bezpośrednią podstawę prawną prowadzenia przez UE działań w zakresie pomocy humanitarnej w państwach trzecich, współpracy z organizacjami międzynarodowymi (ONZ, ICRC), tworzenia Europejskiego Ochotniczego Korpusu Pomocy Humanitarnej;

– prawo wtórne:

- Rozporządzenie Rady (WE) nr 1257/96 z dnia 20 czerwca 1996 r. dotyczące pomocy humanitarnej;
- Wspólne oświadczenie Rady i przedstawicieli rządów państw członkowskich zebranych w Radzie, Parlamencie Europejskim i Komisji Europejskiej (2008/C 25/01) – „Konsensus europejski w sprawie pomocy humanitarnej";
- Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (wersja skonsolidowana po zmianach: Decyzji Parlamentu Europejskiego i Rady (UE) 2019/420 z dnia 13 marca 2019 r. zmieniającej decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności, Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/836 z dnia 20 maja 2021 r. zmieniającego decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności, Decyzji Parlamentu Europejskiego i Rady (UE) 2023/2671 z dnia 22 listopada 2023

r. zmieniającej decyzję nr 1313/2013/UE w celu przedłużenia okresu przejściowego rescEU);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/888 z dnia 20 maja 2021 r. ustanawiające program Europejski Korpus Solidarności oraz uchylające rozporządzenia (UE) 2018/1475 i (UE) nr 375/2014;
- Rozporządzenie Rady (UE) 2016/369 z dnia 15 marca 2016 r. w sprawie udzielania wsparcia w sytuacjach nadzwyczajnych na terenie Unii.

Krajowe ramy prawne pomocy humanitarnej wyznacza:
- Konstytucja Rzeczypospolitej Polskiej z 1997 r., która nie używa wprost pojęcia „pomoc humanitarna", ale tworzy aksjologiczną i normatywną podstawę zaangażowania państwa w pomoc humanitarną, w tym poza granicami RP (art. 9 – przestrzeganie wiążącego Polskę prawa międzynarodowego; art. 146, ust. 1, ust. 4, pkt 1, 9 – kompetencje Rady Ministrów w zakresie polityki wewnętrznej i zagranicznej, wykonania ustaw, kierownictwa w dziedzinie stosunków z innymi państwami i organizacjami międzynarodowymi);
- Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. 2025, poz. 1275) – art. 32.1(5);
- Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz.U. 2003, nr 96, poz. 873);
- Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2009, nr 157, poz. 1240);
- Ustawa z dnia 16 września 2011 r. o współpracy rozwojowej (Dz.U. 2011, nr 234, poz. 1386) – art. 2.1(2), 5.2, 10.2, 13.1(7);
- Ustawa z dnia 12 maja 2022 r. o Zespole Pomocy Humanitarno-Medycznej (Dz.U. 2022, poz. 1095);
- Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024, poz. 1907) – art. 3.4, 4.1(4)k, n, 8.6, 11.1(14), 13.1(15), 13.2(3), 15.1(17), 15.2(3), 17.1(16), 19.1(4), 33.1, 38.6, 38.7, 128.3(3), 170;

- Ustawa z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej (Dz.U. 2003, nr 128, poz. 1176);
- Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (Dz.U. 2022, poz. 583);
- Ustawa z dnia 16 listopada 1964 r. o Polskim Czerwonym Krzyżu (Dz.U. 1964, nr 41, poz. 276);
- Konkordat między Stolicą Apostolską i Rzeczpospolitą Polską z dnia 28 lipca 1993 r. (Dz.U. 1998, nr 51, poz. 318) – art. 21, 22.1;
- Ustawa z dnia 17 maja 1989 r. o stosunku Państwa do Kościoła Katolickiego w Rzeczypospolitej Polskiej (Dz.U. 2023, poz. 1966) – art. 38–40.

Za organizację pomocy humanitarnej na poziomie międzynarodowym odpowiada Biuro Koordynacji Pomocy Humanitarnej ONZ (ang. Office for the Coordination of Humanitarian Affairs, OCHA), które powstało w 1998 r. w wyniku przekształcenia Departamentu Spraw Humanitarnych (ang. Department of Humanitarian Affairs, DHA), utworzonego w 1992 r. Jego mandat obejmuje koordynację działań humanitarnych, rozwój polityki i działania rzecznicze w zakresie pomocy humanitarnej. OCHA pełni funkcję koordynacyjną za pośrednictwem IASC, któremu przewodniczy ERC. Na poziomie Unii Europejskiej pomoc humanitarna świadczona jest za pośrednictwem Dyrekcji Generalnej Komisji Europejskiej ds. Pomocy Humanitarnej i Ochrony Ludności (Directorate-General for European Civil Protection and Humanitarian Aid Operations, DG ECHO) utworzonej w 1992 r., która początkowo działała jako Biuro Pomocy Humanitarnej. Na poziomie krajowym zaś – przede wszystkim poprzez wpłaty na rzecz organizacji i instytucji międzynarodowych, a także wsparcie finansowe udzielane polskim organizacjom pozarządowym prowadzącym działalność humanitarną. W związku z atakiem Rosji na Ukrainę w 2022 r. polski rząd utworzył mechanizm pomocy humanitarnej obejmujący wsparcie pochodzące m.in. z Rządowej Agencji Rezerw Strategicznych i innych instytucji państwa, środków samorządowych, społecznych i prywatnych, którym koordynuje Kancelaria Prezesa Rady Ministrów wraz z Ministerstwem Spraw Zagranicznych, Ministerstwem

Spraw Wewnętrznych i Administracji, Rządową Agencją Rezerw Strategicznych oraz właściwymi wojewodami.

Klaudia Cenda-Miedzińska

Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (tekst mający znaczenie dla EOG), Dz.U. L 347 z 20.12.2013; *Pomoc humanitarna w świetle prawa i praktyki*, P. Grzebyk, E. Mikos-Skuza (red.), Wydawnictwo Scholar, Warszawa 2016; Rozporządzenie Rady (WE) nr 1257/96 z dnia 20 czerwca 1996 r. dotyczące pomocy humanitarnej, Dz.U. L 163 z 2.07.1996, s. 1–6; UN General Assembly, *Strengthening of the coordination of humanitarian emergency assistance of the United Nations*, A/RES/46/182, 12.1991; Wspólne oświadczenie Rady i przedstawicieli rządów państw członkowskich zebranych w Radzie, Parlamencie Europejskim i Komisji Europejskiej, Dz.U. C 25 z 30.01.2008, s. 1–12.

POPULIZM ANTYIMIGRANCKI – termin, który charakteryzuje zjawisko wykorzystywania strachu, uprzedzeń i stereotypów przez populistycznych polityków wobec imigrantów celem zdobycia wyborców. Zjawisko to używa imigrantów jako jednego z elementów zagrożenia bezpieczeństwa na różnych jego poziomach i w różnych obszarach, np. kulturowego, ekonomicznego, i przeciwstawienia ich samych oraz ich kultury wartościom kręgu kulturowego państwa, od którego przybywają.

Sam termin „populizm" jest dla badaczy problematyczny i co najmniej nieprecyzyjny, nie ma też wśród nich zgody, czy stosowanie go w naukach społecznych jest właściwe. Istnieje kilka podejść metodologicznych do tego terminu. Definicję, na którą powołuje się wielu badaczy, stworzył Cas Mudde, badacz radykalizmu prawicowego, dla którego populizm jest ideologią charakteryzującą się 2 cechami: antyelityzmem, czyli przekonaniem, że społeczeństwo podzielone jest na 2 przeciwstawne sobie grupy – jedną z nich stanowią „*pure people* – zwykli porządni ludzie (lud)", natomiast drugą – elity: złe i skorumpowane; oraz suwerennością społeczeństwa (ludu), którą rozumie jako zasadę, „że polityka ma realizować wolę ludu (*general – will*) wyrażoną bezpośrednio, to jest bez udziału politycznych instytucji".

Główną osią definicji populizmu u Roregsa Brubakera jest kategoria „ludu", ale jego ujęcie, w odróżnieniu od Muddego, podkreśla jednak, że

„dyskursywne konstruowanie" tej kategorii odbywa się, po pierwsze, poprzez kontrastowanie jej z politycznymi, ekonomicznymi i kulturowymi elitami (wymiar wertykalny), a po drugie – poprzez przeciwstawianie jej grupom postrzeganym jako zewnętrzne wobec wspólnoty zamkniętej, takim jak uchodźcy, imigranci czy inne mniejszości (wymiar horyzontalny).

Problem z pojęciem populizmu i uznaniem go za ideologię wiąże się z niemożnością porównania go z tradycyjnymi ideologami, z powodu ubogiej treści. Niektórzy autorzy mówią o nim jako o paraideologii, choć to nie wyklucza łączenia go z różnymi rzeczywistymi ideologiami, o czym najlepiej świadczą przykłady z historii XX w. Kluczowe dla populizmu jest wywieranie wpływu na odbiorcę pewnymi stałymi metodami: demagogią, kłamstwem, podsycaniem konfliktów, antagonizmami. Współcześnie używają ich np. Recep Tayyip Erdogan, Władimir Putin, Viktor Orban czy Donald Trump. Populizm nie jest jednak zarezerwowany jedynie dla prawicy, istnieje także lewicowy populizm, który w Polsce do tej pory odrywał marginalną rolę, posługując się uboższą tematyką, najczęściej dotyczącą ekonomii i niesprawiedliwości (zwykle różnego rodzaju mniejszości, np. etnicznych, płciowych itd.).

Populizm bywa też rozumiany jako ruch społeczno-polityczny, którego wyrazem są wystąpienia, w trakcie których wyrażane są „postulaty «klasy ludowej», krytycyzm wobec polityki prowadzonej przez «elity» i żądanie zmian". Antyelityzm i poczucie zdrady narodu przez elity, zdaniem Jerzego Reykowskiego, w Polsce pojawiły się w latach 90. XX w., „a partia polityczna Prawo i Sprawiedliwość upolitycznia to przekonanie. Ruchem populistycznym była też np. Solidarność o silnym antyelitystycznym nastawieniu i dążeniu do suwerenności «ludzi pracy»".

Populizm w opinii autorów może być także – i jest dla populistycznych partii – sposobem uprawiania polityki i formą przywództwa politycznego. Jako przykłady takich działań podaje się dojście do władzy w demokratycznych wyborach, ale – przy okazji rządów partii populistycznych – przy użyciu półlegalnych lub nielegalnych metod w celu osiągnięcia sukcesu politycznego (np. próby fałszowania wyborów, zamykanie w więzieniach lub pozbawianie życia oponentów politycznych itd.). Jednocześnie sposób prowadzania polityki przez taką władzę ma

przypodobać się wspomnianym „klasom ludowym", przy jednoczesnym ignorowaniu potrzeb innych grup.

Populizm może być także rozumiany jako postawa polityczna, czyli promowanie idei populistycznych, np. w postaci poparcia wyrażanego dla jakiejś partii, władzy i podporządkowanie się jej przywódcy. Używa różnych narzędzi i mechanizmów do osiągania swoich celów, a jednym z nich jest tzw. „wielkie kłamstwo" (*big lie*), uznawane przez Josepha P. Forgasa i Williama D. Crano za ulubione narzędzie populizmu. Różnym zagrożeniom ma przeciwdziałać w środowiskach populistycznych „upolitycznienie wiedzy potocznej". Populizm wiąże się też z uznawaniem za prawdziwe informacji pochodzących z mało wiarygodnych źródeł i przetwarzanie ich w myślenie spiskowe.

Mechanizmy populizmu są różne, z powodu różnych uwarunkowań psychologicznych człowieka; jednym z podstawowych może być zła sytuacja ekonomiczna (*economic distress*), niespowodowana brakiem środków do życia, tylko głębszym przekonaniem o niesprawiedliwości w procesie porównywania siebie do osób należących do innej grupy, „które w poczuciu danej jednostki wcale na takie wyróżnienie nie zasługują. Jest to zjawisko, które określa się jako deprywacja względna. Reakcją na nią jest gniew". Innym mechanizmem może być niezadowolenie ze swojej sytuacji dotyczące innych sfer życia niż ekonomiczne, np. tożsamościowej, „i różnych motywów z tą sferą związanych. Jednym z nich jest poczucie własnej wartości, które w społeczeństwach, w których dużą rolę odgrywa ideologia rynkowa, bywa związane z sytuacją materialną danej osoby". Nie jest tutaj istotne, kto rzeczywiście ma mniej, ale jak jest widziany przez innych oraz – przede wszystkim – czy postrzega siebie jako kogoś gorszego. Bardzo istotnym mechanizmem populizmu, zwłaszcza w przypadku antyimigranckiego, jest poczucie zagrożenia w stosunku do siebie i własnej grupy uzasadniane groźbą napływu imigrantów, szczególnie gdy mowa o uchodźcach i imigrantach nielegalnych.

Widmo tego zagrożenia dotyka kilku obszarów, a jednym z nich jest bezpieczeństwo kulturowe. W tym kontekście zagrożeniem może być obcość kulturowa imigrantów, potencjalny konflikt z rodzimymi wartościami, normami i tradycjami, a także napływ obcych wartości,

w tym religijnych (np. napięcia między islamem a chrześcijaństwem). Szczególnym przykładem populizmu skierowanego przeciwko osobom z odmiennych kręgów kulturowych jest populizm islamofobiczny, który może zagrażać tożsamości narodowej. W kontekście imigrantów wywodzących się z kultury islamu pojawia się również zagrożenie terroryzmem lub przestępczością; tym samym poparcie dla takich populistycznych idei może być traktowane jako przeciwdziałanie tym niebezpieczeństwom. Innym zagrożeniem eksponowanym przez populistów jako argument przeciwko imigrantom są kwestie ekonomiczne – przybywający imigranci przedstawiani są jako konkurencja w pozyskiwaniu wsparcia socjalnego oraz na rynku pracy, a także przyczynek do zaniżania wynagrodzenia. Jak pokazują dane CBOS z 2024 r., Polacy właściwie powszechnie wyrażają akceptację dla podejmowania przez cudzoziemców pracy w Polsce (93% – za, 4% – przeciwko), a grupą, która uważa, że powinni mieć możliwość podjęcia dowolnej pracy, są respondenci pomiędzy 35 a 44 rokiem życia, „mieszkańcy największych miast, […] najlepiej wykształceni, kadra kierownicza i specjaliści oraz pracownicy usług, a także ankietowani lepiej sytuowani. […] Sprzeciw wobec pracy cudzoziemców w naszym kraju w większym stopniu niż inni wyrażają ankietowani najsłabiej wykształceni, robotnicy niewykwalifikowani i respondenci uzyskujący najniższe dochody w przeliczeniu na osobę w gospodarstwie domowym". Zdaniem ekspertów antyimigracyjność dla wielu populistów jest tożsama z antyeuropejskością – to Unia Europejska, według populistycznych uproszczeń, sprowadza do Europy imigrantów, a wraz z nimi – zagrożenia bezpieczeństwa. W Polsce przeciwnicy imigracji nie widzieli konieczności tworzenia ruchów społecznych, które zaliczane są do ruchów protestu, ponieważ tematyka antyimigracyjna została wykorzystana przez ugrupowania rządzące: „W Polsce […] ów protest mógł być wykorzystany w ograniczonym stopniu, głównie do wyrażania niezadowolenia z polityki UE w tym obszarze".

Imigracji nie pomagają media społecznościowe – jako platforma wymiany informacji pozostająca poza kontrolą i nadzorem – umożliwia powielanie stereotypów i schematy, np. imigranta lub uchodźcy terrorysty. Statystyki dowodzą natomiast, że to właśnie kraje, do których migranci napływają najliczniej, odnoszą z tego największe korzyści (np. wzrost

PKB, zwiększenie produktywności, wypełnienie luk w pracy niechętnie wykonywanej przez rodzimych mieszkańców, zwiększenie aktywności zawodowej wśród kobiet z powodu możliwości wcześniejszego powrotu na rynek pracy itp.). Wzrost antyimigranckich haseł wywołało w ostatnich latach kilka czynników – ataki terrorystyczne w Europie (mimo że „zagrożenia terroryzmem na terytorium Unii Europejskiej nie można utożsamiać wyłącznie z działalnością fundamentalistów islamskich. W krajach europejskich nadal niebezpiecznym nurtem jest terroryzm separatystyczny, skrajnie lewicowy czy prawicowy. Największym zagrożeniem w przypadku terroryzmu islamistycznego […] są osoby utożsamiające się z fundamentalizmem islamskim i skłonne stosować terroryzm, ale nieujawniające publicznie swoich przekonań"), kryzys migracyjny w 2015 r. w związku z wojną domową w Syrii, Libii i konfliktem w Libanie, wojna w Ukrainie i migracja jej ludności, choć Europy dotyczą także wcześniejsze kryzysy migracyjne, np. te związane z obywatelami państw trzecich i napiętą sytuacją polityczno-ekonomiczną w Afryce Północnej, Subsaharyjskiej, na całym Bliskim Wschodzie, ale i na Bałkanach.

Populizm antyimigrancki wyraża się podejmowaniem różnych działań przez ugrupowania, partie populistyczne używającego retoryki antyimigranckiej, wskazując na skalę mobilizacji (np. setki miast, tysiące uczestników). Przykładami polskich partii, które używają takich figur, są Prawo i Sprawiedliwość oraz Konfederacja, a działania, które podjęły w ostatnim roku, to protesty, np. 80 manifestacji w całej Polsce pod hasłem „Stop imigracji" zorganizowanych przez Konfederację czy manifestacja PiS w Warszawie, z wiodącym wątkiem migracji, ale odbywająca się pod szerszym hasłem „W obronie Polski".

Agenda antyimigracyjna stanowi ważny komponent tożsamości grup radykalnie prawicowych, aczkolwiek brak akceptacji, niechęć, obawy wobec imigrantów i imigracji nie są zarezerwowane jedynie dla środowisk skrajnie prawicowych i w sprzyjających warunkach mogą skutkować właśnie rozwojem społecznych ruchów antyimigracyjnych, niekoniecznie związanych z radykalną prawicą.

Według danych CBOS z 2025 r. ocena skutków obecności przybyszów w Polsce jest zróżnicowana. 69% badanych podziela opinię, „że cudzoziemcy nadmiernie obciążają system świadczeń socjalnych". Minimalnie

mniej, bo 66% respondentów uważa, że obecność imigrantów „przyczynia się do wzrostu przestępczości w naszym kraju". Niebezpiecznym dla ankietowanych problemem jest zaniżanie stawek na rynku pracy przez obecność imigrantów (55%), ale równocześnie 65% badanych ma świadomość uczestnictwa podatków obcokrajowców wpłacanych do budżetu państwa. 51% rozumie, że Polska „potrzebuje obcokrajowców, ponieważ polskie społeczeństwo się starzeje. Prawie połowa (48%) zgadza się z opinią, że obcokrajowcy są niezbędni, aby polska gospodarka się rozwijała (przeciwnego zdania jest jednak 42% respondentów)". Istnieje korelacja między poglądami politycznymi i światopoglądowymi, jeśli chodzi o sympatię dla obcokrajowców: „Najbardziej przychylnym stosunkiem do mieszkających w Polsce cudzoziemców wyróżniają się osoby deklarujące lewicowe poglądy polityczne i nieuczestniczące w praktykach religijnych".

Jeśli chodzi o postrzeganie zagrożenia kulturowego jako jednego z aspektów przybywania imigrantów, według CBOS 40% badanych jest zdania, „że należy przyjmować obcokrajowców, którzy są nam bliscy pod względem kulturowym lub religijnym". 36% nie widzi przeciwskazań w napływie „do Polski uchodźców – osób uciekających przed różnego rodzaju zagrożeniami. Co 10 badany uważa, że każdy, kto ma taką wolę, powinien móc osiedlić się w Polsce. Jedynie 6% jest w ogóle przeciwne osiedlaniu się cudzoziemców w Polsce".

Jak wynika z badania stosunku Polaków do uchodźców oraz postrzegania zagrożenia płynącego z ich strony w analizie Polskiego Sondażu Uprzedzeń z 2021 r. opracowanego przez Paulinę Górską, respondenci dwojako traktują uchodźców, w zależności od ich pochodzenia. Wskazywane były 2 typy zagrożeń: symboliczne (np. dotyczące zagrożenia ze strony kultury muzułmańskiej) i realistyczne (np. zagrożenia dla rynku pracy). „Ukraińców [Polacy, przyp. – KPC] traktowali jednak odmiennie – tutaj niewiele osób uznawało cudzoziemców za jakiekolwiek zagrożenie. Podobnie było z mierzoną skalą dystansu społecznego akceptacją uchodźców – o ile Ukraińców zdecydowanie akceptowano, o tyle innych uchodźców akceptowano w zdecydowanie mniejszym stopniu".

W narracji ruchów antyimigracyjnych widoczne jest sekurytyzowanie imigracji, jak również polityki UE w tym obszarze; ponadto interpretowanie tego problemu w perspektywie konfliktu kulturowego na linii

„my"–„obcy". Dotyczy to jednak głównie jednej grupy imigrantów – z Azji i Afryki. W zdecydowanie mniejszym stopniu odnosi się do imigrantów z Białorusi i imigrantów oraz uchodźców wojennych z Ukrainy. Nie można jednak wykluczyć zmiany w przyszłości.

Katarzyna Pabis-Cisowska

M. Bilewicz, *Psychologiczne źródła dystansu. Czyli dlaczego unikamy kontaktu z obcymi?*, „Nauka" 2016, nr 2; M. Bilewicz, *Stosunek do imigrantów w Polsce. Konsekwencje kontaktu i mowy nienawiści*, „Migracje – Historia i Teraźniejszość" 2023; M. Duszczyk, *Czy migracje położą kres UE*, „Rocznik Strategiczny" 2015/2016; https://www.europarl.europa.eu/topics/pl/article/20180703STO07125/terroryzm-w-ue-ataki-ofiary-smiertelne-i-zatrzymania-w-2019-r (dostęp 8.12.2025); https://www.pap.pl/aktualnosci/konfederacja-chce-zamkniecia-granic-dla-nielegalnej-imigracji-srodowiska-lewicowe (dostęp 8.12.2025); https://www.polityka.pl/tygodnikpolityka/kraj/2318101,1,manifestacja-pis-w-warszawie-przeciw-migracji-mercosur-rzadowi-i-na-zlosc-konfederacji.read (dostęp 8.12.2025); A. Lipiński, *W poszukiwaniu ontologii populizmu – dylematy definicyjne*, „Przegląd Polityczny" 2020, nr 1; C. Mudde, *Exclusionary vs. inclusionary populism: comparing contemporary Europe and Latin America*, „Government and Opposition" 2013, vol. 48; *Postrzegana i postulowana obecność cudzoziemców w Polsce* [komunikat z badań, nr 31/2025], B. Rogucka (oprac.), CBOS 04.2025; *Praca obcokrajowców w Polsce* [komunikat z badań, nr 32/2025], M. Feliksiak (oprac.), CBOS 04.2025; J. Reykowski, *Populizm jako choroba demokracji*, „Nauka" 2023, nr 3; E. Szyszlak, *Współczesne ruchy antyimigranckie w Polsce w kontekście kryzysów uchodźczego i migracyjnych. Zarys problematyki*, „Studia Politologiczne" 2023, t. 68.

POPULIZM PRAWICOWY – w publicystyce często używa się go szeroko, jako etykiety dla bardzo różnych zjawisk: od partii skrajnej prawicy po konserwatywnych krytyków integracji europejskiej. W literaturze politologicznej próbuje się jednak wprowadzić większy porządek, wychodząc od osobnego zdefiniowania elementu „prawicowego" oraz „populistycznego", a następnie analizując ich połączenie. Taki sposób postępowania pozwala odróżnić prawicowy populizm zarówno od klasycznej prawicy, jak i innych odmian populizmu: lewicowego czy centrowego.

Punkt wyjścia stanowi samo pojęcie „prawicy", które ma co najmniej kilka wymiarów. Na osi ekonomicznej tradycyjnie wiąże się je z większym zaufaniem do rynku, sceptycyzmem wobec rozbudowanego państwa

opiekuńczego i przywiązaniem do ochrony własności prywatnej. Na osi kulturowej „prawicowość" oznacza zwykle akcentowanie wartości takich jak tradycja, religia, porządek społeczny, hierarchia, a także nieufność wobec gwałtownych zmian obyczajowych czy eksperymentów społecznych. Wreszcie, w wymiarze tożsamościowym prawica częściej odwołuje się do idei narodu, wspólnoty historycznej, symboliki państwowej i patriotyzmu. Oczywiście, konkretne nurty prawicy mogą różnić się programowo: konserwatywno-liberalne, narodowe, chrześcijańsko-demokratyczne czy neoliberalne inaczej rozkładają akcent między gospodarką, kulturą a tożsamością. W kontekście prawicowego populizmu szczególnie ważny okazuje się wymiar kulturowo-tożsamościowy, związany z naciskiem na naród jako wyobrażoną wspólnotę oraz spójność kulturową i religijną.

W literaturze opisującej współczesną prawicę często pojawia się także pojęcie nativizmu i autorytaryzmu. Nativizm oznacza przekonanie, że państwo powinno „należeć" przede wszystkim do rodzimych członków narodu, podczas gdy obecność „obcych" – migrantów, mniejszości etnicznych czy religijnych – jest postrzegana jako zagrożenie dla tożsamości i spójności wspólnoty. Autorytaryzm natomiast odwołuje się do wartości takich jak dyscyplina, bezpieczeństwo, posłuszeństwo wobec władzy i surowa polityka karna. W ujęciu Muddego tzw. „populistyczna radykalna prawica" łączy właśnie nativizm, autorytaryzm i pewien zakres populizmu, tworząc ideologiczny blok odwołujący się do narodu jako wspólnoty zagrożonej przez elity i obcych. Nie każda prawica ma taki charakter, ale to właśnie te wątki najczęściej pojawiają się w analizach prawicowego populizmu.

Drugim elementem definicji jest samo pojęcie populizmu, które należy do najbardziej spornych kategorii w naukach społecznych. W literaturze spotykamy co najmniej kilka podejść: populizm bywa opisywany jako styl uprawiania polityki, strategia mobilizacji, specyficzny typ przywództwa, forma dyskursu, a także szczególny rodzaj ideologii. W ostatnich dwóch dekadach silnie upowszechniło się tzw. podejście „ideacyjne", zaproponowane m.in. przez Casa Muddego i Cristóbala Rovirę Kaltwassera. W tym ujęciu populizm definiuje się jako „cienko rdzeniową ideologię", która postrzega społeczeństwo jako podzielone na dwa jednorodne i przeciwstawne

obozy, „czysty lud" oraz „skorumpowane elity", i głosi, że polityka powinna być bezpośrednim wyrazem woli ludu.

Określenie „cienko rdzeniowa ideologia" oznacza, że populizm sam w sobie nie zawiera pełnego, rozbudowanego programu dotyczącego wszystkich sfer życia społecznego, lecz koncentruje się na kilku prostych założeniach: moralistycznym podziale na lud i elity, przekonaniu o zdradzie interesów ludu przez elity oraz żądaniu przywrócenia polityce charakteru bezpośredniego wyrazu „woli narodu". Taka „cienkość" sprawia, że populizm może łączyć się z bardzo różnymi, „grubymi" ideologiami – nacjonalizmem, konserwatyzmem, socjalizmem czy ekologizmem – dlatego obserwujemy zarówno populistów lewicowych, odwołujących się do sprzeciwu wobec neoliberalizmu i wielkiego kapitału, jak i prawicowych koncentrujących się na obronie tożsamości narodowej i tradycyjnych wartości.

Populizm w ujęciu ideacyjnym ma również wymiar antypluralistyczny. Skoro „lud" jest przedstawiany jako jednorodny i moralnie wyższy, to z definicji odrzuca się ideę trwałych, legitymowalnych sporów politycznych wewnątrz społeczeństwa. Poglądy innych ugrupowań, mniejszości czy instytucji kontrolnych (mediów, sądów, trybunałów) bywają przedstawiane nie jako odmienne wizje dobra wspólnego, lecz wyraz zdrady interesów ludu lub działania „obcych" na jego szkodę. Ten moralistyczny rys populizmu, podkreślany w tekstach Muddego i jego kontynuatorów, odróżnia go od zwykłego, ostrego sporu politycznego: populiści nie tylko krytykują przeciwników, ale odmawiają im legitymacji, roszcząc sobie wyłączne prawo do reprezentowania „prawdziwego społeczeństwa".

Połączenie tych dwóch elementów – prawicowości i populizmu – prowadzi do pojęcia „prawicowego populizmu" (lub „populizmu prawicowego"). W literaturze anglojęzycznej często używa się określeń *right-wing populism* lub *populist radical right*, podkreślając, że chodzi o konfigurację, w której cienko rdzeniowy populizm łączy się z prawicowym, nativistyczno-konserwatywnym pakietem wartości. Oznacza to, że „lud" jest konstruowany przede wszystkim jako naród – rozumiany etnokulturowo, a nie wyłącznie obywatelsko – zaś głównymi przeciwnikami stają się nie tylko elity polityczne i gospodarcze, lecz również „obcy": migranci, mniejszości etniczne, religijne lub kulturowe. Badania nad prawicowym

populizmem w Europie wskazują, że imigracja jest dla tych ugrupowań nie tylko kwestią ekonomiczną (konkurencji o miejsca pracy), lecz przede wszystkim zagrożeniem dla wyobrażonej tożsamości narodu i jego tradycyjnych wartości.

Prawicowy populizm zachowuje zatem wszystkie elementy „rdzenia" populistycznego: przeciwstawia „prawdziwy lud" skorumpowanym elitom; twierdzi, że istnieje jedna możliwa do zdefiniowania wola narodu, którą tylko on potrafi wyrazić; oskarża elity o zdradę interesów zwykłych obywateli. Jednocześnie dokłada do tego specyficzną wizję wspólnoty, w której centralne miejsce zajmuje naród pojmowany jako wspólnota krwi, kultury, religii i historii. „Lud" w dyskursie prawicowo-populistycznym jest zatem domyślnie narodowy i homogeniczny, a wszystkie formy różnorodności etnicznej, religijnej, obyczajowej traktowane są podejrzliwie. Z perspektywy tych ugrupowań pluralizm kulturowy oraz polityka wielokulturowości jawią się jako projekt elit, narzucany społeczeństwu i rozbijający jego rzekomo naturalną jedność.

Charakterystyczna dla prawicowego populizmu jest także konstrukcja „potrójnej opozycji": przeciw „ludowi" występują zarówno elity, jak i „obcy". Te pierwsze oskarża się o zdradę narodu, korupcję, uległość wobec struktur międzynarodowych (Unia Europejska, organizacje międzynarodowe, globalne rynki), a także promowanie wartości kosmopolitycznych i liberalnych, sprzecznych z rzekomym „zdrowym rozsądkiem" zwykłych ludzi. „Obcych", czyli migrantów, uchodźców, mniejszości religijne, przedstawia się natomiast jako bezpośrednie zagrożenie dla bezpieczeństwa, kultury i dobrobytu wspólnoty narodowej. W ten sposób prawicowy populizm tworzy prostą narrację o oblężonej wspólnocie, która musi odzyskać kontrolę nad własnym państwem i granicami, wypierając „zdeprawowane elity" i powstrzymując napływ „obcych".

W warstwie programowej prawicowy populizm nie jest jednorodny, zwłaszcza w obszarze gospodarki. Choć część tych ugrupowań odwołuje się do tradycyjnych haseł wolnorynkowych, wiele z nich łączy konserwatyzm kulturowy z postulatami ochrony socjalnej i protekcjonizmu. W literaturze opisuje się to często jako „szowinizm dobrobytu": państwo ma być opiekuńcze i hojnie wspierać obywateli, ale tylko „swoich", natomiast dostęp do świadczeń społecznych dla migrantów czy mniejszości powinien

być ograniczany. W efekcie prawicowe ugrupowania populistyczne łączą nativistyczny nacisk na ochronę „naszych" przed „obcymi" z obietnicą, że zasoby państwa będą redystrybuowane w sposób uprzywilejowujący „prawdziwych" członków narodu.

Na tym tle można lepiej uchwycić różnicę między prawicowym populizmem a innymi formami populizmu. Populizm lewicowy koncentruje się przede wszystkim na konflikcie między „ludem" a elitami gospodarczymi i politycznymi, kładąc nacisk na nierówności społeczne, wyzysk i konieczność redystrybucji dóbr. „Obcy" w sensie kulturowym nie są centralną figurą tej narracji, a często stają się wręcz naturalnymi sojusznikami „uciskanych". Populizm prawicowy natomiast łączy krytykę elit z nieufnością wobec mniejszości i migrantów, a podział na „naszych" i „innych" przebiega zarówno na poziomie klasowym, jak i kulturowym. Różne są też postulaty wobec demokracji liberalnej: lewicowi populiści częściej domagają się wzmocnienia mechanizmów partycypacyjnych i ograniczenia władzy kapitału, podczas gdy prawicowi populiści akcentują raczej prymat woli większości nad prawami jednostek i mniejszości, co może prowadzić do erozji liberalnych gwarancji praworządności.

W badaniach nad prawicowym populizmem pojawia się także pytanie o jego relację do skrajnej prawicy. Nie wszystkie ugrupowania określane w ten sposób są populistyczne, część z nich odwołuje się raczej do elitarystycznych, rewolucyjnych projektów przebudowy ustroju, a nie do hasła „władzy ludu". Z drugiej strony, wiele partii prawicowo-populistycznych stara się dystansować od otwarcie ekstremistycznych tradycji, unikając języka rasizmu biologicznego czy jawnego negowania demokracji, a koncentrując się na natywizmie kulturowym, „obronie tożsamości" i krytyce instytucji liberalnych. Projekty takie jak The PopuList czy liczne typologie naukowe próbują precyzyjnie rozróżniać między „radykalną prawicą" działającą w ramach demokracji a „ekstremalną prawicą", która dąży do jej obalenia, wskazując, że populizm może występować po obu stronach tego podziału, choć w praktyce częściej wiąże się z nurtem radykalnym niż otwarcie antysystemowym.

Prawicowy populizm jest oczywiście zjawiskiem historycznie i geograficznie zróżnicowanym. Inaczej wygląda w krajach Europy Zachodniej, gdzie wyrasta z doświadczenia powojennego państwa dobrobytu,

imigracji postkolonialnej i integracji europejskiej, a inaczej w Europie Środkowo-Wschodniej, gdzie nakłada się na doświadczenia transformacji ustrojowej, nierówności społecznych, rozczarowania liberalizmem lat 90. i nieufności wobec instytucji ponadnarodowych. Odmienne są również jego konfiguracje w Stanach Zjednoczonych, gdzie łączy się z tradycją antyfederalizmu, specyficznym konserwatyzmem religijnym i polaryzacją partyjną. Wspólnym mianownikiem pozostaje jednak charakterystyczne połączenie retoryki „woli ludu" z nacjonalizmem kulturowym oraz krytyką elit i „obcych" jako wspólnego zagrożenia dla „zwykłych obywateli".

W literaturze często podkreśla się, że wzrost wpływów prawicowego populizmu nie jest zjawiskiem czysto „ideologicznym", lecz wiąże się z wieloma uwarunkowaniami strukturalnymi. W państwach Europy Zachodniej jako jedno ze źródeł wskazuje się konsekwencje globalizacji gospodarczej: deindustrializację, zanikanie stabilnych miejsc pracy w przemyśle, wzrost znaczenia sektora usług oraz presję konkurencji międzynarodowej. Procesom tym towarzyszy poczucie relatywnej deprywacji części klasy średniej i niższej, które mają wrażenie, że dotychczasowy kontrakt społeczny – obietnica stałej poprawy poziomu życia – przestał obowiązywać. Prawicowy populizm oferuje prostą diagnozę: winne są elity polityczne i gospodarcze, które dopuściły do „wylania" miejsc pracy za granicę, otwarcia granic na migrację oraz uzależnienia państwa od instytucji ponadnarodowych.

W Europie Środkowo-Wschodniej nakładają się na to doświadczenia transformacji ustrojowej. Przejście do gospodarki rynkowej i demokracji liberalnej, choć przyniosło długoterminowy wzrost gospodarczy, pociągnęło za sobą także koszty społeczne: wysokie bezrobocie w latach 90., narastające nierówności i poczucie marginalizacji części regionów. Jednocześnie elity modernizacyjne często posługiwały się językiem technokratycznym, przedstawiając swoje decyzje jako „bezalternatywne" i wynikające z wymogów integracji europejskiej. Prawicowy populizm wykorzystuje to dziedzictwo, przedstawiając się jako głos tych, którzy czują się przegranymi transformacji, oraz kwestionując narrację o konieczności podporządkowania polityki krajowej „dyrektywom z Brukseli". Krytyka elit ma tu zatem nie tylko wymiar aktualnej polityki, lecz także rozliczenia całego okresu transformacji.

Szczególne znaczenie dla wzmocnienia prawicowego populizmu miały kryzysy: finansowy z 2008 r. oraz migracyjny 2015 r. Ten pierwszy podważył wiarygodność neoliberalnego paradygmatu gospodarczego oraz zaufanie do instytucji międzynarodowych, które nie zapobiegły załamaniu rynków; drugi dostarczył wyraźnego, „namacalnego" tematu, wokół którego można było zbudować narrację o zagrożeniu tożsamości narodowej i bezpieczeństwa oraz utracie kontroli nad granicami. Prawicowe ugrupowania populistyczne potrafiły połączyć te wątki: krytykę globalizacji i elit finansowych z ostrzeżeniami przed rzekomą „inwazją" kulturową, przedstawiając siebie jako jedynych obrońców „zwykłych obywateli" przed skutkami decyzji podjętych „ponad ich głowami".

Dyskusja o prawicowym populizmie nie ma wyłącznie charakteru opisowego; w wielu tekstach naukowych pojawia się pytanie, czy jest on jedynie „symptomem" głębszych problemów demokracji liberalnej – takich jak kryzys reprezentacji, rosnące nierówności, poczucie marginalizacji części elektoratu – czy też stanowi samodzielne zagrożenie dla porządku demokratycznego. Część autorów podkreśla, że populistyczna krytyka elit może pełnić funkcję korygującą, zwracając uwagę na zaniedbane problemy społeczne i deficyty partycypacji. Inni jednak akcentują, że w wydaniu prawicowym populizm łatwo przekształca się w projekt ograniczania praw mniejszości, osłabiania niezależności sądów i mediów oraz podporządkowywania instytucji kontrolnych bieżącej woli większości. W takim scenariuszu populistyczna obietnica „oddania głosu zwykłym ludziom" może prowadzić do stopniowego demontażu mechanizmów, które chronią różnorodność i równowagę władz w systemie liberalno-demokratycznym.

W ostatnich latach do tej debaty dochodzi jeszcze jeden wątek: wpływ prawicowego populizmu na politykę migracyjną, integracyjną i europejską. W wielu krajach to właśnie ugrupowania prawicowo-populistyczne narzuciły agendę bezpieczeństwa granic, ograniczenia przyjmowania uchodźców, restrykcyjnej kontroli migracji i rewizji dotychczasowych modeli integracji. Częściowo przejmują ich język także partie głównego nurtu, które starają się odzyskać wyborców zagrożonych odpływem do sił populistycznych. W ten sposób prawicowy populizm oddziałuje na system polityczny nie tylko przez liczbę uzyskanych mandatów, lecz także zmianę języka debaty i zakresu tematów uznawanych za dopuszczalne.

Prawicowy populizm można rozumieć jako splot 2 komponentów: „cienko rdzeniowego" populizmu, który ujmuje politykę jako moralny konflikt między „czystym ludem" a „zepsutymi elitami", oraz prawicowej wizji wspólnoty koncentrującej się na narodzie, tradycji, tożsamości kulturowej i porządku społecznym. Efektem jest ideologiczna konfiguracja, w której „lud" przybiera postać narodu zagrożonego zarówno przez elity, jak i migrację czy mniejszości, a demokracja liberalna postrzegana jest jako projekt zdominowany przez kosmopolityczne elity i zbyt pobłażliwy wobec „obcych". To połączenie tłumaczy jednocześnie atrakcyjność prawicowego populizmu dla części elektoratu oraz napięcia, jakie wywołuje on w obrębie współczesnych demokracji, zmuszonych mierzyć się z pytaniem, jak równocześnie odpowiadać na realne poczucie frustracji społecznej i bronić instytucjonalnego pluralizmu przed logiką moralnej polaryzacji.

Fabian Kobalczyk-Gruda

J.G. Andersen, T. Bjørklund, *Structural Changes and New Cleavages: The Progress Parties in Denmark and Norway*, „Acta Sociologica" 1990, https://journals.sagepub.com/doi/10.1177/000169939003300303 (dostęp 4.12.2025); M. Enggist, *Welfare Chauvinism – Who Cares?*, „NES Paper Series" 2019, https://welfarepriorities.eu/wp-content/uploads/2020/01/22-Enggist-Welfare-Chauvinism-Who-Cares.pdf (dostęp 4.12.2025); L. Ennser-Jedenastik, *Welfare Chauvinism in Populist Radical Right Platforms: The Role of Redistributive Justice Principles*, „Social Policy & Administration" 2018, https://onlinelibrary.wiley.com/doi/10.1111/spol.12325 (dostęp 4.12.2025); R. Haenraets, *The Impact of the Radical Right Political Discourse*, Uniwersytet Warszawski, Warszawa 2024, https://rekrutacja.uw.edu.pl/files/pdf/SPP-P_lek3_25.pdf (dostęp 4.12.2025); R. Havertz, *AfD, Pegida i Ruch Identytarystyczny. Prawicowy populizm w Niemczech*, Instytut Wydawniczy Książka i Prasa, Warszawa 2025; A. Moroska-Bonkiewicz, *Prawicowy populizm a eurosceptycyzm. Na przykładzie Listy Pima Fortuyna w Holandii i Ligi Polskich Rodzin w Polsce*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2010; C. Mouffe, *For a Left Populism*, Verso, London 2018; C. Mudde, *Populist Radical Right Parties in Europe*, Cambridge University Press, Cambridge 2007; C. Mudde, C. Rovira Kaltwasser, *Populism: A Very Short Introduction*, Oxford University Press, Oxford 2017; J.W. Müller, *Co to jest populizm*?, Krytyka Polityczna, Warszawa 2017; *Populism in Europe and the Americas. Threat or Corrective for Democracy?*, C. Mudde, C. Rovira Kaltwasser (eds.), Cambridge University Press, Cambridge 2012; *Populizm – modele i praktyka. Polskie odniesienia*, T. Litwin, M. Nieć, K. Łabędź (red.), Wydawnictwo

Ignatianum, Kraków 2021; *Populizm, nierówności i uwiąd obywatelstwa socjalnego*, „Concilium Civitas. Almanach" 2019/2020, https://conciliumcivitas.pl/almanachy/almanach-2019-20/populizm-nierownosci-i-uwiad-obywatelstwa-socjalnego/ (dostęp 4.12.2025); J. Reykowski, *Populizm jako choroba demokracji*, „Nauka" 2023, nr 3, https://nauka-pan.pl/index.php/nauka/article/view/1037 (dostęp 4.12.2025); M. Rooduijn, A.L.P. Pirro, D. Halikiopoulou, C. Froio, S. van Kessel, S.L. de Lange, C. Mudde, P. Taggart, *The PopuList: A Database of Populist, Far-Left, and Far-Right Parties Using Expert-Informed Qualitative Comparative Classification (EiQCC)*, „British Journal of Political Science" 2024, https://doi.org/10.1017/S0007123423000431 (dostęp 4.12.2025); S. Saxonberg, *Some Thoughts about the Interplay Between Welfare Attitudes and Populism,* „Problemy Polityki Społecznej" 2020, https://www.problemypolitykispolecznej.pl/Some-thoughts-about-the-interplay-between-welfare-attitudes-and-populism,125448,0,1.html (dostęp 4.12.2025); *Welfare chauvinism* [hasło], „Populism Studies" 2024, https://www.populismstudies.org/vocabulary/welfare-chauvinism/ (dostęp 4.12.2025).

PRAKTYKI OPERACYJNE DARCZYŃCÓW HUMANITARNYCH – zdefiniowane w ramach inicjatywy Dobre Donatorstwo Humanitarne (ang. Good Humanitarian Donorship, GHD). W trakcie współprzewodnictwa Stanów Zjednoczonych i Kanady (2014–2016) w GHD członkowie inicjatywy zidentyfikowali najlepsze praktyki donatorstwa humanitarnego w 4 obszarach: sposobów finansowania, podejmowania decyzji w oparciu o dowody, zarządzania ryzykiem oraz wymogów administracyjnych i rozliczeniowych, które przyjęli na dorocznym spotkaniu GHD na wysokim szczeblu, które odbyło się 27 kwietnia 2016 r.

W obszarze finansowania do najlepszych praktyk operacyjnych usprawniających świadczenie pomocy humanitarnej zalicza się:

1. Terminowość, przewidywalność i elastyczność finansowania, tj.
   - przekazywanie informacji o funduszach z wyprzedzeniem, m.in. poprzez regularne konsultacje z partnerami, miękkie deklaracje (*soft pledges*) oraz umowy partnerskie (np. memoranda o porozumieniu), co pozwala minimalizować koszty operacyjne powodowane brakiem pewności co do finansowania operacji humanitarnych;
   - w kontekście kryzysów nawracających, chronicznych lub przedłużających za dobrą praktykę uznaje się przyznawanie

środków na okres wykraczający poza pojedynczy rok budżetowy lub stosowanie instrumentów umożliwiających wieloletnie planowanie z finansowaniem przyrostowym;
– przy założeniu, że środki są wykorzystywane zgodnie z uzgodnionym harmonogramem, dopuszcza się elastyczność finansowania dostosowaną do zmieniających się kontekstów humanitarnych. Dobrą praktykę stanowi:
• udzielanie bezpłatnych przedłużeń w przypadku, gdy opóźnienia w realizacji projektu lub programu pomocy humanitarnej wynikają z nieprzewidzianych przyczyn operacyjnych lub bezpieczeństwa, wniosek o przedłużenie zostanie złożony w odpowiednim czasie, a zakres projektu nie uległ zmianie;
• określenie akceptowalnych alternatyw dla zwrotu niewielkich, wolnych środków pozostających po zakończeniu projektu, uzgodnionych we współpracy z partnerem wdrażającym i przed upływem okresu finansowania;
• dokonywanie doraźnych, elastycznych modyfikacji projektów (*ad hoc*), uzgadnianych pomiędzy darczyńcami a partnerami, w odpowiedzi na zmieniające się okoliczności humanitarne;
• wbudowanie elastyczności w konstrukcję dotacji, tj. projektowanie instrumentów finansowania w taki sposób, aby od początku zawierały one mechanizmy elastycznego reagowania (np. możliwość przesunięć budżetowych, szybkich rewizji działań), co umożliwia partnerom szybką reakcję w kontekście dynamiki potrzeb.

2. Wieloletni sposób finasowania, tj.
– zapewnianie długoterminowych instrumentów finansowania lub planowania dla działań Międzynarodowego Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca oraz organizacji pozarządowych, realizowanych m.in. poprzez porozumienia, umowy partnerskie, umowy o współpracy, kontrakty, dotacje oraz inne zbliżone narzędzia finansowe;
– wspieranie planowania strategicznego i programowego partnerów w perspektywie co najmniej 2-letniej, przy zastosowaniu uzgodnionych budżetów umożliwiających uruchamianie

dodatkowego finansowania w przypadku wystąpienia nowych lub nasilonych potrzeb;
- ustanawianie wieloletnich ram planistycznych oraz wspólne opracowywanie strategii programowania, opartych na uzgodnionych analizach i wspólnym rozumieniu potrzeb humanitarnych przez partnerów;
- zapewnianie spójności i komplementarności pomiędzy finansowaniem humanitarnym a rozwojowym w ramach porozumień wieloletnich, w celu równoczesnego reagowania na bieżące potrzeby humanitarne oraz ograniczania liczby sytuacji wymagających interwencji kryzysowej;
- alokowanie odpowiedniej części środków w ramach wieloletniego finansowania na budżety pomocy humanitarnej kryzysów powtarzających i przedłużających się, zgodnie z procedurami darczyńców, w szczególności poprzez:
  - wieloletnie podstawowe finansowanie partnerów dysponujących sprawdzonymi procedurami wewnętrznej weryfikacji i priorytetyzacji, zwłaszcza w kontekstach, w których darczyńcy nie posiadają własnej reprezentacji regionalnej;
  - finansowanie wieloletnich projektów lub programów ukierunkowanych na reagowanie na określone kryzysy;
  - wieloletnie finansowanie realizowane za pośrednictwem wspólnych mechanizmów finansowych, w tym wspólnych funduszy krajowych oraz Centralnego Funduszu Reagowania Kryzysowego.

W obszarze podejmowania decyzji w oparciu o dowody do najlepszych praktyk operacyjnych usprawniających świadczenie pomocy humanitarnej zalicza się:

1. Produkcję dowodów, zwłaszcza w kontekście podejmowania decyzji finansowych w oparciu o istniejące zasoby wiedzy oraz dowody empiryczne, tj.
   - dzielenie się istotnymi dowodami powstałymi w procesie opracowywania i oceny polityk oraz programów, w tym wytycznymi dotyczącymi polityki i finansowania, wynikami ewaluacji oraz wnioskami z doświadczeń;

- wykorzystywanie oraz współtworzenie otwartych, bezpłatnych i współdzielonych zasobów danych w celu usprawnienia wspólnego ustalania priorytetów działań i programów;
- stosowanie wspólnych narzędzi analizy ryzyka, takich jak indeksy umożliwiające porównywalną ocenę zagrożeń, w tym Indeks Zarządzania Ryzykiem (ang. Index for Risk Management, INFORM), stanowiący wspólną podstawę współpracy na rzecz skuteczniejszego zarządzania ryzykiem klęsk żywiołowych, wzmacniania odporności oraz projektowania programów uwzględniających czynniki ryzyka.

2. Wsparcie w podejmowaniu decyzji:
   - odnoszących się do alokacji środków humanitarnych na podstawie rzetelnych dowodów, przejrzystych procesów oraz jasno określonych kryteriów, obejmujące:
     - podejmowanie decyzji o alokacji środków finansowych w oparciu o rzetelne dowody;
     - wykorzystywanie rzetelnych dowodów spełniających wspólne kryteria darczyńców, w tym opartych na niezależnym i rygorystycznym ustalaniu priorytetów potrzeb w wielu sektorach, wspólnej analizie i konsensusie ekspertów, przejrzystej metodologii oraz solidnej bazie wiedzy;
   - w kontekście skoordynowanej analizy i oceny potrzeb na rzecz planowania działań humanitarnych, w tym takich procesów jak Przegląd Potrzeb Humanitarnych (ang. Humanitarian Needs Overview, HNO) oraz Plan Reagowania Humanitarnego (Humanitarian Response Plan, HRP), które służą ustalaniu wspólnych priorytetów i wzmacnianiu skuteczności odpowiedzi humanitarnej, obejmujące:
     - zapewnienie wsparcia finansowego i rzeczniczego partnerom w celu wzmacniania skoordynowanych, obiektywnych i przejrzystych procesów oceny potrzeb oraz opracowywania planów reagowania obejmujących wielosektorową analizę priorytetów;
     - podejmowanie decyzji o przydziale środków finansowych w oparciu o HNO i HRP w celu zwiększenia synergii między

zbiorowym ustalaniem priorytetów a decyzjami finansowymi darczyńców.

W obszarze zarządzania ryzykiem, zwłaszcza w zakresie bezpieczeństwa personelu i operacyjnego, do najlepszych praktyk operacyjnych usprawniających świadczenie pomocy humanitarnej zalicza się konsultacje z partnerami humanitarnymi jako neutralnymi, bezstronnymi i niezależnymi podmiotami humanitarnymi, obejmujące:

– zarządzanie ryzykiem tj.
- prowadzenie współpracy z partnerami humanitarnymi w zakresie zarządzania ryzykiem, w kwestii zgodności z przepisami prawa oraz ryzykiem powierniczym, zarówno na poziomie centralnym, jak i terenowym;
- poszanowanie ram krytyczności programu stosowanych przez agencje humanitarne jako elementu ich autonomicznych decyzji operacyjnych;
- pogłębianie wzajemnego zrozumienia w sytuacjach, gdy partnerzy uznają za konieczne stosowanie zdalnego zarządzania działaniami humanitarnymi na obszarach podwyższonego ryzyka oraz w uzasadnionych przypadkach, korzystanie z monitoringu zewnętrznego w celu wzmocnienia odpowiedzialności wobec społeczności dotkniętych kryzysem;

– politykę bezpieczeństwa i ochrony, tj.
- zachęcanie partnerów do przyjęcia koncepcji zarządzania ryzykiem oraz wdrażania systematycznego podejścia do zarządzania bezpieczeństwem, w tym opracowania polityk i procedur bezpieczeństwa dostosowanych do kontekstu kraju i charakteru projektu;
- wspieranie rozwoju potencjału oraz wzmacniania protokołów i praktyk bezpieczeństwa lokalnych i krajowych organizacji humanitarnych;
- promowanie zasady „obowiązku opieki" partnerów międzynarodowych wobec partnerów lokalnych, w tym wsparcia w analizie ryzyka, przy jednoczesnym zapewnieniu adekwatnego poziomu odpowiedzialności wszystkich stron oraz środków

bezpieczeństwa dla partnerów lokalnych w sytuacjach przenoszenia ryzyka;
- informowanie partnerów o możliwości uwzględniania, w określonych okolicznościach, kosztów związanych z ochroną sprzętu, personelu, szkoleniami oraz poprawą bezpieczeństwa obiektów w budżetach darczyńców;
- finansowanie, w ramach działań zbiorowych, inicjatyw ukierunkowanych na budowanie potencjału w zakresie bezpieczeństwa;
- dalsze promowanie i wspieranie ram współpracy w obszarze bezpieczeństwa realizowanych przez Departament Bezpieczeństwa i Ochrony (ang. UN Department of Safety and Security, UNDSS), organizacje pozarządowe oraz inicjatywę Saving Lives Together;
- zapewnianie zwiększonego wsparcia dla inicjatyw szkoleniowych organizacji pozarządowych w zakresie zarządzania bezpieczeństwem na poziomie terenowym, a także dla krajowych platform i mechanizmów koordynacji bezpieczeństwa organizacji pozarządowych.

W obszarze wymagań administracyjnych i rozliczeniowych do najlepszych praktyk operacyjnych usprawniających świadczenie pomocy humanitarnej zalicza się:

1. Wymagania administracyjne dotyczące odpowiedzialności i elastyczności, tj.
   – zapewnienie finansowania umożliwiającego rozliczaną elastyczność operacyjną uwzględniającą wsparcie nieobjęte konkretnymi środkami lub o ograniczonym przeznaczeniu dla partnerów wielostronnych oraz finansowanie programowe dla organizacji pozarządowych, przekazywane w odpowiedniej minimalnej liczbie transz.
2. Propozycje i raportowanie obejmujące w szczególności:
   – uznanie potrzeby zachowania równowagi pomiędzy zapewnieniem partnerom odpowiedniego poziomu elastyczności operacyjnej a wymogami rozliczalności darczyńców jako warunku efektywnego działania partnerów humanitarnych;

- przyjęcie do wiadomości postulatów partnerów dotyczących konieczności usprawniania wymogów administracyjnych przez darczyńców w celu zwiększenia efektywności instytucjonalnej i operacyjnej;
- traktowanie odwołań o charakterze strategicznym i całościowym opartych na priorytetach jako podstawy decyzji inwestycyjnych, obejmujących zarówno zbiorowe mechanizmy odwoławcze, takie jak Plany Reagowania Humanitarnego oraz Plany Reagowania na Uchodźców dostosowane do określonych kontekstów, jak i odwołania w sytuacjach kryzysowych odnoszących się do poszczególnych instytucji;
- stosowanie wspólnych wskaźników w sytuacjach wymagających składania wniosków o finansowanie, zgodnych z ramami wskaźników partnerów instytucjonalnych, ramami globalnych klastrów lub podejściami wskaźnikowymi Planów Reagowania Humanitarnego, Planów Reagowania na Uchodźców oraz krajowych mechanizmów odwoławczych;
- wykorzystywanie uniwersalnych raportów programowych sporządzanych przez partnerów wielostronnych w uzgodnionych odstępach czasu, obejmujących zarówno zweryfikowane sprawozdania finansowe, jak i roczne lub kryzysowe raporty opisowe dotyczące osiąganych rezultatów;
- zachęcanie członków inicjatywy GHD do dzielenia się oraz stosowania klauzul umownych uznawanych za dobre praktyki, wspierających spójność z zasadami GHD w zakresie udziału beneficjentów, wsparcia krajowych struktur koordynacyjnych, widoczności darczyńców, przestrzegania standardów oraz promowania odpowiedzialności, efektywności i skuteczności działań humanitarnych.

3. Ocenę i nadzór, tj.
   - zapewnienie przez darczyńców większej spójności między narzędziami i procesami monitorowania i oceny;
   - dostosowywanie się darczyńców do ocen i nadzoru, przy jednoczesnej wymianie informacji na ten temat;

– stosowanie zasady proporcjonalności w zakresie oceny potencjału partnerów organizacji pozarządowych, przy zachowaniu adekwatności złożoności wymogów do skali przyznania wsparcia oraz przejrzystej metodologii oceny zachęcających darczyńców do opracowywania wspólnych podejść.

Klaudia Cenda-Miedzińska

Best Practices in Humanitarian Aid, https://cecil.gmu.edu/best-practices-humanitarian-aid (dostęp 3.02.2026); J. Caccavale, K. Haver, A. Stoddard, *Donor Reporting Requirements Research*, Humanitarian outcomes, 22.02.2016; CAFOD, FAO, World Vision, *Future Humanitarian Financing: Looking Beyond the Crisis*, 13.05.2015; Good Humanitarian Donorship, *Operational Best Practices – From the 2014–2016 Co-Chairmanship*, https://www.ghdinitiative.org/ghd/gns/best-practices.html (dostęp 3.02.2026); Groupe Urgence-Rehabilitation-Development, *Evidence-based decision-making for funding allocations*, 6.11.2016; A. Stoddard, K. Haver, M. Czwarno, *NGOs and Risk: How international humanitarian actors manage uncertainty*, Humanitarian Outcomes 02.2016; UN, *Too important to fail: addressing the humanitarian financing gap: report to the United Nations Secretary-General/ High-Level Panel on Humanitarian Financing*, 01.2016.

PRANIE BRUDNYCH PIENIĘDZY LUB PRANIE PIENIĘDZY – nielegalny, wielostopniowy proceder mający na celu zamaskowanie istnienia, źródła, natury, władztwa lub umiejscowienia środków pochodzących z przestępstwa. Termin wywodzi się z języka angielskiego od sformułowań *dirty money* (brudne pieniądze) oraz *money laundering* (pranie pieniędzy). Pranie brudnych pieniędzy nieodmiennie związane jest z przekształceniem lub transferem wartości majątkowych; ma na celu nadanie pozorów legalności środkom pochodzącym z działalności przestępczej, co w rezultacie ma umożliwić swobodne z nich korzystanie. Wprowadzenie nielegalnie zdobytych dochodów do oficjalnego obrotu gospodarczego jest warunkiem koniecznym dla skutecznego czerpania korzyści z działalności przestępczej, zwłaszcza tej o charakterze zorganizowanym, korupcyjnym czy terrorystycznym. Bez realizacji procederu prania brudnych pieniędzy działalność ta w praktyce byłaby wręcz bezcelowa. Trudno o wiarygodne dane w zakresie skali procederu. Wobec ogromu transakcji na rynkach krajowych czy

międzynarodowych kapitał z przestępstw może bowiem przeniknąć do światowego systemu w sposób niezauważony. Wedle szacunków Organizacji Narodów Zjednoczonych od 2% do 5% światowego produktu krajowego brutto liczonego w bilionach dolarów amerykańskich związane jest z praniem brudnych pieniędzy. Niewątpliwie proceder ma istotne implikacje zarówno dla gospodarki światowej, jak i poszczególnych państw i regionów.

Przekazy historyczne wskazują, że już w starożytności piraci grasujący po Morzu Śródziemnym ukrywali swe łupy przez Republiką, a później Cesarstwem Rzymskim. W I w. po Chrystusie chińscy kupcy stosowali różne środki, w tym zakup ruchomości i wysyłanie pieniędzy za granicę, aby ukrywać swój majątek przed władzą państwową. Jak się jednak wydaje, termin „pranie brudnych pieniędzy" ma swą genezę w działalności Ala Capone w Chicago w latach 20. XX w. Za pomocą kontrolowanych zakładów pralniczych legalizował on swoje przestępcze dochody poprzez dołączanie ich do dziennego utargu. Zauważyć można, że gdyby proceder ten realizował w pełni skutecznie, uchroniłoby to go przed późniejszymi zarzutami oszustw podatkowych. Inni badacze z kolei przywołują chociażby postać Meyera Lansky'ego – ten również działający w erze prohibicji gangster założył wypożyczalnię samochodów, która nie tylko zapewniała transport dla jego nielegalnej działalności, ale także służyła jako legalna przykrywka dla jego przestępczych działań. Termin „pranie brudnych pieniędzy" stał się powszechny podczas afery Watergate z początkiem lat 70. XX w. – brytyjska gazeta „The Guardian" użyła tego sformułowania dla opisu działań komitetu wyborczego Richarda Nixona, który dokonywał transferu nielegalnych środków do Meksyku i z powrotem do Stanów Zjednoczonych z przeznaczeniem na kampanię prezydencką.

Pranie brudnych pieniędzy zwykle jest złożonym procesem. Wyróżnia się 3 odrębne bądź czasem nakładające się na siebie fazy:

1. Lokowanie, czyli fizyczne wprowadzenie nielegalnie uzyskanych pieniędzy do systemu finansowego lub gospodarki detalicznej. Innymi słowy, to wyzbywanie się gotówki pochodzącej z przestępstwa lub przestępstw. Lokowanie to najbardziej ryzykowna faza z punktu widzenia sprawców, bowiem właśnie wtedy pieniądze są najbardziej narażone na wykrycie i zajęcie. Cechą charakterystyczną

lokowania jest powtarzalność relatywnie niewielkich transakcji dokonywanych zwykle w formie gotówkowej. Chodzi o podzielenie dużych porcji pieniędzy na mniejsze, by następnie wprowadzić je do systemu finansowego. Odbywa się to poprzez wpłaty do banków czy innych instytucji finansowych. Elementami przestępczego ukrywania procederu na tym etapie są w szczególności:
- rozdrabnianie wpłat (ang. *smurfing*);
- dzielenie wpłat (ang. *structuring*);
- mieszanie z dochodami z legalnej działalności (ang. *blending*);
- wymiana walut;
- wykorzystanie kasyn.

Rozdrabnianie wpłat wymaga wykorzystania firmujących tzw. słupów, którzy po otwarciu na swoje autentyczne dane rachunków bankowych dokonają na nie zasileń określonymi sumami pieniędzy. Kwoty te nie mogą przekraczać wartości wymagających poinformowania państwowych organów nadzorczych; muszą zatem być relatywnie małe. Dzielenie wpłat polega na założeniu, tym razem na fikcyjne dane, rachunków bankowych; nie występuje tu zatem konieczność użycia firmujących. Podobnie jak przy rozdrabnianiu wpłat i tu dokonuje się zasileń niewielkimi sumami pieniędzy. Mieszanie z dochodami z legalnej działalności wymaga zawyżania przychodów z prowadzonych oficjalnych przedsięwzięć gospodarczych – najbardziej pożądane będę te, w których na co dzień klienci dokonują dużej ilości płatności gotówką i trudno jest określić skalę działalności. Tego rodzaju kryteria spełniają restauracje, kluby nocne, dyskoteki czy *nomen omen* pralnie. Wymiana walut w kantorach jest kolejną metodą ukrywającą fazę lokowania; realizowana jest zwykle przy wykorzystaniu firmujących w kliku czy nawet kilkunastu różnych kantorach czy oddziałach banków. Kasyna natomiast wykorzystuje się, zakupując żetony do gry, by następnie je zwrócić z dyspozycją przelania należności na wskazany rachunek bankowy.

2. Maskowanie polega na odseparowaniu środków od nielegalnego źródła. Realizowane jest przez bardzo dużą liczbę rozmaitych transakcji, najczęściej poprzez bankowość elektroniczną i bez faktycznego ekonomicznego uzasadnienia. Przykładem będą tu zakupy aktywów, transfery zagraniczne, wzajemne usługi podmiotów

piorących brudne pieniądze. W kontekście globalizacji zauważyć należy, iż przestępcy biorący brudne pieniądze starają się wykorzystać zalety rynku globalnego wszędzie tam, gdzie się pojawiają. Nierzadkie zatem jest w tej fazie korzystanie z rajów podatkowych, czyli państw lub terytoriów zależnych z nikłymi bądź w praktyce nieistniejącymi reżimami podatkowymi i kontrolnymi. Współcześnie w ramach Unii Europejskiej prowadzony jest wykaz jurysdykcji niechętnych współpracy podatkowej. Umieszcza się w nim podmioty prawa międzynarodowego, które nie wypełniły w ustalonym terminie zobowiązań do dobrego zarządzania podatkowego bądź odmówiły ich wypełnienia. Obecnie na liście znajdują się Anguilla, Fidżi, Guam, Palau, Panama, Rosja, Samoa, Trynidad i Tobago, Wyspy Dziewicze Stanów Zjednoczonych oraz Vanuatu. Jednocześnie na liście jako państwa lub terytoria zależne, które współpracują z Unią Europejską, ale nie wywiązały się jeszcze z wszystkich zobowiązań, znajdują się: Antigua i Barbuda, Belize, Brytyjskie Wyspy Dziewicze, Brunei, Eswatini, Grenlandia, Jordania, Maroko, Czarnogóra, Seszele oraz Turcja.

3. Integracja jest fazą, w której wykorzystuje się pozornie legalnie posiadane środki poprzez inwestycje gospodarcze. W praktyce chodzi tu o przeniesienie dochodów do pozornie legalnej formy. Przykładami będzie nabycie wartościowych aktywów, takich jak przedsiębiorstwa, nieruchomości, luksusowe samochody, jachty, odrzutowce, dzieła sztuki, sprzęty elektroniczne, kosztowna biżuteria. Inny sposób to np. zaciąganie umów kredytowych i spłacanie ich posiadanymi środkami.

Wymienione fazy procederu łączy tzw. ślad buchalteryjny generowany przez transakcje finansowe realizowane w ramach prania brudnych pieniędzy. Pozwala on na wyśledzenie faktycznego pochodzenia środków. By tego uniknąć, możliwe jest stosowanie przez przestępców instrumentów korupcyjnych, zwłaszcza w odniesieniu do osób zatrudnionych w sektorze finansowym. Nierzadkie jest realizowanie transakcji między podmiotami powiązanymi. Stosunkowo nowe i szerokie możliwości daje im również rynek kryptowalut.

W Stanach Zjednoczonych wprowadzono pierwsze regulacje prawne odnoszące się do prania brudnych pieniędzy. W 1970 r. przyjęto ustawę o organizacjach przestępczych i korupcyjnych (Racketeer Influenced and Corrupt Organizations Act, RICO), która miała na celu przeciwdziałanie infiltracji legalnych przedsiębiorstw przez przestępców oraz ściganie tych, którzy już zdobyli udział w gospodarce. Przede wszystkim jednak w tym samym roku przyjęto ustawę o tajemnicy bankowej (Bank Secrecy Act) określającą wymogi dotyczące prowadzenia dokumentacji i sprawozdawczości przez osoby prywatne, banki i inne instytucje finansowe w celu identyfikacji źródła, wolumenu i ruchu waluty oraz innych instrumentów pieniężnych transportowanych lub przesyłanych do czy ze Stanów Zjednoczonych bądź deponowanych w instytucjach finansowych. Jednocześnie nakazano bankom zgłaszanie transakcji gotówkowych o wartości powyżej 10 tys. dolarów, nakładając wymogi w zakresie prawidłowej identyfikacji osób przeprowadzających transakcje. W 1986 r. wprowadzono natomiast przepisy penalizujące; organem nadzoru w Stanach Zjednoczonych jest FinCEN (Financial Crimes Enforcement Network – Sieć ds. Zwalczania Przestępstw Finansowych), agencja Departamentu Skarbu Stanów Zjednoczonych, której dyrektor jest mianowany przez sekretarza skarbu i podlega podsekretarzowi skarbu ds. terroryzmu i wywiadu finansowego.

W polskim prawodawstwie pranie brudnych pieniędzy penalizowane jest od 1994 r. Przestępstwo to określone zostało w art. 299 Kodeksu karnego. W obecnym brzmieniu unormowanie to stanowi, iż

§1. Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§2. Karze określonej w §1 podlega, kto będąc pracownikiem lub działając w imieniu lub na rzecz banku, instytucji finansowej lub kredytowej lub innego podmiotu, na którym na podstawie przepisów prawa ciąży

obowiązek rejestracji transakcji i osób dokonujących transakcji, przyjmuje, wbrew przepisom, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, dokonuje ich transferu lub konwersji, lub przyjmuje je w innych okolicznościach wzbudzających uzasadnione podejrzenie, że stanowią one przedmiot czynu określonego w §1, lub świadczy inne usługi mające ukryć ich przestępne pochodzenie lub usługi w zabezpieczeniu przed zajęciem.

§3. (uchylony).

§4. (uchylony).

§5. Jeżeli sprawca dopuszcza się czynu określonego w §1 lub 2, działając w porozumieniu z innymi osobami, podlega karze pozbawienia wolności od roku do lat 10.

§6. Karze określonej w §5 podlega sprawca, jeżeli dopuszczając się czynu określonego w §1 lub 2, osiąga znaczną korzyść majątkową.

§6a. Kto czyni przygotowania do przestępstwa określonego w §1 lub 2, podlega karze pozbawienia wolności do lat 3.

§7. W razie skazania za przestępstwo określone w §1 lub 2, sąd orzeka przepadek przedmiotów pochodzących bezpośrednio albo pośrednio z przestępstwa, a także korzyści z tego przestępstwa lub ich równowartość, chociażby nie stanowiły one własności sprawcy. Przepadku nie orzeka się w całości lub w części, jeżeli przedmiot, korzyść lub jej równowartość podlega zwrotowi pokrzywdzonemu lub innemu podmiotowi.

§8. Nie podlega karze za przestępstwo określone w §1 lub 2, kto dobrowolnie ujawnił wobec organu powołanego do ścigania przestępstw informacje dotyczące osób uczestniczących w popełnieniu przestępstwa oraz okoliczności jego popełnienia, jeżeli zapobiegło to popełnieniu innego przestępstwa; jeżeli sprawca czynił starania zmierzające do ujawnienia tych informacji i okoliczności, sąd stosuje nadzwyczajne złagodzenie kary.

Jak widać, dla zaistnienia złożonego czynu zabronionego konieczne jest wykazanie istnienia tzw. przestępstwa bazowego, czyli tego, z którego pochodzą środki będące przedmiotem procederu prania brudnych pieniędzy. Podstawowym dobrem prawnym chronionym poprzez art. 299 Kodeksu karnego jest prawidłowość obrotu gospodarczego, rozumiana jako obrót transparentny oraz oparty o legalne źródła.

Na przestrzeni lat różnorakie unormowania międzynarodowe stworzyły ramy organizacyjne do zwalczania zjawiska prania brudnych pieniędzy, które szczególny nacisk kładą na działania prewencyjne. Kluczowe jest sprawdzanie klientów instytucji finansowych, w tym zwłaszcza banków, ponadto zgłaszanie transakcji podejrzanych, wreszcie regulacje i nadzór nad działalnością instytucji finansowych. Tworzy się również organy kontrolne. W tym miejscu warto przywołać rekomendacje opracowane przez FATF (Financial Action Task Force – Grupę Specjalna ds. Przeciwdziałania Praniu Pieniędzy) – organizację międzynarodową utworzoną w 1989 r. z siedzibą w Paryżu. Rekomendacje FATF określają podstawowe środki, które państwa powinny wprowadzić w celu:

- identyfikacji ryzyka oraz opracowania polityki i koordynacji krajowej;
- zwalczania prania pieniędzy, finansowania terroryzmu i proliferacji;
- stosowania środków zapobiegawczych w sektorze finansowym i innych wyznaczonych;
- ustanowienia uprawnień i obowiązków właściwych organów (np. śledczych, ścigania i nadzorczych) oraz innych środków instytucjonalnych;
- zwiększenia przejrzystości i dostępności informacji o beneficjentach rzeczywistych osób prawnych i porozumień; oraz
- ułatwiania współpracy międzynarodowej.

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2024/1620 z dnia 31 maja 2024 r. utworzono Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (Anti-Money Laundering Authority, AMLA), który w szczególności ma za zadanie monitorować rozwój sytuacji na rynku wewnętrznym i oceniać zagrożenia, podatności i ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu. Ma również monitorować rozwój sytuacji w państwach trzecich i oceniać zagrożenia, podatności i ryzyko związane z ich systemami przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, które mogą mieć rzeczywisty lub potencjalny wpływ na rynek wewnętrzny. Ponadto ma zbierać i analizować informacje pochodzące z własnej działalności nadzorczej oraz organów nadzoru i nadzorczych, dotyczące

słabości zidentyfikowanych w stosowaniu przepisów przez zobowiązane podmioty, narażenia zobowiązanego podmiotu na ryzyko, nałożonych sankcji i podjętych działań naprawczych. W tym celu ma utworzyć centralną bazę danych zawierającą informacje zebrane od organów nadzorczych lub wynikające z działalności urzędu oraz aktualizować ją na bieżąco.

W Polsce ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu reguluje działalność Generalnego Inspektora Informacji Finansowej (GIIF), który jest w szczególności odpowiedzialny za analizowanie informacji dotyczących wartości majątkowych, co do których powziął podejrzenie, że mają one związek z przestępstwem prania brudnych pieniędzy lub finansowania terroryzmu, oraz przeprowadzanie procedury wstrzymania transakcji lub blokady rachunku. GIIF sprawuje również kontrolę wykonywania przez instytucje obowiązane obowiązków w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, prowadząc działania planowe oraz doraźne. Wspomniana ustawa reguluje również szeroki katalog instytucji powiązanych, w tym banków i innych instytucji finansowych, które zobowiązane są stosować środki bezpieczeństwa finansowego w przypadku:

1. Nawiązywania stosunków gospodarczych.
2. Przeprowadzania transakcji okazjonalnej o wartości 15 tys. euro lub większej, bez względu na to, czy jest to pojedyncza operacja, czy kilka, które wydają się ze sobą powiązane, lub która stanowi transfer środków pieniężnych na kwotę przekraczającą wartość 1 tys. euro, bądź transakcji okazjonalnej z wykorzystaniem waluty wirtualnej o wartości 1 tys. euro lub większej.
3. Przeprowadzania gotówkowej transakcji okazjonalnej o wartości 10 tys. euro lub większej, bez względu na to, czy jest przeprowadzana jako pojedyncza operacja, czy kilka, które wydają się ze sobą powiązane.
4. Obstawiania stawek oraz odbioru wygranych o wartości 2 tys. euro lub większej, bez względu na to, czy jest przeprowadzana jako pojedyncza operacja, czy kilka, które wydają się ze sobą powiązane.
5. Podejrzenia prania pieniędzy lub finansowania terroryzmu.
6. Wątpliwości co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta.

W kontekście ustawodawstwa polskiego, będącego pochodną rozwiązań w ramach Unii Europejskiej, warto jeszcze przywołać ustawę z dnia 14 czerwca 2024 r. o ochronie sygnalistów, bowiem obejmuje ona m.in. naruszenia prawa dotyczące przeciwdziałania praniu brudnych pieniędzy oraz finansowaniu terroryzmu.

Jakub Purchla

D. Chodziński, *Pranie pieniędzy jako jedna z form działania zorganizowanych grup przestępczych*, Centrum Szkolenia Policji w Legionowie, Legionowo 2012; L. Gelemerova, *The Anti-Money Laundering System in the Context of Globalisation: A Panopticon Built on quicksand?*, Wolf Legal Publishers, Nijmegen 2011; J. Grzywacz, *Pranie pieniędzy. Metody, raje podatkowe, zwalczanie*, Szkoła Główna Handlowa w Warszawie, Warszawa 2010; M. Hryniewiecka, *Pranie brudnych pieniędzy jako przykład przestępstwa gospodarczego*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2014, t. 76, nr 4; *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations*, Financial Action Task Force, Paris 2012–2022; K. Kluczewski, *Pranie brudnych pieniędzy – ewolucja, konsekwencje oraz metody przeciwdziałania*, „Bezpieczny Bank" 2024, nr 2(95); A. Lebiedowicz, *Przestępstwo prania pieniędzy w polski prawie karnym*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2021, nr 3(43); *Money Laundering Prevention. A Money Services Business Guide*, Financial Crime Enforcement Network, Washington DC 2007; M. Mazur, *Pranie pieniędzy – ujęcie kryminologiczne*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2006, t. 10, nr 2; Rozporządzenie Parlamentu Europejskiego Rady (UE) 2024/1620 z dnia 31 maja 2024 r. w sprawie ustanowienia Urzędu ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010; K. Sadło, *Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu – obowiązki organizacji pozarządowych*, Fundacja Rozwoju Społeczeństwa Obywatelskiego, Warszawa 2011; P. Siejczuk, *Problematyka prania brudnych pieniędzy w regulacjach prawnomiędzynarodowych, europejskich i krajowych*, „Bezpieczeństwo Narodowe" 2012, nr 3–4(23–24); Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j. Dz.U. 2025, poz. 383; Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, t.j. Dz.U. 2025, poz. 644; Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów, Dz.U. 2024, poz. 928.

PROJEKT NA RZECZ ELEKTROWNI JĄDROWEJ W POLSCE (PONI) – pomysł ogólnych założeń ds. kwestii jądrowych powstał w 2003 r. w celu

kształcenia specjalistów w zakresie polityki, technologii oraz eksploatacji obiektów jądrowych poprzez wspieranie, utrzymywanie i zrzeszanie społeczności dla początkujących ekspertów. Działanie obejmuje identyfikację i kształcenie początkujących liderów poprzez budowanie wzajemnych międzynarodowych relacji, pogłębienie zrozumienia i dzielenie się perspektywami rozwoju w kwestiach jądrowych. Utworzenie trwałych relacji zapewnia nowym ekspertom integrację, różnorodne i kreatywne możliwości poznania politycznych, technicznych i operacyjnych aspektów działalności jądrowej, opracowywania i prezentowania nowych koncepcji i pomysłów oraz angażowania się w przemyślane i świadome debaty na rzecz kształtowania świadomości społecznej w zakresie zaplecza jądrowego.

PONI to szeroko rozumiana misja zarówno wewnętrzna, jak i zewnętrzna dla kraju budującego społeczność energetyczną z wykorzystaniem potencjału nuklearnego, która realizuje się poprzez kilka wytyczonych celów:

- identyfikację liderów oraz umożliwienie im zapewnienia obszaru do prowadzenia badań i prezentowania nowych koncepcji oraz pomysłów;
- zachęcanie do debaty publicznej;
- angażowanie szerokiej i zróżnicowanej społeczności w aspekty badawcze z różnych sektorów naukowych w kraju i na arenie międzynarodowej;
- zapewnienie kanału do wymiany informacji i współpracy z wielu dziedzin, m.in. energetyki, szeroko pojętej gospodarki krajowej czy finansów;
- kształcenie profesjonalnej kadry z możliwością nawiązywania międzynarodowych relacji wraz z dzieleniem się doświadczeniami.

Dążenie do poszerzenia swojego zasięgu tak, aby objąć wszystkie poziomy kariery i wykształcenia wśród młodych naukowców, nakłada na działania 3 aspekty:

1. Otwartości – przyjmowanie wszystkich pomysłów i perspektyw programowych.

2. Różnorodności – aktywne poszukiwanie perspektyw interdyscyplinarnych zawierających się w modułach technicznych, operacyjnych, korporacyjnych, rządowych i akademickich oraz zachęcanie tych grup społecznych do współpracy.
3. Kreatywności – promowanie wspólnych oraz innowacyjnych i dynamicznych programów badań angażujących do współpracy wymienione już sektory.

O planach powstania pierwszej elektrowni jądrowej w Polsce mówi się bardzo dużo. Merytoryczne kwestie, jak kalendarium rozpoczęcia prac, wybór lokalizacji, kształcenie kadr, to wiele stron założeń rządowych, które od 2010 r. nie zostały w pełni wdrożone do działania. Zmiany, jakie wdrożyło ówczesne Ministerstwo Gospodarki, dotyczyły modernizacji 2 zasadniczych dokumentów, w tym najważniejszego: Prawa atomowego z 1986 r., na którym oparto „założenia polityki energetycznej Polski do 2020 r.". Zgodnie z programem projekt elektrowni jądrowej ma być weryfikowany i modyfikowany co 4 lata, co teoretycznie pozwoli dopasować się do nowoczesnych rozwiązań technicznych i finansowych.

W dokumencie z 2014 r. *Polityka energetyczna Polski do 2025 r.* przyznano, że obliczenia prognostyczne wskazują na potrzebę rozpoczęcia eksploatacji energetyki jądrowej w ostatnim pięcioleciu rozpatrywanego okresu. Zakładano, że pierwszy blok elektrowni jądrowej powstanie między 2020 a 2025 r. Prace przesuwano, a każda weryfikacja ustawy i dokumentów wyznaczała kolejne lata na uruchomienie jakichkolwiek prac związanych z potencjałem nuklearnym. Wstępnie już na początku 2011 r. Polska Grupa Energetyczna podała do weryfikacji lokalizacje elektrowni: Gąski, Chorzewo i Żarnowiec – wszystkie w okolicy Morza Bałtyckiego, z naturalnym dostępem do wody chłodzącej. Badaniami lokalizacyjnymi miała zajmować się grupa WorleyParsons, która w 2014 r. została odsunięta od podpisanego kontraktu, a dalszymi pracami zajęła się spółka PGE EJ.

Zadaniem spółki była inauguracja Programu wsparcia rozwoju gmin lokalizacyjnych, który miał umacniać relacje pomiędzy gminami wyznaczonymi do inwestycji pierwszej EJ w Polsce. Założono, że koszt budowy tego rodzaju obiektu o mocy 3 GW na tamte czasy wyniesie około 40–60 mld zł. Niestety w 2016 r. PGE EJ1 wycofała się z realizacji zadań w Gąskach. Z przeprowadzonego referendum wynikało, aż 94% mieszkańców

była przeciwko budowie elektrowni. Negatywnym dopełnieniem braku realizacji zadań wynikających z PPEJ było opublikowanie raportu Najwyższej Izby Kontroli w 2018 r., w którym wskazano, że wydatki na realizację Programu polskiej energetyki jądrowej w latach 2014–2017 (III kwartał) wyniosły łącznie 776 mln zł, z czego 552,5 mln stanowiły koszty poniesione przez podmioty administracji publicznej, zaś 223,5 mln – przez PGE SA i jej spółkę zależną PGE EJ1. Natomiast w okresie prac przygotowawczych dotyczących PPEJ w latach 2010–2013 PGE EJ1 poniosła wydatki w wysokości 133,2 mln zł, a „spółka PGE EJ1 odpowiedzialna za realizację zadań związanych z przygotowaniem i budową pierwszej elektrowni jądrowej w Polsce, nie wykonała do końca września 2017 r. żadnego z działań przewidzianych w I etapie PPEJ".

Kolejne deklaracje oraz powrót do pomysłu wybudowania pierwszej EJ w Polsce pojawiły się w 2020 r., po ponownym zmodyfikowaniu Programu polskiej energetyki jądrowej i wdrożeniu poprawek do planu. Najważniejszym aspektem dokumentu *Polityka energetyczna Polski do 2040 r.* jest zakres ramowy, który uwzględnił założenia na dekadę – dopasowując się również do prawa klimatycznego obowiązującego na gruncie europejskim, i wskazał, że lata 2020–2033 będą kluczowe do wdrożenia pierwszych prac w zakresie energii jądrowej. W 2022 r. na potrzeby uruchomienia programu wykonano badania społeczne wśród mieszkańców gmin lokalizacyjnych oraz ościennych pt. *Postawy wobec energetyki jądrowej*. W badaniu wzięło udział 2006 osób z gmin: Choczewo, Gniewino, Krokowa oraz Łęczyce, Nowa Wieś Lęborska i Wicko. Na pytanie dotyczące planów budowy elektrowni jądrowej zdecydowane poparcie w tym zakresie udzieliło od 67% do 79% wszystkich badanych w gminach lokalizacyjnych (Choczewo – 67%, Gniewino – 79%, Krokowa – 76%) oraz od 60% do 80% w gminach ościennych (Łęczyce – 60%, Nowa Wieś Lęborska – 76%, Wicko – 80%). Zdecydowana większość respondentów zgadzała się ze stwierdzeniami, że rozwój energetyki jądrowej w Polsce zapewni mieszkańcom tańszą elektryczność (66% – gminy lokalizacyjne, 76% – gminy ościenne) oraz że Polska potrzebuje elektrowni jądrowej, ponieważ obecne źródła są niewystarczające dla zaspokojenia potrzeb energetycznych kraju (66% – gminy lokalizacyjne, 82% – gminy ościenne). Dodatkowo respondenci zwrócili uwagę na fakt, że zarówno odnawialne

źródła energii, jak i energetyka jądrowa powinny być rozwijane, aby zapewnić modernizację tego sektora przy wsparciu dla środowiska naturalnego, odchodząc od wykorzystania węgla i innych paliw kopalnych, które są wysokoemisyjne (gminy lokalizacyjne: fotowoltaika – 69%, morskie farmy wiatrowej – 58%, oraz energetyka jądrowa – 56%; gminy ościenne: fotowoltaika – 85%, lądowe farmy wiatrowe – 79%, energetyka jądrowa – 77%). Zwrócono również uwagę, że budowa elektrowni jądrowych w Polsce może zwiększyć ilość miejsc pracy w sektorze energetycznym.

Celem PPEJ jest uruchomienie elektrowni jądrowych o łącznej mocy 6–9 GW, stosując znane i sprawdzone reaktory PWR III i III+ generacji. Zwrócić uwagę również należy na aspekty szczegółowe planu:

1. Ukończenie całej inwestycji do 2043 r. z założeniem oddania pierwszego reaktora do użytku w 2033 r.
2. Rozpoczęcie prac w nadmorskiej lokalizacji Lubiatowo-Kopalino, w gminie Choczewo, która została wybrana na miejsce pierwszej EJ w Polsce (Komisja Europejska zatwierdziła w grudniu 2025 r. dokumenty wiążące).
3. Dokonanie szczegółowych analiz przemawiających za wdrożeniem elektrowni jądrowej, nawiązując do szeroko pojętego bezpieczeństwa energetycznego dla kraju skupionego na stabilności dostaw energii elektrycznej, zadbanie o klimat i środowisko przy wykorzystaniu najnowocześniejszych rozwiązań technologicznych oraz zwrócenie uwagi na ekonomikę przyszłości, obniżając koszt energii dla odbiorców końcowych.
4. Rozpisanie podstawowego zadania dla administracji rządowej w celu postępowania prac nad budową, m.in. rozwój zasobów ludzkich – kadry i zaplecze naukowe do rozwiązań przyszłościowych; rozwój infrastruktury energetycznej; wsparcie krajowego przemysłu; wzmocnienie systemu dozoru jądrowego oraz komunikacja i informacja społeczna, aby wspierać pozytywy dla atomu.

W sierpniu 2025 r. spółka PEJ zakończyła prace geologiczne w gminie Choczewo, których celem było zapoznanie się z warunkami hydrogeologicznymi oraz inżynieryjnymi. Zebrane dane pozwoliły na opracowanie wstępnego raportu bezpieczeństwa, który jest konieczny do złożenia wniosku o zezwolenie na budowę elektrowni. Analizy wykonane przez firmę

Bechtel pozwoliły na opracowanie składu chemicznego wód podziemnych, gliny i piasku, które posłużą do wykonania modelu geologicznego dla terenu przeznaczonego pod prace budowlane.

Według planów systemowych dla PEJ w 2028 r. mają zostać uruchomione pierwsze prace *stricte* budowlane pod pierwszy blok reaktora. Zakładając, że elektrownia w Choczewie będzie mieć moc 3000 MW, w 3 blokach po 1000 MW, łączna suma wyprodukowanej energii w ciągu roku, przy założeniu współczynnika mocy na poziomie 90%, wyniesie 23,652 TWh, co wyjaśnia obliczenie zgodne z przyjętymi zasadami przez IAEA: moc całej elektrowni to 3000 MW = 3 GW.

Współczynnik mocy, z jaką jest wykorzystywany reaktor: 90% (współczynnik ten zakłada, jak często elektrownia może pracować z pełną mocą. Obecnie najwyższy współczynnik na świecie zakłada 93% dla elektrowni o mocy 9,9 GW, która produkowałaby około 81 TWh rocznie). Liczba godzin w roku – przy założeniu, że to stabilne źródło, uniezależnione od warunków pogodowych – 365 dni × 24 h = 8760 h. Produkcja energii w MWh: 3000 MW × 0,90 × 8760 h = 23 652 000 MWh, czyli 23,652 TWh.

Elementem prowadzenia polityki wdrażającej program energetyki jądrowej jest również szkolenie kadr. Na zlecenie Ministerstwa Przemysłu tworzone są różnego rodzaju wydarzenia, np. *Polski przemysł dla energetyki jądrowej – szkolenia dla polskiego przemysłu pod kątem wykonania prac dla energetyki jądrowej* – edycja 2024, którego celem jest wyposażenie grup docelowych: budowlanej, elektrycznej i mechanicznej, w niezbędną wiedzę na temat wykorzystywanych technologii, bezpieczeństwa oraz jakości prac wykonywanych zgodnie z zasadami światowych doświadczeń z innych krajów.

Kolejnym przedsięwzięciem była edycja z 2025 r., której celem było podniesienie już istniejących kompetencji technicznych kadr oraz organizacyjnych krajowego przemysłu energetyki jądrowej oraz przekazanie polskiemu przemysłowi najbardziej aktualnych informacji o stanie realizacji inwestycji budowlanych w Choczewie, a także udzielenie informacji o światowych rozwiązaniach dla branży inwestycyjnych. Szkolenia były realizowane przy współpracy z Bureau Veritas (normy europejskie) oraz z ASME (normy amerykańskie).

Na początku 2026 r. Ministerstwo Energii zaproponowało rozwinięcie programu Atom na uczelniach. Projekt ministerialny połączył potencjał polskich uczelni zainicjowany w poprzednich latach i coraz szersze potrzeby w zakresie rozwijającego się przemysłu jądrowego nakładające obowiązek kształcenia wysokiej klasy specjalistów. Program Atom na uczelniach łączy wiedzę teoretyczną z jej zastosowaniem praktycznym, umożliwiając pracę przy projektach dla sektora jądrowego. W przedsięwzięciu uczestniczą polskie uczelnie i krajowe przedsiębiorstwa: Politechnika Gdańska, Politechnika Warszawska, Politechnika Śląska, Politechnika Wrocławska, Politechnika Poznańska oraz Akademia Górniczo-Hutnicza w Krakowie. Dodatkowo studenci mają możliwość uczestniczenia w stażach z przyjętymi normami ISO oraz ASME zgodnymi z wymogami prawa atomowego i dokumentacją środowiskową.

Interdyscyplinarność, umiędzynarodowienie szkoleń i perspektywa kształcenia nowych członków załóg energetycznych pozwalają na dostosowanie rozwiązań krajowych do tych stosowanych na całych świecie z założeniem struktur bezpieczeństwa i wykorzystania potencjału kraju dopasowanego do najnowocześniejszych, sprawdzonych rozwiązań.

Justyna Rokitowska

Center for Strategic and International Studies, *On the Horizon A Collection of Papers from the Next Generation*, R. Younis (ed.), https://nuclearnetwork.csis.org/wp-content/uploads/2021/02/210223_PONI_Horizon_Vol.3.pdf (dostęp 15.12.2025); Izba Gospodarcza Energetyki i Ochrony Środowiska, https://igeos.pl/nuclear/(dostęp 14.01.2026); *Nuclear Energy in Poland Assessment of Readiness for the Construction of the First Nuclear Power Plan, Report*, https://www.bakermckenzie.com/-/media/files/locations/poland/nuclear-energy-in-poland/baker-mckenzie-polityka-insight-report-nuclear-energy-in-poland-2025_eng.pdf (dostęp 14.01.2026); Polityka energetyczna Polski do 2040 r. (PEP2040), https://www.gov.pl/attachment/3209a8bb-d621-4d41-9140-53c4692e9ed8 (dostęp 30.12.2025); Program polskiej energetyki jądrowej do 2040 r., https://www.gov.pl/attachment/af5dae43-de29-4a5d-9ecd-0c96e4d69219 (dostęp 10.01.2026); J. Rokitowska, A. Wasiuta, *Ekonomiczne i społeczne aspekty bezpieczeństwa sektora energetycznego w kontekście zrównoważonego rozwoju*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2019; J. Rokitowska, J. Popławska, A. Wasiuta, *Determinanty ekonomiczne bezpieczeństwa energetycznego – od ery węglowej*

do energetyki obywatelskiej, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2022; Royal United Services Institute, *The 2022 UK PONI Annual Conference EDITORS Ana Alecsandru Jack Crawford A Collection of Papers from Emerging Nuclear Experts*, A. Alecsandru, J. Crawford (eds.), https://static.rusi.org/uk-poni-papers-2022.pdf (dostęp 12.10.2025); Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe, Dz.U. 2026, poz. 1; *Zielone światło z Komisji Europejskiej dla atomu w Polsce. Bruksela zgodziła się na pomoc publiczną dla elektrowni jądrowej na Pomorzu*, https://pej.pl/dla-mediow/aktualnosc/zielone-swiatlo-z-komisji-europejskiej-dla-atomu-w-polsce-bruksela-zgodzila-sie-na-pomoc-publiczna-dla-elektrowni-jadrowej-na-pomorzu/ (dostęp 29.01.2026).

PRZESTĘPCZOŚĆ NIELETNICH (ang. *juvenile delinquency)* – termin powszechnie stosowany w literaturze prawniczej i kryminologicznej obejmujący czyny karalne oraz przejawy demoralizacji popełniane przez osoby, które co do zasady nie podlegają pełnej odpowiedzialności karnej. Minimalny wiek odpowiedzialności karnej jest zróżnicowany w poszczególnych państwach i mieści się najczęściej w przedziale od 12 do 18 lat, podczas gdy wiek pełnej odpowiedzialności karnej w większości porządków prawnych z reguły wynosi 18 lat. W ramach niektórych rozwiązań ustawodawczych osoby, które ukończyły 18 rok życia, mogą nadal podlegać jurysdykcji sądów dla nieletnich, a tym samym być traktowane jak osoby niepełnoletnie, jednak rozwiązanie to ma zazwyczaj charakter wyjątkowy i fakultatywny.

Prawo międzynarodowe nie precyzuje jednoznacznie pojęcia „przestępczości nieletnich", co wynika z różnic w podejściu do penalizacji poszczególnych zachowań w systemach prawnych na całym świecie. Termin ten jest problematyczny i w niektórych kontekstach może przyjmować wydźwięk pejoratywny, obarczony mylącymi negatywnymi założeniami. Z tego względu od kilku lat Organizacja Narodów Zjednoczonych posługuje się określeniem „dzieci pozostające w konflikcie z prawem" (ang. *children in conflict with the law*) lub „dzieci, które są podejrzewane o naruszenie prawa karnego, oskarżone o takie naruszenie lub uznane za winne jego popełnienia" (ang. *children alleged as, accused of, or recognized as having infringed the penal law*) w celu opisania zróżnicowanej i heterogenicznej grupy osób poniżej 18 roku życia, które naruszyły prawo lub są zagrożone jego naruszeniem.

Od lat 80. XX w. problematyka ochrony praw nieletnich była przedmiotem debaty na forum Organizacji Narodów Zjednoczonych oraz Rady Europy, co znalazło odzwierciedlenie w przyjmowanych dokumentach międzynarodowych. Wymienione poniżej akty prawne mają znaczenie moralne i polityczne oraz stanowią katalog reguł i zaleceń, z których część ma charakter wiążący ze względu na ich ujęcie w Konwencji o prawach dziecka (ang. The United Nations Convention on the Rights of the Child) z 1989 r. Są to:

- wzorcowe reguły minimalne dotyczące wymiaru sprawiedliwości wobec nieletnich – tzw. reguły pekińskie (ang. The United Nations Standard Minimum Rules for the Administration of Juvenile Justice) – Rezolucja Zgromadzenia Ogólnego 40/33 z dnia 29 listopada 1985 r., wprowadzające i porządkujące terminologię: nieletni (ang. *juvenile*), nieletni przestępca (ang. *juvenile offender*), system wymiaru sprawiedliwości dla nieletnich (ang. *juvenile justice system*);
- wskazania Narodów Zjednoczonych dotyczące zapobiegania przestępczości nieletnich – tzw. wskazania rijadzkie (ang. The United Nations Guidelines for the Prevention of Juvenile Delinquency) – Rezolucja Zgromadzenia Ogólnego 45/112 z dnia 14 grudnia 1990 r., koncentrujące się na prewencji;
- reguły Narodów Zjednoczonych dotyczące ochrony nieletnich pozbawionych wolności – tzw. reguły hawańskie (ang. The United Nations Rules for the Protection of Juveniles Deprived of their Liberty) – Rezolucja Zgromadzenia Ogólnego 45/113 z dnia 14 grudnia 1990 r., porządkujące terminologię związaną z nieletnimi w instytucjach zamkniętych;
- zalecenia Komitetu Ministrów Rady Europy, m.in.
- zalecenie w sprawie nowych sposobów postępowania z przestępczością nieletnich oraz roli w tym zakresie instytucji wymiaru sprawiedliwości (ang. *New ways of dealing with juvenile delinquency and the role of juvenile justice*) z 24 września 2003 r., promujące sprawiedliwość naprawczą, edukację, minimalizację izolacji oraz resocjalizację nieletnich w środowisku otwartym;

- europejskie reguły wykonywania sankcji i środków orzeczonych wobec nieletnich sprawców czynów karalnych (ang. European Rules for Juvenile Offenders Subject to Sanctions and Measures – ERJOSSM) z 5 listopada 2008 r., w których zawarto zapisy dotyczące obowiązku traktowania młodych sprawców z poszanowaniem praw człowieka, indywidualizacji i proporcjonalności sankcji czy promujące środki alternatywne i resocjalizacyjne, mediacje oraz podejście wielodyscyplinarne.

W polskim systemie prawnym określenie „nieletni" dotyczy osoby, która nie ukończyła 17 roku życia. Co do zasady, nieletni nie podlega odpowiedzialności przewidzianej w Kodeksie karnym, co wynika z art. 10 §1. Kolejne paragrafy tego artykułu wskazują jednak na wyjątki od tej sytuacji: §2 dotyczy nieletnich, którzy po ukończeniu 15 roku życia dopuszczają się czynu zabronionego określonego w następujących artykułach Kodeksu karnego:

- art. 134 – zamach na życie prezydenta RP;
- art. 148 §1–3 – zabójstwo, zabójstwa kwalifikowane;
- art. 156 §1 i 3 – ciężki uszczerbek na zdrowiu (w tym skutkujący śmiercią);
- art. 163 §1 i 3 – sprowadzenie zdarzenia powszechnie niebezpiecznego zagrażającego życiu lub zdrowiu wielu osób;
- art. 166 – przejęcie kontroli nad środkiem transportu z użyciem przemocy lub groźby;
- art. 173 §1 i 3 – sprowadzenie katastrofy w ruchu lądowym, wodnym lub powietrznym zagrażającej życiu lub zdrowiu wielu osób;
- art. 197 §1, 1a, 3–5 – zgwałcenie i przestępstwa seksualne z użyciem przemocy lub wobec małoletniego;
- art. 223 §2 – czynna napaść na funkcjonariusza publicznego ze skutkiem ciężkiego uszczerbku;
- art. 252 §1 i 2 – wzięcie lub przetrzymanie zakładnika;
- art. 280 – rozbój.

Przepis określa przesłanki, na podstawie których nieletni, który dopuścił się czynu zabronionego wskazanego w ustawie, może ponosić odpowiedzialność na zasadach przewidzianych w niniejszym kodeksie.

Obejmują one okoliczności sprawy oraz stopień rozwoju sprawcy, jego właściwości i warunki osobiste, w szczególności bezskuteczność wcześniej stosowanych środków wychowawczych lub poprawczych.

W przypadku orzekania wobec nieletniego na zasadach przewidzianych dla dorosłych kara nie może przekroczyć 2/3 górnej granicy ustawowego zagrożenia, o ile przestępstwo nie jest zagrożone karą dożywotniego pozbawienia wolności; sąd może ponadto zastosować nadzwyczajne złagodzenie kary (art. 10 §3 Kodeksu karnego).

§4 określa zasady odpowiedzialności sprawców w wieku od 17 do 18 lat, wobec których – w razie popełnienia występku – sąd może zamiast kary zastosować środki wychowawcze, lecznicze lub poprawcze przewidziane dla nieletnich, jeżeli przemawiają za tym okoliczności sprawy oraz stopień rozwoju sprawcy, jego właściwości i warunki osobiste.

Odpowiedzialność nieletnich reguluje ustawa z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich (Dz.U. 2022, poz. 1700 z późn. zm.), która weszła w życie 1 września 2022 r., zastępując ustawę z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (t.j. Dz.U. 2018, poz. 969 z późn. zm.). Ustawa obejmuje 7 działów regulujących zagadnienia o charakterze materialnym, procesowym oraz wykonawczym. Już sam tytuł ustawy akcentuje jej wychowawczo-ochronny charakter, którego celem jest wspieranie nieletnich w przezwyciężaniu trudności prowadzących do demoralizacji oraz kształtowanie właściwych postaw społecznych.

W preambule podkreślono nadrzędną rolę rodziców w procesie wychowawczym, wskazując jednocześnie na zasadę subsydiarności państwa, którego ingerencja jest dopuszczalna w przypadku ujawnienia patologii zagrażających prawidłowemu rozwojowi dziecka.

Zgodnie z art. 1 ust. 1 ustawy możliwe jest wszczęcie postępowania w sprawach o demoralizację wobec osób, które ukończyły 10 lat, oraz postępowania w sprawach o czyny karalne wobec osób, które dopuściły się go po ukończeniu 13, a przed ukończeniem 17 roku życia. Przepisy ustawy przewidują także wykonywanie środków wychowawczych, leczniczych lub poprawczych w stosunku do osób, wobec których zostały one orzeczone, nie dłużej jednak niż do ukończenia przez nie 21 lat, chyba że ustawa stanowi inaczej.

Ustawodawca określił katalog przejawów demoralizacji, do których zaliczono m.in. dopuszczanie się czynów zabronionych, naruszanie zasad współżycia społecznego, uchylanie się od obowiązku szkolnego lub nauki, używanie alkoholu oraz substancji psychoaktywnych, a także uprawianie nierządu (art. 4 ust. 1). Zgodnie z ustawą nieletni popełniają „czyny karalne", przez które rozumie się czyn zabroniony przez ustawę jako przestępstwo, przestępstwo skarbowe, wykroczenie lub wykroczenie skarbowe (art. 1 ust. 2).

Na podstawie art. 4 ust. 1–3 ustawy na obywateli oraz instytucje państwowe, samorządowe i placówki oświatowe nałożono obowiązek zawiadomienia właściwych organów o okolicznościach świadczących o demoralizacji nieletniego lub popełnieniu przez niego czynu karalnego. Jednocześnie art. 4 ust. 4 przyznaje dyrektorom szkół kompetencję do zastosowania – za zgodą nieletniego oraz jego rodziców lub opiekunów – środków oddziaływania wychowawczego, jeżeli są one wystarczające, z wyłączeniem przypadków czynów stanowiących przestępstwa ścigane z urzędu lub przestępstwa skarbowe.

Zasadniczymi formami reakcji na zachowania nieletnich są środki wychowawcze, środek leczniczy oraz środek poprawczy, natomiast orzeczenie kary jest dopuszczalne wyłącznie w przypadkach określonych w ustawie, gdy inne środki nie zapewniają resocjalizacji nieletniego (art. 6).

Do środków wychowawczych (art. 7) należą:

- upomnienie;
- zobowiązanie do określonego postępowania (naprawienie szkody, zadośćuczynienie, prace społeczne, przeproszenie pokrzywdzonego, podjęcie nauki lub pracy, uczestnictwo w zajęciach wychowawczych, terapeutycznych lub szkoleniowych, powstrzymanie się od przebywania w określonych środowiskach lub miejscach, powstrzymanie się od kontaktowania się z pokrzywdzonym lub innymi osobami w określony sposób, zaniechanie używania substancji psychoaktywnych);
- nadzór odpowiedzialny rodziców albo opiekuna;
- nadzór organizacji społecznej, pracodawcy lub osoby godnej zaufania udzielających poręczenia za nieletniego;
- nadzór kuratora sądowego;

- skierowanie do ośrodka kuratorskiego lub odpowiedniej organizacji/instytucji;
- zakaz prowadzenia pojazdów;
- przepadek przedmiotów lub korzyści majątkowych związanych z czynem zabronionym;
- umieszczenie w rodzinie zastępczej zawodowej;
- umieszczenie w młodzieżowym ośrodku wychowawczym;
- umieszczenie w okręgowym ośrodku wychowawczym, przy czym sąd kieruje do tej placówki nieletniego, gdy dopuścił się przestępstwa lub przestępstwa skarbowego i przemawiają za tym stopień demoralizacji, rodzaj czynu, okoliczności jego popełnienia oraz nieskuteczność innych środków wychowawczych (art. 14 ust. 1–3).

Wykonywanie tych środków regulują art. 144–211 ustawy.

Ustawa reguluje także stosowanie środków tymczasowych (art. 44), które odpowiadają poszczególnym środkom wychowawczym, ale mają charakter czasowy i stosowane są na czas postępowania sądowego lub do czasu ostatecznego rozstrzygnięcia. Nie przesądzają one o zastosowaniu środków wychowawczych ostatecznych, które mogą być orzeczone dopiero po zakończeniu postępowania.

Do środków tymczasowych należą:

- tymczasowy nadzór organizacji społecznej, pracodawcy lub osoby godnej zaufania;
- tymczasowy nadzór kuratora sądowego;
- tymczasowe skierowanie do ośrodka kuratorskiego lub organizacji/instytucji wychowawczej, terapeutycznej lub szkoleniowej;
- tymczasowe umieszczenie w rodzinie zastępczej zawodowej;
- tymczasowe umieszczenie w młodzieżowym ośrodku wychowawczym;
- tymczasowe umieszczenie w okręgowym ośrodku wychowawczym;
- tymczasowe umieszczenie w zakładzie leczniczym;
- umieszczenie w schronisku dla nieletnich;
- tymczasowe zobowiązanie rodziców lub opiekuna do poprawy warunków wychowawczych, bytowych lub zdrowotnych,

współpracy ze szkołą, poradnią psychologiczno-pedagogiczną lub placówką wychowawczą oraz realizacji obowiązku nauki i socjoterapii nieletniego.

Wykonywanie tych środków regulują art. 289–320 ustawy.

Środkiem leczniczym jest umieszczenie w zakładzie leczniczym (art. 8). Może być orzeczony przez sąd rodzinny w przypadku stwierdzenia u nieletniego choroby psychicznej, innego zakłócenia czynności psychicznych lub uzależnienia (art. 17). Wykonywanie tego środka regulują art. 212–232 ustawy.

Środkiem poprawczym jest umieszczenie nieletniego w zakładzie poprawczym (art. 9). W przypadku popełnienia przez nieletniego czynu karalnego określonego w art. 134, art. 148 §1–3, art. 156 §1 lub 3, art. 163 §1 lub 3, art. 166, art. 173 §1 lub 3, art. 197 §1, 1a, 3–5, art. 223 §2, art. 252 §1 lub 2 albo art. 280 sąd rodzinny co do zasady orzeka umieszczenie w zakładzie poprawczym (art. 15 ust. 2).

Wyjątkowo możliwe jest zastosowanie środka wychowawczego, jeżeli sposób i okoliczności popełnienia czynu, właściwości i warunki osobiste nieletniego oraz jego postawa i zachowanie uzasadniają przypuszczenie, że środek ten będzie skuteczny lub będzie rokował resocjalizację (art. 15 ust. 3). W takim przypadku sąd rodzinny określa rodzaj zakładu poprawczego, w którym środek ma być wykonywany (art. 15 ust. 5).

W uzasadnionych przypadkach, w szczególności ze względu na wysoki stopień demoralizacji nieletniego lub przebieg dotychczasowego procesu resocjalizacji, sąd rodzinny może zagrozić przedłużeniem wykonywania środka poprawczego po ukończeniu przez nieletniego 21 lat albo orzec jego wykonywanie po ukończeniu tego wieku, nie dłużej jednak niż do ukończenia 24 lat (art. 15 ust. 6 pkt 1–2).

Wykonywanie środka poprawczego regulują art. 233–285 ustawy.

Na rodziców (opiekunów) nieletniego mogą zostać nałożone określone obowiązki, w szczególności poprawy warunków wychowawczych, bytowych lub zdrowotnych nieletniego, a także ścisłej współpracy ze szkołą, do której uczęszcza, oraz z poradnią psychologiczno-pedagogiczną, w tym – w razie potrzeby – w zakresie przeprowadzenia odpowiedniej diagnozy. Obowiązki te mogą obejmować również współpracę z podmiotem wykonującym działalność leczniczą lub z młodzieżowym ośrodkiem

socjoterapii w zakresie realizacji obowiązku nauki, socjoterapii oraz pomocy psychologiczno-pedagogicznej, jak również obowiązek naprawienia w całości albo w części szkody wyrządzonej przez nieletniego bądź zadośćuczynienia za doznaną krzywdę. Zasady wykonywania tych środków określają art. 286–288 ustawy.

Poza środkami kierowanymi wobec rodziców lub opiekunów ustawa określa także uprawnienia Policji w sytuacjach, w których zachodzi uzasadnione przypuszczenie, że nieletni dopuścił się przestępstwa lub przestępstwa skarbowego, a jednocześnie istnieje obawa jego ucieczki, ukrycia się, zatarcia śladów czynu karalnego albo brak jest możliwości ustalenia jego tożsamości. W takich przypadkach Policja może dokonać zatrzymania nieletniego, a następnie umieścić go w policyjnej izbie dziecka (art. 48 ust. 1). Analogiczne uprawnienia przysługują Straży Granicznej (art. 48 ust. 2). O zatrzymaniu nieletniego niezwłocznie zawiadamia się właściwy sąd rodzinny oraz rodzica, rodziców albo opiekuna, pod którego stałą pieczą pozostaje nieletni (art. 48 ust. 5).

Ustawa szczegółowo reguluje przebieg postępowania rozpoznawczego w sprawach nieletnich (art. 23–34), określając jednocześnie krąg stron postępowania (art. 35), uprawnienia nieletniego (art. 36), sposób jego działania (art. 37–39) oraz pojęcie osoby pokrzywdzonej (art. 40–41). Dalsze przepisy zawierają szczegółowe unormowania dotyczące przebiegu postępowania w sprawie nieletniego (art. 52–106).

Kolejny rozdział ustawy, obejmujący art. 107–142, poświęcony jest prawom i obowiązkom nieletnich. Wśród rozbudowanego katalogu regulacji na szczególną uwagę zasługuje wprowadzenie nowego rozwiązania dotyczącego zapewnienia odpowiedniego wsparcia dla nieletnich matek umieszczonych w okręgowych ośrodkach wychowawczych, zakładach poprawczych oraz schroniskach dla nieletnich (art. 135). W tym celu w wyznaczonych placówkach przewidziano tworzenie domów dla matki i dziecka, w których dziecko może przebywać do ukończenia 3 roku życia. W młodzieżowych ośrodkach wychowawczych domy te funkcjonują jako odrębne grupy wychowawcze.

Końcowe przepisy ustawy precyzują natomiast zasady organizacji okręgowych ośrodków wychowawczych, zakładów poprawczych oraz

schronisk dla nieletnich (art. 321–344), a także regulacje dotyczące zapewnienia bezpieczeństwa w tych placówkach (art. 345–357).

Na tle obowiązujących regulacji istotne znaczenie ma sposób gromadzenia danych statystycznych dotyczących czynów karalnych popełnianych przez nieletnich. Do końca 2012 r. były one ujmowane w statystykach Policji w momencie skierowania wniosku o wszczęcie postępowania do sądu rodzinnego i nieletnich. Od 2013 r., zgodnie z informacją Biura Prawnego Komendy Głównej Policji, dane te są gromadzone wyłącznie na podstawie postępowań przygotowawczych prowadzonych przez Policję. Choć zasadą jest pozyskiwanie informacji po zakończeniu postępowania sądowego w sprawach nieletnich, brak przepisów zobowiązujących sądy do przekazywania Policji informacji zwrotnej powoduje, że statystyki nie obejmują wszystkich czynów karalnych popełnianych przez nieletnich. Dodatkowo w danych porównywana jest liczba czynów zabronionych stwierdzonych, w tym popełnionych przez nieustalonych sprawców, z liczbą zdarzeń, w których sprawcami byli nieletni. Wskazane nieścisłości metodologiczne sprawiają, że statystyki Policji oddają jedynie część rzeczywistej skali zjawiska, a analiza oparta wyłącznie na tych danych może prowadzić do jego zniekształconej oceny.

Jednocześnie od 1 stycznia 2014 r., na mocy Rozporządzenia Rady Ministrów z dnia 9 sierpnia 2013 r. w sprawie programu badań statystycznych statystyki publicznej na rok 2014 (Dz.U. 2013, poz. 1159), Ministerstwo Sprawiedliwości zostało zobowiązane do gromadzenia i przekazywania do Głównego Urzędu Statystycznego danych dotyczących nieletnich oraz popełnianych przez nich czynów karalnych, co częściowo uzupełnia lukę informacyjną w tym zakresie.

Z danych Komendy Głównej Policji wynika, że w latach 1990–2012 czyny karalne popełniane przez nieletnich stanowiły średnio 6,8% ogółu przestępstw stwierdzonych, przy czym ich udział był najwyższy w latach 1995 (8,5%), 2010 (8,7%) oraz 2011 (8,7%). Statystyki wskazują, że w latach 1990–1995 odnotowano systematyczny wzrost liczby czynów karalnych popełnianych przez nieletnich. W okresie 1996–2008 ich liczba utrzymywała się na zbliżonym poziomie, przy czym wyraźny spadek wystąpił w latach 2002–2003. Następnie, od 2009 r. zaobserwowano ponowny wzrost, który utrzymywał się do 2012 r.

Dane wskazują, że w latach 2013–2025 udział nieletnich dopuszczających się czynów karalnych w ogólnej liczbie stwierdzonych przestępstw wykazywał wyraźną tendencję spadkową, z niewielkimi odchyleniami w latach 2016 i 2024. W analizowanym okresie liczba tych czynów zmniejszyła się z 70 339 (6,6%) w 2013 r. do 16 854 (2,1%) w 2025 r.

Zdecydowana większość czynów karalnych popełnianych przez nieletnich ma charakter przestępstw pospolitych. Statystyki Policji wskazują, że w latach 2013–2014 najczęściej czyny te dotyczyły naruszeń przepisów Ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz.U. 2005, nr 179, poz. 1485, t.j. Dz.U. 2023, poz. 1939) oraz czynów karalnych z kategorii przestępstw przeciwko mieniu, w szczególności kradzieży cudzej rzeczy, rozbojów, a także kradzieży i wymuszeń.

Z kolei w latach 2015–2025 do najczęściej popełnianych przez nieletnich czynów karalnych należały czyny zabronione ustawą o przeciwdziałaniu narkomanii, kradzieże cudzej rzeczy oraz kradzieże z włamaniem. W analizowanym okresie nieletni dopuszczali się również innych czynów karalnych, takich jak uszkodzenie rzeczy, kradzież samochodu (w tym kradzież z włamaniem), udział w bójce lub pobiciu, spowodowanie uszczerbku na zdrowiu oraz zgwałcenie.

W analizowanych latach odnotowywano także pojedyncze przypadki zabójstw z udziałem nieletnich, przy czym ich najwyższą liczbę – 11– stwierdzono w 2016 r.

Ze statystyk publikowanych przez Wydział Statystycznej Informacji Zarządczej Departamentu Strategii i Funduszy Europejskich Ministerstwa Sprawiedliwości za lata 2000–2020 wynika, że na podstawie prawomocnych orzeczeń wydawanych w latach 2000–2008 odnotowano wzrost liczby dziewcząt, wobec których stwierdzono czyny świadczące o demoralizacji oraz czyny karalne. Z kolei od 2009 r. obserwuje się stopniowy spadek liczby dziewcząt dopuszczających się tego rodzaju zachowań, przy jednoczesnym wystąpieniu niewielkich wzrostów w latach 2011, 2016 oraz 2018.

Badania prowadzone na całym świecie wskazują, że w krajach wysoko rozwiniętych obserwuje się wyraźną tendencję spadkową w zakresie popełniania czynów karalnych przez osoby nieletnie. Zjawisko to wiąże się m.in. z rozwojem systemów prewencyjnych, wzrostem efektywności

mechanizmów nadzoru nad nieletnimi oraz zachodzącymi przemianami demograficznymi i społeczno-kulturowymi, które kształtują kontekst wychowawczy i społeczny młodzieży.

Popełnianie czynów karalnych przez nieletnich jest zjawiskiem złożonym, uwarunkowanym wieloma czynnikami. W literaturze przedmiotu wyróżnia się 3 główne grupy czynników wpływających na to zjawisko.

Pierwszą z nich stanowią czynniki rodzinne i środowiskowe, obejmujące m.in. konflikty rodzinne, przemoc domową oraz zaniedbania wychowawcze, takie jak brak zaspokojenia potrzeb materialnych i niematerialnych, niewystarczający nadzór czy brak wsparcia emocjonalnego i poczucia bezpieczeństwa. Istotną rolę odgrywają również doświadczenia związane z przestępczością w rodzinie, marginalizacja społeczna, ubóstwo oraz wpływ środowiska rówieśniczego, zwłaszcza kontakty z osobami dopuszczającymi się czynów karalnych, wynikające z potrzeby przynależności lub chęci zaimponowania otoczeniu.

Drugą grupę stanowią czynniki indywidualne, takie jak zaburzenia emocjonalne (impulsywność, chwiejność emocjonalna, podwyższony poziom lęku), zaburzenia neurorozwojowe, w tym ADHD, a także zaburzenia zachowania przejawiające się agresją, kłamstwami, okrucieństwem czy ucieczkami z domu. Do tej kategorii zalicza się również problemy związane z używaniem substancji psychoaktywnych oraz trudności w funkcjonowaniu szkolnym, w tym brak zaangażowania i przedwczesne opuszczanie systemu edukacji.

Trzecią grupę tworzą czynniki instytucjonalne, związane z funkcjonowaniem szkół, sądów rodzinnych oraz systemów wsparcia społecznego, których działania mogą zarówno ograniczać, jak i sprzyjać zachowaniom antyspołecznym. Badania wskazują, że największą skuteczność w ograniczaniu recydywy osiągają systemy łączące oddziaływania resocjalizacyjne, edukacyjne i terapeutyczne z działaniami wychowawczymi oraz prewencyjnymi. Zintegrowane strategie nie tylko umożliwiają reagowanie na czyny karalne, lecz także wspierają rozwój kompetencji społecznych i emocjonalnych nieletnich, co ma kluczowe znaczenie dla ich długofalowej reintegracji społecznej.

W oparciu o kryteria odpowiedzialności za popełniony czyn, roli sądu oraz innych organów i instytucji w postępowaniu, charakteru stosowanych

środków oraz celu podejmowanej interwencji można wyróżnić następujące modele postępowania z nieletnimi:

1. Model jurydyczny (karnistyczny/sprawiedliwościowy) – ukształtowany w I połowie XX w., oparty na założeniach klasycznej szkoły prawa karnego i koncepcji kary zasłużonej (ang. *just deserts*). Nieletni sprawcy, po przekroczeniu dolnej granicy wieku, traktowani są – z pewnymi ograniczeniami – jako osoby zdolne do ponoszenia odpowiedzialności za swoje czyny. Stosowane sankcje mają charakter zbliżony do kar dla dorosłych, są bezwzględnie oznaczone i proporcjonalne do ciężaru czynu. Zakłada się izolację nieletnich sprawców od dorosłych. Sprawy rozpoznawane są przez sądy karne lub wyspecjalizowane sądy dla nieletnich.
2. Model opiekuńczy – ukształtowany również w I połowie XX w., oparty na pozytywistycznej koncepcji przestępczości. Zakłada, że przestępczość nieletnich wynika głównie z uwarunkowań środowiskowych, za które nieletni nie ponoszą pełnej odpowiedzialności. Celem postępowania jest ochrona dobra dziecka poprzez wychowanie i pomoc. Interwencja ma charakter wychowawczy i prewencyjny, obejmuje także reakcję na przejawy niedostosowania społecznego. Postępowanie jest odformalizowane, a istotną rolę odgrywają specjaliści nauk społecznych.
3. Model kontroli kryminalnej (represyjny) – wykształcony w latach 60. XX w., ukierunkowany na ukaranie oraz izolację nieletnich sprawców. Jego celem jest ochrona porządku publicznego i bezpieczeństwa obywateli poprzez skuteczne zwalczanie przestępczości. Zakłada stosowanie wobec nieletnich procedur zbliżonych do tych, które obowiązują dorosłych sprawców.
4. Model uczestnictwa („minimum interwencji") – ukształtowany w latach 70. XX w., oparty na krytyce resocjalizacji. Odwołuje się do teorii naznaczania społecznego, która zakłada, że formalne reakcje wymiaru sprawiedliwości prowadzą do stygmatyzacji, która sprzyja dalszej karierze przestępczej. Postuluje maksymalne ograniczenie kontroli formalnej, zwłaszcza sądowej, rezygnację ze środków izolacyjnych oraz stosowanie alternatywnych, nieformalnych

sposobów reagowania na czyn karalny. Celem jest poprawa szans życiowych nieletnich.

5. Model multiagencyjny – rozwinięty w latach 70. XX w., wywodzący się z idei sprawiedliwości naprawczej. Nieletni traktowany jest jako osoba niewłaściwie zsocjalizowana, wobec której należy podjąć skoordynowaną interwencję instytucjonalną. Zakłada współpracę m.in. policji, kuratorów, pedagogów i pracowników socjalnych. Preferuje unikanie postępowania sądowego i środków izolacyjnych, koncentrując się na naprawieniu szkody i aktywnym udziale nieletniego w tym procesie.
6. Model neokorekcyjny – ukształtowany w latach 80. XX w., akcentujący odpowiedzialność nieletnich sprawców za popełnione czyny, a w określonych przypadkach także ich rodziców lub opiekunów wobec ofiar i społeczeństwa. Nieletni postrzegany jest jako podmiot zdolny do ponoszenia odpowiedzialności za swoje zachowanie. Model ten zakłada poprawę efektywności wymiaru sprawiedliwości poprzez lepszą koordynację działań różnych instytucji zajmujących się sprawami nieletnich. Ukierunkowany jest zarówno na ograniczanie przestępczości nieletnich, jak i zapobieganie oraz zwalczanie zachowań przedprzestępczych.
7. Model rehabilitacyjny (terapeutyczny) – ukształtowany w latach 90. XX w. oraz na początku XXI w., oparty na założeniu, że przestępczość nieletnich ma często charakter przejściowy, a młody człowiek jest podatny na zmianę. Jego celem jest zmiana zachowania nieletniego poprzez indywidualną diagnozę oraz dostosowanie oddziaływań do rozpoznanych przyczyn i potrzeb w obszarze rodziny, szkoły, zdrowia psychicznego i uzależnień. Obejmuje programy edukacyjne, szkolenia zawodowe, terapię, rozwijanie umiejętności społecznych, wsparcie psychologiczne oraz pracę z rodziną. Model ten zakłada odrębność od systemu dorosłych oraz kładzie silniejszy nacisk na prawa dziecka, zgodnie ze standardami ONZ i Konwencją o prawach dziecka.
8. Model rozwojowy – ukształtowany na początku XXI w., wywodzący się z badań neurobiologicznych. Zakłada, że młody człowiek różni się od dorosłego pod względem neurologicznym, poznawczym

i psychospołecznym, a większość nieletnich naturalnie wychodzi z zachowań przestępczych wraz z dojrzewaniem. Celem jest wsparcie rozwoju poprzez pracę nad otoczeniem nieletniego i jego codzienną rutyną. Istotnym elementem jest probacja – opracowanie indywidualnego planu wspólnie z nieletnim i jego rodziną, objęcie go nadzorem i pomocą kuratora oraz stosowanie stopniowanych, przewidywalnych reakcji na naruszenie zasad i postępy.

W praktyce żaden z przedstawionych modeli nie funkcjonuje w czystej postaci. Systemy postępowania z nieletnimi przyjęte w poszczególnych krajach łączą w zróżnicowanych proporcjach elementy odmiennych koncepcji teoretycznych i rozwiązań instytucjonalnych. Ponadto badania empiryczne wskazują, że w niektórych państwach wykształciły się także alternatywne modele lub specyficzne podejścia interwencyjne. Potrzebę integrowania elementów różnych modeli postępowania z nieletnimi akcentują również dokumenty międzynarodowe dotyczące standardów traktowania młodzieży pozostającej w konflikcie z prawem.

Polski system prawny oraz praktyka jego stosowania odzwierciedlają hybrydowy charakter tych rozwiązań, stanowiąc połączenie tradycyjnego, kontrolnego (represyjnego) podejścia z wyraźnymi, choć nadal fragmentarycznymi, elementami modelu rehabilitacyjnego oraz nowoczesnych koncepcji rozwojowych, wdrażanych w ograniczonym zakresie w ramach wybranych programów i placówek.

Agnieszka Polończyk-Sudoł

R. Ball, S. Baidawi, A. FitzGerald, *Approaches for supporting youth dually involved in child protection and youth justice systems: An international policy analysis*, „Journal of Criminology" 2024, vol. 57, no. 4; M.W. Bernasiewicz, M. Noszczyk-Bernasiewicz, *Przestępczość nieletnich w USA i w Polsce na podstawie wybranych statystyk kryminalnych*, „Archiwum Kryminologii" 2020, t. XLII, nr 2; C. Cavanagh, *Healthy adolescent development and the juvenile justice system: Challenges and solutions*, „Child Development Perspectives" 2022, vol. 16, no. 3; M.D. McShane, M. Cavanaugh, *Understanding Juvenile Justice and Delinquency*, Praeger, Santa Barbara 2015; B. Stańdo-Kawecka, *Założenia modelowe i standardy międzynarodowe dotyczące nieletnich sprawców przestępstw*, „Archiwum Kryminologii" 2007–2008, t. XXIX–XXX; *The Handbook of Juvenile Delinquency and Juvenile Justice*, M.D. Krohn, J. Lane (eds.), John Wiley & Sons, Chichester, West Sussex 2015; Ustawa

z 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich, Dz.U. 2022, poz. 1700 ze zm.; L. Wieczorek, *Przestępczość i demoralizacja nieletnich w Polsce w okresie transformacji ustrojowej*, Wydawnictwo Naukowe „Śląsk", Katowice 2006; J. Włodarczyk-Madejska, *Skazani na wychowanie. Stosowanie środków izolacyjnych wobec nieletnich*, Wydawnictwo Instytutu Nauk Prawnych PAN, Warszawa 2019; S. Young, B. Greer, R. Church, *Juvenile delinquency, welfare, justice and therapeutic interventions: a global perspective*, „BJPsych Bulletin" 2017, vol. 41, no. 1.

PRZESTĘPSTWO – czyn zabroniony uznany za zasadniczo społecznie szkodliwy lub społecznie niebezpieczny, konkretnie zdefiniowany i zagrożony karą na mocy prawa karnego. Pojęcie przestępstwa wywodzi się od określenia z prawa rzymskiego – łac. *crimen* (stąd ang. i fr. *crime*, wł. *crimine*, hiszp. *crimen*, duń. *kriminalitet*), które jest zbliżone znaczeniowo do łac. *delicta* (delikt – przestępstwo, przewinienie) i powszechnie w języku prawniczym oznacza przestępstwo prawa publicznego, inaczej czyn zabroniony w prawie karnym. Polski Kodeks karny z 1997 r. nie zawiera definicji przestępstwa, ale można ją skonstruować na podstawie następujących przepisów części ogólnej: art. 1, 2, 7 i 9.

– Artykuł 1 §1. Odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia.

§2. Nie stanowi przestępstwa czyn zabroniony, którego społeczna szkodliwość jest znikoma.

§3. Nie popełnia przestępstwa sprawca czynu zabronionego, jeżeli nie można mu przypisać winy w czasie czynu.

– Artykuł 2. Odpowiedzialności karnej za przestępstwo skutkowe popełnione przez zaniechanie podlega ten tylko, na kim ciążył prawny, szczególny obowiązek zapobiegnięcia skutkowi.
– Artykuł 7 §1. Przestępstwo jest zbrodnią albo występkiem.

§2. Zbrodnią jest czyn zabroniony zagrożony karą pozbawienia wolności na czas nie krótszy od lat 3 albo karą surowszą.

§3. Występkiem jest czyn zabroniony zagrożony grzywną powyżej 30 stawek dziennych albo powyżej 5 tys. zł, karą ograniczenia wolności przekraczającą miesiąc albo karą pozbawienia wolności przekraczającą miesiąc.

– Artykuł 9 §1. Czyn zabroniony popełniony jest umyślnie, jeżeli sprawca ma zamiar jego popełnienia, to jest chce go popełnić albo przewidując możliwość jego popełnienia, na to się godzi.

§2. Czyn zabroniony popełniony jest nieumyślnie, jeżeli sprawca nie mając zamiaru jego popełnienia, popełnia go jednak na skutek niezachowania ostrożności wymaganej w danych okolicznościach, mimo że możliwość popełnienia tego czynu przewidywał albo mógł przewidzieć.

§3. Sprawca ponosi surowszą odpowiedzialność, którą ustawa uzależnia od określonego następstwa czynu zabronionego, jeżeli następstwo to przewidywał albo mógł przewidzieć.

Na tej podstawie definicję przestępstwa można sformułować następująco, obejmuje czyn, który:

– jest zabroniony pod groźbą kary przez obowiązującą w czasie jego popełnienia ustawę;
– jest zawiniony;
– jest szkodliwy społecznie w stopniu większym niż znikomy.

Wszystkie wymienione elementy muszą wystąpić łącznie, aby czyn został uznany za przestępstwo. Jest to zatem czyn zabroniony pod groźbą kary jako zbrodnia albo występek, przez ustawę obowiązującą w czasie jego popełnienia, bezprawny, zawiniony i społecznie szkodliwy w stopniu wyższym niż znikomy.

Przedstawiona definicja przestępstwa opiera się na 2 odmiennych ujęciach teoretycznych, z których każde akcentuje inny aspekt analizowanego zjawiska. Pierwsze z nich, określane jako definicja materialna, koncentruje się przede wszystkim na społecznej szkodliwości czynu, traktując naruszenie norm prawnych jako element wtórny. W myśl tego ujęcia przestępstwo stanowi czyn człowieka, który jest społecznie niebezpieczny, bezprawny, karalny oraz zawiniony. Drugie ujęcie, określane mianem definicji formalnej, za podstawowe kryterium uznaje wyłącznie relację czynu do obowiązujących przepisów prawa karnego, niezależnie od jego charakteru czy znaczenia społecznego. Zgodnie z tym podejściem przestępstwem jest czyn człowieka zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia.

Analiza przestępstwa wymaga zatem uwzględnienia kilku istotnych elementów składowych:

- czyn człowieka, stanowi podstawowy element struktury przestępstwa, obejmując zarówno działanie, jak i zaniechanie, które można przypisać sprawcy. Zgodnie z art. 115 §1 Kodeksu karnego czynem zabronionym jest zachowanie o znamionach określonych w ustawie karnej. Oznacza to, że dopiero czyn spełniający ustawowe kryteria przestępstwa może zostać oceniony jako czyn zabroniony i pociągać odpowiedzialność karną;
- bezprawność, czyn bezprawny narusza normę prawa karnego i jest zabroniony przepisem pod groźbą określonej kary. Bezprawność jest jednym z ważnych elementów definicji przestępstwa, a jej istnienie jest warunkiem przypisania karalności czynu. W sensie prawnym oznacza to naruszenie zakazu lub nakazu wynikającego z przepisów prawa karnego, przy braku okoliczności wyłączających odpowiedzialność;
- wina, przestępstwem może być wyłącznie czyn zawiniony. Zgodnie z art. 1 §3 Kodeksu karnego nie popełnia przestępstwa sprawca czynu zabronionego, jeżeli nie można mu przypisać winy w czasie jego popełnienia. Oznacza to, że przypisanie winy stanowi niezbędny warunek odpowiedzialności karnej. Wina w prawie karnym materialnym rozumiana jest jako indywidualny zarzut popełnienia czynu zabronionego, który można postawić sprawcy. Granice tego zarzutu wyznacza ustawa, określając zarówno przesłanki przypisania winy, jak i okoliczności ją wyłączające. W odróżnieniu od pozostałych elementów struktury przestępstwa wina ma charakter subiektywny, gdyż jest ściśle związana z psychiką sprawcy. Wyraża ona stopień oraz charakter psychicznego zaangażowania sprawcy w dokonany czyn, w szczególności jego stosunek do czynu zarówno przed jego popełnieniem, jak i w trakcie realizacji zachowania zabronionego. W zależności od tego, w jaki sposób sprawca odnosi się do popełnianego czynu, wina przybiera różne formy, wyróżnia się bowiem umyślną oraz nieumyślną, które determinują zakres odpowiedzialności karnej;
- społeczna szkodliwość czynu, stanowi jeden z podstawowych elementów definicji przestępstwa i odnosi się do stopnia

naruszenia lub zagrożenia dóbr prawnych chronionych przez prawo karne. Zgodnie z art. 115 §2 Kodeksu karnego przy ocenie stopnia społecznej szkodliwości czynu sąd uwzględnia w szczególności rodzaj i charakter naruszonego lub zagrożonego dobra, rozmiary wyrządzonej lub grożącej szkody, a także sposób i okoliczności popełnienia czynu. Ponadto, ocenie podlegają również waga naruszonych przez sprawcę obowiązków, postać zamiaru, motywacja sprawcy, a także rodzaj naruszonych reguł ostrożności oraz stopień ich naruszenia. Uwzględnienie tych kryteriów pozwala na kompleksową ocenę rzeczywistej doniosłości czynu z punktu widzenia interesu społecznego. W prawie karnym przyjmuje się, że czyn może zostać uznany za przestępstwo wyłącznie wówczas, gdy jego społeczna szkodliwość nie jest znikoma, co umożliwia odróżnienie przestępstw od zachowań formalnie bezprawnych, lecz pozbawionych istotnego znaczenia społecznego. Społeczna szkodliwość pełni tym samym funkcję materialnego wyznacznika odpowiedzialności karnej.

Przestępstwo jest czynem zabronionym przez ustawę karną, odpowiadającym opisowi ustawowemu określonego typu przestępstwa. Opis ten zawiera ustawowe znamiona przestępstwa, czyli cechy zdarzenia określone w ustawie, odnoszące się do zachowania sprawcy, jego skutku, okoliczności czynu oraz osoby sprawcy. Znamiona te mają charakter obiektywnie sprawdzalny i podlegają udowodnieniu w postępowaniu karnym, pełniąc funkcję gwarancyjną przed dowolnością w ściganiu i karaniu. Warunkiem przypisania sprawcy odpowiedzialności karnej jest stwierdzenie realizacji wszystkich ustawowych znamion danego typu przestępstwa, obejmujących:

- przedmiot przestępstwa;
- stronę przedmiotową przestępstwa;
- podmiot przestępstwa;
- stronę podmiotową przestępstwa.

Przedmiot przestępstwa stanowią dobra prawne chronione przez prawo karne, takie jak życie, zdrowie, wolność czy bezpieczeństwo, na które skierowany jest czyn zabroniony. Z perspektywy przestępstwa dobra

te określa się jako przedmiot zamachu, natomiast z perspektywy normy prawnokarnej – przedmiot ochrony. W ujęciu dogmatycznym wyróżnia się przedmiot ogólny, obejmujący całokształt dóbr prawnych chronionych przez prawo karne, przedmiot rodzajowy, obejmujący grupę jednorodnych dóbr chronionych przez określony zespół przepisów, oraz przedmiot bezpośredni, będący konkretnym dobrem prawnym naruszonym lub zagrożonym czynem określonego typu.

Strona przedmiotowa przestępstwa obejmuje zewnętrzne elementy czynu zabronionego. Jej podstawowym składnikiem jest zachowanie sprawcy przybierające postać działania rozumianego jako zespół czynności podjętych w określonym celu, lub zaniechania polegającego na powstrzymaniu się od działania, które sprawca mógł i powinien podjąć. Do strony przedmiotowej zalicza się również skutek w postaci zmian w świecie zewnętrznym, będących następstwem czynu, a także przedmiot czynności wykonawczej, na którym realizowane jest przestępstwo. Ponadto obejmuje ona znamiona okoliczności czynu, w szczególności czas, miejsce i sytuację jego popełnienia, które w niektórych typach przestępstw podlegają szczególnemu ustawowemu określeniu.

Podmiotem przestępstwa jest osoba fizyczna indywidualnie określona, która ponosi odpowiedzialność karną za popełnienie czynu zabronionego po ukończeniu 17 roku życia, zgodnie z art. 10 §1 Kodeksu karnego, przy czym granica ta może zostać obniżona w przypadkach określonych w art. 10 §2 Kodeksu karnego. Warunkiem uznania osoby za podmiot przestępstwa jest jej poczytalność, rozumiana jako zdolność do rozpoznania znaczenia czynu i pokierowania swoim postępowaniem w chwili jego popełnienia. W odniesieniu do niektórych typów przestępstw podmiotem może być wyłącznie osoba posiadająca szczególne cechy lub właściwości określone w ustawie, co uzasadnia wyróżnienie przestępstw indywidualnych.

Strona podmiotowa przestępstwa obejmuje psychiczny stosunek sprawcy do popełnionego czynu zabronionego oraz jego skutku. Wyraża się ona w winie, przybierającej postać umyślności albo nieumyślności. Przestępstwo jest popełnione umyślnie, gdy sprawca ma zamiar jego popełnienia, to jest – chce go popełnić albo przewidując możliwość jego popełnienia, na to się godzi. Przestępstwo jest popełnione nieumyślnie,

gdy sprawca nie mając zamiaru jego popełnienia, popełnia je na skutek niezachowania wymaganej ostrożności, mimo że możliwość popełnienia czynu przewidywał albo mógł przewidzieć. Do strony podmiotowej zalicza się również motywy i pobudki działania sprawcy, cel jego zachowania oraz możliwość przypisania winy w sensie prawnokarnym.

Prawo karne wyróżnia formy zjawiskowe przestępstwa, które określają różne sposoby współdziałania osób przy popełnieniu czynu zabronionego. Formy te obejmują sytuacje, w których sprawca swoim zachowaniem w pełni realizuje ustawowe znamiona przestępstwa. Do form zjawiskowych przestępstwa zalicza się:

- współsprawstwo;
- sprawstwo kierownicze;
- podżeganie;
- pomocnictwo.

Sprawca przestępstwa to osoba fizyczna, która swoim zachowaniem w pełni realizuje ustawowe znamiona czynu zabronionego. Wyróżnia się sprawstwo indywidualne, gdy czyn popełniany jest samodzielnie, oraz współsprawstwo, gdy co najmniej 2 osoby działają wspólnie i w porozumieniu, zarówno przed, jak i w trakcie popełnienia czynu.

Sprawstwo kierownicze polega na kierowaniu wykonaniem czynu przez inną osobę lub wykorzystywaniu jej zależności, obejmując decyzję o popełnieniu czynu, prowadzenie jego wykonania, wprowadzanie zmian lub przerwanie.

Podżeganie polega na nakłanianiu innej osoby do popełnienia czynu zabronionego, niezależnie od formy zachowania, natomiast pomocnictwo obejmuje ułatwianie dokonania czynu przez dostarczenie narzędzi, udzielenie rady lub innych środków wspierających jego realizację, przy czym katalog form pomocnictwa nie jest zamknięty.

Czyn przestępczy jest procesem składającym się z kilku kolejnych stadiów:

- przygotowania;
- usiłowania;
- dokonania.

Przygotowanie polega na podejmowaniu czynności zmierzających do stworzenia warunków umożliwiających popełnienie czynu zabronionego,

poprzedzających jego realizację, przy czym sam zamiar popełnienia przestępstwa nie stanowi czynu karalnego. Przygotowanie jest karalne tylko wtedy, gdy ustawa tak stanowi, określa to art. 16 Kodeksu karnego.

Usiłowanie zgodnie z art. 13 §1 Kodeksu karnego występuje, gdy sprawca w zamiarze popełnienia czynu zabronionego działa lub zaniechuje w sposób bezpośrednio zmierzający do jego dokonania, które jednak nie następuje. W usiłowaniu wyróżnia się: zamiar popełnienia czynu, zachowanie zmierzające bezpośrednio ku dokonaniu oraz brak jego faktycznego dokonania. Wyróżnia się usiłowanie udolne i nieudolne.

Dokonanie zachodzi, gdy sprawca swoim działaniem w pełni wyczerpuje ustawowe znamiona przestępstwa.

W literaturze prawniczej wyróżnia się podziały przestępstw, które zależą od przyjętych kryteriów ze względu na:

- wysokość grożącej kary – przestępstwa dzielą się na zbrodnie i występki;
- skutek czynu – przestępstwa materialne, gdy wymaga się wystąpienia określonego skutku, oraz formalne, gdy sam czyn jest zabroniony niezależnie od skutku;
- rodzaj winy sprawcy – przestępstwa umyślne i nieumyślne;
- sposób zachowania sprawcy – przestępstwa popełnione poprzez działanie lub zaniechanie;
- stopień społecznej szkodliwości lub cechy czynu – przestępstwa zasadnicze, kwalifikowane i uprzywilejowane;
- tryb ścigania – przestępstwa ścigane z urzędu oraz z oskarżenia prywatnego;
- rodzaj dóbr chronionych – przestępstwa polityczne i pospolite.

Prawo karne wyróżnia niektóre przestępstwa ze względu na ich szczególny charakter, co wymaga odrębnej analizy w kontekście podmiotowym, przedmiotowym i skutkowym. Do grupy tych przestępstw należą m.in.

- przestępstwa podobne;
- przestępstwa o charakterze terrorystycznym;
- występki o charakterze chuligańskim.

Przestępstwa podobne określone w art. 115 §3 Kodeksu karnego to czyny zabronione należące do tego samego rodzaju, popełnione z użyciem przemocy lub groźby jej użycia, albo w celu osiągnięcia

korzyści majątkowej. Kryterium podobieństwa pozwala na ich grupowanie w orzecznictwie i analizie doktrynalnej oraz ułatwia ocenę społecznej szkodliwości czynu.

Przestępstwo o charakterze terrorystycznym zdefiniowane w art. 115 §20 Kodeksu karnego jest czynem zabronionym zagrożonym karą pozbawienia wolności co najmniej 5 lat, popełnionym w celu poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej RP lub innego państwa bądź organu organizacji międzynarodowej do podjęcia lub zaniechania określonych działań, wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej. Obejmuje to także groźbę popełnienia takiego czynu.

Występek o charakterze chuligańskim wymieniony w art. 115 §21 Kodeksu karnego polega na umyślnym zamachu na dobra prawne, takie jak zdrowie, wolność, cześć, nietykalność cielesną, bezpieczeństwo powszechne, działalność instytucji państwowych lub samorządowych, porządek publiczny, a także na umyślnym niszczeniu, uszkodzeniu lub czynieniu niezdatną do użytku cudzej rzeczy, jeżeli sprawca działa publicznie, bez powodu lub z oczywiście błahego powodu, okazując rażące lekceważenie porządku prawnego.

Część szczególna Kodeksu karnego określa konkretne typy przestępstw oraz przewidziane dla nich sankcje. W odróżnieniu od części ogólnej, która normuje zasady odpowiedzialności karnej, pojęcia przestępstwa, winy, sprawstwa i kar, część szczególna precyzuje czyny zabronione i chronione, które składają się z następujących rodzajów przestępstw przeciwko:

- pokojowi, ludzkości oraz przestępstwa wojenne;
- Rzeczypospolitej Polskiej;
- obronności;
- życiu i zdrowiu;
- bezpieczeństwu powszechnemu;
- bezpieczeństwu w komunikacji;
- środowisku;
- wolności;
- wolności sumienia i wyznania;
- wolności seksualnej i obyczajności;

- rodzinie i opiece;
- czci i nietykalności cielesnej;
- prawom osób wykonujących pracę zarobkową;
- działalności instytucji państwowych oraz samorządu terytorialnego;
- wymiarowi sprawiedliwości;
- wyborom i referendum;
- porządkowi publicznemu;
- ochronie informacji;
- wiarygodności dokumentów;
- mieniu;
- obrotowi gospodarczemu i interesom majątkowym w obrocie cywilnoprawnym;
- obrotowi pieniędzmi i papierami wartościowymi.

Oprócz przestępstw uregulowanych w części szczególnej Kodeksu karnego w polskim systemie prawnym występują też pozakodeksowe, stypizowane w przepisach ustaw szczególnych. Chronią one dobra prawne, które ze względu na swój specyficzny charakter wymagają odrębnej regulacji. Do przestępstw pozakodeksowych zalicza się w szczególności skarbowe i podatkowe, związane z narkomanią i środkami odurzającymi, dotyczące broni, amunicji oraz materiałów wybuchowych, przeciwko ochronie środowiska, bezpieczeństwu w komunikacji, działalności gospodarczej i interesom konsumentów, prawom autorskim i prawom pokrewnym, ochronie zdrowia i bezpieczeństwu publicznemu, ochronie danych oraz cyberbezpieczeństwu, przestępstwa związane z mediami i środkami masowego przekazu, przeciwko bezpieczeństwu państwa i porządkowi publicznemu.

Dariusz Hybś

Z. Borowicz, *Ochrona osób i mienia. Podręcznik dla techników ochrony fizycznej osób i mienia oraz innych kwalifikowanych pracowników ochrony*, Wydawnictwo Dom Organizatora, Toruń 2018; A. Czop, *Przestępczość*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; L. Gardocki, *Pojęcie przestępstwa i podziały przestępstw w polskim prawie karnym*, „Annales Universitatis Mariae Curie-Skłodowska Sectio G" 2013, t. 60,

nr 2; J. Giezek, N. Kłaczyńska, G. Łabuda, *Kodeks karny. Część ogólna. Komentarz*, Wydawnictwo Wolters Kluwer, Warszawa 2007; B. Hołyst, *Zagrożenia ładu społecznego*, Wydawnictwo Naukowe PWN, Warszawa 2013; J. Jerzewska, *Elementy prawa. Podręcznik z ćwiczeniami*, Wydawnictwo Wolters Kluwer Polska SA, Warszawa 2017; A. Marek, V. Konarska-Wrzosek, *Prawo karne*, Wydawnictwo C.H. Beck, Warszawa 2016; A. Rycaj-Pilipczuk, *Wybrane przestępstwa z części szczególnej Kodeksu karnego – przestępstwa przeciwko mieniu*, „Przegląd Policyjny" 2022, t. 147, nr 3; R.A. Stefański, *Kodeks karny. Komentarz*, Wydawnictwo C.H. Beck, Warszawa 2025; Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. 2025, poz. 383, 1818 z późn. zm.

Q

QUASIPAŃSTWO, państwo nieuznawane (parapaństwo) – forma zorganizowanej władzy politycznej funkcjonująca na wydzielonym terytorium i sprawująca nad nim efektywną kontrolę administracyjną, wojskową i społeczną, lecz pozbawiona powszechnego lub pełnego uznania międzynarodowego. Zjawisko quasipaństwowości lokuje się pomiędzy klasycznym modelem państwa a strukturami niepaństwowymi: z jednej strony, obejmuje ono podmioty posiadające rozwinięte instytucje władzy, aparat bezpieczeństwa, system prawa, mechanizmy kontroli terytorium i elementy tożsamości zbiorowej. Z drugiej – jego byt międzynarodowy pozostaje ograniczony, kwestionowany lub całkowicie negowany przez społeczność międzynarodową oraz państwo macierzyste. Quasipaństwa spełniają część standardowych kryteriów państwowości, szczególnie tych wyrażonych w Konwencji z Montevideo z 1933 r., która wskazuje na konieczność posiadania ludności, terytorium, aparatu władzy oraz zdolności do wchodzenia w relacje międzynarodowe. W przypadku parapaństw kryteria te występują w sposób niejednorodny: zwykle dysponują ludnością, realnie kontrolowanym obszarem i władzą wykonawczą, natomiast

brak im zdolności do prowadzenia oficjalnych stosunków zewnętrznych ze względu na odmowę uznania przez inne państwa.

Geneza quasipaństw związana jest najczęściej z kryzysami państwowości, erozją suwerenności oraz konfliktami etnopolitycznymi prowadzącymi do zerwania więzi między centrum państwa a peryferiami. Quasipaństwa mogą powstawać zarówno w wyniku długotrwałych procesów dezintegracyjnych, jak i gwałtownych wydarzeń politycznych, takich jak secesja zbrojna, rozpad struktur bezpieczeństwa, interwencja zewnętrzna lub wojna domowa. Charakterystycznym elementem ich powstawania jest osłabienie lub faktyczny upadek państwa macierzystego na danym terytorium, co tworzy „próżnię władzy", umożliwiając lokalnym elitom wyłonienie alternatywnego ośrodka rządzenia. W literaturze proces ten określa się jako „konkurencyjną budowę instytucji", ponieważ nowo powstałe struktury parapaństwowe zaczynają pełnić funkcje dotychczas zastrzeżone dla centralnej administracji państwowej, m.in. poboru podatków, egzekwowania prawa, świadczenia usług publicznych oraz organizacji sił bezpieczeństwa. Częstym czynnikiem sprzyjającym utrwaleniu quasipaństwa jest wsparcie polityczne, militarne lub finansowe ze strony państwa patronackiego, które dostrzega w powstałym podmiocie instrument wpływu oraz środek destabilizacji państwa macierzystego.

Istotnym aspektem quasipaństwowości jest jej trwałość. Choć wiele parapaństw powstaje w wyniku konfliktów zbrojnych o ograniczonym zasięgu, część z nich ulega stabilizacji, przekształcając się w struktury funkcjonujące przez lata, a nawet dekady. Terytoria takie określane są często w literaturze jako „zamrożone konflikty", ponieważ nie dochodzi ani do reintegracji z państwem macierzystym, ani do pełnej legalizacji ich statusu na arenie międzynarodowej. Tego typu sytuacja występuje np. w Naddniestrzu, Abchazji, Osetii Południowej czy Górskim Karabachu, gdzie quasipaństwa stworzyły własne instytucje władzy, lecz pozostają zależne od wsparcia zewnętrznego oraz pozbawione międzynarodowej podmiotowości. Zjawisko to wpływa na kształt regionalnej architektury bezpieczeństwa, utrwalając mechanizmy nieformalnej kontroli militarnej oraz politycznej ze strony państw patronackich, a jednocześnie ograniczając zdolność państwa macierzystego do wykonywania suwerenności w pełnym zakresie.

Quasipaństwa wykazują wysoki poziom wewnętrznego zorganizowania. W wielu z nich powstaje rozbudowany aparat biurokratyczny, administracja centralna i lokalna, organy bezpieczeństwa, sądownictwo oraz instytucje odpowiadające za edukację, opiekę zdrowotną i podstawową infrastrukturę. Mimo braku uznania międzynarodowego podmioty te potrafią wytworzyć względnie stabilne mechanizmy zarządzania, co zwiększa ich odporność na presję zewnętrzną i legitymizuje ich istnienie w oczach części mieszkańców. W wymiarze symbolicznym rozwijają one własne znaki państwowe, takie jak flagi, godła, hymny oraz budują narracje historyczne, które mają uzasadniać ich odrębność polityczną i etniczną. Tego rodzaju działania stanowią element procesu tworzenia „narodu politycznego", kluczowego dla utrzymania wewnętrznej spójności quasipaństwa.

Z perspektywy prawa międzynarodowego quasipaństwa pozostają konstrukcjami problematycznymi; nie posiadają pełnej osobowości prawnomiędzynarodowej, nie są członkami organizacji międzynarodowych, nie uczestniczą w negocjacjach dyplomatycznych w sposób formalny i nie dysponują zdolnością traktatową. W praktyce oznacza to, że ich relacje zewnętrzne ograniczają się do kontaktów nieformalnych, często prowadzonych za pośrednictwem państwa patrona lub organizacji pozarządowych. Jednocześnie ich istnienie jest zazwyczaj traktowane jako naruszenie integralności terytorialnej państwa macierzystego, co wzmacnia międzynarodową tendencję do odmowy uznania. Paradoks quasipaństw polega więc na napięciu między efektywnością rządzenia a brakiem legitymizacji prawnej: sprawują one realną kontrolę nad terytorium, lecz w świetle prawa międzynarodowego pozostają bytami nielegalnymi.

Funkcjonowanie quasipaństwa opiera się na specyficznej konfiguracji instytucjonalnej, w której formalne braki w zakresie międzynarodowej legitymizacji zastępowane są rozbudowaną efektywnością rządzenia w wymiarze wewnętrznym. Pomimo braku uznania parapaństwa tworzą struktury typowe dla państw: aparat administracyjny, siły zbrojne, policję, system sądowniczy, organy podatkowe oraz sieć instytucji usług publicznych. W wielu przypadkach ich administracja cechuje się większą przewidywalnością i stabilnością niż struktury państwa macierzystego w okresach kryzysu, co sprzyja budowaniu lokalnej akceptacji dla alternatywnego

ośrodka władzy. Wytwarzanie efektywności rządzenia jest zatem warunkiem koniecznym przetrwania quasipaństwa – bez sprawnego systemu świadczenia usług publicznych parapaństwo nie uzyskałoby minimalnego poziomu legitymizacji społecznej, który pozwala mu na utrzymanie ciągłości funkcjonowania mimo sporów o jego legalność.

Kluczową rolę w systemie quasipaństwa odgrywają siły bezpieczeństwa, stanowiące fundament jego przetrwania. W odróżnieniu od klasycznych państw, gdzie armia jest elementem stabilnego systemu instytucjonalnego, w quasipaństwach aparat siłowy ma charakter dualny. Z jednej strony, przejmuje funkcje obrony terytorium i utrzymania kontroli nad granicami, z drugiej – jest narzędziem wewnętrznej stabilizacji i gwarantem ciągłości władzy. W większości parapaństw siły zbrojne wywodzą się bezpośrednio z frakcji uczestniczących w konflikcie, co powoduje ich głęboką politizację oraz silne powiązanie z elitami władzy. Często są one także finansowane, szkolone lub bezpośrednio wspierane sprzętowo przez państwa patronackie, co czyni je jednym z kluczowych instrumentów wpływu zewnętrznego. Struktury bezpieczeństwa quasipaństw rzadko podlegają pełnej cywilnej kontroli, a ich funkcjonowanie opiera się na logice militaryzacji życia społecznego, w którym aparat przymusu staje się centralnym elementem zarówno w kontekście stabilizacji wewnętrznej, jak i utrzymania *status quo* w relacjach z państwem macierzystym.

Niejednokrotnie z gospodarką quasipaństw wiąże się zjawisko tak zwanej „ekonomii konfliktowej" polegającej na powiązaniu lokalnych systemów ekonomicznych z warunkami długotrwałej niestabilności politycznej. Brak uznania międzynarodowego uniemożliwia im pełnoprawny udział w światowych rynkach finansowych, transakcjach bankowych czy oficjalnych wymianach handlowych, co prowadzi do powstania nieformalnych i półlegalnych kanałów gospodarczych. W praktyce gospodarka parapaństw opiera się na mieszance legalnych, nieformalnych i niekiedy przestępczych źródeł dochodów. Przykładowo w Naddniestrzu funkcjonuje rozbudowany przemysł ciężki oraz infrastruktura energetyczna, ale jednocześnie znaczną część obrotu gospodarczego stanowią alternatywne przepływy towarowe, niepodlegające pełnej kontroli celnej państwa macierzystego. W Abchazji i Osetii Południowej istotną rolę odgrywa gospodarka pomocowa, silnie powiązana z transferami z Federacji Rosyjskiej.

W Górskim Karabachu (do 2020) kluczowe znaczenie miały subsydia i transfery finansowe z diaspory ormiańskiej. Model gospodarki quasipaństwa jest więc konsekwencją jego politycznego osadzenia, czyli im silniejsza zależność od państwa patronackiego, tym większy udział gospodarki pomocowej i mniejszy potencjał samodzielnego rozwoju.

W sferze społeczno-politycznej quasipaństwa prowadzą aktywną politykę budowania tożsamości zbiorowej, ponieważ stabilność ich istnienia zależy od zdolności przekonania mieszkańców o zasadności separacji od państwa macierzystego. Proces ten obejmuje zarówno wcześniej wspomniane tworzenie nowych symboli, jak i reinterpretację wydarzeń historycznych, które mają uzasadniać polityczną odrębność wspólnoty. Władze quasipaństw promują narracje odnoszące się do walki o niepodległość, obrony przed zewnętrzną agresją lub rzekomego prawa do samostanowienia, co umożliwia im budowanie poczucia wspólnoty politycznej, mimo ograniczeń strukturalnych. Kształtowanie tożsamości odbywa się również poprzez system edukacji, media lokalne czy ceremonie państwowe, które utrwalają poczucie „normalności" istnienia quasipaństwa. W Naddniestrzu funkcjonuje spójny system symboliki odwołujący się do dziedzictwa radzieckiego, natomiast w Abchazji i Osetii Południowej dominują narracje etnonacjonalistyczne. Choć tożsamości quasipaństw są w dużej mierze projektami politycznymi, ich skuteczność wynika z długoletniego oddziaływania na lokalne społeczeństwo, co prowadzi do utrwalenia nowej formy lojalności politycznej, trudnej do odwrócenia.

Istnienie quasipaństw ma bezpośredni wpływ na architekturę bezpieczeństwa regionalnego. Parapaństwa stanowią zazwyczaj węzły niestabilności, których nieuregulowany status generuje ciągłe ryzyko eskalacji, a sama ich obecność jest wykorzystywana jako narzędzie polityki państw patronackich. W regionie Kaukazu Południowego quasipaństwa utrwalają rywalizację między Rosją a Gruzją oraz Armenią i Azerbejdżanem. W Naddniestrzu ich istnienie jest bezpośrednio związane z utrzymywaniem wpływów rosyjskich w Mołdawii i blokowaniem jej pełnej integracji euroatlantyckiej. Status quasipaństw zakłóca również funkcjonowanie organizacji międzynarodowych, które w praktyce muszą prowadzić działania na rzecz stabilizacji, nie mogąc jednocześnie oficjalnie uznać żadnej ze stron za legalny podmiot państwowy. Parapaństwa pełnią w tym sensie

rolę swego rodzaju szarej strefy bezpieczeństwa, w której reguły prawa międzynarodowego nie działają w pełni, a instrumenty polityki międzynarodowej napotykają ograniczenia wynikające z braku jednolitego podmiotu odpowiedzialnego za sytuację na terytorium.

Funkcjonowanie quasipaństwa jest także związane z problemem odpowiedzialności międzynarodowej. Ponieważ parapaństwo nie jest uznanym podmiotem prawa międzynarodowego, trudno pociągnąć je do odpowiedzialności za naruszenia praw człowieka, przestępstwa międzynarodowe czy działania sprzeczne z konwencjami międzynarodowymi. Odpowiedzialność tę często przenosi się na państwo patronackie, jeśli to ono sprawuje decydujący wpływ na funkcjonowanie quasipaństwa. Jednocześnie państwo macierzyste nie jest w stanie wykonywać swojej suwerenności na okupowanym lub kontrolowanym przez separatystów terytorium, co prowadzi do sytuacji prawnego zawieszenia. Powstaje wówczas stan długotrwałego naruszenia integralności terytorialnej, który nie ma jednoznacznych instrumentów egzekwowania w ramach współczesnego systemu międzynarodowego.

Relacje quasipaństw z państwami patronackimi stanowią jeden z najbardziej charakterystycznych elementów ich funkcjonowania. Bez wsparcia zewnętrznego nie są one w stanie utrzymać stabilności gospodarczej, militarnej ani politycznej. Państwo patronackie dostarcza im zasobów strategicznych, takich jak ochrona militarna, pomoc finansowa, energia, sprzęt wojskowy, szkolenie kadr administracyjnych i bezpieczeństwa, a często także zapewnia im polityczne parasole ochronne na forach międzynarodowych. W przypadku Naddniestrza, Abchazji i Osetii Południowej funkcję tę pełni Federacja Rosyjska, która wykorzystuje quasipaństwa jako narzędzie projekcji wpływów na obszarze poradzieckim oraz mechanizm blokowania procesów integracji euroatlantyckiej państw regionu. Relacja ta ma charakter asymetryczny i choć parapaństwo zachowuje pozory autonomii, to kluczowe decyzje strategiczne uzależnione są od interesów i priorytetów państwa patronackiego. Zależność ta nie jest jedynie polityczna, ponieważ obejmuje także instytucjonalne powiązania, takie jak udział rosyjskich funkcjonariuszy w strukturach administracyjnych quasipaństw, integrację systemów prawnych czy stosowanie rosyjskich walut i standardów gospodarczych. W rezultacie quasipaństwo staje się

przestrzenią, w której interesy lokalnych elit i państwa patronackiego ulegają fuzji, a to utrudnia realizację procesów pokojowych i uniemożliwia powrót regionu pod efektywną jurysdykcję państwa macierzystego.

Specyfika relacji quasipaństw ze społecznością międzynarodową jest zdeterminowana ich statusem nieuznawanych podmiotów. Formalnie nie są one uczestnikami stosunków międzynarodowych, choć w praktyce wchodzą w nie poprzez kanały nieoficjalne, półformalne lub za pośrednictwem państwa patronackiego. Organizacje międzynarodowe, takie jak ONZ, OBWE czy Unia Europejska, nie mogą uznać ich podmiotowości, ale jednocześnie zmuszone są do podejmowania działań na rzecz stabilizacji, monitorowania sytuacji bezpieczeństwa, prowadzenia dialogu z lokalnymi władzami lub implementacji programów pomocowych. W ten sposób quasipaństwa stają się uczestnikami miękkiej dyplomacji, czyli nieformalnych spotkań, konsultacji roboczych czy inicjatyw humanitarnych, mimo że nie przysługuje im status strony traktatowej. Konsekwencją takiego stanu jest niepełna inkluzja quasipaństw w struktury międzynarodowe, przy jednoczesnym faktycznym uczestniczeniu w procesach negocjacyjnych dotyczących bezpieczeństwa i zarządzania konfliktem. Z perspektywy państw macierzystych prowadzi to do dylematu: angażowanie się w dialog z władzami quasipaństw może być postrzegane jako ich legitymizacja, jednak brak dialogu grozi eskalacją konfliktu i pogorszeniem sytuacji humanitarnej.

Jednym z kluczowych aspektów funkcjonowania quasipaństw jest ich wpływ na dynamikę bezpieczeństwa międzynarodowego. Parapaństwa stanowią punkty zapalne, wokół których skupia się strategiczna rywalizacja mocarstw. Ich status sprzyja militaryzacji regionów, a obecność nieuregulowanego konfliktu tworzy warunki do utrzymywania długotrwałego napięcia. Quasipaństwa mogą być również wykorzystywane jako obszary prowadzenia operacji wywiadowczych, strefy przerzutu nielegalnych towarów czy przestrzenie umożliwiające państwom patronackim testowanie taktyk hybrydowych. Ich istnienie utrwala konflikty o zamrożonym charakterze, które choć nie prowadzą do pełnoskalowych działań wojennych, to generują ryzyko incydentalnej eskalacji, stanowią instrument nacisku politycznego oraz osłabiają funkcjonalność całych regionów. Z perspektywy prawa międzynarodowego quasipaństwa stają

się obszarami wyłączonymi spod skutecznego egzekwowania norm, co sprzyja naruszeniom praw człowieka, osłabia przejrzystość działań administracyjnych oraz utrudnia monitorowanie działalności sił zbrojnych i grup paramilitarnych. Brak jasnej odpowiedzialności międzynarodowej pogłębia ten problem, umożliwiając zarówno quasipaństwom, jak i ich patronom operowanie w strefie strategicznej niejednoznaczności.

Procesy transformacji quasipaństw są nierozerwalnie związane z szerszym kontekstem geopolitycznym. W literaturze przedmiotu wyróżnia się kilka możliwych scenariuszy ich przyszłości, takich jak reintegracja z państwem macierzystym, utrwalenie quasipaństwowości i dalsza stabilizacja struktur wewnętrznych, stopniowa integracja z państwem patronackim (często w formie pełzającej aneksji) lub uzyskanie międzynarodowego uznania. Ten ostatni scenariusz jest najbardziej odległy i teoretyczny, ponieważ quasipaństwa rzadko spełniają warunki określone w Montevideo, a społeczność międzynarodowa konsekwentnie odrzuca próby ich jednostronnej legitymizacji. Reintegracja jest z kolei uzależniona od zdolności państwa macierzystego do zapewnienia bezpieczeństwa i odbudowy struktur na terenach zajętych, co bywa utrudnione przez długotrwałą obecność wojsk państwa patronackiego lub zakorzenienie lokalnych elit w strukturach quasipaństwowych. Niemniej, najbardziej prawdopodobnym scenariuszem w perspektywie średnioterminowej jest zatem dalsze trwanie quasipaństw w formie niepełnej podmiotowości międzynarodowej, przy funkcjonalnej zależności od państw patronackich i jednoczesnym stopniowym rozwoju instytucjonalnym.

W ujęciu syntetycznym quasipaństwo należy rozumieć jako twór polityczny znajdujący się na pograniczu legalności i efektywności, w którym nominalny brak podmiotowości międzynarodowej współistnieje z realnym sprawowaniem władzy nad terytorium i ludnością. To specyficzna hybryda struktur politycznych, zbyt rozwinięta, by nazwać ją jedynie separatystycznym ruchem zbrojnym, lecz niewystarczająco legitymizowana, by uznać ją za pełnoprawne państwo. Fenomen quasipaństwowości wynika zarówno z kryzysów wewnętrznych państw macierzystych, jak i geopolitycznych strategii państw zewnętrznych, które wykorzystują parapaństwa jako narzędzie realizacji własnych interesów. Quasipaństwa stanowią zatem nie tylko odrębny problem badawczy na gruncie nauk o bezpieczeństwie, ale

również ważny element współczesnej architektury międzynarodowej, której stabilność zależy od zdolności do zarządzania konfliktami, w których formalne normy prawne rozmijają się z praktyką polityczną.

Jarosław Indyk

L. Antonowicz, *Podręcznik prawa międzynarodowego*, LexisNexis, Warszawa 2011; M. Balcerzak, R. Bierzanek, M. Kałduński, J. Symonides, *Prawo międzynarodowe publiczne*, Wolters Kluwer Polska, Warszawa 2023; L. Broers, *Armenia and Azerbaijan: Anatomy of a Rivalry*, Edinburgh University Press, Edinburgh 2019; N. Caspersen, *Unrecognized States: The Struggle for Sovereignty in the Modern International System*, Polity Press, Cambridge 2011; A. Florea, *De Facto States in International Politics (1945–2011): A New Dataset*, „*International Studies Quarterly*" 2014, vol. 40, no. 4; S.D. Krasner, *Sovereignty: Organized Hypocrisy*, Princeton University Press, Princeton 1999; J. Łysek, *Fenomen quasi-państwowości. Analiza porównawcza para-państw na obszarze byłego ZSRR*, [w:] *(R)ewolucje w przestrzeni postradzieckiej*, J. Biniewska, A. Majewska (red.), Wydawnictwo Agata Majewska, Kraków 2015; S. Pegg, *International Society and the De Facto State*, Routledge, London 2019; J. Raubo, *Państwa upadłe jako czynnik destabilizujący bezpieczeństwo międzynarodowe*, [w:] *Świat współczesny. Wyzwania, zagrożenia i współzależności*, W. Malendowski (red.), INPiD UAM, Poznań 2008; W. Reno, *When States Fail: Causes and Consequences*, Princeton University Press, Princeton 2004; B. Stanisławski, *Para-States, Quasi-States, and Black Spots: Perhaps Not States, But Not "Ungoverned Territories"*, „*International Studies Review*" 2008, vol. 10, no. 2; P. Szeląg, *The "limited recognition" problem and the international presence of the Republic of Kosovo*, „Balcania Posnaniensia. Acta et Studia" 2024, vol. 31.

R

RESTYTUCJA wywodzi się ze starożytności i odnosi się do prawa rzymskiego *restitutio ad integrum* oznaczającego przywrócenie stanu sprzed popełnienia czynu zabronionego oraz zwrot rzeczy nabytych w tym czasie od ich prawowitego właściciela. W czasach współczesnych „restytucja" wiąże się z obowiązkiem naprawienia szkody wyrządzonej przez jedno państwo innemu. Odbywa się to najczęściej poprzez zwrot zrabowanych dóbr ich prawowitym właścicielom.

Jak zauważa Adam Szpunar, „istota restytucji polega na fizycznym powrocie dobra do właściciela, co stanowi najpełniejszą formę naprawienia szkody". Służyła ona ochronie osób poszkodowanych wskutek oszustwa, przemocy lub niekorzystnych umów. W średniowieczu restytucja miała wymiar nie tylko prawny, lecz także moralny i religijny – zwrot rzeczy był wymagany jako warunek pokuty.

Celem restytucji jest zawsze to, żeby poszkodowany odzyskał to, co utracił, albo żeby sytuacja wróciła do normy, jakby określona szkoda nigdy się nie wydarzyła. To jak próba cofnięcia czasu w konkretnej sprawie, choć oczywiście tylko w zakresie możliwości prawa czy natury. Najczęściej używa się tego pojęcia w kontekście prawa majątkowego i historii.

Wiele krajów, w tym Polska, miało okresy, kiedy państwo konfiskowało, czyli zabierało, prywatne majątki, np. podczas wojen, rewolucji albo przy zmianie ustroju politycznego.

W Polsce największy problem z restytucją dotyczy mienia znacjonalizowanego przez władze komunistyczne po II wojnie światowej, kiedy to tysiące domów, kamienic, gruntów, fabryk i majątków ziemskich przeszły na własność państwa bez zgody i często bez odszkodowania dla właścicieli. Restytucja mienia w tym sensie oznacza właśnie ten trudny i długotrwały proces, w którym dawni właściciele lub ich spadkobiercy starają się o to, by te zabrane nieruchomości zostały im zwrócone albo żeby otrzymali za nie sprawiedliwe odszkodowanie. Jest to proces bardzo skomplikowany, ponieważ od tych zdarzeń minęło wiele lat, a mienie wielokrotnie zmieniało właścicieli, często w dobrej wierze. Restytucja ma jednak zastosowanie nie tylko do wielkich historycznych krzywd; w prawie karnym i cywilnym jest to podstawowy mechanizm, który ma zniwelować skutki przestępstwa lub innej szkody. Jeśli np. ktoś uszkodził samochód w wyniku wypadku, to restytucja polega na jego naprawie i przywróceniu go do stanu sprzed zdarzenia. Jeśli ktoś coś ukradł, restytucja polega na fizycznym zwrocie tej rzeczy jej prawowitemu właścicielowi. Jeśli zwrot rzeczy jest niemożliwy, bo np. została zniszczona albo sprzedana, restytucja przyjmuje formę odszkodowania pieniężnego, czyli zwrotu jej pełnej wartości. Zawsze chodzi o to, by przywrócić finansową lub rzeczową równowagę, która została naruszona.

Termin ten jest wykorzystywany także w ochronie przyrody i ekologii; restytucja ekologiczna określa celowe działania prowadzące do przywrócenia gatunków roślin lub zwierząt na tereny, z których na skutek działań człowieka lub zmian środowiskowych całkowicie zniknęły. Może to być np. program hodowli i wypuszczania na wolność żubrów czy bobrów na obszarze, gdzie kiedyś żyły, ale wyginęły. Restytucja może też dotyczyć środowiska – np. rekultywacja, czyli przywrócenie naturalnego stanu zdegradowanego obszaru, takiego jak stare wysypisko śmieci czy teren po kopalni. Celem jest zachowanie równowagi w naturze.

Restytucja w polityce i społeczeństwie oznacza przywrócenie czegoś, co zostało utracone – może chodzić o mienie, instytucje, prawa, tradycje, symbole narodowe, a także utraconą tożsamość kulturową. Roger Griffin

wskazuje, że ruchy odwołujące się do restytucji często mają na celu nie tylko odbudowę materialną, ale także moralną, tworząc narrację o odzyskaniu dawnej chwały czy prawdy historycznej. Restytucja pełni zatem funkcję zarówno praktyczną, jak i symboliczną – pozwala społeczeństwom na nowo definiować swoją przeszłość i tożsamość. Współcześnie restytucja nie ogranicza się do działań prawnych, takich jak zwrot mienia czy rekompensaty, ale obejmuje również procesy kulturowe i edukacyjne. Odwołanie do przeszłości pozwala jednostkom zbudować więź z własną historią i poczucie stabilności w świecie pełnym zmian. Jak zauważa Zdzisław Krasnodębski, proces restytucji bywa odpowiedzią na poczucie niepewności społecznej i zagubienia wartości po okresach kryzysu lub transformacji politycznej.

W Europie historia restytucji jest długa i złożona. Po wojnach, rewolucjach czy zmianach granic państwowych wiele społeczeństw próbowało przywrócić utracone prawa, mienie i instytucje. W Polsce po 1918 i 1989 r. procesy restytucyjne obejmowały odbudowę instytucji państwowych, przywracanie symboli narodowych i kościelnych, a także reformę systemu edukacji i kultury. W okresie międzywojennym restytucja była również narzędziem konsolidacji narodowej – przywracano tradycje i symbole, które integrowały młode państwo po rozbiorach. Współczesna restytucja praw własności, szczególnie po 1989 r., obejmowała zwrot majątków prywatnych lub rekompensaty za mienie utracone w okresie PRL.

Jak wskazuje socjolog Anthony Giddens, takie działania mają wymiar nie tylko prawny, ale również psychologiczny – dają społeczeństwu poczucie sprawiedliwości i odtwarzają ciągłość historyczną. Restytucja obejmuje również przywracanie wartości kulturowych i edukacyjnych; może to być odbudowa zabytków, renowacja muzeów, przywracanie tradycji lokalnych, a także rewitalizacja języka i literatury narodowej. Współczesna Polska doświadcza tego m.in. poprzez kultywowanie świąt narodowych, odbudowę pomników historycznych czy programy edukacyjne przybliżające historię państwa. W Europie Zachodniej, np. we Francji czy Niemczech, restytucja często dotyczyła ochrony dziedzictwa kulturowego związanego z przeszłością kolonialną, wojenną czy migracyjną; jest ściśle powiązana z pojęciem pamięci historycznej. Przywracanie dawnych wartości i instytucji to jednocześnie interpretacja przeszłości. Jak zauważa Jan Assmann

w swoich badaniach nad pamięcią kulturową, proces restytucji kształtuje społeczne narracje – decyduje o tym, które wydarzenia, symbole i postacie są pamiętane, a które – zapomniane. W tym sensie restytucja może zarówno integrować społeczeństwo, jak i wykluczać grupy uznane za „obce" wobec oficjalnej narracji.

W Polsce współczesna restytucja obejmuje zarówno aspekty materialne (zwrot mienia po PRL), jak i symboliczne – np. odbudowę Pałacu Saskiego w Warszawie czy przywracanie nazw ulic związanych z historią narodową. W Europie Środkowo-Wschodniej restytucja często łączy się z budowaniem tożsamości narodowej po transformacji ustrojowej, natomiast w Europie Zachodniej można obserwować ją w wymiarze edukacyjnym i kulturalnym – odbudowę muzeów, ochronę dziedzictwa historycznego czy reinterpretację przeszłości kolonialnej. Restytucja może wzmacniać poczucie wspólnoty i bezpieczeństwa społecznego poprzez odtworzenie więzi historycznych i moralnych, jednak, jak zauważa Zdzisław Krasnodębski, nadmierne idealizowanie przeszłości może prowadzić do nostalgii, która ogranicza zdolność społeczeństwa do adaptacji do współczesnych wyzwań.

Społeczeństwa skoncentrowane na restytucji mogą być mniej otwarte na zmiany, bardziej podatne na polaryzację i manipulacje polityczne, a także bardziej skłonne do konfliktów z grupami, które nie wpisują się w przywracaną wizję przeszłości. Restytucja pełni więc podwójną rolę – z jednej strony, jest narzędziem odbudowy i integracji społecznej, z drugiej – może stawać się mechanizmem wykluczania i konserwacji podziałów. Restytucja posiada pewne ryzyka: pierwszym z nich są problemy z udowodnieniem prawa własności, szczególnie gdy dokumentacja historyczna jest niekompletna. Restytucje mogą wywołać napięcia międzynarodowe, szczególnie między państwami z trudną historią, co może być wykorzystywane do celów propagandowych. Nie zawsze możliwe jest również jednoznaczne ustalenie własności historycznej, gdyż może ono naruszać interes publiczny. Występują także trudności ze zwracanymi dobrami, ponieważ państwa bądź społeczności, które je otrzymują, nie zawsze mają odpowiednie warunki do ich przechowywania i ochrony, a co za tym idzie – mogą pojawić się problemy z konserwacją i udostępnianiem obiektów publiczności. Restytucja ma potencjał zarówno uzdrawiający,

jak i destrukcyjny; może wzmacniać więzi społeczne i moralne fundamenty państwa, lecz instrumentalizowana – staje się źródłem nieufności i konfliktów.

Podsumowując, restytucja to słowo-klucz oznaczające powrót do pierwotnej sprawiedliwości lub stanu, niezależnie od tego, czy mówimy o zwracaniu skradzionych obrazów, odzyskiwaniu domu po nacjonalizacji czy przywracaniu rzadkich zwierząt do ich naturalnego środowiska. Jest to zasada mówiąca, że szkoda powinna zostać usunięta, a krzywda – naprawiona, tak aby poszkodowany nie ponosił negatywnych konsekwencji niesłusznych działań.

Żanna Osikowicz

R. Griffin, *The Nature of Fascism*, Routledge, London 1991; A. Herman, *Od PKWN do własności. Restytucja mienia przejętego dekretem reformy rolnej*, Nowy Świat, Warszawa 2010; K. Kolańczyk, *Prawo rzymskie*, Wolters Kluwer, Warszawa 1997; Konwencja UNESCO w sprawie środków zmierzających do zakazu i zapobiegania nielegalnemu wywozowi, przywozowi i przenoszeniu własności dóbr kultury, Paryż, 14 listopada 1970 r., Dz.U. 1974, nr 20, poz. 106; W. Kowalski, *Restytucja dóbr kultury jako element polityki państw w stosunkach międzynarodowych*, „Santander Art and Culture Law Review" 2025, nr 1; Z. Krasnodębski, *Upadek idei postępu*, OMP, Kraków 2014; J. Pruszyński, *Dziedzictwo kultury*, Wolters Kluwer, Warszawa 2001; *Raport o stratach poniesionych przez Polskę w wyniku agresji i okupacji niemieckiej w czasie II wojny światowej 1939–1945*, Ministerstwo Spraw Zagranicznych, Warszawa 2022, https://www.gov.pl/web/re/raport (dostęp 22.01.2026); A. Szpunar, *Ustalenie odszkodowania w prawie cywilnym*, Wydawnictwa Prawnicze, Warszawa 1975; M. Wróbel, *Restytucja mienia w prawie polskim*, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2017; K. Zeidler, *Restytucja dóbr kultury ze stanowiska filozofii prawa*, Wolters Kluwer, Warszawa 2011.

REWANŻYZM – zjawisko polityczne i społeczne, które polega na dążeniu do odzyskania utraconych terytoriów, przywrócenia dawnej pozycji państwa lub narodu oraz naprawienia historycznych krzywd, które są postrzegane jako niesprawiedliwe. Dziś termin ten odnosi się zarówno do polityki państw, jak i narracji historycznej, kulturowej czy edukacyjnej. Rewanżyzm wyróżnia się tym, że nie jest tylko reakcją na wcześniejsze upokorzenia, ale także narzędziem mobilizacji społecznej i politycznej.

Jego znaczenie w historii XX w. było szczególnie widoczne w Europie, gdzie zmiany granic i militarne klęski prowadziły do długotrwałych napięć między państwami. W XIX w. idea rewanżyzmu zyskała na sile dzięki rozwojowi państw narodowych i nacjonalizmów. W tym kontekście utrata terytoriów lub klęska militarna była postrzegana jako „krzywda całego narodu", a nie tylko rządzących. Zjawisko to stało się motorem polityki zagranicznej, propagandy i edukacji, a w wielu przypadkach doprowadziło do rewizji granic oraz wybuchu konfliktów zbrojnych.

Termin *revanchisme* powstał we Francji w XIX w. i odnosił się pierwotnie do potrzeby odzyskania terytoriów utraconych na skutek klęski militarnej. Jego najbardziej znany kontekst to wojna francusko-pruska (1870–1871), po której Francja utraciła Alzację i Lotaryngię. Klęska ta wywołała w społeczeństwie francuskim poczucie głębokiej narodowej krzywdy, które szybko przerodziło się w ruch polityczny. Rewanżyzm francuski miał charakter masowy i wpłynął zarówno na politykę zagraniczną, jak i kulturę, edukację oraz literaturę. Choć Francja była pierwszym krajem, w którym termin nabrał masowego znaczenia, idee rewanżyzmu były obecne w historii dużo wcześniej. W starożytności państwa i plemiona podejmowały działania odwetowe po klęskach militarnych, jak np. Kartagina po I wojnie punickiej czy różne plemiona germańskie w obliczu ekspansji Rzymu. W średniowieczu dynastie również dążyły do odbicia utraconych ziem, ale te ruchy miały charakter elitarny z uwagi na feudalny system państw, przez co nie mobilizowały całego społeczeństwa. Nowoczesny rewanżyzm różni się tym, że jest związany z państwami narodowymi, masową edukacją, propagandą i rozwojem prasy. W XX w. narracja rewanżystyczna dotarła do całych społeczeństw, stając się częścią tożsamości narodowej. Rany historyczne, traumatyczne doświadczenia klęsk i utraty ziem były pielęgnowane w literaturze, sztuce i retoryce politycznej. W rezultacie rewanżyzm stał się ideologią, która w znacznym stopniu kształtowała politykę państw oraz przygotowywała grunt pod międzynarodowe konflikty, szczególnie w Europie XIX i XX w.

Rewanżyzm bardzo często funkcjonuje poprzez narracje dotyczące przeszłości. Państwa stosujące politykę rewanżystyczną wykorzystują pamięć historyczną jako element mobilizacji społeczeństwa i legitymizacji własnych działań. Proces ten polega na selektywnym doborze wydarzeń

historycznych, które mają potwierdzać tezę o krzywdzie narodu i nieuczciwym traktowaniu przez inne państwa lub społeczności. W ten sposób tworzy się uproszczoną wizję dziejów, w której własne społeczeństwo przedstawiane jest jako ofiara, a przeciwnicy – jako agresorzy. Oprócz tego często dochodzi do tworzenia heroicznych narracji, które podkreślają odwagę i bohaterstwo przodków walczących o utracone ziemie czy niepodległość. Tego typu narracje mogą wzmacniać poczucie dumy narodowej, ale też prowadzą do polaryzacji społecznej i stygmatyzacji grup mniejszościowych.

Rewanżyzm jest postępowaniem dążącym, jak wynika z nazwy, do rewanżu, odwetu, zwłaszcza w polityce; państwa pragną m.in. odzyskania terytoriów, wpływów lub prestiżu utraconych w wyniku przegranej wojny, niekorzystnego traktatu pokojowego lub wcześniejszych porażek politycznych. Rewanżyzm bazuje na silnym poczuciu krzywdy, chęci zemsty i przywrócenia dawnej potęgi. Często przybiera formę agresywnej polityki lub narracji, która ma wyrównać tzw. rachunki. Wynika on zwykle z poczucia zranienia bądź upokorzenia, chęci przywrócenia równowagi. Ważnym elementem polityki rewanżystycznej jest także demonizacja przeciwników – zarówno w mediach, jak i systemie edukacji.

Rafał Stobiecki oraz Andrzej Nowak podkreślają w swoich pracach, że pamięć historyczna jest podatna na manipulację, zwłaszcza gdy staje się narzędziem w rękach elit politycznych. Rewanżyzm oparty na polityce pamięci może prowadzić do erozji debaty publicznej oraz utraty zdolności do krytycznego analizowania własnej historii. Państwa, które pragną ograniczać wpływ rewanżyzmu na swoje społeczeństwa, muszą stosować szeroki zestaw narzędzi politycznych, edukacyjnych i kulturowych. Istotną rolę odgrywa edukacja historyczna, oparta na krytycznym myśleniu i weryfikacji źródeł. Uczniowie i studenci powinni mieć dostęp do różnorodnych interpretacji historycznych, co pozwoli im uniknąć uproszczeń i manipulacji.

Równie istotna jest dyplomacja kulturalna, która pozwala budować pozytywny wizerunek państwa za granicą i przeciwdziałać narracjom rewanżystycznym. W Polsce znaczenie dyplomacji publicznej zostało podkreślone w ustawie o działalności dyplomacji publicznej. Kultura narodowa, prezentowana w sposób otwarty i pluralistyczny, staje się

narzędziem dialogu, a nie konfrontacji. Dużą rolę odgrywają także akty prawne dotyczące ochrony dziedzictwa kulturowego: ustawa o ochronie zabytków podkreśla znaczenie materialnej i niematerialnej kultury dla tożsamości narodowej.

Ochrona dziedzictwa jest jednym ze sposobów przeciwdziałania narracjom, które mają na celu zawłaszczenie przeszłości lub jej reinterpretację w duchu rewanżyzmu. Wreszcie, kluczowe jest wzmacnianie odporności społeczeństwa na dezinformację. Państwa europejskie rozwijają strategie walki z manipulacją informacyjną, co jest szczególnie istotne w kontekście rosyjskich narracji rewanżystycznych. Przeciwdziałanie rewanżyzmowi wymaga zatem połączenia edukacji, prawa, kultury i polityki informacyjnej, co tworzy fundament dla stabilnego bezpieczeństwa kulturowego.

Rewanżyzm umożliwia rozliczenia wcześniejszych nadużyć władzy, przywrócenie poczucia sprawiedliwości społecznej oraz mobilizowanie społeczeństwa do naprawy błędów przeszłości, jednak jak każde z tych pojęć posiada liczne wady, ponieważ prowadzi do pogłębiania podziałów, utrwalania konfliktów politycznych, osłabienia stabilności instytucji, wykorzystywania odwetu jako narzędzia walki politycznej, paraliżu współpracy między grupami społecznymi, spadku zaufania do państwa i prawa oraz tworzenia cyklu niekończących się działań odwetowych, które zamiast naprawiać, często pogarszają funkcjonowanie państwa. Wśród wad rewanżyzmu można wymienić eskalacje konfliktu; odwet wywołuje często skutek przeciwny i może wzmocnić konflikt. Państwo nastawione na tego rodzaju działanie staje się czynnikiem destabilizującym, co przyczynia się do zwiększenia poziomu nieufności między sąsiadami oraz może wywołać wojny lokalne, a także doprowadzić do osłabienia sojuszy i izolacji międzynarodowej. Sojusznicy mogą obawiać się współpracy z państwem, które działa impulsywnie lub odwetowo, bo – kierując się emocjami – jest też bardziej podatne na manipulacje, daje się łatwo sprowokować.

Rewanżyzm prowadzi do kosztownych inwestycji militarnych, ponieważ często rewanż skutkuje zakupem nowej broni bądź magazynków. Państwo, które prowadzi taką politykę, traci często możliwość negocjacji oraz wpływy w organizacjach międzynarodowych. Rewanżyzm to działanie pod wpływem emocji, a nie na skutek zaplanowanej decyzji, w związku z czym często szkodzi określonym interesom, powoduje błędne oceny ryzyka oraz

implikuje impulsywne decyzje wojskowe. Ruchy rewanżystyczne najczęściej pojawiają się w społeczeństwach, które doświadczyły klęski, okupacji lub znaczącego osłabienia z punktu widzenia pozycji geopolitycznej. Liderzy polityczni często odwołują się do tych wydarzeń, by mobilizować nastroje społeczne, przedstawiając naród jako ofiarę niesprawiedliwości i wskazując siebie jako tych, którzy mogą przywrócić mu należny status. Tego typu retoryka scala społeczeństwo wokół wspólnego poczucia krzywdy, jednocześnie ujmując konflikty polityczne w kategoriach moralnych – między obrońcami narodu a tymi, którzy rzekomo dopuścili do jego upadku.

Atrakcyjność rewanżyzmu wzmacnia symboliczne narracje, selektywne odwołania do historii oraz idealizowane wizje chwalebnej przeszłości. Zestawienie tych obrazów z postrzeganym osłabieniem współczesnym pozwala działaczom rewanżystycznym uzasadniać politykę mającą „naprawić" historyczne błędy. Mogą to być roszczenia terytorialne, wzmożona militaryzacja czy projekty kulturowe mające na celu umocnienie jednolitej tożsamości narodowej. Jednocześnie rewanżyzm niesie ze sobą poważne zagrożenia: na arenie międzynarodowej może podsycać rywalizację, destabilizować regiony i osłabiać normy stosowane w dyplomacji.

W polityce wewnętrznej często sprzyja erozji instytucji demokratycznych, koncentrując władzę w rękach liderów, którzy roszczą sobie wyjątkowe prawo do ochrony narodu. Podkreślanie zemsty i przywracania dawnej potęgi zawęża przestrzeń politycznego kompromisu, przedstawiając go jako zdradę i utrwalając długoterminowe wrogości. Współczesny rewanżyzm łączy tradycyjne elementy nacjonalizmu z nowoczesnymi narzędziami wpływu politycznego, takimi jak propaganda medialna, dezinformacja czy presja ekonomiczna. Dzięki temu państwa mogą odtwarzać narrację o historycznych krzywdach, unikając jednocześnie otwartej wojny, chociaż w niektórych przypadkach prowadzi to do regionalnych lub globalnych konfliktów.

Pojęcie rewanżyzmu pokazuje, jak silnie pamięć historyczna potrafi kształtować współczesną politykę. Choć może dawać poczucie dumy i jedności, często czyni to kosztem pokoju, współpracy oraz zasad inkluzywności, które stanowią fundamenty życia demokratycznego.

Żanna Osikowicz

Bezpieczeństwo kulturowe człowieka w dobie kryzysu jego tożsamości, J. Gierszewski, A. Pieczywok (red.), Difin, Warszawa 2022; A. Branach-Kallas, *Szok Wielkiej Wojny – o traumie indywidualnej, traumie kulturowej oraz portretach gueules cassées we współczesnej literaturze brytyjskiej i francuskiej*, Wydawnictwo PAN, Warszawa 2018; K. Karagezjan, *Rewanżyzm. Iluzja czy realne zagrożenie?*, Wydawnictwo Agencji Prasowej Nowosti, Moskwa 1984; C. Kwiatkowski, *Niewola resentymentu. Rewizjonizm, rewanżyzm, polityka pamięci rozrachunkowej*, „Kultura i Polityka" 2013, nr 13; M. Snegovaya, A. Lanoszka, *Reclaiming what is ours: Elite continuity and revanchism*, „European Journal of International Security" 2024, https://doi.org/10.1017/.

REZERWA STRATEGICZNA – celowo posiadany, przechowywany i utrzymywany różnego rodzaju asortyment (np. materiały, sprzęty, surowce czy też medykamenty) mający kluczowe znaczenie dla zapewnienia ciągłości funkcjonowania państwa w sytuacji nadzwyczajnej. Dzięki zgromadzonym zasobom możliwe jest zabezpieczenie podstawowych potrzeb podmiotów systemu bezpieczeństwa narodowego oraz osób poszkodowanych w wyniku sytuacji kryzysowej lub kryzysu, a dalej zapewnienie wsparcia w ramach obrony cywilnej. Ponadto celem rezerwy strategicznej jest utrzymanie lub odtworzenie infrastruktury krytycznej, a także sprawne działanie gospodarki państwa. Posiadane rezerwy mogą również stanowić istotny element polityki zagranicznej, bowiem za ich pośrednictwem możliwa jest realizacja polskich interesów narodowych, a także tych wprost wynikających ze zobowiązań sojuszniczych wobec innych państw lub organizacji międzynarodowych, których Polska jest stroną.

Podążając za definicją Mariana Kuliczkowskiego, rezerwy strategiczne to zapasy materiałów będące w dyspozycji najważniejszych organów państwowych, które zostały zgromadzone i zabezpieczone w czasie pokoju celem zaspokojenia wzrastających potrzeb w czasie sytuacji kryzysowej lub wojny. Kuliczkowski wskazuje również, że są one tworzone na wypadek zagrożenia państwa, naruszenia jego bezpieczeństwa, porządku i zdrowia publicznego, wystąpienia klęski żywiołowej lub innych szczególnych sytuacji, które mogą zachwiać dotychczasowy łańcuch dostaw usług lub materiałów, również tych

wpisujących się w infrastrukturę krytyczną, gospodarkę czy działalność międzynarodową.

Odwołując się do definicji Aleksandra Szlachty, można wskazać, że rezerwy strategiczne to świadomie zgromadzone zapasy kluczowych środków (produkcyjnych, konsumpcyjnych oraz walut), których głównym celem jest zagwarantowanie ciągłości produkcji oraz zaopatrzenia ludności na wypadek wystąpienia sytuacji kryzysowej.

Zgodnie z Ustawą z dnia 17 grudnia 2020 r. o rezerwach strategicznych (t.j. Dz.U. 2021, poz. 255) są one tworzone na wypadek zagrożenia bezpieczeństwa i obronności państwa, bezpieczeństwa, porządku i zdrowia publicznego oraz wystąpienia klęski żywiołowej lub sytuacji kryzysowej, w celach wsparcia wykonywania zadań w zakresie bezpieczeństwa i obronności państwa, ochrony ludności i obrony cywilnej, odtworzenia infrastruktury krytycznej, złagodzenia zakłóceń w ciągłości dostaw służących funkcjonowaniu gospodarki i zaspokojeniu podstawowych potrzeb obywateli, ratowania ich życia i zdrowia, realizacji interesów narodowych Rzeczypospolitej Polskiej w dziedzinie bezpieczeństwa narodowego, wypełnienia jej zobowiązań międzynarodowych, a także udzielania pomocy i wsparcia podmiotom prawa międzynarodowego publicznego. Zatem na podstawie przedstawionego art. 3 ustawy można uznać, że rezerwy te stanowią kluczowy element bezpieczeństwa narodowego i stabilności państwa, mając szerokie zastosowanie od obronności, przez wsparcie gospodarki, po ratowanie życia i zdrowia obywateli w sytuacjach kryzysowych, tym samym odpowiadając na potrzeby z zakresu zarządzania kryzysowego, a także ochrony ludności i obrony cywilnej. Za utrzymywanie rezerwy strategicznej na odpowiednim poziomie odpowiada Rządowa Agencja Rezerw Strategicznych (RARS) – podmiot, który powstał na mocy wspomnianej już ustawy, a ponadto jest również agencją wykonawczą w rozumieniu Ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. 2009, nr 157, poz. 1240), która podlega ministrowi właściwemu do spraw wewnętrznych. Rządowa Agencja Rezerw Strategicznych zastąpiła w 2020 r. Agencję Rezerw Materiałowych (ARM).

Do zadań Rządowej Agencji Rezerw Strategicznych należy m.in.

- utrzymywanie rezerw strategicznych, w tym ich przechowywanie, dokonywanie wymiany lub zamiany oraz przeprowadzanie konserwacji przechowywanych rezerw strategicznych;
- udostępnianie rezerw strategicznych oraz realizacja innych zadań w ramach udzielania pomocy i wsparcia podmiotom prawa międzynarodowego publicznego;
- wykonywanie decyzji uprawnionych organów lub podmiotów dotyczących zakupu, magazynowania i wydawania określonych asortymentów towarów;
- kontrola podmiotów przechowujących rezerwy strategiczne oraz realizujących inne umowy zawarte z agencją w ramach utrzymywania rezerw strategicznych;
- realizacja zadań w zakresie tworzenia oraz utrzymywania rezerw ropy naftowej i paliw agencyjnych, zgodnie z przepisami Ustawy z dnia 16 lutego 2007 r. o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym (t.j. Dz.U. 2007, nr 52, poz. 343).

Rezerwy strategiczne tworzone i utrzymywane są na podstawie Rządowego Programu Rezerw Strategicznych, który określa zasoby, a także ich rodzaj i ilość. Niniejszy program powstaje w ramach zespołu pod przewodnictwem prezesa Rady Ministrów przy wsparciu agencji. W jego skład wchodzą m.in. minister obrony narodowej, minister sprawiedliwości, minister właściwy do spraw wewnętrznych, minister właściwy do spraw zdrowia i inni przedstawiciele Rady Ministrów. Oprócz tego przy tworzeniu programu pracuje również Rządowe Centrum Bezpieczeństwa, a także inne organy administracji publicznej oraz podmioty związane z obronnością, utrzymaniem porządku publicznego bądź zarządzaniem kryzysowym. Rządowy Program Rezerw Strategicznych jest finansowany z budżetu państwa.

Rezerwy strategiczne są przechowywane w specjalnie przeznaczonych do tego magazynach RARS, jednakże, jeżeli zaistnieje taka potrzeba, agencja może przekazać asortyment zewnętrznym podmiotom

celem ich magazynowania: odbywa się to na podstawie umów oraz określonego finansowania.

Rezerwy strategiczne powinny być gromadzone w obrębie 4 głównych obszarów, które są podstawą do zapewnienia ciągłości funkcjonowania systemu bezpieczeństwa narodowego oraz jego podmiotów:

- technicznym (np. maszyny i urządzenia budowlane, oświetleniowe oraz telekomunikacyjne, agregaty prądotwórcze, asortyment przeciwpowodziowy, stalowe konstrukcje służące do budowy mostów oraz drogowych i kolejowych, cysterny wykorzystywane do przewozu wody pitnej, a także sprzęt związany z transportem wodnym);
- medycznym (np. leki, opatrunki, sprzęt medyczny, m.in. respiratory, pompy infuzyjne, ssaki, kardiomonitory, surowice i szczepionki, sprzęt kwaterunkowy, odzież ochronna, wyroby medyczne jednorazowego użytku);
- żywnościowym (np. woda pitna, zboże i produkty zbożowe, produkty mleczne, mięso, tłuszcze);
- paliwowym i naftowym.

Jako przykład wykorzystania asortymentu Rządowej Agencji Rezerw Strategicznych można wskazać pandemię Covid-19, podczas której w szczególny sposób uruchomiono rezerwy medyczne. Wówczas dystrybuowano leki, opatrunki, preparaty dezynfekujące, szczepionki, środki ochrony indywidualnej (tj. maski, rękawiczki, gogle), sprzęt medyczny (tj. respiratory, kardiomonitory, aparaty USG i RTG itp.), a także odzież ochronną. Kolejnym przykładem jest powódź, która nawiedziła południe Polski we wrześniu 2024 r. (w szczególności województwa dolnośląskie, śląskie i opolskie). Wówczas RARS przekazała niezbędne środki do usuwania stanu klęski żywiołowej na wskazanym obszarze, co umożliwiło mieszkańcom tych terenów rozpoczęcie odbudowy zniszczeń, a także powrót do względnie normalnego życia. Do środków przekazanych przez agencję należy zaliczyć m.in. mosty tymczasowe, agregaty prądotwórcze, zapory przeciwpowodziowe, mobilne rębaki, nagrzewnice, kontenery mieszkalne i techniczne czy też środki higieniczne. Oprócz tego agencja brała również aktywny udział w budowie zastępczej szkoły w Żaleźnie oraz przedszkola i szkoły w Stroniu Śląskim. Łącznie w wyniku usuwania

skutków powodzi w ciągu roku RARS przeznaczyła środki o wartości niespełna 85 mln zł.

W ramach wsparcia międzynarodowego należy przedstawić przykład pomocy Ukrainie. Rządowa Agencja Rezerw Strategicznych przekazała na rzecz tego państwa leki, żywność, a także środki medyczne.

Rezerwy strategiczne stanowią istotny element funkcjonowania systemu bezpieczeństwa narodowego; nieprzerwanie powinny być utrzymywane na odpowiednim poziomie, bowiem w sytuacji wystąpienia zagrożenia o różnej etiologii (naturalnego, technicznego, wynikającego z działalności człowieka) władza publiczna winna posiadać odpowiednie zasoby oraz narzędzia do skutecznej reakcji, zarówno na poziomie zaspokajania potrzeb, jak i pomocy w redukcji skutków zaistniałego wydarzenia. Ponadto posiadane rezerwy strategiczne dają możliwość odtworzenia powstałych zniszczeń w ramach ostatniej fazy zarządzania kryzysowego. Znaczenie rezerw strategicznych stale wzrasta z uwagi na dynamicznie zmieniające się środowisko bezpieczeństwa, a także ustawę z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, na podstawie której rezerwy strategiczne zostały ujęte jako niezbędne ogniwo systemu w ramach obrony cywilnej państwa.

Żaneta Zając, Przemysław Wywiał

Działania RARS po powodzi w 2024 r., Rządowa Agencja Rezerw Strategicznych, https://www.gov.pl/web/rars/dzialania-rars-po-powodzi-w-2024-roku (dostęp 5.12.2025); A. Kawęcka, *Nabycie przez Rządową Agencję Rezerw Strategicznych własności nieruchomości Skarbu Państwa – w trybie art. 75 „nowej" ustawy o rezerwach strategicznych*, „Folia Iuridica Universitatis Wratislaviensis" 2022, t. 11(1); M. Kuliczkowski, *Rezerwa strategiczna*, [w:] *Słownik terminów z zakresu bezpieczeństwa*, J. Pawłowski, B. Zdrodowski, M. Kuliczkowski (red.), Wydawnictwo Adam Marszałek, Toruń 2020; Rządowa Agencja Rezerw Strategicznych, https://www.gov.pl/web/rars/rezerwy-medyczne (dostęp 5.12.2025); A. Szajkowska, J. Czech, *Rola Rządowej Agencji Rezerw Strategicznych w czasach niepewności. Procedury zakupowe*, https://funduszeueswietokrzyskie.pl/images/prezentacja%20RARS.pdf (dostęp 5.12.2025); Ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych, t.j. Dz.U. 2021, poz. 255; Ż. Zając, *Działania wybranych podmiotów systemu bezpieczeństwa narodowego w Polsce w przeciwdziałaniu skutkom pandemii*

Covid-19 w latach 2020–2022 [rozprawa doktorska], Uniwersytet Komisji Edukacji Narodowej, Kraków 2025.

ROSYJSKA AGENCJA PROJEKTOWANIA SPOŁECZNEGO, APS (ros. Агентство Социального Проектирования, ang. Social Design Agency, SDA) – przedsiębiorstwo informatyczne działające od 2001 r., które na zlecenie Kremla od lat prowadzi w sieci kampanię dezinformacyjną, której celem są mieszkańcy krajów Zachodu, a także państw byłego Związku Radzieckiego. Agencja zaangażowana jest praktycznie w większość operacji informacyjnych prowadzonych przez Kreml.

APS to agencja dysponująca znacznym budżetem, z profesjonalną kadrą podzieloną na zespoły z konkretnymi zadaniami. To kompetentna organizacja łącząca zdolność do produkcji i dystrybucji treści na dużą skalę, narzędzia marketingowe, działania psychologiczne i klasyczne szpiegostwo. Kampanie przez nią prowadzone są elementem długoterminowych operacji informacyjnych ukierunkowanych na osłabienie demokracji i społeczeństwa na Zachodzie poprzez pogłębianie podziałów społecznych.

Agencja działa na podstawie zadań powierzonych jej przez państwo rosyjskie i jest bezpośrednio przez nie finansowana. Wraz ze swoją spółką partnerską Structura National Technologies[23] podjęła próbę przeprowadzenia wielu operacji mających na celu podważenie demokracji i osłabienie międzynarodowego wsparcia dla Ukrainy. APS zajmuje się przede wszystkim tworzeniem treści, a Struktura – ich dystrybucją. Służą one jako przykrywki do transferu funduszy z Kremla. Po rozpoczęciu pełnoskalowej wojny w 2022 r. Kreml zlecił agencji podżeganie antyukraińskich protestów w całej Europie.

Agencja pozycjonuje się jako organizacja zapewniająca klientowi pełne wsparcie medialne; obejmuje to analizę zachodniego pola

[23] Agencja PR Structura National Technologies to rosyjska firma technologiczna i *public relations*, która została objęta sankcjami międzynarodowymi (m.in. przez Wielką Brytanię, USA i UE) za zaangażowanie w szeroko zakrojone kampanie dezinformacyjne. Ze względu na charakter działalności i sankcje firma ta nie funkcjonuje jako standardowa, transparentna agencja PR. Informacje o jej usługach w tradycyjnym rozumieniu *public relations* nie są dostępne, ponieważ jej działania koncentrują się na operacjach wpływu i dezinformacji.

informacyjnego, identyfikację potencjalnych zagrożeń, proponowanie rozwiązań i ich wdrażanie. Formalnie zajmuje się projektowaniem i realizacją tzw. projektów społeczno-politycznych oraz usługami specjalistycznymi w sferze komunikacji. Natomiast w kontekście wojny z Ukrainą i rosyjskiej machiny propagandowej stała się jednym z kluczowych podmiotów dezinformacyjnych o znaczeniu międzynarodowym. Jej faktyczne działania są ściśle powiązane z rosyjskimi służbami państwowymi i polityką Kremla, zwłaszcza w obszarze informacji, propagandy i dezinformacji.

Od 2022 r. *Agencja Projektowania Społecznego* została zidentyfikowana jako kluczowy element rosyjskiej kampanii dezinformacyjnej prowadzonej w kontekście pełnoskalowej agresji na Ukrainę. W 2024 r. APS próbowała wzniecić protesty w 6 krajach europejskich, jednak pomimo rosyjskiego finansowania tych działań kłamstwa stale napotykają trudności w internecie, a boty i fałszywe strony internetowe mają ograniczoną interakcję.

Agencja odpowiada za rozległą, szkodliwą sieć internetową, powszechnie znaną jako Doppelganger, która zalewa media społecznościowe fałszywymi postami, podrobionymi dokumentami i materiałami deepfake. Odgrywa też kluczową rolę w operacji „Overload", będąc odpowiedzialną za produkcję i dystrybucje treści. Te oszukańcze taktyki mają na celu zamaskowanie prawdy o nielegalnej inwazji Rosji na Ukrainę i odwrócenie uwagi od prawdziwej natury wojny. Ich niejasne działania są częścią skoordynowanej próby wykorzystania oszukańczych operacji informacyjnych do podważania demokracji w celu osiągnięcia określonych celów.

APS rozpoczyna przygotowanie do swoich operacji poprzez badanie sytuacji politycznej, społecznej i ekonomicznej w danym kraju, starając się identyfikować potencjalne napięcia oraz frustracje w społeczeństwie. Jeden dział analizuje tradycyjną prasę, podczas gdy inny bada trendy w mediach społecznościowych; następnie na podstawie zebranych informacji, podejmuje się decyzje, które z nich będą rozwijane.

Zespół Illji Gambashidzego działa w 3 obszarach. Pierwszym z nich jest monitoring: grupa 24 pracowników codziennie analizuje pro- i antyrosyjskie artykuły i posty ponad 1 tys. liderów opinii w 6 językach i opracowuje raporty na temat potencjalnych kampanii informacyjnych. Drugim jest analityka: specjaliści agencji badają grupę docelową i tworzą tzw. „temniki" dla wykonawców. Trzecim jest kreatywność: autorzy piszą

artykuły, uwzględniając styl dziennikarski właściwy dla wybranego kraju, a ilustratorzy tworzą do nich karykatury.

We wrześniu 2024 r. europejscy dziennikarze otrzymali wyciek wewnętrznych dokumentów z Agencji Projektowania Społecznego – organizacji objętej sankcjami w UE i USA, która według amerykańskich organów ścigania tworzy kampanie dezinformacyjne na zlecenie rosyjskiej administracji prezydenckiej. Potwierdzają to dochodzenia niemieckich mediów: „Sueddeutsche Zeitung", „Westdeutscher Rundfunk (WDR)", „Norddeutscher Rundfunk (NDR)", estońskiego portalu Delfi, a także ukraińskiego projektu „Schematy" Radia Swoboda, które pokazują mechanizm działania „machiny kłamstw" Putina.

Z analizy przejętych plików wynika, że APS zajmuje się projektowaniem i przygotowywaniem kampanii rozsiewających fałszywe rosyjskie narracje i promujących rosyjskie interesy – m.in. podważanie wizerunku Ukrainy i promowanie rosyjskich interesów poprzez szerzenie dezinformacji.

Według amerykańskiego wywiadu kuratorem APS jest pierwszy wiceszef rosyjskiej administracji prezydenckiej Siergiej Kirijenko. W kampanię zaangażowana jest również inna pracownica administracji Putina Sofia Zacharowa. Agencją dyskredytującą Ukrainę kieruje rosyjski strateg polityczny Gambaszydze.

W ciągu 4 miesięcy, od stycznia do kwietnia 2024 r., zespół Gambaszydzego wyprodukował prawie 40 tys. artykułów, grafik, falsyfikatów rządowych dokumentów, postów, filmów i memów oraz prawie 34 mln komentarzy z fałszywych kont. Dokumenty APS potwierdzają, że zespół Gambashidzego tworzy i rozpowszechnia w mediach społecznościowych sfabrykowane filmy stylizowane na materiały zachodnich mediów, w szczególności mające na celu dyskredytację Ukraińców za granicą, ograniczenie pomocy wojskowej i materialnej dla Ukrainy, a nawet wiadomości, które miałyby zmienić przebieg wyborów do Parlamentu Europejskiego w czerwcu 2024 r. APS zajmuje się również rozpowszechnianiem fałszywych dokumentów urzędowych, takich jak komunikaty prasowe niemieckiego Ministerstwa Spraw Wewnętrznych i polskiej Służby Celnej. Jednym z celów realizowanych przez APS jest sprawienie, żeby Niemcy „bali się przyszłości tak bardzo, jak to możliwe" – napisał dziennik „Tageschau".

Dziennikarze znaleźli również dowody w wycieku APS sfałszowanych dokumentów ukraińskiego rządu, a także sfałszowany rozkaz domniemanego naczelnego dowódcy Sił Zbrojnych Ukrainy Ołeksandra Syrskiego, który przyrównuje poddanie się żołnierzy do zdrady stanu. Celem tych działań, jak wynika z opisu zadania rosyjskiej agencji, jest „zdyskredytowanie wojskowo-politycznego kierownictwa Ukrainy i zdemoralizowanie Sił Zbrojnych Ukrainy".

Rosyjscy analitycy APS uważnie badają pole informacyjne Ukrainy, identyfikują drażliwe tematy i wykorzystują je do polaryzacji społeczeństwa; należą do nich np. mobilizacja, straty na polu bitwy, ograniczenia wolności słowa w stanie wojennym, redukcja pomocy wojskowej, korupcja i kontrofensywa. Rosyjscy propagandyści aktywnie spekulują również na temat relacji prezydenta Wołodymyra Zełenskiego z jego poprzednikiem Petrem Poroszenką, merem Kijowa Witalijem Kliczką, a także byłym dowódcą Sił Zbrojnych Ukrainy Walerijem Załużnym.

Dziennikarze odkryli również, że dzięki botom w ukraińskim segmencie mediów społecznościowych zespół Gambashidzego promuje destrukcyjne i prorosyjskie narracje; w tym celu wykorzystuje memy, karykatury i fejki.

APS wykorzystuje boty do publikowania komentarzy w mediach społecznościowych, a także tworzy fałszywe filmy i memy, aby zdyskredytować ukraińskie kierownictwo i zdemoralizować armię. Agencja próbowała również wpłynąć na wybory do Parlamentu Europejskiego w czerwcu 2024 r., wspierając partie prawicowe promujące narracje prorosyjskie. Śledztwo ujawniło, że APS, która oficjalnie deklaruje wsparcie medialne, w rzeczywistości zajmuje się rozpowszechnianiem dezinformacji.

Boty Gambashidzego odgrywają ważną rolę w promowaniu różnych destrukcyjnych i prorosyjskich narracji w ukraińskim segmencie sieci społecznościowych. W ten sposób APS rozpowszechnia memy, karykatury i fake newsy. Użytkownicy z Ukrainy często sami demaskują jednak rosyjski ślad takich „wpisów" poprzez błędy gramatyczne i logiczne.

Według ujawnionych dokumentów, stratedzy polityczni Gambashidzego stoją za powstaniem i promocją prorosyjskiego ruchu politycznego Inna Ukraina Wiktora Medwedczuka, byłego deputowanego ludowego oskarżonego o zdradę stanu, który ogłosił powstanie ruchu w styczniu

2023 r., występując w rosyjskiej telewizji po wymianie jeńców wojennych. Medwedczuk pozycjonuje się jako zwolennik rozmów pokojowych, sprzeciwiając się zagrożeniu nuklearnemu i „wykorzystywaniu Ukrainy jako poligonu doświadczalnego dla zachodniej broni".

Właśnie fundusz inwestycyjny 8VC, powiązany z rosyjskimi oligarchami, pomógł Muskowi kupić Twittera za ponad 44 mld dolarów w 2022 r. W skład funduszu wchodzą synowie rosyjskiego oligarchy Petra Awena i byłego członka Rady Federacji Rosyjskiej Wadima Moszkowicza[24].

Działania APS obejmują m.in.

- tworzenie i koordynowanie fałszywych stron internetowych – APS prowadziła ogromną sieć stron podszywających się pod autentyczne media lub organizacje rządowe w krajach takich jak Niemcy, Francja, Włochy, Ukraina, Wielka Brytania. Ich celem było rozpowszechnianie zmanipulowanych narracji i ataków informacyjnych sprzyjających Moskwie oraz podważanie wiarygodności realnych mediów;
- wspieranie kampanii rosyjskiej sieci RRN (Recent Reliable News – Najnowsze Wiarygodne Wiadomości), mającej na celu zniekształcanie informacji i rozpowszechnianie propagandy wspierającej rosyjską wojnę na Ukrainę. Kampania ta, w której uczestniczyły organy rządowe lub podmioty powiązane z państwem rosyjskim, opiera się na fałszywych stronach internetowych podszywających się pod krajowe media i witryny rządowe, a także fałszywych kontach w mediach społecznościowych. Ta skoordynowana i ukierunkowana manipulacja informacjami jest częścią szerszej hybrydowej kampanii Rosji przeciwko UE i państwom członkowskim.

[24] Synowie prezesa Alfa-Group Petra Awena i byłego członka Rady Federacji Rosyjskiej Wadima Moszkowicza pracują w funduszu 8VC, który stał się największym inwestorem zakupu serwisu społecznościowego Twitter (obecnie X) przez amerykańskiego miliardera Elona Muska. „Washington Post" uzyskał dokument z Sądu Okręgowego Północnej Kalifornii, w którym wymieniono inwestorów Muska zaangażowanych w zakup portalu społecznościowego w 2022 r. za ponad 44 mld dolarów. Musk został zmuszony do ujawnienia dokumentu na mocy postanowienia sądowego wydanego na początku 2024 r.

Agencja była wskazywana jako kluczowy podmiot kampanii RRN – systematycznych działań mających na celu:

- manipulowanie opinią publiczną;
- szerzenie prorosyjskich przekazów politycznych;
- obniżenie poparcia dla państw wspierających Ukrainę;
- podważanie suwerenności i integralności terytorialnej Ukrainy oraz państw europejskich.

Wyciek wewnętrznych materiałów Agencji Projektowania Społecznego ujawnił, że:

- tworzyła kampanie dezinformacyjne adresowane zarówno do społeczeństw europejskich, jak i ukraińskich;
- jej strategia obejmowała m.in. kampanie wywoływania strachu, polaryzowania opinii i legalizowania narracji prorosyjskich;
- zespół APS w analizowanych nagraniach określał swoje działania jako „rosyjskie oddziały ideologiczne", a sam jego szef Gambaszydze był identyfikowany przez amerykańskie służby jako kluczowa osobistość w tej dezinformacyjnej „wojnie informacyjnej" Kremla.

Według analiz Ośrodka Studiów Wschodnich i materiałów zachodnich wywiadów Agencja *Projektowania Społecznego* nie działa w izolacji, a jest częścią większej sieci podmiotów wspierających rosyjską operację wpływu znaną jako „Doppelgänger". W tej sieci APS współpracowała z innymi strukturami, takimi jak ANO Dialog – rosyjska organizacja non profit utworzona przez moskiewski Departament Informacji i Technologii i ściśle powiązana z administracją prezydencką; Inforos – portal internetowy ściśle powiązany z rosyjskim wywiadem wojskowym (GRU) i odpowiedzialny za utworzenie ponad 270 portali internetowych, które rozpowszechniają propagandę wspierającą rosyjską wojnę agresyjną przeciwko Ukrainie; Struktura (ros. Grupa Kompanii Struktura, ang. Company Group Structura), również zaangażowana w propagandę. Kontaktowane były bezpośrednio z przedstawicielami Kremla, wykonywały zadania i raportowały postępy tych kampanii.

28 lipca 2023 r. Agencja *Projektowania Społecznego* została oficjalnie wpisana na listę sankcyjną Rady UE jako podmiot prowadzący działania podważające integralność terytorialną Ukrainy i wspierające narracje

Kremla. Decyzja ta podkreśliła, że organizacja aktywnie wspiera rosyjską wojnę informacyjną oraz jest powiązana z władzami Federacji Rosyjskiej. Podobne działania sankcyjne wobec APS podjęły także władze USA, uznając jej rolę w wojnie informacyjnej za część większego rosyjskiego aparatu propagandowego.

Minister spraw zagranicznych Wielkiej Brytanii David Lammy powiedział: „Putinowi tak bardzo zależy na osłabieniu europejskiego wsparcia dla Ukrainy, że ucieka się do nieudolnych i nieskutecznych działań mających na celu wzniecenie niepokojów społecznych. Dzisiejsze sankcje wysyłają jasny sygnał: nie będziemy tolerować waszych kłamstw i ingerencji i zamierzamy was ścigać. Rozpaczliwe próby Putina, by nas podzielić, poniosą porażkę. Będziemy ograniczać Kreml i wspierać Ukrainę tak długo, jak będzie to konieczne".

W Polsce skupiono się na antyunijnej retoryce, krytyce rządu Donalda Tuska, protestach rolników i pomocy dla Ukrainy.

Z dokumentów uzyskanych przez dziennikarzy wynika, że APS próbowało m.in. wpłynąć na wybory parlamentarne w UE, które odbyły się w czerwcu 2024 r. Celem było wsparcie sił prawicowych, które, zgodnie z oczekiwaniami ekipy Gambashidzego, powinny promować narracje prorosyjskie. Dokument proponuje „przeprowadzenie kompleksowej kontrkampanii przeciwko liberalnym globalistom, ich programowi i prominentnym przedstawicielom", takim jak przewodnicząca Komisji Europejskiej Ursula von der Leyen. Miała ona objąć głównie Niemcy, Francję, Hiszpanię, Włochy i Polskę.

Kampania składała się z 4 głównych punktów:

- oskarżenia polityków sprawujących władzę o bezpodstawne sianie paniki, w szczególności w związku z możliwym atakiem Rosji na UE;
- krytykowanie poparcia dla równości płci i praw osób LGBT jako „doprowadzania naszych dzieci do szaleństwa";
- podważanie obecnej polityki gospodarczej, posługując się przykładami wysokiej inflacji i bezrobocia;
- oskarżanie globalistów UE o totalitaryzm i militaryzację, jak w Ukrainie.

Zadanie miało zostać zrealizowane przy użyciu standardowych narzędzi agencji – rozpowszechnianie podróbek za pośrednictwem mediów społecznościowych w różnych formach. W szczególności APS wspierała partie Alternatywa dla Niemiec i Francuski Front Narodowy: zespół Gambashidzego dążył do podniesienia ratingów obu sił politycznych do 20%. W Niemczech APS starało się przekonać ponad połowę obywateli, że „nie chce poświęcać swojego dobrobytu w imię zwycięstwa nad Rosją", i promowało narrację, że Stany Zjednoczone rzekomo wykorzystują Niemcy w wojnie gospodarczej i hybrydowej z Rosją, podczas gdy kraj pozostaje nieuzbrojony, oddając Ukrainie wszystko, co ma. Ta kampania dezinformacyjna obejmowała w szczególności rozpowszechnianie twierdzeń, że w Ukrainie popełniane są zbrodnie wojenne z użyciem niemieckiej broni i że jest ona sprzedawana na czarnym rynku. Plany APS wobec Francji były podobne: jedyną istotną różnicą była chęć udowodnienia przez strategów politycznych, że ponad 25% Francuzów chciało wyjścia swojego kraju z NATO.

Ostatecznie, pomimo faktu, że większość miejsc w parlamencie pozostała w rękach sił demokratycznych, notowania „prawicy" i tak wzrosły. W ujawnionych dokumentach ekipa Gambashidzego przypisuje sobie tę zasługę. „Ogólnie rzecz biorąc, ogólny sukces prawicy w wyborach europejskich jest dziś postrzegany na całym świecie jako sukces rosyjskiej polityki zagranicznej i, co ważniejsze, sukces rosyjskiej propagandy", napisano w jednym z dokumentów. Zauważono jednak, że liderzy partii prawicowych nie zawsze spełniają oczekiwania Rosji; przykładami są Marine Le Pen, liderka francuskiej skrajnej prawicy, która „oklaskiwała prezydenta Ukrainy Wołodymyra Zełenskiego w Paryżu" podczas jego przemówienia w Zgromadzeniu Narodowym w czerwcu 2024 r., oraz premier Włoch Giorgia Meloni, która żarliwie wspiera Ukrainę, mimo że należy do partii prawicowej.

Podsumowując, Agencja *Projektowania Społecznego* działała nie na klasycznym polu walki, lecz „frontach narracyjnych" i medialnych. Manipulacje informacjami miały:

- wpływać na postawy społeczne i polityczne w Europie;
- erodować zaufanie do instytucji demokratycznych;

– wzmacniać antyukraińskie i prorosyjskie narracje w krajach zachodnich;
– osłabiać poparcie dla sankcji i wsparcia wojskowego wobec Ukrainy.

To sprawia, że APS jest uznawana dziś za narzędzie wojny hybrydowej i informacyjnej Federacji Rosyjskiej – część systemu oddziaływania, który uzupełnia działania militarne.

Agencja *Projektowania Społecznego* działa na granicy technologii, komunikacji i propagandy, wykorzystuje nowoczesne narzędzia internetowe (fałszywe portale, social media), operuje w wielu językach i targetuje różne grupy społeczne. Działalność APS pokazuje, że walkę o narrację społeczną i polityczną prowadzi się dziś równolegle do działań militarnych i jest to część szerszej konfrontacji o wpływy polityczne, społeczne i kulturowe.

APS stworzyła sieć co najmniej 120 stron podszywających się pod istniejące serwisy informacyjne i rządowe, do których podstępnie przekierowuje niczego niepodejrzewających użytkowników mediów społecznościowych. Stosowane taktyki obejmowały unikanie popularnych słów kluczowych, aby ominąć narzędzia moderacji treści i uniknąć usunięcia konta.

Olga Wasiuta

K. Chawryło, *„Doppelgänger" – schemat rosyjskiej operacji wpływu przeciwko Zachodowi*, 13.09.2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-09-13/doppelganger-schemat-rosyjskiej-operacji-wplywu-przeciwko-zachodowi?utm_source=chatgpt.com (dostęp 11.12.2025); Decyzja Rady w sprawie zmiany decyzji 2014/145/WPZiB w sprawie środków ograniczających w związku z działaniami podważającymi integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażającymi, Bruksela, 25.07.2023, https://data.consilium.europa.eu/doc/document/ST-11607-2023-INIT/pl/pdf?utm_source=chatgpt.com (dostęp 11.12.2025); *Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities*, 28.07.2023, https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/ (dostęp 10.12.2025); A. Kozłowski, *#CyberMagazyn: Social Design Agency – rosyjska fabryka trolli na sterydach*, 15.11.2025, https://cyberdefence24.pl/armia-i-sluzby/cybermagazyn-social-design-agency-rosyjska-fabryka-trolli-na-sterydach

(dostęp 12.12.2025); *Media o wycieku wewnętrznych dokumentów. Pokazują, jak działa machina propagandowa Kremla*, 18.09.2024, https://tvn24.pl/swiat/rosja-wyciekly-dokumenty-agencji-projektowania-spolecznego-odpowiada-za-kampanie-dezinformacyjne-kremla-st8095662?utm_source=chatgpt.com (dostęp 12.12.2025); *Sanctions List Search*, https://sanctionssearch.ofac.treas.gov/Details.APSx?id=45230 (dostęp 12.12.2025); M. Sieradzka, *Rosyjskie fake newsy mają osłabić spójność Zachodu*, 12.02.2024, https://www.dw.com/pl/niemieckie-media-wyciek%C5%82y-dokumenty-putinowskiej-fabryki-k%C5%82amstw/a-70237252 (dostęp 12.12.2025); *Social Design Agency*, https://socialdesignagency.com/ (dostęp 10.12.2025); *UK sanctions Putin's interference actors*, 28.10.2024, https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors (dostęp 12.12.2025); *США запровадили санкції проти політтехнологів РФ – поширювали дезінформацію в Латинській Америці*, 20.03.2024, https://www.radiosvoboda.org/a/news-ssha-sanktsiyi-rosiys%CA%B9ki-polittekhnolohy/32870580.html (dostęp 10.12.2025); І. Оліщук, *Журналісти викрили російську креативну агенцію на поширенні фейків про Україну. «Агенція соціального дизайну» дискредитує вище керівництво України, її громадян, а також лідерів країн-союзниць*, 17.09.2024, https://zaxid.net/rosiyska_kreativna_agentsiya_poshiryuye_feyki_pro_ukrayinu_v_yevropi_ta_ssha_n1593850 (dostęp 10.12.2025); Я. Погончук, *Журналісти викрили кремлівське агентство, що займається дискредитацією України*, 17.09.2024, https://24tv.ua/agentstvo-sotsialnogo-dizaynu-poshiryuye-feyki-shho-viyavilo_n2642759 (dostęp 12.12.2025); М. Савчук, А. Миронюк, *Темники, меми, «реєстр фейків та допреальності». Як працює агенція-підрядник Кремля із дезінформації*, 16.09.2024, https://www.radiosvoboda.org/a/skhemy-kreml-dezinformatsiya-APS-hambashydze/33121898.html (dostęp 12.12.2025).

ROSYJSKA FUNDACJA PRAVFOND (Fundacja Wspierania i Ochrony Praw Rodaków Mieszkających za Granicą; ang. Fund for Support and Protection of the Rights of Compatriots Living Abroad; ros. Фонд поддержки и защиты прав соотечественников, проживающих за рубежом, w skrócie – Правфонд) – rosyjska organizacja państwowa, która oficjalnie zajmuje się pomocą prawną dla Rosjan za granicą, jednak według licznych śledztw dziennikarskich i raportów wywiadowczych z lat 2024–2025 służy jako narzędzie rosyjskich służb specjalnych do finansowania propagandy, operacji wpływu oraz wspierania agentów Kremla w Europie.

Fundacja Pravfond została utworzona w 2012 r. na mocy dekretu ówczesnego prezydenta Rosji Dmitrija Miedwiediewa przy wsparciu rosyjskiego Ministerstwa Spraw Zagranicznych oraz agencji Rossotrudniczestwo. Fundacja jest finansowana przez Federację Rosyjską w celu realizacji celów polityki zagranicznej rządu rosyjskiego; stanowi unikalną strukturę rosyjskiej „miękkiej siły", odgrywającą ważną rolę wspierającą w realizacji polityki podziału rządu rosyjskiego. Analizy ekspertów fundacji służą potwierdzeniu głównych przekazów propagandowych Kremla, w tym o wspieraniu neonazizmu i ksenofobii przez władze ukraińskie. Bezpodstawne oskarżenia o nazizm, rusofobię i masowe prześladowania osób rosyjskojęzycznych są wykorzystywane przez fundację, zgodnie z polityką Kremla, do tworzenia niestabilności i podziałów w wielu krajach sąsiadujących z Rosją.

Dyrektor wykonawczy fundacji wyraził poparcie dla prezydenta Putina i rosyjskiej wojny z Ukrainą. Minister spraw zagranicznych Rosji Siergiej Ławrow potwierdził konsekwentną działalność fundacji w zakresie przeciwdziałania ksenofobii, neonazizmowi i próbom fałszowania historii, dlatego Fundacja Wspierania i Ochrony Praw Rodaków Mieszkających za Granicą ma za zadanie pomagać materialnie i przynosić korzyści rządowi FR, który odpowiada za aneksję Krymu i destabilizację Ukrainy.

W radzie zarządzającej fundacją zasiadają wysocy rangą rosyjscy urzędnicy, w tym Ławrow, minister spraw zagranicznych Rosji; Grigory Karasin, przewodniczący Komitetu Spraw Zagranicznych Rady Federacji Zgromadzenia Federalnego; Igor Masłow, szef Departamentu Stosunków Międzyregionalnych i Kulturalnych Administracji Prezydenta; Michaił Galuzin, wiceminister spraw zagranicznych; oraz Jewgienij Primakow, szef Rossotrudniczestwa. Dyrektor wykonawczy fundacji Aleksandr Udalcow został ukarany przez Unię Europejską za wspieranie wojny przeciwko Ukrainie.

Na swojej stronie internetowej fundacja opisuje siebie jako organizację zaprojektowaną przede wszystkim do udzielania ukierunkowanej pomocy prawnej dla rodaków mieszkających za granicą w przypadkach, gdy ich prawa lub wolności są rzekomo zagrożone; wsparcie projektów walki z rusofobią oraz udzielanie wsparcia rosyjskim NGO za granicą. W praktyce jednak funkcjonuje jako geopolityczne narzędzie Kremla – instrument

„miękkiej siły" mający na celu rozszerzanie wpływów w Europie, Gruzji, Mołdawii, Ukrainie i Azji Środkowej. Fundacja finansuje obronę szpiegów i przestępców, utrzymuje siatki wpływu oraz wspiera kampanie propagandowe na kilku kontynentach.

Pod pretekstem pomocy swoim obywatelom za granicą fundacja finansowała projekty dezinformacyjne oraz obronę prawną osób podejrzewanych o szpiegostwo; korzystała z pośredników, kont zagranicznych i aktywów kryptograficznych, aby dyskretnie kontynuować swoją działalność w Unii Europejskiej.

Unia Europejska nałożyła sankcje na Pravfond i jego dyrektora wykonawczego Udalcewa w czerwcu 2023 r. za wykorzystywanie budżetu do finansowania i wspierania realizacji interesów Kremla w polityce zagranicznej, prorosyjskiej propagandy w różnych krajach, zwłaszcza w byłych republikach radzieckich. Część wsparcia trafiała do osób oskarżonych o szpiegostwo, przestępstwa cybernetyczne lub aktywności propagandowe prokremlowskie. Fundacja Pravfond używała wielu obejść (pośrednicy, zagraniczne konta, kurierskie przesyłki gotówki, kryptowaluty), by omijać przepisy. W grudniu 2025 r. rząd brytyjski nałożył nowe sankcje na Pravfond, oskarżając organizację o bycie „przykrywką" dla rosyjskiego wywiadu wojskowego (GRU), co potwierdza, że rządy europejskie traktują Pravfond jako podmiot zaangażowany w tzw. zagraniczną wojnę informacyjną i obejmują go restrykcjami.

Międzynarodowe śledztwa mediów (konsorcjum Projekt dochodzeniowy w sprawie korupcji i przestępczości zorganizowanej (OCCRP)[25] i partnerzy (28 mediów), w tym Le Monde, The Guardian, Meduza, duńska DR i polskie Frontstory.pl) ujawniły wyciek tysięcy wewnętrznych dokumentów i maili fundacji Pravfond, które uzyskał duński nadawca

[25] OCCRP (Organized Crime and Corruption Reporting Project) – konsorcjum ośrodków śledczych, mediów i dziennikarzy z Europy Wschodniej, Kaukazu, Azji Środkowej i Ameryki Środkowej. Założone w 2006 r., jest jedyną organizacją dziennikarstwa śledczego specjalizującą się w przestępczości zorganizowanej i korupcji. Publikuje swoje materiały w lokalnych mediach oraz na swojej stronie internetowej w języku angielskim i rosyjskim. OCCRP jest spółką zależną organizacji non profit Journalism Development Network z siedzibą w Stanach Zjednoczonych, w stanie Maryland.

publiczny DR[26], wskazujących, że jest ona ściśle powiązana z rosyjskim służbą wywiadu zagranicznego (SWR). System numeracji umów wskazuje, że w ciągu dekady przyznano ponad tysiąc grantów o wartości co najmniej 6,3 mln dolarów beneficjentom m.in. w Europie, USA i Australii. Po objęciu sankcjami w czerwcu 2023 r. Pravfond nie zaprzestał przelewów; środki nadal trafiały do organizacji w Hiszpanii, Niemczech czy krajach bałtyckich, co potwierdzają wewnętrzne raporty i dane bankowe w posiadaniu OCCRP.

W zbiorze danych fundacji, który trafił do reporterów DR, było ponad 49 tys. maili i 22 tys. dokumentów, a wśród nich – ponad 360 umów dotacyjnych. Z systemu ich numeracji wynika, że fundusz przyznał jeszcze 713 dodatkowych dotacji, których nie ma w „dostępnym" archiwum. Analiza wycieku wskazuje, że korespondencja obejmuje co najmniej 21 tys. nadawców i odbiorców

Z dokumentów i reportaży wynika, że Pravfond zajmował się obroną prawną osób znanych w międzynarodowych sprawach (w reportażach pojawiają się nazwiska historycznie kojarzone z rosyjskimi operacjami zagranicznymi); finansowaniem prorosyjskich mediów i projektów informacyjnych, zwłaszcza w krajach bałtyckich i w Europie Środkowo-Wschodniej. Ponadto pomimo sankcji nałożonych w 2023 r. przez Unię Europejską fundacja nadal wysyła pieniądze do odbiorców w krajach Europy – jest wykorzystywana do przekazywania pieniędzy agentom Kremla i rozszerzania wpływów Moskwy w społeczeństwach zagranicznych pod pretekstem „wsparcia". I tak w 2024 r. w Danii aresztowano kobietę mającą powiązania z fundacją Pravfond, oskarżoną o wspieranie rosyjskich operacji dezinformacyjnych.

Śledztwa dziennikarskie potwierdziły, że Pravfond finansował pomoc prawną agentów powiązanych z Kremlem, handlarzy bronią i ludźmi oraz osób zamieszanych w sprawy terrorystyczne – w tym pokrywał koszty obrony zabójcy Gruzina Zelimchana Changoszwilego. Jednak

[26] DR (Danish Broadcasting Corporation) – duński publiczny nadawca radiowo-telewizyjny, najstarsza i największa firma medialna w kraju, założona w 1925 r. DR jest odpowiedzialny za programy telewizyjne i radiowe oraz za dostarczanie informacji, edukacji i kultury Duńczykom.

umieszczenie na czarnej liście nie powstrzymało gruzińskich podmiotów przed utrzymywaniem z nią relacji. Korespondencja między fundacją a jej gruzińskimi partnerami ujawnia co najmniej 10 oddzielnych maili omawiających alternatywne metody finansowania. Obejmowały one korzystanie z ormiańskich kont bankowych, przelewy pieniężne do rosyjskich banków w celu późniejszego wypłacenia gotówki, a nawet dostarczanie środków do Gruzji za pośrednictwem prywatnych usług przekazów pieniężnych.

Jak w czerwcu 2024 r. napisał „The Guardian", fundusz opłacał m.in. obronę prawną znanego rosyjskiego handlarza bronią Viktora Buta oraz zabójcy Wadima Krasikowa, a także zatrudniał wielu byłych oficerów rosyjskiego wywiadu jako dyrektorów swoich przedstawicielstw w krajach europejskich. Wśród nich są m.in. Władimir Pozdorowkin, zidentyfikowany przez europejskie źródła wywiadowcze jako agent SWR, który w oficjalnych dokumentach publicznych widnieje jako koordynator Pravfondu ds. operacji w krajach nordyckich i bałtyckich, oraz Anatolij Sorokin, również związany z rosyjskim wywiadem, odpowiedzialny za region Bliskiego Wschodu, Mołdawii i Naddniestrza.

W maju 2025 r. opublikowano wyniki szeroko zakrojonego międzynarodowego śledztwa dziennikarskiego opartego na wycieku tysięcy maili fundacji („The Pravfond Files"). Materiały te zostały pozyskane przez organizację OCCRP, wraz z zaprzyjaźnionymi mediami, co umożliwiło Stowarzyszeniu Dziennikarzy Śledczych iFact[27] z Gruzji ich zbadanie. Spośród tysięcy maili i dokumentów zidentyfikowano 4 organizacje, które otrzymały do 800 tys. euro dofinansowania z Rosji, nadal swobodnie działają w Gruzji i aktywnie promują prorosyjskie narracje. Dokumenty te potwierdziły, że Pravfond instruował zagraniczne media, jak kształtować

[27] Stowarzyszenie Dziennikarzy Śledczych iFact – niekomercyjna organizacja medialna założona w 2016 r. przez Nino Bakradze i Nino Gagueę (Gruzja). Od samego początku celem iFact było podnoszenie jakości dziennikarstwa śledczego i dostarczanie społeczeństwu ważnych informacji w zrozumiałej formie. iFact jest członkiem międzynarodowych sieci dziennikarzy śledczych, takich jak Organized Crime and Corruption Reporting Project (OCCRP) oraz Global Investigative Journalists Network (GIJN).

narrację, oraz finansował prawników na Litwie, którzy obecnie stoją przed komisjami dyscyplinarnymi za współpracę z rosyjskim wywiadem.

Pod przykrywką 23 ośrodków pomocy prawnej – od Hiszpanii po Mongolię – Pravfond buduje infrastrukturę wpływu i zapewnia bezpośrednie finansowanie propagandy i operacji wywierania wpływu. Działacze tych placówek redagują rosyjskojęzyczne portale, drukują podręczniki usprawiedliwiające okupację sowiecką krajów nadbałtyckich (np. sporny e-podręcznik historii Litwy, z przedmową rosyjskiego ministra spraw zagranicznych Siergieja Ławrowa, który przedstawiał okupację kraju przez Związek Radziecki w pozytywnym świetle) oraz organizują konferencje wymierzone w „rusofobię". Fundusz sfinansował także setki artykułów na łotewskim portalu IMHOclub oraz powstanie sieci kanałów Telegram w krajach bałtyckich.

Estońska służba KAPO[28] określa Pravfond jako „przedłużenie rosyjskich służb specjalnych", które pod pozorem walki z dyskryminacją kontroluje diasporę. Podobny pogląd wyraża łotewska VDD[29]. Brytyjski analityk Edward Lucas, cytowany przez „The Guardian", zwraca uwagę, że państwa rzadko płacą za kosztowną obronę prawną cudzoziemców, jeśli nie chodzi o operację wpływu.

Ujawnione dokumenty Pravfondu pokazują, jak Rosja łączy soft power z operacjami wywiadowczymi; z pozoru filantropijna organizacja w praktyce przeznacza fundusze na obronę agentów, wzmacnia prorosyjską narrację i karmi sieci lojalnych kontaktów – często wprost pod nosem państw, które objęły ją sankcjami.

Pravfond prowadzi centra prawne zajmujące się prawami człowieka w 19 krajach, w tym w Armenii, Irlandii, Hiszpanii, Kazachstanie, Chinach, Mongolii, Francji, Ukrainie, Mołdawii i Serbii. W większości

---

[28] KAPO (est. Kaitsepolitseiamet) – Estońska Służba Bezpieczeństwa Wewnętrznego (Policja Bezpieczeństwa) będąca centralną agencją bezpieczeństwa narodowego Estonii; działa pod nadzorem Ministerstwa Spraw Wewnętrznych.

[29] VDD (*valsts drošības dienests*) – łotewska Służba Bezpieczeństwa Państwa – główny organ kontrwywiadu i bezpieczeństwa narodowego, odpowiedzialny za ochronę konstytucyjnego porządku, bezpieczeństwo państwa, zwalczanie terroryzmu i szpiegostwa, zwłaszcza ze strony Rosji i Białorusi, co często podkreślają ich raporty.

z nich fundacja współpracuje tylko z 1 takim centrum; jedynie w Gruzji, Kirgistanie i Abchazji – z 2 jednocześnie.

Finansowanie operacji w Europie:

- agenturalna pomoc prawna: fundacja opłacała prawników dla rosyjskich agentów i przestępców, w tym dla zabójcy Zelimchana Changoszwilego w Berlinie (Wadima Krasikowa – agenta FSB) oraz Wiktora Buta, aresztowanego handlarza bronią. Obaj zostali skazani i przekazani Rosji w ramach wymiany więźniów;
- propaganda: finansuje portale internetowe, w tym prorosyjskie kanały na Telegramie i czasopisma szerzące kremlowską narrację w krajach takich, jak Gruzja, Litwa, Estonia i Łotwa. W Gruzji fundacja przekazała do 800 tys. euro organizacjom promującym rosyjskie wpływy;
- siatki wpływów: działa w ponad 40 krajach, w tym w Gruzji, krajach bałtyckich i na Bałkanach, gdzie fundacja wspierała lokalnych prawników i aktywistów współpracujących z rosyjskimi służbami;
- skala środków: dokumenty z wycieku (obejmujące dane do końca 2024 r.) wskazują, że fundacja przyznała ponad tysiąc grantów, z czego średnia wartość jednego wynosiła około 16 500 dolarów;
- sankcje i obejście prawa: od 2023 r. Pravfond jest objęty sankcjami Unii Europejskiej i USA; mimo to fundacja kontynuuje działalność w Europie w 2024 i 2025 r., stosując takie techniki, jak przemyt gotówki czy przelewy przez konta osób trzecich (np. w Czarnogórze czy Irlandii).

Pravfond finansuje prawników, wydarzenia i osoby, które szerzą propagandę i podważają demokratyczny porządek w Europie, mimo że organizacja znajduje się na unijnej liście sankcyjnej. A w 2025 r. organizacja koncentrowała się na zwalczaniu „rusofobii" oraz wspieraniu kampanii informacyjnych uderzających w pomoc wojskową dla Ukrainy.

Dziennikarze Frontstory.pl znaleźli dowody na współpracę prorosyjskich Polaków z moskiewskim, rządowym funduszem Pravfond i ustalili, że z niego były finansowane różne działania w Polsce: co najmniej 35 tys. euro z moskiewskiego funduszu trafiło do 4 prorosyjskich aktywistów i ich prawników w Polsce, finansując m.in. renowację pomników Armii Czerwonej

oraz działalność marginalnych ugrupowań politycznych. Polskie ABW i sądy od lat miały informacje o powiązaniach tych osób z Rosją.

Dziennikarze Frontstory.pl znaleźli w korespondencji Pravfondu umowy z Rosjanami oskarżonymi i skazanymi w Europie za szpiegostwo. Jednym z nich jest Stanisław Szypowski, 39-letni prawnik, który był zatrzymany przez polskie służby w 2014 r. Pravfond przyznał mu zwrot kosztów na obsługę prawną. Z więzienia Szypowski wyszedł po 7 latach, nie został wydalony z Polski, bo rok przed aresztowaniem dostał obywatelstwo. Inny „dziennikarz" pod przykrywką Leonid Swiridow został wydalony z Polski w 2015 r. – MSZ odebrało mu akredytację na wniosek ABW, a poprzednio, już w 2006 r., akredytację cofnęły mu Czechy. W Polsce Swiridow zbudował szeroką sieć kontaktów, a na Facebooku chwalił się zdjęciami z Wojciechem Jaruzelskim, Lechem Wałęsą, Leszkiem Millerem, Radosławem Sikorskim, Markiem Belką czy Andrzejem Wajdą. Zorganizował wycieczkę dla dziennikarzy do Rosji, w której brali udział m.in. Agnieszka Piwar, autorka kremlowskiego Sputnika, obecna redaktor naczelna „Tygodnika NIE" Agnieszka Wołk-Łaniewska czy historyk Paweł Dybicz, wicenaczelny „Przeglądu". W grudniu 2018 r. Swiridow wrzucił na Facebooka zdjęcia z Grzegorzem Braunem na tle świątecznych dekoracji, z kolei na fotografii ze stycznia 2025 r. pojawił się obok Tomasza Szmydta – zbiegłego na Białoruś byłego sędziego podejrzanego o szpiegostwo na rzecz Białorusi. Zarządzany przez Kreml fundusz opłacał procesy sądowe Swiridowa związane z unieważnieniem zezwolenia na pobyt w UE i wpisaniem do wykazu osób niepożądanych.

Przedstawiciele kilku europejskich agencji wywiadowczych poinformowali OCCRP, że ich zdaniem Pravfond działa poza zakresem swojej misji, pełniąc rolę narzędzia w rękach rosyjskich służb wywiadowczych oraz przeznacza znaczną część swoich środków na projekty mające na celu wpływanie na opinię publiczną w kierunku prorosyjskim. Dziesiątki umów znalezionych przez reporterów w archiwum mailowym dotyczą pracy w mediach, np. w Grecji Pravfond zapewnił finansowanie klubowi Dialogos, grecko-rosyjskiemu stowarzyszeniu, którego strona internetowa deklaruje, że jego celem jest „kształtowanie pozytywnego wizerunku Rosji w Grecji i Grecji w Rosji". Dialogos zorganizował wiele konferencji przy wsparciu Pravfondu, w tym wydarzenia upamiętniające osiągnięcia Związku Radzieckiego w II wojnie światowej i celebrujące konstytucję Rosji.

Inny beneficjent fundacji, popularny łotewski portal cyfrowy o nazwie IMHOclub, opublikował setki artykułów o takich tytułach, jak „Dlaczego Łotwa czyni z Rosji swojego wroga?" i „No cóż, Bałtowie, jak wam idzie bez Lenina?", w których liczni autorzy dyskredytują Łotwę i Unię Europejską, a także wyrażają poparcie dla rosyjskiej inwazji na Ukrainę. Dokumenty mailowe pokazują, że Pravfond przekazał IMHOclub co najmniej 6,4 mln rubli (65 800 dolarów) od 2022 r., w tym na organizację wirtualnej „konferencji antyfaszystowskiej" z udziałem prorosyjskich aktywistów i polityków z wielu krajów, która doprowadziła do przyjęcia antyukraińskiej rezolucji. Pravfond zapłacił również prawie 17 tys. euro na pokrycie kosztów sądowych oskarżonych.

Pravfond działa również w Mołdawii, gdzie wśród beneficjentów grantów znalazł się Aleksiej Pietrowicz, działacz prokremlowski, którego organizacja otrzymała prawie pół miliona rubli (7500 dolarów) na mobilną wystawę zatytułowaną *Nieśmiertelny Stalingrad*, upamiętniającą zwycięstwo Związku Radzieckiego w II wojnie światowej, podczas gdy tuż obok trwała rosyjska inwazja na Ukrainę.

Podsumowując, Pravfond finansuje obronę prawną osób oskarżonych o szpiegostwo, działalność dywersyjną lub agenturalną, wspiera organizacje i osoby powiązane z rosyjskimi służbami specjalnymi, jest elementem strategii „ochrony rodaków", używanej przez Rosję jako uzasadnienie ingerencji politycznej. Stanowi część szerszego ekosystemu tzw. *soft power* Kremla, obok Rossotrudniczestwa, mediów państwowych i fundacji kulturowych wykorzystywane do ochrony i wspierania prorosyjskich interesów oraz agentury pod przykrywką pomocy prawnej „rodakom" za granicą. Działalność fundacji jest uważana za zagrożenie dla bezpieczeństwa wewnętrznego państw UE i NATO. Po agresji Rosji na Ukrainę w 2022 r. fundacja znalazła się pod zwiększoną obserwacją, a jej działalność w wielu krajach została ograniczona lub objęta sankcjami pośrednimi. Pravfond nie jest klasyczną organizacją charytatywną, działa na styku prawa, polityki, wpływu i operacji informacyjnych oraz stanowi przykład instrumentalizacji prawa i organizacji pozarządowych w wojnie hybrydowej.

Olga Wasiuta

B. Hlebowicz, *Rosyjska organizacja „praw człowieka finansowała propagandę Kremla w 48 państwach*, 3.06.2024, https://wyborcza.pl/7,75399,31025288,rosyjska-organizacja-praw-czlowieka-finansowala-propagande.html (dostęp 13.12.2025); A. Jawor, *Pravfond na usługach Kremla. Jak rosyjski fundusz wspiera szpiegów i propagandę?*, 28.05.2025, https://infosecurity24.pl/za-granica/Pravfond-na-uslugach-kremla-jak-rosyjski-fundusz-wspiera-szpiegow-i-propagande (dostęp 13.12.2025); M. Laine, *How Russian public fund Pravfond continued to subsidize its allies in Europe despite sanctions*, OCCRP, 22.05.2025, https://www.lemonde.fr/en/pixels/article/2025/05/22/how-russian-public-fund-Pravfond-continued-to-subsidize-its-allies-in-europe-despite-sanctions_6741523_13.html (dostęp 13.12.2025); D. Leloup, T. Eydoux, L. Minisini, M. Vaudano, *Pravfond, the discreet slush fund for Russian spies and their foreign legal woes*, 2.06.2024, https://www.lemonde.fr/en/pixels/article/2024/06/02/Pravfond-the-discreet-slush-fund-for-russian-spies-and-their-foreign-legal-woes_6673513_13.html?utm_source=chatgpt.com (dostęp 13.12.2025); I. Lozovsky, M. Laine, *Russian Foundation, Aimed at Helping 'Compatriots' Abroad, Supports Spies, Criminals, and Propagandists*, 21.05.2025, https://www.occrp.org/en/project/dear-compatriots/russian-foundation-aimed-at-helping-compatriots-abroad-supports-spies-criminals-and-propagandists (dostęp 11.12.2025); A. Morozova, *Estońskie MSZ wydala rosyjskiego dyplomatę powiązanego z Pravfondem*, 20.08.2025, https://frontstory.pl/estonskie-msz-wydala-rosyjskiego-dyplomate-powiazanego-z-Pravfondem-newsletter-sledz/ (dostęp 11.12.2025); A. Morozova, D. Flis, M. Możański, A. Pawłowska, K. Story, *Komu płaci Moskwa? Ujawniamy dokumenty rosyjskiego funduszu Pravfond***,** 13.02.2025, https://frontstory.pl/podcast-Pravfond-rosja-szpiegostwo/ (dostęp 11.12.2025); A. Morozova, A. Pawłowska, D. Flis, M. Możański, *Komu płaci Moskwa. Ujawniamy dokumenty funduszu Pravfond*, 21.05.2025, https://frontstory.pl/Pravfond-szpiegostwo-rosja/(dostęp 11.12.2025); *New UK action against foreign information warfare*, 9.12.2025, https://www.gov.uk/government/publications/new-uk-action-against-foreign-information-warfare/new-uk-action-against-foreign-information-warfare (dostęp 13.12.2025); *The Foundation for the Support of Compatriots*, https://www.opensanctions.org/entities/NK-jYnxeGfNKtfaD4Ze5v8Xa3/ (dostęp 12.12.2025).

ROSYJSKA OPERACJA DEZINFORMACYJNA „DOPPELGÄNGER" (niem. *doppelgänger,* „zły sobowtór") – jedna z największych i najdłużej trwających rosyjskich kampanii informacyjnych wymierzonych w państwa UE i NATO, która działa w co najmniej 10 krajach Europy i została uruchomiona po rosyjskiej inwazji na Ukrainę w 2022 r. Operację stworzyła moskiewska Agencja Projektowania Społecznego (APS, ang. Social Design

Agency). Według rosyjskich organów podatkowych firma została założona w grudniu 2017 r. Dokumenty ujawnione we wrześniu 2024 r. wskazywały, że w 2024 r. firma zatrudniała około 100 pracowników. APS była nadzorowana przez Kreml, a prezydent Rosji został osobiście poinformowany o jej działaniach.

Operacja została po raz pierwszy zidentyfikowana przez organizację pozarządową EU DisinfoLab jesienią 2022 r. Nazwali ją „Doppelgänger" ze względu na wykorzystywanie sobowtórów popularnych stron internetowych. Ich badania wykazały, że trwała co najmniej od maja 2022 r. – jej istnienie i metody zostały następnie potwierdzone przez innych badaczy z organizacji prywatnych, publicznych i pozarządowych. „Doppelgänger" wykorzystuje wiele „klonów" autentycznych mediów (co najmniej 17, w tym „Bild", „20 minutes", „Ansa", „The Guardian" czy „RBC Ukraine") i atakuje użytkowników fałszywymi artykułami, filmami i ankietami. W tym celu osoby odpowiedzialne za tę akcję kupiły dziesiątki domen internetowych z nazwami podobnymi do autentycznych mediów i skopiowały ich projekty. Po ujawnieniu tych informacji wiele mediów, w tym „Le Monde", „Süddeutsche Zeitung" i „20 minutes", złożyło pozwy, oskarżając o sprzeniewierzenie nazwy.

To kolejny przykład operacji wieloplatformowej, której rdzeń znajduje się na stronach internetowych i profilach wzmacniających w mediach społecznościowych, takich jak Facebook i Twitter. Operacja wykorzystuje różne formaty, od filmów po reklamy internetowe; przedstawia Ukrainę jako upadłe, skorumpowane i nazistowskie państwo, promuje kremlowską narrację na temat wojny w Ukrainie, np. negowanie masakry w Buczy. Sieje strach wśród Niemców, Włochów, Francuzów, Łotyszy i Brytyjczyków, podkreślając, że sankcje wobec Rosji zrujnują im życie.

Celem kampanii jest zdyskredytowanie zachodnich rządów i ich polityki, szczególnie w kontekście reakcji na rosyjską inwazję na Ukrainę oraz szerzenie dezinformacji za pośrednictwem stron internetowych imitujących renomowane media i rozpowszechniających fałszywe wiadomości m.in. w takich krajach, jak Francja, Niemcy, Stany Zjednoczone i Polska. Treści były często rozpowszechniane za pośrednictwem fałszywych kont w mediach społecznościowych. Unia Europejska odkryła kampanię i nadała jej nazwę jesienią 2022 r.

Głównym celem kampanii w Niemczech było zwiększenie poparcia dla AfD przy jednoczesnym osłabieniu Partii Zielonych. Co więcej, miała na celu wzbudzenie obaw o przyszłość i zaszczepienie w niemieckim społeczeństwie przekonania, że nie należy poświęcać własnego dobrobytu dla „zwycięstwa nad Rosją".

W całej Europie głównym celem było osłabienie poparcia dla Ukrainy i destabilizacja jej sojuszników, zwłaszcza Niemiec i Francji. Zaproponowano również kampanię przeciwko partiom centrowym w Niemczech, Francji, Włoszech, Hiszpanii i Polsce, a wzmocnienie partii skrajnie prawicowych i prawicowo-populistycznych, co zostało zidentyfikowane w UE jako sposób na skierowanie decyzji Parlamentu Europejskiego w kierunku prorosyjskim. Kolejny przeciek ujawnił, że rosyjska kampania dezinformacyjna podczas wyborów do Parlamentu Europejskiego w 2024 r. przedstawiała skrajnie prawicowe frakcje jako „partie pokoju" i jednocześnie dyskredytowała przewodniczącą Komisji Europejskiej Urszulę von der Leyen.

Charakterystyczną cechą kampanii „Doppelgänger" było rozpowszechnianie dezinformacji za pośrednictwem stron internetowych podszywających się pod renomowane publikacje we Francji i Włoszech, a także w Niemczech, Ukrainie, Łotwie, Wielkiej Brytanii, Stanach Zjednoczonych i Polsce (np. „Le Monde", „The Guardian", „Ansa" i „Der Spiegel").

W okresie od lutego do sierpnia 2023 r. Kreml zakupił 47 domen podszywających się pod autentyczne portale informacyjne z Europy, w tym „Le Parisien" (Francja), „Welt" (Niemcy) oraz „Politykę" i Polskie Radio (Polska). To tam zamieszczano materiały promujące eurosceptyzm lub mające na celu osłabić pozycję jednej strony politycznej na rzecz innej.

Badacze z Qurium[30] i EU DisinfoLab[31] w 2024 r. przeanalizowali działalność tej sieci dezinformacyjnej i poinformowali, że działa ona

[30] QuriumMedia Foundation – szwedzką fundacją non profit, dostawca rozwiązań z zakresu bezpieczeństwa cyfrowego i dochodzeń kryminalistycznych dla niezależnych mediów i organizacji praw człowieka, https://www.qurium.org/.

[31] EU DisinfoLab – niezależna europejska organizacja non profit, która zajmuje się zwalczaniem zaawansowanych kampanii dezinformacyjnych wymierzonych w UE, jej państwa członkowskie, kluczowe instytucje i wartości, https://www.lobbyfacts.eu/datacard/eu-disinfolab?rid=593474530364-05.

w Europie co najmniej od maja 2022 r. i jest opisywana przez Metę[32] jako „najbardziej wytrwała kampania prowadzona przez Rosję" oraz „jedna z największych na świecie", jak dodaje niemieckie Federalne Ministerstwo Spraw Zagranicznych. Wykorzystuje sieć fałszywych kont botów do rozpowszechniania linków prowadzących do fałszywych wersji prawdziwych serwisów informacyjnych, takich jak francuski „Le Monde", niemiecki „Der Spiegel", brytyjski „The Guardian" i innych. Jej istnienie i metody zostały następnie potwierdzone przez innych badaczy z organizacji prywatnych, publicznych i pozarządowych.

W ocenie specjalistów została ona zbudowana w sposób skrupulatny, a ważną rolę odegrały europejskie firmy i osoby prywatne – jak się okazuje, wspierały operację, świadomie lub nie, poprzez świadczenie usług podmiotom powiązanym z Rosją (np. konfiguracja serwerów).

Operacja „Doppelgänger" jest prowadzona za pośrednictwem nowo powstałych rosyjskich dostawców działających w Europie. W celu realizacji kampanii stworzono infrastrukturę na terenie Europy (minimum w 10 państwach) – wykorzystano do tego różne firmy, przede wszystkim w Wielkiej Brytanii. Podstawą jej działalności w Europie i Rosji jest grupa Aeza[33], dostawca hostingu z siedzibą w Sankt Petersburgu. Według badaczy Aeza „umożliwia przestępcom działanie na własnych serwerach i zazwyczaj znajduje swoich

---

[32] Meta Platforms, Inc. (powszechnie znana jako Meta) – amerykański gigant technologiczny, który jest właścicielem wielu popularnych platform społecznościowych i usług komunikacyjnych. Firma założona przez Marka Zuckerberga zmieniła nazwę z Facebook, Inc. na Meta Platforms w 2021 r., co odzwierciedlało jej nowe strategiczne ukierunkowanie na rozwój wirtualnej rzeczywistości. Meta koncentruje się na tworzeniu technologii, które łączą ludzi, a jej model biznesowy opiera się głównie na reklamach, dzięki czemu większość usług jest bezpłatna dla użytkowników. Firma inwestuje również w sztuczną inteligencję (AI) i rozwój immersyjnych doświadczeń w metawersum, https://www.meta.com/pl-pl/about/company-info/.

[33] Grupa Aeza – rosyjski dostawca usług hostingowych działający od 2021 r. głównie za pośrednictwem zarejestrowanej w Wielkiej Brytanii spółki Aeza International Ltd (AS210644). Od momentu powstania Aeza stała się znanym dostawcą usług hostingowych, umożliwiając cyberprzestępcom i organizacjom rządowym działania za pośrednictwem odpornej na nadużycia infrastruktury. Jest postrzegana przez Grupa Insikt jako jedno z najważniejszych źródeł zweryfikowanej złośliwej infrastruktury, co poświadcza Recorded Future 2024 Malicious Infrastructure Report.

klientów w szarej sieci", np. firma prawdopodobnie świadczy swoje usługi operatorom infrastruktury złośliwego oprogramowania znanym jako Lumma i Meduza. Niektóre z europejskich firm hostingowych wymienionych w raporcie są bezpośrednio lub pośrednio powiązane z Aeza.

Działania rosyjskiego rządu w ramach operacji „Doppelgänger" w serwisie społecznościowym X w czerwcu 2024 r. zostały przeanalizowane przez CeMAS (Niemcy), Science Feedback (Francja), Fundację Obrony Demokracji (Wielka Brytania), Alliance4Europe (Włochy), Demagog, BIQdata.pl/Gazeta Wyborcza (Polska) oraz Centrum Badawcze Media Detector (Ukraina).

W ramach tej operacji kremlowskie służby specjalne tworzą strony internetowe i profile w mediach społecznościowych, które pod względem treści i wyglądu imitują prawdziwe media zachodnie do publikowania fałszywych wiadomości, do których linki są rozpowszechniane za pośrednictwem fałszywych kont na Facebooku, Twitterze i w innych mediach społecznościowych. Kampania miała na celu przede wszystkim promowanie rosyjskich narracji propagandowych na temat Ukrainy, ale rozpowszechniała również rasistowskie, antysemickie i antyislamskie treści wśród odbiorców w Stanach Zjednoczonych i Europie.

W 2024 r. niemieckie Federalne Ministerstwo Spraw Wewnętrznych wspólnie z Ministerstwem Spraw Zagranicznych i Ministerstwem Sprawiedliwości utworzyło nową jednostkę do przeciwdziałania kampaniom dezinformacyjnym typu „Doppelgänger".

Operacja była również określana jako RRN (Recent Reliable News – Najnowsze Wiarygodne Wiadomości); „Matrioszka", „Overload" (od nieoficjalnej nazwy podprojektów mających na celu publikację fałszywych reportaży wideo) i „Storm 1099/Storm 1679" (tak Microsoft określił sieć stron internetowych służących do publikowania dezinformacji).

Operacja „Doppelgänger" charakteryzuje się rozpowszechnianiem dezinformacji za pośrednictwem stron internetowych podszywających się pod renomowane publikacje we Francji, Niemczech, Ukrainie, Łotwie, Włoszech, Wielkiej Brytanii, Stanach Zjednoczonych i Polsce (np. „Le Monde", „The Guardian", „Ansa", „Der Spiegel" i „Fox News"). W niektórych przypadkach podszywano się pod strony internetowe agencji rządowych (np. francuskiego czy niemieckiego Ministerstwa Spraw

Wewnętrznych) lub organizacji międzynarodowych (np. NATO), wykorzystując m.in. *typosquatting*[34].

Fałszywe media publikowały artykuły, materiały wideo, sfabrykowane sondaże oraz treści satyryczne o charakterze deprecjonującym, wymierzone m.in. w Wołodymyra Zełenskiego. Część materiałów była następnie powielana i rozpowszechniana przez inne powiązane witryny. Sieć ta, poza licznymi klonami serwisów, obejmowała również pseudoserwis weryfikacyjny „Wojna z fałszerstwami", publikacje RRN zawierające materiały autorstwa zwolenników reżimu rosyjskiego funkcjonujących w państwach zachodnich, a także niewielkie strony internetowe podszywające się pod media społeczno-polityczne."

Dezinformacja była rozpowszechniana za pomocą komentarzy, repostów i reklam przez skoordynowane fałszywe konta na Facebooku, Twitterze i innych platformach mediów społecznościowych. Meta poinformowała, że w ciągu zaledwie kilku miesięcy w 2022 r. wydano ponad 100 tys. dolarów na reklamę określonych projektów. Konta były często wykorzystywane jednorazowo do rozpowszechniania konkretnej fałszywej wiadomości, a do innych materiałów stworzono nową sieć „botów". Aby ominąć blokowanie fałszywych witryn medialnych, ich adresy ukryto za łańcuchem przekierowań, a w celu stworzenia wrażenia autentycznego zasobu wewnętrzne linki na tych stronach prowadziły do prawdziwych zasobów publikacji.

Zaangażowanie Rosji w kampanię dezinformacyjną potwierdziły liczne wskaźniki: źle napisane teksty z błędami tłumaczenia maszynowego, wykorzystanie jako ilustracji zdjęć z rosyjskich mediów prorządowych, metadane wideo (rosyjski jako język systemu, znaczniki czasu w rosyjskich strefach czasowych, nazwy projektów w języku rosyjskim), rejestracja domen i hosting stron internetowych za pośrednictwem

[34] *Typosquatting* (przechwytywanie adresów URL) – cyberatak, w którym przestępcy rejestrują błędnie wpisane nazwy domen (np. Goggle.com zamiast Google.com), aby oszukać użytkowników popełniających błędy w pisowni, kierując ich na złośliwe strony w celu wyłudzenia informacji, rozsyłania złośliwego oprogramowania lub innych oszustw. Te fałszywe strony imitują legalne witryny, wykorzystując błędy użytkowników do kradzieży informacji, rozprzestrzeniania wirusów lub generowania przychodów z reklam.

rosyjskich firm. Po opublikowaniu fake newsów za pośrednictwem sieci „Doppelgänger" były one aktywnie rozpowszechniane przez rosyjskie ambasady i ośrodki kultury.

Infrastruktura techniczna operacji „Doppelgänger", jak twierdzą badacze, obejmuje ponad 300 stron sieciowych i 100 tys. adresów IP o wartości rynkowej 5 mln euro lub koszt dzierżawy około 50 tys. euro miesięcznie. „Ta ogromna inwestycja w infrastrukturę może być możliwa jedynie dzięki znacznemu wsparciu finansowemu ze strony podmiotów zewnętrznych" – czytamy w raporcie.

Niemiecka organizacja dziennikarska non profit Correctiv, która brała udział w śledztwie, twierdzi, że raport Qurium na ten temat został udostępniony agencjom rządowym w co najmniej 2 krajach europejskich, w tym w Niemczech, już wiosną tego roku. „Jednak informacje te najwyraźniej nie zostały wykorzystane do powstrzymania kampanii. Rodzi to pytania o to, jak poważnie europejskie władze walczą z dezinformacją" – stwierdził Correctiv.

Od 4 do 28 czerwca 2024 r. opublikowano 1366 prorosyjskich postów na platformie X, które dyskredytowały zachodnie rządy, krytykowały Ukrainę i wsparcie Zachodu, poruszały kontrowersyjne tematy i atakowały zachodnie sojusze we wszystkich monitorowanych językach. Według X łączna liczba wyświetleń tych postów do końca czerwca 2024 r. przekroczyła 4,66 mln.

Analitycy z Alliance4Europe i AI Forensics zbadali również dystrybucję postów reklamowych w serwisie Doppelgänger na Facebooku. Według Meta w czerwcu 2024 r. w tym serwisie społecznościowym wykryto 98 reklam o treści prorosyjskiej skierowanych do Francji, Niemiec, Polski i Włoch; dotarły one do około 560 tys. użytkowników. „Te operacje wpływu są częścią złożonej strategii wojskowej, której celem jest podważenie, a ostatecznie zniszczenie demokracji. Demokracja nie może funkcjonować bez realnej sfery publicznej i potrzebujemy podejścia obejmującego całe społeczeństwo, aby ją chronić. Potrzebujemy zasobów i współpracy między badaczami i analitykami, skutecznego egzekwowania prawa przez organy regulacyjne oraz skutecznej rozliczalności platform technologicznych" – powiedział Omri Preis, dyrektor Alliance4Europe.

Według FBI APS pełniła funkcję koordynatora i operatora kampanii, która w okresie od stycznia do kwietnia 2024 r. wygenerowała i rozpowszechniła na całym świecie prawie 40 tys. treści i 33,9 mln komentarzy. Operacja nadal znajdowała nowe cele, takie jak wybory parlamentarne UE w 2024 r. i igrzyska olimpijskie w 2024 r. w Paryżu.

Rosyjska operacja dezinformacyjna „Doppelgänger" skoncentrowała się również na Polsce przy wykorzystaniu usług i infrastruktury europejskich firm do manipulacji przed wyborami prezydenckimi w 2025 r. Jak wynika z raportu Alliance4Europe, dezinformatorzy linkowali artykuły z 13 polskich mediów w fałszywych postach oraz stosowali inne metody dezinformacji. Raport ujawnił, że od 4 marca do 4 kwietnia 2025 r. na platformie X pojawiło się prawie 300 wpisów ingerujących w wybory w Polsce. Trolle korzystały z tekstów opublikowanych na takich stronach, jak Najwyższy Czas, wPolityce, Bankier, Fakt, Fronda, Gazeta Prawna, Money, PolsatNews, Rzeczpospolita, Salon24, TVPInfo, WNP i Interia.

Podsumowując, operacja „Doppelgänger":

- jest w pełni zgodna z rosyjską propagandą i odnosi się do wojny w Ukrainie i jej konsekwencji. Treści obejmują:
- podważanie ukraińskiego rządu i narodu: są oni przedstawiani jako „naziści", „skorumpowani" lub kłamcy, np. twierdzenie, że od początku wojny w Niemczech pojawiło się więcej nazistów pod wpływem ukraińskich uchodźców;
- wspieranie zniesienia sankcji wobec Rosji, ponieważ rzekomo mają one dramatyczny wpływ na europejskie społeczeństwa, którym grozi poważny niedobór żywności i energii, np. Niemcy będą musiały radzić sobie z mniejszą ilością świeżego chleba, masła i piwa, a cena gazu wzrośnie trzykrotnie;
- obejmuje założenie ponad 50 domen podszywających się pod autentyczne media, zakupionych między majem a wrześniem 2022 r.:
- w tym 17 mediów lub agencji informacyjnych, m.in. „Bild", „Ansa", „The Guardian" lub „20 Minutes";
- zawiera ślady około 80 fragmentów dezinformacji; pozostałe domeny mogły być wcześniej używane lub uśpione na potrzeby przyszłych operacji;

– działa w wielu językach: głównie niemieckim, następnie włoskim, francuskim, angielskim, łotewskim, ukraińskim i rosyjskim. Treść była trójskładnikowa:
- pierwsza składała się z artykułów dezinformacyjnych podszywających się pod dziennikarzy lub media;
- druga – z filmów dezinformacyjnych podszywających się pod autentycznych dostawców mediów. Zostały one wstawione wraz z tekstem dezinformacyjnym na sklonowane strony internetowe;
- ostatnia – z tendencyjnych ankiet prezentowanych tak, jakby pochodziły z wiarygodnych źródeł, jednak w rzeczywistości były promowane przez sklonowane media. Ich wątpliwe wyniki zostały później ponownie wykorzystane w innych zasobach;

– bazuje na podszywaniu się pod treści medialne: artykuły, domeny, strony internetowe i filmy z informacjami antyukraińskimi i prokremlowskimi. Polega na fabrykowaniu dezinformacji, zniekształcaniu wydarzeń, wymyślaniu zupełnie nowych lub sfabrykowanych internetowych sondaży opinii. Tego rodzaju historie można podsumować w 2 głównych kategoriach:
- „Ukraina jako państwo upadłe": narracja ta łączy zarzuty dotyczące korupcji w ukraińskich władzach z tezą o rzekomej obecności ideologii nazistowskiej w społeczeństwie, sugerując jednocześnie, że sami Ukraińcy preferowaliby życie w Rosji. W tym ujęciu podważana jest zasadność ponoszenia przez państwa europejskie znaczących nakładów finansowych na wsparcie Ukrainy.
- „Nadchodzi zima": wspierając Ukrainę i nie znosząc sankcji wobec Rosji, rządy zachodnie ponoszą odpowiedzialność za kontynuowanie wojny, a w konsekwencji – za pogarszanie warunków życia swoich obywateli: brak gazu, puste półki, brak chleba, masła i piwa.

Olga Wasiuta

A. Alaphilippe, Yet more evidence of Russia's boundless impunity to spread misinformation in the EU, 11.07.2024, https://www.disinfo.eu/publications/yet-more-evidence-of-russias-boundless-impunity-to-spread-misinformation-in-the-eu/ (dostęp 15.12.2025); A. Alaphilippe, G. Machado, R. Miguel, F. Poldi, *Doppelganger Media clones serving Russian propaganda*, Qurium, 27.09.2022, https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf (dostęp 15.12.2025); K. Chawryło, *„Doppelgänger" – schemat rosyjskiej operacji wpływu przeciwko Zachodowi*, 13.09.2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-09-13/doppelganger-schemat-rosyjskiej-operacji-wplywu-przeciwko-zachodowi (dostęp 16.12.2025); *Doppelganger strikes back: FIMI activities in the context of the EE*, 24.06.2024, https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf (dostęp 15.12.2025); *ELECTION REPORT Assessment of 1101 Foreign Information Manipulation and Interference in the 2025 Polish Presidential Election*, Alliance4Europe, Debunk.org, GLOBSEC, EU DisinfoLab, DFRLab, Institute for Strategic Dialogue (ISD), https://fimi-isac.org/wp-content/uploads/2025/08/FDEI-POLISH-ELECTION-COUNTRY-REPORT-2025-2.pdf (dostęp 15.12.2025); *Illegal Doppelganger Operation: Targeting the Polish Elections*, 17.04.2025, CDN, Reports, https://alliance4europe.eu/doppelganger-poland-elections (dostęp 15.12.2025); K. Jabłonowski, *Rosjanie ingerują w polskie wybory. Nowy raport*, 18.04.2025, https://www.tvp.info/86242761/kampania-dezinformacyjna-doppelganger-rosjanie-chca-ingerowac-w-polskie-wybory-prezydenckie (dostęp 16.12.2025); A. Jawor, *#CyberMagazyn: Rosyjski sobowtór. Jak Kreml prowadzi operacje wpływu?*, 30.03.2024, https://cyberdefence24.pl/cyberbezpieczenstwo/sobota-cybermagazyn-rosyjski-sobowtor-jak-kreml-prowadzi-operacje-wplywu (dostęp 16.12.2025); A. Mężyński, *Operacja „Doppelganger". Rosja wzięła Polskę na celownik przed wyborami, 25.04.2025,* https://forsal.pl/kraj/bezpieczenstwo/artykuly/9785098,operacja-doppelganger-rosja-wziela-polske-na-celownik-przed-wyboram.html (dostęp 16.12.2025); S. Palczewski, *Rosyjska operacja w Europie. Serwery ulokowane w Warszawie*, 12.07.2024, https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjska-operacja-w-europie-serwery-ulokowane-w-warszawie (dostęp 16.12.2025); J. Pamment, D. Tsurtsumia, *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*, Psychological Defence Agency, 12.05.2025, https://mpf.se/download/18.7cffbee41969f6d83e115221/1747230166207/Beyond%20Operation%20Doppelganger.pdf (dostęp 15.12.2025); *Rosyjska operacja „Doppelganger". Kreml atakuje Polskę przed wyborami prezydenckimi*, 2.05.2025, https://www.bankier.pl/wiadomosc/Rosyjska-operacja-doppelganger-Kreml-atakuje-Polske-przed-wyborami-prezydenckimi-8931031.html (dostęp 16.12.2025); D. Uhlig, *Akcja Doppelgänger. Ujawniamy, jak rosyjskie służby mieszały w Polsce*, https://demagog.org.pl/analizy_i_raporty/akcja-doppelganger-ujawniamy-jak-rosyjskie-sluzby-mieszaly-w-polsce/ (dostęp 16.12.2025).

ROSYJSKA OPERACJA DEZINFORMACYJNA „KYLO” (również projekt „Kylo”) – kryptonim tajnej wojny informacyjnej i kampanii dezinformacyjnej opracowanych w 2022 r. pod nazwą projekt „Kylo” przez rosyjską Służbę Wywiadu Zagranicznego (SWZ), do których dotarły i które ujawniły w raportach śledczych niemiecki dziennik „Der Spiegel” i niezależny rosyjski portal The Insider w oparciu o zhakowaną korespondencję SWZ.

Zaledwie kilka miesięcy po rozpoczęciu przez Rosję pełnej inwazji na Ukrainę, w maju 2022 r. grupa pracowników Służby Wywiadu Zagranicznego FR, której pracownicy działają pod przykrywką Międzynarodowego Centrum Bezpieczeństwa „Mirotworec”, ujawniła tę operację podczas zamkniętej dyskusji przy okrągłym stole w senacie Rosji. Informacje wskazywały, że Moskwa dążyła do prowadzenia na Zachodzie kampanii dezinformacyjnych na temat Ukrainy, „podsycania lęków egzystencjalnych i kreowania wrogości wobec (ukraińskich) uchodźców uciekających przed wojną”.

„Der Spiegel” i The Insider opublikowały artykuł śledczy zatytułowany *Operacja „Kylo”* ujawniający plany rosyjskiego wywiadu zagranicznego (SWZ) mające na celu manipulowanie zachodnią opinią publiczną. Raport, oparty na zhakowanej korespondencji funkcjonariuszy rosyjskiej Służby Wywiadu Zagranicznego, rzuca światło na wyrafinowaną strategię Kremla w zakresie prowadzenia „wojny informacyjnej” przeciwko Zachodowi. Wspólne śledztwo ujawniło rosyjski spisek szpiegowski, który miał na celu wywołanie „paniki i terroru” na Zachodzie.

Zhakowane dokumenty to wytyczne pracowników Służby Wywiadu Zagranicznego (następcy KGB), odpowiedzialnych za prowadzenie działań informacyjnych. Podstawowe założenie tej operacji to: „Moralność i etyka w działaniach nie gra żadnej roli”, zaś główni wykonawcy – agentura operacyjna i agentura wpływu, pożyteczni „idioci”.

Raport śledczy „Der Spiegel” i The Insider przedstawia kompleksowy obraz taktyk dezinformacyjnych SWZ i ich wpływu na społeczeństwa zachodnie. Analizując metody i cele SWZ, raport podkreśla wagę zrozumienia i przeciwdziałania takim szkodliwym działaniom.

Projekt „Kylo” koncentruje się na szerzeniu strachu i niepewności w celu destabilizacji rządów zachodnich i osłabienia wsparcia dla Ukrainy. Operacja ta wykorzystuje fałszywe instytucje pozarządowe do

organizowania demonstracji antyestablishmentowych i zaawansowane technologie, aby ominąć tradycyjne kanały medialne, a tym samym bezpośrednio wpływać na zachodnich odbiorców za pomocą kampanii dezinformacyjnych. Kontakty z rosyjską Służbą Wywiadu Zagranicznego (SWZ) zostały nawiązane za pośrednictwem oficera Michaiła Kolesowa, 45-letniego oficera SWZ. Operacja miała na celu „wprowadzenie nowego schematu do podejścia propagandowego Kremla", który był „systematyczny, ukierunkowany i aktywny, o charakterze ofensywnym", jak wynika z raportu. Oficer SWZ zasugerował, że zamiast forsować typowe prorosyjskie argumenty o konflikcie, operacja powinna „pogłębić wewnętrzne sprzeczności między elitami rządzącymi" na Zachodzie, w tym w USA, które wśród służb specjalnych znane są jako „główny przeciwnik" Rosji. Obejmowało to rekrutów SWZ tworzących fałszywe reklamy podszywające się pod nagłówki wiadomości, nieistniejące organizacje pozarządowe i strony internetowe, publikowanie manipulacyjnych treści na platformach społecznościowych, w tym YouTubie, oraz zatrudnianie osób do udziału w protestach na Zachodzie w celu ich filmowania i rozpowszechniania w internecie.

Wyciekłe dokumenty, przeznaczone dla różnych agencji rządowych, ujawniają strategię Kremla: szerzenie dezinformacji na drażliwe tematy zachodnie, publikowanie fałszywych informacji podszywając się pod radykalne ukraińskie i europejskie siły polityczne (zarówno prawdziwe, jak i stworzone na zlecenie), odwoływanie się do emocji – przede wszystkim strachu – zamiast do racjonalności oraz wykorzystywanie nowych platform internetowych zamiast przestarzałych, takich jak RT i Sputnik. Dokumenty szczegółowo opisują również lokalne kampanie przeciwko rosyjskim emigrantom, w tym próby zdyskredytowania osoby zbierającej fundusze dla Fundacji Antykorupcyjnej Aleksieja Nawalnego, która przeniosła się do Stanów Zjednoczonych. Te lokalne działania dezinformacyjne są częścią szerszej strategii mającej na celu osłabienie opozycji i ruchów opozycyjnych za granicą.

Operacja miała być całkowicie niezauważalna – bez żadnych powiązań z rosyjskimi służbami wywiadowczymi, ale to nie powstrzymało The Insider i jego partnera śledczego „Der Spiegel" przed powiązaniem jej z rosyjskimi służbami wywiadowczymi, a konkretnie – z Służbą Wywiadu

Zagranicznego, która zajmuje się szpiegostwem zagranicznym. Głównym celem, jak wynikało z serii wyciekłych maili i dokumentów, było podsycenie nastrojów antyrządowych na Zachodzie, osłabienie pozycji Zachodu w kontekście globalnego konfliktu i wzmocnienie własnej pozycji międzynarodowej. Wykorzystując zaawansowane technologie i narzędzia cybernetyczne, Rosja stara się wpływać na opinię publiczną na masową skalę, zwłaszcza w związku z poparciem Ukrainy, a kluczowymi emocjami, na których należało żerować, jak intonowali planiści SWZ, były „strach", „panika" i „horror" – kampania manipulacji psychospołecznej rodem z podręcznika z czasów zimnej wojny, opracowanego przez Departament D Pierwszego Zarządu Głównego KGB. „D" oznaczało dezinformację.

Architektem operacji był Kolesow, weteran rosyjskiego wywiadu zagranicznego z 20-letnim stażem. Przyznał on, że Rosja poniosła całkowitą porażkę w wojnie propagandowej z Zachodem od czasu pełnej inwazji i zaproponował nowe i aktywne działania mające na celu osłabienie wsparcia dla Ukrainy. 23 maja 2022 r. wysłał sobie mailem dokument w wordzie zatytułowany po prostu *Propaganda*. Wyglądało to na zarys prezentacji, którą miał wygłosić 3 dni później, podczas zamkniętego posiedzenia w senacie Rosji poświęconego „wojnie informacyjnej z Zachodem". Forum, któremu przewodził były radziecki dyplomata, a obecnie zaciekle antyzachodni senator Aleksiej Puszkow, zgromadziło rozpoznawalne media reżimu Władimira Putina, w tym rzeczniczkę Ministerstwa Spraw Zagranicznych, specjalistów od wojny psychologicznej z Ministerstwa Obrony oraz lojalnych wobec reżimu Putina dziennikarzy. Puszkow był poważnie zaniepokojony dominacją nastrojów proukraińskich na zachodnich platformach internetowych, zaledwie 6 miesięcy po rozpoczęciu wojny, która miała potrwać nie dłużej niż 3 dni. Kolesow zaproponował wykorzystać nieufność wobec ukraińskich uchodźców w Europie, wzmocnić argumenty, że stanowią oni obciążenie dla zachodnich rządów, i uszczuplić zasoby przeznaczone dla rdzennych mieszkańców.

Taktyka SWZ obejmuje publikowanie fałszywych informacji pod przykrywką radykalnych ukraińskich i europejskich sił politycznych, odwoływanie się do emocji – przede wszystkim strachu – zamiast racjonalności oraz wykorzystywanie nowych platform internetowych zamiast przestarzałych, takich jak RT i Sputnik.

Szczególnie wymowny fragment dokumentów podkreśla nacisk, jaki SWZ kładzie na wzbudzanie strachu w celu manipulowania percepcją społeczną. Według Kolesowa agencja miałaby opracować wskaźniki mierzące zaangażowanie użytkowników, w tym współczynniki klikalności, czas spędzony na czytaniu treści generowanych przez SWZ oraz publikowane komentarze. „Proponuje się, że motywem przewodnim naszej kampanii poznawczej w krajach (zachodnich) będzie wzbudzanie najsilniejszej emocji w ludzkiej psychice – strachu" – czytamy w dokumencie. „To właśnie strach o przyszłość, niepewność jutra, niezdolność do tworzenia długoterminowych planów, niepewny los dzieci i przyszłych pokoleń. Pielęgnowanie tych bodźców zalewa podświadomość jednostki paniką i przerażeniem".

Główne założenia projektu „Kylo" opierają się na psychologicznej manipulacji i wywoływaniu silnych emocji u odbiorców. Najważniejszym celem jest zaszczepienie w społeczeństwach zachodnich strachu i niepewności co do przyszłości. Operacja ma na celu:

- manipulowanie zachodnią opinią publiczną, w szczególności podsycanie nastrojów antyrządowych i sprzeciwu wobec wspierania Ukrainy;
- pogłębienie wewnętrznych sprzeczności w państwach zachodnich poprzez żerowanie na takich emocjach, jak „strach", „panika" i „przerażenie";
- szerzenie dezinformacji na wrażliwe tematy zachodnie w środowisku informacyjnym;
- wniknięcie/tworzenie organizacji pozarządowych, sił politycznych i podsycanie radykalnych nastrojów, które mają prowadzić narrację sprzeczną z racją stanu danego państwa, wywoływać wątpliwości i niechęć do prowadzonych działań obronnych;
- tworzenie sieci i grup ulegających teoriom spiskowym. Nadrzędnym sposobem działania jest odwoływanie się do emocji zamiast do racjonalnego myślenia. Działanie ma być systematyczne, ukierunkowane, aktywne, ofensywne;
- wywoływanie lęku o przyszłość ekonomiczną i bezpieczeństwo;
- wzbudzanie niepewności związanej z migracją oraz przyszłością dzieci i kolejnych pokoleń;

– prowokowanie antyrządowych protestów oraz obniżenie poparcia dla rządów i instytucji międzynarodowych.

Cele średnioterminowe obejmują dyskredytację Ukrainy i „nazistów nastawionych na nią w oczach zbiorowości Zachodu". Długoterminowym celem projektu jest podważenie stabilności politycznej państw zachodnich, osłabienie ich sojuszu z Ukrainą oraz doprowadzenie do spadku poparcia dla sankcji i pomocy wojskowej dla tego kraju. Wyciekłe dokumenty SWZ ujawniły systematyczne podejście mające na celu całkowite ukrycie powiązań z rosyjskimi służbami wywiadowczymi.

Kluczowe taktyki operacji „Kylo" obejmowały:

– podawanie się za legalne podmioty: plan zakładał stworzenie strony internetowej fałszywie oznaczonej jako „niezależna agencja śledcza", która miała służyć jako centrum informacyjne dla manipulacyjnych treści generowanych przez SWZ, w tym materiałów drukowanych, audio i wideo, przeznaczonych na platformy takie jak YouTube i TikTok;
– wykorzystanie nowych platform: operacja kładła nacisk na nowoczesne środki komunikowania, media społecznościowe i inne nowe platformy internetowe, takie jak TikTok, YouTube, Facebook oraz Telegram, które miały być pod kontrolą Kremla; a nie przestarzałe, kontrolowane przez państwo kanały, takie jak RT i Sputnik. Projekt zakładał wykorzystanie „unikalnego algorytmu" i specjalnego oprogramowania do masowego atakowania urządzeń elektronicznych użytkowników tymi treściami. Tworzone są krótkie, atrakcyjne wizualnie treści, które łatwo się rozprzestrzeniają i trafiają do szerokiej publiczności. Treści te często podsycają negatywne emocje, takie jak strach i niepewność. Dużą rolę odgrywają reklamy wyświetlane w social mediach spersonifikowane pod konkretnych użytkowników. Ten punkt jest bardzo istotny, bo to właśnie social media stają się głównym narzędziem wykorzystywanym w wojnie w sieci;
– ataki cybernetyczne: wykorzystywane są również cyberataki, takie jak fałszywe ostrzeżenia o zagrożeniach bezpieczeństwa, które mają na celu wywoływanie paniki w krajach zachodnich.

Przykładem jest zakłócanie przygotowań do igrzysk olimpijskich w Paryżu w 2024 r.;
- tworzenie fałszywych organizacji pozarządowych (NGO's), stron internetowych i mediów, które udają niezależne źródła informacji i mają wpływać na zachodnią opinię publiczną;
- zaawansowane algorytmy: SWZ opracowało specjalne oprogramowanie oraz algorytmy, które pozwalają na efektywne targetowanie treści do określonych grup odbiorców. Algorytmy te śledzą zaangażowanie użytkowników oraz dopasowują treści w zależności od ich preferencji;
- odwoływanie się do emocji, a nie racjonalności: strategia koncentrowała się na manipulacji psychologicznej, wyraźnie celując w „strach", „panikę" i „przerażenie", a funkcjonariusze SWZ opracowywali wskaźniki mierzące zaangażowanie użytkowników (np. współczynniki klikalności, czas spędzony na czytaniu treści generowanych przez SWZ oraz publikowane komentarze, aby ocenić skuteczność kampanii) za pomocą treści wywołujących strach;
- protesty i prowokacje: w ramach projektu organizowane są fikcyjne protesty, w których uczestniczą opłacani demonstranci w różnych miastach europejskich (np. w Paryżu, Brukseli, Madrycie), aby symulować powszechne nastroje antyukraińskie, które następnie byłyby filmowane i rozpowszechniane w mediach w celu stworzenia wrażenia szerokiego niezadowolenia społecznego;
- maskowanie pochodzenia: treści miały być publikowane, podczas gdy agenci podszywali się pod radykalne siły polityczne z Ukrainy lub Europy, aby jeszcze bardziej ukryć rosyjskie pochodzenie;
- ignorowanie etyki: wewnętrzne dokumenty wyraźnie stwierdzały, że „moralność i etyka nie powinny odgrywać żadnej roli" w tej wojnie psychologicznej.

W czasie, gdy niektórzy zachodni politycy sugerowali, że ukraińscy uchodźcy, którzy uciekli przed wojną, stają się obciążeniem dla zasobów państwa, rekruci SWZ próbowali wykorzystać sytuację, tworząc fałszywe

strony internetowe z wiadomościami i publikując artykuły z nagłówkami: „Jak Ukraińcy okradają Niemcy z dobrobytu gospodarczego". Setki tysięcy kont w mediach społecznościowych próbowało skierować internautów do tych stron, publikując obrazy z „sensacyjnymi hasłami", takimi jak „Niemcy popadają w bezdomność" i „Nawet chleb jest luksusem", a następnie zamieszczając do nich linki. „To właśnie strach o przyszłość, niepewność jutra, niemożność tworzenia długoterminowych planów, niepewny los dzieci i przyszłych pokoleń. Pielęgnowanie tych bodźców zalewa podświadomość jednostki paniką i przerażeniem".

Nowa propozycja Kolesowa sformułowana sztucznym językiem – w równym stopniu łączącym teorię krytyczną, pseudonaukę i żargon marketingowy – miała zatem na celu wplecenie nowego schematu w kremlowską propagandę: „systematyczną, ukierunkowaną, aktywną i ofensywną". Zamiast przedstawiać proste prorosyjskie argumenty, zasugerował, że SWZ powinna teraz dążyć do „pogłębienia wewnętrznych sprzeczności między elitami rządzącymi" na Zachodzie poprzez stworzenie fałszywej organizacji pozarządowej – w rzeczywistości podstawionej organizacji finansowanej i zarządzanej przez agentów Kremla – w celu wzniecenia antyestablishmentowych demonstracji na terytorium „glawnego protiwnika", czyli „głównego przeciwnika", jak Stany Zjednoczone nazywane są w rosyjskich służbach specjalnych, a także w państwach „satelitarnych".

Fałszywe reklamy podszywające się pod nagłówki wiadomości, wszystkie stworzone przez rekrutów SWZ, byłyby widoczne na niemal każdym ekranie komputera stacjonarnego lub urządzeniu mobilnym używanym przez odbiorców docelowych na Zachodzie, zachęcając ich do kliknięcia i przejścia do „zasobów internetowych kontrolowanych przez nas". Jedną ze strategii Kolesowa było sprawianie wrażenia bardziej proukraińskiego niż legalne grupy społeczeństwa obywatelskiego, wysuwanie wygórowanych żądań w sprawie ukraińskich uchodźców, aby obrona ich interesów była postrzegana jako niesprawiedliwa.

„Prowadzenie wojen sieciowych w cyberprzestrzeni UE w oparciu o rosnące żądania ukraińskich migrantów i nowe fale irytacji lokalnej ludności, wywołane tym faktem, według wstępnych szacunków, będzie bardzo skuteczne zarówno teraz, jak i w dającej się przewidzieć przyszłości". Ta metoda przejmowania kontroli nad sprawą od wewnątrz, a następnie

dyskredytowania jej od wewnątrz poprzez ekstremistyczne pozowanie jest dla rosyjskich służb specjalnych uświęconym rzemiosłem.

Wykorzystanie przez SWZ kwestii uchodźców nie było jedynie teoretyczne. Niemieckie władze zidentyfikowały ponad 20 pozornie legalnych portali informacyjnych, które odpowiadały właśnie na te obawy, z artykułami zatytułowanymi (płynnym niemieckim) „Jak Ukraińcy okradają Niemcy z dobrobytu gospodarczego". Berlin ustalił, że portale te są częścią szeroko zakrojonej operacji rosyjskich wpływów, podobnie jak setki tysięcy kont w mediach społecznościowych, które publikują kafle ze zdjęciami z sensacyjnymi hasłami rodem z epoki weimarskiej – „Niemcy popadają w bezdomność", „Nawet chleb jest luksusem" – odsyłającymi do fałszywych serwisów informacyjnych.

Kolesow podzielił się swoim projektem wniosku z innym oficerem SWZ Michaiłem Kuleminem, którego awatar na WhatsAppie, w karykaturalnej wersji „niewykrywalności", przedstawia Jamesa Bonda. W rzeczywistości między majem 2022 a wrześniem 2023 r. wymienili się ponad 10 wersjami projektu „Kylo", a w jednym przypadku, 29 maja 2023 r., przesłali kopię Eduardowi Czernowolcewowi, szefowi służby naukowo-technicznej FSB, rosyjskiej służby bezpieczeństwa wewnętrznego, która nadzoruje m.in. główną jednostkę hakerską FSB oraz Instytut Nauk Sądowych, organ produkujący trucizny takie jak nowiczok, wojskowy środek paralityczno-drgawkowy używany w próbach zabójstw Siergieja Skripala i Aleksieja Nawalnego.

Najbardziej rozbudowana wersja projektu „Kylo" pojawiła się 9 stycznia 2023 r. i była oznaczona dziwacznym napisem „SVR-Project" łączącym cyrylicę i język angielski, gdzie rosyjska litera „W" („V") to logo bitcoina, a „O" w słowie „project" to kula ziemska, niemożliwie zapożyczona wprost z emblematu SWZ.

Zgodnie z tym dokumentem SWZ miała rekrutować zespoły do pracy w różnych krajach docelowych; obejmowała ona nie tylko materiały drukowane, ale także audio i wideo udostępniane na YouTubie i innych platformach społecznościowych – łączone w „krótkie filmy" publikowane raz lub 2 razy dziennie, prawdopodobnie w celu łatwiejszego odbioru, jak na TikToku. Linki do treści generowanych przez SWZ są wbudowywane w elektroniczne środki komunikacji grupy docelowej za pomocą

unikalnego algorytmu opartego na nowym module platformy Storm i specjalnym oprogramowaniu.

Koszt takiej operacji wpływu jest określany jako dość niski: 3 dolary za użytkownika miesięcznie. Co ciekawe, w 2023 r. w całej Europie doszło do wielu sponsorowanych przez Rosję prowokacji, pozornie zgodnych z operacją „Kylo". Badania przeprowadzone przez europejskie konsorcjum medialne ujawniły, że grupa rosyjskich najemników stale pojawiała się na protestach w dużych miastach, takich jak Paryż, Bruksela, Madryt i Haga, potępiając zachodnie dostawy broni na Ukrainę. Konsorcjum stwierdziło, że mężczyźni ci zostali prawdopodobnie wynajęci przez rosyjskie służby specjalne. Okazało się nawet, że jeden z nich to student z Petersburga szukający w internecie, jakby dosłownie podążając za wskazówkami Kolesowa, ochotników, którzy mieliby zostać sfotografowani za 80–100 euro. Zdjęcia miały być wykorzystywane w mediach społecznościowych, aby zasygnalizować, że protesty antyukraińskie są masowym zjawiskiem w Europie.

Docelową grupę odbiorców w Służbie Wywiadu Federacji Rosyjskiej podzielono na 2 kategorie: „racjonalną" (20–30%) i „kognitywną" (70–80%). Aby wpłynąć na pierwszą grupę, wykorzystuje się materiały potwierdzające i opowiadające o wydarzeniach, które naprawdę miały miejsce. Natomiast na większość ludzi Rosja wpływa poprzez emocje. „Odwołanie się nie do rozumu, ale do emocji, właśnie do irracjonalnego składnika zmysłowej i psychologicznej percepcji człowieka, przyczynia się do najszybszego i najpewniejszego osiągnięcia celów postawionych przed machiną propagandową" – stwierdzono w opublikowanych dokumentach rosyjskiego wywiadu.

9 września 2024 r. Sztab Generalny Wojska Polskiego poinformował o wycieku informacji na temat rosyjskiej operacji „Kylo". Ujawnione dokumenty potwierdzają stałe i systematyczne działania Rosji mające na celu szerzenie dezinformacji i propagandy w USA i krajach europejskich, m.in. w Polsce. **W**ojskowi ostrzegli „przed uleganiem narracjom propagowanym przez nowe ruchy i teorie spiskowe, nawołujące do wyłączenia Polski ze wsparcia Ukrainy". Według komunikatu wojska metodą działania rosyjskich służb było tworzenie, przejmowanie i radykalizowanie działań

różnych grup i organizacji. W Polsce zauważono takie prorosyjskie grupy, jednak z uwagi na prawne ograniczenia nie podano ich nazw.

Projekt „Kylo" to chyba pierwsze ujawnione całościowe podejście do tematyki wojny w sieci przy relatywnie niskich nakładach, co pozwala osiągnąć duże efekty i realnie wpływać na całe społeczeństwa.

Działania te mają jeszcze jedną cechę: zmuszają przeciwnika do wydawania potężnych nakładów finansowych. Jako przykłady możemy wskazać:

- sytuację na granicy polsko-białoruskiej;
- podpalenia w Polsce mające wytworzyć atmosferę strachu i przerażenia;
- podsycanie protestów na granicy Polski z Ukrainą: zaostrzają wewnętrzne niepokoje, podważają zaufanie do rządu oraz instytucji Unii Europejskiej;
- ataki cybernetyczne, np. na PAP i zamieszczenie fałszywej depeszy informującej o mobilizacji.

Olga Wasiuta

I.I. Berman, N. Sturza, *Information Warfare Watch No. 36*, 30.07.2024, https://www.afpc.org/publications/bulletins/information-warfare-watch/information-warfare-watch-no-36 (dostęp 22.11.2025); I. van Brugen, *Russian Spy Plot To Sow 'Panic and Terror' in US Leaked in Bombshell Report*, 5.07.2024, https://www.newsweek.com/russia-spy-plot-project-kylo-us-west-1921545 (dostęp 20.11.2025); M. Bruno, *Russian Disinformation Campaigns Dismantled by International Law Enforcement*, 22.07.2024, https://www.dyami.services/post/russian-disinformation-campaigns-dismantled-by-international-law-enforcement (dostęp 20.11.2025); *Był przeciek: operacja "Kylo"*, 9.09.2024, https://www.facebook.com/SztabGenWP/posts/by%C5%82-przeciek-operacja-kylo-wyp%C5%82yn%C4%99%C5%82y-dokumenty-kt%C3%B3re-potwierdzaj%C4%85-ci%C4%85g%C5%82e-i-syste/562767422758841/ (dostęp 22.11.2025); R. Dobrokhotov, C. Grozev, M. Rosenbach, F. Schmid, W. Wiedmann-Schmidt, *So manipulieren Moskaus Agenten die deutsche Debatte über den Ukrainekrieg*, 4.07.2024, https://www.spiegel.de/politik/propaganda-so-manipulieren-russische-agenten-die-deutsche-debatte-ueber-den-ukrainekrieg-a-5c0203d4-b10e-45a8-86f7-a26ce9a817c3 (dostęp 22.11.2025); Ch. Grozev, R. Dobrokhotov, M.Weiss, *"Morality and ethics should play no part": Leaks reveal how Russia's foreign intelligence agency runs disinformation campaigns in the West*, 4.07.2024, https://theins.ru/en/politics/272870 (dostęp 22.11.2025); M.

Joshi, *Explosive Russian Spy Plot Uncovered: Projekt Kylo's Scheme to Incite Panic in the US*, 7.07.2024, https://regtechtimes.com/explosive-russian-spy-plot-uncovered-project-kylo/ (dostęp 25.11.2025); S. Pamfleti, *How Russia's foreign intelligence agency runs disinformation campaigns in the West*, 8.07.2024, https://pamfleti.net/english/bota/si-agjencia-e-jashtme-e-inteligjences-ruse-drejton-fushatat-e-keqinformimit-i235273 (dostęp 25.11.2025); *Post Sztab Generalny WP, 9.09.2024,* https://x.com/SztabGenWP/status/1833026717239378138 (dostęp 22.11.2025); *„Projekt Kylo" – ciemna strona mocy w wojnie w sieci*, https://spolecznosc.payload.pl/projekt-kylo-ciemna-strona-mocy-w-wojnie-w-sieci-22266801.html (dostęp 19.11.2025); *Russian Spy Plot Revealed in Joint Investigation*, 6.07.2024, https://www.sofx.com/russian-spy-plot-revealed-in-joint-investigation/ (dostęp 25.11.2025); M. Seldon, *New Investigative Report By Der Spiegel and The Insider Unveils Russia's Disinformation Tactics: "Operation Kylo"*, 8.07.2024, https://www.hstoday.us/subject-matter-areas/cybersecurity/new-investigative-report-by-der-spiegel-and-the-insider-unveils-russias-disinformation-tactics-operation-kylo/ (dostęp 22.11.2025); A. Verkhovetska, *Rosja prowadzi w Polsce operację dezinformacyjną, której celem jest szerzenie wśród społeczeństwa strachu przed ukraińskimi uchodźcami*, 27.11.2024, https://pl.naszwybir.pl/operacja-dezinformacyjna/ (dostęp 19.11.2025); Ю. Кириченко, *Росія проводить у Польщі дезінформаційну операцію з метою поширити серед населення страх щодо українських біженців*, 12.09.2024, https://naszwybir.pl/kylo/ (dostęp 20.11.2025).

ROSYJSKA OPERACJA DEZINFORMACYJNA „MATRIOSZKA" – strategia dezinformacyjna wymierzona w media i organizacje zajmujące się weryfikacją faktów, prowadzona przez Rosję w celu szerzenia dezinformacji i manipulowania opinią publiczną w krajach europejskich, w tym w Mołdawii, Niemczech i Francji, pod którą kryje się wiele warstw na różnych poziomach. Nazwa operacji nawiązuje do tradycyjnych rosyjskich lalek, w których wnętrzu znajdują się mniejsze lalki. Co ciekawe, całość ma znamiona skoordynowanej operacji.

W przeciwieństwie do innych strategii dezinformacyjnych i ingerencji w media społecznościowe koncentruje się ona nie na indywidualnych użytkownikach i profilach, ale na mediach i weryfikatorach faktów, co stwarza przeciążenie informacjami i ułatwia rozprzestrzenianie się dezinformacji w cyfrowym ekosystemie.

Operacja miała wystartować, według badaczy, w maju 2022 r. i od tego czasu ciągle ewoluuje. Początkowo działania te koncentrowały się

na Twitterze (obecnie funkcjonującym pod nazwą X), gdzie powiązane z kampanią konta rozpowszechniały linki do dezinformujących artykułów rosyjskojęzycznych stron. Na początku operacja „Matrioszka" polegała głównie na rozpowszechnianiu fałszywych graffiti i postów podszywających się pod wizualną tożsamość zachodnich mediów, instytucji i organizacji pozarządowych. Do tej pory treści te zostały opublikowane w języku francuskim, angielskim, włoskim, niemieckim, rosyjskim i ukraińskim.

Pierwotny styl działania funkcjonował do sierpnia 2022 r.; wtedy bowiem powiązane konta zaczęły rozsiewać rosyjską propagandę na „skalę przemysłową". W sierpniu 2022 r. kampania przeszła reformę, rozszerzając swoje działania na inne platformy, takie jak Facebook, YouTube, TikTok i Instagram. Wykorzystywano deepfake'i oraz organizowano spotkania i konferencje, które sprawiały wrażenie rzetelnych, aby zmylić odbiorców. Same portale z rosyjską dezinformacją, które przypominają rzeczywiste serwisy informacyjne, a są wykorzystywane w ramach „Matrioszki", funkcjonują m.in. dzięki przekierowaniom czy botom.

Operacja „Matrioszka", jak twierdzą eksperci, to „ogromne przedsięwzięcie dywersyjne" wymierzone w dziennikarzy. Kampania ta nie tylko polega na rozpowszechnianiu fałszywych wiadomości o podłożu antyukraińskim, ale także na rzucaniu wyzwań zachodnim mediom, aby je weryfikowały. Wydaje się, że jest to element wojny Rosji z Ukrainą, która toczy się od 2022 r. i która pochłonęła dziesiątki tysięcy istnień ludzkich.

Działalność danej operacji polega na publikowaniu fałszywych treści (raportów, graffiti, memów itp.), które są następnie rozpowszechniane w skoordynowany sposób w odpowiedzi na posty publikowane w sieci X przez media, słynne osoby i serwisy weryfikujące fakty z ponad 60 krajów. Organizatorzy kampanii „Matrioszka" kontaktują się bezpośrednio ze swoimi adresatami w sieci X lub za pośrednictwem poczty elektronicznej, prosząc ich o weryfikację fałszywych treści. Służy to rozpowszechnianiu i wzmacnianiu przede wszystkim antyukraińskiej narracji, ale atakuje również europejską politykę wsparcia Ukrainy i wiele europejskich osobistości politycznych. Gdy weryfikatorzy odmawiają, Rosjanie oskarżają ich o cenzurę, podsycając swoją narrację o braku rzetelności mediów. Z kolei w przypadku, gdy fact-checkerzy podejmują

się sprawdzenia fałszywych informacji, ich uwaga zostaje rozproszona, co również działa na korzyść Rosjan.

Główne cele i metody operacji:

- sianie niezgody, podważanie zaufania do instytucji demokratycznych i wpływanie na wyniki wyborów;
- podszywanie się pod legalne media: operacja „Matrioszka" działa w ukryciu, podszywając się pod autentyczne zagraniczne media, wykorzystując botnety i fałszywe konta, aby szerzyć propagandę i dezinformację oraz zdyskredytować proeuropejski kurs wybranych krajów;
- dyskredytacja mediów, osób publicznych i organizacji zajmujących się weryfikacją faktów będących celem ataku oraz promowanie treści prorosyjskich;
- wykorzystanie różnorodnych taktyk, w tym deepfake'ów stworzonych z wykorzystaniem sztucznej inteligencji w celu wzmocnienia przekazów propagandowych. Pojawiły się również doniesienia o finansowaniu przez Rosję osób (np. księży w Mołdawii) w celu wpływania na wyborców za pośrednictwem mediów społecznościowych;
- nasilenie działań przed ważnymi wyborami w różnych krajach, w szczególności wywarcie wpływu na wybory parlamentarne w Mołdawii (wrzesień 2025 r.), aby zdyskredytować proeuropejskie stanowisko kraju i jego przywódców, takich jak prezydent Maia Sandu;
- rozpowszechnianie narracji skierowanych przeciwko Ukrainie (np. przedstawiających ukraińskich uchodźców jako „chciwych" lub „niewdzięcznych") oraz wsparciu Zachodu dla tego kraju. Pogłoski o skandalach korupcyjnych i drażliwych kwestiach społecznych, takich jak rocznica zamachów w Paryżu w 2015 r., również były wykorzystywane do siania podziałów we francuskim społeczeństwie;
- rozpowszechnianie fałszywych informacji mających na celu zdyskredytowanie przywódców innych krajów (np. prezydenta Francji Emmanuela Macrona i prezydenta Ukrainy

Wołodymyra Zełenskiego), podsycanie wewnętrznych podziałów i podważanie zaufania do instytucji demokratycznych;
- tworzenie materiałów propagandowych w taki sposób, aby sprawiały wrażenie wewnętrznej krytyki lub dyskusji w kraju docelowym, a nie ingerencji zewnętrznej;
- wykorzystywanie istniejących luk w zabezpieczeniach, takich jak skandale korupcyjne czy niepokoje społeczne, aby wzmocnić swoje wpływy.

W styczniu 2024 r. AFP Factuel, francuska spółka zależna AFP Fact Check (dział weryfikacji faktów francuskiej agencji informacyjnej Agence France-Presse, która publikuje w kilku językach), we współpracy z Antibot4Navalny (grupa specjalizująca się w analizie operacji wpływu Rosji na sieci społecznościowe, która zaproponowała termin operacja „Matrioszka"[35], nawiązując do lalek układanych jedna w drugiej) przedstawiła dowody uzasadniające istnienie tej strategii funkcjonującej co najmniej od września 2023 r. Od tego czasu cała sieć, na której opiera się ta strategia, została ujawniona.

Konta, wykorzystywane w ramach operacji „Matrioszka", działają na platformach społecznościowych, takich jak X, które proszą różne oficjalne profile o weryfikację publikowanych informacji. Po przeanalizowaniu tych treści okazuje się, że to samo konto już wcześniej sprawdziło ich prawdziwość, a później publikuje ono treści z zamiarem rozpowszechniania dezinformacji, zaś inne profile proszą o weryfikację nowych materiałów. Cykl ten powtarza się aż do momentu zidentyfikowania pierwotnego konta, które rozpowszechniło fałszywe informacje. Treści są zazwyczaj krytyczne wobec Ukrainy, NATO, wydatków wojskowych USA oraz innych państw wspierających Ukrainę.

---

[35] Nazwę tę nadała rosyjska grupa Antibot4Navalny, działająca w Rosji w sieci X od 2018 r., która identyfikuje rosyjskie boty: https://twitter.com/antibot4navalny. Kampania została udokumentowana również przez Agence France Presse (międzynarodowa agencja informacyjna o charakterze ogólnym i multimedialnym założona w sierpniu 1944 r. w Paryżu), https://factuel.afp.com/doc.afp.com.34H32VP. Natomiast fińska firma ChechFirst, która specjalizuje się w analizie danych i badaniach dla zwalczania dezinformacji i manipulacji, zwłaszcza w internecie, nadała jej nazwę operacja „Overload", https://checkfirst.network/wpcontent/uploads/2024/06/Operation_Overload_WEB.pdf.

Eksperci zgadzają się, że wśród motywacji odpowiedzialnych za tę kampanię jest chęć odwrócenia uwagi mediów i skłonienia ich do marnowania czasu i zasobów na nieistotne śledztwa, jak ma to miejsce w przypadku Antibot4Nawalny, który przypisuje tę strategię prorosyjskim aktorom.

Operacja „Matrioszka" od miesięcy próbuje manipulować aktywnością głównych mediów i zespołów specjalizujących się w walce z dezinformacją, stosując fałszywe ostrzeżenia o oszustwach w mediach społecznościowych oraz żądania dochodzenia. Setki mediów, w tym korporacje takie jak brytyjskie BBC i amerykańskie CNN, były celem tych działań, zwłaszcza jeśli chodzi o weryfikacje faktów. Nie jest to więc treść wirusowa, lecz wiadomości wysyłane do samych mediów nadają im istotność, bez możliwości ustalenia, czy ich pochodzenie jest prawdziwe.

Agencja informacyjna EFE Verifika[36] regularnie otrzymywała dużą ilość próśb mailowych o zbadanie wiadomości tekstowych, fotografii i filmów napisanych po angielsku, oraz z adresów oznaczonych anglosaskimi nazwiskami, od końca grudnia 2023 r. Poprzez porównanie podejrzanych spraw z bazą danych Antibot4Navalny, która zebrała w ciągu kilku miesięcy na przełomie lat 2023/2024 co najmniej 550 publikacji tego typu, potwierdzono, że te same relacje kwestionowały inne media, instytucje i osoby publiczne. Według Antibot4Navalny operacja „Matrioszka" stara się również przeanalizować reakcję weryfikatorów faktów na prośby o identyfikację fałszywych informacji.

Operacja „Matrioszka", która jest aktywnie prowadzona na platformie X co najmniej od września 2023 r., charakteryzuje się dwuetapowym modelem operacyjnym:

- pierwsza grupa kont, tzw. „seederzy" (siewniki), publikuje fałszywe treści;
- druga grupa kont, tzw. „cytujący", repostuje wpisy „seedera" w odpowiedzi na posty mediów, celebrytów i serwisów weryfikujących fakty.

[36] Agencja informacyjna EFE (jedna z głównych hiszpańskich agencji prasowych) prowadzi usługę o nazwie EFE Verifica, która zajmuje się weryfikacją informacji i zwalczaniem dezinformacji (fake newsów). Jest to usługa dziennikarska, a nie rządowa czy finansowa.

„Cytujący” kontaktują się z wybranymi osobami lub organizacjami, prosząc o weryfikację autentyczności lub wiarygodności treści publikowanych przez „seederów”. Od września 2023 do czerwca 2024 r. operatorzy kampanii „Matrioszka” przeprowadzili co najmniej 90 operacji, podczas których udoskonalali i przetestowali różne metody rozpowszechniania treści i zwracania na nie uwagi wśród odbiorców.

Operacje zazwyczaj obejmują 2 lub 3 konta „seederów”, które stanowią główne źródło treści rozpowszechnianych w odstępie kilku minut w sieci X. Po około 30–40 minutach 2 lub 3 konta cytujących zaczynają udostępniać te wpisy, komentując najnowsze. Osoby cytujące często dodają tekst, reakcje wyrażane słowami lub emotkami, albo po prostu wspominają odbiorcę, a każdy taki dodatek jest unikalny dla danej operacji i cytującego. Drugi etap trwa zazwyczaj kilka godzin, a przerwy między repostami wynoszą średnio 45 sekund.

VIGINUM zidentyfikował błędy, które najprawdopodobniej nie wystąpiłyby, gdyby zostały zautomatyzowane, w tym:

- użycie przez cytującego tekstu innego cytującego podczas tej samej operacji;
- użycie błędnych tagów w postach niektórych cytujących;
- literówki i błędy w niewielkiej liczbie postów cytujących;
- ponowne opublikowanie w wątku komentarzy zamiast odpowiedzi na post adresata.

Co więcej, konta X biorące udział w kampanii „Matrioszka” są wykorzystywane do przeprowadzania kilku kolejnych operacji, przy czym konto cytującego niemal systematycznie staje się kontem siewcy i odwrotnie. Poza schematem rozpowszechniania, operacja dezinformacyjna „Matrioszka” zmieniała się kilkakrotnie od momentu jej powstania, prawdopodobnie w celu przetestowania skuteczności nowych metod. VIGINUM zidentyfikował posty automatycznie tłumaczone na chiński, reposty udostępniane przez „seederów” oraz modyfikacje w profilach kont zaangażowanych w kampanię.

Co więcej, od września 2023 do lutego 2024 r. większość kont „seederów” i „cytujących” została najwyraźniej zakupiona od wyspecjalizowanej firmy. Kilka tygodni przed wykorzystaniem w kampanii „Matrioszka” nazwy profili kilku kont były powiązane z WebMasterMarket, firmą

sprzedającą m.in. konta w sieci X. Miały one również wspólne cechy, takie jak powiązania z osobami pochodzenia azjatyckiego, starą datę utworzenia oraz niedawne posty promujące zasoby cyfrowe, takie jak memecoiny[37].

Użyte konta zostały utworzone na krótko przed rozpoczęciem kampanii, a wszystkie profile zawierają sztucznie wygenerowane zdjęcia, brakuje natomiast informacji o użytkowniku i lokalizacji, nie ma też obserwujących oraz subskrybentów.

Na chwilę obecną VIGINUM uważa, że konta używane w kampanii „Matrioszka" mogły zostać zakupione przez jej operatorów od różnych grup, a nawet zhakowane. Niektóre media publicznie poinformowały o otrzymaniu maili z zaproszeniem do przeglądania treści publikowanych w Telegramie lub na stronach internetowych powiązanych z ekosystemem „Prawda". Wiadomości te zostały wysłane przez operatorów kampanii „Matrioszka", aby zwrócić uwagę wybranych osób na fałszywe treści; w międzyczasie mogą oni lepiej analizować ich działania i stosowane przez nich metody, a tym samym świadomie i skutecznie generować dezinformację.

Antibot4Navalny bezpośrednio oskarża prorosyjskich aktorów o tworzenie kont w celu przeprowadzenia tego procesu, głównie za pośrednictwem poczty elektronicznej. Te fałszywe ostrzeżenia o oszustwach w wiadomościach publikowanych przez renomowane podmioty generują fałszywy alarm, który rozpowszechnia dezinformację o zagrożeniach związanych z mechanizmami kontroli informacji. Wśród mediów objętych operacją „Matrioszka" znajdują się m.in. EFE, BBC i CNN EFE.

Chociaż media i osoby weryfikujące fakty odgrywają kluczową rolę w naszym społeczeństwie, potencjalne ryzyko destabilizacji, na jakie są narażone, jest niepokojące. Należy zauważyć, że wszystkie publikowane wiadomości przechodzą proces analizy i weryfikacji faktów, zanim zostaną

[37] Memecoin to kryptowaluta oparta na internetowym memie, żarcie lub zjawisku kulturowym, której wartość wynika z popularności w mediach społecznościowych, a nie z jakiejkolwiek technologii. Przykładami są dogecoin i shiba inu, których popularność jest w dużej mierze napędzana marketingiem wirusowym i rekomendacjami celebrytów, takich jak Elon Musk. Memcoiny są bardzo zmienne i niosą ze sobą znaczne ryzyko, ale ich prostota i wirusowy charakter przyciągają wielu początkujących inwestorów.

ostatecznie rozstrzygnięte. Dlatego operacja „Matrioszka" zakłóca ten porządek, maksymalnie wykorzystując czas, jaki media poświęcają na odkrywanie prawdy.

Śledztwo przeprowadzone przez VIGINUM ujawniło, że wiele rozpowszechnianych treści zostało wcześniej opublikowanych przez rosyjskie kanały Telegram, uwikłane w manipulowanie informacjami. Oczywistym celem kampanii jest podważenie zaufania do niektórych mediów, publicznych osób i serwisów zajmujących się weryfikacją faktów, przy jednoczesnym rozpowszechnianiu treści służących interesom Rosji.

VIGINUM uważa, że głównym celem operacji „Matrioszka" jest zdyskredytowanie zachodnich osobistości i mediów zaangażowanych w weryfikację faktów, jeśli zareagują na fałszywe treści. Jest skierowana do podmiotów, na których posty odpowiadają konta powiązane z kampanią. Według danych zebranych przez VIGINUM każda operacja jest skierowana do 50–150 podmiotów i osób w serwisie X; większość z nich to media (AFP, BBC, USA Today), organizacje zajmujące się weryfikacją faktów lub zwalczaniem dezinformacji (EU Disinfo Lab, program France 24 „Info ou Intox", Fact Check Bulgaria) oraz osoby pracujące dla tych organizacji lub zajmujące się weryfikacją faktów.

VIGINUM zaobserwował również, że działania związane z daną operacją były skierowane przeciwko uniwersytetom, funduszom inwestycyjnym, organizacjom międzynarodowym, organom rządowym i partiom politycznym. Chociaż operatorzy regularnie aktualizują listę swoich celów, niektóre organizacje i osoby wydają się mimo to niemal systematycznie atakowane, zwłaszcza krajowe i międzynarodowe agencje prasowe.

W sumie VIGINUM zidentyfikował ponad 500 różnych kont X, które były celem ataków od początku kampanii we wrześniu 2023 r. Chociaż najbardziej ucierpiały kraje zachodnie, kampania „Matrioszka" objęła swoim zasięgiem również instytucje w Ukrainie, na Bałkanach, Kaukazie, Bliskim Wschodzie, w Ameryce Łacińskiej, Azji i Afryce, a także amerykańską i irańską opozycję. Wśród tych celów znajduje się co najmniej 40 francuskich kont X, w tym mediów, organizacji zajmujących się weryfikacją faktów, osób publicznych i organów rządowych.

W każdym kraju organizacje i osoby publiczne są atakowane w tej samej kolejności, co sugeruje, że operatorzy korzystają z ustalonej listy. VIGINUM zidentyfikował błędy, które potwierdzają teorię, że konta są zarządzane ręcznie. W swoim dochodzeniu określił wspólne cechy stosowania sztucznych procedur (operacji koordynowanych między fałszywymi kontami) w schemacie kampanii.

„Matrioszka" rozpowszechnia 3 rodzaje treści podszywających się pod media, instytucje i organizacje pozarządowe:

- reportaże wideo z nieprawdziwą treścią wykorzystujące identyfikację wizualną i czcionki organizacji. To fałszywe doniesienia tworzone z wykorzystaniem darmowych zdjęć stockowych i muzyki;
- fałszywe zrzuty ekranu prezentujące fragment artykułu, relację z Instagrama lub krótki film z YouTube'a odnoszące się do mediów, organizacji lub osoby;
- fałszywe dokumenty urzędowe podszywające się pod organ rządowy.

Inne posty obejmują rozpowszechnianie fałszywych obrazów graffiti na ulicach dużych miast zachodnich, tworzonych z wykorzystaniem montażu fotografii prawdziwego miejsca i karykatury wymierzonej w osobowości ukraińskie lub europejskie. Te zmanipulowane obrazy mogą również parodiować tożsamość wizualną artystów ulicznych, takich jak np. Lekto.

Narracje promowane przez te publikacje są wymierzone przede wszystkim w Ukrainę i mają na celu zdyskredytowanie jej rządu i prezydenta lub krytykę przybycia ukraińskich uchodźców do krajów zachodnich. Przykładowo wiele fałszywych graffiti, często o charakterze antysemickim, przedstawia Wołodymyra Zełenskiego jako żebraka lub zbrodniarza wojennego, a ukraińskich uchodźców w Europie – jako zagrożenie.

Inne narracje mają na celu zdyskredytowanie rządów europejskich, a zwłaszcza ich polityki wspierającej Ukrainę. W związku z tym Francja stanowi główny cel dla operatorów kampanii. Media takie jak BFMTV, „Le Parisien", „Libération", „Le Monde" i „La Montagne", a także Bank Francji, miasto Paryż i Dyrekcja Generalna ds. Bezpieczeństwa Wewnętrznego zostały zmanipulowane za sprawą operacji „Matrioszka", której celem

było w szczególności wzbudzenie nieufności wobec francuskich instytucji i członków rządu.

Co więcej, VIGINUM zauważyło, że wiele operacji było wymierzonych w organizację igrzysk olimpijskich i paraolimpijskich w 2024 r. – propagowano informacje, że będzie to porażka zarówno wśród francuskiej, jak i międzynarodowej publiczności, podważając w ten sposób reputację francuskich mediów głównego nurtu i oficjalnych instytucji. Od początku masowej inwazji na Ukrainę w lutym 2022 r. rosyjski mechanizm wpływu regularnie atakował weryfikatorów faktów i wykorzystywał znaczne zasoby, aby zdyskredytować analizy zachodnich mediów.

Polska również stała się celem rosyjskich operacji dezinformacyjnych – straszy się Polaków Ukraińcami, wykorzystując sztuczną inteligencję do tworzenia zmanipulowanych treści. Prorosyjskie media aktywnie działają w polskim internecie, próbując wpływać na społeczne nastroje i podsycać konflikty. Badania przeprowadzone przez GLOBSEC wskazują, że propaganda Kremla ma swoje ulubione tematy, które są regularnie wykorzystywane do manipulacji opinią publiczną.

Co więcej, stosuje się tę strategię, aby zrozumieć, jak działają media i osoby weryfikujące fakty, analizując ich metody w celu późniejszego przeprowadzenia bardziej technicznych i strategicznych ataków. Istnienie tego rodzaju struktur operacyjnych potwierdza fakt: wszyscy obywatele są narażeni na dezinformację w swoim codziennym życiu, zwłaszcza za pośrednictwem mediów społecznościowych i portali internetowych.

Taktyka ta stosowana przez Rosjan ma na celu uniemożliwienie odróżnienia prawdy od kłamstwa, bezpośrednio podważając integralność informacji i manipulując dyskursem na poziomie regionalnym i globalnym.

Rosyjskie operacje dezinformacyjne, takie jak „Matrioszka”, pokazują, jak skomplikowane i wielowymiarowe mogą być działania propagandowe w erze cyfrowej. Kluczowe jest, aby społeczeństwa demokratyczne były świadome zagrożeń związanych z dezinformacją i rozwijały narzędzia do jej wykrywania i zwalczania. Współpraca międzynarodowa, edukacja medialna i wzmocnienie niezależnych mediów są niezbędne, aby przeciwdziałać szkodliwym wpływom i chronić integralność informacyjną.

Olga Wasiuta

Agence France Presse, https://factuel.afp.com/doc.afp.com.34H32VP (dostęp 11.10.2025); M. Czerniak, *„Matrioszka" i propaganda w sieci. Specjalistka NASK mówi o technikach dezinformacji*, 6.04.2025, https://expressbydgoski.pl/matrioszka-i-propaganda-w-sieci-specjalistka-nask-mowi-o-technikach-dezinformacji/ar/c1p2-27438139 (dostęp 12.10.2025); R. Godos, A. Biescas, S. Hernández, *Matrioska: la operación prorrusa que intenta manipular a verificadores de todo el mundo con alertas falsas*, 22.05.2024, https://verifica.efe.com/operacion-matrioska-prorrusa-manipular-verificadores-alertas-falsas/ (dostęp 10.10.2025); M. Jastrzębski, *MATRIOSZKA, Rosja i Jastrząb*, Wydawnictwo Helion, Gliwice 2013, https://onepress.pl/pobierz-fragment/matrioszka-rosja-i-jastrzab-maciej-jastrzebski-,matrio/pdf?srsltid=AfmBOorSJzawj9d5aZbgUHPNbPrkI4ObppMDka1VJO-3Tnvsf3xJnCwos (dostęp 12.10.2025); D. Jemioło, *Matrioszka – kolejna rosyjska kampania dezinformacyjna*, 24.05.2024, https://www.securitymagazine.pl/pl/a/matrioszka-kolejna-rosyjska-kampania-dezinformacyjna (dostęp 12.10.2025); M. Kostecki, *„Matrioszka": rosyjska kampania dezinformacyjna uderza w media i fact-checkerów*, https://demagog.org.pl/analizy_i_raporty/matriosza-rosyjska-kampania-uderza-w-media-i-fact-checkerow/ (dostęp 12.10.2025); G. Kubera, *Rosyjska propaganda zalewa Mołdawię przed wyborami*, 26.07.2025, https://businessinsider.com.pl/polityka/rosyjska-propaganda-zalewa-moldawie-przed-wyborami/znydzfc (dostęp 12.10.2025); P. Makowiec, *Matrioszka w akcji. Odkryto kolejną siatkę dezinformacyjną*, 22.05.2024, https://cyberdefence24.pl/cyberbezpieczenstwo/matrioszka-w-akcji-odkryto-kolejna-siatke-dezinformacyjna (dostęp 12.10.2025); T. Marie-Courtois, J. Mansour, *"Matriochka", la nouvelle campagne de désinformation anti-ukrainienne à destination des médias occidentaux*, 30.01.2024, https://archive.ph/2G4ML#selection-705.3-791.16 (dostęp 10.10.2025); *MATRYOSHKA. A pro-Russian campaign targeting media and the fact-checking community* [technical report], 2024, https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf (dostęp 10.10.2025); *New anti-Ukraine disinfo campaign aims to bog down Western media*, 29.01.2024, https://www.rfi.fr/en/international-news/20240129-new-anti-ukraine-disinfo-campaign-aims-to-bog-down-western-media (dostęp 10.10.2025); C. Ramírez, *Qué es la Operación Matrioska y cómo se vincula a la desinformación sobre la guerra en Ucrania*, 17.06.2024, https://www.vozdeamerica.com/a/que-es-la-operacion-matrioska-como-se-vincula-a-la-desinformacion-sobre-guerra-en-ucrania/7654935.html; https://x.com/antibot4navalny/X (dostęp 11.10.2025); M. Świerczek, *„System matrioszek", czyli dezinformacja doskonała. Wstęp do zagadnień*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-424b0c20-ea1c-444d-bcf8-a6d4b78cfdfc (dostęp 11.10.2025); *МАТРЕШКА. Пророссийская информационная операция, направленная*

против СМИ и сообщества фактчекеров, Технический доклад, Июнь 2024, https://www.sgdsn.gouv.fr/files/files/Publications/20240614_NP_SGDSN_VIGINUM_Matriochka_RU_VF.pdf (dostęp 12.10.2025).

ROSYJSKA OPERACJA „PORTAL KOMBAT" (znana również jako sieć Pravda) – zakrojona na szeroką skalę rosyjska kampania dezinformacyjna, oparta na sieci stron internetowych w różnych językach, gdzie publikowane są niskiej jakości treści powtarzające fałszywe i manipulacyjne twierdzenia z rosyjskich mediów państwowych, która działa w Europie, w tym w Polsce, i Stanach Zjednoczonych.

Według badań sieć ta obejmuje około 500 stron internetowych tworzących treści w 15 różnych językach. Dzięki zastosowaniu sztucznej inteligencji i dużych modeli językowych Rosjanie są w stanie szybko generować narracje zgodne z celami politycznymi Kremla.

W lutym 2024 r. francuska agencja rządowa VIGINUM, odpowiedzialna za przeprowadzanie analiz i ochronę Francji przed zagraniczną ingerencją cyfrową, opublikowała raport demaskujący tzw. operację „Portal Kombat", znaną też jako sieć Pravda. Chociaż jej korzenie sięgają 2014 r., w ciągu 10 lat przekształciła się ona ze zwykłego regionalnego agregatora wiadomości w wyrafinowane narzędzie rosyjskiej wojny hybrydowej. Pierwotna nazwa „Portal Kombat" – gra słów nawiązująca do brutalnej gry wideo *Mortal Kombat* – wskazywała już na agresywność tej kampanii cyfrowej. Na jej celowniku znalazły się takie państwa, jak Ukraina, Stany Zjednoczone, Francja, Niemcy, Polska, Wielka Brytania i inne kraje europejskie, a także niektóre afrykańskie. Ogromna ilość produkowanych treści zapewnia, że modele AI uwzględniają te rosyjskie narracje dezinformacyjne. Innymi słowy, Kreml aktywnie ingeruje w przestrzeń informacyjną, aby wpływać na odpowiedzi, które generują wybierani przez użytkowników asystenci AI.

Śledztwo przeprowadzone przez Digital Forensic Research Lab (DFRLab)[38] oraz fińską firmę CheckFirst wykazało, że rosyjski ekosystem stron internetowych znany jako Pravda rozbudował swoją infrastrukturę w 2024

[38] Laboratorium Badań Kryminalistycznych nad Cyfrową Informacją (The Digital Forensic Research Lab, DFRLab) działające przy Atlantic Council bada dezinformację, ujawniając

r. Operacja, wcześniej nazwana „Portal Kombat", rozwinęła się, obejmując więcej krajów i rozprzestrzeniając treści w większej liczbie państw w Europie, Afryce i Azji. Sukces tej sieci w zakresie wpływania na globalną przestrzeń informacyjną stał się szczególnie zauważalny po tym, jak badacze z DFRLab i CheckFirst odnotowali, że materiały z portali Pravda zaczęły być cytowane w Wikipedii w różnych językach, w tym po polsku i węgiersku. To właśnie za pośrednictwem Wikipedii narracje te przeniknęły również do modeli językowych sztucznej inteligencji. Krótki test przeprowadzony przez badaczy wykazał, że ChatGPT, Copilot, Perplexity i Gemini bez wahania powoływały się na strony powiązane z siecią Pravda – w ten sposób prorosyjskie narracje są rozpowszechniane w sposób ukryty i utrwalane za pośrednictwem popularnych technologii używanych przez miliony ludzi na całym świecie.

Doniesienia na temat operacji „Portal Kombat" pojawiły się także w Parlamencie Europejskim; raporty dotyczące ewolucji sieci Pravda można znaleźć w publikacjach DFRLab z Atlantic Council[39] oraz Europejskiego Obserwatorium Mediów Cyfrowych (EDMO)[40], które wykazały, że dezinformacja o polityce lub instytucjach UE stanowiła 15% wszystkich przypadków wykrytych w maju 2024 r. – najwyższa wartość od czasu rozpoczęcia śledzenia dezinformacji UE w 2023 r. Ekosystem Pravda nie łączy się z rosyjskimi mediami o tej samej nazwie.

Od czasu publicznego potępienia w lutym 2024 r. przez Francję, Niemcy i Polskę podmioty stojące za siecią „Portal Kombat" kontynuowały swoją wrogą działalność, dążąc w szczególności do jej rozszerzenia na inne obszary geograficzne. W istocie VIGINUM zaobserwowało kontynuację skrupulatnej „siatki informacyjnej" obejmującej niemal wszystkich członków Unii Europejskiej, i to na kilka tygodni przed wyborami europejskimi

kłamstwa i fałszywe wiadomości, dokumentując naruszenia praw człowieka i budując odporność cyfrową na całym świecie.

[39] Atlantic Council jest amerykańskim think tankiem działającym w dziedzinie spraw międzynarodowych, założonym w 1961 r. Zarządza 16 ośrodkami regionalnymi i programami funkcjonalnymi związanymi z bezpieczeństwem międzynarodowym i globalnym dobrobytem gospodarczym.

[40] Europejskie Obserwatorium Mediów Cyfrowych (EDMO) – niezależna sieć weryfikacji faktów.

w czerwcu 2024 r. Ponadto kilka krajów spoza Europy kontynentalnej również stało się celem ataków.

Głównym celem operacji jest rozpowszechnianie prokremlowskich narracji na temat wojny w Ukrainie i innych kwestii geopolitycznych, usprawiedliwianie inwazji na Ukrainę („specjalna operacja wojskowa”), dyskredytowanie Ukrainy i jej przywódców, rozpowszechnianie i osłabienie poparcia dla Ukrainy w krajach zachodnich, zwłaszcza w Europie i Stanach Zjednoczonych (w szczególności we Francji, Niemczech, Polsce, Hiszpanii, Austrii, Wielkiej Brytanii i Stanach Zjednoczonych), a także wśród społeczności rosyjskojęzycznych, zasianie wątpliwości co do instytucji demokratycznych. Sieć stara się również zdyskredytować amerykański przemysł zbrojeniowy. Infrastrukturą cyfrową zarządza rosyjska firma internetowa TigerWeb z siedzibą w okupowanym Symferopolu (Krym).

Operacja wykorzystuje sieć ponad 224 witryn internetowych, które mają identyczne parametry techniczne (wspólny adres IP hostowany na serwerze w Rosji), naśladujące wygląd i charakter lokalnych mediów informacyjnych w różnych krajach, rozpowszechniające propagandę usprawiedliwiającą rosyjską inwazję na Ukrainę i dyskredytującą ukraińskie władze. Nazwy wielu witryn zawierają słowo „Pravda” (np. Pravda-fr.com, Pravda-de.com, Pravda-pl.com), grę słów, co jest ironicznym zabiegiem propagandowym.

Początkowo sieć koncentrowała się na odbiorcach rosyjskojęzycznych i mieszkańcach okupowanych terytoriów ukraińskich, ale po pełnej inwazji w 2022 r. ponownie skupiła się na krajach zachodnich, w tym Wielkiej Brytanii i USA, Francji, Austrii, Niemczech, Polsce, Hiszpanii i innych krajach UE, a także na lokalnej społeczności w Afryce i Azji.

Serwisy nie generują oryginalnych treści, lecz masowo rozpowszechniają i wzmacniają materiały z rosyjskich państwowych agencji informacyjnych (takich jak TASS, RIA) oraz prorosyjskich kont w mediach społecznościowych, zwłaszcza Telegramu. Treści są automatycznie tłumaczone na różne języki Unii Europejskiej, w tym francuski, niemiecki, hiszpański, angielski, a także grecki, włoski, bułgarski, duński i niderlandzki; optymalizowane pod kątem wyszukiwarek, często przy użyciu botów, aby sztucznie zwiększyć ich zasięg oraz wiarygodność i obejść sankcje. Sieć „Portal Kombat” próbuje manipulować dużymi modelami językowymi

(czatbotami AI), zalewając internet prokremlowskimi treściami, które następnie są wykorzystywane do szkolenia systemów sztucznej inteligencji.

Badania agencji VIGINUM wykazały, że same w sobie serwisy te nie przyciągają dużej liczby czytelników, wzmacniają jednak prorosyjskie narracje w przestrzeni informacyjnej, a linki do nich są czasami postrzegane przez inne legalne źródła jako wiarygodne, co nadaje dezinformacji pozory autentyczności.

W okresie poprzedzającym wybory do Parlamentu Europejskiego w 2024 r. ekosystem Pravda ewoluował i uruchomił nowe strony internetowe, skierowane niemal do każdego kraju członkowskiego Unii Europejskiej, a także Europejskiego Partnerstwa Wschodniego. Ponadto pojawiło się wiele stron internetowych wymierzonych w kraje francuskojęzyczne w regionie Sahelu, w Afryce. Podobne zostały zarejestrowane przed wyborami do parlamentu Gruzji w październiku 2024 r. W trakcie wysiłków na rzecz zjednoczenia wszystkich domen (News-pravda(.)com), jesienią 2024 i na początku 2025 r. sieć korzystała ze 140 subdomen skierowanych do ponad 83 krajów i regionów na całym świecie. Pierwsza seria 4 domen zarejestrowanych 26 kwietnia 2024 r. była skierowana do państw bałtyckich oraz Republiki Mołdawii – działała po rosyjsku, prawdopodobnie próbując wpłynąć na rosyjskojęzyczne mniejszości w tych krajach.

3 sierpnia 2024 r. pojawiło się 21 nowych domen wymierzonych w miasta ukraińskie, również w języku rosyjskim, zaś jesienią 2024 r. ekosystem Pravda powrócił do najwyższego poziomu portalu domenowego News-pravda(.)com. Domena specyficzna dla USA – Us.news-pravda(.)com – ukazała się 4 listopada 2024 r., na dzień przed wyborami prezydenckimi w USA. 8 listopada pojawiły się 3 kolejne domeny, które zaczęły atakować USA, UE, NATO, kanclerza Niemiec Olafa Scholza, prezydenta Francji Emmanuela Macrona oraz prezydenta elekta Donalda Trumpa.

Między 3 grudnia 2024 a 8 stycznia 2025 r. pojawiło się 28 nowych subdomen skierowanych do wielu krajów w Europie, w tym Malty, Islandii, Irlandii, Bałkanów, Republiki Serbskiej w Bośni i Hercegowinie oraz Czarnogóry. Treści były tworzone w językach mniejszości, takich jak kataloński, galicyjski, baskijski, walijski i szkocki. Dodatkowe subdomeny kierowane były do Afryki (Algierii, Mali, Senegalu, Kamerunu, Gwinei, Gambii, Erytrei, Egiptu, Mauretanii, Nigerii, Czadu, Sudanu Południowego i Sudanu),

Kaukazu (Osetii, Abchazji) oraz maoryskojęzycznych odbiorców z Nowej Zelandii. Później sieć rozszerzyła swój zasięg, koncentrując się na krajach azjatyckich, w tym na Korei Południowej i Północnej, Tajwanie, Japonii i Singapurze. Najwcześniejsze przypadki występowania ekosystemu Pravdy wskazują na rosyjską firmę informatyczną z siedzibą na Krymie.

W toku swoich badań VIGINUM przeanalizował sieć 193 portali informacyjnych należących do tej samej infrastruktury cyfrowej, które można podzielić na 3 odrębne ekosystemy, zbudowane według kryteriów wizualnych (grafika stron internetowych), czasowych (data utworzenia stron internetowych) i terytorialnych (kraje docelowe).

Pierwszy ekosystem stron internetowych zidentyfikowany przez VIGINUM obejmuje kilka krajów zachodnich, które publicznie wyraziły swoje poparcie dla Ukrainy po inwazji Rosji:

- Pravda-fr(.)com: Francja;
- Pravda-de(.)com: Niemcy, Austria i Szwajcaria;
- Pravda-pl(.)com: Polska;
- Pravda-es(.)com: Hiszpania;
- Pravda-en(.)com: Wielka Brytania i Stany Zjednoczone.

Poza podobną nazwą domeny, te 5 stron internetowych, zarejestrowanych 24 czerwca 2023 r., ma identyczne parametry techniczne: wspólny adres IP hostowany na serwerze zlokalizowanym w Rosji, tę samą architekturę HTML, ten sam schemat graficzny i sekcje oraz te same linki zewnętrzne.

Co więcej, strony te rozpowszechniają treści o podobnej prokremlowskiej narracji, w szczególności na temat rzekomej legalności specjalnej operacji wojskowej, zniesławiające Ukrainę i jej przywódców lub krytykujące kolektywny Zachód.

Sieć jest najbardziej skoncentrowana w przestrzeni postsowieckiej i na Bałkanach. Pomimo że regiony te stanowią zaledwie 9% populacji wszystkich badanych krajów, odpowiadają za ponad 50% wszystkich zarejestrowanych przekazów dezinformacyjnych. W krajach byłego ZSRR liczba takich przekazów była 31,8 razy wyższa niż w Europie Zachodniej.

Wybór regionów docelowych wynika głównie z czynników geopolitycznych. Najsilniejszą presję odnotowuje się w państwach peryferyjnych UE i NATO, w szczególności w Mołdawii, gdzie aktywność sieci jest o 19,7%

wyższa niż na Łotwie, która zajęła drugie miejsce. 10 krajów o największej aktywności sieciowej przedstawia się następująco:

1. Mołdawia.
2. Łotwa.
3. Estonia.
4. Serbia.
5. Armenia.
6. Litwa.
7. Gruzja.
8. Słowacja.
9. Bułgaria.
10. Czechy.

Obecność sieci na Słowacji, która zajęła 8 miejsce w rankingu, jest szczególnie zauważalna. Analitycy wskazują, że Mołdawia, Łotwa, Litwa, Bułgaria, Serbia i Słowacja są uważane za niedoskonałe demokracje, podczas gdy Armenia i Gruzja to reżimy hybrydowe. Strategia Kremla ma zatem na celu osłabienie rozwoju demokracji i ograniczenie reform w tych państwach.

Rosyjskie wysiłki zmierzające do wprowadzania dezinformacji do szybko rozwijającej się przestrzeni informacyjnej AI stanowią poważne zagrożenie dla globalnego bezpieczeństwa, ponieważ może to prowadzić do manipulowania opinią publiczną, osłabiania zaufania do rzetelności informacji cyfrowych i rozpowszechniania pozornie wiarygodnych narracji na niespotykaną dotąd skalę. Raport Centrum Polityki Cyfrowej w Centrum Innowacji w Zarządzaniu Międzynarodowym (Digital Policy Hub in Centre for International Governance Innovation) wskazuje, że Rosja wychodzi poza tradycyjne metody propagandy i zwraca się w kierunku wykorzystywania dużych modeli językowych. Poprzez *grooming LLM* Moskwa normalizuje nieprawdziwe informacje, aby wyglądały jak oparte na faktach. Nawet cieszące się sporym zaufaniem platformy, takie jak Wikipedia, nagłaśniają kremlowską dezinformację poprzez cytowanie źródeł z sieci Pravda.

„Portal Kombat" jest przykładem skoordynowanej rosyjskiej operacji mającej na celu wykorzystanie wojny informacyjnej do osiągnięcia celów politycznych, takich jak podważanie złożonej i ewoluującej taktyki wojny hybrydowej Rosji, a także zaufania do demokratycznych instytucji, i osłabienie

wsparcia dla Ukrainy, często przed ważnymi wydarzeniami politycznymi, takimi jak wybory do Parlamentu Europejskiego.

Olga Wasiuta

V. Châtelet, A. Lesplingar, *Russia's so-called "Pravda" network expands worldwide*, 24.02.2025, https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/ (dostęp 23.11.2025); A. Desmarais, *Russiagate to Portal Kombat: The foreign misinformation campaigns shifting the European elections,* 6.06.2024, https://www.euronews.com/next/2024/06/06/russiagate-to-portal-kombat-the-foreign-misinformation-campaigns-shifting-the-european-ele (dostęp 27.11.2025); *EDMO*, https://ec.europa.eu/newsroom/edmo/newsletter-archives/52424 (dostęp 23.11.2025); *PORTAL KOMBAT. A structured and coordinated pro-Russian propaganda network* [technical report], 2024, https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf (dostęp 25.11.2025); *PORTAL KOMBAT. Expansion of the pro-Russian propaganda network: new domain names* [technical report], 2024, https://www.sgdsn.gouv.fr/files/files/Publications/20240428_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK-REPORT_NEW%20DOMAIN%20NAME_%28PART3%29_ENG_VF.pdf (dostęp 25.11.2025); *The Atlantic Council's Digital Forensic Research Lab (DFRLab)*, https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/(dostęp 27.11.2025); *The Digital Policy Hub*, https://ires2015.sites.olt.ubc.ca/files/2023/05/CIGI-Digital-Policy-Hub.pdf (dostęp 23.11.2025); *The Pravda Network*, https://dfrlab.org/the-pravda-network/ (dostęp 23.11.2025); *Великі мовні моделі: нове поле бою російської інформаційної війни*, EUvsDisinfo, 23.01.2025, https://euvsdisinfo.eu/ua/%D0%B2%D0%B5%D0%BB%D0%B8%D0%BA%D1%96-/ (dostęp 26.11.2025); *Нове дослідження, як російська пропагандистська мережа «Правда» маніпулює ШІ та Вікіпедією для поширення брехні в Європі*, 28.04.2025, https://disinfo.detector.media/post/nove-doslidzhennia-iak-rosiiska-propahandystska-merezha-pravda-manipuliuie-shi-ta-vikipediieiu-dlia-poshyrennia-brekhni-v-yevropi (dostęp 26.11.2025); *Пов'язана з Росією дезінформаційна мережа Portal Kombat розпочала масштабну кампанію з дискредитації американської оборонної промисловості*, 19.04.2025, https://newsua.one/news-military/111536.html (dostęp 26.11.2025).

ROSYJSKA OPERACJA „PRZECIĄŻENIE” (ang. *operation „Overload”*) – nazwa zaawansowanej trwającej prorosyjskiej kampanii informacyjnej, działań propagandowych i dezinformacyjnych; to również skoordynowana akcja wojny informacyjnej prowadzona przez prorosyjskie podmioty, kampania wpływu mająca na celu manipulowanie opinią publiczną i sianie niezgody,

która wykorzystuje nowoczesne techniki wpływu, w tym treści generowane przez sztuczną inteligencję (AI). Operacja *podszywa się pod wiarygodne źródła, aby siać zamęt i podważyć zaufanie opinii publicznej do europejskich i amerykańskich instytucji. Publikuje zmanipulowane filmy i zdjęcia, często opatrzone skradzionymi logotypami mediów, na platformach X (dawniej Twitter), Bluesky, TikTok i Telegram. Operacja kontaktuje się również bezpośrednio z badaczami i weryfikatorami faktów po to, by odwrócić ich uwagę od pilniejszych śledztw lub wygenerować relacje, które zwiększą jej postrzegany wpływ.* Z uwagi na taktykę wielokrotnego rozpowszechniania informacji za pośrednictwem platform publicznych i kanałów prywatnych (mail) badacze nazwali tę kampanię operacją „Przeciążenie".

Operacja „Przeciążenie" była analizowana przez liczne firmy zajmujące się cyberbezpieczeństwem, organizacje non profit i agencje rządowe. Do najważniejszych instytucji, które analizowały i przygotowały raporty o operacji (znanej również pod alternatywnym kryptonimem „Matrioszka" lub „Storm-1679"), należą:

- CheckFirst: fińska firma badająca dezinformację w internecie, która jest współautorem obszernego raportu na temat operacji „Przeciążenie";
- Instytut Dialogu Strategicznego (Institute for Strategic Dialogue, ISD): brytyjska organizacja non profit monitorująca ekstremizm i dezinformację w internecie, która opracowała liczne raporty szczegółowo opisujące ewoluującą taktykę operacji, wykorzystanie sztucznej inteligencji i jej cele;
- Recorded Future: firma wywiadowcza zajmująca się cyberbezpieczeństwem, której dział badań nad zagrożeniami, Insikt Group, opublikował szczegółowe analizy działań w ramach operacji „Przeciążenie", metody kampanii i jej ukierunkowania wpływu na wybory w państwach demokratycznych;
- Reset Tech: organizacja non profit zajmująca się bezpieczeństwem w sieci, która wspólnie z CheckFirst opracowała pierwszy raport dotyczący operacji „Przeciążenie";
- VIGINUM: francuska agencja rządowa ds. czujności i ochrony przed zagraniczną ingerencją cyfrową, która również dokumentowała kampanię, ale pod nazwą „Matrioszka";

- EU DisinfoLab: organizacja non profit, która koordynuje działania z innymi podmiotami i publikuje aktualizacje oraz materiały związane z kampanią;
- Debunk.org: organizacja zajmująca się weryfikacją faktów, która była celem operacji „Overload" i analizowała otrzymane w jej ramach maile i treści;
- Centrum Bezpieczeństwa Internetowego (Center for Internet Security, CIS): organizacja non profit monitorująca ekstremizm i dezinformację w internecie, która zgłosiła działania operacji wymierzone w wybory prezydenckie w USA w 2024 r. oraz sytuację polityczną w USA;
- różne media i organizacje zajmujące się weryfikacją faktów: kampania objęła ponad 800 podmiotów z ponad 75 krajów, które udostępniły dane do analizy. Wśród nich znalazły się BBC, Agence France-Presse (AFP) oraz członkowie Europejskiej Sieci Standardów Weryfikacji Faktów (EFCSN). Organizacje te współpracują ze sobą i dzielą się swoimi wynikami, często za pośrednictwem takich sieci jak Centrum Wymiany Informacji i Analiz FIMI (FIMI-ISAC), aby zapewnić kompleksowe zrozumienie zagrożenia, jakie stwarza ta trwająca operacja wpływu.

Operacja „Overload", która po raz pierwszy została udokumentowana w czerwcu 2024 r., podbija nowe platformy i wykorzystuje narzędzia sztucznej inteligencji, aby atakować weryfikatorów faktów, media i odbiorców międzynarodowych za pomocą kremlowskiej propagandy i wywołać „eksplozję treści" skupioną na zaostrzaniu istniejących napięć wokół wyborów na świecie, Ukrainy i imigracji oraz innych kontrowersyjnych kwestii. Jej mechanizm polega na zalewaniu redakcji, dziennikarzy i fact-checkerów fałszywymi zgłoszeniami – często stylizowanymi na prośby o weryfikację informacji. Pomimo dogłębnych badań szczegółowo opisujących ewoluującą taktykę i skalę operacji działania moderacji treści pozostają w dużej mierze niewystarczające, szczególnie na X.

Operacja wykorzystuje wielowarstwowe taktyki, w tym bezpośrednie wysyłki maili, zaangażowanie mediów społecznościowych i masową dystrybucję treści manipulacyjnych, aby wywołać podział w społeczeństwie i zmienić opinię publiczną na temat Ukrainy, w szczególności we Francji

i Niemczech. Według Reset.Tech i CheckFirst kampania dezinformacyjna trwa co najmniej od sierpnia 2023 r.

Początkowo wykryto skoordynowaną kampanię antyukraińską na portalu społecznościowym X, jednak później badacze ustalili, że treści tam publikowane pochodziły z niewielkiej grupy rosyjskojęzycznych kanałów Telegram, a także były rozpowszechniane za pośrednictwem innych rosyjskich portali społecznościowych (VKontakte, Odnoklassniki) i stron internetowych powiązanych z Kremlem, w tym rosyjskich mediów państwowych i stron internetowych niedawno ujawnionej sieci Pravda (inaczej operacja „Portal Kombat"). Ostatnim etapem operacji jest kampania mailowa skierowana bezpośrednio do organizacji zajmujących się weryfikacją faktów.

Głównym celem operacji jest zasypywanie dziennikarzy i weryfikatorów faktów uporczywymi, przypominającymi spam prośbami o weryfikację nieautentycznych treści, odwrócenie uwagi od prowadzenia legalnych dochodzeń i obalenia rosyjskiej dezinformacji. Operacja ma również wykorzystać organizacje medialne do wstrzykiwania złośliwych treści i prokremlowskich narracji do głównego nurtu dyskursu politycznego za pośrednictwem zaufanych stron. Kolejnym celem jest próba wykorzystania profesjonalistów do wzmocnienia fałszywych twierdzeń operacji poprzez ich obalenie i dotarcie do szerszego grona odbiorców. Wreszcie, bezpośrednie wprowadzenie treści wpływających na główny nurt dyskusji na temat spornych kwestii politycznych, podważając zaufanie publiczne do procesu demokratycznego, prowokując wewnętrzne obawy USA związane z przemocą polityczną i „wojną domową" oraz wykorzystując istniejące podziały społeczne.

Trzeba podkreślić, że operacja nie ma przekonywać odbiorców do konkretnej narracji, ale przytłoczyć ich ogromną ilością sprzecznych, fałszywych lub zmanipulowanych informacji, rozmyć granice między faktami a fikcją poprzez zalewanie przestrzeni informacyjnej treściami generowanymi masowo, co prowadzi do „przeciążenia" informacyjnego odbiorców.

Schemat działalności tej operacji jest prosty: produkuje się mnóstwo fałszywych lub zmanipulowanych treści i zalewa nimi media społecznościowe. Dla każdej narracji najpierw umieszczana jest masa manipulacyjnych treści w rosyjskojęzycznych kanałach Telegramu, następnie

są one publikowane na znanych stronach internetowych związanych z Kremlem. Kolejny krok ma miejsce w portalu społecznościowym X, gdzie atakujący rozpowszechniają fałszywe treści i wchodzą w interakcję z mediami, instytucjami i weryfikatorami faktów. Ostatnim etapem jest skoordynowana wysyłka mailingowa, która odsyła odbiorcę do wcześniej opublikowanych treści na Telegramie, X lub na kontrolowanych stronach internetowych.

Celem jest odwrócenie uwagi i zepchnięcie na margines najważniejszych kłamstw – by w końcu tropicielom fake newsów zabrakło czasu. Niektóre prośby brzmią wręcz groteskowo, ale odmowa weryfikacji w oczach części odbiorców staje się dowodem na „nieuczciwość i stronniczość” fact-checkerów.

Operacja „Przeciążenie” służy zarówno propagandzie krajowej, jak i celom FIMI (zagranicznej ingerencji i manipulacji informacjami). Podczas gdy badania Reset.Tech i CheckgfFirst koncentrują się na tym drugim, fałszywe treści pojawiają się w rosyjskim segmencie mediów społecznościowych i są rozpowszechniane na rosyjskojęzycznych stronach internetowych z wyraźnym celem promowania militarnej agendy Kremla wśród lokalnej publiczności. Ta kampania dezinformacyjna wciąż trwa, rozszerzając swoją skalę i wykorzystując nowe techniki, taktyki i procedury.

Główne aspekty operacji „Overload”:

- kampania mailowa skierowana do redakcji i weryfikatorów faktów;
- napływ manipulacyjnych treści do mediów społecznościowych;
- kluczowa rola Telegramu w tworzeniu i dystrybucji fałszywych treści;
- kampania skoordynowanych działań nieautentycznych w X w celu osiągnięcia określonych celów.

Unikatowym aspektem operacji „Overload” jest lawina maili wysyłanych do redakcji i weryfikatorów faktów w całej Europie. Autorzy tych wiadomości wzywają odbiorców do weryfikacji treści, które rzekomo znaleźli w internecie. Temat maila często zawiera prośbę o weryfikację twierdzeń krótko opisanych w treści wiadomości. Następnie wyświetlana

jest krótka lista linków, które przekierowują odbiorców do wiadomości w Telegramie, X lub znanych prorosyjskich stron internetowych, takich jak Pravda i Sputnik.

Niektóre z narracji forsowanych przez operację „Overload" obejmują:

- podsycanie strachu przed przemocą polityczną: wzmacniając obawy przed niepokojami społecznymi, a nawet wojną domową, operacja ma na celu wywołanie strachu i niepewności;
- wywołanie silnych emocji: treści są konstruowane tak, aby wzbudzać strach, gniew lub niepewność, co utrudnia racjonalną analizę faktów;
- targetowanie kandydatów: w szczególności wiceprezydent USA Kamala Harris była głównym celem działań dezinformacyjnych w ramach operacji. Treści fałszywie łączyły ją z wieloma skandalami mającymi na celu zniszczenie jej reputacji przed wyborami;
- oczernianie Ukraińców i społeczności LGBTQIA+[41]: operacja prowokuje negatywne nastroje wobec tych społeczności, odpowiednio zmniejszając poparcie społeczne dla Ukrainy i wykorzystując podziały społeczne w różnych państwach;
- chaos informacyjny: zasypanie opinii publicznej tak dużą liczbą treści (często generowanych przy użyciu sztucznej inteligencji, w tym fałszywych filmów i głosów), że trudno odróżnić prawdę od fałszu;
- erozja zaufania: podważenie zaufania do służb, rządu i całego systemu państwowego, co ma osłabić wewnętrzną spójność i odporność społeczeństw zachodnich na rosyjskie działania; podważanie wiarygodności mediów poprzez zalewanie przestrzeni informacyjnej ogromną ilością treści, często fałszywych lub zmanipulowanych.

[41] Społeczność **LGBTQIA+** to akronim używany do zbiorczego określania osób o różnych orientacjach seksualnych i tożsamościach płciowych, które nie są heteronormatywne. Społeczność ta dąży do równych praw, akceptacji społecznej i walki z dyskryminacją.

Ostatecznym zamiarem tej strategii jest doprowadzenie do „przeciążenia systemu” informacyjnego Zachodu, co ma osłabić jego zdolność do reagowania na rosyjskie działania i wspierania Ukrainy.

Kluczowe aspekty tej operacji to:

- gwałtowny wzrost wykorzystania treści generowanych przez sztuczną inteligencję (filmy, memy, głosy, fałszywe wizerunki i wiadomości), które służą do rozpowszechniania rosyjskiej propagandy i fake newsów i aby uwiarygodnić prorosyjskie i antyukraińskie narracje. Materiały te, często trudne do odróżnienia od prawdziwych, mają zacierać granicę między faktem a fikcją;
- ekosystem ukrytych kanałów i powiązanych kont: zarządzanych przez sieci koordynacyjne, które ponownie wykorzystują te same materiały w dziesiątkach różnych grup; mają one na celu masowe rozpowszechnianie dezinformacji;
- przytłoczenie informacjami: dostarczenie ogromnej ilości sprzecznych lub fałszywych informacji, sensacyjnych lub emocjonalnie naładowanych treści, że staje się niemożliwe odróżnienie prawdy od fałszu, co ma prowadzić do apatii, chaosu, nieufności i spadku zaufania do wiarygodnych źródeł informacji oraz siania niezgody;
- wykorzystanie platform społecznościowych: głównymi ośrodkami dystrybucji tych treści są Telegram i X (dawniej Twitter). Telegram jest opisywany jako „inkubator” propagandy, gdzie treści są tworzone i przechowywane, a następnie rozpowszechniane na większych platformach, takich jak X lub TikTok, często opatrzone fałszywymi logotypami renomowanych zachodnich mediów, aby nadać im pozory wiarygodności;
- „długa wojna nerwów” (ros. *война на истощение нервов*): działania te wpisują się w szerszą strategię Rosji określaną w jej wewnętrznych analizach wojskowych, w której ostateczny wynik zależy od zdolności systemu do wytrzymania presji informacyjnej i psychologicznej w czasie.

Operacja „Przeciążenie” to kolejny etap lub uzupełnienie operacji „Kylo” – kampanii polegającej na rozpowszechnianiu fake newsów przez sieć fałszywych portali i kont społecznościowych, które podszywały się

pod europejskie media. I tak, od połowy 2022 r. do setek redakcji trafiły tysiące maili i wiadomości w mediach społecznościowych zawierających spreparowane materiały; często dotyczyły one Ukrainy, Niemiec, Francji i innych państw wspierających Kijów. Każdy materiał był dokładnie przygotowany – wyglądał jak realne doniesienie wymagające sprawdzenia. W rzeczywistości miało to jeden cel: przeciążyć systemy weryfikacyjne i promować rosyjską propagandę.

Obie operacje korzystają z tych samych metod: profesjonalnej kreacji, manipulacji wizualnej i psychologicznej, a także strategii „posiewu dezinformacji" – gdzie choćby obalone fake newsy mogą osiągać efekt, jeżeli dotrą do dużej liczby osób przed ich sprostowaniem.

Operacja „Przeciążenie" polega na tworzeniu witryn z fałszywymi wiadomościami, fałszywych zasobów sprawdzania faktów i dźwięku generowanego przez sztuczną inteligencję, który naśladuje legalne media. W taki sposób próbowano podważyć wybory we Francji w 2024 r. i igrzyska olimpijskie w Paryżu, choć z minimalnym sukcesem. Później skupiono się na wyborach prezydenckich w USA w 2024 r., a celem było podważenie zaufania do procesu wyborczego, wykorzystanie dzielących kwestii społecznych, podsycanie obaw przed przemocą polityczną i atakowanie kandydatów, w szczególności wiceprezydent Kamali Harris. Chodziło nie o skłonienie wyborców do postawienia krzyżyka przy konkretnym nazwisku – raczej o chaos i deprecjację instytucji odpowiedzialnych za weryfikację faktów.

Poprzez fałszywe informacje, imitację stron sprawdzających fakty i syntetyczny dźwięk generowany przez AI stara się wpływać na opinię publiczną, udając zaufane źródła medialne. Kampania jest skierowana przede wszystkim do mediów, weryfikatorów faktów i badaczy, mając na celu przeciążenie zasobów śledczych i wprowadzenie fałszywych narracji do głównego nurtu dyskursu, ale jest również bezpośrednio skierowana do ogółu społeczeństwa.

Kluczowe taktyki i techniki:

- podszywanie się pod zaufane marki medialne albo renomowane serwisy informacyjne, aby uwiarygodnić swoje operacje wywierania wpływu. Poprzez kupno logotypów, używanie podobnych czcionek i układów oraz fałszywe przypisanie treści

prawdziwym dziennikarzom, tworzone są materiały (również wideo i obrazy z publicznie dostępnych źródeł, które wydają się uzasadnione;

- treści generowane przez sztuczną inteligencję: jednym z nowszych osiągnięć w zestawie narzędzi operacji „Przeciążenie" jest wykorzystanie sztucznej inteligencji do generowania realistycznych podkładów głosowych. Treści te, często wykorzystywane w krótkich filmach, dodatkowo wzmacniają postrzeganą wiarygodność i utrudniają odróżnienie prawdziwych informacji od fałszywych;
- kierowanie reklam do mediów i organizacji zajmujących się weryfikacją faktów: operacja „Overload" skupia się głównie na organizacjach medialnych, weryfikatorach faktów i badaczach. Zalewając ich prośbami podobnymi do spamu i fałszywymi leadami[42], przeciąża się ich zasoby, a to utrudnia obalanie rosyjskiej dezinformacji i grozi nieumyślnym informowaniem o fałszywych treściach, a tym samym wstrzykiwaniem rosyjskich złośliwych narracji do głównego nurtu dyskursu politycznego;
- operacja wykorzystuje również zautomatyzowane boty do rozpowszechniania swoich wpływowych treści w mediach społecznościowych. Ta taktyka, określana jako skoordynowane nieautentyczne zachowanie, pomaga wzmocnić fałszywe narracje na platformach mediów społecznościowych, dzięki czemu treści są bardziej rozpowszechnione i widoczne dla ogółu społeczeństwa.

Jednym z nowszych osiągnięć operacji „Przeciążenie" jest jej poleganie na sztucznej inteligencji, która jest wykorzystywana do tworzenia lektorów i sprawiania, że fałszywe treści medialne wyglądają tak, jakby

[42] Fałszywe leady – wprowadzanie reklamodawców w błąd poprzez podawanie nieprawdziwych lub zmyślonych danych potencjalnych klientów, które mogą być skradzione, niekompletne lub zmyślone. Jest to forma oszustwa, w której nieuczciwi pośrednicy lub oszuści generują leady, za które reklamodawca płaci, mimo że nie ma szans na konwersję, często wykorzystując podobne lub identyczne dane kontaktowe do stworzenia wielu fałszywych zgłoszeń.

pochodziły z legalnych mediów. Pozwala to na szybkie tworzenie wysokiej jakości dezinformacji na dużą skalę, co utrudnia jej wykrycie i obalenie.

Operacja „Overload" koncentruje się na konkretnych celach geopolitycznych, ze szczególnym uwzględnieniem 6 krajów: Francji, Niemiec, Mołdawii, Polski, Ukrainy i Stanów Zjednoczonych. Narracje zawarte w mailach nadal są zdominowane przez retorykę antyukraińską; słowa „ukraiński", „Ukraina", „Zełenski" i „Ukraińcy" należą do najczęściej używanych terminów obecnych w treści maili od początku operacji.

W 2025 r. operacja zdywersyfikowała swoje kluczowe wątki narracyjne, od typowej antyukraińskiej retoryki po systemowe próby ingerencji w wybory wymierzone w kilka krajów, w tym przeciwko Mołdawii i jej proeuropejskiej prezydent Mai Sandu, oskarżając ją o korupcję i niekompetencję. Dezinformacja oparta na płci, skoordynowane kampanie oszczerstw przeciwko politykom i bezpośrednie podżeganie do przemocy również stanowią część arsenału narracyjnego.

Amalgamacja treści, czyli łączenie tej samej historii w wielu formatach, rozpowszechnianych różnymi kanałami, pozostaje podstawową taktyką, techniką i procedurą tej operacji. Ma na celu stworzenie wielowarstwowej iluzji autentyczności, dodatkowo wzmocnionej przez szersze wykorzystywanie przez agentów różnorodnych formatów treści.

W 2025 r. platformy mediów społecznościowych najwyraźniej zintensyfikowały działania mające na celu usuwanie treści związanych z operacją „Overload", ograniczając jej zasięg i wpływ. X usunął 73% badanych postów, w porównaniu z zaledwie 20% w pierwszym kwartale 2025 r., z kolei na TikToku i Bluesky wskaźniki usunięć przekroczyły 90%. Może to odzwierciedlać rosnącą świadomość platform dotyczącą operacji lub fakt, że korzystanie z botów i innych technik manipulacyjnych jest na tyle bezczelne, że uruchamia automatyczne systemy moderacji.

Operacja „Przeciążenie" to niezwykle złożona kampania ze względu na jej szeroki zasięg i znaczący wpływ. Koordynowana na wielu poziomach z wykorzystaniem różnorodnych technik ma na celu wzmacnianie fałszywych narracji, sianie niezgody, tworzenie zamieszania i polaryzację opinii publicznej na temat Ukrainy, a wszystko to z korzyścią dla Kremla. Intensywność kampanii charakteryzuje się częstymi, dobrze skoordynowanymi atakami, szczególnie podczas kluczowych wydarzeń w Europie.

Wyrafinowane taktyki, takie jak agregacja treści i podszywanie się pod inne osoby, dodatkowo zwiększają jej wiarygodność i skuteczność.

Operacja próbuje napędzać polaryzację w państwach poprzez forsowanie narracji, które pogłębiają istniejące podziały w kontrowersyjnych kwestiach i dyskredytują kluczowe postacie polityczne. Próbuje wzmocnić także teorie spiskowe dotyczące oszustw wyborczych i sfałszowanych wyborów, podszywając się pod legalne media, aby podważyć zaufanie do procesu demokratycznego.

Podszywanie się pod prawdziwe media, instytucje akademickie i osoby publiczne w ramach operacji ma realne konsekwencje. Ataki na te podmioty wskazują na szerszy cel kampanii: dalsze podważanie zaufania do mediów i instytucji w krajach zachodnich. Niewłaściwe wykorzystanie ich wizerunków i przekazów ma negatywne konsekwencje dla reputacji tych osób i organizacji. Platformy mediów społecznościowych ponoszą odpowiedzialność za rozpowszechnianie tych treści, z których wiele narusza ich własne zasady dotyczące nieautentyczności i/lub podszywania się pod inne osoby.

Operacja wykorzystuje wiele taktyk mających na celu manipulowanie opinią publiczną wokół wyborów w państwach demokratycznych. Obejmują one szerzenie obaw o bezpieczeństwo wyborów, podważanie zaufania do instytucji oraz rozpowszechnianie mylących treści. Choć jej wpływ pozostaje ograniczony, taktyki te uwypuklają ciągłe zagrożenia dla procesów demokratycznych.

„Przeciążenie" jest postrzegane jako ewolucja rosyjskich operacji dezinformacyjnych, wykorzystująca nowoczesne technologie do osiągnięcia efektu paraliżu informacyjnego. Jest przykładem, jak Rosja wykorzystuje luki w moderacji platform społecznościowych i rozwój technologii AI do prowadzenia wojny informacyjnej na masową skalę.

Olga Wasiuta

18 września: Operacja Overload: mądrzejsza, odważniejsza, wspierana przez sztuczną inteligencję, https://www.disinfo.eu/outreach/our-webinars/18-september-operation-overload-smarter-bolder-powered-by-ai/ (dostęp 14.11.2025); A. Atanasova, F. Poldi, G. Kuster, *Operation Overload. More Platforms, New Techniques, Powered by AI*, 2025, https://checkfirst.network/wp-content/uploads/2025/06/

Overload%C2%A02_%20Main%20Draft%20Report_compressed.pdf (dostęp 12.11.2025); *Coordinated disinformation network uses AI, media impersonation to target German election*, *13.02.2025*, https://www.isdglobal.org/digital_dispatches/coordinated-disinformation-network-uses-ai-media-impersonation-to-target-german-election/ (dostęp 12.11.2025); *EFCSN Statement on Operation Overload. REPORT*, 4.06.2024, https://efcsn.com/news/2024-06-04_efcsn-statement-on-operation-overload-report-by-checkfirst/ (dostęp 14.11.2025); K. Krajewski, D. Frąckiewicz, *Russian Influence Operations as a tool of cognitive warfare in German Elections: Analysis of Methods, Objectives, and Effectiveness*, https://www.defencesciencereview.com.pl/pdf-209689-128083?filename=Russian%20Influence.pdf (dostęp 10.11.2025); *Operation Overload Impersonates Media to Influence 2024 US* Election, 23.10.2024, https://assets.recordedfuture.com/insikt-report-pdfs/2024/ta-ru-2024-1023.pdf (dostęp 12.11.2025); *Operation Overload*, 2024, https://checkfirst.network/wp-content/uploads/2024/09/Operation_Overload_ Activity_Update_September_2024.pdf (dostęp 10.11.2025); *OPERATION OVERLOAD. More Platforms, New Techniques, Powered by AI Activity Update*, 2025, https://checkfirst.network/wp-content/uploads/2025/06/Overload% C2%A02_%20Main%20 Draft%20Report_compressed.pdf (dostęp 14.11.2025); *Operation Overload: An AI fuelled escalation of the Kremlin-linked propaganda effort*, https://checkfirst.network/operation-overload-an-ai-fuelled-escalation-of-the-kremlin-linked-propaganda-effort/ (dostęp 14.11.2025); *Operation Overload: Draining fact-checkers' resources*, 27.08.2024, https://ipi.media/ipimedia/operation-overload-draining-fact-checkers-resources/ (dostęp 10.11.2025); H. Padalko, *AI and Information Manipulation: Russia's Interference in the US Elections*, https://www.cigionline.org/static/documents/DPH-paper-Padalko_7Fz4cUS.pdf (dostęp 10.11.2025); *Russian Influence Operations as a tool of cognitive warfare in German Elections: Analysis of Methods, Objectives, and Effectiveness*, https://www.defencesciencereview.com.pl/pdf-209689-128083?filename=Russian%20Influence.pdf (dostęp 14.11.2025); *Stolen voices: Russia-aligned operation manipulates audio and images to impersonate experts*, https://www.isdglobal.org/digital_dispatches/stolen-voices-russia-aligned-operation-manipulates-audio-and-images-to-impersonate-experts/ (dostęp 10.11.2025).

ROSYJSKA OPERACJA DEZINFORMACYJNA „UNDERCUT" (podcięcie) – jedna z najnowszych rosyjskich ukrytych kampanii wpływu dezinformacyjnego w ramach wojny kognitywnej, która wykorzystuje zaawansowane technologie, zwłaszcza generowanie treści przez sztuczną inteligencję (AI), m.in. fałszywe materiały wideo i audio (*deepfakes*)

podające się za renomowane media, do szerzenia dezinformacji na platformach takich jak X (dawniej Twitter) i podszywania się pod inne źródła, by wpływać na opinię publiczną.

Operacja jest prowadzona od grudnia 2023 r. przez rosyjską Agencję Projektowania Społecznego (APS, ang. Social Design Agency) i ukazuje wieloaspektowy charakter operacji wpływu w celu nastawienia opinii publicznej przeciwko Ukrainie i osłabienia wsparcia Zachodu. APS jest odpowiedzialna za współpracę z rosyjską administracją prezydencką, planowanie strategiczne, monitorowanie i analizę źródeł zachodnich, planowanie narracji, produkcję treści i ich rozpowszechnianie. Operacja została objęta sankcjami przez USA, co dowodzi zdolności operacyjnej APS do prowadzenia wielu operacji wpływu równolegle dla wspierania globalnych celów wpływów rosyjskiej administracji prezydenckiej.

Operacja „Undercut” to element szerszej strategii Rosji mającej na celu destabilizację zachodnich sojuszy i przedstawienie ukraińskiego rządu jako nieskutecznego i skorumpowanego. Wykorzystuje ona sztuczną inteligencję do tworzenia fałszywych treści, podszywając się pod renomowane media, aby osłabić poparcie dla Ukrainy i wpłynąć na wybory w państwach demokratycznych.

Zgodnie z raportem Insikt Group Recorded Future[43] rosyjska operacja „Undercut” opiera się na fałszywych lub wprowadzających w błąd materiałach wideo oraz zdjęciach wykreowanych za pomocą sztucznej inteligencji, które mają udawać te publikowane przez znane media. Nagrania przedstawiały np. ukraińskich polityków jako skorumpowanych i podważały sens pomocy wojskowej dla Ukrainy, manipulując narracjami o rzekomej nieskuteczności dostarczanego tam zaawansowanego sprzętu wojskowego.

Operacja wykorzystuje zaawansowane metody manipulacji opinią publiczną, rozpowszechnia dezinformację skierowaną do odbiorców w Stanach Zjednoczonych, Ukrainie i Europie.

---

[43] Insikt Group Recorded Future – największa na świecie amerykańska firma zajmująca się analizą zagrożeń. Indeksuje internet, w tym otwartą sieć, dark web i źródła techniczne. Jej siedziba znajduje się w Bostonie, a biura i pracownicy są rozlokowani na całym świecie. Recorded Future współpracuje z ponad 1800 firmami i organizacjami rządowymi w ponad 75 krajach.

Kluczowe cechy operacji „Undercut”:

- dezinformacja;
- wykorzystanie sztucznej inteligencji do tworzenia przekonujących, ale fałszywych materiałów wideo i audio (deepfakes);
- fałszywe treści podszywające się pod autentyczne, wiarygodne źródła, zwiększając ich wiarygodność;
- działania prowadzone głównie na mediach społecznościowych, w tym na platformie X.

Jest to przykład nowoczesnej wojny informacyjnej, gdzie technologia AI jest narzędziem do tworzenia i dystrybucji fałszywych narracji.

Najważniejsze cele operacji „Undercut”:

- osłabianie zachodniego poparcia dla Ukrainy i sugerowanie, że pomoc militarna i finansowa dla Ukrainy jest nieskuteczna, kosztowna i nieopłacalna. Narracje te mają obniżać poparcie społeczne dla dalszego wsparcia, zarówno w Europie, jak i USA, poprzez próby podważenia poparcia dla umożliwienia Ukrainie ataków na cele w Rosji; oskarżenia Ukrainy o sponsorowanie ataków na Crocus City Hall i finansowanie „terrorystycznych” sił antywagnerowskich w Mali i Nigrze; promowania postępów sił rosyjskich w Kursku i na Krymie; podważenia skuteczności zachodniego sprzętu wojskowego w Ukrainie; promowania nowej rosyjskiej doktryny nuklearnej, która ma na celu odstraszenie ukraińskich ataków dalekiego zasięgu wymierzonych w Moskwę;
- dyskredytacja ukraińskich przywódców i ukazanie ukraińskich władz jako skorumpowanych, niekompetentnych lub niegodnych zaufania, co ma podważyć autorytet Kijowa i osłabić jego pozycję na arenie międzynarodowej oraz zmniejszyć poparcie społeczne dla dalszej pomocy finansowej i wojskowej dla Ukrainy, szczególnie wśród odbiorców europejskich;
- wzmocnienie antyukraińskich nastrojów w nadziei na ograniczenie napływu zachodniej pomocy wojskowej. Kampania próbuje również przedstawić zaangażowanie USA i UE jako w dużej mierze nieskuteczne i błędne;

– kształtowanie międzynarodowego postrzegania uczciwości wyborów w USA i próba przedstawienia Ukrainy jako odpowiedzialnej za drugą próbę zamachu na byłego prezydenta Trumpa; zaostrzenie wewnętrznych i międzynarodowych niepokojów związane z wyborami w UE i USA w 2024 r.;
– manipulowanie opinią publiczną w sprawie konfliktu izraelsko-palestyńskiego, zarzucając stronniczość Zachodu i manipulację danymi wywiadowczymi. Uwypuklając kwestie podziałów w polityce globalnej, operacja „Undercut” rozprasza i pogłębia podziały, osłabiając sojusze Zachodu i odwracając uwagę od wojny w Ukrainie;
– wzmacnianie podziałów i napięć społeczno-politycznych w społeczeństwach zachodnich, wsparcie skrajnie prawicowych narracji i krytyka przywódców UE z wykorzystaniem istniejących kontrowersji politycznych (np. wyborczych, społecznych kwestii wewnętrznych i konfliktów geopolitycznych), aby podsycać niepokój o stabilność polityczną Zachodu. Konta w mediach społecznościowych powiązane z operacją „Undercut” publikowały treści wspierające skrajnie prawicowe partie polityczne w Europie i wykorzystujące napięcia między państwami członkowskimi UE, Ukrainą i Brukselą w kwestiach takich jak stosunki UE–Rosja i wprowadzenie dodatkowych sankcji wobec Rosji. Narracje łączone były z aktualnymi wydarzeniami, aby bardziej efektywnie manipulować emocjami odbiorców. Łącząc los Ukrainy z tymi kontrowersyjnymi tematami, operacja próbuje podsycić niepokój i spolaryzować opinię publiczną;
– podważanie zaufania do mediów, instytucji i polityków poprzez podszywanie się pod znane i wiarygodne źródła informacji lub tworzenie profesjonalnie wyglądających fałszywych treści medialnych, co ma osłabiać zaufanie do niezależnych mediów i instytucji demokratycznych.

Metody i taktyki stosowane w ramach operacji:

– wykorzystanie treści generowanych przez sztuczną inteligencję, takich jak filmy, obrazy, głosy, które wyglądają jak produkowane

przez prawdziwe redakcje, co utrudnia ich wczesne rozpoznanie jako fałszywych;

- impersonacja mediów, podszywanie się pod znane media lub ich formaty, np. wykorzystanie podobnych nazw, logotypów czy układów graficznych z myślą o zwiększeniu wiarygodności treści w oczach odbiorców, tworzenie treści trudnych do odróżnienia od prawdziwych wiadomości. Wykorzystując elementy brandingu[44] szanowanych mediów, operacja zwiększa wiarygodność swoich treści, wprowadzając odbiorców w błąd i podważając zaufanie do autentycznych źródeł medialnych;
- wykorzystanie istniejących napięć między Unią Europejską a państwami członkowskimi, w tym w kwestiach pomocy dla Ukrainy i rosyjskich sankcji; zdyskredytowanie przywódców UE; zaostrzenie napięć związanych z konfliktem izraelsko-palestyńskim oraz krytyki igrzysk olimpijskich w Paryżu w 2024 r. Przykładowo treści w języku polskim określały przewodniczącą Komisji Europejskiej Ursulę von der Leyen mianem „marionetki" niemieckiego rządu wkrótce po jej reelekcji 18 lipca 2024 r. i oskarżały ją o wpływanie na polską politykę, twierdząc, że idee premiera Polski Donalda Tuska i von der Leyen „zniszczyły polską gospodarkę";
- zaostrzenie istniejących napięć między państwami członkowskimi UE a Ukrainą. Konta publikowały treści podsumowujące uzasadnione oświadczenia wydane przez wysokich rangą ministrów Niemiec, Polski, Węgier, Słowenii i Słowacji, próbując przedstawić je jako naciski państw UE na Brukselę, aby naprawiła stosunki z Rosją, zawetowała dalsze sankcje i zablokowała drogę Ukrainy do UE. Konta wykorzystywały również domniemaną odpowiedzialność Ukrainy (według Rosji)

[44] *Branding* – strategiczny proces tworzenia i budowania unikalnego wizerunku marki w umysłach konsumentów, aby wyróżnić ją na tle konkurencji i wywołać pozytywne skojarzenia, lojalność oraz więź emocjonalną. Obejmuje on wszystko – od nazwy, logotypu i kolorystyki, po komunikację, jakość produktów/usług, obsługę klienta i wartości, które firma reprezentuje, tworząc spójne doświadczenie na każdym etapie kontaktu z klientem.

za sabotaż gazociągu Nord Stream jako spekulatywny powód wzrostu napięć;
- wielojęzyczne kampanie i targetowanie: treści są tworzone i kierowane do odbiorców w różnych językach w zależności od regionu (angielskim, niemieckim, francuskim, polskim, tureckim, hebrajskim itd.), eliminując akcenty, które mogłyby zdradzić ich rosyjskie pochodzenie, co zapewnia, że przekaz dociera do szerokiego spektrum odbiorców i maksymalizuje wpływ;
- koordynacja z innymi operacjami: „Undercut” współdzieli taktyki, infrastrukturę i czasem narracje z innymi operacjami wpływu powiązanymi z rosyjskimi aktywami, takimi jak „Doppelgänger” czy inne kampanie wpływu w sieci.

Konta w ramach operacji „Undercut” promowały narracje dyskredytujące rząd USA i jego sojuszników, w tym Ukrainę, Wielką Brytanię, Francję, Niemcy, Polskę i Turcję. Konta próbowały manipulować opinią publiczną na temat taktycznych wydarzeń związanych z rosyjską inwazją na Ukrainę, w tym ukraińskiej inwazji na Kursk, odstraszając zachodnich sojuszników od jej wspierania za pomocą gróźb nuklearnych oraz dyskredytując ukraińskie przywództwo polityczne i wojskowe.

W okresie od sierpnia do września 2024 r. w ramach operacji „Undercut” opublikowano 2 filmy popierające ewoluującą doktrynę nuklearną Rosji wobec Ukrainy; pokazano, że Rosja robi to, aby umożliwić odwet w przypadku ataków konwencjonalnych na Moskwę, nawet ze strony państw nieposiadających broni jądrowej, takich jak Ukraina.

Zgodnie z raportem Insikt Group z listopada 2024 r. nie publikowano żadnych materiałów w święta rosyjskie, takie jak 7 stycznia, czyli prawosławne Boże Narodzenie, lub 9 maja (Dzień Zwycięstwa), co stanowi dodatkowe przesłanki wskazujące na to, że sieć jest obsługiwana z Rosji.

Operacja „Undercut” funkcjonuje równolegle do innych kampanii propagandowych, takich jak „Doppelgänger” czy „Przeciążenie”, i wykorzystuje podobne narzędzia dezinformacyjne, w tym fałszywe materiały (deepfake'i), podszywanie się pod zaufane media, treści wspierane przez boty i narracje dostosowane do lokalnych odbiorców. Operacja „Undercurt” w pewnym stopniu kontynuowała „Doppelgängera” pod kątem narracji czy adresowanych grup społecznych, jednak używała oddzielnej

infrastruktury, kont w mediach społecznościowych oraz mechanizmów dostarczania treści. Wygenerowała minimalne zaangażowanie, przez co nie można zaliczyć jej do udanych.

W przeciwieństwie do wykorzystywania fałszywych stron internetowych, operacja „Undercut” produkuje przede wszystkim filmy i obrazy wzbogacone sztuczną inteligencją, podszywające się pod główne media informacyjne, aby wzmocnić swoją narrację za pomocą popularnych hashtagów w krajach docelowych. Taktyka jest podobna do operacji „Overload” (śledzonej również jako „Matrioszka”), która dzieli infrastrukturę z kampanią „Doppelgänger”.

Operacja „Undercut” przesyła treści na platformy mediów społecznościowych za pośrednictwem kont prawdopodobnie obsługiwanych przez ludzi. Treści te przybierają 2 formy: filmów wzbogaconych sztuczną inteligencją oraz obrazów cytujących lub podszywających się pod zachodnie media. Dla porównania, konta „Doppelgängera” zwykle publikują zamaskowane linki do nieautentycznych stron internetowych.

Chociaż Insikt Group odkryła wiele podobieństw między operacjami „Undercut” i „Doppelgänger”, takich jak narracja, grupy docelowe i styl wizualny niektórych zasobów, sieci te wykorzystują odrębną infrastrukturę, konta w mediach społecznościowych i mechanizmy dostarczania, aby dotrzeć do grup docelowych.

Operacja „Undercut” nie jest odosobnionym przypadkiem, lecz częścią szerszej strategii informacyjnej Federacji Rosyjskiej, która obejmuje wojnę informacyjną i kognitywną – działania zmierzające do wpływania na przekonania i oceny społeczeństw oraz ich procesy decyzyjne bez użycia przemocy fizycznej. Rosyjska kampania dezinformacyjna jest systemowa i wielopłaszczyznowa, wykorzystuje różne narzędzia od mediów tradycyjnych po zaawansowane technologie cyfrowe, aby kształtować percepcję rzeczywistości zgodnie z interesami Kremla.

Zgodnie z wnioskiem z raportu Insikt Group z listopada 2024 r. oczekuje się, że APS będzie kontynuować prowadzenie operacji wpływu, w tym „Undercut”, prawdopodobnie odbudowując infrastrukturę dla kampanii „Doppelgänger” i wykorzystując sprawdzone treści oraz taktyki wzmacniania. Zlecone przez Administrację Prezydenta Rosji operacje mają na celu kształtowanie globalnej opinii publicznej na temat Ukrainy

i wykorzystywanie ważnych wydarzeń do podważania wsparcia dla tego kraju. Śledztwo, które wykorzystuje dane z Recorded Future, źródeł rządowych i innych raportów, podkreśla wartość współpracy międzysektorowej w celu ujawnienia i zakłócenia tych destabilizujących działań.

Operacja „Undercut” stała się jedną z najbardziej reprezentatywnych kampanii demonstrujących, jak sztuczna inteligencja i nowoczesne technologie mogą być wykorzystywane do tworzenia i rozpowszechniania dezinformacji. Wykorzystanie deepfake'ów, fałszywych serwisów informacyjnych i nieistniejących profili pozwala propagandzistom na tworzenie przekonujących ataków informacyjnych na dużą skalę.

Pomimo ograniczonego efektu krótkoterminowego takie operacje podważają zaufanie do tradycyjnych mediów, dzielą opinię publiczną i utrudniają skoordynowane działania międzynarodowe. Ujawnienie operacji „Undercut” po raz kolejny podkreśla potrzebę wzmocnienia środków identyfikacji i przeciwdziałania operacjom dezinformacyjnym, a także zwiększenia kompetencji cyfrowych użytkowników.

Olga Wasiuta

K. Chawryło, *Urwać łeb hydrze. Jak walczyć z rosyjską dezinformacją*, „Ośrodek Studiów Wschodnich” 2025, nr 91, https://www.osw.waw.pl/sites/default/files/PW_91_Urwa%C4%87-%C5%82eb-hydrze.pdf (dostęp 5.01.2026); R. Lakshmanan, *AI-Powered Fake News Campaign Targets Western Support for Ukraine and U.S. Elections*, 29.11.2024, https://thehackernews.com/2024/11/ai-powered-fake-news-campaign-targets.html (dostęp 3.01.2026); D. Nowak, *Nowy wymiar dezinformacji*, https://fibn.pl/archiwa/820#:~:text=Nowy%20wymiar%20dezinformacji-,Raportu%20%E2%80%9ERecorded%20Future%E2%80%9E (dostęp 5.01.2026); *“Operation Undercut” Shows Multifaceted Nature of SDA's Influence Operations*, 26.11.2024, https://static.fintek.pl/uploads/2024/12/TA-RU-2024-1126.pdf (dostęp 3.01.2026); *“Operation Undercut” Shows Multifaceted Nature of SDA's Influence Operations*, 26.11.2024, https://www.recordedfuture.com/research/operation-undercut-shows-multifaceted-nature-sdas-influence-operations?utm_source=chatgpt.com (dostęp 3.01.2026); *Russia's “Operation Undercut” Campaign Uses AI/Fake News to Undermine Ukraine Support*, 6.12.2024, https://www.global-influence-ops.com/russias-operation-undercut-campaign-uses-ai-fake-news-to-undermine-ukraine-support/?utm_source=chatgpt.com (dostęp 3.01.2026); *Threat intelligence – from tactical tool to strategic imperative*, https://pages.recordedfutureext.

com/2025-State-of-Threat-Intelligence-Report.html?utm_id=2%5B%E2%80%-A6%5Dampaign=whyrf2_stofti&utm_content=landingpage_home_hero&_gl=1*-1003glz*_gcl_au*NTE0NTAxODAxLjE3NjM5MTM1OTE (dostęp 4.01.2026); J. Vijayan, *'Operation Undercut' Adds to Russia Malign Influence Campaigns*, 27.11.2024, https://www.darkreading.com/cybersecurity-operations/operation-undercut-russia-malign-influence-campaigns?utm_source=chatgpt.com (dostęp 4.01.2026); G. Wojtulewicz, *Rosja wykorzystuje sztuczną inteligencję stworzoną przez Polaków do szerzenia dezinformacji?*, 12.12.2024, https://fintek.pl/rosja-wykorzystuje-sztuczna-inteligencje-stworzona-przez-polakow-do-szerzenia-dezinformacji/(dostęp 5.01.2026); Р. Мельник, *Дослідники виявили нову інформаційну операцію Росії з використанням ШІ-відео*, 12.12.2024, https://detector.media/infospace/article/235900/2024-12-12-doslidnyky-vyyavyly-novu-informatsiynu-operatsiyu-rosii-z-vykorystannyam-shi-video/ (dostęp 5.01.2026).

ROSYJSKA POWSTAŃCZA ARMIA (ros. Русская Повстанческая Армия, RPA) – paramilitarna rosyjska organizacja polityczna utworzona 29 grudnia 2014 r. w Kijowie. RPA jest niezależną organizacją zrzeszającą rosyjskich uchodźców i emigrantów, którzy zaczęli walczyć w szeregach sił ATO na wschodniej Ukrainie w ramach batalionów ochotniczych.

Rosyjska Powstańcza Armia została utworzona do walki z rosyjskim imperializmem i reżimem Putina, a jej głównym zadaniem jest przekształcenie Rosji w społeczeństwo demokratyczne, wolne od władzy oligarchów. „Już teraz Rosjanie walczą ramię w ramię z Ukraińcami przeciwko agresji Putina w Donbasie. Rosyjska Powstańcza Armia uważa za konieczne pomóc Ukraińcom w walce z imperialnym zagrożeniem ze strony Putina, a także widzi cel powstania przeciwko obecnemu reżimowi w Rosji w imię wolności ludzi" – napisano w oświadczeniu.

Już w 2015 r. Andriej Kuzniecow, znany rosyjski bloger opozycyjny, który wyemigrował z Rosji na Ukrainę, odważnie ogłosił utworzenie tzw. Rosyjskiej Powstańczej Armii. Ta niewielka grupa bojowników przyznała się do wielu incydentów w Rosji w tamtym czasie.

Tak, bojownicy RPA w swoim komunikacie wideo opublikowanym na YouTubie jesienią 2015 r. przypomnieli swoim rodakom, że jeszcze kilka lat temu Ukraińców uważali za braci, ale w wyniku „bękarckiej propagandy Putina" wszystko się zmieniło. „Krym został wypchnięty. Potem rozpętano rzeź, która miała na celu «wyzwolenie» Donbasu" – mówi jeden

z rosyjskich rebeliantów. „Reprezentujemy tutaj rosyjską armię rebeliantów, tych, którzy nie zdradzili swoich ideałów, którzy nie zdradzili swoich braci, Ukraińców" – dodał. „Teraz walczymy o wolny Donbas, wolny od putinowskiej junty i kremlowskiego drania".

22 stycznia 2015 r. na wniosek Prokuratury Generalnej FR do opublikowanego 29 grudnia 2014 r. rejestru stron zabronionych dodano film *Utworzenie Rosyjskiej Powstańczej Armii (RPA)*, który od tego czasu uzyskał ponad 9 tys. wyświetleń na YouTubie. Zablokowano również nagranie wideo z konferencji prasowej RPA z 3 stycznia 2015 r., zawierający „nawoływania do walki z reżimem Putina przy użyciu broni w ręku". W konsekwencji, 28 stycznia 2015 r. Roskomnadzor umieścił witrynę udostępniającą wideo z YouTube w rejestrze stron zakazanych. Tego samego dnia z YouTube'a usunięto film *Utworzenie Rosyjskiej Powstańczej Armii (RPA)*, po czym odblokowano stronę na terytorium Rosji.

Na swojej stronie VK przedstawiciele Rosyjskiej Powstańczej Armii napisali: „My, obywatele Rosji i etniczni Rosjanie, znajdujący się za granicą, ze względu na naszą aktywną postawę obywatelską, jesteśmy stawiani przez państwo w sytuacji, w której nie możemy swobodnie wyrażać swoich opinii i brać udziału w życiu kraju. W tej sytuacji zmuszeni byliśmy opuścić nasz dom i kontynuować walkę na terytorium zaprzyjaźnionych z nami państw, które także cierpiały z powodu imperializmu oligarchicznego. Naszym celem jest utworzenie Rosyjskiej Powstańczej Armii jako przeciwwagi dla obecnego reżimu. Jesteśmy gotowi bronić interesów narodów Rosji zarówno w walce politycznej, jak i z bronią w ręku. Dążymy do celów stworzenia nowej, wolnej Rosji, która nie będzie postrzegana przez cały świat jako zagrożenie, ale będzie wiarygodnym i szanowanym sojusznikiem i partnerem".

RPA pozycjonuje się jako „armia rosyjskiej opozycji" w konfrontacji z władzami rosyjskimi. Organizacja prowadzi działalność podziemną na terytorium Federacji Rosyjskiej i wyznaje nacjonalizm, narodowy liberalizm, centroprawicę, atlantycyzm, antykomunizm, krytykę islamizmu i eurazjatyzmu. „Ogłaszając utworzenie Rosyjskiej Powstańczej Armii, wzywamy wszystkich Rosjan wolnej woli i czystych serc do włączenia się w naszą walkę o odnalezienie przez naród rosyjski swojej historycznej ojczyzny, o położenie kresu niekończącego się trudu w zdobywaniu

tożsamości narodowej i suwerenności. Wzywamy do walki o nasze rosyjskie państwo narodowe. O Rosję Narodów, a nie o państwo imperialnej nomenklatury neosowieckiej, dla którego państwo to jest celem samym w sobie i usprawiedliwieniem wszelkiego ucisku praw i wolności… Jesteśmy pokoleniem, które zmieni bieg historii. Stawiamy sobie cel, dla którego warto żyć, walczyć i umierać. Tym celem jest wolność".

Wymogi i cele RPA zostały określone w manifeście:

- obalenie reżimu Putina i nomenklatury neosowieckiej, opartej na sile przemocy i ucisku, która przywłaszczyła sobie bogactwo i zasoby mineralne narodów Rosji;
- zakończenie wojny w Ukrainie i wszelkich prób sił odwetowych wzniecania konfliktów międzyetnicznych na przestrzeni poradzieckiej;
- utrwalenie suwerenności narodu rosyjskiego w Federacji Rosyjskiej i na świecie.

W swoim manifeście organizatorzy RPA wskazali, że szkolenie „bojowników" tej jednostki rozpoczęło się 9 stycznia 2015 r. „Wzywamy w nasze szeregi Rosjan z Estonii, Łotwy, Litwy, Ukrainy, USA i innych krajów, którzy zmuszeni byli uciekać z Rosji, która pozbawiła nas możliwości swobodnego życia, pracy i tworzenia, aby stanęli z nami ramię w ramię i zakończyli historyczną niesprawiedliwość wobec naszego narodu" – napisano na portalu Ruposters.ru.

Po obaleniu znienawidzonego przez siebie „reżimu" zamierzają utworzyć państwa, w których „równość wszystkich narodów Federacji Rosyjskiej i ich rzeczywiste prawo do rozwoju narodowego, samostanowienia i niepodległości państwa" będą miały na celu „wstąpienie do NATO". Finansowanie tej armii ma się odbywać, jak wynika z tekstu dokumentu, za pośrednictwem instytucji bankowych ukraińskiego biznesmena Igora Kołomojskiego.

RPA ustanawia następujące główne zasady jako podstawę nowej państwowości narodów Rosji:

1. Równość wszystkich narodów Federacji Rosyjskiej i ich rzeczywiste prawo do rozwoju narodowego, samostanowienia i niepodległości państwa. Przestrzeganie Konstytucji Federacji Rosyjskiej i ustaw podstawowych.

2. Rzeczywista, a nie fikcyjna federalizacja i decentralizacja władzy w Rosji. Powrót wybieralnej władzy na wszystkich poziomach. Głównym organem ustawodawczym Federacji Rosyjskiej jest parlament. Tworzenie partii regionalnych i republikańskich oraz form rządów. Budżet regionalny powinien działać na korzyść regionu.
3. Zabezpieczenie ziemi narodowi rosyjskiemu bez uszczerbku dla interesów innych narodów Rosji. Rosyjska reprezentacja narodowa w organach rządu federalnego – parlamencie.
4. Utrzymanie pokoju i nawiązanie przyjaznych stosunków ze wszystkimi krajami oraz pełny rozwój współpracy międzynarodowej. Przyznanie republikom narodowym w ramach Federacji Rosyjskiej samodzielnego wyboru współpracy gospodarczej i rozwoju. Wzmocnienie relacji w ramach polityki zagranicznej z krajami Europy Wschodniej, które są najbliżej Rosji kulturowo i historycznie. Pozycjonowanie Rosji jako równoprawnego uczestnika tworzenia Nowej Europy.
5. Desowietyzacja społeczeństwa rosyjskiego (historia, kultura, zabytki).
6. Liberalizacja gospodarki, reformy i przekształcenia mające na celu zmniejszenie przepaści pomiędzy bogatymi a biednymi dla wzbogacenia narodu, a w szczególności każdego obywatela. Tworzenie warunków dla wolnego handlu i konkurencji. Uczciwa prywatyzacja z prawnie ustalonymi zobowiązaniami inwestycyjnymi gwarantującymi zatrudnienie obywateli Federacji Rosyjskiej. Atrakcyjność inwestycyjna dla kapitału zagranicznego, uczciwe zasady gry zbudowane na odpowiednich ramach prawnych. Nacjonalizacja monopoli i przedsiębiorstw zajmowanych przez współpracowników Putina, a następnie prywatyzacja.
7. Bezpłatna sprzedaż ziemi obywatelom Federacji Rosyjskiej. Amnestia ziemska. Wszystko, co znajduje się na ziemi i pod ziemią, podglebiem, należy do właściciela i tylko on ma prawo tym rozporządzać według własnego uznania.
8. Zapewnienie nienaruszalności praw własności prywatnej i wyników pracy. Niedopuszczalność rewizji prywatyzacji. Zmniejszenie udziału państwa w gospodarce. Likwidacja monopoli. Prywatyzacja

przedsiębiorstw państwowych i sprzedaż majątku państwowego obywatelom Federacji Rosyjskiej.

9. Równość wobec prawa, bez względu na zasługi dla państwa. Nikt nie ma prawa żądać zwiększenia praw lub odmiennego traktowania ze względu na deklarowaną wyjątkowość. Równy dostęp do podstawowej edukacji i opieki zdrowotnej. Ustanowienie Rosji jako państwa prawnego. Dekryminalizacja i utworzenie niezależnego systemu sądowniczego i prawnego. Zapewnienie możliwości zaskarżenia wątpliwych i niesłusznych orzeczeń sądów. Likwidacja Sądu Basmannego w Moskwie i wymiaru sprawiedliwości „Basmannego" w Rosji.
10. Każdy obywatel Federacji Rosyjskiej ma prawo do ochrony swojego życia, rodziny i mienia. Swobodna sprzedaż broni.
11. Wolność słowa i zgromadzeń. Nikt nie ma prawa być potępiany za słowa i opinie.
12. Federacja Rosyjska jest państwem świeckim. Kościół jest oddzielony od państwa. Żadnej religii nie można ustanowić jako państwowej ani obowiązkowej. Organizacje religijne nie mają prawa wspierać instytucji państwowych i są zobowiązane do prowadzenia swojej działalności wyłącznie w oparciu o własne środki.
13. Lustracja, zgodnie z którą nikt nie może być skazany za pracę w organach państwowych za czasów reżimu Putina, lecz będzie musiał opuścić zajmowane stanowisko i złożyć sprawozdanie na temat charakteru uzyskiwanych dochodów, legalności podejmowanych decyzji oraz faktów dotyczących naruszenia prawa. Rzeczywista ocena prawna działań reżimu Putina. Postawienie przed sądem osób odpowiedzialnych za katastrofę w Rosji. Nie uznajemy osobistego prawa Putina do rozporządzania majątkiem obywateli Rosji w imię geopolitycznych gier prezydenta.

W marcu 2024 r. Rosyjska armia ogłosiła zniszczenie domu z żołnierzami Sił Zbrojnych Federacji Rosyjskiej w Kozinkach, gdzie później była zasadzka na przybyłą grupę ewakuacyjną specnazu GRU.

Olga Wasiuta

A. Pat, *Украина: Русская повстанческая армия обнародовала свой манифест*, 29.12.2014, https://newsland.com/post/3191814-ukraina-russkaia-povstancheskaia-armiia-obnarodovala-svoi-manifest (dostęp 17.04.2025); N. Peterson, *Russian Dissident Looks to Raise 'Rebel Army' in Ukraine to Overthrow Putin*, 18.05.2015, https://live-daily-signal.pantheonsite.io/2015/05/18/russian-dissident-looks-to-raise-rebel-army-in-ukraine-to-overthrow-putin/ (dostęp 10.05.2024); J. Rogoża, *Sądownictwo w Federacji Rosyjskiej*, 2021, https://www.studocu.com/pl/document/uniwersytet-marii-curie-sklodowskiej-w-lublinie/dietetyka/j-rogoza-sadownictwo-w-federacji-rosyjskiej-2021/61082192 (dostęp 19.04.2025); *В батальоне ОУН воюют россияне, которых на родине обвиняют в сепаратизме*, 10.04.2015, https://news.obozrevatel.com/politics/65823-v-batalone-oun-voyuyut-rossiyane-kotoryih-na-rodine-obvinyayut-v-separatizme.htm (dostęp 10.05.2025); М. Векленко, *Поджоги, диверсии, вооруженное подполье. Русская Повстанческая Армия начала войну против Кремля*, 18.11.2016, https://patrioty.org.ua/blogs/podzhogi-diversii-vooruzhennoe-podpole-russkaia-povstancheskaia-armiia-nachala-voinu-protiv-kremlia-142355.html (dostęp 10.05.2025); *В Киеве создадут Российскую повстанческую армию для борьбы с Путиным*, 28.12.2014, https://incident.obozrevatel.com/crime/53702-v-kieve-sozdadut-rossijskuyu-povstancheskuyu-armiyu-dlya-borbyi-s-putinyim.htm (dostęp 10.05.2025); *В Киеве создана Русская Повстанческая Армия. Разбор их политической программы*, 28.12.2014, https://sputnikipogrom.com/politics/26996/lets-fight-for-mnogonationalnost/ (dostęp 17.04.2025); *Манифест Русской Повстанческой Армии*, 8.02.2016, https://dobrovoletz.blogspot.com/2016/02/blog-post.html (dostęp 17.04.2025); А. Кузнецов, *Именно в эмиграции происходит та сплавка российской оппозиции, которая была на украинском Майдане*, 8.09.2015, http://eurorussians.com/russian-rebel-army/ (dostęp 19.04.2025); *Роскомнадзор заблокировал YouTube*, 28.01.2015, https://www.securitylab.ru/news/470566.php (dostęp 29.03.2025); *Роскомнадзор заблокировал YouTube за «Создание Русской Повстанческой Армии (РПА)»*, 28.01.2015, https://ru.wikinews.org/wiki/%D0%A0%D0%BE%D1% (dostęp 29.03.2025); *Русская Повстанческая Армия*, https://vk.com/russian_rebel_army (dostęp 17.04.2025); *Русская повстанческая армия, не путать с „боевиками"*, 21.03.2024, https://twitter.com/FilonenkoOles/status/1770720871931322791 (dostęp 17.04.2025); *«Русская повстанческая армия» призывает освободить Донбасс от «кремлевского ублюдства»*, https://antikor.com.ua/ru/articles/63584-russkaja_povstancheskaja_armija_ prizyvaet_osvoboditj_donbass_ot_kremlevskogo_ubljudstva_video (dostęp 17.04.2025).

ROSYJSKIE OPERACJE FIMI (ang. Foreign Information Manipulation and Interference – manipulacja informacjami i ingerencja w informacje)

– wzorzec celowych, skoordynowanych działań podmiotów państwowych lub niepaństwowych mających na celu manipulowanie środowiskiem informacyjnym w celu negatywnego wpływu na demokratyczne wartości, procesy i instytucje. Wykracza to poza prostą dezinformację, koncentrując się na manipulacyjnych zachowaniach mających na celu osłabienie procesów politycznych, i może obejmować cyberataki, rozpowszechnianie narracji polaryzujących oraz tworzenie syntetycznych mediów. Te operacje polegają na wykorzystaniu sztucznej inteligencji do tworzenia fałszywych filmów wideo lub nagrań audio polityków, co miało miejsce w Mołdawii i Wielkiej Brytanii. FIMI może być wykorzystywana do wpływania na wyniki wyborów poprzez zniechęcanie do głosowania lub wzbudzanie wątpliwości co do samego procesu.

Rosyjskie kampanie dezinformacyjne nie są tylko luźnym zbiorem przypadkowych kłamstw – to celowa, zaplanowana, zorganizowana i skoordynowana manipulacja będąca wytworem starannie zbudowanego systemu. 19 marca 2025 r. szefowa unijnej dyplomacji Kaja Kallas przedstawiła trzeci raport Europejskiej Służby Działań Zewnętrznych (ESDZ) na temat zagrożeń związanych z zagranicznymi manipulacjami informacjami i ingerencjami w informacje (FIMI). Dokument ten koncentruje się na ujawnianiu operacji FIMI i rozwija ustalenia pierwszego raportu poświęconego analizowaniu FIMI, a także drugiego, który kompleksowo omawia sposoby reagowania. Trzeci analizuje 4 elementy systemu FIMI – oficjalne kanały państwowe, media kontrolowane przez państwo, kanały powiązane z państwem i kanały zbieżne z państwowymi.

Struktura rosyjskich operacji FIMI jest opisywana w raporcie poprzez analogię do góry lodowej, aby pokazać, że duża część tego systemu manipulacji skrywa się pod powierzchnią. Raport przedstawia to zjawisko z szerszej perspektywy, co umożliwia analizę zasięgu sieci manipulacyjnych i wzajemnych powiązań między nimi w systemie, który nazwano galaktyką FIMI.

FIMI koncentruje się na manipulacjach, a nie tylko na samej fałszywej narracji. Opisuje schemat zachowań, które w większości nie są nielegalne, ale które zagrażają lub wpływają negatywnie na wartości, procedury i procesy polityczne. Może być prowadzona zarówno przez podmioty

państwowe, jak i niepaństwowe, a także wykorzystywać pośredników działających w kraju lub za granicą.

Nazwy tych kampanii są dosyć chwytliwe, np. „Doppelgänger" („Sobowtór"), „False Façade" („Fałszywa Fasada"), „Overload", „Portal Kombat" czy „Matrioszka". Mają tę zaletę, że przyciągają uwagę do tych manipulacji informacjami, ale mogą czasami być mylące i nie wskazywać jasno na realne zagrożenie, które kryje się za tymi nazwami.

Głównym celem jest wprowadzanie w błąd, oszukiwanie lub zmuszanie opinii publicznej do osiągnięcia określonych celów politycznych. Chociaż dezinformacja jest jej elementem, FIMI obejmuje szerszy zakres taktyk mających na celu ingerowanie w procesy demokratyczne i wydarzenia polityczne. FIMI zagraża wartościom demokratycznym poprzez podważanie zaufania publicznego, ingerowanie w wybory i polaryzowanie społeczeństw.

Zagraniczne manipulacje informacjami i ingerencje w nie opierają się na rozległej, wzajemnie połączonej sieci – galaktyce FIMI. Składa się ona zarówno z jawnych, jak i ukrytych kanałów działających na wielu platformach, których celem jest rozpowszechnianie, ponowne wykorzystywanie, wzajemna promocja oraz ukrywanie prawdziwego pochodzenia treści manipulacyjnych. Mołdawia jest od dawna wykorzystywana jako miejsce testowania i rozwijania rosyjskich operacji FIMI – często intensyfikacja działań ma miejsce właśnie w okolicach ważnych wydarzeń, takich jak wybory, wizyty międzynarodowe lub protesty, aby zmaksymalizować wpływ.

Na każdego oficjalnego rządowego lub kremlowskiego propagandystę działającego w finansowanych przez państwo kanałach rosyjskiej telewizji przypada wiele mniej lub bardziej widocznych kanałów – stron internetowych, blogów, kont w mediach społecznościowych, influencerów i pseudokomentatorów, którzy nagłaśniają, zaprzeczają, wyśmiewają, podkręcają, kwestionują lub zaciemniają przekaz. A wszystko po to, by realizować szerszy cel Kremla, jakim jest zdominowanie przestrzeni informacyjnej.

FIMI bazuje na szerokim, dobrze finansowanym i stworzonym specjalnie do tego celu systemie, który składa się z części widocznych i niewidocznych. Obejmuje on zarówno elementy państwowe, jak i niepaństwowe. Jest elastyczny, doskonale się dopasowuje i wykorzystuje ukierunkowane

podejście, aby kształtować opinie i wpływać na zachowania odbiorców w krajach sąsiadujących z Rosją i bardziej odległych miejscach.

Wcześniejsze badania dotyczące rosyjskich działań dezinformacyjnych i manipulacyjnych dostarczyły informacji na temat złożonego systemu kryjącego się za kremlowskimi kłamstwami. Porównywano go do cyfrowej hydry z wieloma ramionami i zdolnością do zmieniania się i przekształcania pod presją.

Trzeci raport ESDZ na temat zagrożeń FIMI rozwija wcześniejsze ustalenia badaczy i daje świeże spojrzenie na system kryjący się za rosyjskimi operacjami FIMI, ukazując go przez pryzmat wskaźników technicznych i behawioralnych. To nowy sposób obserwacji stron internetowych, kont w mediach społecznościowych i innych kanałów cyfrowych wykorzystywanych w manipulacji informacjami, który pozwala zobaczyć więcej niż tylko wierzchołek góry lodowej.

4 poziomy struktury FIMI:

1. Oficjalne kanały państwowe, które w najbardziej otwarty i jawny sposób pokazują swoje powiązania z Kremlem. Zaliczają się do nich rosyjskie władze, instytucje oraz ich przedstawiciele, którzy wyrażają oficjalne stanowisko Rosji. Na przestrzeni ostatnich lat główny dezinformacyjny przekaz płynął z Kremla i od przedstawicieli władz, takich jak minister spraw zagranicznych czy szef rosyjskiej agencji wywiadowczej. W wielu przypadkach to oni dyktowali reszcie systemu ton nagłaśniania pewnych fałszywych narracji. W niektórych przypadkach sami rozpowszechniali teorie spiskowe z anonimowych źródeł, wynosząc je na najwyższy poziom polityczny. Te oficjalne kanały mają też dostęp do międzynarodowych forów, które często wykorzystują, aby legitymizować prokremlowską dezinformację na najwyższym szczeblu politycznym.
2. Źródła kontrolowane przez państwo, które są finansowane, zarządzane i objęte kontrolą redakcyjną przez podmioty państwowe lub wyznaczone przez państwo. Ich powiązania z państwem rosyjskim pozostają jawne. Do tej kategorii zalicza się większość rosyjskich federalnych kanałów telewizyjnych, takich jak RT czy Sputnik. Wiele z nich jest objętych sankcjami UE za wspieranie rosyjskiej inwazji na Ukrainę.

3. Kanały powiązane z państwem, które działają pod nadzorem państwowym, ale publicznie nie ujawniają swoich powiązań. Funkcjonują one w szarej strefie, ukrywając informacje o swoim pochodzeniu i zacierając granice między wpływami władz, mediów i podmiotów internetowych, aby realizować określone cele polityczne i strategiczne. Ich zadaniem jest kształtowanie narracji, manipulowanie opiniami, podsycanie podziałów i działanie w nieprzejrzysty sposób. Powiązanie ich z konkretnym sprawcą (np. Kremlem) wymaga badań i stałych wysiłków.

Dobrym przykładem tego rodzaju źródła może być NewsFront – portal zarejestrowany na terenie bezprawnie zajętego Krymu i działający w wielu językach europejskich, określający swoją działalność jako „dziennikarstwo dokumentalne". Tak naprawdę został założony przez osoby blisko związane z państwem rosyjskim i mające związki z rosyjskimi służbami wywiadu zagranicznego. Od lat publikuje on prokremlowskie narracje i jest zaangażowany w szersze operacje manipulowania informacjami w internecie, nagłaśniając rosyjski przekaz. Działania NewsFront były ujawniane przez platformy internetowe i rządy, co pokazało, że w niektórych przypadkach informacje z otwartych źródeł muszą być uzupełniane o poufne lub zastrzeżone dane, aby możliwe było wiarygodne powiązanie ich z konkretnym kanałem.

Innym przykładem jest kampania „Doppelgänger", wielostronna operacja FIMI mająca swoje źródło w Rosji, w której uczestniczyła cała sieć nieprawdziwych stron internetowych i która była wymierzona w Ukrainę i wybory do Parlamentu Europejskiego.

4. Kanały zbieżne z państwowymi – źródła, których przy obecnym stanie wiedzy nie można powiązać z kontrolą lub finansowaniem przez państwo, jednak zestaw pewnych wskaźników technicznych i behawioralnych (takich jak wspólna infrastruktura, schematy systematycznego rozpowszechniania tych samych narracji dezinformacyjnych) wskazuje na wysoką i powtarzalną zbieżność z innymi znanymi i sklasyfikowanymi już częściami rosyjskiej infrastruktury FIMI. To np. konta w mediach społecznościowych, blogi lub strony internetowe podszywające się pod inne źródła odgrywały istotną

rolę w niedawno ujawnionych rosyjskich operacjach wywierania wpływu, np. „Fałszywej Fasadzie" lub „Portal Kombat".

Jak dotąd nie udało się ich powiązać z Kremlem, jednak wciąż odgrywają systemową rolę w operacjach FIMI i są integralną częścią rosyjskiego systemu manipulacji informacjami i ingerencji w informacje.

Te 4 warstwy nie funkcjonują jednak w oderwaniu od siebie; tworzą jednolitą infrastrukturę – sieć, w której różne kanały, zarówno przypisywane Rosji, jak i nieprzypisane żadnemu podmiotowi, współdziałają ze sobą w celu koordynacji działań w zakresie manipulacji informacjami i wywierania wpływu. Tę sieć nazywamy galaktyką operacji FIMI.

Na podstawie analizy 505 incydentów FIMI, opisanych w raporcie, udało się zidentyfikować 38 tys. unikalnych kanałów, z których każdy odgrywał określoną rolę w tej galaktyce manipulacji informacjami. Aby lepiej zrozumieć ich wzajemne powiązania oraz *modus operandi*, w raporcie przeanalizowano 2055 najbardziej aktywnych kanałów, za pośrednictwem których operacje manipulacji informacjami są wzmacniane i koordynowane. Należą do nich najważniejsze media kontrolowane przez państwo lub z nim powiązane, takie jak – w przypadku Rosji – RIA Nowosti, TASS, RT, Sputnik Africa itp. oraz – w przypadku Chin – CGTN, Global Times, Xinhua i inne. Im większa sieć powiązań, tym częstsze zaangażowanie kanału w incydenty FIMI i tym większe znaczenie danego kanału w ogólnej architekturze operacji FIMI.

Chińska infrastruktura FIMI również opiera się na kontrolowanych przez państwo mediach pełniących funkcję kluczowych węzłów odpowiedzialnych za produkcję i dystrybucję treści. W szczególności chińskie profile dyplomatyczne odgrywają rolę węzłów wzmacniających w tej galaktyce. Oznacza to, że systematycznie udostępniają i nagłaśniają treści rozpowszechniane przez kluczowe węzły, takie jak kanały CGTN i Global Times. Jednak poza zidentyfikowanymi i przypisanymi elementami galaktyki Chiny wykorzystują także pozornie niezależne kanały, aby potajemnie rozszerzać swoje działania w zakresie manipulacji informacjami.

Oprócz manipulacji informacją Rosja stosuje inne metody destabilizacji państw UE; to szeroki wachlarz narzędzi hybrydowych obejmujących agentów wpływu i pseudoekspertów. Wszystko to mieści się w ramach

koncepcji Zagranicznej Manipulacji Informacją i Ingerencji (FIMI). Termin ten jest szerszy od „dezinformacji" będącej częścią FIMI.

FIMI nie jest nową praktyką, Rosja stosowała tzw. „środki aktywne" już w czasach sowieckich. Termin ten był używany w odniesieniu do operacji mających na celu wpływanie na politykę innych państw. Do radzieckich środków aktywnych należały dyplomacja, propaganda, agitacja, dezinformacja, fałszowanie dokumentów, umieszczanie materiałów w prasie oraz operacje mające na celu wywieranie wpływu politycznego.

FIMI jest zasadniczo tym samym co „środki aktywne", ale praktyczny mechanizm, na którym się opiera, uległ zmianie. Treść i cele pozostają te same, natomiast forma stała się bardziej złożona, a system – rozwinięty.

Dziś rosyjska dezinformacja nabiera charakteru sieci. Rosja ma swoje klucze do każdego regionu, dostosowuje się do bieżących wydarzeń w krajach, zna wewnętrzne problemy i nastroje, punkty newralgiczne i nimi manipuluje.

W przypadku Polski stosuje np. taktykę zniechęcania i nieufności wobec polskich i europejskich instytucji, podsyca już istniejące problemy społeczne i stara się wprowadzać retorykę antyukraińską, antyeuropejską, antynatowską itd.

Takie dostosowywanie narracji do konkretnych krajów zostało również wykorzystane podczas wyborów do Parlamentu Europejskiego, które odbyły się latem 2024 r. Biorąc pod uwagę, że głosowało 450 mln osób z 27 krajów, różnorodność i liczba dezinformacji oraz manipulacyjnych wpływów jest ogromna.

Ponadto dużym obszarem dezinformacji, nie tylko w kontekście wyborów, ale ogólnie, jest dezinformacja dotycząca migrantów. Kolejną grupę stanowiły narracje zniesławiające; np. Ursulę von der Leyen oskarżono o posiadanie przodków związanych z nazizmem. Te narracje się powtarzają, nawet jeśli niektóre z nich są dostosowane do lokalnego kontekstu, ale mają też pewien wymiar ponadnarodowy.

Jak pokazuje galaktyka, architektura FIMI została zaprojektowana tak, aby była zróżnicowana, trwała i elastyczna wobec odbiorców docelowych – nie opiera się więc wyłącznie na jednej platformie; może obejmować konta na głównych platformach mediów społecznościowych, np. X (dawniej Twitter), Facebook, Telegram, YouTube i TikTok, a także kontrolowane

przez państwo lub nieautentyczne serwisy informacyjne. Treści mogą być przekształcane w różne formaty – filmy, artykuły, memy, materiały generowane przez sztuczną inteligencję – wszystko po to, by skutecznie dostarczać manipulacyjne narracje podatnym grupom odbiorców. A „pranie" informacji stanowi kluczową technikę służącą do ukrywania źródła manipulacyjnych treści.

Podobnie jak w poprzednich latach najbardziej aktywnymi źródłami zagrożeń FIMI były Rosja i Chiny. Ich taktyki, techniki i procedury (TTP) nieustannie ewoluują, aby wykorzystywać pojawiające się nowe technologie i obchodzić nakładane restrykcje. W ostatnich 2 latach częściej korzystano ze sztucznej inteligencji, która umożliwia i ułatwia tworzenie treści, co wykorzystywały m.in. państwowe podmioty FIMI, takie jak RIA Nowosti, a także pozwala na automatyzację i zwiększenie skali dystrybucji treści.

FIMI, czy też wykorzystywanie informacji jako broni, jest dla Kremla narzędziem do realizacji celów geopolitycznych, a w 2025 r. było także próbą budowania „fałszywej fasady", za którą próbowano ukrywać operacje wybielania informacji. Rosja starała się wykorzystywać konkretne lokalne problemy, szerząc starannie dobrane i ukierunkowane treści, a zwłaszcza biorąc na celownik wybory w różnych miejscach świata, jednak głównym elementem rosyjskich operacji FIMI w 2025 r. było – podobnie jak przez 3 lata pełnoskalowej wojny – osłabianie Ukrainy i zachodniego wsparcia dla niej.

Na celowniku rosyjskich operacji FIMI, poza UE, znalazła się także Mołdawia. Przeprowadzone na przełomie października i listopada 2024 r. wybory prezydenckie i referendum w sprawie członkostwa Mołdawii w UE wywołały znaczną eskalację rosyjskich operacji. Rosja wykorzystuje złożoną, wielopoziomową i elastyczną infrastrukturę FIMI. Działania te strategicznie łączyły istniejącą już infrastrukturę z nowo opracowanymi materiałami i kampaniami mającymi na celu wywieranie wpływu na wyborców i manipulowanie ich zachowaniami. Co istotne, rosyjska infrastruktura FIMI, wykorzystywana wcześniej przeciwko Ukrainie, została użyta do ataków na Mołdawię, a jej sieci i narracje zostały dopasowane do nowego frontu ingerencji. Na celowniku Kremla znalazły się także wybory we Francji i Niemczech.

Analiza próby 505 incydentów FIMI wskazuje jasno, że stanowi globalne zagrożenie o istotnych implikacjach lokalnych, szczególnie w kontekście wyborów zarówno w UE, jak i na świecie. Przykładowo rosyjskie podmioty FIMI w 2024 r. systematyczne prowadziły operacje wymierzone w wybory europejskie, stopniowo intensyfikując działania w tygodniach poprzedzających głosowanie i kontynuując je także po wyborach.

W 2025 r. rosyjskie operacje FIMI osiągnęły bezprecedensowy poziom wyrafinowania, integrując zaawansowaną sztuczną inteligencję z klasycznymi technikami hybrydowymi. Działania te są ukierunkowane przede wszystkim na destabilizację państw UE i NATO, podważanie wsparcia dla Ukrainy oraz ingerencję w procesy demokratyczne.

Kluczowe trendy i incydenty w 2025 r.

- ingerencje wyborcze: rosyjskie sieci, w tym podmioty takie jak Social Design Agency, przeprowadziły masowe kampanie przed wyborami prezydenckimi w Polsce (maj/czerwiec 2025). Zidentyfikowano ponad 10 tys. kont w mediach społecznościowych szerzących narracje mające wpłynąć na wynik wyborów. Podobne operacje odnotowano w Czechach oraz w Niemczech, gdzie stosowano deepfake'i uderzające w czołowych polityków (np. Annalenę Baerbock i Roberta Habecka);
- operacja „Doppelgänger": Rosja kontynuuje klonowanie stron znanych mediów i instytucji publicznych, aby uwiarygadniać dezinformację. W marcu 2025 r. raporty wskazały na użycie ogromnych cyfrowych arsenałów, w tym tysięcy zautomatyzowanych kanałów;
- zatruwanie modeli AI: nowym zjawiskiem jest „zatrucie" (ang. *poisoning*) dużych modeli językowych (LLM). Rosyjskie sieci dążą do wprowadzenia kremlowskich narracji bezpośrednio do systemów AI, co ma na celu manipulowanie „cyfrową pamięcią" i przyszłymi odpowiedziami generatywnymi;
- eskalacja podczas ćwiczeń Zapad 2025: operacje informacyjne stały się integralną częścią manewrów wojskowych. Wykorzystano m.in. incydenty z rosyjskimi dronami naruszającymi przestrzeń powietrzną Polski we wrześniu 2025 r., by budować strach przed wojną z NATO i testować spójność Sojuszu.

Cele strategiczne FIMI w latach 2025–2026:

- podważanie instytucji: erozyjne działania wymierzone w zaufanie do rządów, mediów i procesów wyborczych;
- narracje antyukraińskie: przekonywanie społeczeństw zachodnich, że pomoc Ukrainie jest bezcelowa lub szkodliwa dla ich gospodarek;
- wojna kognitywna: wykorzystywanie polaryzacji społecznej (np. wokół kwestii światopoglądowych czy płci) do pogłębiania podziałów wewnętrznych.

UE i NATO wzmocniły mechanizmy obronne poprzez tzw. FIMI Toolbox oraz nową inicjatywę – Europejska Tarcza Demokracji (European Democracy Shield). W lipcu i grudniu 2025 r. nałożono kolejne sankcje na rosyjskie organizacje (m.in. Rybar[45], fundacja Pravfond[46]) i osoby odpowiedzialne za prowadzenie wojny informacyjnej. Monitoringiem i zwalczaniem tych zagrożeń w Polsce zajmują się m.in. Rządowe Centrum Bezpieczeństwa oraz biura analityczne takie jak EUvsDisinfo.

Olga Wasiuta

3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations, 2025, https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf (dostęp 5.12.2025); *A glossary: who is who in the FIMI zoo?*, 22.04.2025, https://euvsdisinfo.eu/a-glossary-who-is-who-in-the-fimi-zoo/ (dostęp 5.12.2025);

---

[45] Rybar – rozbudowany projekt i popularny kanał w Telegramie prowadzony przez rosyjskiego blogera Michaiła Zwinczuka, który ma w sieci medialnej ponad 150 kanałów o łącznej widowni 13 mln osób w segmencie rosyjskim, zaś w zagranicznym – 110 kanałów i łącznie 3 mln widzów. Miesięczny budżet projektu to 4 mln rubli (ok. 250 tys. zł), A. Mierzyńska, *Niezależny kanał o wojnie? Raczej projekt rosyjskiego wywiadu. Uważajcie na Rybara!*, 23.12.2022, https://oko.press/rybar-niezalezny-kanal-rosyjski-wywiad.

[46] Rosyjska fundacja Pravfond (pełna nazwa: Fundacja Wspierania i Ochrony Praw Rodaków Mieszkających za Granicą) – rosyjska organizacja państwowa, która służy jako narzędzie rosyjskich służb specjalnych do finansowania propagandy, operacji wpływu oraz wspierania agentów Kremla w Europie, A. Morozova, A. Pawłowska, D. Flis, M. Możański, *Ujawniamy dokumenty funduszu Pravfond*, 21.05.2025, https://frontstory.pl/pravfond-szpiegostwo-rosja/.

*Exposing and analysing Russia's FIMI operation*s, 16.05.2025, https://euvsdisinfo.eu/exposing-and-analysing-russias-fimi-operations/ (dostęp 7.12.2025); *Operation False Façade: Insights from a FIMI Information Laundering Scheme*, 2024, https://euvsdisinfo.eu/uploads/2024/05/EEAS-TechnicalReport-False-Facade.pdf (dostęp 4.12.2025); *Struktura rosyjskich operacji FIMI*, 2.04.2025, https://euvsdisinfo.eu/pl/struktura-rosyjskich-operacji-fimi/ (dostęp 5.12.2025); *The architecture of Russia's FIMI operations*, 2.04.2025, https://euvsdisinfo.eu/the-architecture-of-russias-fimi-operations (dostęp 4.12.2025); *Ujawnianie i analizowanie rosyjskich operacji FIMI*, 16.05.2025, https://euvsdisinfo.eu/pl/ujawnianie-i-analizowanie-rosyjskich-operacji-fimi (dostęp 5.12.2025); *Wkrocz do galaktyki: analiza powiązań operacji wpływu*, 9.04.2025, https://euvsdisinfo.eu/pl/wkrocz-do-galaktyki-analiza-powiazan-operacji-wplywu/ (dostęp 5.12.2025); *Архітектура російських операцій FIMI*, 2.04.2025, https://euvsdisinfo.eu/ua/%D0%B0%D1%80%D1%85% (dostęp 6.12.2025); *Відлуння впливу: за лаштунками російських операцій FIMI в Африці*, 28.04.2025, https://euvsdisinfo.eu/ua/%d0%b2%d1 (dostęp 5.12.2025); *Викриття й аналіз операцій FIMI Росії*, 16.01.2025, https://euvsdisinfo.eu/ua/%d0%b2%d0%b8%d0%ba%d1% (dostęp 6.12.2025); *Реагування Підрозділу стратегічних комунікацій ЄСЗС на FIMI у 2023 році*, 28.06.2024, https://euvsdisinfo.eu/ua/%d1%80%d0%b5%d0% (dostęp 5.12.2025).

ROSYJSKA SIEĆ DEZINFORMACYJNA STORM-1516 (Burza-1516), CopyCop albo False Façade („Fałszywa Fasada") – 3 nazwy nowej, tajnej, zakrojonej na szeroką skalę rosyjskiej kampanii manipulacji informacjami i ingerencji (FIMI), działającej na niespotykanym dotąd poziomie wyrafinowania. Nie jest to po prostu najnowsza rosyjska kampania dezinformacyjna, ale kompleksowa operacja wpływu, której celem jest podważenie zaufania, zawłaszczenie rzeczywistości i ostatecznie zmiana nastrojów społecznych w Europie i Ameryce Północnej.

Trzeba podkreślić, że kilka organizacji i instytucji zajmuje się analizowaniem tej rosyjskiej sieci dezinformacyjnej, w tym VIGINUM[47], zespół badawczy Grupy Insikt[48] (która dała nazwę tej operacji – CopyCop), ba-

[47] VIGINUM – francuska służba techniczna i operacyjna odpowiedzialna za monitorowanie i ochronę przed zagraniczną ingerencją cyfrową, działająca przy Sekretariacie Generalnym ds. Obrony i Bezpieczeństwa Narodowego.

[48] Zespół badawczy Insikt Group działa w ramach Recorded Future, Inc. – amerykańskiej prywatnej firmy zajmującej się cyberbezpieczeństwem, w ramach projektu badawczego

daczy z Clemson University[49], Newsguard[50], Microsoft oraz inne. Każda z tych instytucji analizuje tę operację pod inną nomenklaturą. Nazwa „Fałszywa Fasada" została nadana przez Europejską Służbę Działań Zewnętrznych (ESDZ) i firmę zajmującą się cyberbezpieczeństwem Recorded Future, natomiast niektóre elementy tej operacji zbadało Centrum Analiz Zagrożeń Microsoftu. Istnieją również istotne powiązania między tą siecią a kampanią „Portal Kombat", odkryte przez władze francuskie.

Operacja ta została uruchomiona pod koniec 2023 r. i obejmuje sieć 230 nieprawdziwych stron internetowych, wśród których znajdują się zarówno domeny aktywne, jak i uśpione. Udają one zachodnie media, przyjmując nazwy, w których pojawiają się nazwy miast z UE, Wielkiej Brytanii i USA, np. Boston Times czy London Crier. Pokazuje to, że celem geograficznym operacji FIMI jest wywieranie wpływu na kraje Zachodu. Kampania koncentruje się na „praniu" starannie wybieranych informacji przez źródła o jawnych i niejawnych powiązaniach.

Pierwszy raport o działalności tej sieci pojawił się w grudniu 2023 r. przygotowany przez organizację Media Forensics Hub firmy Clemson, opisując dodatkowe ustalenia dotyczące prorosyjskiej kampanii dezinformacyjnej, po raz pierwszy publicznie zidentyfikowanej, a następnie nazwanej Storm-1516 przez Centrum Analizy Zagrożeń firmy Microsoft. Kampania ta trwa co najmniej od sierpnia 2023 r. i odniosła kilka sukcesów. Storm-1516 jest ściśle powiązany z tzw. Rosyjską Fundacją Walki z Niesprawiedliwością. Centrum Analizy Zagrożeń Microsoftu twierdzi, że działania operacyjne „najprawdopodobniej obejmują weteranów Agencji Badań Internetowych".

Głównym celem Storm-1516 jest zdyskredytowanie Ukrainy, co najprawdopodobniej doprowadzi do wstrzymania zachodniej pomocy dla tego kraju w kontekście inwazji Rosji. Jednocześnie operacja bezpośrednio

---

Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America.

[49] Clemson University – amerykański uniwersytet publiczny w mieście Clemson, w stanie Karolina Południowa, założony w 1889 r.

[50] Newsguard – amerykańska firma zajmująca się dostarczaniem danych, analiz i informacji, które pomagają przedsiębiorstwom i konsumentom identyfikować wiarygodne informacje online.

atakuje europejskich przywódców i ich otoczenie, szczególnie w okresach wyborczych we Francji, Stanach Zjednoczonych, Niemczech i innych krajach. W tym celu zazwyczaj rozpowszechnia się deepfake'i i filmy, czasami wykorzystując aktorów amatorów.

Operacja ma również na celu manipulowanie opinią publiczną i sianie podziałów geopolitycznych w krajach docelowych poprzez rozpowszechnianie prorosyjskich narracji i dezinformacji, często związanych z drażliwymi kwestiami, takimi jak wojna w Ukrainie, konflikt Izraela z Hamasem i wybory w państwach demokratycznych.

Choć rzeczywisty wpływ na cyfrową debatę publiczną pozostaje trudny do oszacowania, VIGINUM zauważa, że wiele narracji propagowanych za pośrednictwem tej operacji osiągnęło wysoki poziom widoczności w internecie, a niektóre z nich zostały nawet nagłośnione przez osoby publiczne i polityków Zachodu. Chodzi nie tyle o przekonanie, co o wprowadzenie w błąd, uniemożliwiając publiczności odróżnienie prawdy od fikcji, aż do momentu, gdy niedowierzanie stanie się dla niej czymś oczywistym. Kiedy słyszysz, jak ktoś mówi: „Już nie wiem, w co wierzyć", zdajesz sobie sprawę, że to działa.

To, co czyni Storm-1516 bardziej niebezpiecznym od poprzedników, to jego skala przemysłowa i ewolucja technologiczna. To dezinformacja w erze masowej precyzji; operacja wspomagana sztuczną inteligencją, zdolna do generowania i rozpowszechniania wielojęzycznych treści za pomocą kont typu *burner* i deepfake'ów, które odzwierciedlają legalne źródła. Wśród nich znalazły się jak dotąd fałszywe strony podszywające się pod „Le Monde", „Bild", „The Guardian" i „Deutsche Welle". To kognitywne operacje specjalne wykraczające poza zwykłą propagandę.

Operatorzy Storm-1516 kontynuują obecnie swoją działalność w stałym tempie operacyjnym i najprawdopodobniej będą nadal dostosowywać swoje taktyki, techniki i procedury (TTP), w szczególności aby nadać swoim treściom większą wiarygodność, próbować obejść mechanizmy moderacji platform, utrudnić monitorowanie i techniczne przypisywanie swoich działań lub odnawiać infrastrukturę ataku.

W świetle tych elementów VIGINUM uważa, że działania Storm-1516 spełniają kryteria zagranicznej ingerencji cyfrowej i stanowią poważne zagrożenie dla francuskiej i europejskiej debaty cyfrowej.

I tak w jednym przypadku zespół Storm-1516 stworzył fałszywą francuską stronę polityczną oferującą wyborcom 100 euro „premii Macrona" w zamian za oddanie głosu. Miało to na celu nie tylko wprowadzenie w błąd, ale także delegitymizację samego procesu wyborczego. W innym przypadku spreparowane filmy *deepfake* przedstawiały groźby Hamasu dotyczące ataku na igrzyska olimpijskie w Paryżu. Jak zwykle nadawcy nie pozostawili adresu zwrotnego. To nie są samotne wilki ani nieuczciwi żartownisie, ale pełnomocnicy władzy państwowej, skoordynowani w celu siania chaosu i osłabiania woli Europy do wspierania Ukrainy oraz zdolności do wspólnego reagowania na rosyjską agresję.

Istotą operacji jest technika zwana „praniem informacji", która obejmuje 3 fazy:

- umieszczanie: treści były początkowo umieszczane na różnych platformach, czasami z wykorzystaniem sztucznej inteligencji generatywnej, aby tworzyć przekonujące, ale fałszywe historie. Przykładem jest fałszywe wideo, w którym twierdzono, że prezydent Ukrainy Wołodymyr Zełenski kupił luksusową willę od króla Karola III;
- warstwowanie: treści te były następnie rozpowszechniane za pośrednictwem sieci pośredniczących w celu ukrycia ich pochodzenia. Sieć co najmniej 23 fałszywych stron internetowych, podszywających się pod legalne media we Francji, Wielkiej Brytanii i Stanach Zjednoczonych, automatycznie tłumaczyła i przedrukowywała treści, usuwając odniesienia do oryginalnych rosyjskich źródeł;
- integracja: sfabrykowane „artykuły informacyjne" były następnie przechwytywane i rozpowszechniane przez oficjalne rosyjskie media kontrolowane przez państwo oraz agencje dyplomatyczne, dzięki czemu dezinformacja wyglądała jak autentyczne wiadomości z Zachodu.

Kampania była skierowana głównie do odbiorców we Francji, Wielkiej Brytanii i Stanach Zjednoczonych. Operacja została zidentyfikowana jako część szerszego ekosystemu rosyjskich kampanii FIMI, w tym dobrze udokumentowanych operacji „Doppelgänger" („Sobowtór") i „Portal Kombat".

Kluczowym etapem w procesie działania Storm-1516 jest wykorzystanie zestawu fałszywych stron z wiadomościami online. Większość treści to tysiące artykułów generowanych przez sztuczną inteligencję, skradzionych i przepisanych z autentycznych źródeł. Te artykuły są krótkie i ustandaryzowane; ponieważ są tworzone w sposób zautomatyzowany, charakteryzują się pewnymi spójnościami. Wśród tej masy prawdziwych wiadomości kryje się niewielka liczba dłuższych, bardziej złożonych artykułów.

Na początku marca 2024 r. Insikt Group zidentyfikowała złowrogą sieć wpływu, która umiejętnie wykorzystuje nieautentyczne amerykańskie, brytyjskie i francuskie media do publikowania treści politycznych na dużą skalę; również modele językowe związane ze Stanami Zjednoczonymi, Wielką Brytanią, Ukrainą, Izraelem i Francją. Sieć ta jest prowadzona z Rosji i prawdopodobnie ma powiązania z rządem rosyjskim. Storm-1516 szeroko wykorzystuje generatywną sztuczną inteligencję do plagiatu i modyfikowania treści z legalnych mediów, aby dopasowywać polityczne przekazy do określonych uprzedzeń. Obejmuje to treści krytyczne wobec polityki Zachodu oraz wspierające rosyjskie perspektywy w kwestiach międzynarodowych, takich jak wojna rosyjsko-ukraińska czy napięcia między Izraelem a Hamasem.

A już w maju i czerwcu 2024 r. Grupa Insikt udokumentowała działalność tej operacji, a także próby wpłynięcia na przedterminowe wybory we Francji w 2024 r ., wybory prezydenckie w USA w 2024 r. oraz wybory federalne w Niemczech w 2025 r. Raporty innych organizacji, takich jak Clemson University, VIGINUM, NewsGuard, Microsoft, Europejska Służba Działań Zewnętrznych i projekt Gnida, w dużej mierze potwierdziły wstępne oceny celów, zadań i infrastruktury sieci. Co więcej, udowodniono, że za część działań sieci odpowiada John Mark Dougan[51], obywatel

[51] Obywatel USA John Dougan pracuje dla Rosji, promując narrację Moskwy za granicą. Wcześniej służył w armii USA i był zatrudniony w amerykańskim sektorze ścigania. W tym czasie było prowadzonych przeciw niemu 11 dochodzeń wewnętrznych. Dougan ubiegał się o azyl w Rosji w 2016 r., po tym, jak oskarżono go o prowadzenie kampanii doxxingu, której celem było pozyskanie danych osobowych wielu urzędników państwowych. Został oskarżony o wymuszenia i podsłuchy, po czym uciekł do Rosji, którą odwiedzał już kilkakrotnie. Obecnie jest obywatelem rosyjskim. Podobnie jak innym amerykańskim dysydentom, Moskwa udzieliła mu azylu. Następnie rozpoczął pracę jako dziennikarz,

USA mieszkający w Moskwie przy wsparciu moskiewskiego Centrum Ekspertyzy Geopolitycznej oraz Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej. CopyCop wykorzystuje te strony jako infrastrukturę do rozpowszechniania dezinformacji, tworzenie deepfake'ów i fałszywych treści wymierzonych w przywódców politycznych w USA, Ukrainie, Francji i innych krajach oraz do publikowania treści generowanych przez sztuczną inteligencję o tematyce prorosyjskiej i antyukraińskiej, wspierając w ten sposób ofensywne działania Rosji w globalnym środowisku informacyjnym.

W 2024 r. operacja skupiła się głównie na wyborach we Francji, później na wyborach prezydenckich w Stanach Zjednoczonych, rozpowszechniając treści ukierunkowane na YouTubie za pośrednictwem filmów skierowanych do przywódców politycznych Francji, Ukrainy i Unii Europejskiej. Następnie rozszerzyła swoje wpływy na główne media w USA i Wielkiej Brytanii. W ciągu 24 godzin od opublikowania oryginalnych artykułów na rosyjskich stronach internetowych zbierała, modyfikowała i rozpowszechniała je w amerykańskich witrynach o tematyce wyborczej, używając ponad tysiąca fałszywych tożsamości dziennikarzy. Sieć dostosowała się do ostatnich analiz, przenosząc infrastrukturę na amerykańskie serwery, by zminimalizować powiązania z rosyjskim rządem.

---

a obecnie, z pomocą rosyjskiego wywiadu wojskowego (GRU) zarządza różnymi stronami internetowymi przypominającymi amerykańskie gazety oraz kanałami na YouTubie. Publikowane przez niego treści zawierają rosyjską propagandę mającą na celu szerzenie rosyjskich wpływów i destabilizację wrogich celów, w tym ojczyzny Dougana, Stanów Zjednoczonych. Chociaż temu zaprzecza, jest powiązany z ponad 150 stronami internetowymi, które szerzą rosyjską propagandę na całym świecie. Wśród nich znajdują się „DC Weekly", „New York News Daily", „Boston Times", „Chicago Chronicle" i inne. Dougan wykorzystuje YouTube'a i inne media społecznościowe do publikowania swojej pracy. Występuje również w różnych rosyjskich programach jako dziennikarz-ekspert. Moskwa jest znana z werbowania zachodnich ekspertów do tworzenia propagandy w języku angielskim. Dougan jest jedną z tych osób. Jego łącznikiem w rosyjskim wywiadzie wojskowym GRU jest Jurij Choroszewski, który należy do jednostki 29155 specjalizującej się w operacjach sabotażu i ingerencji międzynarodowej. Dougan otrzymuje również fundusze od Instytutu Moskiewskiego, kolejnej organizacji promującej narrację Putina, https://greydynamics.com/john-dougan-russian-intelligences-american-propagandist/.

Od końca 2023 r. VIGINUM również obserwuje i dokumentuje działania rosyjskiego sposobu manipulacji informacją znanego jako Storm-1516 jako zbiór zachowań, narzędzi, taktyk, technik, procedur i zasobów przeciwnika wykorzystywanych w ramach 1 lub więcej operacji informacyjnych. Jest on odpowiedzialny za kilkadziesiąt operacji informacyjnych wymierzonych w odbiorców zachodnich, w tym francuskich.

Natomiast zespół badawczy Grupy Insikt od marca 2025 r. obserwuje operację Storm-1516, analizując co najmniej 200 nowych fikcyjnych witryn medialnych, których celem są Stany Zjednoczone, Francja i Kanada, a także witryny podszywające się pod marki medialne oraz partie i ruchy polityczne we Francji, Kanadzie i Armenii. Operacja utworzyła również regionalną sieć witryn podszywających się pod fikcyjną organizację weryfikującą fakty, publikując treści w językach tureckim, ukraińskim i suahili, których sieć nigdy wcześniej nie oferowała. Wliczając 94 witryny skierowane do Niemiec, zgłoszone przez Grupę Insikt w lutym 2025 r., łączna liczba witryn utworzonych przez operatorów CopyCop w 2025 r. przekroczyła 300. Stanowi to znaczący wzrost od czasu pierwszego zgłoszenia sieci w 2024 r., a wiele z nich nie zostało jeszcze publicznie udokumentowanych. Prawie wszystkie strony to fikcyjne lokalne media w USA, Francji, Kanadzie i Norwegii; partie i ruchy polityczne we Francji, Kanadzie i Armenii lub fikcyjne organizacje zajmujące się weryfikacją faktów, publikujące w języku tureckim, ukraińskim i suahili.

Następny raport o działalności Storm-1516, przygotowany przez VIGINUM, pojawił się w maju 2025 r. i opierał się na analizie 77 operacji informacyjnych udokumentowanych i przeprowadzonych przez Storm-1516 między jego domniemaną datą pojawienia się a 5 marca 2025 r., kiedy to była wykorzystywana głównie do atakowania interesów Ukrainy. I tak spośród 77 operacji informacyjnych przeanalizowanych przez VIGINUM 35 miało na celu zaszkodzenie wizerunkowi Ukrainy, jej przywódcom lub otoczeniu poprzez powielanie narracji używanych przez rosyjski rząd od czasu rewolucji godności z 2014 r. lub dostosowywanie ich do bieżących wydarzeń. VIGINUM uważa, że operacje te mają na celu przede wszystkim zdyskredytowanie Ukrainy w oczach odbiorców zachodnich, aby podważyć europejskie poparcie społeczne dla pomocy udzielanej w kontekście pełnoskalowej inwazji Rosji na Ukrainę. Narracje rozpowszechniane przez

Storm-1516 twierdzą np., że ukraiński rząd wspiera terroryzm, rekrutując członków Państwa Islamskiego do walki w Ukrainie lub organizując wspólne szkolenia członków Hamasu i batalionu Azow. Często atakują one Zełenskiego, oskarżanego na przemian o bycie neonazistą, narkomanem, homoseksualistą lub o prywatną krytykę przywódców głównych państw udzielających pomocy Ukrainie. Otoczenie prezydenta Ukrainy również jest celem tych operacji, w szczególności oskarża się jego żonę Olenę Zełenską o rzekome defraudacje i handel ludźmi na szkodę ludności ukraińskiej. Najczęściej powtarzana narracja oskarżała Zełenskiego i jego bliskich o wydawanie zachodnich pieniędzy na luksusowe nieruchomości za granicą, rzekomo przygotowując się do ucieczki z Ukrainy, która była przedstawiana jako bliska przegranej wojny.

VIGINUM szczegółowo opisuje główne narracje i wykorzystywane treści, ich łańcuch dystrybucji oraz zagranicznych aktorów zaangażowanych w prowadzenie manipulacji informacją.

Analiza VIGINUM dotycząca różnych operacji informacyjnych pokazuje, że rosyjski aparat wpływu włożył znaczne wysiłki w koordynację działań dużej sieci aktorów, organizacji i manipulacji informacją działających z terytorium Rosji oraz w innych krajach, od początku pełnoskalowej inwazji Rosji na Ukrainę w 2022 r.

Chociaż zasięg sieci pod względem języków docelowych i krajów się rozszerzył, jej główne cele niemal na pewno pozostają niezmienne: osłabienie poparcia dla Ukrainy i pogłębienie rozdrobnienia politycznego w krajach zachodnich, które ją popierają. Grupa Insikt zauważyła również, że CopyCop realizuje dodatkowe, drugorzędne cele, takie jak promowanie geopolitycznych celów Rosji w jej rozszerzonej strefie wpływów, obejmującej Armenię i Mołdawię. Narracje i treści CopyCop wspierające te cele są regularnie wzmacniane przez ekosystem influencerów w mediach społecznościowych, a także przez inne rosyjskie sieci wpływów, takie jak „Portal Kombat" i „InfoDefense".

Podobnie jak cele, taktyka, techniki i procedury CopyCop pozostają w dużej mierze niezmienne, z niewielkimi usprawnieniami mającymi na celu zwiększenie zasięgu, odporności i wiarygodności sieci. Taktyki i techniki wykorzystywane do rozpowszechniania treści zazwyczaj obejmują deepfake'i, obszerne teczki mające na celu ośmieszenie ofiar

oraz sfabrykowane wywiady z rzekomymi sygnalistami wysuwającymi oskarżenia na temat przywódców politycznych państw członkowskich NATO, takich jak Stany Zjednoczone, Francja i Niemcy. Grupa Insikt zidentyfikowała również nowe dowody na to, że CopyCop wykorzystuje samodzielnie hostowane, nieocenzurowane modele LLM (Large Language Models), oparte na *open source* Llama 3 firmy Meta, do generowania treści AI, zamiast polegać na zachodnich dostawcach usług.

Do 2025 r. CopyCop rozszerzył swoje języki docelowe o turecki, ukraiński i suahili, a także zasięg geograficzny – o Mołdawię, Kanadę i Armenię, jednocześnie utrzymując wpływy skoncentrowane na Stanach Zjednoczonych i Francji. Sieć wykorzystuje również nową infrastrukturę do publikacji treści, znacząco zwiększając swoje wysiłki w celu dotarcia do nowych odbiorców.

Fałszywe treści promowane przez strony internetowe CopyCop wcześniej często zawierały deepfake'i i fałszywe wywiady, np. nieprawdziwe oskarżenia wysuwane przez fałszywych informatorów pod adresem niektórych przywódców politycznych. Podczas gdy sieć nadal produkuje i rozpowszechnia te treści, nowe, skoncentrowane na Francji strony CopyCop zaczęły publikować filmy pod marką fałszywej strony internetowej, na której są promowane. Przykładowo Courrierfrance24(.)fr promował film, który zawierał grafikę z transmisji telewizyjnej z logo „Courrier France 24" i został zmontowany tak, aby przypominał autentyczne transmisje telewizyjne.

Sieć próbuje coraz częściej podszywać się pod legalne media, wykorzystując wizerunki medialne i wyższą jakość produkcji – taktykę stosowaną również w innych rosyjskich operacjach wpływu, takich jak „Overload" i „Doppelgänger". Grupa Insikt udokumentowała już wcześniej wykorzystywanie przez sieć profili dziennikarzy generowanych przez sztuczną inteligencję, a nowe strony internetowe CopyCop również wykorzystują skradzione tożsamości dziennikarzy.

Oprócz obsługi fikcyjnych marek medialnych CopyCop nadal okazjonalnie podszywa się pod legalne firmy, np. BBC, a także amerykańskie i francuskie partie polityczne. 22 lipca 2025 r. zarejestrował domenę Tvfrance2(.)fr (używając adresu jeanmoreau90(@)proton(.)me) i zaczął hostować stronę internetową podszywającą się pod francuskiego nadawcę

publicznego France Télévisions. 24 lipca 2025 r. na stronie opublikowano artykuł, w którym stwierdzono, że francuski rząd sprzedał większościowy udział w EDF, francuskim dostawcy energii, wicepremierowi Ukrainy Ołeksijowi Czernyszowowi.

Sieć coraz częściej prowadzi również operacje mające na celu zwiększenie wpływu, celując w Mołdawię i Armenię przed wyborami parlamentarnymi w tych krajach w 2025 i 2026 r. To ogólny trend obserwowany w całym rosyjskim ekosystemie wpływów.

W 2025 r. sieć znacznie rozszerzyła swoją działalność: założyła liczne fikcyjne strony internetowe, których celem są takie kraje jak Stany Zjednoczone, Francja, Kanada, Armenia, Mołdawia i Ukraina, mające rozpowszechniać prorosyjskie narracje i osłabiać poparcie dla Ukrainy, a jednocześnie destabilizować sytuację polityczną w krajach zachodnich i regionach sąsiednich.

W 2025 r. rosyjska sieć dezinformacyjna Storm-1516 pozostaje jednym z najbardziej aktywnych podmiotów prowadzących operacje psychologiczne (PSYOP) i kampanie dezinformacyjne wymierzone w Ukrainę oraz państwa Zachodu. Najważniejsze aspekty ich obecnej działalności oraz przewidywane kierunki ewolucji ich taktyk, technik i procedur (TTP):

1. Stałe tempo operacyjne (High Operational Tempo). Storm-1516 operuje w modelu „fabryki treści". Działania charakteryzują się:
   - szybką reakcją na wydarzenia: grupa potrafi w ciągu kilkunastu godzin od wystąpienia istotnego wydarzenia politycznego (np. szczytu NATO czy wyborów) stworzyć i wypromować sfabrykowane dowody wideo lub dokumenty;
   - masowością: wykorzystują sieć botów i farm trolli do zalewania platform takich jak X (dawniej Twitter), Telegram i TikTok krótkimi, sensacyjnymi materiałami.
2. Ewolucja TTP w 2025 r. Analitycy ds. bezpieczeństwa wskazują, że grupa będzie nadal dostosowywać swoje metody, aby omijać coraz skuteczniejsze systemy moderacji i detekcji AI:
   - zaawansowane deepfake'i: przejście od prostych manipulacji do wysokiej jakości generatywnego wideo i audio, co utrudnia szybką weryfikację przez fact-checkerów;

- „pranie" informacji (Information Laundering): Storm-1516 coraz częściej wykorzystuje rzekomych „dziennikarzy śledczych" lub „sygnalistów" z krajów zachodnich (często postacie fikcyjne lub opłacone), aby uwiarygodnić swoje narracje przed wprowadzeniem ich do głównego nurtu mediów;
- wykorzystanie lokalnych narracji: zamiast tworzyć ogólne komunikaty, grupa dostosowuje treści do specyficznych lęków społecznych w poszczególnych krajach (np. kwestie inflacji w Polsce, spory o pomoc wojskową w USA czy napięcia społeczne we Francji).

3. Główne cele ataków. W 2025 r. ich aktywność koncentruje się na:
   - podważaniu zaufania do instytucji demokratycznych poprzez fabrykowanie dowodów na korupcję polityków wspierających Ukrainę;
   - dyskredytowaniu Sił Zbrojnych Ukrainy: tworzenie fałszywych nagrań mających świadczyć o rzekomych zbrodniach lub nielegalnym handlu bronią z Zachodu;
   - wpływaniu na procesy wyborcze: choć główne wybory w USA już się odbyły, grupa pozostaje aktywna przy wyborach parlamentarnych i lokalnych w Europie w 2025 r.

Storm-1516 to przeciwnik wysoce adaptacyjny: jego siła nie tkwi w jakości pojedynczego kłamstwa, ale w skali i uporczywości, z jaką wprowadza chaos informacyjny do przestrzeni publicznej.

W porównaniu z innymi rosyjskimi sieciami wpływów jego oddziaływanie pozostaje znaczące: ukierunkowane treści publikowane przez influencerów za pośrednictwem stron internetowych firmy oraz ekosystem prorosyjskich influencerów w mediach społecznościowych i tzw. „dziennikarzy" regularnie osiągają wysokie wskaźniki organicznego zaangażowania na wielu platformach społecznościowych i ustanowiły precedens w zakresie przebicia się do głównego nurtu politycznego. Konsekwentna identyfikacja i publiczne nagłośnienie tych sieci powinno pozostać priorytetem dla rządów, dziennikarzy i badaczy, którzy dążą do ochrony instytucji demokratycznych przed rosyjskimi wpływami.

Storm-1516 jest obecnie dojrzałym sposobem działania informacyjnego, który daje sponsorom możliwość realizacji zarówno krótkoterminowych

działań w reakcji na bieżące wydarzenia, jak i bycia częścią długoterminowych strategii mających na celu zdyskredytowanie europejskich i północnoamerykańskich osób publicznych lub organizacji, szczególnie przed ważnymi wydarzeniami i procesami wyborczymi.

Storm-1516 to przedsmak tego, co będzie dalej. Dezinformacja jest teraz skalowalna, mikrotargetowana i wystarczająco przekonująca, by wpłynąć na wynik wyborów, rozbić sojusze i sparaliżować reakcje.

Olga Wasiuta

Analysis of the Russian information manipulation set Storm-1516, 2025, https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf (dostęp 12.10.2025); *Building a false façade*, 2.05.2024, https://euvsdisinfo.eu/building-a-false-facade/ (dostęp 10.10.2025); *CopyCop Deepens Its Playbook with New Websites and Targets*, 17.09.2025, https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-ru-2025-0917.pdf (dostęp 11.10.2025); Ch. Kremidas-Courtney, *Storm-1516: A wake-up call for Europe's cognitive defence*, 13.05.2025, https://www.epc.eu/publication/Storm-1516-A-wake-up-call-for-Europes-cognitive-defence-650d24/ (dostęp 10.10.2025); D. Linvill, P. Warren, *Infektion's Evolution: Digital Technologies and Narrative Laundering*, 2023, https://tigerprints.clemson.edu/mfh_reports/3 (dostęp 11.10.2025); *Operation False Façade: Insights from a FIMI Information Laundering Scheme*, 2024, https://euvsdisinfo.eu/uploads/2024/05/EEAS-TechnicalReport-False-Facade.pdf (dostęp 10.10.2025); *Russia-Linked CopyCop Expands to Cover US Elections*, 24.06.2024, https://assets.recordedfuture.com/insikt-report-pdfs/2024/cta-ru-2024-0624.pdf (dostęp 12.10.2025); *Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale*, 9.05.2024, https://assets.recordedfuture.com/insikt-report-pdfs/2024/cta-2024-0509.pdf (dostęp 12.10.2025); *Russian Influence Assets Converge on Moldovan Elections*, 3.09.2025. https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-ru-2025-0903.pdf (dostęp 11.10.2025).

ROSYJSKIE FORTYFIKACJE W WOJNIE W UKRAINIE – fortyfikacje obronne, jakie zostały zbudowane przez Siły Zbrojne Federacji Rosyjskiej, prywatne firmy wojskowe współpracujące z Kremlem, milicje Donieckiej i Ługańskiej Republiki Ludowej oraz administracje obwodów graniczące z Ukrainą od II połowy 2022 r. W literaturze niniejsza tematyka określana jest mianem „wojny okopowej" (*tranche warfare*), w której okop oznacza fortyfikację służącą głównie do obrony; zapewnia pozycję obronną pod

ziemią, dzięki czemu żołnierze są lepiej chronieni przed ogniem broni maszynowej i artylerią przeciwnika. Ponadto siły atakujące prowadzące ofensywę w miejscu, gdzie znajdują się okopy, muszą się przez nie przebić, co naraża je na większe straty i spowolnienie natarcia. W polskiej nomenklaturze wojskowej używane jest pojęcie „wojny pozycyjnej". Podręcznik walki pododdziałów wojsk zmechanizowanych opublikowany przez Dowództwo Wojsk Lądowych w 2000 r. definiuje ją jako wojnę, która polega na utrzymaniu terenu, dążeniu do rozbicia nacierających zgrupowań przeciwnika przed przednią linią obrony lub rejonie pierwszego rzutu. Regulamin działań wojsk lądowych z 2008 r. dodaje, że istotą wojny pozycyjnej jest opór i utrzymanie pasa obrony (rejonu). Aby to osiągnąć, musi być ona odpowiednio silna, dobrze rozbudowania pod względem inżynieryjnym, wsparta ogniowo, ubezpieczona i osłonięta przed uderzeniami z powietrzna. W obronie pozycyjnej większość sił znajduje się w głównym obszarze obrony i w połączeniu z odwodami dąży do załamania natarcia. W przeciwieństwie do obrony manewrowej, obrona pozycyjna nie daje pełnej możliwości zniszczenie przeciwnika. Nie musi być także głęboka, ale prowadzona na różnej głębokości, zależnej od zadania, możliwości wojsk i charakteru terenu.

Jak zauważył Eldar Jakubovic, pierwsza wzmianka o „wojnie okopowej" pochodzi z okresu bitwy pod Medyną w 627 r. – wówczas muzułmanie pod dowództwem Mahometa, broniący osady przed beduińskim plemieniem Kurajszytów, zbudowali fosę, której atakujący nie mogli sforsować i po 2 tygodniach oblężenia zdecydowali się wycofać. Wojna okopowa towarzyszyła następnie każdej epoce historycznej, zarówno w starożytności, kiedy używali jej w walce Rzymianie, średniowieczu, gdy stosowano ją zarówno do obrony, jak również oblegania zamków, okresie nowożytnym, m.in. w czasie wojny krymskiej, wojnie secesyjnej oraz I i II wojnie światowej. W pierwszym etapie wojny rosyjsko-ukraińskiej nic nie wskazywało na to, że któraś ze stron przygotowywała się do wojny okopowej. Pierwsze informacje na temat budowania okopów i różnego rodzaju budowli inżynieryjnych pojawiły się w II połowie 2022 r. Motywacją do ich utworzenia były udane ukraińskie ofensywy w obwodzie charkowskim i chersońskim, w wyniku których Rosja utraciła zdobyte wcześniej tereny.

Do 2025 r. powstało kilku linii obronnych:

- linia Wagnera/linia Prigożyna w obwodach donieckim i ługańskim;
- linia Surowikina w obwodzie chersońskim i zaporoskim;
- linie obronne w rosyjskich obwodach biełgorodzkim i kurskim.

Jako pierwsza we wrześniu 2022 r. w pobliżu miasta Gorskoje, w obwodzie ługańskim zaczęła powstać linia Wagnera; miała się rozciągać na wschód od ówczesnej granicy Ukrainy z separatystycznymi republikami, od miejscowości Kreminna do Switłodarśka o łącznej długości 217 km. W następnej kolejności w listopadzie 2022 r. na lewym brzegu Dniepru zaczęto budować linię Surowikina; składała się ona z rowów przeciwpancernych, okopów oraz pól minowych i ciągnęła na długości ponad 100 km. W kolejnych miesiącach wybudowano linie obrony przy granicy z Ukrainą w obwodzie biełgorodzkim; pracami kierowali członkowie Grupy Wagnera na zlecenie lokalnych władz. Linia składała się co najmniej z 3 rzędów „smoczych zębów".

Biorąc pod uwagę bardzo długą granicę lądową między Rosją, a Ukrainą, wybudowanie linii obronnych oddzielających walczące strony wydawało się mało prawdopodobne. Umocnienia w obwodzie biełgorodzkim traktowane w związku z tym były głównie jako zabiegi mające na celu budowę poczucia bezpieczeństwa wśród mieszkańców. O wiele bardziej zasadne, z rosyjskiego punktu widzenia, wydawało się budowanie linii obronnych na terenach odebranych Ukrainie. Władze w Kijowie wielokrotnie podkreślały bowiem, że celem politycznym wojny jest odebranie utraconych ziem. Intensywność prac była różna i wynikała z prowadzenia przez Siły Zbrojne Ukrainy działań ofensywnych lub prawdopodobieństwa ich wystąpienia. W marcu i kwietniu 2023 r. koncentrowano się na budowie lub umacnianiu fortyfikacji na Krymie, w okolicach przesmyku Perekop oraz obwodzie ługańskim i donieckim, w okolicach Lisyczańska. W czasie wakacji prace prowadzone były celem łączenia istniejących linii oraz budowania kolejnych za tymi, które już zostały ukończone. Sytuacja taka miała miejsce szczególnie w obwodzie zaporoskim, w pobliżu Andrijiwki oraz innych miejscach, przez które przebiegały drogi w kierunku Mariupola. Prace polegały nie tylko na budowaniu linii obronnych i pól minowych, ale także umocnień i schronów na lotniskach takich jak port lotniczy w Berdiańsku. W sierpniu 2024 r., kiedy wojska ukraińskie przekroczyły

granicę z Rosją w obwodzie kurskim, nowe fortyfikacje zaczęły powstawać na północ od Sudży, w okolicach miejscowości Rylsk i innych miastach wzdłuż trasy E38. Prace trwały co najmniej do wiosny 2025 r., a następnie wraz ze zmniejszeniem zdolności ofensywnych ukraińskiego wojska koncentrowały się na budowaniu schronów na lotniskach.

Wraz z rosnącą liczbą umocnień pojawiały się pytania odnoszące się do kosztów, jakie ponosi rosyjskie wojsko. W zależności od przedsiębiorstwa, które zajmowało się sprzedażą „smoczych zębów", ich cena wahała się między 5 tys. a 16 tys. rubli za sztukę. Radzieckie regulaminy wojskowe zalecały, aby linie obronne składały się z 4 rzędów „smoczych zębów", a odległość między nimi była nieco mniejsza od długość czołgu przeciwnika (3,4 m w przypadku czołgów T-64 i T-72). Przy średniej cenie produktu 10 tys. rubli koszt kilometra linii obronnych wynosił 10 mln rubli. Jeśli konstrukcje wybudowane zostały według radzieckich instrukcji, tylko te na linii Wagnera (217 km) kosztowały 2,2 mld rubli, nie licząc transportu, instalacji, okopów i pól minowych. Według „Moscow Times" nie są to jednak wydatki duże, biorąc pod uwagę, że Rosja wydaje około miliarda rubli na godzinę prowadzenia wojny.

Podejście do „wojny okopowej" zaczęło zmieniać się w połowie 2023 r. pod wpływem powszechnego użycia bezzałogowych statków powietrznych, szczególnie dronów z widokiem pierwszej osoby FPV. Olbrzymia ilość używanych maszyn, zarówno rozpoznawczych, jak również bojowych, skutecznie ustanawiała „strefy śmierci" o głębokości od 5 do 10 km wzdłuż linii frontu. Konwencjonalne fortyfikacje w postaci szerokich okopów oraz dużych miejsc schronienia dla plutonów bądź kompanii okazywały się łatwym celem i tym samym stawały się bezużyteczne. W czasie bitwy o Awdijiwkę (jesień 2023 – luty 2024) dokładnie zlokalizowane przez stronę rosyjską ukraińskie silnie ufortyfikowane pozycje (schrony, stanowiska dowodzenia, okopy i szlaki logistyczne) zostały zniszczone przy pomocy dronów FPV, ataków lotniczych oraz ostrzału artyleryjskiego.

Podobna sytuacja miała miejsce w czasie rosyjskich działań zaczepnych w obwodzie charkowskim w maju 2024 r. Rozległe i kosztowne umocnienia graniczne budowane w starym stylu okazały się nie do utrzymania. Brygady ukraińskie zmuszone zostały do ich porzucenia na rzecz mobilnej taktyki obronnej. W 2025 r. walka dronowa jeszcze bardziej się

nasiliła, powiększając „strefę rażenia" do 35–40 km od linii frontu. Miejsca schronienia dla piechoty musiały zostać jeszcze bardziej rozproszone i zmniejszone do grup liczących 3–8 osób. Większego znaczenia nabrała kwestia kamuflażu i ukrycia. Miejsca stacjonowania pododdziałów piechoty są starannie dobierane, biorąc pod uwagę naturalne osłony w postaci linii drzew, lasów, zagajników itp.

W czasie budowy linii fortyfikacji bierze się pod uwagę konieczność złagodzenia skutków wybuchu ładunku przenoszonego przez drony FPV oraz staranne zabezpieczenie wszystkich elementów schronów. Są one również inżynieryjnie przygotowane na użycie broni masowego rażenia poprzez odpowiednią filtrację powietrza, ukryte punkty wejścia i wyjścia oraz dużą głębokość, jeśli pozwalają na to warunki hydrologiczne. Mniejsza gęstość wojsk po stronie ukraińskiej w związku z koniecznością ich rozproszenia wymusiła także budowę stanowisk strzeleckich w wybranych miejscach, tak aby dawały one szanse na utrzymanie długiej linii frontu. Bardzo często używaną przeszkodą jest drut kolczasty, „zęby smoka" z kolei wykorzystywane są na głównej linii obrony i uznawane za przeszkodę bardzo drogą i łatwo wykrywalną z powietrza. W okolicach głównej linii obrony znajdują się linie „alternatywne", często niezidentyfikowane przez przeciwnika, co doprowadza do jego zaskoczenia oraz zmniejsza ryzyko, że pojedyncze przerwanie fortyfikacji doprowadzi do zwinięcia całego punktu oporu. Zaleca się również, żeby większość stanowisk obronnych stanowiły wabiki, a rotacje dokonywane były rzadziej ze względu na ataki dronów. Niezbędne jest zatem wyposażanie schronów w zaplecze kwatermistrzowskie z zapasami wody i żywności umożliwiające przebywanie w nim załogi przez dłuższy czas.

Ukraina zdecydowała się na rozbudowę linii obronnych stosunkowo późno, ponieważ w listopadzie 2023 r. Wówczas w wyniku zarządzeń ogłoszonych przez prezydenta Zełenskiego utworzony został specjalny sztab, który miał odpowiadać za planowanie robót oraz przygotowanie niezbędnych materiałów i ciężkiego sprzętu. Na jego czele stanęli wicepremier Mychajło Fedorow i minister obrony narodowej Rustem Umierow. Finalnie miały powstać 2 linie obrony: pierwsza w pasie poszczególnych grup operacyjnych i druga znajdująca się na zapleczu frontu, oddalona o kilkadziesiąt kilometrów. Budową pierwszej miały zajmować się

wojskowe oddziały saperów, a drugiej – administracje obwodowe i przedsiębiorstwa budowlane wspierane przez siły zbrojne. Informacje na temat przetargów i miejsc, gdzie mają powstać fortyfikacje, utajniono, jednak w rosyjskich mediach społecznościowych pojawiły się zdjęcia z dronów przedstawiające ich postać. Kluczowy nacisk położono na przygotowanie pozycji obronnych na głównym kierunku rosyjskiego natarcia w 2024 r., czyli na linii Wuhłedar–Kurachowe–Pokrowsk–Konstantynówka–Kramatorsk–Słowiańsk.

Bardzo trudno jest określić łączną długość linii fortyfikacyjnych po stronie rosyjskiej i ukraińskiej. Wiadomo, że Rosjanie obawiając się ukraińskich natarć w domenie lądowej, zbudowali ich znacznie więcej. Ukraińcy zmuszeni zostali do konstruowania w momencie, kiedy przeciwnik przejął inicjatywę. Portal *deep state* szacował, że na koniec 2023 r. Rosjanie dysponowali ponad 6 tys. km różnego rodzaju umocnień; najsilniej ufortyfikowane znajdowały się w obwodzie zaporoskim (1869 km) oraz donieckim (1865 km). W obwodzie ługańskim zidentyfikowano ponad 1140 km umocnień, w chersońskim – 886 km, wzdłuż Dniepru do Nowej Kachowki, na Krymie – około 265 km. Nie wszystkie jednak są w taki sam sposób użytkowane; niektóre zostały zalane wodą i nie nadają się do obsadzenia przez piechotę. Sytuacja taka miała miejsce m.in. wzdłuż lewego brzegu Dniepru, gdzie wysadzona została tama elektrowni wodnej w Nowej Kachowce. Nie zmienia to faktu, że właśnie fortyfikacje okazały się jedną z głównych przyczyn sukcesu Rosjan w czasie nieudanej ukraińskiej ofensywy w obwodzie zaporoskim. Ich brak po stronie ukraińskiej z kolei przyczynił się do postępów Rosjan pod Bachmutem i Awdijiwką.

Tomasz Wójtowicz

B. Africk, *Russian field fortifications in Ukraine*, https://read.bradyafrick.com/p/russian-field-fortifications-in-ukraine (dostęp 7.12.2025); J. Ber, *Ukraina: spóźniona rozbudowa systemu fortyfikacji*, https://www.osw.waw.pl/pl/publikacje/analizy/2024-03-15/ukraina-spozniona-rozbudowa-systemu-fortyfikacji (dostęp 7.12.2025); *Deep State Maps*, https://deepstatemap.live/en#6/49.4383200/32.0526800 (dostęp 8.12.2025); E. Jakubovic, *Revolutionizing Trench Warfare*, https://www.researchgate.net/publication/393516335_Revolutionizing_Trench_Warfare (dostęp 6.12.2025); *Podręcznik walki pododdziałów wojsk zmechanizowanych (pluton,*

drużyna), Dowództwo Wojsk Lądowych, Wyższa Szkoła Oficerska im. T. Kościuszki, Warszawa 2000; *Regulamin działań wojsk lądowych*, Dowództwo Wojsk Lądowych, Pion Szkolenia, Warszawa 2008; *Russia's War in Ukraine: Fortification for Drone Warfare*, https://icds.ee/en/russias-war-in-ukraine-fortification-for-drone-warfare/ (dostęp 8.12.2025); O. Vasyliuk, *Military fortifications in Ukraine – what comes next?*, https://uwecworkgroup.info/military-fortifications-in-ukraine-what-comes-next/ (dostęp 8.12.2025); *Путин потребовал не жалея сил искать иностранных шпионов*, https://www.moscowtimes.ru/2022/12/20/update-1-mosbirzha-summarnyy-oborot-na-vsekh-rynkakh-v-22g-prevysil-1-kvadrillion-rubley-blagodarya-repo-a29121 (dostęp 7.12.2025).

ROSYJSKI KORPUS OCHOTNICZY (ros. Русский Добровольческий Корпус, RDK) – jednostka wojskowo-polityczna Sił Zbrojnych Ukrainy zrzeszająca rosyjskich ochotników – etnicznych Rosjan (99%), obywateli Federacji Rosyjskiej mieszkających w Ukrainie i w innych krajach europejskich. Część z nich brała udział w rewolucji godności, walczyła w operacji antyterrorystycznej we wschodniej Ukrainie (ukr. Антитерористична Операція на Сході України, АТО) i w operacji połączonych sił (ukr. Операція Об'єднаних Сил, ООС), a także protestowała w swojej ojczyźnie przeciwko reżimowi Putina. Bojownicy RDK w pełni uznają integralność terytorialną Ukrainy w jej oficjalnych granicach, a od 24 lutego 2022 r. postanowili zjednoczyć się w jednostkę i bronić jej suwerenności i niepodległości środkami wojskowymi. RDK została utworzona w sierpniu 2022 r.

Po rozpoczęciu pełnoskalowej inwazji wojsk rosyjskich na Ukrainę bojownicy ochotniczej jednostki Rosyjskiego Korpusu Ochotniczego (RDK) chwycili za broń. Utworzony w sierpniu 2022 r. i kierowany przez znanego skrajnie prawicowego ideologa Denisa Nikitina (Kapustina) Rosyjski Korpus Ochotniczy wiosną 2023 r. trafił na pierwsze strony międzynarodowych gazet, kiedy zgłosił transgraniczny nalot na 2 wioski w rosyjskim obwodzie briańskim, w którym według oficjalnych rosyjskich raportów zginęło 2 cywilów, a 2 innych zostało rannych. Korzystając z obecności w mediach społecznościowych, RDK opublikował filmy z terytorium Rosji, aby poprzeć swoje twierdzenia o odpowiedzialności.

Rosyjski Korpus Ochotniczy ogłosił swoje utworzenie w sierpniu 2022 r. w oświadczeniu na nowo utworzonym kanale Telegram: „My,

rosyjscy ochotnicy mieszkający w Ukrainie, postanowiliśmy chwycić za broń i stworzyć formację wojskową – Rosyjski Korpus Ochotniczy – aby wraz z naszymi ukraińskimi towarzyszami bronić ich ojczyzny, która nas chroni, a następnie kontynuować walkę ze zbrodniczym reżimem Putina i jego poplecznikami".

Według założyciela i dowódcy RDK Nikitina (Kapustina), korpus wchodzi w skład 1 kompanii 98 batalionu Obrony Terytorialnej „Azow-Dnipro" 108 brygady Sił Zbrojnych Ukrainy na kierunku Zaporoże–Donieck i podlega Głównemu Zarządowi Wywiadu Ministerstwa Obrony Ukrainy, a pierwotnie był częścią Międzynarodowego Legionu Ukrainy. RDK to jedna z najbardziej tajemniczych jednostek Obrony Terytorialnej Ukrainy.

W kwietniu 2023 r. Kapustin zamieścił wideo, w którym wzywa białych nacjonalistów ze Stanów Zjednoczonych, Wielkiej Brytanii, Niemiec i innych krajów do walki z Putinem, ponieważ Rosja przekształciła się w państwo policyjne, a rosyjski nacjonalizm „skręcił całkowicie w złym kierunku". Negatywnie wypowiadał się również o prezydencie Ukrainy Wołodymyrze Zełenskim.

Podczas wywiadu z rosyjskim opozycjonistą Markiem Feyginem dowódca RDK, Kapustin, oświadczył, że wszystkie działania jego jednostki na Ukrainie są koordynowane z ukraińskim dowództwem wojskowym. Informacja ta pojawiła się zaraz po pierwszym wtargnięciu RDK na terytorium Rosji, w lutym 2023 r., kiedy jednostka na krótko zajęła osadę przy granicy ukraińsko-rosyjskiej, a następnie się wycofała.

Rosyjski Korpus Ochotniczy ma tysiące zwolenników nie tylko wśród tych, którzy wyemigrowali z terytorium Federacji Rosyjskiej, ale także w obrębie Rosji. Próby zorganizowania rosyjskiego ruchu ochotników, który jako odrębna struktura miałaby walczyć z reżimem Putina i jego armią w Ukrainie, trwały przez kilka lat, od 2014 r.

Rosyjski Korpus Ochotniczy jest obecnie spójną jednostką o przejrzystej strukturze, powiązaniach pionowych i poziomych, oficjalnie wchodzącą w skład Sił Zbrojnych Ukrainy; jej członkowie otrzymują pensje, kontrakty i bilety wojskowe. Zaopatruje ich duża grupa wolontariuszy i wspiera emigracja rosyjska reprezentowana przez setki i tysiące zwolenników, także w Federacji Rosyjskiej. Szkolenie dla tych, którzy nie mają doświadczenia, trwa miesiąc, jest to łączona walka zbrojna, specjalne

szkolenie taktyczne, praca saperska. Następnie rozdziela się ludzi według specjalizacji.

DRK jest wpisany na listę organizacji terrorystycznych zakazanych na terytorium Federacji Rosyjskiej.

Niestety tzw. opozycja liberalna i propaganda rosyjska próbują oczernić RDK, nazywając członków tej organizacji nazistami i zdrajcami. Nikt się z nimi nie kontaktował i nie zaoferował pomocy, a można to zrobić na różne sposoby: wolontariatem, finansowo, informacyjnie. Nikt nie oczekuje, że politycy opozycji chwycą za broń i staną po stronie RDK, ale jest wiele innych sposobów, aby pomóc, ale ambicje imperialne są w ten czy inny sposób osadzone w kontekście opozycji systemowej i niesystemowej.

W odróżnieniu od legionu Wolność Rosji kierownictwo korpusu opiera się nie na byłym rosyjskim personelu wojskowym, który po kapitulacji trafił do legionu, ale na rosyjskich prawicowych emigrantach mieszkających w Ukrainie. Na początku wojny ludzie ci walczyli samotnie lub w małych grupach w ramach różnych jednostek ukraińskiej obrony terytorialnej, w tym z pułku Azow.

Ochotników korpusu można zaklasyfikować jako należących do prawicowo-konserwatywnego spektrum politycznego, wyznających tradycjonalistyczne przekonania, a raczej skrajnie prawicowe lub neonazistowskie. Grupa składa się głównie z antyputinowskich skrajnie prawicowych rosyjskich ekstremistów, którzy mają powiązania z ukraińskimi skrajnie prawicowymi grupami, według Michaela Colborne'a, badacza portalu śledczego Bellingcat. Jednocześnie sami bojownicy aktywnie posługują się symbolami Rosyjskiej Armii Wyzwolenia (ros. Русской Освободительной Армии, ROA), a także flagą Ukrainy.

Na portalu Telegram RDK napisał, że jego ideologia opiera się na „zasadzie bezkompromisowości": odrzuca wszelką współpracę z następcą reżimu sowieckiego, rządem Putina oraz jego przedstawicielami i lojalistami za granicą. Według RDK „Putin i jego poplecznicy niszczą Rosjan jako etos, zastępując ich sztuczną koncepcją «narodu politycznego», a teraz postanowili zniszczyć ukraińską grupę etniczną… kierowani strachem przed wolnością i prawdą".

Formacja wojskowa twierdzi, że realizuje misje bojowe na południowym wschodzie Ukrainy, będąc w „aktywnej obronie". Jednym

z problemów Rosyjskiego Korpusu Ochotniczego jest brak statusu jednostki prawnej. Teraz niektórzy bojownicy są indywidualnie zarejestrowani w obronie terytorialnej, a raczej w jednej z jej struktur – ochotniczych formacjach wspólnot terytorialnych. Ale w Korpusie są też ludzie, którzy nadal nie otrzymali żadnego oficjalnego statusu.

Struktura Korpusu:

- 1 pluton szturmowy;
- 1 kompania bezzałogowych statków powietrznych;
- grupa wywiadowcza;
- pluton moździerzy (dowódca Oleksij Levkin);
- oddział wolnokozacki RDK.

Od początku wojny na pełną skalę ochotnicy RDK brali udział w działaniach wojennych w obwodach czernihowskim, kijowskim, chersońskim, zaporoskim i donieckim, a także na terytorium Rosji w rejonach przygranicznych – w obwodach briańskim i biełgorodzkim.

Nie podają liczby ochotników, ale wnioski można wyciągnąć na podstawie poziomu zadań, które wykonują: zaczęli od udziału w walce pozycyjnej ramię w ramię z 98 batalionem Azow Dniepr, 111 brygadą w kierunku Doniecka, później przeszli do bardziej dynamicznych zadań, takich jak praca z systemem HIMARS, napad na pozycje Sił Zbrojnych Federacji Rosyjskiej.

Korpus od początku był grupą przyjaciół i znajomych, którzy zadawali sobie pytanie: dlaczego w Ukrainie nie ma rosyjskiego batalionu, a są białoruski, brytyjski, czeczeński? Stąd pomysł, aby zjednoczyć się w 1 jednostkę? W korpusie nie są tylko etniczni Rosjanie, ale w większości osoby z FR, którzy trafili na Ukrainę w wyniku walki z reżimem Kremla. Ochotnicy RDK są przeciwko „uformowania" wszystkich obywateli Rosji w nowy naród polityczny, w tym Buriatów, Czeczenów, Dagestańczyków i Kałmuków, w oparciu o tezę, że „oni wszyscy są Rosjanami".

Selekcja odbywa się w kilku etapach i nie każdy może ją przejść. Wszystkich nowych kandydatów traktuje się bardzo ostrożnie, aby uniknąć problemów związanych ze szpiegostwem, zagranicznymi agentami, prowokacjami itp. Najpierw przeprowadza się kilka rozmów, jeśli zajdzie taka potrzeba – prosi się Służbę Bezpieczeństwa Ukrainy o sprawdzenie danej osoby. Potem następuje dokładne zapoznanie się z zespołem (jak

człowiek zachowuje się na treningu, na boisku, jakie ma umiejętności i charakter). I dopiero wtedy trafia on na front.

Po ogłoszeniu mobilizacji na terytorium Federacji Rosyjskiej do korpusu napływały listy od chętnych do wstąpienia w ich szeregi. Zdarzają się przypadki, gdy nawet tym, którzy są chętni do walki, trzeba odmówić. Zwykle są to osoby bez doświadczenia wojskowego i wtedy próbuje się ich wpasować w cywilną strukturę korpusu: wyszukuje się zadania niezwiązane z frontem, żeby nie odpychać ochotników. Żadna z służb ukraińskich nie podtrzymywała obywateli Rosji, zwłaszcza po 24 lutego 2022 r. W tym tragicznym dniu w Ukrainie przebywało około 300 tys. obywateli Federacji Rosyjskiej i wszyscy znaleźli się w bardzo trudnej sytuacji – ich pozwolenia na pobyt stały wygasły, a Ukraina nie chciała im przedłużyć pobytu. Żołnierze Sił Zbrojnych Ukrainy posiadający obce obywatelstwo przechodzą przez procedurę uzyskania obywatelstwa ukraińskiego w przyspieszonym tempie.

Przedstawiciele RDK podkreślają, że nie było łatwo „przebić się przez lód podejrzeń" władz ukraińskich, ale tę selektywność zaufania rozumieją wszyscy członkowie korpusu. Udało im się pokonać ukraińską biurokrację, mur nieporozumień i podejrzeń. Oficjalnie walczą od sierpnia 2022 r. – wtedy (według dokumentów) powstał korpus. Sami podwójnie nieufnie podchodzą do osób chcących wstąpić w szeregi Rosyjskiego Korpusu Ochotniczego. Zdecydowano, że niektórzy bojownicy wystąpią publicznie z odkrytymi twarzami – raczej ci, którzy nie mają rodziny w FR. Po pierwsze, były to osoby publiczne jeszcze przed wojną. Po drugie, ludzie w maskach nie budzą zaufania, ponieważ nie ponoszą żadnej odpowiedzialności za to, co mówią – otwarta twarz dodaje natomiast powagi ich słowom.

Ochotnicy Rosyjskiego Korpusu Ochotniczego bronią suwerenności i niepodległości Ukrainy środkami militarnymi. Wojna prowadzona przez Federację Rosyjską w Ukrainie w celu zajęcia terytoriów i wyniszczenia ludności cywilnej jest sprzeczna z wszelkimi normami prawa międzynarodowego, zasadami prowadzenia działań wojennych oraz moralnymi i etycznymi, w wyniku czego korpus uznał ją za zbrodniczą. RDK uznaje Federację Rosyjską za państwo terrorystyczne i stwierdza niemożność i niedopuszczalność prowadzenia z nią negocjacji dyplomatycznych.

Główne cele wojskowo-polityczne RDC to ochrona i przywrócenie integralności terytorialnej Ukrainy w granicach z 1991 r. oraz obalenie reżimu rządzącego w Federacji Rosyjskiej.

Po osiągnięciu głównych celów Rosyjski Korpus Ochotniczy wzywa do:

- organizacji międzynarodowego trybunału dotyczącego wszystkich osób zaangażowanych w rozpętanie, prowadzenie i wspieranie agresywnej wojny przeciwko Ukrainie;
- odmowy przejęcia przez Federację Rosyjską terytoriów faktycznie zaanektowanych podczas wojen agresywnych;
- całkowitej reformy ustroju państwowego Federacji Rosyjskiej;
- zagwarantowania wolności narodowej narodu rosyjskiego;
- uznania i poszanowania prawa narodów zamieszkujących terytorium Federacji Rosyjskiej do samostanowienia.

W styczniu 2023 r., według dowódcy RDK Nikitina, grupa liczyła tylko 19 osób, mając jeden karabin maszynowy, 15 karabinów Kałasznikow i 4 pudła naboi, ale w kolejnym roku wiele się zmieniło. Jako jednostka ochotnicza korpus nie miał też na bieżąco wsparcia rządowego, a swoje potrzeby pokrywał ze środków osobistych i działalności wolontariatu.

Nikitin zapowiedział uzupełnienie szeregów swojej jednostki 10 grudnia 2023 r., podkreślając, że do Ukrainy przybyli nowi ochotnicy bez doświadczenia bojowego, wśród których są również wagnerowcy. „Tym razem przyjechali do nas nie tylko młodzi, nieuzbrojeni rekruci, ale także profesjonalni wojskowi – niektórzy weterani PKW «Wagnera» odpowiedzieli na moje wezwanie i także przybyli na Ukrainę, aby walczyć z prawdziwym wrogiem narodu ukraińskiego i rosyjskiego – machiną terroru Putina". Według Nikitina wchodzili oni w skład 98 batalionu TRO Azow Dnipro. W przyszłości podporządkowanie może ulec zmianie. Jeden z przywódców RDK Ilja Bogdanow powiedział w rozmowie z dziennikarzami latem 2023 r., po napadzie na obwód biełgorodzki: „Możemy znaleźć się obok «wagnerów» w kolejnej wojnie z reżimem Putina".

RDK znacznie się rozrósł, zwiększył również swoje możliwości wykonywania zadań bojowych. Kiedy ochotnicy dostają nową broń, bardzo to doceniają, ponieważ rozumieją, że zwracają na siebie uwagę i pomagają w walce. To jedna z jednostek, która już na początku 2024 r. liczyła ponad tysiąc bojowników, wśród których byli w szczególności przedstawiciele

PMC Wagner i Storm Z; miała swoje bazy, znacznie więcej broni strzeleckiej, karabinów maszynowych, moździerzy, jednostek UAV, własny system rekrutacji. W trakcie ostatnich lat zmienił się także stosunek społeczeństwa ukraińskiego do RDK: im bardziej jego członkowie wykazywali się udziałem w odważnych operacjach, tym bardziej społeczeństwo ukraińskie zwracało się w ich stronę. Znana jest też struktura RDK, na którą na początku 2024 r. składały się następujące jednostki:

- 1 pluton szturmowy;
- 2 pluton szturmowy;
- 1 kompania UAV;
- grupa wywiadowcza;
- pluton moździerzy (dowódca Oleksij Levkin);
- oddział wolnokozacki Rosyjskiego Korpusu Ochotniczego (ros. Вольно-казачий Отряд Русского Добровольческого Корпуса).

Ta ostatnia jednostka składająca się z kozackich ochotników, którzy chwycili za broń, aby walczyć razem z narodem ukraińskim przeciwko reżimowi na Kremlu, walczy za wyzwolenie terytoriów kozackich od reżimu kremlowskiego; zapewnienie ludności zamieszkującej południowe tereny Rosji prawa do samostanowienia i alternatywy dla obecnej drogi rozwoju; zachowanie tradycji kozackich i wojskowej kultury politycznej. To ochotnicy zarówno z Federacji Rosyjskiej, jak i z Ukrainy, którzy pokazali się już w niektórych gorących rejonach – Awdijiwce i Swatowym. Ich główne zadania to:

- pomoc Ukrainie w walce z okupantami z Federacji Rosyjskiej;
- zdobycie realnego doświadczenia bojowego i kwalifikacji;
- zjednoczenie w jednej jednostce aktywnych zwolenników idei kozackiej.

Korpus zgodził się wziąć udział w konferencji prasowej zorganizowanej w dniu 31 sierpnia 2022 r. z udziałem Rosyjskiego Legionu Wolności i Narodowej Armii Republikańskiej. Tego samego dnia Ilja Ponomariew, szef polityczny Narodowej Armii Republikańskiej, podpisał porozumienie o utworzeniu wspólnego centrum politycznego z Rosyjskim Legionem Wolności i oświadczył, że Rosyjski Korpus Ochotniczy również zgodził się przystąpić do tego samego porozumienia. Jednak RDK wydał później

oficjalne oświadczenie, że nie podpisał żadnej deklaracji, nie zgodził się na wstąpienie do centrum politycznego Ponomariewa, nie przyjął biało-niebiesko-białej flagi za swój symbol ani nie uznał Ponomariewa za swojego przywódcę politycznego. Przedstawiciele RDK powstrzymują się od publicznej krytyki legionu Wolność Rosji.

21 października 2022 r. na konferencji prasowej agencji informacyjnej Interfax-Ukraine upubliczniono memorandum Rosyjskiego Korpusu Ochotniczego.

Udział w działaniach wojennych

W 2022 r. bojownicy Rosyjskiego Korpusu Ochotniczego brali udział w:

- działalności partyzanckiej w Irpeniu i Buczy;
- bitwie o Moszczun;
- wypadach do obwodów czernihowskiego i chersońskiego;
- czteromiesięcznej aktywnej obronie stacjonarnego odcinka frontu na wysuniętych pozycjach wraz z żołnierzami 98 Batalionu Obrony Terytorialnej Azow Dnipro w obwodach zaporoskim i donieckim;
- desancie i kontrsabotażu na Wyspie Żmiiny;
- działalności dywersyjnej i realizacji zadań specjalnych na kierunku południowym wspólnie z innymi grupami;
- pracy z HIMARS;
- organizacji komórek konspiracyjnych na terenie Federacji Rosyjskiej i nadzorze nad ich działalnością partyzancką.

Rosyjskojęzyczna redakcja BBC wskazała, że najwyraźniej w 2022 r. ochotnicy RDK operowali w rejonach Zaporoża i Doniecka. W rozmowie z Polskim Radiem w lutym 2023 r. szef sztabu RDK Aleksander „Fortuna" stwierdził, że bojownicy „przeszli cały front", z wyjątkiem kierunku na Charków. Według bojowników Rosyjskiego Korpusu Ochotniczego jednostka spędziła 4 miesiące na froncie zaporoskim, od lipca do listopada 2022 r., i brała udział w działaniach wojennych wraz z 98 Batalionem Obrony Terytorialnej Azow Dniepr.

24 stycznia 2023 r. ochotnicy RDK w ramach jednostki specjalnej Głównego Wydziału Wywiadu Ministerstwa Obrony Ukrainy (GUR MOU) wzięły udział w nocnym nalocie na brzeg Nowej Kachowki. Po wykonaniu zadania grupa wróciła na prawy brzeg Dniepru. Dzięki temu

nalotowi wywiad otrzymał kompleksowe dane na temat liczby, składu i lokalizacji rezerw wroga. Część RDK wchodziła w skład garnizonu wojskowego na Wyspie Wężowej. Według niepotwierdzonych informacji RDK dysponuje co najmniej jedną HIMARS, o czym świadczy film opublikowany na oficjalnym kanale jednostki.

W dniu 2 marca 2023 r. władze rosyjskie zgłosiły atak na przygraniczne wioski Lubeczany i Suszany, w obwodzie briańskim, w wyniku którego co najmniej sześciu żołnierzy rosyjskich zostało rannych. Wkrótce po tym odpowiedzialność za atak przejął Rosyjski Korpus Ochotniczy: celem operacji było pokazanie, że wolni Rosjanie z bronią w rękach potrafią walczyć z reżimem Putina. Rząd ukraiński zaprzeczył jakiemukolwiek zaangażowaniu, nazywając to albo operacją pod fałszywą flagą, albo atakiem ze strony antyrządowych zwolenników w Rosji. Wiele rosyjskich ruchów nacjonalistycznych oskarżało tę grupę o zdradę stanu za wspieranie Ukrainy; jest także uznawana za organizację terrorystyczną przez Federację Rosyjską. Właśnie w 2023 r. RDK zyskała rozgłos, biorąc udział w transgranicznym nalocie w obwodzie briańskim, w Rosji, w którym wzięło udział 45 osób.

6 kwietnia 2023 r. Rosyjski Korpus Ochotniczy ponownie oświadczył, że przekroczył granicę z obwodem briańskim, wkraczając do wsi Słuczowsk. Choć władze rosyjskie twierdziły, że zapobiegnięto próbie napadu, Rosyjski Korpus Ochotniczy opublikował film przedstawiający członków grupy przebywających na terytorium Rosji. W czasie nalotu prowadzone były działania bojowe.

W dniu 22 maja 2023 r. w rejonie Grajworonu, w rosyjskim obwodzie biełgorodzkim, legion Wolność Rosji i Rosyjski Korpus Ochotniczy wspólnie przeprowadziły operację, a następnie przedostały się do samego Grajworonu. Gubernator obwodu biełgorodskiego Wiaczesław Gładkow w oświadczeniu przyznał, że „na terytorium obwodu grajworońskiego wkroczyła grupa dywersyjno-rozpoznawcza Sił Zbrojnych Ukrainy". Kilka kanałów Telegramu opublikowało film, który rzekomo pokazywał wjazd ukraińskich czołgów w rejon przejścia granicznego Grajworon, w obwodzie biełgorodskim. Według różnych ukraińskich mediów rosyjscy ochotnicy, walczący po stronie Ukrainy, zajęli także rosyjskie przejście graniczne w Kózince, na zachód od Biełgorodu, miejscowość Góra-Podol

i wezwali mieszkańców rosyjskich regionów przygranicznych, aby pozostali w domach i „nie stawiali oporu". Według doniesień zaatakowany został rejon stacjonowania jednostki wojskowej rosyjskich strategicznych sił rakietowych: w rejonie Grajworona znajduje się rosyjska jednostka wojskowa 25624 (w mieście Biełgorod-22), która wchodzi w skład strategicznych sił rakietowych Federacji Rosyjskiej i stanowi umowną nazwę centralnej bazy przechowywania broni nuklearnej.

Moskwa przyznała, że grupa dywersyjno-rozpoznawcza ukraińskich sił zbrojnych jest ścigana wspólnie przez służbę graniczną, Gwardię Rosyjską i FSB. Rosyjskie źródła w administracji obwodu grajoworonowskiego poinformowały opinię publiczną o możliwości częściowej ewakuacji przygranicznych wsi w najbliższej przyszłości. Natomiast GUR Ukrainy potwierdził, że legion Wolność Rosji i RDK prowadzą operację na terytorium obwodu biełgorodskiego, a rezultatem powinno być zwiększenie bezpieczeństwa i ochrona ukraińskiej ludności cywilnej przed atakami terrorystycznymi i ostrzałem ze strony grup terrorystycznych oraz utworzenie „strefy bezpieczeństwa". Dodano, że operację przeprowadzają wyłącznie Rosjanie.

24 maja 2023 r. RDK zorganizował konferencję prasową po ukraińskiej stronie granicy, na której dowódca Kapustin oświadczył, że jest usatysfakcjonowany wynikami nalotu: przed opuszczeniem terytorium Rosji po 24 godzinach jednostki przejęły broń, w tym transporter opancerzony, i wzięły jeńców; zapowiedziano również więcej takich najazdów i zdementowano doniesienia, jakoby bojownicy używali broni dostarczonej Ukrainie przez zachodnich sojuszników, aby pomóc bronić się przed inwazją Rosji. Zaznaczono, że 2 bojowników zostało rannych, zaprzeczając twierdzeniom rosyjskiej strony o ciężkich stratach zadanych ochotnikom. Ukraina ze swojej strony zapewniła wsparcie jedynie w postaci środków medycznych, paliwa i żywności. Z kolei legion Wolność Rosji podał, że 2 jego bojowników zginęło, a 10 zostało rannych.

Na początku czerwca RDK ponownie wkroczył na terytorium Federacji Rosyjskiej i poinformował o rozpoczęciu drugiej fazy operacji. Zaatakowano obwód biełgorodski, gdzie po tymczasowym zajęciu wsi Nowaja Tawołżanka i zbliżaniu się do miasta Szebekino wzięto do niewoli około 10 rosyjskich żołnierzy. Następnie dowódca Rosyjskiego Korpusu

Ochotniczego zwrócił się do gubernatora obwodu Wiaczesława Gładkowa z propozycją spotkania w celu wymiany jeńców, na co ten ostatecznie się nie zgodził. 7 czerwca RDK opuścił terytorium Federacji Rosyjskiej.

Lider grupy Nikitin wyraźnie stwierdził, że operacja briańska została zatwierdzona przez ukraińskie władze, a jej bojownicy w ciągu ostatnich kilku miesięcy publikowali filmy z pola bitwy. „Ukraina pomaga nam w każdej możliwej walce. Nie bylibyśmy w stanie mieć broni, gdyby nie było pomocy ze strony państwa, co najmniej, a także na terytorium Ukrainy jesteśmy pod jurysdykcją Ministerstwa Obrony Ukrainy. Co więcej, grupa jest również zaopatrywana i wykorzystuje broń z arsenału ukraińskiego wojska".

23 sierpnia 2023 r. Jewgienij Prigożin zginął w katastrofie lotniczej. RDK postanowił wykorzystać moment i zwrócił się do wagnerowców, w szczególności do tych, dla których „słowa lojalność i honor nadal mają znaczenie", wzywając ich do opowiedzenia się po stronie Ukrainy i zemsty za zabójstwo ich przywódcy. „Jeżeli nie popełniliście zbrodni wojennych na terytorium Ukrainy, to proponujemy, abyście wstąpili w nasze szeregi i najpierw dokończyli tę cholerną maszynkę do mielenia mięsa zwaną «specjalną operacją wojskową», a potem ponownie pomaszerować na Moskwę, ale tym razem nie zatrzymywali się 200 km od Moskiewskiego Okręgu Wojskowego, a dotarli do końca!".

W dniu 31 października 2023 r., podczas szturmu na linię umocnień wroga w rejonie awdijowskich zakładów koksowniczo-chemicznych 1 plutonem szturmowym RDK był wzięty jeniec wojskowy Ministerstwa Obrony Federacji Rosyjskiej.

Ochotnicy RDK przeprowadzili kolejną akcję na terenie obwodu briańskiego Federacji Rosyjskiej 9 listopada 2023 r. Grupa dywersyjno-rozpoznawcza RDK skutecznie zaatakowała wrogi transport rosyjskiej służby granicznej w obwodzie briańskim. Według doniesień zlikwidowano podpułkownika FSB Federacji Rosyjskiej Serhija Szatyja, który pełnił funkcję zastępcy szefa wydziału logistyki. Według własnych oświadczeń w 2023 r. RDK brał udział w 13 operacjach.

Wiosną i wczesnym latem 2023 r. naloty Rosyjskiego Korpusu Ochotniczego na terytorium Federacji Rosyjskiej stały się główną wiadomością dla wielu światowych mediów, jednak potem, aż do początku marca 2024 r.,

nic nie było słychać o takich operacjach specjalnych. W pierwszej połowie 2024 r. RDK powróciła do przestrzeni informacyjnej razem z legionem Wolność Rosji i Batalionem Syberyjskim. Rosyjski Korpus Ochotniczy prowadzi walki zarówno przeciw Rosji, jak i na terytorium Ukrainy: od połowy 2022 r. realizuje wspólne operacje specjalne ramię w ramię z jednostką specjalną Timura z GUR Ministerstwa Obrony Ukrainy. Oficer tej jednostki, posługujący się pseudonimem „Iwanow", opisuje bojowników RDK jako jednych z najbardziej zmotywowanych i oddanych żołnierzy, z jakimi kiedykolwiek miał do czynienia.

Głównym celem nalotów na Briańsk i Biełgoród było pokazanie ludziom, że Rosjanie przybyli, aby wyzwolić Rosję spod reżimu Putina, a także wycofanie sił armii rosyjskiej z innych obszarów frontu.

Według Ilji Bogdanowa podczas nalotów RDK i legionu Wolność Rosji na terytorium Federacji Rosyjskiej wszystkie ataki artyleryjskie na tereny zaludnione przeprowadzała wyłącznie strona rosyjska. „To jest ich zwykła taktyka, absolutnie nie mają szacunku dla ludności cywilnej. Cele tej operacji zostały osiągnięte, ponieważ RDK i LSR ściągnęły rosyjskie rezerwy, złamały logistykę wroga, powaliły plany obronne, a także uzyskały korzyści medialne".

RDK podkreśla, że jedną z najważniejszych zasad, których przestrzegają żołnierze korpusu, jest bezkompromisowość. Oznacza to zasadnicze odrzucenie jakiejkolwiek współpracy z przedstawicielami reżimu Putina, ponieważ współczesna Rosja stoi za wyniszczeniem Rosjan jako narodu etnicznego, próbując przekształcić go w naród polityczny. Ponadto Kreml próbuje zniszczyć także Ukraińców, bo rząd Putina jest pełen strachu przed prawdą i wolnością. Dlatego oprócz zwrotu okupowanych terytoriów Ukrainy bojownicy ochotniczych formacji wojskowych są zainteresowani wyzwoleniem samej Rosji ze szponów reżimu Putina.

W 2024 r. Rosyjski Korpus Ochotniczy prowadził działania bojowe w kierunku Awdijiwki, Zaporoża, Łymana, a także na terytorium Rosji. Największą operację korpusu rozpoczęto 12 marca 2024 r. na terenie obwodów biełgorodskiego i kurskiego, w zachodniej Rosji, przy wsparciu innych jednostek rosyjskich, w tym legionu Wolność Rosji i Batalionu Syberyjskiego. Celem było usunięcie części rosyjskich rezerw wojskowych z terytorium Ukrainy. W tym dniu toczyły się walki o wieś Tiotkino,

w obwodzie kurskim, gdzie ochotnikom udało się zniszczyć 2 składy broni okupantów. Wieś znalazła się pod kontrolą plutonu szturmowego RDK. GUR stwierdził, że grupy te działały autonomicznie na terytorium Federacji Rosyjskiej jako niezależne struktury, realizując własne zadania.

13 marca 2024 r. wojska rosyjskie po raz kolejny poniosły straty z rąk bojowników RDK, a w wyniku ataków na obwód biełgorodski ponad 45 tys. lokalnych mieszkańców zostało pozbawionych prądu w regionie. 16 marca 2024 r. Nikitin opublikował wideo z 25 rosyjskimi poborowymi, którzy zostali schwytani i zabrani do RDC.

Szef sztabu RDK „Fortuna" stwierdził, że w ręce RDK trafiły tajne dane rosyjskich naukowców zajmujących się rakietami – wiele tajnych informacji o rosyjskim programie rakietowym, dane osobowe kilkudziesięciu czołowych inżynierów-konstruktorów, a także niektórych kierowników procesów przy produkcji rakiet w FR. RDK planuje upublicznienie tej informacji. „Dziś RDK jest platformą wojskowo-polityczną, która pomaga Ukrainie militarnie dotrzeć do granic z 1991 r. Dla Ukrainy wojna tam się zakończy, a dla nas będzie to trwało. I to już będzie walka o całkowity demontaż reżimu Putina, w ogóle tamtejszego systemu politycznego. Jak teraz widzimy, jest to walka o strefę przygraniczną i jej demilitaryzację" – podkreśla Bogdanow.

Natomiast Nikitin uważa, że naloty RDK na Rosję, z jednej strony, zszokowały rosyjskie kierownictwo wojskowo-polityczne i samych Rosjan, z drugiej zaś – wywarły pozytywne wrażenie na ukraińskiej armii. Według niego liczba ochotników chcących wstąpić do RDK rośnie wskutek wiadomości o pomyślnych działaniach Rosyjskiego Korpusu Ochotniczego. Naloty na terytorium Rosji to coś, co zwykli obywatele utożsamiają z RDK.

W przyszłości planuje się utworzenie rosyjskiego państwa narodowego na terytorium regionów zamieszkałych w przeważającej mierze przez etnicznych Rosjan. Zachęca się także republiki narodowe do korzystania z prawa do samostanowienia. Praktycznie niemożliwe będzie uratowanie Rosji po klęsce w wojnie w obecnych granicach. W przeciwnym razie dojdzie do krwawej wojny pomiędzy regionami i państwami, które powstaną na ich miejscu.

Legion Wolność Rosji i Rosyjski Korpus Ochotniczy od wiosny 2023 r. prowadzą operację na terytorium obwodu biełgorodskiego, mającą na

celu utworzenia „pasa bezpieczeństwa" dla ochrony ukraińskiej ludności cywilnej – poinformował w komentarzu dla opinii publicznej przedstawiciel Głównego Zarządu Wywiadu Ministerstwa Obrony Ukrainy Andrij Jusow. Według niego operację przeprowadzają wyłącznie obywatele Rosji.

Planując działania wojskowe na terytorium FR, bojownicy RDK nie wiedzieli, jakie będą konsekwencje, jak zachowa się władza miejscowa i centralna, natomiast Kreml zaczął gorączkowo ściągać wojska z okupowanych terytoriów Ukrainy. Swoją działalnością RDK chciał pokazać, że z bronią w ręku można walczyć, że nie wszystko stracone, że jest cel i grupy, do których można dołączyć i kontynuować walkę przeciwko reżimowi Putina i że mogą to robić nie tylko obywatele innych krajów, ale także Federacji Rosyjskiej. Dzięki temu otrzymali możliwość prowadzenia działań, czego nie da się zrobić w samej Rosji. Doświadczenia, jakie zdobyła armia ukraińska, nie ma żadna inna armia na świecie.

Istotnym wyróżnieniem Rosyjskiego Korpusu Ochotniczego jest to, że składa się z ochotników. Oznacza to, że każdy walczy wyłącznie z własnej woli: nie są to więźniowie, uciekinierzy czy ludzie przyciśnięci do muru przez jakieś życiowe okoliczności, ale ludzie, którzy walczą, bo uważają, że to słuszne. To tak naprawdę walka o ich przyszłość, bo szczerze wierzą, że upadek Federacji Rosyjskiej pozwoli im wrócić do domu.

Sam fakt istnienia tej jednostki jest bezpośrednim kontrargumentem dla szerzonych przez rosyjską propagandę tez, że Ukraina nienawidzi wszystkiego, co rosyjskie, i zabrania komunikacji w języku rosyjskim, przy jednoczesnym tłumieniu praw obywateli Federacji Rosyjskiej. Ochotnicy z RDK nie są w Ukrainie po raz pierwszy, są wśród nich ci, którzy walczyli o lotnisko w Doniecku, Szyrokino, Debalcewo w 2014 r. W 2022 r. korpus realizował zadania na południu i wschodzie Ukrainy, uczestniczył także w obronie Kijowa. Ochotnicy nie ujawniają swoich nazwisk, jednocześnie zauważają, że część z nich była kiedyś znana w Rosji ze swoich poglądów i walczyła z reżimem Kremla jeszcze przed 2014 r. Teraz większość woli jednak pozostać incognito, ponieważ w Rosji mieszkają w dalszym ciągu ich krewni.

Olga Wasiuta

Belgorod: Russian paramilitary group vows more incursions, 24.05.2023, https://www.bbc.com/news/world-europe-65703548 (dostęp 3.06.2025); S. Blann, *Kremlin accuses Ukrainian saboteurs of attack inside Russia*, 2.03.2023, https://apnews.com/article/russia-ukraine-war-missile-strike-apartment-building-d2b8fc376956d2bedc44d3a0d711f260 (dostęp 23.05.2025); R. Dixon, F. Ebel, M. Ilyushina, *Kremlin accuses Ukraine of violent attack in western Russia*, 2.03.2023, https://www.washingtonpost.com/world/2023/03/02/bryansk-russia-attack-ukraine-saboteurs/ (dostęp 17.05.2025); R. Dixon, M. Ilyushina, *Alleged 'terrorist' attack in west Russia fuels hard-line pressure on Putin, 3.03.2023,* https://www.washingtonpost.com/world/2023/03/03/bryansk-russia-terrorist-attack-border/ (dostęp 17.05.2025); *Founder of Russian Volunteer Corps: attack on Bryansk region coordinated with Ukrainian authorities*, https://novayagazeta.eu/articles/2023/03/03/founder-of-russian-volunteer-corps-attack-on-bryansk-region-coordinated-with-ukrainian-authorities-en-news (dostęp 12.05.2025); *International Legion*, https://militaryland.net/ukraine/international-legion/ (dostęp 13.06.2025); *Kremlin accuses Ukraine of violent attack in western Russia*, „The Washington Post" 2.03.2023, https://www.washingtonpost.com/world/2023/03/02/bryansk-russia-attack-ukraine-saboteurs/ (dostęp 23.05.2025); S. Parkin, *The rise of Russia's neo-Nazi football hooligans*, 24.04.2018, https://www.theguardian.com/news/2018/apr/24/russia-neo-nazi-football-hooligans-world-cup (dostęp 12.05.2025); *Rosyjski Korpus Ochotniczy znów wkroczył do Rosji*, 1.06.2023, https://mil.in.ua/pl/news/rosyjski-korpus-ochotniczy-znow-wkroczyl-do-rosji/ (dostęp 12.06.2025); S. Shalunov, *Vladimir Putin's failing invasion is fueling the rise of Russia's far right*, 14.12.2022, https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-failing-invasion-is-fueling-the-rise-of-russias-far-right/ (dostęp 27.05.2025); *Ukraine briefing: G-20 'marred by Russia's unprovoked and unjustified war,' Blinken says*, 2.03.2022, https://www.washingtonpost.com/world/2023/03/02/russia-ukraine-war-news/ (dostęp 4.06.2025); *Ukrainian Reserve Officer Says Russia Is Forming Special 'Storm Z' Units*, 7.04.2023, https://www.newsweek.com/ukrainian-reserve-officer-says-russia-forming-special-storm-z-units-1793135 (dostęp 30.05.2025); Т. Левченко, «*Русский добровольческий корпус» в составе ВСУ: за что русские воюют против Путина*, 20.12,2022, https://ru.krymr.com/amp/russkiy-dobrovolcheskiy-korpus-vsu-voyna-intervyi/32185108.html (dostęp 15.05.2025); *Итоги года*, 2.01.2023, https://telegra.ph/Itogi-goda-01-02-2 (dostęp 16.04.2025); *"Російський добровольчий корпус" заявив, що до його лав вступили колишні вагнерівці, 10.12.2023,* https://novynarnia.com/2023/12/10/rosijskyj-dobrovolchyj-korpus/ (dostęp 27.05.2025); „*Смуги безпеки": у ГУР розповіли про те, що відбувається у Бєлгородській області росії*, 22.05.2023, https://kievvlast.com.ua/news/smugi-bezpeki-u-gur-rozpovili-pro-te-shho-vidbuvaetsya-u-belgorodskij-oblasti-rosii (dostęp

12.06.2025); *"Диверсионно-разведывательная группа" зашла в Белгородскую область. Что известно*, 22.05.2023, https://www.bbc.com/russian/news-65673136 (dostęp 12.06.2025); *«Русский добровольческий корпус» – это подразделение ВСУ? Российские партизаны? Или агенты ФСБ? Что известно, а что нет о «диверсии» в пограничных селах Брянской области*, 2.03.2023, https://meduza.io/feature/2023/03/02/russkiy-dobrovolcheskiy-korpus-eto-podrazdelenie-vsu-rossiyskie-partizany-ili-agenty-fsb (dostęp 15.05.2025); Е. Венкина, *Основатель РДК объявлен в розыск в РФ*, 27.03.2023, https://www.dw.com/ru/osnovatel-russkogo-dobrovolceskogo-korpusa-obavlen-v-rozysk-v-rf/a-65131489 (dostęp 12.05.2025). *В Брянской области произошла одна из самых громких диверсий за последнее время*, 3.03.2023, https://www.vedomosti.ru/politics/articles/2023/03/03/965086-ukraina-sovershila-odnu-iz-samih-gromkih-diversii (dostęp 12.05.2025); *Лидера «Русского добровольческого корпуса» Дениса Капустина заочно приговорили к пожизненному сроку*, 16.11.2023, https://www.bbc.com/russian/articles/cow2e314kw4o (dostęp 12.05.2025); Д. Горська, *«В Україні я воюю за те, щоб такої країни як Росія взагалі не було на карті», – колишній офіцер ФСБ Ілля Богданов*, 30.01.2024, https://www.sestry.eu/statti/v-ukrayini-ya-voyuyu-za-te-shchob-takoyi-krayini-yak-rosiya-vzagali-ne-bulo-na-karti----kolishniy-oficer-fsb-illya-bogdanov (dostęp 30.05.2025); М. Ткачук, *Боєць "РДК" Ілля Богданов після рейду по Росії: Ми можемо опинитися поруч із "вагнерами" в наступній війні проти режиму Путіна*, 29.06.2023, https://nov.ynarnia.com/2023/06/29/ibogdanov/ (dostęp 30.05.2025); *"Російський добровольчий корпус" показав новий бойовий вихід у Брянську область*, *6.04.2023,* https://novynarnia.com/2023/04/06/rosijskyj-dobrovolchyj-korpus-pokazav-novyj-bojovyj-vyhid-u-bryansku-oblast/ (dostęp 27.05.2025); А. Євич, *Найзагадковіший підрозділ ЗСУ. Як облаштований Російський добровольчий корпус*, 26.10.2022, https://glavcom.ua/publications/najzahadkovishij-pidrozdil-zsu-jak-oblashtovanij-rosijskij-dobrovolchij-korpus-884024.html (dostęp 27.05.2025); А. Мазуренко, *„РДК" і „Свобода России" заявили про звільнення двох населених пунктів на Бєлгородщині*, 22.05.2023, https://www.pravda.com.ua/news/2023/05/22/7403263/ (dostęp 4.06.2025); *Бєлгород скиглить про атаку дрона на будівлю ФСБ, – ЗМІ*, *13.03.2024,* https://novynarnia.com/2024/03/13/byelgorod-skyglyt (dostęp 22.05.2025); *Бійці РДК беруть участь у боях під Авдіївкою, під час штурму в полон взяли росіянина*, 31.10.2023, https://nv.ua/ukr/ukraine/events/de-zaraz-voyuyut-biyci-rdk-podrobici-novini-ukrajini-50364568.html (dostęp 12.06.2025); *Русский Добровольческий Корпус*, 31.10.2023, https://t.me/russvolcorps/753 (dostęp 15.05.2025); *Бійці Російського добровольчого корпусу заявили про перетин кордону у Брянській області РФ*, 2.03.2023, https://mil.in.ua/uk/news/bijtsi-rosijskogo-dobrovolchogo-korpusu-zayavyly-pro-peretyn-kordonu-u-bryanskij-oblasti-rf/ (dostęp 2.06.2025).

S

SEKTA – grupa o charakterze religijnym, ideologicznym lub społecznym, która wyłoniła się z istniejącego *status quo* poprzez negację zastanego porządku, postulująca inny ład, co na ogół jest postrzegane jako postawa radyklana, ekstremistyczna, bezkompromisowa, a nawet błędna.

Najczęściej mniejsza grupa odłącza się od większej poprzez zakwestionowanie jej zasad, kierując się własnymi poglądami, często naukami konkretnej osoby (lidera). Taka postać zazwyczaj ma silną pozycję i jest postrzegana jako charyzmatyczny przywódca, guru, teolog lub wizjoner, a nawet istota boska (*sacrum*). Członkostwo w takiej grupie ma charakter dobrowolny, a przynależność często staje się dla jednostki głównym źródłem tożsamości. Oznacza to, że osoba przystępująca do sekty musi zaakceptować jej zasady, sposób myślenia i wyznawane wartości. Członkowie rzadko kiedy uważają swoją grupę za sektę, najczęściej postrzegają ją jako jedyną prawdziwą drogę. Sekta nie zawsze musi wywodzić się bezpośrednio z religii, może też funkcjonować poza strukturami związków religijnych, bez powiązań organizacyjnych, obrzędowych czy doktrynalnych. Nie zawsze jest też formą otwartego protestu wobec wspólnot religijnych; często powstaje po prostu jako alternatywny ruch z własną interpretacją

zasad wiary, praktyk i wartości. Pierwotnie sekta była postrzegana jako grupa religijna, powszechnie akceptowalne jest określaniem tym mianem również grup powstałych na podłożu ideologicznym, kulturowym, socjoekonomicznym czy politycznym.

Pierwotne znaczenie słowa „sekta" pochodzi od łacińskiego terminu *sequi* („iść za kimś, towarzyszyć, naśladować"). Jego etymologia wywodzi się także od łacińskiego *secare* („odcinać, odrąbywać, wyodrębniać"), co podkreśla moment odłączenia się od większej wspólnoty religijnej. W klasycznej łacinie *secta* oznaczała sposób myślenia lub życia, a także partię polityczną bądź szkołę filozoficzną, której zasady ktoś przyjmował. Etymologicznie termin ten miał charakter neutralny i nie był nacechowany negatywnie.

Jednym z fundamentów socjologii religii jest teoria kościoła i sekty. Jej oryginalne sformułowania przedstawili Max Weber, Ernst Troeltsch i Helmut Richard Niebuhr. Była to polemika do materializmu historycznego, a zwłaszcza *Geschichte des Sozialismus in Einzeldarstellungen* (1895) i *Entstehung des Christentums* (1908) Karola Kautzky'ego. Marksiści zakładali, że sekta to pojęcie piętnujące ruchy asystemowe przez zwolenników utrzymania istniejącego *status quo*. Relacja między kościołem (panujący ład) a sektą (grupa upośledzona, aspirująca) opiera się na konflikcie klasowym, stąd stygmatyzacja nawet na poziomie semantycznym. Zatem relacja między kościołem a sektą jest relacją dialektyczną. Weber i Troeltsch odrzucili wpisywanie religii jedynie do teorii walki klas i postulowali, że ma ona swoją własną dialektykę wynikającą z niej samej. Sekty były radykalne, bezkompromisowe i odrzucały istniejący porządek społeczny. Dialektyka między kościołem a sektą jest częściowo napędzana ideami; w chrześcijaństwie jest nią Kazanie na Górze, umieszcza ono Królestwo Boże w radykalnej opozycji do świata świeckiego (Troeltsch). Pierwsi chrześcijanie byli zatem opozycją między radykalnymi ideałami a doktryną judaizmu. Przystępując do sekty, stawało się częścią „wybranych" (Weber). Sekta miała postawę separatystyczną, którą wzmacniały prześladowania. Izolowała się, zamiast dostosować do zastanego świata, a nawet wręcz mu się przeciwstawiała (Troeltsch).

W przeciwieństwie do sekty, kościół jest konserwatywny; reprezentuje „moralność szanowanej większości", idzie na kompromis ze światem

i akceptuje porządek świecki. Ustępuje wobec wojny, przemocy, tyranii i przejmowania własności prywatnej, sprzymierza się z państwem i „klasami rządzącymi", stając się integralną częścią hegemonicznego porządku społecznego.

Reakcje sekt na ten świat są zróżnicowane – od akceptacji po różny stopień odrzucenia. Niektóre są rewolucyjne, inne – reformatorskie. Niektóre dążą do zmiany świata, inne się wycofują, co jest reakcją na utratę nadziei na zmianę społeczeństwa. Wiele sekt odrzucało formalnie wykształcone duchowieństwo, a zamiast niego wybrało jednostki kierujące się inspiracją, a nie wiedzą, które nie były „produktem" istniejącego systemu, a co za tym idzie – jego protektorami/utrwalaczami.

Z czasem termin *secta* w kontekście religijnym zaczął być używany nie tylko opisowo, ale też oceniająco. Współcześnie coraz częściej w tym kontekście stosuje się pojęcie „nowy ruch religijny" (NMR). Stało się tak, ponieważ pojęcie to zaczęło być kojarzone bardzo negatywnie, głównie z zagrożeniem społecznym, manipulacją czy przestępczością. Termin NMR ma charakter bardziej neutralny i pozwala opisywać takie grupy bez przypisywania im od razu złych intencji. Wiele organizacji religijnych zaczęło określać się tym mianem, aby uniknąć automatycznie negatywnych skojarzeń.

W tradycji chrześcijańskiej znaczenie zmieniło się z neutralnego na bardziej negatywne. Zaczęto kojarzyć je z odrzuceniem oficjalnej doktryny i autorytetu kościoła. W okresie reformacji słowo sekta zaczęło być powszechnie używane na określenie ruchów, które powstały w wyniku rozłamów w chrześcijaństwie, choć oficjalnie dla „oderwania się" i „odłamu" używa się raczej terminu „schizma". Postrzeganie grup religijnych jako sekt i zagrożenia społecznego ma charakter historycznie powtarzalny; w tym znaczeniu sekta to grupa, która w pewnym momencie oderwała się od jednego z dużych kościołów panujących i funkcjonuje w izolacji od reszty społeczeństwa.

Istotnym czynnikiem są także nierówności społeczne, zarówno jeśli dotyczą one w sposób bezpośredni (grupa upośledzona), jak i jeśli należy się do grupy uprzywilejowanej, ale nie akceptuje się panującego ładu społecznego. W sytuacjach, kiedy rośnie poczucie niesprawiedliwości, ponieważ jakaś grupa jest spychana na margines, rodzi się napięcie – wtedy

mogą pojawić się formy protestu, także religijne, przybierające formy sekt. Równie istotne są zmiany polityczne i niezadowolenie społeczeństwa z panującej władzy: szuka ono wtedy różnych form wyrażenia sprzeciwu. Sekty mogą w takim momencie pełnić rolę podobną do ruchów opozycyjnych w polityce.

W praktyce najczęściej powstają w niższych warstwach społecznych, zazwyczaj wśród ludzi, którzy czują się wyobcowani i wykluczeni z życia społecznego. Przynależność do takiej grupy daje im poczucie wspólnoty i wpływu na coś większego. Sekty pojawiają się w okresach dużych zmian społecznych i intelektualnych, kiedy wzrasta poziom edukacji czy przychodzą wpływy z zewnątrz.

Proces werbowania do formacji jest zazwyczaj bardzo dobrze zaplanowany i stopniowy. Ważne, aby przekonać potencjalnego kandydata, że jest to całkowicie jego decyzja. Rekrutacja zazwyczaj zaczyna się od niezobowiązujących wydarzeń, takich jak pikniki, koncerty czy spotkania tematyczne, które nie wzbudzają podejrzeń. Już wtedy stosowane są różnego rodzaju techniki manipulacji: jedna z najpopularniejszych to tak zwany *love bombing*, czyli bombardowanie miłością. Sektę ukazuje się jako grupę, gdzie wszyscy są mili, dają poczucie wyjątkowości, prawią komplementy i są uśmiechnięci. Kolejnym krokiem jest wzbudzenie u kandydata poczucia zobowiązania, np. poprzez zaproszenie na kolejne spotkanie czy wręczenie upominku. Rekruterzy są wyszkoleni tak, aby umieć dostosować poziom rozmowy do różnych rodzajów osobowości. Takie działania mają stopniowo zwiększyć ciekawość oraz zaangażowanie, dzięki którym kandydat zdecyduje się dołączyć do grupy.

Grupy tego typu zazwyczaj izolują się od świata zewnętrznego i funkcjonują w zamkniętej strukturze. Mają rozbudowaną hierarchię władzy i ścisłe zasady, których osoby spoza ugrupowania nie znają, a którym członkowie muszą się podporządkować. W praktyce często wiąże się to z łamaniem podstawowych norm społecznych oraz negatywnym wpływem na ludzi, ich rodziny i otoczenie.

Hierarchia w sekcie opiera się na tzw. stopniach wtajemniczenia, które pełnią funkcję rang. Tworzy to pozory wewnętrznego porządku i sprawiedliwości, a przy tym zwiększa kontrolę nad członkami. Istotnym elementem jest również funkcjonujący system kar i nagród. Są to m.in.

wyróżnienia, pochwały czy awanse w hierarchii, ale również publiczne upomnienia czy ośmieszanie. Takie zabiegi zwiększają lojalność członków oraz poszerzają uzależnienie od lidera czy grupy.

Przebudowa osobowości to jeden z najistotniejszych mechanizmów działania sekt. Polega na całkowitej zmianie tożsamości i przekonań człowieka tak, aby nie wymagał dalszej kontroli. Taka osoba sama zaczyna myśleć i działać zgodnie z logiką grupy. Jest to proces, który odbywa się etapowo; na początku ma miejsce tzw. rozmrażanie – podważenie prawdziwości wizji świata stworzonego przez jednostkę i dostarczenie nadmiaru informacji. Wywołuje to dysonans poznawczy i często przyjmuje formę publicznej spowiedzi, a pytania uczestników nierzadko mają na celu przekonać jednostkę, że nie jest dość silna duchem, że ma jakieś okropne wady, a jej problemy są wynikiem popełnionych grzechów. Często doprowadza się celowo do wyczerpania psychicznego oraz fizycznego; stosuje się wtedy takie metody, jak narażenie na stres, ciągłe napięcie czy brak snu. Jednostka, która zwątpiła w swoją wizję świata, powoli obojętnieje i zaczyna przejmować punkt widzenia otaczającej ją grupy. Następnie poddawana jest manipulacji, która ma ją przekonać, że jedynie udział w tej grupie jest gwarantem wybawienia, często ma to charakter mistyczny, jest świadkiem „cudów" czy licznych „świadectw". Następnie dochodzi do procesu zamrażania, czyli całkowitej internalizacji (uwewnętrznienia) nowego systemu wartości. Żeby do tego mogło dojść, należy całkowicie zaprzeczyć dawnej tożsamości.

Intensywna indoktrynacja prowadzi do zastąpienia dotychczasowych przekonań nowym systemem wartości. Na tym etapie sekta musi upewnić się, że wszystkie wątpliwości zostały oddalone i może dojść do ostatecznego zamrożenia.

Ugrupowanie i jej lider stają się jedynym źródłem prawdy i bezpieczeństwa. Ostatnim punktem jest utrwalenie nowej tożsamości: członek zaczyna w pełni identyfikować się z grupą, często towarzyszy temu zerwanie z innymi grupami (np. rodziną), zmiana imienia, przywódca często nazywany jest „ojcem", współwyznawcy – „braćmi", co ma zastąpić rodzinę. Ostatnim etapem jest uzależnienie od sekty; polega ono na przekonaniu o niebezpieczeństwie świata zewnętrznego. Celowo zakłóca się równowagę emocjonalną, chwaląc ludzi w jednym momencie po to, by za chwilę

ich zganić. Wykorzystanie technik kształtowania postaw, jakimi są kary i nagrody, powoduje, że człowiek zaczyna czuć się bezradny i całkowicie zależny od grupy. Często sekty mają charakter apokaliptyczny – tylko pozostanie w nich gwarantuje zbawienie w czasie nadchodzącego końca świata. Inną metodą kontroli jest wywoływanie lęku związanego z myślą o odejściu z sekty. Członkom grupy opowiada się historie o ludziach, którzy opuścili sektę, zawsze tragiczne dla odchodzących. Notowane były też przypadki zmuszania do dokonania czynów zabronionych, co stawało się potem pretekstem do szantażu.

W powstaniu i rozwoju sekt bardzo dużą rolę odgrywa przywódca: najczęściej jest to osoba, która potrafi jasno wyrazić emocje, frustracje i potrzeby innych – dzięki temu staje się dla grupy kimś w rodzaju przewodnika. Taka osoba zazwyczaj pochodzi z tej samej klasy społecznej co jego zwolennicy, co sprawia, że łatwiej mu zdobyć ich zaufanie. Lider nadaje kierunek całemu ruchowi i koncentruje grupę wokół jednej, głównej idei. Jego głos trafia do ludzi pominiętych przez system czy zagubionych. Bardzo często to przywództwo decyduje o tym, czy dana sekta się rozwinie i przetrwa. Musi być przykładem dla innych w wyznawanych wartościach.

Działalność sekt może też naruszać prawa i wolności człowieka osobiste, społeczne, polityczne czy kulturalne. Zazwyczaj mają cechy, które są postrzegane negatywnie przez instytucje religijne i państwowe: silną władzę jednego przywódcy, wykorzystywanie członków w sposób instrumentalny, łączenie celów religijnych z politycznymi lub finansowymi, brak samokrytyki, próby całkowitego odcięcia się od zewnętrznej kontroli, np. rodziny czy mediów, oraz oczekiwanie pełnego posłuszeństwa.

Nie wszystkie sekty mają ten sam charakter czy poziom zagrożenia. Różnią się od siebie w zależności od metody działania, sposobu, w jaki powstały, działalności, otwarcia na społeczeństwa, doktryny czy struktury. Na tej podstawie możemy wyróżnić kilka głównych typów sekt:

1. Sekty odwołujące się do Biblii i chrześcijaństwa. Do tej grupy należą osoby, dla których autorytetem jest Biblia, jednak interpretują ją w inny, specyficzny sposób. Bardzo często polega to na pomijaniu powszechnie przyjętych zasad odczytywania tekstów religijnych. Dokonują oni własnych tłumaczeń, które znacząco odbiegają od

tych uznanych przez kościoły chrześcijańskie. W centrum ich doktryny stoi Jezus Chrystus. Członkowie wykazują duże zaangażowanie we wspólnotę. Grupy powstają poprzez wyłamanie się z tradycyjnych kościołów chrześcijańskich. Przykładem takiej sekty mogą być świadkowie Jehowy, którzy posługują się własnym przekładem Pisma Świętego.

2. Sekty orientalne. Tego typu sekty odwołują się do myśli Dalekiego Wschodu; czerpią z takich wierzeń jak buddyzm, hinduizm czy dżinizm. Głównym autorytetem jest mistrz duchowy, nazywany guru, oraz teksty uznawane przez członków za święte. Doktryna opiera się zazwyczaj na wierze w konkretne bóstwo, reinkarnacji i rozwoju duchowym. Duży nacisk kładzie się na samorozwój, wegetarianizm oraz całkowite oddanie mistrzowi. Przykładem może być Międzynarodowe Stowarzyszenie Świadomości Kryszny (Hare Kryszna).
3. Sekty odwołujące się do nowego mesjasza lub objawienia. Ten typ sekt charakteryzuje przekonanie, że przywódca grupy, nazywany przez członków prorokiem czy mesjaszem, otrzymał objawienie, które wskazuje drogę do zbawienia świata. Staje się ono podstawą wiary i zasad postępowania członków. Przekazywane przez niego słowa mają rangę świętych tekstów. Objawienie może być jednorazowe lub trwać przez dłuższy okres. Za tego typu ugrupowanie można uznać Kościół Zjednoczeniowy Moona.
4. Sekty synkretyczne. W tym przypadku doktryna opiera się na łączeniu elementów wielu religii i filozofii pochodzących z różnych części świata. Jej celem jest stworzenie nowej, uniwersalnej religii, nieuznającej podziałów. Tego typu grupy wyróżniają się dużą tolerancją i szacunkiem dla różnych wierzeń. Ich zasady oraz struktura zależą od konkretnej grupy, jednak elementem łączącym jest scalenie wielu idei w jeden system. Przykładem jest ugrupowanie Zaproszenie do Życia.
5. Grupy New Age. Ich ideologia opiera się na przekonaniu, że świat jest aktualnie w okresie przemiany i wszystkie religie wymagają reform. Członkowie wierzą w boskość człowieka i jego nieograniczone możliwości. Podstawowymi założeniami jest panteizm,

reinkarnacja czy monizm. Tego typu ruchy często nie posiadają określonej struktury organizacyjnej, dlatego nie zawsze są traktowane jako sekty w tradycyjnym sensie. Często czerpią z różnych nurtów duchowych i ezoterycznych, takich jak okultyzm, magia, gnoza czy wierzenia związane z UFO i cywilizacjami pozaziemskimi.

Sposób funkcjonowania sekt najlepiej widać na przykładach organizacji, których działania miały znaczący wpływ na bezpieczeństwo publiczne. Jedną z nich jest grupa pochodząca z Japonii o nazwie Aum Shinrikyo (Najwyższa Prawda). Frakcja powstała w latach 80. jako szkoła jogi, jednak szybko przeobraziła się w groźną organizację apokaliptyczną. Jej ideologia łączyła elementy buddyzmu, hinduizmu i chrześcijaństwa z wizją końca świata, który miał wystąpić w wyniku globalnej wojny. Działania lidera Shoko Asahary, który był uznawany za mesjasza mogącego ocalić ludzkość, doprowadzały do całkowitego podporządkowania i porzucenia dawnego życia. Sekta miała dobrze wykształconych członków, ogromne zasoby finansowe i własne laboratoria, w których pracowano nad bronią biologiczną i chemiczną. W 1994 r. dokonali ataku sarinem w Matsumoto, a rok później – w tokijskim metrze, gdzie śmierć poniosło 13 osób, a tysiące zostało rannych.

Gałąź Dawidowa jest kolejnym przykładem radykalnej sekty. Wywodziła się z ruchu adwentystycznego i działała w Teksasie. Jej członkowie wierzyli w nadchodzącą apokalipsę i ich misję jako boskich wybrańców. Liderem grupy był David Koresh, który uważał się za nową inkarnację Chrystusa. Sekta działała w zamknięciu, odrzucając prawo i zasady świata zewnętrznego. W 1993 r. doszło do konfrontacji z FBI i ATF, która zakończyła się pożarem siedziby sekty i śmiercią kilkudziesięciu osób.

Działalność sekt jest realnym zagrożeniem dla bezpieczeństwa społeczeństwa, państwa, jak i samej jednostki. Poprzez techniki psychomanipulacji kontrolują emocje, zachowania i sposób myślenia swoich członków. Bardzo często skutkuje to izolacją od rodziny, ograniczeniem dostępu do służby zdrowia, utratą zdolności do podejmowania samodzielnych decyzji oraz pełnym uzależnieniem ekonomicznym i emocjonalnym. Przez to, że sekta staje się dla członka jedynym źródłem wartości i wzorców, dochodzi do rozbijania rodzin czy całkowitego zrywania więzi społecznych.

Na poziomie społecznym sekta może destabilizować wspólnoty, radykalizować członków, powodować oraz wzmacniać konflikty. Dla bezpieczeństwa państwa największym zagrożeniem są przede wszystkim sekty, które nie przestrzegają zasad prawa i obowiązków względem instytucji publicznych. Ich działalność w sposób hermetyczny znacząco utrudnia kontrolę przez służby.

To zjawisko jest od wielu lat przedmiotem analiz instytucji bezpieczeństwa w Polsce, m.in. w raportach Biura Bezpieczeństwa Narodowego *O stanie bezpieczeństwa państwa* z 1995 r. i Ministerstwa Spraw Wewnętrznych i Administracji o nazwie *Raport o niektórych zjawiskach związanych z działalnością sekt w Polsce* z 2000 r. Podkreślają one konieczność monitorowania sekt i oceniania ich działalności pod kątem zdrowia, praw człowieka i porządku publicznego. Podstawy prawne w tym zakresie znajdują się w Konstytucji Rzeczypospolitej Polskiej w art. 13 i 53 oraz ustawie o gwarancjach wolności sumienia i wyznania z 1989 r. Dopuszczają one ograniczenia wolności religijnej w przypadku zagrożenia bezpieczeństwa państwa.

Przemysław Mazur, Martyna Czerniak

Adventist Today, „Religion and the Waco Cult" 1993, vol. 1, no. 1; M. Bendza, *Sekty: trudności ze zdefiniowaniem zjawiska. Próba ukazania niebezpieczeństwa*, „Elpis" 2005, nr 7; C.M. Cusack, D.L. Kirby, *Sects, Cults, and New Religions: An Introduction*, [w:] *Sects, Cults, and New Religions*, t. 1, C.M. Cusack, D.L. Kirby (eds.), Routledge, London–New York 2014; R. Danzig, M. Sageman, T. Leighton, L. Hough, H. Yuki, R. Kotani, Z.M. Hosford, *Aum Shinrikyo: Insights Into How Terrorists Develop Biological and Chemical Weapons*, Center for a New American Security, Washington DC 2012; Etymonline.com, https://www.etymonline.com/word/sect (dostęp 15.10.2025); M. Gajewski, *Nowe ruchy religijne i sekty – między zbawieniem a destrukcją…*, Dom Wydawniczy Rafael, Kraków 2002; W.S. Goldstein, *The dialectics of religious conflict: Church – sect, denomination and the culture wars*, „Culture and Religion" 2011, no. 12:01; K. Kaczmarek, *Sekty z innego punktu widzenia*, „W Drodze" 2001, nr 5; I. Kamiński, *Sekty i alternatywne ruchy religijne. Stan wiedzy – próba systematyzacji*, „Roczniki Kulturoznawcze" 2021, t. XII, nr 4; J. Matwiejuk, *Sekty w polskim systemie prawnym*, „Elpis" 2005, t. 7; M. Soliński, *Niebezpieczeństwa płynące z sekt destrukcyjnych*, [w:] *Problemy i kwestie społeczne*, K. Białożyt, B. Uliasz, M. Soliński (red.), Uniwersytet Pedagogiczny

im. KEN w Krakowie, Kraków 2014; B. Stasiak, *Instytucjonalne pojęcie sekty*, „Łódzkie Studia Teologiczne" 2016, t. 25, nr 3; E. Troeltsch, *The social teaching of the Christian churches*, John Knox Press, Louisville 1992; M. Zaśko-Zielińska, *Sekta czy nowy ruch religijny: Zderzenie poglądów, zderzenie punktów widzenia*, [w:] *Punkt widzenia w języku i w kulturze*, Wydawnictwo UMCS, Lublin 2004; M. Weber, *'Churches' and 'sects' in North America*, [w:] *The Protestant ethic and the 'spirit of capitalism' and other writings*, M. Weber (ed.), Penguin, New York 2002; B.R. Wilson, *The Social Dimensions of Sectarianism. Sects and New Religious Movements in Contemporary Society*, Clarendon Press, Oxford 1990.

SHARENTING – praktyka udostępniania zdjęć, filmów, danych osobowych i informacji na temat dzieci przez ich rodziców lub opiekunów prawnych, w szczególności za pośrednictwem platform mediów społecznościowych, komunikatorów oraz publicznie dostępnych stron internetowych. Magdalena Gadamska-Kyrcz (2023), powołując się na definicję Fundacji Orange, wskazuje również na „bezrefleksyjność" i „nadmierność" takiego udostępniania jako istotne elementy definicyjne. Wyznaczenie granicy między uzasadnionym i nadmiernym udostępnianiem tego typu treści byłoby uznaniowe i podlegałoby każdorazowo ocenie. Należy jednak podkreślić, iż liczne badania ankietowe wykazują istotne rozpowszechnienie zjawiska i niski stopień społecznej świadomości związanej z sharentingiem, co może przekładać się na brak refleksji po stronie udostępniających.

Nasilenie i rozpowszechnienie sharentingu jest konsekwencją zmian społecznych dotyczących zachowań rodzicielskich, form korzystania z technologii oraz przeniesienia znaczącej części życia społecznego do sfery cyfrowej. Nie jest to jednak zjawisko nowe, występowało bowiem w innych formach i z mniejszą intensywnością także przed „erą mediów społecznościowych" (np. pokazywanie zdjęć dzieci w formie analogowej).

Termin wywodzi się od połączenia angielskich słów *share* („udostępniać") i *parenting* („rodzicielstwo"). Wiktoria Grabalska i Rafał Wielki (2022) wskazują, iż określeniem tym w 2010 r. jako pierwsi posłużyli się dziennikarze „Wall Street Journal" w artykule krytycznie oceniającym praktyki rodziców w mediach społecznościowych. Termin *sharenting*, choć nieformalny w swoim pochodzeniu i nieposiadający uniwersalnej definicji prawnej, jest przedmiotem rosnącego zainteresowania akademickiego i prawnego ze względu na implikacje dla prywatności, etyki

i bezpieczeństwa, jakie niesie nadmierne udostępnianie informacji na temat dzieci w internecie. Ma również istotne znaczenie w kontekście tożsamości cyfrowej, praw małoletnich i ochrony danych osobowych. Z drugiej strony, wskazuje się na konieczność zagwarantowania swobody ekspresji i możliwości dzielenia się istotnymi informacjami na temat życia rodzinnego także w środowisku cyfrowym, co z kolei rodzi naturalny konflikt na linii prywatność–wolność ekspresji.

Co do zasady, zjawisko sharentingu charakteryzuje się dokumentacją życia dziecka, która może mieć charakter regularny i systematyczny. W wielu wypadkach informacje na temat dziecka udostępniane są od jego urodzenia, a niejednokrotnie nawet wcześniej (np. obrazy USG płodu). Typowe przykłady obejmują publikowanie zdjęć z sali porodowej, a następnie dokumentowanie istotnych wydarzeń w życiu i rozwoju dziecka. W skrajnych przypadkach dochodzi nawet do transmisji na żywo z przebiegu porodu. Ze względu na upublicznianie informacji, a następnie ich trwałe indeksowanie przez wyszukiwarki i algorytmy mediów społecznościowych, rodzice lub opiekunowie przyczyniają się do tworzenia tożsamości cyfrowej dziecka i pozostawiania tzw. cyfrowych odcisków palców, bez wiedzy lub (świadomej) zgody dziecka.

Można wyróżnić wiele rodzajów sharentingu – ich klasyfikacja jest zależna od kontekstu i celu udostępniania informacji. I tak, *oversharenting* dotyczy nadmiernego dzielenia się materiałami dotyczącymi dziecka: w ocenie Gadamskiej-Kyrcz może obejmować chociażby zakładanie dzieciom profili w mediach społecznościowych i prowadzenie ich „niejako w ich imieniu". *Commercial sharenting* jest z kolei nastawiony na komercyjne wykorzystywanie wizerunku dziecka w celu uzyskania gratyfikacji finansowej (tzw. monetyzowanie treści). W przypadku parental trollingu chodzi o udostępnianie treści, które mają charakter ośmieszający lub upokarzający. W wielu wypadkach są one prezentowane jako forma żartu, lecz mogą mieć długotrwałe skutki dla reputacji oraz zdrowia psychicznego dzieci, także w okresie dorosłości.

Status prawny sharentingu jest złożony i na ten moment wymyka się regulacjom prawnym. Odpowiednie przepisy mogą być wywodzone subsydiarnie z prawa cywilnego, w tym prawa do wizerunku czy prywatności, jak również z ustawodawstwa dotyczącego ochrony danych

osobowych (np. Ogólne rozporządzenie o ochronie danych, tzw. RODO). Ze względu jednak na istotę władzy rodzicielskiej, praktyczne egzekwowanie praw dzieci i osób małoletnich jest uzależnione w dużej mierze od prawnych opiekunów i pozostawia im istotny poziom swobody w decydowaniu o rozporządzaniu wizerunkiem dziecka. W konsekwencji prawo do prywatności dziecka podlega istotnym ograniczeniom. Może to także kolidować z prawem do bycia zapomnianym.

W przestrzeni międzynarodowej podstawowe normy etyczne dotyczące sharentingu wyznaczać może m.in. Konwencja o prawach dziecka chwalona przez Zgromadzenie Ogólne Narodów Zjednoczonych (UNCRC), która gwarantuje prawo do ochrony przed wykorzystywaniem, w tym cyfrowym. Nie powinna być jednak traktowana jako podstawa prawna dochodzenia naruszeń, lecz pewien katalog ogólnych zasad, który może w przyszłości stanowić punkt odniesienia dla konkretnych przepisów cywilnych lub karnych w poszczególnych krajach. Prace nad uregulowaniem sharentingu były lub są prowadzone w co najmniej kilku krajach UE.

W praktyce orzeczniczej pojawiają się precedensowe przypadki zobowiązania prawnych opiekunów bądź członków rodziny do np. usunięcia zdjęć dzieci udostępnionych w internecie. Argumentacja może być w tym wypadku oparta na konieczności uzasadnionej ochrony interesu dziecka, w tym prawa do prywatności oraz zabezpieczenia jego danych biometrycznych. Anna Hernacka-Janikowska (2023) wskazuje, iż w polskim systemie prawnym odpowiednie przepisy ochronne można wywodzić z prawa do wizerunku (art. 23 Kodeksu cywilnego), prawa do intymności (art. 191a §1 Kodeksu karnego) czy ochrony przed treściami pedofilskimi (art. 202 §1 Kodeksu karnego).

Sharenting stwarza istotne zagrożenia dla bezpieczeństwa osób, które padają jego ofiarami, szczególnie ze względu na dostępność szczegółowych danych osobowych nieletnich w miejscach publicznych lub słabo chronionych środowiskach cyfrowych. Zagrożenia te mogą obejmować (wyliczenie przykładowe):

1. Kradzież tożsamości – obrazy i dane osobowe, takie jak wizerunek, dane personalne, daty urodzenia, mogą być gromadzone i wykorzystywane do kradzieży tożsamości lub tworzenia

syntetycznych tożsamości. Na bazie udostępnionych materiałów mogą być tworzone m.in. fałszywe profile lub dokumenty dzieci.
2. Oszustwa i wyłudzenia – współczesne technologie, w szczególności *deep fakes*, pozwalają m.in. na kopiowanie wizerunku oraz klonowanie głosu ofiary na podstawie upublicznionych materiałów, a następnie ich wykorzystywanie do prób podszywania się, jak również wyłudzeń (np. udoskonalona „metoda na wnuczka").
3. Profilowanie i śledzenie zachowań – udostępnianie danych może się przyczyniać do długotrwałego profilowania cyfrowego, a wobec agregacji istotnej ilości danych udostępnione treści mogą być analizowane pod kątem targetowania behawioralnego.
4. Nękanie i ośmieszanie – udostępnianie treści poniżających może być źródłem cyberbullyingu, a ich zwielokrotnianie może się przyczyniać do długotrwałych negatywnych konsekwencji reputacyjnych i psychologicznych.
5. Tworzenie treści pedofilskich – wobec istotnego rozwoju narzędzi sztucznej inteligencji udostępniane materiały mogą być podstawą do tworzenia treści pedofilskich (ang. Child Sexual Abuse Materials, CSAM), zarówno od podstaw (całkowita synteza) bądź poprzez nałożenie twarzy dziecka na już istniejące nagranie (technika *face-swap*). Hernacka-Janikowska (2023) przywołuje dane, z których wynika, iż ponad połowę treści pedofilskich cyrkulujących online stanowią kopie zdjęć lub wideo zamieszczanych właśnie w ramach sharentingu.
6. *Doxxing* – możliwość ponownego ujawniania danych osobowych i prywatnych informacji o dziecku, w tym o miejscu zamieszkania, w celu jego zastraszania i nękania.
7. Porwania – eksponowanie wizerunków dzieci może być impulsem do ich porwania, zwłaszcza wobec łatwości w ustalaniu lokalizacji na podstawie metadanych bądź dodatkowych informacji (np. lokalizacyjnych) ujawnianych online.

Te wektory zagrożeń są nasilane przez rosnącą dostępność narzędzi umożliwiających agregację dużej liczby danych, jak również manipulowanie i modyfikowanie treści audio i wizualnych.

Udostępnianie treści w ramach sharentingu to zjawisko globalne, które istotnie przybrało na sile wraz z rozwojem mediów społecznościowych. Motywacje osób udostępniających obejmują m.in. chęć podzielenia się istotnymi informacjami na temat życia rodzinnego (np. z poczucia szczęścia czy dumy), ale również czynniki finansowe (monetyzacja wizerunku dzieci) czy chęć dowartościowania się (np. poprzez publikację atrakcyjnych i „podobających się" treści). Niektórzy autorzy wskazują również na istotną rolę ograniczenia relacji społecznych związanego z narodzinami dziecka, kompensowanego następnie aktywnością w sieci, oraz znaczenie presji grupowej i chęć dostosowania się do trendów panujących online.

Maria Giulia Conti i współpracownicy (2024) wskazują, iż nawet 75% ankietowanych rodziców posiadających konta w mediach społecznościowych deklaruje publikowanie zdjęć lub historii o swoich dzieciach, w szczególności przed 5 rokiem życia. Podobne trendy obserwuje się na całym świecie. Raport Komisarza ds. Dzieci w Wielkiej Brytanii wykazał, iż rodzice mogą publikować średnio setki zdjęć dzieci online, zanim te ukończą 13 rok życia. Anna Borkowska i Marta Witkowska (2020) wskazują, iż „23% dzieci zaczyna cyfrowe życie, zanim fizycznie przyjdzie na świat […], 81% dzieci poniżej 2 r. ż. z krajów Unii Europejskiej, USA, Australii, Nowej Zelandii i Japonii ma cyfrowy ślad w postaci zdjęć opublikowanych w internecie przez rodziców, a 5% z nich posiada swój profil społecznościowy. Średnia wieku «cyfrowych narodzin» dziecka wynosi 6 miesięcy". Badania naukowe przeprowadzone w Polsce także wskazują na stały wzrost liczby i częstotliwości udostępniania w internecie treści związanych z dziećmi. Co więcej, 45% nastolatków przyznaje, iż znajduje się na zdjęciach umieszczanych przez rodziców w mediach społecznościowych. Marcin Niedbała (2024) podkreśla, iż 1/4 ankietowanych odczuwa z tego powodu wstyd lub skrępowanie.

W badaniach wskazuje się również na niską społeczną świadomość długoterminowych konsekwencji udostępniania zdjęć i informacji na temat dzieci. Należy także odnotować tendencję do bagatelizowania zagrożeń ze względu na poczucie pozornej intymności, gdy materiały są rozpowszechniane w ograniczonych kręgach towarzyskich. Takie udostępnianie nie wyklucza bowiem wtórnej multiplikacji materiałów

bądź też ich wykorzystania do szkodliwych celów przez osoby pozornie „zaufane".

Istotnym elementem przeciwdziałania zjawisku sharentingu są społeczne kampanie edukacyjne i informacyjne. W Polsce kluczową rolę w tym procesie odgrywa NASK (Naukowa i Akademicka Sieć Komputerowa) – Państwowy Instytut Badawczy, który regularnie publikuje materiały uświadamiające rodziców, w tym poradniki cyfrowe odnoszące się do bezpieczeństwa w sieci. W 2020 r. wydano m.in. poradnik dla rodziców zatytułowany *Sharenting i wizerunek dziecka w sieci*. W przestrzeni międzynarodowej ważnym elementem budowania świadomości była kampania #ShareWithCare przeprowadzona przez Deutsche Telekom, w ramach której zrealizowano m.in. wideo edukacyjne *Message from Ella*.

Mateusz Łabuz

A. Borkowska, M. Witkowska, *Sharenting i wizerunek dziecka w sieci*, NASK, Warszawa 2020; B. Chrostowska, *Sharenting – skala i wielowymiarowość zjawiska (nierozważnego) ujawniania przez rodziców informacji o dzieciach w mediach społecznościowych*, „Problemy Wczesnej Edukacji" 2018, nr 4(43); M. Conti, *Sharenting: characteristics and awareness of parents publishing sensitive content of their children on online platforms*, „Italian Journal of Pediatrics" 2024, no. 50; M. Gadamska-Kyrcz, *Sharenting jako jedno z niebezpieczeństw dla dzieci*, „Ochrona Ludności i Dziedzictwa Kulturowego" 2023, nr 3; W. Grabalska, R. Wielki, *„Czy dzieci powinny trafiać do sieci?" Prawne i kryminologiczne aspekty zjawiska sharentingu*, „Prawo w Działaniu" 2022, nr 49; A. Hernacka-Janikowska, *(Nie)bezpieczeństwo dziecka w sieci – analiza krytyczna zjawiska sharentingu, troll parentingu i monetyzacji wizerunku dziecka*, „Studia Prawnoustrojowe" 2023, nr 61; S. Kubiak, *Sharenting – współczesne zagrożenie czy szansa?*, „Political Dialogues" 2023, nr 23; J. Maniszewska-Ejsmont, *Sharenting a prawa dziecka – rozważania nad władzą rodzicielską w dobie mediów społecznościowych*, „Palestra" 2022, nr 2; M. Niedbała, *Sharenting jako zagrożenie dobra dziecka. Pomiędzy koniecznością ingerencji sądu opiekuńczego, a potrzebą edukacji społeczeństwa*, „Law, Education, Security" 2024, nr 2; S. Smith-Kang, *Making the News: "Sharenting" in the Modern World*, https://www.first5la.org/article/making-the-news-sharenting-in-the-modern-world (dostęp 17.07.2025); I. Tomaszewska-Gałuszka, *Sharenting – zdjęcia dzieci mogą stać się łupem cyfrowych porywaczy*, 2024, https://demagog.org.pl/analizy_i_raporty/sharenting-zdjecia-dzieci-moga-stac-sie-lupem-cyfrowych-porywaczy/ (dostęp 07.07.2025).

SOCJALIZM DEMOKRATYCZNY – za optymalny ustrój w gospodarce uważa socjalizm, ale to demokrację preferuje jako formę sprawowania władzy. W takim systemie środki produkcji stanowiłyby własność całego społeczeństwa, które sprawowałoby nadzór nad funkcjonowaniem gospodarki poprzez demokratyczne zarządzanie państwem. Takiej formule najlepiej odpowiada system republikański.

W szerszym rozumieniu poprzez socjalizm demokratyczny rozumie się zabiegi zmierzające do wprowadzenia ustroju socjalistycznego, ale poprzez działania pokojowe, a nie rewolucyjne – niosące ze sobą destrukcję i gwałtowne zaburzenia społeczne. Ta filozofia polityczna zmierza do likwidacji ustroju kapitalistycznego, a nie do jego reformowania. Jej początki związane są z socjalizmem utopijnym oraz ruchem czartystów w Wielkiej Brytanii. Podobnie jak przedstawiciele tych nurtów, socjaliści demokratyczni optowali za demokratycznym podejmowaniem decyzji i publiczną własnością środków produkcji. W Wielkiej Brytanii pod koniec XIX w. poglądy oparte na socjalizmie demokratycznym głosiła Liga Socjalistyczna Williama Morrisa, a także Towarzystwo Fabiańskie i Niezależna Partia Pracy. George Douglas Howard Cole w latach 20. XX w. podjął starania o stworzenie systemu pozostającego w opozycji do radzieckiego autorytaryzmu, co spowodowało wzrost zainteresowania demokratycznym socjalizmem. Poglądy te popierał i prezentował m.in. George Orwell, który podkreślał, iż ustrój wprowadzony przez Włodzimierza Lenina w Rosji nie ma nic wspólnego z socjalizmem, jest tylko dyktaturą skrywaną pod jego hasłami.

Eugene V. Debs był przedstawicielem idei socjalizmu demokratycznego w USA. Ten zdeklarowany socjalista aż pięciokrotnie startował w wyborach na urząd prezydenta tego kraju. Innym promotorem tej ideologii w Stanach Zjednoczonych był Daniel De Leon, przywódca Socjalistycznej Partii Pracy i aktywny działacz II Międzynarodówki. Innym ważnym politykiem tej opcji politycznej był Norman Thomas, były pastor kościoła prezbiteriańskiego i sześciokrotny kandydat na urząd prezydenta Stanów Zjednoczonych, który przewodził Socjalistycznej Partii Ameryki powstałej w 1901 r. w wyniku połączenia Partii Socjaldemokratycznej i Socjalistycznej Partii Pracy. Podobnie jak Eugene V. Debs postrzegał on socjalizm jako system gospodarczy oparty na produkcji dla potrzeb społecznych

oraz społecznej własności środków produkcji, zamiast zysków i prywatnej własności. Współczesnym politykiem promującym idee socjalizmu demokratycznego w USA jest senator Bernard Sanders, związany z regionalną Postępową Partią Vermontu. To najdłużej urzędujący niezrzeszony kongresmen w historii USA, jawnie deklarujący swe poglądy socjalistyczne. Bez powodzenia kandydował w prawyborach prezydenckich Partii Demokratycznej (wybory w 2016), przegrywając z Hillary Clinton.

W Europie socjalizm demokratyczny stał się doktryną Włoskiej Partii Socjaldemokratycznej, która powstała w 1947 r. na skutek rozłamu we Włoskiej Partii Socjalistycznej. Jej przywódca Giuseppe Saragat został w 1964 r. wybrany na urząd prezydenta Włoch, który sprawował do grudnia 1971. Następnie uzyskał godność dożywotniego senatora.

Za ważnego przedstawiciela socjalizmu demokratycznego uważany był szwedzki premier Olof Palme, który wyrażał swoje przywiązanie do tego nurtu poprzez wrażliwość społeczną, dążenie do równości i sprawiedliwości, przy jednoczesnym odrzuceniu komunizmu. Był przeciwnikiem liberalizmu gospodarczego, prezentował radykalny antykolonializm i okazywał znaczącą pomoc dla krajów Trzeciego Świata. Realizując politykę wewnętrzną, kontynuował budowę tzw. państwa opiekuńczego, pomimo trudności związanych z finansowaniem wysokiego poziomu świadczeń socjalnych. Olof Palme został zastrzelony 28 lutego 1986 r. w centrum Sztokholmu, a żałobę po jego śmieci ogłoszono nie tylko w Szwecji, ale także w Nikaragui, Portugalii, Indiach i Argentynie.

To właśnie w tym ostatnim kraju działał polityk starający się również wcielać w życie zasady socjalizmu demokratycznego Salvador Allende. Już na studiach prezentował poglądy marksistowskie, ale zdecydowanie odrzucał komunizm rewolucyjny; realizował daleko idące reformy w duchu socjalizmu, lecz wyłącznie w drodze pokojowych, demokratycznych przemian. Wprawdzie odrzucał i negował ustrój kapitalistyczny, także ten neoliberalny, ale czynił to z poszanowaniem zasad demokracji parlamentarnej. W latach 1970–1973 pełnił urząd prezydenta Chile z ramienia lewicowej koalicji Jedność Ludowa (Unidad Popular). Po zwycięstwie w wyborach zaczął wprowadzać zapowiadane w trakcie kampanii wyborczej reformy – w duchu socjalizmu demokratycznego. Allende określał je jako *La vía chilena al socialismo* (chilijska droga do socjalizmu). Bardzo

szybko nastąpiły w Chile pozytywne zmiany, takie jak wzrost gospodarczy, ograniczenie bezrobocia i inflacji, wzrost redystrybucji dochodów i konsumpcji. Znacznie podwyższone zostały wynagrodzenia pracownicze, obniżono podatki i wprowadzono bezpłatną dystrybucję niektórych towarów tzw. pierwszej potrzeby. Objęto państwowym systemem ubezpieczeń inwalidów, sieroty, osoby starsze, zwiększono emerytury dla wdów. W ramach tzw. Narodowego Planu Mlecznego 50% chilijskich dzieci otrzymywało codziennie darmową porcję mleka. Podobne wsparcie dotyczyło matek nowo narodzonych dzieci. Podjęto decyzję o zamrożeniu cen oraz czynszów i przystąpiono do nacjonalizacji przemysłu miedziowego. Uruchomiono program reformy rolnej, dokonując parcelacji wielkich majątków ziemskich i przekazania ziemi bezrolnym chłopom. Poważne zamiany nastąpiły także w sferze edukacji – liczba studentów między 1970 a 1973 r. wzrosła o 89%, podobnie jak rekrutacja w szkołach. Po przeprowadzeniu nacjonalizacji zagranicznych i rodzimych koncernów rząd przejął część kontrolowanych przez te podmioty mediów. Allende stracił władzę na skutek zamachu stanu 11 września 1973 r. – tego dnia poniósł śmierć podczas ataku na pałac prezydencki w Santiago. W ten sposób zakończyła się największa w historii próba wprowadzania zmian opartych na zasadach socjalizmu demokratycznego.

Idee socjalizmu demokratycznego dosyć wcześnie pojawiły się także na pozostających pod zaborami terenach Polski. Przykładem była tu będąca we władzy monarchii austro-węgierskiej Galicja, znacznie opóźniona cywilizacyjnie, ale zachowująca relatywnie duże swobody polityczne i narodowe. To tutaj dynamicznie, pod hasłami socjalizmu demokratycznego, rozwijał się ruch socjalistyczny. Na początku lat 70. XIX w. na terenie Lwowa zdefiniowano filozofię socjalizmu demokratycznego, która stała się bazą programową polskiego ruchu socjalistycznego aż do lat 40. XX w.

Lwów na mapie rozwoju ruchu socjalistycznego nie znalazł się przypadkowo: było to efektem powstania tam dużego środowiska robotniczego, w którym dominowali drukarze, będący od lat 20. XIX w. stosunkowo najlepiej zorganizowaną i uświadomioną grupą. Ich aktywność spowodowała, iż 50 lat później środowisko robotników było już zrzeszone w różnych organizacjach samopomocowych. Tamtejszy ziemianin hrabia Leon Rzewuski był wydawcą ukazującego się we Lwowie czasopisma „Postęp"

i to na jego łamach wyraził pogląd, że socjalizm i demokracja są ze sobą ściśle powiązane. W swoim artykule stwierdził, iż „socjalizm jest demokracji praktyczne zastosowanie do życia ludowego […]. Związek oczywisty łączący koniecznie polityczną demokrację z demokracją ekonomiczną, liberalizm z socjalizmem". Jak podkreślał Mateusz Śliwa, był to czas, gdy ideologia socjalistyczna nie była jeszcze spójną i opisaną doktryną, stąd każdy radykalny pogląd był nazywany socjalistycznym. Katalizatorem ożywienia agitacji socjalistycznej we Lwowie był moment pojawienia się tam w 1870 r. historyka, socjologa i byłego zesłańca Bolesława Limanowskiego. Podczas swego wystąpienia w robotniczym stowarzyszeniu Gwiazda wygłosił on 2 odczyty *O kwestii robotniczej*, wyrażając pogląd, że podstawą dobrobytu wszystkich społeczeństw są 3 elementy: ziemia, kapitał i praca. Jak wyjaśniał, praca buduje i powoduje wzrost kapitału, sprawia, że człowiek podporządkowuje sobie siły natury i wykorzystuje je do swoich potrzeb. Wskazywał, że praca poza sferą czysto materialną spełnia także istotną rolę kulturotwórczą, będąc integratorem społeczeństwa i czyniąc człowieka obywatelem, a naród – ojczyzną. Według Limanowskiego praca miała być kreatorem nowego porządku społecznego i stać się najwyższą wartością. Eksponował on także rolę nauki, wiedzy i inteligencji w tworzeniu nowego ładu społecznego. Jego zdaniem rola oświaty miała zdecydowanie wzrosnąć, gdy praca stanie się główną dominantą w społeczeństwie. Edukacja i nauka posłużą wówczas rozwojowi kwalifikacji zawodowych, ale przede wszystkim transformacji społecznej świadomości oraz zmianie poglądów społeczeństwa na to, co w życiu jest najważniejsze. Swoje poglądy Limanowski przedstawiał nie tylko podczas odczytów i spotkań, ale także na łamach czasopism, takich jak ukazująca się w latach 1872–1874 „Czcionka" i wydawana w latach 1878–1892 „Praca". W tych periodykach swoje publikacje zamieszczali zarówno Polacy, jak i Ukraińcy.

Limanowski zdefiniował pojęcie socjalizmu demokratycznego, który jego zdaniem winien urzeczywistnić wolność klasy pracującej poprzez budowę nowej organizacji społeczeństwa, w oparciu o 3 zasady. Po pierwsze, praca musi stać się wiodącym czynnikiem, w ustroju społecznym. Po drugie, życie i praca każdego człowieka należą do społeczeństwa. Po trzecie, środki produkcji muszą stanowić wyłączną własność ludzi pracujących.

Postrzegał socjalizm jako system teoretyczno-praktyczny wynikający z głębokiego poczucia sprawiedliwości, egalitarny i żądający równości dla wszystkich, odrzucający wszelkie formy wyzysku. Jego zdaniem tylko ten ustrój uznawałby pracę jako wartość nadrzędną i sprawiał, że ludzie ją wykonujący byliby naprawdę wolni. Twierdził, że tak rozumiany socjalizm jest ważnym elementem świadomości społecznej, będąc jednocześnie naturalną fazą rozwoju ludzkości. W polskiej kulturze idee socjalistyczne zostały wzbogacone o dążenia patriotyczne związane z potrzebą odzyskania utraconej niepodległości. Limanowski wbrew krytykom, którzy uważali, iż socjalizm jest tylko przejściową chorobą wieku i swoistą patologią społeczną, dowodził, że jest on naturalną kontynuację tradycji demokratycznej i stanowi etap konieczny w rozwoju polskiego społeczeństwa. To miał być warunek *sine qua non* dopełnienia polskiego procesu dziejów w oparciu o zasady demokracji. Socjalizm miał więc zmierzać do urzeczywistnienia demokracji, która była możliwa do spełnienia tylko w niepodległym, suwerennym państwie polskim, rządzonym przez ludzi pracy. To oni, w ramach ustroju demokratycznego, mogliby zapewnić przestrzeganie zasady obywatelskiego równouprawnienia i sprawiedliwej organizacji pracy, a w konsekwencji – utrwalić zgodność interesu jednostki z interesem społecznym. Podstawowym warunkiem takiego społeczeństwa jest przekształcenie państwa w zbiorowe dzieło ludu, który sprawując władzę, sprawiłby, że cała twórczość ludzka miałaby uspołeczniony charakter.

Socjaliści lwowscy wskazywali, że demokracja to rodzaj społecznej solidarności. Podkreślali, że ich determinacja do oparcia się na ustroju demokratycznym wynika z interesu ludzi pracy, gdyż tylko w tym ustroju mogą zostać zrealizowane takie wartości podstawowe, jak sprawiedliwość, wolność, samostanowienie jednostki czy godność człowieka. Konkludując, przyjmowali, iż wyłącznie w warunkach pełnego zaangażowania społeczeństwa i na zasadach demokracji mogą zostać spełnione idee i cele socjalizmu, takie jak wyzwolenie człowieka i całej ludzkości. Dla nich socjalizm oznaczał automatycznie demokratyzm. W wydanym w 1880 r. dokumencie *Program socjalistów polskich i ruskich Wschodniej Galicji* przedstawione zostały zasady socjalizmu oraz zadania galicyjskiego ruchu socjalistycznego. Konieczność likwidacji kapitalizmu i stworzenia w jego miejsce ustroju sprawiedliwości społecznej miała swe źródło

w zachodnioeuropejskiej koncepcji socjalizmu, który bazował na pracach Karola Marksa i Ferdynanda Lassalle'a. W programie wskazywano na różne formy realizacji socjalizmu, podkreślając, iż „walka pracy z kapitałem toczyć się musi na gruncie narodowym". Twórcy programu akcentowali demokratyczną wizję nowego ustroju społecznego, eksponując rolę samorządów lokalnych, tworzących wolną federację opierającą się o solidarność interesów. Członkowie samorządów mieli być wybierani w głosowaniu powszechnym przez wszystkich obywateli. To autorzy tego programu sformułowali przesłanie, że warunkiem prawdziwej wolności jest solidarność. Nie sposób nie dostrzec w dziejach Polski znaczenia idei socjalizmu demokratycznego postulowanych przez socjalistów lwowskich.

Poza Limanowskim i grupą socjalistów ze Lwowa ważnym reprezentantem idei socjalizmu demokratycznego był Adam Ciołkosz. Prowadził on badania wskazujące w sposób precyzyjny różnice ideologiczne między socjalizmem demokratycznym a komunizmem. Wskazywał, że są to 2 całkowicie odrębne nurty ruchu robotniczego. Ciołkosz od najmłodszych lat wykazywał zainteresowanie kwestiami społecznymi, najpierw tworząc *skauting* w rodzinnym Tarnowie, a następnie jako żołnierz-ochotnik walcząc w I wojnie światowej o niepodległość Polski. Swoje poglądy socjalistyczne formułował i propagował już podczas studiów na Uniwersytecie Jagiellońskim, działając w ruchu młodzieżowym. Będąc w okresie międzywojennym członkiem Polskiej Partii Socjalistycznej (PPS), został wybrany posłem do sejmu RP. Ze względu na głoszone poglądy i ostrą krytykę sanacyjnych rządów został skazany w procesie brzeskim. Na początku II wojny światowej uciekł z kraju i zamieszkał w Wielkiej Brytanii; od początku swego pobytu w Londynie krytykował ustrój komunistyczny jako zbrodniczy system niszczący prawdziwy, demokratyczny socjalizm. Jako ofiara Armii Czerwonej podczas wojny polsko-bolszewickiej w 1920 r. w praktyce poznał, czym jest komunistyczny reżim.

Negatywny i krytyczny stosunek Ciołkosza wobec komunizmu był wynikiem nie tylko jego patriotycznej postawy, ale też skrystalizowanych poglądów politycznych i ideowych. W swoich publikacjach podnosił, że komunizm w Związku Radzieckim odwrócił się od naukowego marksizmu, negując takie wartości jak wolności obywatelskie i swobody demokratyczne. Według Ciołkosza w latach 30. XX w. komunizm wbrew

leninowskiej tezie nie stanowił radykalnej wersji socjalizmu, lecz był osobnym nurtem totalitarnym, który jedynie wykorzystywał retorykę i symbole socjalistyczne. Komuniści związani ideologicznie ze Związkiem Sowieckim chętnie szermowali takimi wartościami, jak socjalizm, demokracja, wolność, sprawiedliwość czy prawa obywatelskie. Były to jedynie propagandowe hasła, niemające żadnego pokrycia w rzeczywistości.

Ciołkosz w swojej krytyce komunizmu twierdził, że w historii nie istnieją zjawiska niezmienne i ponadczasowe, a preferowane przez komunistów myślenie dialektyczne, odwołujące się do marksizmu, podporządkowane zostało uprawianiu propagandy i tworzeniu tzw. nowomowy. Podkreślał, że pomimo upływu 50 lat od zakończenia rewolucji w Rosji w dalszym ciągu działa tam system totalitarny, który spowodował śmierć 40 mln ludzi. Ciołkosz wskazywał, iż warunkiem pełnego, twórczego rozwoju każdego człowieka są wolność i demokracja; jeśli zostaną ograniczone, skutkuje to poważnymi społecznymi zakłóceniami. Jego zdaniem istnieje naturalna ewolucja, która łączy tradycję marksistowską z poglądami socjalistów demokratycznych. Wspólne jest dla nich dążenie do wyrwania jednostki z niewoli stworzonej przez niesprawiedliwe stosunki społeczno-ekonomiczne oraz działanie państwa w interesie większości, za jej przyzwoleniem.

Ciołkosz nie wierzył w istnienie ustrojów pośrednich pomiędzy demokracją a systemami totalitarnym czy autorytarnym. Wskazywał na deficyt wolności i demokracji w sanacyjnej Polsce, uznając, że uzdrowienie tego systemu jest niemożliwe; twierdził, że trzeba go zlikwidować i wprowadzić realną demokrację. Jego zdaniem Józef Piłsudski dążył do całkowitej likwidacji partii i stronnictw politycznych. Obawiał się, iż zwiększenie kompetencji prezydenta RP spowoduje, że będzie on poza kontrolą innych organów władzy, co oznacza negację istoty demokracji parlamentarnej. Podkreślał, że demokracja to nie tylko rządy większości, ale też szanowanie praw mniejszości i każdego człowieka. Był orędownikiem równouprawnienia, prowadzenia szkół z ojczystym językiem wykładowym, finansowania przez państwo potrzeb kulturalnych mniejszości oraz uwzględniania praw językowych mniejszości narodowych zarówno w administracji, jak i w sądownictwie. Na emigracji krytykował politykę gen. Sikorskiego, piętnując ograniczenia demokracji w życiu publicznym wychodźstwa

i brak klarownych oświadczeń rządu co do demokratycznego charakteru przyszłego państwa.

Po wojnie natychmiast obnażył prawdziwe oblicze partii socjalistycznej stworzonej w Polsce przez nowy reżim – pisał, iż zmierza ona do policyjnego totalitaryzmu będącego całkowitym zaprzeczeniem polskiego socjalizmu, opartego na ponad półwiecznej tradycji demokratycznej i niepodległościowej. Propagując idee socjalizmu demokratycznego, wskazywał, że ustrój ZSRR i innych państw bloku radzieckiego nie miał nic wspólnego z socjalizmem – określał go mianem brutalnego totalitaryzmu. Radziecki komunizm był, według niego, odnowionym imperializmem rosyjskim, noszącym takie same cechy jak nazizm. Pisał, iż komunizm gwałci prawa człowieka, narusza ludzką godność, czyniąc z obywateli niewolników. Takiemu komunizmowi przeciwstawiał idee socjalizmu demokratycznego; wskazywał, że socjalistom obcy był kult jednostki, a będąc za internacjonalizmem, manifestowali, że ich ojczyzną jest Polska, a jedynym suwerenem – polskie społeczeństwo. Wprawdzie przeprowadzane w Polsce po wojnie zmiany, takie jak reforma rolna, nacjonalizacja wielkiego przemysłu czy powszechna i bezpłatna edukacja, były zbieżne z programem głoszonym jeszcze przed wojną przez socjalistów, ale komuniści realizując je, jednocześnie likwidowali demokrację i swobody obywatelskie, a w to miejsce wprowadzali dyktaturę monopartii. Ciołkosz jako socjalista uważał, że Polsce winna zostać przywrócona pełna wolność i ustrój demokratyczny, ale w sposób bezkrwawy poprzez przeprowadzenie wolnych wyborów do zgromadzeń konstytucyjnych.

Ciołkosz był jednym ze współautorów deklaracji noszącej tytuł *Cele i zadania socjalizmu demokratycznego*, która została przyjęta w 1951 r. we Frankfurcie nad Menem przez I kongres odrodzonej Międzynarodówki Socjalistycznej. Obradujący uznali komunizm za narzędzie nowego imperializmu, zaś socjalizm demokratyczny został zdefiniowany jako demokracja polityczna, gospodarcza, społeczna i międzynarodowa – tak pojmowany nie wskazywał na konieczność wywodzenia przekonań jego zwolenników z jednej doktryny politycznej. Istotne było to, że zmierzają oni do jednego celu: ustroju sprawiedliwości społecznej, dobrobytu i pokoju.

Doktryna socjalizmu demokratycznego była krytyką kapitalizmu; wskazywano, iż powoduje on niesprawiedliwy podział dochodu społecznego i generuje koncentrację władzy gospodarczej. Zalecano uspołecznienie środków produkcji, ale tylko w kluczowych dla gospodarki państwa przedsiębiorstwach. Za szczególnie istotną kwestię uznano sprawiedliwy podział dochodu narodowego i zapewnienie właściwych stosunków w miejscu pracy.

Deklaracja definiuje socjalizm demokratyczny, eksponując 4 charakteryzujące go obszary. Pierwszy z nich to demokracja polityczna polegająca na uznawaniu rządów politycznych opartych na powszechnym, równym i tajnym głosowaniu, pluralizmie partyjnym, wolności słowa, mediów i zgromadzeń oraz prawie do opozycji. Drugi odnosi się do demokracji gospodarczej, w której zapewniona jest aktywność państwa jako moderatora interesów społecznych, planowanie gospodarcze w interesie większości oraz kontrola własności prywatnej, ale bez stosowania nacjonalizacji przymusowej. Dopuszczono tu możliwość współistnienia różnych form własności. Trzeci obszar dotyczy demokracji społecznej mającej zagwarantować prawa socjalne, takie jak prawo do pracy, opieki zdrowotnej, edukacji, zabezpieczenia emerytalnego. Obejmuje także zwalczanie wszelkich przejawów nierówności ze względu na płeć, rasę czy pochodzenie. Czwarta sfera reguluje demokrację międzynarodową, która winna zapewnić dążenie do światowego pokoju, eliminację każdego rodzaju wyzysku oraz międzynarodową solidarność z narodami i klasami pracującymi.

Andrzej Czop

D.F. Busky, *Democratic Socialism: A Global Survey*, Praeger, London 2000; A. Ciołkosz, *Karol Marks a powstanie styczniowe*, „Teki Historyczne" 1963; A. Ciołkosz, *Róża Luksemburg a rewolucja rosyjska*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2022; A. Friszke, *Myśl polityczna Adama Ciołkosza*, [w:] *Myśl polityczna na wygnaniu. Publicyści i politycy polskiej emigracji powojennej*, Instytut Studiów Politycznych Polskiej Akademii Nauk, Warszawa 1995; P.R. Gregory, R. Stuart, *Comparing Economic Systems in the Twenty-First Century*, Houghton Mifflin, Boston 2004; B. Limanowski, *O kwestii robotniczej. Rzecz ułożona podług dwóch odczytów w „Gwieździe" z dnia 19 marca i 2 kwietnia 1871 r.*, Drukarnia J. Dobrzańskiego

i K. Gromana, Lwów 1871; B. Limanowski, *Socjalizm jako konieczny objaw dziejowego rozwoju*, Związkowa Drukarnia we Lwowie, Lwów 1878; R. Miliband, *Socialism for a Sceptical Age*, Verso, London–New York 1994; W. Najdus, *Polska Partia Socjalno-Demokratyczna Galicji i Śląska 1890–1918*, Wydawnictwo Naukowe PWN, Warszawa 1983; L.B. Paszkiewicz, *Karol Marks i marksizm w refleksjach Adama Ciołkosza emigracyjnego socjalisty demokratycznego*, „Wrocławskie Studia Politologiczne" 2018, nr 25; R. Pipes, *Rosja bolszewików*, Bellona, Warszawa 2022; K. Popiel, *Choroba wieku. Wybór pism*, Księgarnia Akademicka, Kraków 2001; D. Reisman, *Democratic Socialism in Britain: Classic Texts in Economic and Political Thought, 1825–1952*, Pickering & Chatto Ltd., London 1996; M. Śliwa, *Lwów i początki idei socjalizmu demokratycznego na ziemiach polskich*, [w:] *Lwów: miasto, społeczeństwo, kultura: studia z dziejów Lwowa*, t. 2, H.W. Żaliński, K. Karolczak (red.), Wydawnictwo Naukowe Wyższej Szkoły Pedagogicznej, Kraków 1998; J. Tomlinson, *Democratic Socialism and Economic Policy: The Attlee Years, 1945–1951*, Cambridge University Press, Cambridge 1997; F. Tych, *Polskie programy socjalistyczne 1878–1918*, Książka i Wiedza, Warszawa 1975.

SIŁY ZBROJNE REPUBLIKI CHIŃSKIEJ. Mówiąc o siłach zbrojnych Republiki Chińskiej, trzeba podkreślić, iż nie chodzi tu o Chińską Armię Ludowo-Wyzwoleńczą z Chin kontynentalnych, tylko o Narodowe Siły Zbrojne z Republiki Chińskiej, znanej bardziej pod nazwą Tajwan. Sytuacja tych 2 podmiotów przypomina podział Półwyspu Koreańskiego, jednak oba państwa są z reguły uznawane przez większość krajów na arenie międzynarodowej. Kwestia Chin i Tajwanu jest bardziej skomplikowana. Po zakończeniu II wojny światowej, kiedy Japończycy opuścili już Chiny doszło do wojny domowej (1945–1949) pomiędzy 2 największymi partiami w Chinach, czyli Komunistyczną Partią Chin a Kuomintangiem (Partia Narodowa), w wyniku czego nastąpił podział kraju. Komunistom udało się wygrać konflikt pomimo początkowej przewagi nacjonalistów. Partia Narodowa mogła liczyć na wsparcie ze strony USA, jednak nacjonaliści z Czang Kaj-szekiem na czele słabo sobie radzili w zwalczaniu rosnącej korupcji w szeregach własnej partii oraz ignorowali tereny wiejskie, na których to komuniści zdobywali coraz większe poparcie. Efektem ich nieudolnej polityki była całkowita utrata Chin kontynentalnych, w których 1 października 1949 r. Mao Zedong proklamował Chińską Republikę

Ludową. Nacjonaliści musieli się ewakuować na Tajwan, gdzie kontynuowali istniejącą już od 1912 r. Republikę Chińską.

Amerykanie początkowo zakładali, że sprawa Tajwanu jest przegrana; uważali, że wkrótce i tak odbiją ją komuniści, a zniechęceni nieudolną polityką Czang Kaj-szeka również nie wyrażali dużej aprobaty wobec dalszego wspierania nacjonalistów. Wszystko się jednak zmieniło za sprawą wojny koreańskiej, która to przekonała Amerykanów do dalszej współpracy z Tajwanem dla zabezpieczenia swojej strefy wpływów w regionie Azji Wschodniej. Tajwan odegrał wtedy kluczową rolę jako pośrednik do dostarczania uzbrojenia Korei Południowej. Amerykański generał Douglas MacArthur nazwał w 1950 r. Tajwan „niezatapialnym lotniskowcem", co również dzisiaj znajduje swoje odbicie w strategii amerykańskiej. Do lat 70. XX w. ChRL i Tajwan trwały jako 2 osobne podmioty. ChRL była uznawana głównie przez blok wschodni, a Tajwan – przez zachodni. Jednak w 1971 r. rząd w Tajpej zaczął odczuwać pierwsze gwałtowne zmiany w światowej polityce, kiedy to Tajwan utracił swoje miejsce w Radzie Bezpieczeństwa ONZ na rzecz ChRL. Kolejnym ważnym wydarzeniem była wizyta amerykańskiego prezydenta Richarda Nixona w ChRL w 1972 r. oraz podpisanie przez niego komunikatu szanghajskiego, którego treść zawierała zapiski m.in. o istnieniu jednych Chin, których to częścią jest Tajwan. Najdotkliwszym jednak ciosem było oficjalne nawiązanie relacji przez Amerykanów z Chinami kontynentalnymi w 1979 r. – tym samym USA oficjalnie zerwało relacje z Tajwanem, co uczyniły również inne państwa, a sam Tajwan dzisiaj jest uznawany przez pojedyncze podmioty.

Amerykanie zastosowali taką strategię głównie w celu osłabienia ZSRR, jednak tym samym doprowadzili do niejednoznacznej polityki wobec Tajwanu. Pomimo iż dalej oficjalnie go nie uznają, pozostają jego głównym sojusznikiem. Dzisiejsza obrona Tajwanu w dużej mierze zależy od tego, jakie wsparcie otrzymuje wyspa od USA oraz w jaki sposób rozwija ona swoją armię. Obrona Tajwanu stanowi dzisiaj jedno z największych wyzwań geopolitycznych, a sama Cieśnina Tajwańska jest postrzegana jako potencjalne miejsce, w którym rozpocznie się konflikt zbrojny pomiędzy Chinami a Stanami Zjednoczonymi, a nawet III wojna światowa.

Siły Zbrojne Republiki Chińskiej (chiń. 中華民國國軍; pinyin: Zhōnghuá Mínguó Guójūn; dosł. Narodowe Siły Zbrojne Republiki Chińskiej)

składają się z armii, marynarki wojennej (w tym korpusu piechoty morskiej), sił powietrznych i żandarmerii wojskowej. Wojsko działa pod cywilną kontrolą Ministerstwa Obrony Narodowej, organu na szczeblu gabinetowym nadzorowanego przez Yuan (Parlament) Tajwański. Do końca lat 70. minionego stulecia głównym zadaniem Sił Zbrojnych Republiki Chińskiej było przygotowanie kontrofensywy mającej na celu odbicie Chin kontynentalnych z rąk komunistów, czego przykładem są takie inicjatywy jak projekt Chwała Narodowa. W związku ze zmianami strategicznymi i ewolucją sytuacji politycznej na Tajwanie uwaga sił zbrojnych skupiła się na obronie samego Tajwanu przed potencjalną inwazją ze strony Armii Ludowo-Wyzwoleńczej (ChAL-W) Chińskiej Republiki Ludowej, która w dalszym ciągu jest postrzegana jako główne zagrożenie dla niezawisłego bytu Republiki Chińskiej. Siły Zbrojne Republiki Chińskiej utrzymują obecnie liczebność około 150 tys. osób czynnych, z możliwością zmobilizowania do 1,67 mln rezerwistów w razie stanu wyjątkowego lub wojny pełnoskalowej. Dostępna jest znaczna liczba byłych poborowych, ponieważ wszyscy zdolni do służby wojskowej mężczyźni będący obywatelami Republiki Chińskiej są zobowiązani do odbycia co najmniej rocznej obowiązkowej służby wojskowej po ukończeniu 18 roku życia. Najwyższym rangą wojskowym w Siłach Zbrojnych Tajwanu jest szef sztabu generalnego; obecnie funkcję tę pełni admirał Mei Chia-shu, który jest odpowiedzialny za gotowość bojową sił zbrojnych przed cywilną strukturą dowodzenia podporządkowaną ministrowi obrony narodowej i prezydentowi Republiki Chińskiej.

Siły lądowe Tajwanu liczą około 95 tys. żołnierzy; są odpowiedzialne za obronę na lądzie głównej wyspy (Tajwanu) oraz kilku mniejszych znajdujących się pod kontrolą rządu w Tajpej. W 2015 r. siły lądowe zostały zorganizowane w 3 korpusy armijne, 5 brygad piechoty, 3 zmechanizowane brygady piechoty, 4 brygady pancerne, 3 brygady lotnicze i 5 brygad artylerii, z łącznie 1100 czołgami i 1600 działami artyleryjskimi. Liczba brygad piechoty została stopniowo zmniejszona z 25 w 2005 r. do 5 w 2016 r., a liczba brygad pancernych – z 5 do 4 w 2010 r., podczas gdy brygady artylerii zostały zwiększone, a brygady lotnictwa armii – utworzone w 2015 r. Sprzęt obejmujący m.in. ponad tysiąc czołgów i 2 tys. transporterów opancerzonych jest pochodzenia amerykańskiego, południowokoreańskiego

oraz rodzimej produkcji. Na czele wojsk lądowych Tajwanu stoi generał Lu Kun-hsiu.

Położenie geopolityczne Tajwanu sprawia, że marynarka wojenna odgrywa szczególną rolę wśród określonych rodzajów sił zbrojnych Republiki Chińskiej. Oficjalna nazwa to Marynarka Wojenna Republiki Chińskiej (chin. 中華民國海軍; pinyin: Zhōnghuá Mínguó Hǎijūn). Ten segment na tle innych rodzajów wojsk tajwańskich jest stosunkowo silny (i w miarę nowoczesny, zwłaszcza gdy idzie o małe jednostki). Mówiąc wprost – wobec zdecydowanej przewagi marynarki wojennej Chin Ludowych siły morskie Tajwanu nie mają szans na powstrzymanie inwazji z kontynentu bez wsparcia z zewnątrz w postaci US Navy lub Japońskich Morskich Sił Samoobrony. Podstawę floty tajwańskiej tworzą 4 niszczyciele, 21 fregat, 13 korwet, 30 małych okrętów rakietowych oraz 5 okrętów podwodnych. W budowie znajduje się kilka kolejnych okrętów. Obiecująco wygląda program rozbudowy sił podwodnych w oparciu o własny przemysł stoczniowy – jest to kluczowe, gdyż obrona floty Chin Ludowych pozostawia, wedle amerykańskich ekspertów, dużo do życzenia. Należy jednak pamiętać, że spora część dużych jednostek – niszczyciele amerykańskiego typu Issac Kidd z końca lat 70. minionego stulecia oraz 8 fregat budowanych na licencji amerykańskiej u progu lat 90. XX stulecia typu Oliver Hazard Perry – to jednostki już nieco przestarzałe. Jednak oprócz udanych przedsięwzięć nie brak posunięć chybionych, jak np. duży okręt desantowy Yu Shan, oddany do służby 2 lata temu, mogący pełnić funkcje helikopterowca, którego przydatność do obrony wyspy jest jednak raczej dyskusyjna. Marynarka Wojenna Tajwanu liczy prawie 40 tys. personelu (z tego 10 tys. to żołnierze piechoty morskiej), w sporej części zawodowego, o sporych kompetencjach fachowych. Dowódcą floty jest admirał Chiang Cheng-kuo.

Siły Powietrzne Republiki Chińskiej (chin. 中華民國空軍; pinyin: Zhōnghuá Mínguó Kōngjūn) odgrywają bardzo istotną rolę wśród poszczególnych rodzajów sił zbrojnych Tajwanu. Ich podstawowym zadaniem jest obrona przestrzeni powietrznej nad i wokół wyspy podlegającej jurysdykcji terytorialnej rządu Republiki Chińskiej. Priorytety tajwańskich sił powietrznych obejmują rozwój sieci rozpoznania i nadzoru dalekiego zasięgu, integrację systemów C4ISTAR w celu zwiększenia skuteczności

walki, zakup broni przeciwlotniczej, myśliwców nowej generacji oraz wzmocnienie lotnisk i innych obiektów w celu zapewnienia odporności na niespodziewany atak. Personel tego komponentu sił zbrojnych Tajwanu liczy 35 tys. żołnierzy, w większości kadry zawodowej o dużym stopniu profesjonalizacji. Siły powietrzne Tajwanu liczą prawie 600 samolotów – ich podstawę tworzą amerykańskie F-16 oraz francuskie Mirage 2000. Sztab generalny Sił Powietrznych Republiki Chińskiej prowadzi intensywne studia nad wojną w przestrzeni powietrznej między Ukrainą a Rosją. W trybie pilnym rozbudowywana jest obrona antyrakietowa oraz antydronowa. Obecnie dowódcą sił powietrznych Tajwanu jest generał Cheng Jung-feng.

Siły zbrojne Republiki Tajwańskiej tworzą dość skuteczne ramię obrony Republiki Chińskiej. Czynnikiem dodatkowo sprzyjającym obronie wyspy są klifowe brzegi (płaskie plaże nadające się do dokonania desantu są nieliczne). Ponadto akweny okalające Tajwan są burzliwe, a dni bez sztormowej pogody – rzadkie; trudno przewidzieć z całą pewnością, kiedy nastąpią. Pomimo tych sprzyjających okoliczności w sytuacji pełnoskalowej inwazji Chin Ludowych na Tajwan armia tajwańska nie dałaby rady sama odeprzeć ataku; niezbędna byłaby zewnętrzna pomoc amerykańskiej VII floty i japońskie wsparcie.

Karol Kochnowski

Axiois, Pressure grows for Taiwan to boost its defense force, https://www.axios.com/2022/06/28/taiwan-military-defense-weapons-china-invasion-threat (dostęp 28.01.2026); K. Brown, *Tajwan Krótka historia małej wyspy i jej wpływ na losy świata*, Copernicus Center Press Sp. z o.o., Kraków 2025; *DW, Taiwan's army 'ill-prepared' for attack*, https://www.dw.com/en/taiwans-army-ill-prepared-for-potential-chinese-attack/a-57102659 (dostęp 29.01.2026); *Does Taiwan's Military Stand a Chance Against China? Few Think So*, https://www.wsj.com/world/asia/taiwan-military-readiness-china-threat-us-defense-11635174187 (dostęp 29.01.2026); M. Mazza, *Taiwan: The "ROC" In a Hard Place*, [w:] *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners*, G.J. Schmitt (ed.), Strategic Studies Institute, U.S. Army War College, West Point 2020; K. Ronneberg, *Tajwan – wyspa w oku cyklonu*, Wydawnictwo Szczeliny, Kraków 2025; T. Yoshiara, J.R. Holmes, *Der rote Stern über dem Pazifik: Chinas Aufstieg*

als Seemacht – und wie antworten die USA, Mittler in Maximilian Verlag GmbH & Co. KG, Hamburg 2011.

SŁUŻBA KONTRWYWIADU WOJSKOWEGO RP (dalej: SKW) jest jedną z polskich służb specjalnych powołaną do ochrony bezpieczeństwa Sił Zbrojnych RP oraz przeciwdziałania zagrożeniom związanym z działalnością wywiadowczą, sabotażową, terrorystyczną oraz innymi działaniami wymierzonymi w obronność i interesy militarne Polski. SKW działa zarówno na terenie kraju, jak i poza jego granicami, szczególnie w miejscach, gdzie przebywają polskie kontyngenty wojskowe. Służba została utworzona 1 października 2006 r. na mocy Ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego. Zastąpiła rozwiązane Wojskowe Służby Informacyjne (WSI), które były krytykowane za nadużycia i brak reform po 1989 r. Działalność SKW jest nadzorowana przez ministra obrony narodowej, a jej operacje są realizowane zgodnie z polskim prawem, w szczególności ustawą o służbach specjalnych. Służba Kontrwywiadu Wojskowego składa się z centralnej jednostki kierowniczej oraz terenowych jednostek operacyjnych, które współpracują z wojskowymi i innymi instytucjami związanymi z obronnością; ma uprawnienia do prowadzenia operacji wywiadowczych, analitycznych oraz kontrwywiadowczych. Do głównych zadań służby należy ochrona informacji niejawnych i przeciwdziałanie szpiegostwu – identyfikuje i neutralizuje zagrożenia związane z działalnością obcych służb wywiadowczych, które próbują zdobywać informacje o polskich siłach zbrojnych, technologii wojskowej czy planach operacyjnych. Przeprowadza kontrolę i weryfikację osób, które mają dostęp do tajemnic państwowych i wojskowych. Aby przystąpić do Służby Kontrwywiadu Wojskowego (SKW) Rzeczypospolitej Polskiej, kandydat musi spełniać określone wymagania formalne i osobowościowe oraz przejść wieloetapowy proces rekrutacyjny. Przede wszystkim kandydaci powinni posiadać polskie obywatelstwo, być pełnoletni, cieszyć się pełnią praw publicznych i niekaralnością. Kluczowe jest także ukończenie studiów wyższych, choć w niektórych przypadkach preferowane są konkretne specjalizacje, takie jak bezpieczeństwo narodowe, prawo, stosunki międzynarodowe, informatyka czy lingwistyka. Jednym z ważniejszych etapów jest uzyskanie poświadczenia bezpieczeństwa, co

wymaga przejścia szczegółowego postępowania sprawdzającego, które weryfikuje wiarygodność kandydata, jego przeszłość, powiązania oraz odporność na czynniki mogące narazić go na szantaż czy manipulacje. Istotnym wymogiem jest także bardzo dobra kondycja psychiczna i fizyczna, ponieważ praca w SKW bywa wymagająca, zarówno pod względem intelektualnym, jak i emocjonalnym. Kandydaci powinni wykazywać się zdolnościami analitycznymi, odpornością na stres oraz umiejętnością zachowania tajemnicy. Rekrutacja obejmuje wiele testów psychologicznych, sprawdzających osobowość i inteligencję, a także rozmowy kwalifikacyjne, podczas których oceniane są motywacje, lojalność wobec państwa i zdolności interpersonalne. W zależności od stanowiska mogą być wymagane dodatkowe umiejętności, takie jak znajomość języków obcych, obsługa nowoczesnych technologii czy doświadczenie w pracy wywiadowczej lub wojskowej. Praca w służbie opiera się na zasadach lojalności, dyskrecji i pełnego podporządkowania na rzecz bezpieczeństwa państwa. Kandydaci muszą być świadomi, że służba wymaga gotowości do pracy w trudnych warunkach, również poza granicami kraju, oraz zdolności do działania w sytuacjach kryzysowych. Po przyjęciu do SKW nowi członkowie przechodzą szkolenia przygotowujące ich do specyfiki zadań, które mogą obejmować zarówno działania kontrwywiadowcze, jak i zabezpieczanie operacji wojskowych oraz ochronę informacji niejawnych. Rekrutacja wygląda podobnie jak w przypadku innych służb, ale posiada dodatkowe specjalne wymagania. Służba analizuje lojalność, powiązania międzynarodowe i podatność na werbunek. Zabezpiecza misje wojskowe w krajach objętych konfliktami zbrojnymi, takich jak Afganistan czy Irak. Służba Kontrwywiadu Wojskowego odegrała kluczową rolę w ochronie polskich kontyngentów wojskowych uczestniczących w misjach NATO w Afganistanie, realizowanych w ramach Międzynarodowych Sił Wsparcia Bezpieczeństwa, oraz późniejszej Resolute Support, które wymagały szczególnego zabezpieczenia przed zagrożeniami związanymi z terroryzmem, działalnością talibów, a także potencjalną infiltracją przez obce wywiady. Do zadań kontrwywiadu należała m.in. ochrona kontrwywiadowcza polskiego kontyngentu wojskowego. Monitorowała ona zagrożenia, w tym próby infiltracji polskich baz przez talibów oraz grupy terrorystyczne; prowadziła działania mające na celu weryfikację lokalnych

współpracowników, tłumaczy oraz dostawców, którzy mieli dostęp do baz wojskowych i infrastruktury polskiego kontyngentu. Zapewnienie bezpieczeństwa informacji było jednym z priorytetów SKW; obejmowało to ochronę systemów komunikacyjnych, zapobieganie wyciekom danych oraz przeciwdziałanie próbom pozyskania informacji przez talibów. Służba współpracowała z polskimi dowódcami na miejscu, dostarczając analizy wywiadowcze i ostrzegając przed potencjalnymi zagrożeniami – jednym z najpoważniejszych dla polskich żołnierzy były ataki z wykorzystaniem improwizowanych ładunków wybuchowych. Prowadziła także wspólne operacje mające na celu eliminację kluczowych zagrożeń, takich jak liderzy grup terrorystycznych odpowiedzialni za ataki na siły koalicyjne. Monitorowała potencjalne przypadki nielojalności lub zdrady wśród członków polskiego kontyngentu oraz współpracowników, aby zapobiec sabotażowi lub wyciekom informacji. Prowadziła dogłębne analizy i weryfikację osób zatrudnianych jako tłumacze, przewoźnicy i dostawcy usług dla polskich baz. W kilku przypadkach zidentyfikowano współpracowników, którzy byli powiązani z talibami lub lokalnymi grupami terrorystycznymi, co zapobiegło poważnym incydentom. Wykryto próby podsłuchu i zakłócania komunikacji wojskowej przez grupy wrogie siłom koalicyjnym, dzięki czemu wprowadzono dodatkowe zabezpieczenia w systemach łączności, co zwiększyło bezpieczeństwo operacyjne polskiego kontyngentu. Służba Kontrwywiadu Wojskowego w Afganistanie pełniła niezwykle istotną rolę w ochronie polskich sił zbrojnych i wspieraniu ich działań w trudnym, niestabilnym środowisku konfliktu zbrojnego. Dzięki swojej elastyczności, współpracy międzynarodowej oraz zaawansowanym metodom operacyjnym skutecznie przeciwdziałała zagrożeniom, które mogły wpłynąć na bezpieczeństwo żołnierzy i realizację misji NATO. Służba Kontrwywiadu Wojskowego RP odegrała istotną rolę w zapewnieniu bezpieczeństwa polskim żołnierzom podczas misji stabilizacyjnych w Afganistanie i Iraku. Jej działania obejmowały ochronę kontrwywiadowczą kontyngentu wojskowego, w tym identyfikację i neutralizację zagrożeń związanych z działalnością grup terrorystycznych oraz przeciwdziałanie infiltracji baz przez lokalne siatki przestępcze. Służba zajmowała się weryfikacją współpracowników lokalnych, takich jak tłumacze czy dostawcy, aby zapobiec sytuacjom, w których osoby te mogłyby działać na szkodę polskich sił.

Ważnym elementem była także ochrona informacji niejawnych i systemów komunikacyjnych, co ograniczało możliwość wycieku danych o operacjach wojskowych. Ponadto SKW współpracowała z innymi służbami wywiadowczymi państw koalicyjnych, co pozwalało na wymianę informacji i skuteczniejsze przeciwdziałanie zagrożeniom, takim jak improwizowane ładunki wybuchowe (IED) czy ataki na polskie konwoje. Dzięki swojej działalności kontrwywiad znacząco zwiększył bezpieczeństwo polskich żołnierzy i wspierał realizację celów misji w wymagającym środowisku operacyjnym Iraku.

Służba współpracuje z innymi jednostkami wywiadowczymi NATO, UE i państw sojuszniczych, wymieniając informacje i koordynując działania w ramach wspólnych operacji obronnych. Przeciwdziała atakom terrorystycznym wymierzonym w obiekty wojskowe oraz zajmuje się ochroną infrastruktury krytycznej przed cyberatakami. Akcje i działania Służby Kontrwywiadu Wojskowego:

1. Zwalczanie infiltracji wywiadowczej: w 2018 r. SKW zidentyfikowała przypadki działań obcych wywiadów, które próbowały zdobyć informacje o modernizacji polskiej armii, w tym zakupie systemu obrony powietrznej Patriot. Dzięki skutecznej pracy operacyjnej udało się ograniczyć wyciek danych.
2. Zabezpieczenie misji wojskowych: służba odgrywała kluczową rolę w ochronie polskich kontyngentów w Afganistanie i Iraku.
3. Walka z cyberprzestępczością: uczestniczyła w neutralizacji ataków cybernetycznych wymierzonych w polskie systemy obronne. Wspólnie z innymi służbami udało się wykryć grupy hakerskie związane z obcymi państwami, które próbowały uzyskać dostęp do systemów NATO.
4. Weryfikacja kandydatów do służby wojskowej: w 2020 r. SKW zidentyfikowała osoby, które próbowały wstąpić do polskiej armii mimo powiązań z grupami ekstremistycznymi lub obcymi służbami wywiadowczymi, co pozwoliło na wykluczenie ich z procesu rekrutacji. Pomimo że służba koncentruje się przede wszystkim na ochronie sił zbrojnych, jej działalność ma również znaczenie dla ogólnego bezpieczeństwa społecznego. Zabezpiecza strategiczne obiekty, takie jak bazy wojskowe, magazyny broni czy sieci

komunikacyjne, co ma kluczowe znaczenie dla funkcjonowania państwa w sytuacjach kryzysowych. Działania związane z eliminacją zagrożeń terrorystycznych przyczyniają się do ochrony społeczeństwa przed atakami na obiekty wojskowe, które mogłyby mieć szerokie skutki dla bezpieczeństwa publicznego. Prowadzi działania informacyjne w zakresie cyberbezpieczeństwa i ochrony przed dezinformacją, co wpływa na świadomość obywateli w zakresie zagrożeń współczesnego świata. Służba Kontrwywiadu Wojskowego odgrywa kluczową rolę w ochronie polskiej armii, a pośrednio także w zapewnieniu bezpieczeństwa narodowego i społecznego. Dzięki swojej elastyczności i zdolności do reagowania na współczesne zagrożenia, takie jak szpiegostwo, terroryzm czy cyberprzestępczość, przyczynia się do utrzymania stabilności i ochrony interesów Rzeczypospolitej Polskiej.

Żanna Osikowicz

Służba Kontrwywiadu Wojskowego, https://www.infor.pl/prawo/encyklopedia-prawa/s/5733223,sluzba-kontrwywiadu-wojskowego.html (dostęp 15.01.2026); A. Pepłoński, *Kontrwywiad II Rzeczypospolitej*, Bellona, Warszawa 2002; https://www.skw.gov.pl (dostęp 15.01.2026); A. Zaręba, *Solidarność. Narodziny i upadek ruc*hu, Wydawnictwo Iskry, Warszawa 2015.

SŁUŻBA WOJSKOWA KOBIET – w rozumieniu ogólnym to obowiązkowy lub dobrowolny (w zależności od kraju) sposób pełnienia służby w siłach zbrojnych lub innych formacjach militarnych. Kobiety na ogół objęte są innymi regulacjami w tym zakresie niż mężczyźni, co wynika z kultury danego kraju i polityki bezpieczeństwa.

Służba kobiet w siłach zbrojnych występowała w historii w wielu kulturach, choć na ogół stanowiła formę odstępstwa od normy, jaką była służba mężczyzn. W starożytnej Grecji powstał mit o Amazonkach, plemieniu wojowniczych kobiet, które dla większej sprawności bojowej amputowały sobie piersi; w walce miały być skuteczniejsze od męskich przeciwników. W historii notujemy wiele kobiet pełniących ważne role wojskowe, np. Joanna d'Arc dla armii francuskiej podczas wojny stuletniej czy Emila Plater podczas powstania listopadowego w Polsce. Również

w innych kulturach notujemy takie przypadki, jak choćby przywództwo wojskowe Aiszy, wdowy po Muhammadzie (Mahomecie) w wojnie o sukcesję zakończonej przegraną bitwą pod Basrą (tzw. bitwa Wielbłądzia).

Współcześnie państwa narodowe wprowadziły służbę wojskową wyłącznie dla mężczyzn, kobiety pojawiały się w niej na początku tylko w formie ochotniczej i tylko w formacjach pomocniczych – pełniły funkcje pielęgniarek, łączniczek czy sanitariuszek. Z czasem zaczęto dopuszczać je do służby w formacjach operacyjnych, choć często wynikało to z braków kadrowych. Przykładem może być rosyjski pułk kawalerii kozackiej pod dowództwem Aleksandry Kudaszewej, jeden z pierwszych oddziałów, w którym służyli żołnierze obojga płci. W czasie I i II wojny światowej kobiety służyły głównie w ochotniczych formacjach wsparcia, takich jak chiński Batalion Kobiet z Guangxi oraz Amerykański Korpus Kobiet w Armii (Women's Army Corps; od 1942 WAVES – Women Accepted for Volunteer Emergency Service), brytyjskie Auxiliary Territorial Service (ATS), niemieckie Kriegshelferinnen (marynarka), Luftnachrichtenhelferinnen (siły powietrzne), Nachrichtenhelferin (siły lądowe) czy polskie Platerówki (1 Samodzielny Batalion Kobiecy im. Emilii Plater) wzorowane na oddziałach Armii Czerwonej. Kobiety podczas II wojny światowej służyły też w formacjach partyzanckich czy regularnych oddziałach operacyjnych, udowadniając swoją przydatność również w takich działaniach, czego wynikiem było dopuszczenie kobiet do kwalifikacji wojskowej.

Kobiety w armii służą w wielu krajach na całym świecie; obowiązkowa służba wojskowa jest w ich przypadku aktualnie powszechna tylko w niektórych państwach, takich jak np. Norwegia, Szwecja, Izrael, Wietnam, Laos, Korea Północna. Tego rodzaju rozwiązania planują wprowadzić także m.in. Dania, Litwa, Łotwa, Estonia czy Finlandia. W większości jednak obowiązkowy pobór do wojska dotyczy wyłącznie mężczyzn, a kobiety mogą wstępować dobrowolnie.

Norwegia jest pierwszym krajem NATO, który w 2015 r. wprowadził neutralny pod względem płci obowiązkowy pobór do sił zbrojnych. Konstytucja jasno określa, że każdy obywatel w wieku od 19 do 44 lat ma obowiązek pełnić służbę dla ochrony ojczyzny, bez względu na urodzenie czy stan majątkowy. Służba może trwać maksymalnie 19 miesięcy (najpierw

12, a dopiero później dodatkowe 7). Za decyzją o wprowadzeniu takiego modelu przywołuje się 2 kluczowe argumenty:

- z uwagi na kwestie równości wszyscy obywatele, niezależnie od płci, powinni mieć takie same prawa i obowiązki, wśród których znalazł się obowiązek obrony narodu;
- konieczność maksymalizacji zdolności operacyjnej i skuteczności poprzez zatrudnienie najlepiej wyszkolonych obywateli oraz uwzględnienie różnorodnych perspektyw.

Z roku na rok w norweskich siłach zbrojnych przybywa kobiet. Z danych wynika, że w 2017 r. ich odsetek wynosił 21%, w 2020 r. – 33%, natomiast w 2024 r. – 34%. Oznacza to, że 1/3 wojska stanowią kobiety.

Szwecja jest drugim krajem europejskim, w którym funkcjonuje obowiązkowa służba wojskowa dla kobiet. W 2017 r. ponownie, po 7 latach przywróciła obowiązkową służbę wojskową – podlegają jej mieszkańcy w wieku od 16 do 70 lat, w tym również kobiety. Decyzja ta była spowodowana przede wszystkim reakcją na zmieniającą się sytuację geopolityczną. Kobiety podlegają takiej samej selekcji jak mężczyźni, przechodzą testy sprawności fizycznej, psychologiczne oraz społeczne, a dzięki temu mają dostęp do wszystkich stanowisk wojskowych. Szkolenie obejmuje jednostki lądowe, morskie oraz powietrzne – pozwala to w pełni wykorzystać potencjał w ramach strategii obronnej kraju.

Obowiązkowa służba wprowadzona została na razie tylko w tych 2 krajach europejskich, natomiast w innych, np. w Polsce czy Niemczech, kobiety mogą służyć całkowicie dobrowolnie, co daje im możliwość wyboru jednostki czy specjalizacji, a później nawet stanowiska.

Istotnymi przykładami obowiązkowej służby wojskowej kobiet są Izrael i Korea Północna. W pierwszym wymienionym kraju służba trwa od 16 do 24 miesięcy, a później uzyskuje się kwalifikacje do służby zawodowej. Kobiety aktualnie pełnią służbę w większości (około 90%) formacji Sił Obronnych Izraela (w tym w korpusie pancernym, siłach powietrznych). Pomimo że proces rekrutacji zakłada równy dostęp dla kobiet do wszystkich ścieżek służby, w praktyce nadal płeć odkrywa kluczową rolę przy procesie kwalifikacji. Wyzwaniem jest również kwestia wspólnej służby kobiet i żołnierzy religijnych. Kluczowe jest przestrzeganie zasad separacji płci oraz radzenie sobie z wyzwaniami wynikającymi z pełnego włączenia

kobiet do jednostek bojowych. Niemniej sformowano przynajmniej 3 bataliony bojowe, w których służą i kobiety, i mężczyźni, są to bataliony Lwy Jordanu i Gepard oraz najbardziej znany 33 Batalion Karakal, który udowodnił swoją przydatność podczas walk z Hamasem 7 października 2023 r., zabijając ok. 100 bojowników bez strat własnych.

Kobiety i mężczyźni kwaterują oddzielne, natomiast pensje za obowiązkową służbę są takie same, niezależnie od płci. W 2024 r. aż 18 kobiet awansowało na stopień pułkownika, w porównaniu z 2016 r., gdy tylko 7 dostało awans na ten stopień. Od tamtej pory ich liczba stopniowo wzrasta. Pomimo występujących ograniczeń w przydziale do jednostek frontowych czy też uprzedzeń religijnych kobiety w wojsku są traktowane dużo lepiej niż w innych państwach autorytarnych. W 2014 r. stanowiska bojowe, takie jak piechota, obsługa czołgów i pojazdów opancerzonych, obsługa artylerii czy pilotowanie samolotów bojowych, zajmowało mniej niż 4% kobiet pełniących służbę wojskową.

Drugim krajem, w którym funkcjonuje obowiązkowa służba wojskowa dla kobiet, jest Korea Północna. Ich sytuacja jest znacznie trudniejsza niż w państwach demokratycznych; służba trwa około 8 lat i obowiązuje kobiety w wieku około 17–18 lat. Nie jest to zwyczajna służba wojskowa, bo w praktyce kobiety są często wysyłane do dodatkowych ciężkich przymusowych prac (kopalnie, farmy, budowa infrastruktury). Podlegają wyczerpującym wymaganiom fizycznym, takim samym jak mężczyźni, bardzo często w ekstremalnych warunkach bytowych (ograniczenia żywności, opieki medycznej, podstawowych potrzeb). Kobiety nie mają możliwości wyboru jednostki czy stanowiska, zostają przydzielane zgodnie z potrzebami państwa, gdyż służba jest ściśle związana z polityką ukierunkowaną na lojalność wobec reżimu. Brak posłuszeństwa może skutkować poważnymi konsekwencjami dla danej osoby, jak i całej rodziny. W porównaniu z innymi krajami, w których funkcjonuje obowiązkowa służba wojskowa dla kobiet i mężczyzn (np. Norwegia, Szwecja, Izrael), kobiety w Korei Północnej doświadczają znacznie gorszych warunkowych bytowych.

Rok 1999 był przełomowy w kontekście służby kobiet w polskich siłach zbrojnych – wówczas po raz pierwszy uzyskały one możliwość rekrutacji do wyższych szkół oficerskich. Wprowadzono liczne przepisy regulujące ich udział w całym procesie oraz pozwalające na późniejszą

służbę; obejmowały przede wszystkim normy wychowania fizycznego, odpowiednią infrastrukturę umożliwiającą zakwaterowanie kobiet w akademikach, natomiast po ukończeniu studiów ustawa o służbie wojskowej żołnierzy zawodowych z dnia 11 września 2003 r. gwarantowała dostęp do wszystkich stanowisk służbowych i w rezultacie – takie same warunki dla obu płci (możliwości rozwoju, szkolenia, pełnienia służby, edukacji, wynagrodzenia, wyróżnienia, awansowania czy zwalniania z określonych stanowisk). Początkowo kobiety mogły służyć tylko do 50 roku życia, czyli o 10 lat krócej niż mężczyźni, co stanowiło swego rodzaju dyskryminację związaną z ograniczeniem możliwości awansu na wyższe stopnie. W pierwszym okresie zapisy ustawy nie zyskały jednak dużej popularności wśród kobiet. Wymienia się kilka istotnych czynników, które miały na to wpływ:

- brak wystarczających informacji o możliwości służby kandydackiej;
- zmiany organizacyjne w Siłach Zbrojnych RP;
- brak dostępu kobiet do korpusu szeregowych.

W 1999 r. przyjęto 69 kobiet, a w 2003 r. stanowiły one około 0,3% ogólnej liczby żołnierzy. Rozpoczęcie członkostwa Polski w Organizacji Traktatu Północnoatlantyckiego (NATO) spowodowało potrzebę strukturalnych i systematycznych zmian w wielu obszarach państwa, które miały spowodować zwiększenie liczby kobiet w Wojsku Polskim. Należy zaznaczyć, że skuteczność zwiększania liczby kobiet w służbie wojskowej była niewystarczająca w porównaniu z innymi krajami i dopiero kolejne lata pokazały, że zmiany i większe zaangażowanie mają ogromne znaczenie dla rozwoju służby wojskowej kobiet. Dowodem na to są aktualne dane, które pokazują, że odsetek kobiet w Wojsku Polskim zwiększa się sukcesywnie z roku na rok.

W Wojsku Polskim aktualnie służy ponad 34 tys. kobiet. Należą one do następujących kategorii: żołnierki zawodowe – 21 tys., w terytorialnej służbie wojskowej – 7,5 tys., w dobrowolnej zasadniczej służbie wojskowej – 4 tys., a w aktywnej rezerwie i służbie kandydackiej – około 1,8 tys. Najwięcej kobiet służy w korpusie szeregowych (23,5 tys.), później podoficerskim (ponad 6,8 tys.) oraz oficerskim (ponad 3,8 tys.). Kobiety w Wojsku Polskim służą we wszystkich rodzajach sił zbrojnych, w tym

wojskach lądowych (ponad 10 tys.), Wojskach Obrony Terytorialnej (ok. 8,5 tys.), marynarce wojennej (ponad 900), siłach powietrznych (prawie 3 tys.), żandarmerii wojskowej (ponad 300) oraz wojskach specjalnych (około 170). Statystyki wykazują, że z roku na roku liczba kobiet w wojsku stale wzrasta; służą one na wielu stanowiskach, w tym medycznych, wychowawczych, technicznych, dowódczych, a także jako szeregowi żołnierze.

Dane dotyczące służby wojskowej kobiet w Siłach Zbrojnych RP pokazują, jak istotne są działania instytucjonalne w zakresie włączenia kobiet do środowiska wojskowego, kształcenia kadry oficerskiej oraz rozpowszechniania wiedzy na temat bezpieczeństwa. Wojskowe uczelnie (np. Wojskowa Akademia Techniczna – WAT, Akademia Sztuki Wojennej – AszWoj) sprzyjają zwiększaniu udziału kobiet w służbie wojskowej, co jest szczególnie istotne w kontekście przełamywania stereotypów. W konsekwencji obecność kobiet w Siłach Zbrojnych RP jest coraz bardziej naturalna i powszechna. Udział w różnych rodzajach służby obrazuje postępujące zmiany, profesjonalizację i równouprawnienie w armii.

Pojawienie się kobiet w zdominowanej przez mężczyzn strukturze wywołało wiele problemów dla nich samych. W 2004 r. Departament Obrony USA powołał Zespół ds. Opieki nad Ofiarami Napaści Seksualnych, którego ustalenia wskazały na potrzebę utworzenia silniejszej i scentralizowanej organizacji, która zajęłaby się tym problemem. Ostatecznie powołano Biuro ds. Zapobiegania i Reagowania na Napaści Seksualne (Sexual Assault Prevention and Response Office – SAPRO). W 2021 r. 8% kobiet w wojsku doświadczyło niechcianego kontaktu seksualnego; był to najwyższy odsetek od czasu rozpoczęcia gromadzenia danych przez Departament Obrony USA w 2004 r. Z szacowanych 35 900 przypadków napaści na tle seksualnym zgłoszono zaledwie 7260. Jednocześnie 1,5% mężczyzn w siłach zbrojnych również doświadczyło takiego kontaktu. Kolejnym ważnym problemem jest molestowanie seksualne czy mobbing na podłożu płciowy.

Kobiety od dawna pełnią w wojsku różne funkcje i odgrywają kluczową rolę w wielu formacjach, jednak w ostatnich latach coraz częściej zaczęły obejmować funkcje przywódcze i bojowe, a nie tylko administracyjne. Służba wojskowa wśród kobiet aktualnie cieszy się dużą popularnością: dowodem na to są państwa, w których nie jest ona obowiązkowa, a i tak

dane wskazują na wysoki odsetek kobiet w tego rodzaju strukturach. Obecność kobiet w armiach obrazuje, że potrafią wspierać nie tylko działania militarne, ale także stają się integralną częścią struktur operacyjnych i decyzyjnych. Kraje demokratyczne oferują dobrowolność, profesjonalizm i stabilność, dzięki czemu armia stale się powiększa. Nie każde państwo ma jednak taką samą misję, przez co w krajach autorytarnych kobiety często podlegają obowiązkowej mobilizacji. Zestawienie ilustruje, jak różnorodne mogą być warunki służby w zależności od ustroju.

Przemysław Mazur, Anna Ząber

M. Górski, *Najlepsi z najlepszych. Szwedzki pomysł na rekrutów*, https://defence24.pl/polityka-obronna/najlepsi-z-najlepszych-szwedzki-pomysl-na-rekrutow (dostęp 1.11.2025); *Kobiety w wojsku*, https://media.terytorialsi.wp.mil.pl/informacje/848511/kobiety-w-wojsku, (dostęp 10.11.2025); J. Koons, *Sexual Assault in the Military*, „CQ Researcher" 2013; A. Kuczyńska-Zonik, *Kobiety w armii. Obowiązkowa służba wojskowa w państwach nordyckich i bałtyckich*, „Komentarze Instytutu Europy Środkowej" 2025, nr 1375; K. Kuśmirek, *Służba kobiet w siłach zbrojnych*, „Czasopismo Naukowe Instytutu Studiów Kobiecych" 2017, nr 1(2); A. Pęzioł, *Wojskowa służba kobiet w siłach zbrojnych Rzeczypospolitej Polskiej w kontekście rozwiązań międzynarodowych oraz szkolnictwa wyższego na przykładzie Wojskowej Akademii Technicznej*, „Fides, Ratio et Patria. Studia Toruńskie" 2024, nr 20; M. Pogońska-Pol, *Kobiety w izraelskiej armii – trudy codzienności*, „Acta Universitatis Lodziensis. Folia Historica" 2018, nr 102; *Przybywa kobiet w polskiej armii. Wojsko dostosowuje infrastrukturę i wyposażenie*, https://raportcsr.pl/coraz-wiecej-kobiet-w-polskiej-armii-wojsko-dostosowuje-infrastrukture-i-wyposazenie/ (dostęp 10.11.2025); *Strefa obrony. Służba wojskowa kobiet w Siłach Obronnych Izraela*, https://strefaobrony.pl/sluzba-wojskowa-kobiet-w-silach-obronnych-izraela/ar/c1p2-26703745 (dostęp 12.11.2025).

STAŁA WSPÓŁPRACA STRUKTURALNA W DZIEDZINIE OBRONNOŚCI (ang. Permanent Structured Cooperation, PESCO) – formalnie ustanowiona decyzją Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. To mechanizm współpracy Unii Europejskiej w ramach wspólnej polityki bezpieczeństwa i obrony, który umożliwia grupie państw członkowskich pogłębioną współpracę obronną oraz przyjęcie dodatkowych obowiązków w zakresie obronności. PESCO ma na celu mobilizację państw

członkowskich do łączenia zasobów, koordynowania inwestycji i poprawy interoperacyjności sił zbrojnych. Opiera się na zobowiązaniach przyjętych przez uczestniczące państwa członkowskie w zakresie poziomu i struktury wydatków obronnych, planowania i ich harmonizacji, współpracy operacyjnej, wspólnego usuwania luk w zdolnościach oraz wzmacniania europejskiej bazy technologiczno-przemysłowej sektora obronnego (EDTIB). Tym, co odróżnia PESCO od innych formatów współpracy, jest prawnie wiążący charakter tych zobowiązań.

Mechanizm stałej współpracy strukturalnej został po raz pierwszy zapisany w Traktacie ustanawiającym Konstytucję dla Europy (tzw. Konstytucji Europejskiej) w art. III-312, który ostatecznie nie został ratyfikowany. Następnie inicjatywa została wprowadzona do Traktatu z Lizbony z 2009 r., nadając Unii Europejskiej możliwość ustanowienia stałej współpracy strukturalnej (PESCO) między tymi państwami członkowskimi, których zdolności wojskowe spełniają określone kryteria oraz które zobowiązują się do przyjęcia bardziej wiążących gwarancji w dziedzinie obronności. PESCO postrzegano jako narzędzie służące do wdrażania wspólnej obrony przewidzianej w art. 42 TUE, jednak sceptycyzm wobec dalszej integracji, ujawniony po odrzuceniu Konstytucji Europejskiej, spowodował, że mechanizm nie został uruchomiony. Ówczesny przewodniczący Komisji Europejskiej Jean-Claude Juncker określił PESCO mianem „śpiącej królewny" Traktatu z Lizbony. Do ponownego podjęcia inicjatywy skłoniły UE zmiany w środowisku bezpieczeństwa po 2014 r., w tym aneksja Krymu przez Federację Rosyjską czy powstanie państwa islamskiego i kryzys migracyjny.

Między państwami członkowskimi, zwłaszcza Francją a Niemcami, istniały wyraźne różnice co do kształtu PESCO. Francja opowiadała się za niewielką grupą państw o wysokich zdolnościach wojskowych, natomiast Niemcy forsowały model możliwie inkluzywny, otwarty także na państwa o słabszym potencjale wojskowym. Wypracowany kompromis polegał na ujęciu PESCO jako procesu, czyli mechanizmu z natury inkluzywnego, w ramach którego nie wszystkie państwa muszą uczestniczyć we wszystkich projektach i nie muszą od razu dysponować określonymi zdolnościami, lecz zobowiązują się do ich stopniowego osiągnięcia. Pozwoliło

to połączyć francuski postulat wzmacniania zdolności wojskowych z niemieckim dążeniem do niewykluczającej formuły współpracy.

Podstawę prawną do ustanowienia PESCO stanowił art. 42 ust. 6 Traktatu o Unii Europejskiej, który mówi, iż „państwa członkowskie, które spełniają wyższe kryteria zdolności wojskowej i które zaciągnęły w tej dziedzinie dalej idące zobowiązania, mając na względzie najbardziej wymagające misje, ustanawiają stałą współpracę strukturalną w ramach Unii". Następnie art. 46 traktatu doprecyzowuje, że „państwa członkowskie pragnące wziąć udział w stałej współpracy strukturalnej, o której mowa w art. 42 ust. 6, które spełniają kryteria i które przyjęły zobowiązania w zakresie zdolności wojskowych wymienione w Protokole w sprawie stałej współpracy strukturalnej, notyfikują swój zamiar Radzie i wysokiemu przedstawicielowi Unii do spraw zagranicznych i polityki bezpieczeństwa". Dodatkowo „w terminie 3 miesięcy od notyfikacji, o której mowa w ust. 1, Rada przyjmuje decyzję ustanawiającą stałą współpracę strukturalną i określającą listę uczestniczących państw członkowskich. Rada stanowi większością kwalifikowaną po konsultacji z wysokim przedstawicielem". Następnie w art. 46 ust. 3 czytamy, że: „każde państwo członkowskie, które na późniejszym etapie pragnie wziąć udział w stałej współpracy strukturalnej, notyfikuje swój zamiar Radzie i wysokiemu przedstawicielowi. Rada przyjmuje decyzję potwierdzającą udział zainteresowanego państwa członkowskiego, które spełnia kryteria i przyjmuje zobowiązania, o których mowa w art. 1 i 2 Protokołu w sprawie stałej współpracy strukturalnej. Rada stanowi większością kwalifikowaną po konsultacji z wysokim przedstawicielem. W głosowaniu biorą udział tylko członkowie Rady reprezentujący uczestniczące państwa członkowskie. Większość kwalifikowaną określa się zgodnie z art. 238 ust. 3 lit. a Traktatu o funkcjonowaniu Unii Europejskiej".

Państwa mogą wycofać się ze stałej współpracy strukturalnej, notyfikując swoją decyzję Radzie, która przyjmuje do wiadomości, że uczestnictwo zainteresowanego państwa członkowskiego zakończyło się. Protokół nr 10 w sprawie stałej współpracy strukturalnej, załączony do Traktatu o Unii Europejskiej, stanowi, że PESCO jest dostępna dla każdego państwa członkowskiego, które ma większe zdolności i zobowiązuje się do intensywnego rozwijania potencjału obronnego poprzez rozwój krajowych

wkładów i ich udział w siłach wielonarodowych, głównych europejskich programach wyposażenia oraz działaniach EDA w zakresie rozwoju zdolności obronnych, badań, zakupów i uzbrojenia.

7 września 2017 r. ministrowie spraw zagranicznych państw członkowskich Unii Europejskiej osiągnęli porozumienie w sprawie uruchomienia 10 pierwszych projektów w ramach PESCO. Następnie, 13 listopada 2017 r., dokument akcesyjny podpisało 23 z 28 państw członkowskich, a 7 grudnia 2017 r. – kolejne dwa: Irlandia i Portugalia. Ostatecznie 11 grudnia 2017 r., na mocy decyzji Rady, stała współpraca strukturalna została formalnie zainaugurowana z udziałem 25 państw. Pierwotnie z uczestnictwa w PESCO zrezygnowała Dania objęta klauzulą *opt-out* w odniesieniu do Wspólnej polityki bezpieczeństwa i obrony, jednak w następstwie rosyjskiej zbrojnej inwazji na Ukrainę w lutym 2022 r. parlament Danii 8 kwietnia 2022 r. przyjął propozycję przystąpienia kraju do układu obejmującą udział w Europejskiej Agencji Obrony oraz PESCO. Zniesienie klauzuli *opt-out* zatwierdzono na skutek referendum w Danii, które zostało przeprowadzone 1 czerwca 2022 r., a jego wynik wszedł w życie 1 lipca tego samego roku. Następnie rząd Danii przystąpił do analizowania możliwości uczestnictwa w PESCO, a decyzję o przystąpieniu zaakceptował ostatecznie duński parlament w marcu 2023 r. 23 maja 2023 r. Rada Unii Europejskiej formalnie zatwierdziła członkostwo Danii w PESCO. Początkowo poza mechanizmem pozostało również Zjednoczone Królestwo, które utrzymywało podobne zastrzeżenia, a następnie wystąpiło z Unii Europejskiej w 2020 r. Malta natomiast zrezygnowała z uczestnictwa w PESCO, obawiając się, że akcesja mogłaby pozostawać w sprzeczności z jej neutralnością, zakorzenioną w zasadach ustrojowych państwa. W rezultacie pozostaje ona jedynym państwem członkowskim Unii Europejskiej, które nie bierze udziału w tej formie współpracy. Od listopada 2020 r. w PESCO mogą uczestniczyć również państwa trzecie, jednak ich uczestnictwo przejawia się w udziale w konkretnych projektach, a nie w pełnym członkostwie. W 2021 r. do uczestnictwa w projekcie mobilności wojskowej zostały zaproszone Kanada, Norwegia i USA, w 2022 r. – Wielka Brytania, a w 2025 r. – Szwajcaria.

Celem PESCO jest wzmocnienie zdolności UE w dziedzinie międzynarodowego bezpieczeństwa, zapewnienie ochrony obywatelom UE,

a także maksymalizowanie efektywności wydatków na obronność. Uczestniczące państwa członkowskie opracowują projekty, współpracując w celu ulepszenia szkoleń i ćwiczeń wojskowych oraz wspólnego wzmacniania swoich zdolności, w tym także w cyberprzestrzeni. PESCO ma stanowić uzupełnienie dla bezpieczeństwa NATO, a nie jego konkurencję.

Współpraca w ramach PESCO odbywa się poprzez uruchamiane projekty dotyczące różnych obszarów, np. systemy lądowe, powietrzne i morskie, szkoleniowe, dotyczące nowoczesnych technologii, w tym systemów kwantowych. Obecnie (stan na listopad 2025), uruchomionych jest 75 projektów PESCO w różnych obszarach: każdy ma państwa koordynujące oraz uczestniczące. Poszczególne kraje mogą być też obserwatorami. Polska uczestniczy w 13 projektach PESCO i jest obserwatorem w 23 kolejnych. Wśród tych 13 jest również zainicjowany decyzją Rady UE z listopada 2019 r. projekt Centrum Szkolenia Medycznego na potrzeby Wojsk Specjalnych (SMTC), którego Polska jest koordynatorem.

Europejska Służba Działań Zewnętrznych (ESDZ), w tym Sztab Wojskowy UE (EUMS), oraz Europejska Agencja Obrony (EDA) wspólnie pełnią funkcję Sekretariatu PESCO, zapewniając w ramach Unii 1 punkt kontaktowy we wszystkich sprawach.

W debacie publicznej pojawiają się spekulacje, że PESCO to krok do stworzenia wspólnej armii UE, jednak w dokumentach i analizach eksperckich podkreśla się jasno, że to jedynie mechanizm oparty na wspólnych projektach państw uczestniczących.

Agnieszka Warchoł

Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States; *Permanent Structured Cooperation* (PESCO), https://www.pesco.europa.eu/#projects (dostęp 19.11.2025); *PESCO – stała współpraca strukturalna*, https://eur-lex.europa.eu/PL/legal-content/glossary/pesco-permanent-structured-cooperation.html (dostęp 19.11.2025); *PESCO*, https://www.pesco.europa.eu/about/ (dostęp 19.11.2025); *Poland – UE*, https://www.gov.pl/web/national-defence/poland---european-union, (dostęp 19.11.2025); Protokół (nr 10) w sprawie stałej współpracy strukturalnej ustanowionej na mocy artykułu 42 Traktatu o Unii

Europejskiej, Dz.U.UE C z dnia 30 marca 2010 r.; *Unia Europejska*, https://www.gov.pl/web/obrona-narodowa/ue-unia-europejska, (dostęp 19.11.2025).

STOWARZYSZENIE CYWILNYCH ZESPOŁÓW RATOWNICZYCH Z PSAMI (STORAT) – ochotnicza organizacja pozarządowa powstała w 2000 r. w Rzeszowie, działająca przeważnie na terenie Polski. Powstanie stowarzyszenia było efektem wieloletniej pracy osób zaangażowanych i zajmujących się szkoleniem psów i ratownictwem, które postanowiły swoją wiedzę i doświadczenie wykorzystać, aby wspierać właścicieli psów zainteresowanych współpracą ze zwierzętami przy poszukiwaniach i akcjach ratunkowych. Głównym zadaniem stowarzyszenia jest stworzenie na terenie całego kraju sieci zespołów ratowniczych, które współpracując z publicznymi służbami ratowniczymi i interwencyjnymi takimi jak Policja, Państwowa Straż Pożarna (PSP) i GOPR, włączałyby się do akcji poszukiwawczych, zwiększając szanse odnalezienia zaginionych. Od 2001 r. organizacja jest uwzględniona w planie ratowniczym województwa podkarpackiego. Została również wpisana do Krajowego Rejestru Organizacji Pożytku Publicznego i prowadzi działalność nieodpłatną w zakresie ratownictwa.

Celem statutowym stowarzyszenia jest wykorzystywanie psów w ratownictwie poszukiwawczym, lawinowym, katastrofowym (gruzowym) i innym. Ponadto prowadzi aktywność w zakresie profilaktyki – zapobiegania wypadkom oraz ochrony środowiska. Cele, o których mowa, są realizowane poprzez organizowanie i prowadzenie zespołów ratowniczych, w tym zrzeszanie i szkolenie ratowników i psów ratowniczych, wykonywanie działalności ratowniczo-poszukiwawczej, pomoc przy likwidacji skutków klęsk żywiołowych i katastrof oraz współpracę z organizacjami krajowymi i zagranicznymi. W ramach prowadzenia działalności zapobiegawczej realizują zadania związane z propagowaniem inicjatyw i postaw w zakresie umiejętnego korzystania ze środowiska naturalnego, programowaniem i prowadzeniem działalności profilaktycznej w zakresie bezpiecznego wypoczynku, prowadzeniem działalności informacyjnej i instruktażowej w zakresie szkolenia psów ratowniczych oraz współpracę z organami administracji, samorządami terytorialnymi, organizacjami społecznymi, gospodarczymi, naukowymi, jak również służbami

publicznym. W obszarze aktywności na rzecz ochrony środowiska naturalnego celem organizacji STORAT jest propagowanie wzorców zdrowego stylu życia w zgodzie z naturą, wnioskowanie w sprawach zagrożenia środowiska naturalnego oraz współpraca z jednostkami zajmującymi się ochroną środowiska naturalnego.

Szczególna aktywność stowarzyszenia jest związana ze szkoleniem zespołów ratowniczych i włączeniem ich do akcji ratowniczo-poszukiwawczych. Sam wybór psa, który może pracować w służbach mundurowych, szkolenie i egzamin są rygorystyczne. Zwierzę takie musi posiadać określone cechy, a kryteria doboru i selekcji zależą od wielu czynników, m.in. ról i zadań, jakie zostaną mu powierzone. Zwraca się uwagę przede wszystkim na:

- cechy fizyczne – ważne są wytrzymałość, zwinność oraz siła, które umożliwiają psu efektywną pracę w trudnych warunkach;
- temperament – pies musi być spokojny, posłuszny i odporny na stres, aby skutecznie wykonywać zadania ratownicze;
- zdolności węchowe – wyjątkowo wyczulony zmysł węchu umożliwia szybkie i precyzyjne lokalizowanie osób w akcjach ratowniczych; pozwala wykrywać zapachy niewidoczne dla technologii, co stanowi niezwykle ważny element powodzenia każdej akcji.

Popularne rasy wykorzystywane w działalności służb to labradory, owczarki niemieckie i border collie, wybierane ze względu na inteligencję i wytrzymałość. Ponadto każdy pies ratowniczy musi posiadać metrykę wystawioną przez organizację zrzeszoną w Międzynarodowej Federacji Kynologicznej (FCI) – w przypadku psów rasowych – oraz być oznakowany elektronicznym nośnikiem informacji (chip).

Psy, które mają realizować działania ratowniczo-poszukiwawcze, przechodzą testy kwalifikacyjne w odniesieniu do wcześniej wymienionych cech; ma to na celu wykluczenie zwierząt agresywnych, tchórzliwych, niewystarczająco sprawnych fizycznie i niewspółpracujących z człowiekiem. Po zaliczeniu testu zwierzęta są objęte programem szkolenia w zakresie posłuszeństwa, sprawności oraz określonych sprawności pracy węchowej; szkolone są do poszukiwań w 3 odmiennych specjalnościach: tropiący, lawinowy, gruzowy. Po zakończeniu szkolenia, a przed dopuszczeniem

do udziału w akcjach poszukiwawczo-ratowniczych psy są poddawane egzaminom certyfikacyjnym w oparciu o międzynarodowe regulaminy psów ratowniczych IRO (Internationale Rettungshunde Organisation) oraz regulamin Państwowej Straży Pożarnej. Należy zaznaczyć, że Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 28 grudnia 2021 r. w sprawie psów używanych w akcjach ratowniczych to podstawowy dokument określający zasady dotyczące psów używanych w PSP. Akt prawny reguluje kwestie ras psów dopuszczonych do służby ratowniczej, kryteriów zdrowotnych i użytkowych ich doboru, sposobu szkolenia, specjalności ratowniczych oraz przydzielania zwierząt do opiekunów. Rozporządzenie jest głównym źródłem prawnym, które określa zasady dotyczące egzaminów dla psów ratowniczych i ich kwalifikacji do pracy.

Po egzaminie kolejnym testem weryfikującym przydatność psów jest zaliczenie co najmniej 2 akcji pozorowanych – dopiero po uzyskaniu kompletu pozytywnych wyników, zaliczeniu egzaminów minimum w klasie A wg IRO lub klasy 1 wg regulaminu PSP i wymogów dodatkowych, zwierzęta uzyskują licencję psa ratowniczego STORAT – jest ona wydawana tylko na 1 rok kalendarzowy, aby utrzymać dobry poziom wyszkolenia. Przewodnik wraz z psem musi w tym czasie ponownie zaliczać określone testy, by uzyskać licencję na rok następny.

Podstawowy skład zespołu poszukiwawczego to przewodnik z psem i nawigator. Rolą przewodnika jest szkolenie i trening psa, a nadzór nad tym prowadzi Komisja Szkolenia Psów STORAT. Nawigator natomiast odpowiada za orientację w terenie i planowe prowadzenie zespołu poszukiwawczego w czasie akcji, zaś nadzór nad jego szkoleniem prowadzi główny nawigator. Stowarzyszenie współpracuje i bierze udział w działaniach z różnymi podmiotami ratowniczymi, stąd kluczowe jest odpowiednie przygotowanie. Należy pamiętać, że samo wyszkolenie zwierzęcia nie jest wystarczające do podjęcia działań ratunkowych; konieczne są również określone umiejętności nawigatorów oraz przewodników psów, od których wymaga się odpowiedniej sprawności fizycznej, teoretycznych wiadomości z zakresu psychologii psa i teorii zapachów, praktycznego udzielania pierwszej pomocy przedmedycznej (w stowarzyszeniu STORAT działają ratownicy, którzy posiadają odpowiednie kwalifikacje zgodne z warunkami określonymi w Ustawie z dnia 8 września 2006 r. o Państwowym

Ratownictwie Medycznym) oraz przedweterynaryjnej, posługiwania się sprzętem (mapy, kompas, GPS, radiotelefon itp.) oraz umiejętności optymalnego włączenia się do akcji ratowniczej z jej uczestnikami. Dzięki takiemu przygotowaniu oraz uczestnictwu w akcjach poszukiwawczo-ratowniczych u odpowiednio wyszkolonych psów następuje wyzwolenie efektu synergetycznego na bazie ludzkiej wiedzy, doświadczeń, umiejętności i sprzętu technicznego oraz zwierzęcego instynktu i zmysłów, co wpływa na skuteczność i powodzenie działań ratowniczych. Współpraca ta przekłada się na konkretne oszczędności czasu i zasobów ludzkich. Szacuje się, że 1 wyszkolony pies ratowniczy, pracujący z przewodnikiem i nawigatorem, potrafi w tym samym czasie wykonać pracę, która wymagałby zaangażowania nawet 100 osób w normalnych akcjach. Pies porusza się z dużą prędkością, niezależnie od gęstości poszycia leśnego czy pory dnia, a jego zdolności wyczuwania zapachu ludzkiego z odległości nawet 800 m czynią go najskuteczniejszym narzędziem w rękach ratowników.

STORAT działa dzięki wolontariuszom i reaguje na wezwania odpowiednich służb. W 2012 r. organizacja wsparła poszukiwania po katastrofie kolejowej pod Szczekocinami, będąc jedną z pierwszych, które wykorzystały psy w tak dużej akcji. Ponadto stowarzyszenie może pochwalić się licznymi akcjami zakończonymi sukcesem, jak ta, która miała miejsce w listopadzie 2025 r. w miejscowości Nadrzecze, w powiecie biłgorajskim. Organizacja została poproszona o pomoc w poszukiwaniach 60-letniego chorego mężczyzny. Do akcji wyjechało 7 osób i 3 psy. Po zebraniu informacji i wyznaczeniu terenu zespoły ruszyły do działań, które zostały zaplanowane w kierunku wskazanym przez policyjnego psa tropiącego. W godzinach porannych (ok. 1.30) jeden z zespołów z psem STORAT zgłosił odnalezienie zaginionego, który po zabezpieczeniu został przekazany zespołowi ratownictwa medycznego. Prócz aktywnego uczestnictwa w akcjach poszukiwawczych stowarzyszenie organizuje pokazy edukacyjne o bezpieczeństwie, profilaktyce zaginięć i dobrostanie zwierząt, a współpracując z Państwową Strażą Pożarną i Policją, dostarcza certyfikowane zespoły do poszukiwań.

Podsumowując, STORAT powstało nie tylko z pasji do zwierząt i możliwości ich wykorzystania, ale również w odpowiedzi na rosnące potrzeby związane z usprawnieniem działań ratowniczych i dlatego jest

ważnym elementem w budowaniu odporności na zagrożenia bezpieczeństwa publicznego. Jako podmiot pozarządowy typu non profit opiera się na zasadach samopomocy i aktywności społecznej, angażując inicjatywy lokalne oraz osoby dobrej woli. Jej działalność wynika z prawdziwej chęci pomagania, zaangażowania, a także gotowości niesienia pomocy osobom w sytuacji bezpośredniego zagrożenia życia i zdrowia. Aby działać skutecznie na rzecz społeczeństwa, ratownicy muszą posiadać specjalistyczną wiedzę, dysponować odpowiednim sprzętem i doświadczeniem (praca ze zwierzętami), co umożliwi im prowadzenie akcji w różnych, nierzadko bardzo wymagających warunkach otoczenia. Zespoły poszukiwawczo-ratownicze z psami stanowią krytyczny i niezastąpiony zasób w strukturze bezpieczeństwa wewnętrznego państwa; ich unikalna zdolność do szybkiej i precyzyjnej lokalizacji osób zaginionych lub uwięzionych, zarówno w środowisku naturalnym, jak i w wyniku katastrof budowlanych, czyni je kluczowym elementem w działalności służb. W kontekście działań ratowniczych, zwłaszcza poszukiwań wielkoobszarowych (teren otwarty) i operacji USAR (Urban Search and Rescue – gruzowiska), szybkość reakcji i efektywność identyfikacji poszkodowanych mają decydujące znaczenie dla przeżywalności. Psy ratownicze, dzięki przewadze sensorycznej nad technologiami, są w stanie przeszukać rozległe lub skomplikowane obszary w czasie nieosiągalnym dla zespołów ludzkich, co bezpośrednio wpływa na zwiększenie wskaźnika odnajdywania ofiar. Niestety mimo ogromnego znaczenia ich pracy organizacja musi mierzyć się z różnymi problemami; największym wyzwaniem są kwestie finansowe – zdobycie środków wymaga zarówno zaangażowania ze strony samej organizacji, jak i wsparcia od beneficjentów i innych instytucji oraz firm prywatnych; ponadto występują problemy legislacyjne – STORAT musi kontynuować starania o pełne równouprawnienie psów ratowniczych NGO z psami służbowymi. Obejmuje to nie tylko kwestie statusu prawnego podczas akcji, ale także dostęp do państwowego systemu emerytalnego dla psów-ratowników oraz terenów szkoleniowych. Należy jednak podkreślić, że istotnym atutem działania stowarzyszenia jest zdolność do aktywizacji i mobilizacji społeczeństwa do udziału w działaniach na rzecz bezpieczeństwa powszechnego. Natomiast współpraca z innymi podmiotami oraz ciągłe doskonalenie, również w obszarze technologicznym, sprawiają, że

organizacja stanowi ważny element dla przyszłości ratownictwa specjalistycznego w Polsce.

Żaneta Mrożek

Egzamin specjalności ratowniczej gruzowiskowej klasy I, https://storat.pl/wp-content/uploads/2020/08/Gruzowiskowy_klasy_I.pdf, (dostęp 20.01.2026); *GPR OSP Wołczkowo*, https://www.psyratownicze.eu/ (dostęp 20.01.2026); *International Search and Rescue Dog Organisation*, https://www.iro-dogs.org/en/ (dostęp 20.01.2026); Międzynarodowy regulamin egzaminów psów poszukiwawczo-ratowniczych (SAR) IRO i FCI, https://storat.pl/wp-content/uploads/2025/07/Regulamin-IRO-FCI_2025.pdf (dostęp 20.01.2026); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 28 grudnia 2021 r. w sprawie psów używanych w akcjach ratowniczych, Dz.U. 2022, poz. 20; S.J. Rysz, *Ostrzeganie, alarmowanie, powiadamianie ratunkowe*, Difin, Warszawa 2017; *Stowarzyszenie Cywilnych Zespołów Ratowniczych z Psami*, https://storat.pl/ (dostęp 20.01.2026); P.A. Toczyński, *Wykorzystanie psów w działaniach zarządzania kryzysowego*, „Studia Bezpieczeństwa Narodowego" 2022, nr 26; S. Ukraiński, *Udana akcja poszukiwawcza zespołu ratowniczego STORAT*, https://rzeszow.tvp.pl/49981649/udana-akcja-poszukiwawcza-zespolu-ratowniczego-storat (dostęp 20.01.2026); Ustawa z dnia 7 kwietnia 1989 r. – prawo o stowarzyszeniach, Dz.U. 1989, nr 20, poz.104 z późn. zm.; Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie, Dz.U. 2003, nr 96, poz. 873 z późn. zm.; Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym, Dz.U. 2017, poz. 2195 z późn. zm.; J. Ziobro, *Ratownictwo transgraniczne jako forma współpracy i integracji międzynarodowej oraz środek w procesie zapewniania bezpieczeństwa powszechnego – wybrane aspekty organizacji transgranicznych działań ratowniczych*, „Zeszyty Naukowe SGSP" 2020, nr 73/1; *Związek Kynologiczny w Polsce*, https://zkwp.pl/ (dostęp 20.01.2026).

STREFA ZDEMILITARYZOWANA – obszar, na którym na podstawie wiążących postanowień prawa międzynarodowego zabronione jest lokowanie sił zbrojnych, rozmieszczanie uzbrojenia oraz utrzymywanie infrastruktury mogącej służyć prowadzeniu działań wojennych. Zakaz dotyczy zwykle zarówno wojsk lądowych, morskich i powietrznych, jak i instalacji dowodzenia, składów amunicji, lotnisk, baz marynarki czy umocnień inżynieryjnych. Terytorium takie jest „wyłączone" z bezpośredniej rywalizacji militarnej między stronami konfliktu lub potencjalnymi

przeciwnikami. Stanowi instrument mający ograniczać prawdopodobieństwo nagłego wybuchu walk, zmniejszać ryzyko incydentów granicznych oraz tworzyć przestrzeń sprzyjającą negocjacjom politycznym. Z reguły pojawia się w sytuacji, w której państwa lub inni uczestnicy stosunków międzynarodowych nie są w stanie osiągnąć pełnego, kompleksowego porozumienia pokojowego, lecz jednocześnie dążą do ustabilizowania linii rozgraniczenia. Z tego względu strefa zdemilitaryzowana bywa rozumiana jako narzędzie zarządzania konfliktem, a nie ostatecznego jego rozwiązania.

Geneza tej instytucji wiąże się z ewolucją prawa wojennego i praktyki traktatowej od XIX w. Już wcześniejsze porozumienia pokojowe przewidywały tworzenie pasów terytorium, z których zwyciężony przeciwnik miał obowiązek wycofać wojska lub podporządkować je szczególnemu reżimowi kontroli. Z upływem czasu zaczęto jednak kształtować bardziej sformalizowane rozwiązania, w których demilitaryzacja miała obejmować nie tylko chwilowe wycofanie jednostek, lecz trwałe ograniczenie suwerenności wojskowej państwa na danym obszarze. Przykładem były postanowienia dotyczące Nadrenii po I wojnie światowej, a także demilitaryzacja niektórych archipelagów czy cieśnin morskich. Równolegle rozwijała się koncepcja neutralizacji określonych terytoriów, w ramach której państwa zgadzały się nie tylko na brak wojsk, lecz także na powstrzymanie się od ich wykorzystywania jako zaplecza operacyjnego. Po II wojnie światowej, wraz z powstaniem Organizacji Narodów Zjednoczonych i rozwojem mechanizmów bezpieczeństwa zbiorowego, strefy zdemilitaryzowane stały się jednym z rozwiązań stosowanych przez Radę Bezpieczeństwa oraz państwa zawierające porozumienia rozejmowe.

Z perspektywy prawa międzynarodowego strefę zdemilitaryzowaną ustanawia się zazwyczaj na podstawie traktatu pokojowego, układu o zawieszeniu broni, porozumienia rozdzielającego wojska lub rezolucji organu międzynarodowego upoważnionego do działania w imieniu społeczności międzynarodowej. Prawidłowo skonstruowany reżim normatywny określa dokładny przebieg granic strefy, wskazuje zakazane kategorie działań i instalacji oraz przewiduje mechanizmy weryfikacji. Nie chodzi jedynie o obowiązek niewprowadzania wojsk, lecz także o zakaz szkolenia formacji paramilitarnych, składowania uzbrojenia, prowadzenia

prac fortyfikacyjnych czy rozmieszczania systemów rozpoznania i rażenia. W dokumentach ustanawiających tego typu obszar spotyka się ponadto zapisy dotyczące demontażu istniejącej infrastruktury militarnej, obowiązku rozminowania, a także ograniczeń w użyciu przestrzeni powietrznej nad strefą. Pełna skuteczność tych postanowień zależy od przewidzenia procedur monitoringu, w tym prawa do inspekcji międzynarodowych, stałej obecności obserwatorów lub rozmieszczenia kontyngentów pokojowych.

W praktyce najczęściej wyróżnia się 2 podstawowe modele organizacji strefy zdemilitaryzowanej: w pierwszym państwa same sprawują kontrolę nad przestrzeganiem ograniczeń, przy czym opierają się głównie na środkach technicznych i wzajemnej obserwacji. Tego rodzaju rozwiązanie może funkcjonować relatywnie stabilnie tam, gdzie poziom zaufania między stronami jest umiarkowanie wysoki, a koszt naruszenia porozumienia przewyższa potencjalne korzyści militarne. W drugim modelu istotną rolę odgrywa organizacja międzynarodowa, która otrzymuje mandat do obecności na terenie strefy i nadzoru nad statusem demilitaryzacji. Wówczas to misje obserwacyjne ONZ, siły rozdzielające lub wielonarodowe kontyngenty pokojowe pełnią funkcje strażnika porozumienia. Dysponują one możliwością zgłaszania naruszeń, ułatwiania dialogu wojskowego i cywilnego oraz pośredniczenia w rozwiązywaniu incydentów. Obecność podmiotu trzeciego może ograniczać pokusę naginania postanowień przez którąś ze stron, lecz nie eliminuje problemu asymetrii politycznej czy wojskowej.

Znanym i często przywoływanym przykładem strefy zdemilitaryzowanej jest obszar oddzielający Republikę Korei i Koreańską Republikę Ludowo-Demokratyczną, ustanowiony na mocy porozumienia rozejmowego z 1953 r. Został on wytyczony wzdłuż linii frontu, w formie pasa o znaczącej szerokości, który formalnie ma pozostawać pozbawiony infrastruktury bojowej oraz stałej obecności wojsk. W praktyce jego otoczenie należy do najbardziej zmilitaryzowanych regionów świata, z silnie umocnionymi pozycjami, rozbudowanymi systemami obserwacji oraz licznymi polami minowymi. Strefa pełni jednocześnie funkcję symbolicznej granicy konfliktu oddzielającej 2 antagonistyczne systemy polityczne. Jej trwanie przez dziesięciolecia pokazuje, że demilitaryzacja terytorium nie musi prowadzić do stopniowego zaniku sporu, lecz może utrwalać sytuację

„zamrożonej" konfrontacji, w której działania zbrojne zostały przerwane, ale nie doprowadzono do zawarcia traktatu pokojowego.

Inny typowy przypadek stanowiły strefy utworzone na Bliskim Wschodzie po wojnach arabsko-izraelskich. Na Wzgórzach Golan wyznaczono linię rozdziału wojsk syryjskich i izraelskich oraz obszar, w którym obecne są siły pokojowe ONZ sprawujące nadzór nad przestrzeganiem zobowiązań. Mandat tych sił obejmuje obserwację ruchów wojsk, kontrolę przestrzegania zakazu budowy nowych umocnień oraz pośredniczenie w kontaktach między stronami. Podobne rozwiązania zastosowano w Egipcie i Izraelu, na półwyspie Synaj po zawarciu porozumienia pokojowego, wyznaczając strefy o różnym stopniu dopuszczalnej obecności wojsk, aż po obszary wymagające pełnego zaniechania aktywności militarnej. Z kolei na Cyprze wytyczono szeroki pas ziemi pod kontrolą Organizacji Narodów Zjednoczonych, który oddziela społeczności grecko- i turecko-cypryjską. Chociaż nie ma on statusu klasycznej strefy zdemilitaryzowanej w ścisłym prawnym sensie, pełni funkcję rozdzielającą oraz ograniczającą możliwość bezpośredniego starcia sił zbrojnych obu stron.

Specyficzną kategorią są terytoria, których demilitaryzacja wynika nie tyle z bezpośredniego konfliktu zbrojnego, ile z dążeń społeczności międzynarodowej do utrzymania stabilności w danym regionie lub ochrony wartości szczególnie ważnych, jak środowisko naturalne. Przykładem może być archipelag Wysp Alandzkich, objęty reżimem demilitaryzacji i neutralizacji już w XIX w., a następnie potwierdzany w kolejnych porozumieniach. Państwo sprawujące suwerenność nad tym obszarem przyjęło zobowiązanie do niewznoszenia tam fortów, nieutrzymywania garnizonów oraz niewykorzystywania wysp jako bazy dla operacji wojennych. Z kolei traktat antarktyczny wprowadza zasadę pokojowego wykorzystania kontynentu oraz zakaz rozmieszczania tam instalacji o charakterze militarnym, co stanowi rozszerzoną postać demilitaryzacji. W tym wypadku motywacja jest szersza: chodzi o zapewnienie, by obszar szczególnie wrażliwy z punktu widzenia badań naukowych i ekosystemów nie stał się przedmiotem rywalizacji strategicznej.

Strefy zdemilitaryzowane mają doniosłe znaczenie w teorii bezpieczeństwa międzynarodowego, ponieważ łączą elementy ograniczania zbrojeń, budowy zaufania oraz kontroli konfliktu. Tworzą one fizyczny

dystans między potencjalnymi przeciwnikami, co zmniejsza prawdopodobieństwo przypadkowych incydentów wynikających z bliskości jednostek wojskowych, takich jak naruszenia granicy, ostrzał ostrzegawczy czy niezamierzone wtargnięcia. Mogą również pełnić funkcję sygnału politycznego, świadczącego o woli stabilizacji sytuacji oraz gotowości do poddania części atrybutów suwerenności międzynarodowej regulacji. W tym sensie można je postrzegać jako narzędzie przejściowe między stanem intensywnej konfrontacji a ewentualnym przyszłym porozumieniem pokojowym, które dopiero w dalszej perspektywie usunęłoby potrzebę istnienia takiego obszaru.

Jednocześnie należy zauważyć, że skuteczność stref zdemilitaryzowanych pozostaje uzależniona od wielu czynników politycznych i wojskowych. Jednym z nich jest równowaga sił między stronami: jeśli któraś posiada zdecydowaną przewagę militarną, może traktować reżim demilitaryzacji jako obciążenie, które ogranicza jej swobodę strategiczną; pojawia się wtedy pokusa stopniowego naruszania zobowiązań, wprowadzania do strefy „nieuzbrojonych" formacji bezpieczeństwa czy rozbudowy infrastruktury o podwójnym zastosowaniu cywilno-wojskowym. Innym czynnikiem jest obecność aktorów niepaństwowych, którzy mogą wykorzystywać obszar wyłączony spod kontroli wojskowej do działań nieregularnych, przemytu czy ataków terrorystycznych. W takich okolicznościach państwa skłonne są żądać renegocjacji statusu strefy, argumentując konieczność zapewnienia bezpieczeństwa ludności cywilnej.

Współczesne konflikty, w których coraz większą rolę odgrywają środki oddziaływania na odległość, technologie informacyjne oraz działania hybrydowe, stawiają przed ideą demilitaryzacji nowe wyzwania. Tradycyjne wyobrażenie strefy zdemilitaryzowanej jako pasa ziemi pozbawionego fizycznej obecności wojsk nie wystarcza w warunkach, gdy decydujące znaczenie mają systemy rakietowe o zasięgu setek kilometrów, platformy bezzałogowe, zdolności cybernetyczne i satelitarne. Z jednej strony, ograniczenia co do rozmieszczania instalacji militarnych na konkretnym terytorium wciąż mogą zmniejszać ryzyko nagłego uderzenia, utrudniać przygotowanie ofensywy lądowej i komplikować logistykę; z drugiej zaś – coraz większa część potencjału militarnego znajduje się poza obszarem geograficznie rozumianej strefy, co osłabia bezpośredni wpływ

demilitaryzacji na równowagę sił. Pojawia się więc pytanie o możliwość rozszerzenia logiki strefy zdemilitaryzowanej na przestrzeń powietrzną, cyberprzestrzeń czy niektóre domeny kosmiczne.

Istotne są również skutki społeczne i gospodarcze funkcjonowania takich obszarów. W wielu przypadkach strefy wytycza się wzdłuż granic zamieszkanych przez ludność cywilną, której codzienne życie ulega poważnym ograniczeniom: utrudniony bywa dostęp do ziem uprawnych, źródeł wody, infrastruktury transportowej; pojawiają się wymuszone przesiedlenia lub zakazy przebywania na niektórych terenach.

Analiza stref zdemilitaryzowanych wymaga także rozróżnienia między nimi a innymi formami ograniczania aktywności militarnej. Od stref wolnych od broni jądrowej różnią się one przede wszystkim zakresem regulacji: w tym drugim przypadku państwa zobowiązują się nie rozmieszczać określonej kategorii uzbrojenia, natomiast nie rezygnują z obecności konwencjonalnych sił zbrojnych. Z kolei korytarze humanitarne czy strefy bezpieczeństwa dla ludności cywilnej ustanawiane są zazwyczaj na krótszy okres i mają służyć konkretnym działaniom w sytuacji bezpośredniego zagrożenia. Strefa zdemilitaryzowana odznacza się większym stopniem trwałości i obejmuje kompleksowe ograniczenia, które wpływają zarówno na planowanie operacyjne, jak i długoterminową politykę obronną państw.

Jednocześnie w literaturze pokojoznawczej oraz w badaniach nad transformacją konfliktu coraz silniej akcentuje się wymiar normatywny stref zdemilitaryzowanych. Wskazuje się, że nie są one wyłącznie technicznym narzędziem zarządzania napięciami, lecz również instytucją odzwierciedlającą dominujące w danym okresie wyobrażenia o dopuszczalnych granicach użycia siły oraz roli społeczności międzynarodowej w nadzorowaniu sporów. Strefy takie bywają interpretowane jako materialny przejaw „odpowiedzialności za pokój", rozumianej w kontekście gotowości do przyjęcia na siebie przez państwa określonych ograniczeń w działaniu, w zamian za minimalizowanie ryzyka ponownego wybuchu wojny. Jednocześnie pojawiają się głosy krytyczne podkreślające, że tam, gdzie strefy zdemilitaryzowane utrzymują się przez dziesięciolecia, mogą one służyć raczej utrwalaniu podziałów politycznych i etnicznych niż ich przezwyciężaniu. W takim ujęciu stają się one „zamrożonymi granicami

konfliktu", trudnymi do naruszenia właśnie dlatego, że ich status został umocniony normatywnie i instytucjonalnie.

Ważnym polem refleksji jest także zastosowanie koncepcji stref zdemilitaryzowanych w konfliktach wewnątrzpaństwowych. W tego typu sytuacjach porozumienia o wyłączeniu z obecności wojskowej określonych obszarów zawierane są między rządem a zbrojnymi aktorami niepaństwowymi, często z udziałem mediatorów międzynarodowych. Przykłady obejmują miasta lub regiony, które na czas negocjacji mają zostać „odmilitaryzowane", aby umożliwić powrót uchodźców, przeprowadzenie wyborów lub dostarczanie pomocy humanitarnej. Tego rodzaju rozwiązania napotykają jednak specyficzne trudności. Po pierwsze, część uczestników konfliktu dysponuje jedynie rozproszonymi strukturami zbrojnymi, co utrudnia weryfikację stopnia ich wycofania. Po drugie, brak jednoznacznie ukształtowanych linii frontu oraz wielość ośrodków lojalności sprawiają, że wyznaczenie stabilnej strefy zdemilitaryzowanej wymaga znacznie większych nakładów organizacyjnych niż w konfliktach między państwami. Po trzecie wreszcie, utrwalenie statusu takiego obszaru może prowadzić do faktycznej autonomizacji terytorium i osłabienia suwerenności państwa, co bywa postrzegane jako politycznie nieakceptowalne.

Odrębny nurt badań koncentruje się na symbolicznych i tożsamościowych aspektach istnienia stref zdemilitaryzowanych. Granice tego typu obszarów często zyskują znaczenie w dyskursie publicznym, stając się elementem narracji narodowych, pamięci zbiorowej oraz polityki historycznej. W przypadku Korei linia rozdziału jest nie tylko faktyczną granicą wojskową, lecz również silnym symbolem podziału narodu, wykorzystywanym zarówno w przekazie propagandowym, jak i w kulturze popularnej. Podobne mechanizmy występują w innych regionach, gdzie strefy zdemilitaryzowane są traktowane jako namacalny dowód przeżytej traumy wojennej, ale też miejsce projekcji nadziei na przyszłe pojednanie. W tych warunkach każda próba modyfikacji ich statusu – czy to w kierunku dalszej liberalizacji, czy przeciwnie, remilitaryzacji – wywołuje silne reakcje emocjonalne, wykraczające poza czysto techniczne debaty o bezpieczeństwie.

Nie bez znaczenia pozostaje problem zarządzania cywilnego strefami zdemilitaryzowanymi. O ile w części przypadków obszary te są w praktyce

niemal całkowicie niezamieszkane, o tyle w innych sytuacjach funkcjonują tam społeczności lokalne, które muszą dostosować się do specyficznego reżimu prawnego. Pojawia się pytanie o zakres kompetencji władz państwowych oraz ewentualny udział organizacji międzynarodowych w administrowaniu tym terytorium. W literaturze opisuje się rozwiązania, w których instytucje międzynarodowe odgrywają istotną rolę nie tylko w nadzorze nad brakiem obecności wojsk, lecz również w mediowaniu sporów lokalnych, koordynowaniu projektów odbudowy infrastruktury oraz wspieraniu inicjatyw pojednawczych. Tego typu praktyki zbliżają strefy zdemilitaryzowane do szerszych koncepcji „zarządzania powojennego" i „pokojotwórstwa", w których bezpieczeństwo militarne postrzega się jako jeden z wielu wymiarów stabilizacji.

Kolejny wymiar refleksji dotyczy metod badawczych wykorzystywanych do analizy funkcjonowania stref zdemilitaryzowanych. Ze względu na ich specyfikę oraz ograniczony dostęp do części danych wojskowych badacze często sięgają po podejścia jakościowe, takie jak studia przypadku, analiza dokumentów, wywiady z uczestnikami procesów negocjacyjnych oraz obserwacja działań organizacji międzynarodowych. Coraz częściej wykorzystuje się także dane ilościowe i narzędzia geoinformacyjne pozwalające na analizę rozmieszczenia infrastruktury, dynamiki osadnictwa czy zmian środowiskowych w obrębie strefy. Porównawcze analizy różnych przypadków umożliwiają identyfikowanie czynników sprzyjających trwałości reżimu demilitaryzacji bądź przeciwnie, prowadzących do jego erozji. Uwagę zwracają zwłaszcza sytuacje, w których podobnie skonstruowane strefy przynoszą odmienny rezultat: w jednych przypadkach stają się stabilnym elementem architektury bezpieczeństwa regionalnego, w innych zaś nie zapobiegają nawrotowi przemocy.

Wreszcie warto zauważyć, że dyskusja nad przyszłością stref zdemilitaryzowanych wpisuje się w szerszą debatę o transformacji ładu międzynarodowego oraz zmianie charakteru wojen. Część autorów wskazuje, że w warunkach rosnącej roli aktorów niepaństwowych, prywatyzacji przemocy oraz hybrydyzacji działań zbrojnych tradycyjnie rozumiane pasy terytorialnej demilitaryzacji mogą tracić znaczenie jako główne narzędzie ograniczania ryzyka. Inni podkreślają jednak, że właśnie w obliczu tej złożoności pojawia się zapotrzebowanie na czytelne,

przestrzennie zdefiniowane mechanizmy regulacyjne, które wyznaczają minimalne „wyspy porządku" w niestabilnym otoczeniu. Z tego punktu widzenia strefy zdemilitaryzowane pozostają istotnym laboratorium dla innowacyjnych rozwiązań prawnych i instytucjonalnych, testowanych w konkretnych konfliktowych kontekstach, a następnie przenoszonych – przynajmniej częściowo – do szerszych reżimów bezpieczeństwa regionalnego i globalnego.

W literaturze przedmiotu wskazuje się, że ustanawianie stref zdemilitaryzowanych może pełnić funkcję wskaźnika dojrzałości reżimów bezpieczeństwa w danym regionie. Tam, gdzie istnieją rozwinięte mechanizmy konsultacji wojskowych, przejrzystości ćwiczeń oraz wymiany informacji, demilitaryzacja określonych obszarów może stać się naturalnym etapem pogłębiania współpracy. Przykładów takich rozwiązań dostarczają niektóre porozumienia rozbrojeniowe z okresu zimnej wojny, w których strony decydowały się na wprowadzenie stref ograniczonego zbrojenia lub zakazu rozmieszczania wybranych systemów uzbrojenia w pobliżu granic. W regionach o słabych instytucjach bezpieczeństwa, wysokim poziomie wrogości i częstych naruszeniach zawieszeń broni sama próba ustanowienia strefy zdemilitaryzowanej napotyka zwykle poważne trudności, a jej trwałość staje pod znakiem zapytania.

Strefa zdemilitaryzowana jest wyspecjalizowanym instrumentem prawa i polityki międzynarodowej, którego zadaniem jest wyłączenie określonego terytorium z bezpośredniej rywalizacji militarnej. Jej istnienie opiera się na założeniu, że fizyczne odsunięcie sił zbrojnych oraz redukcja infrastruktury wojskowej mogą przyczynić się do obniżenia ryzyka konfliktu zbrojnego, stworzenia przestrzeni dla negocjacji oraz stabilizacji linii rozgraniczenia. Doświadczenia historyczne pokazują jednak, że skuteczność tego rozwiązania zależy od wielu uwarunkowań: równowagi sił, stopnia woli politycznej, roli organizacji międzynarodowych, obecności aktorów niepaństwowych oraz charakteru współczesnych technologii wojskowych. Strefy zdemilitaryzowane mogą utrwalać stan „zamrożonego" konfliktu, ale także, w sprzyjających okolicznościach, stać się elementem szerszego procesu pokojowego, dlatego w analizie tej instytucji podkreśla się przede wszystkim jej ambiwalentny charakter: jest ona jednocześnie narzędziem

ograniczania zagrożeń i wskaźnikiem trwających sporów, których sama demilitaryzacja terytorium nie jest w stanie definitywnie zakończyć.

Fabian Kobalczyk-Gruda

L. Beehner, G. Meibauer, *The Futility of Buffer Zones in International Politics*, „Orbis" 2016, vol. 60, no. 2; L.M. Brady, *From War Zone to Biosphere Reserve: The Korean DMZ as a Nature Conservation Area*, „Notes and Records: The Royal Society Journal of the History of Science" 2021; T. Brańka, *Demilitaryzacja i neutralizacja na przykładzie Wysp Alandzkich,* „Przegląd Politologiczny" 2017, nr 4; *Demilitarization Regimes in Contemporary International Law,* National and Kapodistrian University of Athens, Faculty of Law, Athens 2021; M. Dnistrianskyi, *Modern Conflicts Regarding the Political Status of Territories*, „Bulletin of Geography. Socio-Economic Series" 2022, no. 57; B. Ní Ghráinne, *Safe Zones and the Internal Protection Alternative*, British Institute of International and Comparative Law, Cambridge 2020; B. Ní Ghráinne, *Safe Zones and the Internal Protection Alternative*, „International and Comparative Law Quarterly" 2020, vol. 69, no. 2; A. Gustafsson, *Aspects Regarding the Svalbard Demilitarisation in Relation to Norway Joining the Atlantic Alliance in 1949, and Reflections on the Åland Islands' Demilitarised and Neutralised Status in the Event of a Finnish NATO Accession*, „Journal of Autonomy and Security Studies" 2018, vol. 2, no. 2; *Establishment of Zones of Peace or Demilitarization*, [w:] *Assembly for Peace: GA Digital Handbook on Peace and Security*, United Nations University, Tokyo 2024; *International Committee of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, ICRC, Geneva 2019; *International Legal Regulation of Demilitarized Zones, University of Vienna*, Faculty of Law, Vienna 2024; Z.M. Jaffal, W.F. Mahameed, *Prevent Environmental Damage During Armed Conflict*, „BRICS Law Journal" 2018; E. Katz, *Between Here and There: Buffer Zones in International Law*, „University of Chicago Law Review" 2017, vol. 84, no. 3; K. Kingma, N. Schrijver, *Demilitarization*, [w:] *Max Planck Encyclopedia of Public International Law*, Oxford University Press, Oxford 2015; W. Lippert, *Conventional Arms Control Agreements in Europe: Conditions of Success and Failure*, „Central European Journal of International and Security Studies" 2024; I.V. Roianova, *Comparative Analysis of Demilitarized and Neutralized Territories in International Law*, „Theory and Practice of Jurisprudence" 2019; *"Safe zones": A Protective Alternative to Flight or a Tool of Refugee Containment? Clarifying the International Legal Framework Governing Access to Refugee Protection against the Backdrop of "Safe Zones" in Conflict-Affected Contexts*, „International Review of the Red Cross" 2022; S. Spiliopoulou Åkermark, *What is the Essence of the Institution of Demilitarisation? Reflections*

upon Completion of the Åland Islands Demilitarisation Research Project, „Journal of Autonomy and Security Studies" 2018, vol. 2, no. 2; S. Spiliopoulou Åkermark, S. Heinikoski, P. Kleemola-Juntunen, *Demilitarisation and International Law in Context: The Åland Islands*, Routledge, London–New York 2018; S. Spiliopoulou Åkermark, T. Hyttinen, P. Kleemola-Juntunen, *Life on the Border: Dealing with Territorial Violations of the Demilitarised and Neutralised Zone of the Åland Islands*, „Nordic Journal of International Law" 2019, vol. 88; *The Demilitarisation of Åland in a Nutshell*, Åland Islands Peace Institute, Mariehamn 2022.

SZOWINIZM OPIEKUŃCZY – postawa polityczna i społeczna, która zakłada, że dostęp do świadczeń socjalnych – takich jak zasiłki, opieka zdrowotna, edukacja czy mieszkalnictwo komunalne – powinien być ograniczony dla imigrantów, a w pełni dostępny jedynie dla rdzennych obywateli. U podstaw tego myślenia leży przekonanie o „zasługiwaniu" (*deservingness*). Zgodnie z tą logiką państwo dobrobytu jest owocem wielopokoleniowej pracy, wyrzeczeń i płacenia podatków przez konkretną nację. Przybysze z zewnątrz, którzy nie kontrybuowali do tego systemu historycznie, są postrzegani jako „pasażerowie na gapę" (*free-riders*), którzy nadużywają gościnności gospodarzy.

Kluczowym argumentem w analizie tego zjawiska jest fakt, że w wielu państwach europejskich (szczególnie w modelu skandynawskim czy zachodnioeuropejskim), rozbudowany socjal stał się immanentną częścią tożsamości narodowej. Wysoki poziom zaufania społecznego, solidarność i redystrybucja dóbr są traktowane jako unikalne cechy kultury europejskiej. W tej optyce napływ imigrantów o odmiennym zapleczu kulturowym jest interpretowany jako zagrożenie dla tego modelu. Argumentacja szowinizmu opiekuńczego brzmi następująco: aby utrzymać wysoki standard opieki dla „swoich", należy zamknąć system przed „obcymi"; jest to forma „solidarności zamkniętej". Zjawisko to jest silnie eksploatowane przez partie populistyczne, które pozycjonują się jako obrońcy „zwykłych ludzi" przed elitami i imigrantami. W narracji tych ugrupowań bezpieczeństwo kulturowe jest nierozerwalnie związane z ekonomicznym. Hasła typu „najpierw nasi obywatele" sugerują, że zasoby są grą o sumie zerowej – każdy zasiłek przyznany imigrantowi jest postrzegany jako odebrany rdzennemu mieszkańcowi.

Paradoks szowinizmu opiekuńczego polega jednak na tym, że w dłuższej perspektywie może on generować zagrożenia dla bezpieczeństwa wewnętrznego, zamiast je niwelować. Europa, borykająca się z kryzysem demograficznym, potrzebuje rąk do pracy, aby utrzymać system emerytalny. Tworzenie systemowej dyskryminacji poprzez odmawianie imigrantom dostępu do siatki bezpieczeństwa socjalnego prowadzi do powstawania klasy wykluczonych – prekariatu bez perspektyw na integrację. Spychanie grup imigranckich na margines, przy jednoczesnym oczekiwaniu ich wkładu w rynek pracy, prowadzi do frustracji, radykalizacji i powstawania gett biedy. W ten sposób mechanizm, który miał chronić spójność kulturową („nasz styl życia"), w rzeczywistości ją podkopuje, tworząc głębokie pęknięcia społeczne i strefy braku bezpieczeństwa wewnątrz państwa.

Szowinizm jest pojęciem, które wywodzi się z języka francuskiego i związane jest z postacią Nicolasa Chauvina, żołnierza napoleońskiego przedstawianego jako fanatyczny patriota, bezkrytycznie oddany cesarzowi i ojczyźnie. Z czasem termin ten zaczął funkcjonować w naukach społecznych jako określenie postawy charakteryzującej się przesadnym, często irracjonalnym uwielbieniem własnej grupy, połączonym z pogardą lub wrogością wobec innych. Współcześnie szowinizm rozumiany jest jako skrajna forma etnocentryzmu, w której jednostka lub zbiorowość nie tylko uznaje swoją kulturę, naród czy wspólnotę za lepszą, ale także aktywnie umniejsza i marginalizuje inne grupy. Jest to zjawisko o charakterze emocjonalnym i ideologicznym, które nie opiera się na racjonalnych przesłankach, lecz na silnym poczuciu lojalności wobec własnej wspólnoty. Często wiąże się ono z lękiem przed utratą tożsamości, dominacją kulturową czy zagrożeniem ze strony obcych wpływów, co sprawia, że szowinizm można traktować jako mechanizm obronny, choć w praktyce prowadzi on do konfliktów społecznych.

Szowinizm przybiera różne formy w zależności od tego, jaka sfera życia społecznego staje się jego przedmiotem. Najczęściej mówi się o szowinizmie narodowym, który polega na przekonaniu o wyższości własnej nacji nad innymi i objawia się w gloryfikacji historii, tradycji oraz kultury narodowej, często połączonej z lekceważeniem lub demonizowaniem innych wspólnot. Szowinizm opiekuńczy pojawia się przede wszystkim

jako reakcja na poczucie zagrożenia kulturowego, które w warunkach współczesnego świata jest coraz bardziej odczuwalne.

Globalizacja, migracje, rozwój mediów i technologii sprawiają, że granice kulturowe stają się płynne, a tradycyjne wzorce podlegają nieustannym przemianom. W takiej sytuacji część społeczeństw zaczyna odczuwać lęk przed utratą własnej tożsamości, co prowadzi do wzmożonej troski o zachowanie dziedzictwa narodowego. Szowinizm opiekuńczy jest więc formą obrony, która polega na nadmiernym podkreślaniu wyjątkowości własnej kultury i konieczności jej ochrony przed wpływami zewnętrznymi. Przejawia się to w praktyce poprzez krytykę obcych tradycji, sprzeciw wobec zjawisk uznawanych za zagrożenie dla spójności wspólnoty, a także postulaty ograniczenia migracji czy regulacji dotyczących języka i mediów.

W debatach publicznych można zauważyć, że osoby przyjmujące postawę szowinistyczną w tym wymiarze często argumentują, iż otwartość na inne kultury prowadzi do rozmycia własnej tożsamości i osłabienia więzi społecznych. W konsekwencji szowinizm opiekuńczy staje się narzędziem mobilizacji społecznej, które ma na celu obronę tradycji, symboli i wartości uznawanych za fundament wspólnoty. Zjawisko to ma jednak charakter dwuznaczny: z jednej strony, może sprzyjać wzmacnianiu poczucia wspólnoty i mobilizować do działań na rzecz ochrony dziedzictwa kulturowego, co w praktyce oznacza większe zainteresowanie historią, językiem czy sztuką narodową, z drugiej zaś – gdy przybiera skrajną formę, prowadzi do izolowania i wrogości wobec innych kultur, co utrudnia dialog międzykulturowy i może generować konflikty społeczne. W tym sensie szowinizm opiekuńczy jest zarówno reakcją obronną, jak i potencjalnym źródłem napięć.

Warto podkreślić, że szowinizm opiekuńczy nie jest zjawiskiem marginalnym – pojawia się w wielu krajach, zarówno w Europie, jak i poza nią, gdzie społeczeństwa mierzą się z wyzwaniami związanymi z migracją, integracją czy globalnym przepływem idei. W Polsce przejawia się on w dyskusjach o ochronie języka polskiego, tradycji narodowych czy symboli religijnych, natomiast w krajach zachodnich widoczny jest w ruchach społecznych broniących „czystości kulturowej" wobec napływu imigrantów. Szowinizm opiekuńczy, rozumiany jako szczególna forma przesadnej troski o własną kulturę i tradycję, posiada zarówno pozytywne, jak i negatywne aspekty; z jednej strony, jego obecność może być postrzegana

jako mechanizm mobilizujący wspólnotę do działań na rzecz ochrony dziedzictwa. W praktyce oznacza to większe zainteresowanie historią, językiem ojczystym, sztuką narodową czy lokalnymi zwyczajami. Postawy opiekuńcze sprzyjają wzmacnianiu więzi społecznych, budowaniu poczucia wspólnoty i dumy z własnej tożsamości; dzięki nim możliwe jest przeciwdziałanie procesom zaniku tradycji, marginalizacji języka czy utraty symboli narodowych. W tym sensie szowinizm opiekuńczy może pełnić funkcję ochronną, wspierając działania państwa i instytucji kultury, które dążą do zachowania dziedzictwa w warunkach globalizacji. Jednakże obok tych pozytywnych efektów pojawiają się również konsekwencje negatywne.

Szowinizm opiekuńczy, gdy przybiera formę skrajną, prowadzi do izolacjonizmu i zamknięcia się na dialog międzykulturowy. Nadmierne podkreślanie wyjątkowości własnej kultury może skutkować wrogością wobec innych tradycji, a nawet tworzeniem stereotypów i uprzedzeń wobec obcych. W praktyce oznacza to ryzyko konfliktów społecznych, utrudnienie w integracji migrantów czy osłabienie zdolności do współpracy międzynarodowej. Zjawisko to może także ograniczać rozwój kultury, która w naturalny sposób czerpie inspiracje z kontaktów zewnętrznych. W efekcie zamiast chronić dziedzictwo, szowinizm opiekuńczy może prowadzić do jego stagnacji i zamknięcia w schematach, które nie odpowiadają na wyzwania współczesności.

Dwuznaczny charakter szowinizmu opiekuńczego sprawia, że należy go traktować jako zjawisko wymagające równowagi. O ile umiarkowana troska o kulturę jest pożądana i wspiera bezpieczeństwo kulturowe, o tyle skrajne postawy mogą stać się źródłem napięć i zagrożeń. Współczesne społeczeństwa powinny zatem dążyć do takiego modelu ochrony kultury, który łączy troskę o własną tożsamość z otwartością na dialog i współpracę. Tylko w ten sposób możliwe jest zachowanie dziedzictwa przy jednoczesnym uczestnictwie w procesach globalnych, które choć niosą ryzyko, stanowią również szansę na rozwój i wzbogacenie kultury.

Szowinizm opiekuńczy w praktyce przejawia się w różnorodnych działaniach społecznych, politycznych i kulturowych, które mają na celu ochronę tożsamości narodowej i dziedzictwa kulturowego. W wielu krajach można zauważyć tendencję do podkreślania wyjątkowości własnej tradycji oraz krytycznego odnoszenia się do wpływów zewnętrznych. W Polsce

przykładem takiej postawy są debaty dotyczące roli języka polskiego w przestrzeni publicznej, ochrony symboli narodowych czy znaczenia tradycji religijnych w życiu społecznym. W praktyce oznacza to działania na rzecz zachowania czystości językowej, sprzeciw wobec nadmiernego zapożyczania słów obcych, a także postulaty dotyczące obecności symboli narodowych w szkołach czy instytucjach publicznych. Podobne zjawiska można zaobserwować w innych krajach europejskich, gdzie szowinizm opiekuńczy przybiera formę ruchów społecznych broniących „czystości kulturowej" wobec napływu imigrantów.

Termin ten, wprowadzony do szerszego obiegu naukowego w latach 90. XX w. przez skandynawskich badaczy Jørgena Goul Andersena i Tora Bjørklunda, opisuje swoistą hybrydę ideologiczną. Łączy on w sobie elementy typowe dla lewicy – takie jak poparcie dla silnego interwencjonizmu państwowego i rozbudowanych osłon socjalnych – z elementami prawicowego nacjonalizmu kulturowego. Jest to doktryna, która mówi „tak" dla państwa opiekuńczego, ale stawia wyraźne zastrzeżenie: jego beneficjentami mogą być wyłącznie „nasi". Fundamentem tej postawy jest przekonanie o skończoności zasobów oraz specyficznie pojmowana umowa społeczna. Klasycy myśli liberalnej, z Miltonem Friedmanem na czele, wielokrotnie wskazywali na fundamentalną sprzeczność między swobodnym przepływem osób a istnieniem państwa socjalnego. Friedmanowska teza głosi, że „nie można mieć jednocześnie otwartych granic i państwa opiekuńczego", ponieważ napływ osób niekontrybuujących do systemu (imigrantów o niskich kwalifikacjach) doprowadzi do jego załamania finansowego. Szowinizm opiekuńczy jest próbą rozwiązania tego dylematu nie poprzez likwidację socjalu (co postulowali liberałowie), ale zamknięcie granic systemu redystrybucji. Szowinizm opiekuńczy to jedna z najbardziej podstępnych form seksizmu – maskuje nierówność pozorną troską. Choć wydaje się niewinny, prowadzi do utrwalania tradycyjnych ról płciowych, ograniczania wolności kobiet i wzmacniania patriarchalnych struktur społecznych. Jego obecność w kulturze, mediach i relacjach interpersonalnych sprawia, że często pozostaje niezauważony. Zrozumienie istoty tego zjawiska stanowi kluczowy krok w kierunku budowania społeczeństwa opartego na prawdziwej równości, autonomii i wzajemnym szacunku.

Szowinizm opiekuńczy należy traktować jako zjawisko złożone, które wymaga równowagi między troską o własną tożsamość a otwartością na współpracę i wymianę kulturową. Współczesne społeczeństwa powinny dążyć do modelu bezpieczeństwa kulturowego, w którym ochrona dziedzictwa idzie w parze z umiejętnością prowadzenia dialogu międzykulturowego. Tylko w ten sposób możliwe jest zachowanie trwałości kultury w zmieniającym się świecie, bez popadania w izolacjonizm czy konflikty. Szowinizm opiekuńczy, jeśli pozostaje w granicach umiarkowanej troski, może być wartościowym elementem polityki bezpieczeństwa kulturowego, ale w formie skrajnej staje się czynnikiem destabilizującym, który utrudnia budowanie społeczeństwa otwartego i różnorodnego.

Żanna Osikowicz

J. Andersen, T. Bjørklund, *Structural Changes and New Cleavages: The Progress Parties in Denmark and Norway*, „Acta Sociologica" 1990, vol. 33, no. 3; Z. Bauman, *Obcy u naszych drzwi*, Wydawnictwo Naukowe PWN, Warszawa 2016; M. Bodziany, *Zagrożenia bezpieczeństwa kulturowego w dobie nowoczesności*, „Colloquium" 2024, t. 16, nr 3; S. Castles, M.J. Miller, *Czas migracji. Międzynarodowe przepływy ludności we współczesnym świecie*, Wydawnictwo Naukowe PWN, Warszawa 2011; G. Krzywiec, *Szowinizm po polsku. Przypadek Romana Dmowskiego*, Wydawnictwo Neriton, Warszawa, 2009; M. Lesińska, *Polityka migracyjna w obliczu kryzysu: Wnioski dla Polski*, „Studia Migracyjne – Przegląd Polonijny" 2018, nr 4(170); P. Mazur, K. Pabis-Cisowska, *Bezpieczeństwo kulturowe*, [w:] *Encyklopedia bezpieczeństwa*, t. 1: *A–C*, O. Wasiuta, S. Wasiuta (red.), Wydawnictwo Libron, Kraków 2021; W. Van Oorschot, *Making the difference in social Europe: deservingness perceptions among citizens of European welfare states*, „Journal of European Social Policy" 2006, vol. 16(1); R. Zięba, *Bezpieczeństwo międzynarodowe w XXI wieku*, Wydawnictwo Naukowe Scholar, Warszawa 2018.

ŚRODKOWOEUROPEJSKA WSPÓŁPRACA OBRONNA (ang. Central European Defence Cooperation, CEDC) stanowi nieformalny, regionalny format współpracy państw Europy Środkowej w dziedzinie bezpieczeństwa i obronności. Zainicjowany został w 2010 r. przez ministerstwa obrony Austrii, Chorwacji, Czech, Słowacji, Węgier i Słowenii. Od 2017 r. status obserwatora posiada również Polska, co pozwala jej na zaangażowanie w dyskusje bez pełnych praw decyzyjnych. CEDC funkcjonuje jako

platforma wzmacniania bezpieczeństwa subregionalnego oraz pogłębiania współpracy państw mierzących się z podobnymi wyzwaniami geostrategicznymi. Podstawowym celem formatu jest stworzenie względnie zinstytucjonalizowanej, a jednocześnie elastycznej platformy współdziałania w zakresie planowania obronnego, koordynacji działań wojskowych oraz zwiększania interoperacyjności sił zbrojnych państw członkowskich. Działania te mają na celu bardziej efektywne wykorzystanie ograniczonych zasobów narodowych.

Format CEDC charakteryzuje się elastycznością, a jego funkcjonowanie nie nakłada zobowiązań traktatowych, co odróżnia go od sformalizowanych struktur bezpieczeństwa, takich jak NATO czy Unia Europejska. Jednocześnie pełni wobec nich funkcję komplementarną, umożliwiając szybszą i mniej zbiurokratyzowaną koordynację działań w obszarze obronności o znaczeniu regionalnym. Taki model współpracy sprzyja efektywnemu reagowaniu na wspólne wyzwania bezpieczeństwa, bez naruszania suwerenności państw członkowskich. Podstawą funkcjonowania CEDC jest podejście zakładające wspólną identyfikację, rozwój oraz wykorzystanie zdolności wojskowych, którego celem jest ograniczenie dublowania struktur, redukcja kosztów oraz zwiększenie zbiorowej gotowości operacyjnej. Mechanizm ten ma szczególne znaczenie w obszarach, w których poszczególne państwa nie dysponują wystarczającą skalą zasobów do samodzielnego rozwijania pełnych zdolności obronnych.

Współpraca w ramach formatu realizowana jest na poziomie politycznym i wojskowym, obejmując m.in. konsultacje ministrów obrony, wspólne ćwiczenia wojskowe, projekty szkoleniowe, harmonizację procesów logistycznych oraz działania w zakresie zarządzania kryzysowego. Proces decyzyjny opiera się na zasadzie konsensusu pomiędzy ministrami obrony i skupia się na inicjowaniu wspólnych przedsięwzięć. CEDC nie stosuje formalnych mechanizmów głosowania ani prawa weta, a ustalenia podejmowane w ramach spotkań nie mają charakteru prawnie wiążącego. Ich realizacja odbywa się poprzez dobrowolne zobowiązania narodowe, przy zachowaniu pełnej suwerenności państw uczestniczących w zakresie prowadzenia własnej polityki obronnej. Na poziomie operacyjnym wdrażanie uzgodnień wspierane jest przez wyspecjalizowane grupy robocze. Format zorganizowany jest na zasadzie rotacyjnej prezydencji,

sprawowanej corocznie przez 1 z państw członkowskich. Zapewnia to bieżące koordynowanie działań oraz ustalanie harmonogramu współpracy, jednak bez kompetencji do ich bezpośredniego realizowania. Państwo przewodniczące odpowiada za organizację kluczowych wydarzeń, w tym 2 spotkań dyrektorów ds. polityki obronnej, z których 1 bywa rozszerzane o partnerów z Bałkanów Zachodnich, oraz corocznego spotkania ministrów obrony pełniącego funkcję najwyższego forum decyzyjnego w ramach CEDC.

Pierwsze formalne spotkanie ministrów obrony państw CEDC odbyło się 21 czerwca 2012 r. w Frauenkirchen. Podczas tego posiedzenia ministrowie potwierdzili wolę pogłębienia współpracy w obszarze łączenia zdolności wojskowych, wskazując m.in. na potencjalne wspólne projekty w zakresie obsługi i konserwacji śmigłowców, ewakuacji medycznej oraz szkoleń związanych z przeciwdziałaniem improwizowanym urządzeniom wybuchowym. Spotkanie to stworzyło fundament dla dalszego rozwoju formatu jako elastycznej, konsensualnej platformy współpracy obronnej w Europie Środkowej.

Do kluczowych obszarów aktywności i inicjatyw podejmowanych w ramach CEDC należy zaliczyć:

1. Ćwiczenia wojskowe i podnoszenie interoperacyjności sił zbrojnych państw uczestniczących – ich zasadniczym celem jest ujednolicanie procedur operacyjnych oraz synchronizacja działań wojskowych i pozawojskowych w kontekście zagrożeń o charakterze regionalnym.

   W ramach tego obszaru szczególne znaczenie mają:
   - ćwiczenia z zakresu reagowania kryzysowego – testowanie zdolności szybkiego reagowania na sytuacje nadzwyczajne, w tym migracyjne i hybrydowe;
   - współpraca w szkoleniach logistycznych i sztabowych – szczególnie w zakresie transportu i zabezpieczenia operacji wojskowych;
   - programy dotyczące koordynacji szkolenia oficerów, prowadzone m.in. przez akademie wojskowe państw członkowskich.

Ćwiczenia organizowane w ramach CEDC mają zazwyczaj charakter praktyczny i obejmują szkolenia terenowe, symulacje stanowisk

dowodzenia (Command Post Exercises) oraz warsztaty eksperckie. Ich celem jest zwiększenie koordynacji pomiędzy jednostkami wojskowymi, służbami policyjnymi oraz strażą graniczną, co odzwierciedla nacisk formatu na pragmatyczne współdzielenie zdolności przy jednoczesnym braku ponadnarodowych struktur dowodzenia. Sztandarową inicjatywą w tym zakresie jest cykl ćwiczeń COOPSEC (Cooperative Security), zapoczątkowany w celu wykorzystania doświadczeń wyniesionych z kryzysu migracyjnego lat 2015–2016. Ćwiczenia COOPSEC 17, przeprowadzone w 2017 r., obejmowały warsztaty analityczne oraz tygodniowe szkolenie terenowe, których zamierzeniem było usprawnienie koordynacji pomiędzy ministerstwami obrony w zakresie zarządzania ruchami migracyjnymi oraz wsparcia organów egzekwowania prawa w ramach ustawowych mandatów sił zbrojnych. Kraje członkowskie CEDC koncentrowały się wówczas na rozwijaniu synergii regionalnej w odpowiedzi na migracyjne szlaki przebiegające przez Europę Środkową. Kolejna edycja, COOPSEC 19, zrealizowana w 2019 r., rozszerzyła formułę ćwiczeń o udział obserwatorów z Bośni i Hercegowiny, Grecji, Czarnogóry, Macedonii Północnej, Rumunii oraz Serbii. Zarówno komponent teoretyczny, jak i praktyczny ćwiczeń ukierunkowany był na wzmocnienie międzynarodowej zdolności reagowania na różne scenariusze migracyjne. W ramach CEDC podejmowano również specjalistyczne szkolenia w zakresie operacji specjalnych, wsparcia medycznego, szkolenia pilotów oraz obrony chemicznej, biologicznej, radiologicznej i jądrowej (CBRN). Istotną inicjatywą były warsztaty eksperckie z zakresu komunikacji strategicznej (StratCom) poświęcone zwalczaniu dezinformacji i fałszywych narracji, zorganizowane 8 czerwca 2021 r. pod przewodnictwem chorwackiej prezydencji.

1. Współpraca w zakresie ochrony granic i zarządzania kryzysowego – jeden z najbardziej rozpoznawalnych obszarów aktywności formatu, który przejawia się m.in. w tworzeniu wspólnych zespołów wsparcia granicznego, delegowanych w razie potrzeby do ochrony granic państw regionu; wymianie informacji operacyjnych dotyczących ruchów migracyjnych i zagrożeń przestępczych; opracowywaniu standardów szkolenia służb mundurowych w zakresie kontroli granicznej; rozwijaniu mechanizmów koordynacji pomocy kryzysowej na granicach zewnętrznych UE oraz

przygotowywaniu projektów dotyczących budowy odporności na zagrożenia hybrydowe w odpowiedzi na rosnące zagrożenia informacyjne i cybernetyczne.

Państwa członkowskie zintensyfikowały wymianę informacji dotyczących bezpieczeństwa granic, procedur operacyjnych, a także rozwijały wspólne mechanizmy wsparcia dla działań ochronnych realizowanych głównie na szlaku bałkańskim. W tym kontekście CEDC służyła jako forum uzgadniania stanowisk w instytucjach europejskich, a także platforma współpracy praktycznej służb mundurowych.

1. Konsultacje polityczne i harmonizacja stanowisk – format odgrywa ważną rolę w kształtowaniu wspólnych stanowisk państw regionu, szczególnie w kontekście debat dotyczących bezpieczeństwa europejskiego. Obejmuje spotkania ministrów obrony, konsultacje ekspertów ds. planowania obronnego, wspólne stanowiska prezentowane na forach UE i NATO oraz dialog w obszarze planów obronnych i strategii regionalnych.
2. Współpraca logistyczna i operacyjna – obejmuje ujednolicenie procedur transportu wojskowego, wymianę zdolności logistycznych podczas ćwiczeń, prace nad wspólnymi standardami transportu lotniczego i lądowego oraz wzajemną pomoc w operacjach humanitarnych i ewakuacyjnych.
3. Projekty szkoleniowe i edukacyjne, które obejmują intensywną współpracę na poziomie szkolnictwa wojskowego, m.in.
   - organizacja seminariów i warsztatów dla młodszej kadry;
   - projekty dotyczące wspólnego szkolenia oficerów;
   - współpraca akademii wojskowych w zakresie badań nad bezpieczeństwem regionalnym.

Współpraca w ramach formatu obejmuje działania w wielu rozległych obszarach, dbając jednocześnie o rozwój zdolności kompatybilnych z instrumentami Unii Europejskiej, takimi jak Europejski Fundusz Obrony oraz Stała Współpraca Strukturalna (PESCO), przy jednoczesnym wzmacnianiu synergii UE–NATO, bez powielania funkcji realizowanych w ramach tych struktur. Przykładem jest platforma językowa CEDC, której celem jest standaryzacja szkolenia w zakresie języka wojskowego oraz zwiększenie wielojęzycznej interoperacyjności w operacjach

wielonarodowych, co wpisuje się w cele inicjatyw realizowanych w ramach PESCO. Istotnym obszarem współpracy są również projekty, które koncentrują się na specjalistycznej współpracy szkoleniowej w zakresie zdalnie pilotowanych systemów powietrznych wykorzystywanych do celów rozpoznania i nadzoru; rządowych sieci łączności służące bezpiecznej wymianie danych oraz procedur ewakuacji medycznej usprawniających logistykę w ramach wspólnych misji. CEDC rozwinęło wiele inicjatyw wspierających cele NATO w zakresie tzw. inteligentnej obrony oraz unijne koncepcje łączenia zdolności wojskowych. Stopień ich wdrażania pozostaje zróżnicowany w różnych krajach ze względu na odmienne priorytety strategiczne i możliwości budżetowe państw uczestniczących.

Początkowa faza współpracy w ramach formatu koncentrowała się przede wszystkim na wymianie informacji dotyczących planowania obronnego, koordynacji stanowisk państw Europy Środkowej w ramach instytucji europejskich oraz wzmacnianiu interoperacyjności na poziomie sztabowym. W odróżnieniu od bardziej sformalizowanych sojuszy wojskowych CEDC od samego początku akcentowało praktyczne podejście do współpracy, ukierunkowane na przeciwdziałanie zagrożeniom asymetrycznym oraz ograniczanie niestabilności regionalnej, bez tworzenia rozbudowanych struktur instytucjonalnych. Zmiana środowiska bezpieczeństwa w Europie po 2014 r., związana z aneksją Krymu, destabilizacją wschodniej flanki Unii Europejskiej oraz kryzysem migracyjnym po 2015 r., istotnie wpłynęła na pogłębienie współpracy oraz redefinicję priorytetów w ramach CEDC. Państwa członkowskie zaczęły postrzegać format nie tylko jako luźną platformę współpracy wojskowej, lecz również narzędzie wzmacniania odporności regionalnej wobec zagrożeń hybrydowych i niestabilności transgranicznej. Szczególną rolę odegrała w tym kontekście Austria, która mimo swojej tradycyjnej neutralności zintensyfikowała działania na rzecz zwiększenia bezpieczeństwa regionalnego, przy jednoczesnym zachowaniu spójności z ramami UE oraz NATO.

Kluczowym momentem rozwoju współpracy były lata 2015–2016, kiedy to masowe, nieregularne przepływy migracyjne do Europy skłoniły państwa CEDC do rozszerzenia współpracy o komponenty cywilno-wojskowe. Obejmowały one m.in. rozmieszczanie żołnierzy do patroli granicznych, budowę infrastruktury zabezpieczającej oraz wsparcie logistyczne.

Wraz z rozwojem współpracy państwa regionu, położone wzdłuż szlaku bałkańskiego, zaczęły intensyfikować koordynację w takich obszarach, jak wymiana informacji o ruchach migracyjnych, wspólne szkolenia służb granicznych, wsparcie operacji ochronnych na zewnętrznych granicach UE oraz przygotowywanie wspólnych stanowisk w europejskiej debacie nad polityką migracyjną. Od tego momentu bezpieczeństwo granic stało się jednym z kluczowych filarów działalności CEDC, obok klasycznej współpracy wojskowej. Równolegle wzmocniono dialog polityczny na szczeblu ministrów obrony oraz regularne konsultacje eksperckie, umacniając rolę CEDC jako elastycznej platformy regionalnej współpracy w zakresie bezpieczeństwa.

Współcześnie CEDC przechodzi swoistą transformację od niezobowiązującego forum konsultacyjnego w kierunku coraz bardziej operacyjnego i zorientowanego na działania formatu regionalnego. Pozostaje elastyczny i nie nakłada twardych zobowiązań wobec członków, co pozwala na szybkie reagowanie na regionalne zagrożenia bezpieczeństwa. W dalszym ciągu pełni funkcję skutecznego forum politycznych konsultacji między państwami Europy Środkowej, ale posiada też rzeczywisty wpływ m.in. na koordynację stanowisk w UE i NATO, wymianę informacji polityczno-strategicznej, budowanie regionalnego konsensusu w kwestiach migracyjnych i bezpieczeństwa granic oraz wzmacnianie pozycji państw środkowoeuropejskich w szerszych debatach europejskich. Jednocześnie w ramach formatu nie ukształtowały się stabilne struktury organizacyjne – brakuje stałego sekretariatu, wspólnego budżetu obronnego, wspólnych projektów zbrojeniowych oraz sił przygotowanych do działań pod egidą CEDC. Z tego powodu znaczenie polityczne pozostaje ograniczone do konsultacji, a nie podejmowania wiążących decyzji. Ponadto państwa członkowskie wykazują znaczące rozbieżności w ocenie i priorytetyzacji zagrożeń zewnętrznych, w szczególności agresji Rosji na Ukrainę. Pomimo zbiorowego potępienia inwazji w odbiorze niektórych państw formatu Rosja nie stanowi egzystencjalnego zagrożenia dla bezpieczeństwa regionu, np. Węgry pod rządami premiera Viktora Orbána bagatelizują bezpośrednie zagrożenie dla Europy, priorytetowo traktując stabilność gospodarczą. Również Słowacja ograniczyła pomoc wojskową dla Ukrainy i wstrzymuje się od zdecydowanych potępień rosyjskich działań hybrydowych. Ta

powściągliwość niektórych państw wynikała w dużej mierze od rosyjskich dostaw energetycznych. Podczas gdy CEDC osiąga przyrostowe sukcesy w rozwoju zdolności i dialogu regionalnym, jego skuteczność pozostaje ograniczona neutralnym statusem Austrii, rozbieżnymi priorytetami krajowymi, takimi jak nacisk Węgier na suwerenność w zakresie zamówień obronnych, oraz przewagą dwustronnych lub kierowanych przez NATO ram dla operacji na większą skalę. Czynniki te wskazują, że CEDC działa jako mechanizm uzupełniający, a nie niezależny filar obronny, podczas gdy ministerialne spotkania służą rozwiązywaniu współczesnych wyzwań, takich jak zagrożenia hybrydowe i dezinformacja.

Sabina Olszyk

CEDC Defence Ministers Discussed Hybrid Threats and Misinformation, 19.12.2020, https://www.czdefence.com/article/cedc-defence-ministers-discussed-hybrid-threats-and-misinformation (dostęp 16.12.2025); *Central European defence cooperation will increase, Oxford Analytica*, 13.09.2017, https://doi.org/10.1108/OXAN-DB213573 (dostęp 9.12.2025); *Central European Defence Cooperation*, 16.04.2021, https://www.morh.hr/en-central-european-defence-cooperation/ (dostęp 16.12.2025); P. Müller, *Europeanization and regional cooperation initiatives: Austria's participation in the Salzburg Forum and in Central European Defence Cooperation*, „OZP – Austrian Journal of Political Science" 2016, vol. 45, no. 2, https://doi.org/10.15203/ozp.1102.vol45iss2 (dostęp 16.12.2025); B. Nemeth, *Militarisation of cooperation against mass migration – the Central European Defence Cooperation (CEDC)*, „Defence & Security Analysis" 2018, vol. 34, no. 1, https://doi.org/10.1080/14751798.2018.1421401 (dostęp 15.12.2025); *The security of Central Europe in one and indivisible*, 23.09.2025, https://defence.hu/news/the-security-of-central-europe-is-one-and-indivisible.html (dostęp 16.12.2025).

T

TECHNOOPTYMIZM polega na złudnym wręcz przekonaniu, iż za każdą technologią kryje się postęp i jest to zbawienne dla rozwoju cywilizacji, pozytywnie wpływając na niemalże wszystkie aspekty ludzkiej egzystencji. Z technooptymizmem koresponduje inny trend opisywany w literaturze przedmiotu jako technosolucjonizm. Technooptymizm nie jest pojęciem skonstruowanym współcześnie, bowiem pojawił się po II wojnie światowej. Do najbardziej znanych zwolenników tego trendu zalicza się Billa Gatesa, Elona Muska czy też Marca Andreessena. Ten ostatni, inwestor z Doliny Krzemowej, 23 października 2023 r. opublikował Techno-Optimist Manifesto (tzw. manifest technooptymisty), w którym stanowczo wezwał do nieograniczonego postępu technologicznego mającego na celu pobudzenie rynków, zwiększenie produkcji energii, poprawę edukacji i wzmocnienie demokracji liberalnej. Miliarder, który dorobił się fortuny, współtworząc Mosaic i Netscape – firmę z lat 90. XX w., twórca pionierskiej przeglądarki internetowej, sam uznaje siebie za technooptymistę, twierdząc, że „nie ma takiego problemu materialnego – czy to stworzonego przez naturę, czy przez technologię – którego nie dałoby się rozwiązać za pomocą większej liczby technologii". Manifest stanowi swoistą pochwałę technologii

traktowanej w kategoriach jedynej nadziei na lepszą przyszłość dla całej ludzkości. Śmiała teza Andreessena: „Nasza cywilizacja została zbudowana na technologii. Technologia jest chwałą ludzkiej ambicji i osiągnięć, ostrzem postępu i realizacją naszego potencjału. Gloryfikowaliśmy ją przez setki lat – aż do niedawna. Jestem tutaj, aby przynieść dobre wieści. Możemy awansować na o wiele wyższy poziom życia. Mamy narzędzia, systemy, pomysły. Mamy wolę. Nadszedł czas, aby ponownie podnieść flagę technologii. Nadszedł czas, aby zostać technooptymistami", wzbudziła wiele kontrowersji i stała się przyczyną sporu w środowiskach reprezentowanych przez przeciwników cywilizacji zachodniej, którzy w technologii upatrują zagrożenie dla niemalże wszystkich dziedzin aktywności ludzkiej.

Technooptymistów cechuje bezkrytyczna wiara w nieograniczone możliwości technologii i jej pozytywny wpływ na politykę, gospodarkę, biznes i inne kluczowe dziedziny życia. Przedstawiciele podejścia zbyt optymistycznie nawołują do implementacji innowacyjnych rozwiązań, bagatelizując potencjalne konsekwencje niepewnych projektów technologicznych. Częstokroć technooptymiści zapominają, iż zarówno rozwój technologiczny, jak i przemożna rola współczesnych mediów internetowych sprzyjają rozpowszechnianiu szkodliwych treści, a sztuczna inteligencja dodatkowo ten sfalsyfikowany obraz uwiarygodnia i petryfikuje.

Krytycy technooptymizmu są zdania, iż jako stanowisko ideologiczne technooptymizm czyni interesy niektórych osób (tych, które dysponują ogromną władzą i zasobami) nadrzędnymi wobec wszystkich pozostałych jednostek i grup. Jego zwolennicy mogą celowo ignorować fakt, że większość problemów społecznych, takich jak technologia, jest dziełem ludzi. Przeciwnicy technoptymizmu stawiają również zarzut, iż zjawisko to wiąże się z pragnieniem lepszej przyszłości, przy jednoczesnym braku odpowiedzi na pytania o to, jak ta przyszłość będzie kreowana, jak będzie wyglądała i kto będzie beneficjentem tych zmian.

Niewątpliwie wdrażanie nowoczesnych technologii przyczynia się do licznych korzyści, niemniej jednak innowacyjność sama w sobie może generować konkretne zagrożenia i wyzwania dla współczesnych państw oraz społeczeństw. Analiza korzyści i strat związanych z wdrażaniem innowacyjności pozwala wyprowadzić następujące wnioski.

Po pierwsze, technologie w sposób pośredni i bezpośredni oddziałują na nasze życie prywatne oraz zawodowe, kreują sposób, w jaki wykorzystujemy czas wolny, wchodzimy w interakcje interpersonalne, modelują zachowania konsumenckie itp. Niestety coraz częściej obserwujemy zanik tradycyjnych więzi międzyludzkich spowodowany funkcjonowaniem jednostek bardziej w świecie wirtualnym niż realnym. Jest to szczególnie niebezpieczne dla dzieci oraz młodzieży, którzy z uwagi na swoje ograniczone możliwości poznawcze wykazują trudności z odróżnianiem fikcji od rzeczywistości. Natomiast w przypadku kreowaniu zachowań konsumenckich sztuczna inteligencja skłania nas często do wyborów produktów, które niekoniecznie są nam w danym momencie potrzebne, co może generować zbędne wydatki w budżetach domowych. Znane platformy internetowe, takie jak Facebook, Instagram, YouTube, Tik Tok czy też X, korzystają na szeroką skalę z rozbudowanych algorytmów rekomendacji treści: zabieg ten ma służyć utrzymaniu użytkownika oraz wygenerowaniu dużej liczby interakcji poprzez kliknięcia, „lajki", udostępnienia. W konsekwencji ma utrzymać przychody z reklam, które sponsorują funkcjonowanie platform. System polubień i wyświetleń niewiele ma wspólnego z wiarygodnością, bowiem jest sztucznie kreowany przez fałszywe konta oraz boty. Sfalsyfikowane treści uwiarygadnia technologia; dzięki sztucznej inteligencji można wygenerować fałszywe zdjęcia, nagrania, a także wypowiedzi, zatem proces rzetelnego uwiarygodnienia jest mocno ograniczony. Zdecydowane korzyści z wykorzystania technologii odnoszą przeważnie korporacje i gospodarka globalna, gdyż wszelkie innowacje napędzają ich wzrost ekonomiczny.

Po drugie, nowoczesne technologie komunikacyjne i informacyjne są skutecznym narzędziem aktywizacji jednostek w ważnych momentach dziejowych dla danej społeczności. Następuje szybka konsolidacja działań, dzięki którym możliwe stają się sprzeciw wobec niedemokratycznych decyzji władzy i jej indolencji, krytyka oraz podważanie obowiązujących porządków społecznych, a nawet naciski obywateli na struktury władzy.

Media społecznościowe zaczęły odgrywać niebagatelną rolę w wydarzeniach tzw. Arabskiej Wiosny Ludów 2010 r., polskich protestów przeciw ACTA w 2012 r., Euromajdanie 2013–2014, demonstracjach w Turcji w 2013 r., protestach żółtych kamizelek we Francji w 2018 r. Umożliwiły

szybką mobilizację tłumów, błyskawiczny przepływ informacji, co zdecydowanie zmieniło dynamikę protestów i demonstracji i przeorganizowało dotychczas funkcjonujące modele kultury politycznej. Niemniej jednak bezrefleksyjny zachwyt nad możliwościami, jakie niosą ze sobą media społecznościowe, może doprowadzić do: 1) znacznej polaryzacji społeczeństw i kreowania tzw. „baniek informacyjnych" (a niekiedy tzw. „komór echa"), sprzyjając tym samym działaniom zorganizowanej dezinformacji i falsyfikacji otaczającej nas rzeczywistości; 2) propagowania treści sensacyjnych i teorii spiskowych; 3) wzbudzania skrajnych emocji, które nie służą rzetelnej debacie publicznej. Sieci społecznościowe we współczesnym świecie mogą wspierać lub niszczyć debatę publiczną, oddziaływać na wyniki wyborów, referenda, kształtować poziom zaufania obywateli do polityków, państwa i jego instytucji. Z uwagi na destrukcyjne oddziaływanie baniek informacyjnych na mechanizmy demokracji zrozumienie logiki ich funkcjonowania warunkuje poniekąd kompetencje obywatelskie.

Po trzecie, z jednej strony, technologie zapewniają realny rozwój w kluczowych dla ludzkiej egzystencji obszarach – edukacji, polityce, biznesie, środowisku, opiece zdrowotnej, lecz zauważalny jest także ich negatywny wpływ na generowanie nierówności społecznych, marginalizowanie określonych grup, zwłaszcza seniorów czy też osób z niepełnosprawnościami. Jak słusznie zauważył amerykański socjolog Neil Postman, technologia jest jednocześnie błogosławieństwem i brzemiennym w skutkach wynalazkiem ludzkości, niosącym ze sobą mocno nieprzewidywalne i silnie oddziaływujące na egzystencję człowieka konsekwencje. W swojej publikacji *Technopol. Triumf techniki nad kulturą* zdemaskował stechnicyzowaną mentalność ludzkości owładniętą ideą, że technologia jest w stanie wyręczyć nas w myśleniu i działaniu.

Początków debaty na temat janusowego oblicza technologii możemy doszukiwać się w drugiej połowie lat 80. XX w., kiedy to niemiecki socjolog Urlich Beck wydał swoją publikację *Społeczeństwa ryzyka*. Tożsamy tok rozumowania daje się zauważyć w rozważaniach Mary Douglas, Niklasa Luhmanna, Anthony'ego Giddensa, Zygmunta Baumana oraz Brunona Latoura.

Po czwarte, największe emocje budzi fakt eksploatacji na szeroką skalę sztucznej inteligencji. W procesie nauczania SI, zapewniając

wszechstronność i szeroką dostępność, może wspomagać proces samokształcenia. Przy umiejętnym wykorzystaniu potencjału SI jesteśmy w stanie sami zdobywać wiedzę i odpowiadać na nurtujące nas pytania; natomiast z punktu widzenia edukatorów SI zapewnia personalizację nauki, rozwija umiejętność krytycznego myślenia oraz często staje się realnym wsparciem dla nauczycieli. Niestety, jakkolwiek pozytywna, odsłona chociażby ChatGPT demaskuje również konkretne zagrożenia związane z 1) potencjalną dezinformacją; 2) umniejszaniem znaczenia edukatorów; 3) rozleniwieniem poznawczym (*lazy minds*); 4) oszustwami akademickimi; 5) ryzykiem plagiatu i stronniczości; 6) wyparciem zasad etycznych; 7) nierównym dostępem do technologii; 8) osłabieniem i deficytem relacji interpersonalnych (a w konsekwencji alienacją społeczną), które coraz częściej są zastępowane przez kontakt z wirtualnym asystentem.

Podobnie jak w przypadku technosolucjonizmu, do którego należy podchodzić z rezerwą, technooptymizm również wymaga racjonalnego podejścia opartego na rzetelnych analizach otaczającej nas rzeczywistości i potencjału ludzkiego, bowiem rozwiązanie naglących problemów współczesnego świata to proces kompleksowy, uwzględniający nie tylko zastosowanie innowacji. Zdecydowanie obranie postawy technooptymisty, który usilnie wierzy w technologiczne rozwiązania problemów globalnych, jest wygodne i uzasadnione, zwłaszcza jeśli znajdujemy się w gronie najbogatszych ludzi na świecie i posiadamy realne możliwości uzyskania profitów z branż technologicznych.

Julia Anna Gawęcka

S. Kuruliszwili, *Technologie generatywnej sztucznej inteligencji – nowe perspektywy i nowe wyzwania edukacyjne*, „Forum Pedagogiczne" 2024, t. 14, nr 2.1; M. Lakomy, *Od „arabskiej wiosny" do powstania „lajków" w kontekście współpracy Federacji Rosyjskiej i Unii Europejskiej*, „Przegląd Polityczny" 2013; N. Postman, T*echnopol. Triumf techniki nad kulturą*, Muza, Warszawa 2004; A. Przegalińska, P. Oksanowicz, *Sztuczna inteligencja. Nieludzka, arcyludzka*, Społeczny Instytut Wydawniczy Znak, Kraków 2020; *Społeczny wymiar technologii. Repertuary ryzyka i emancypacyjne nadzieje*, https://sotechlab.agh.edu.pl/wp-content/uploads/2023/11/Raport-Spoleczny-wymiar-technologii-2.pdf (dostęp 27.01.2026); Techno-Optimist Manifesto, https://a16z.com/the-techno-optimist-manifesto/ (dostęp 28.01.2026).

TECHNOSOLUCJONIZM – zjawisko charakterystyczne dla XX i XXI w. Technooptymizm polega na złudnym wręcz przekonaniu, iż za każdą technologią kryje się postęp, natomiast technosolucjonizm odnosi się do przeświadczenia, iż wszelkie problemy ludzkość jest w stanie rozwiązać, wykorzystując innowacje technologiczne. Technosolucjonizm odnosi się do procesu myślowego, zgodnie z którym wszystkie problemy społeczne (związane z bezpieczeństwem, zdrowiem, transportem, edukacją czy też środowiskiem) można rozwiązać, udostępniając jednostkom konkretne rozwiązania technologiczne.

Marta Chalimoniuk-Nowak – ekspertka ds. strategii, innowacji i bezpieczeństwa, słusznie wskazuje na niezrozumiały trend bezrefleksyjnej implementacji narzędzi sztucznej inteligencji (SI) w takich sektorach, jak chociażby administracja publiczna i instytucje państwowe. W opinii Chalimoniuk-Nowak takie nieprzemyślane poczynania, niepoprzedzone obligatoryjną analizą stopnia utylitarności i poziomu bezpieczeństwa zastosowania rozwiązań SI, ich przemożnego wpływu na kulturę organizacji czy też kompetencji cyfrowych jednostek oraz jakości danych wejściowych, są zgubne i mogą prowadzić do nieodwracalnych problemów w funkcjonowaniu poszczególnych podmiotów. W konsekwencji dochodzi do zatracenia orientacji przez użytkowników i tworzenia błędnego postrzegania rzeczywistości.

Na gruncie polskim obserwujemy niestety deficyt wyważonych dyskusji nad wpływem i możliwościami wykorzystania technologii, a w zamian obserwujemy wykrystalizowanie się 2 przeciwstawnych obozów – bezrefleksyjnych zwolenników technosolucjonizmu oraz zagorzałych przeciwników wszelkich innowacyjnych rozwiązań – postawy technofobiczne czy też antytechowe. O ile pierwsza grupa prezentuje poglądy zgoła bezkrytyczne i utożsamiające chociażby sztuczną inteligencję ze zbawiennym wpływem na ludzką egzystencję, o tyle przedstawiciele drugiej obrali krytyczną narrację, upatrując w technologii główną przyczynę nadmiernej polaryzacji współczesnych społeczeństw, a także innych istotnych problemów. Zagadnienia korzystania z innowacji technologicznych, zwłaszcza sztucznej inteligencji, budzą zatem współcześnie skrajne emocje, co nie ułatwia rzetelnych analiz tych istotnych dla funkcjonowania państwa i społeczeństwa kwestii. W tym miejscu wydaje się brakować obligatoryjnej

opinii przedstawicieli kolejnego poglądu, mianowicie – technorealizmu, który w sposób bardziej pragmatyczny i wyważony analizuje rolę innowacji technologicznych w konkretnych obszarach działalności człowieka.

Pojęcie technosolucjonizmu zostało wyprowadzone z terminu solucjonizm w 2013 r. i spopularyzowane przez amerykańskiego badacza Evgeny'ego Morozova. Technosolucjonizm prezentuje przekonanie, że wszystkie problemy mają naturę inżynieryjną, zatem należy je rozwiązać, wykorzystując innowacje technologiczne. Morozov w swojej publikacji z 2010 r. *The Net Delusion* argumentował, że entuzjaści technologii (tzw. „cyberutopijni") przeceniają wyzwalający się potencjał internetu. Publikacja z 2013 r. *To Save Everything, Click Here: The Folly of Technological Solutionism* stanowi kontynuację tego nurtu, prezentując polemiczną krytykę tych, którzy zbyt łatwo przyjmują technologię cyfrową jako narzędzie wolności i demokracji.

Warto nadmienić, iż Morozow opublikował swoje przemyślenia w przełomowym momencie w historii technologii cyfrowej i internetu, zatem w czasie szczególnego wzrostu zainteresowań cyfryzacją i jej konkretnymi zastosowaniami w różnych obszarach aktywności ludzkiej. Coraz większa część populacji globalnej korzystała ze smartfonów, a w wielu sektorach przedmioty codziennego użytku, podłączone do sieci internetowej, stały się normalnością. Nowe oblicze zastosowań technologicznych, z uwagi na pojawiające się w latach 2007–2012 kryzysy gospodarcze i społeczne, przewartościowały niejako kierunki i style prowadzenia polityk w poszczególnych państwach, zwłaszcza że w kwestiach rozwiązywania dylematów społecznych i socjalnych rządy wykazywały daleko idącą indolencję. Nawet w państwach uchodzących za mocarstwa światowe (w tym także w Stanach Zjednoczonych Ameryki) dotychczas prowadzona polityka publiczna okazała się niewystarczająca w obliczu pojawiających się problemów. W rezultacie firmy technologiczne z kalifornijskiej Doliny Krzemowej, w odpowiedzi na rosnącą bezradność instytucji państwowych, zaczęły pozycjonować się na nowych rynkach z ambicjami społecznymi, proponując rozwiązanie spornych kwestii społecznych z użyciem gotowych, niedrogich i łatwych do implementacji narzędzi cyfrowych. Zatem w obszarach takich jak zdrowie, bezpieczeństwo czy też ochrona środowiska z entuzjazmem zaczęto wykorzystywać udogodnienia oferowane

przez nowoczesne technologie, co w konsekwencji upowszechniło trend, zgodnie z którym kwestie społeczne zostały sprowadzone do aspektów czysto technicznych. Od tego momentu firmy sektora prywatnego przejęły zadania zarezerwowane dotychczas dla administracji publicznej, co radykalnie zmieniło charakter i cel usług oraz wsparcia dostępnego w rozwiązywaniu problemów społecznych.

Prywatyzacja rozwiązywania problemów społecznych i środowiskowych ma również swoje ciemne strony. Po pierwsze, jest w dużym stopniu uzależniona od wypłacalności oferowanych usług i docelowych odbiorców. Opracowywane technologie muszą opierać się na rentownych modelach biznesowych, jednak w przypadku poważnych cięć budżetowych konieczne jest pobieranie opłat od beneficjentów za świadczone im usługi, co z kolei może prowadzić do wykluczenia osób najbardziej narażonych bądź poszukiwania alternatywnych źródeł finansowania, a w perspektywie – czasu komercjalizacji danych gromadzonych przez usługodawców. Ponadto tak rozumiana prywatyzacja sprowadza się do nadmiernego rozdrobnienia zakresu usług i oznacza także trudności w ich weryfikacji oraz ocenie. Po drugie, wdrażanie technosolucjonizmu doprowadziło do powszechnego zjawiska pociągania jednostek do odpowiedzialności za problemy społeczne i środowiskowe, przy jednoczesnym zdejmowaniu odpowiedzialności z rządów, a czasem nawet legitymizowania ich braku zaangażowania. W 2011 r. mieszkańcy La Courneuve (region Île-de-France we Francji) zostali wezwani przez lokalnych radnych do ograniczenia zużycia energii wszelkimi możliwymi sposobami – decyzja ta wywołała falę niezadowolenia. Radni zezwolili na utworzenie w regionie dużej liczby centrów przechowujących dane cyfrowe na temat wysokiego zużycia energii i dążących do nasycenia energią w celu utrzymania konkurencyjności.

Można zatem śmiało stwierdzić, że ma miejsce tzw. inżynieria problemów społecznych. Technosolucjonizm opiera się na sprowadzeniu złożonego, wieloczynnikowego problemu społecznego (w zakresie np. bezpieczeństwa, sprawiedliwości, edukacji, zdrowia itp.) do problemu mierzalnego, który można modelować. Jest to proces złudny i pozbawiony sensu, bowiem w takim przypadku celem jest jedynie efektywne rozwiązanie konkretnego problemu, pozbawione obligatoryjnej analizy przyczyn źródłowych, co w konsekwencji uniemożliwia podjęcie kompleksowych

działań. Ponadto wyrwane z kontekstu w ten sposób proponowane rozwiązania generują ryzyko oderwania od rzeczywistości, co skutkuje aktywnością nieadekwatną do pojawiających się problemów.

Technosolucjonizm w przypadku sztucznej inteligencji przejawia się głównie w przeświadczeniu, iż wystarczająca liczba danych i algorytmy uczenia maszynowego są w stanie rozwiązać wszystkie problemy. Jednak, jak podkreślał Morozov, zwolennicy technosolucjonizmu zapominają o kwestiach bezpieczeństwa informacji i wieloaspektowości problemów ludzkiej egzystencji, co w konsekwencji podważa niejako potencjał tego zjawiska.

Nadzieją na racjonalną eksploatację możliwości sztucznej inteligencji może być niechęć do posiłkowania się SI w życiu prywatnym, zwłaszcza w kontekście zdrowia, oraz świadomość konieczności uwzględniania aspektów etycznych.

Należy również podkreślić, iż sztuczna inteligencja rewolucjonizuje oblicze działań wojennych i systemów obronnych we współczesnym świecie. Technologie oferowane szeroko przez SI znajdują zastosowanie w wyposażeniu armii mocarstw globalnych oraz stają się coraz częściej kluczowym elementem strategii militarnych współczesnych państw. Autonomiczne systemy uzbrojenia, zaawansowane sieci cyberbezpieczeństwa, systemy rozpoznania i obserwacji, a także logistyka i inteligentne zarządzanie łańcuchami dostaw to tylko niektóre egzemplifikacje efektywnego wykorzystania SI, co zdecydowanie zwiększa możliwości operacyjne współczesnych sił zbrojnych.

O postępującej transformacji technologicznej w obszarze zbrojeń świadczą inwestycje globalne w wojskowe zastosowania SI, które w 2024 r. wynosiły 9,31 mld dolarów. Szacuje się, że do 2030 r. wydatki te mogą osiągnąć wartość 19,29 mld dolarów, co zapewnia 13% wzrostu rocznie. Ameryka Północna ma znaczący udział w rynku sztucznej inteligencji wykorzystywanej w armii, odpowiadając za 32,8% przychodów w 2024 r. Prawdopodobnie rynek sztucznej inteligencji w sektorze militarnym w regionie Azji i Pacyfiku będzie rósł najszybciej ze wszystkich skumulowanych rocznych wskaźników wzrostu inwestycji (Compound Annual Growth Rate, CAGR) w latach 2025–2030.

Trend ten jest charakterystyczny dla rządów poszczególnych państw na całym świecie, które inwestują znaczne środki w najnowocześniejsze

technologie, aby zwiększyć wydajność, precyzję i efektywność systemów obronnych. Rozwój wyspecjalizowanych układów scalonych SI, zaprojektowanych do obsługi intensywnych potrzeb obliczeniowych w zastosowaniach wojskowych, dodatkowo przyspiesza tę tendencję. Wspomniane układy umożliwiają podejmowanie decyzji w czasie rzeczywistym, szybsze przetwarzanie danych i płynną integrację SI z operacjami obronnymi, co czyni je nieodzownymi w nowoczesnej walce.

Ponadto rosnące stosowanie dużych zbiorów danych (*big data*) w sektorze obronnym wpływa na sposób analizowania i reagowania na potencjalne zagrożenia. Analityka dużych zbiorów danych, oparta na sztucznej inteligencji, usprawnia gromadzenie informacji wywiadowczych, możliwości predykcyjne i planowanie operacyjne, zapewniając bardziej proaktywne podejście do bezpieczeństwa narodowego. Ciekawy jest również fakt rosnących inwestycji sektora prywatnego w badania, które napędzają innowacje, prowadząc do rozwoju autonomicznych dronów, narzędzi cyberbezpieczeństwa opartych na SI oraz systemów robotycznych. Z racji rosnących napięć geopolitycznych, konfliktów transgranicznych i potrzeby zapewnienia przewagi technologicznej państwa podejmują także wysiłki implementacji sztucznej inteligencji w swoich strategiach obronnych, umacniając tym samym rolę w kształtowaniu przyszłości współczesnych operacji wojskowych.

Szkolenia i symulacje, łączące zasady inżynierii systemowej i oprogramowania, mają niebagatelne znaczenie w przygotowywaniu żołnierzy do operacji wojskowych poprzez realistyczne modele i scenariusze. Armia amerykańska inwestuje w zaawansowane technologie, takie jak rzeczywistość wirtualna, rozszerzona czy mieszana, aby udoskonalić szkolenie piechoty, czyniąc je bezpieczniejszym i skuteczniejszym. Immersyjne technologie pozwalają żołnierzom ćwiczyć złożone scenariusze bojowe, wzmacniając gotowość indywidualną i zespołową. Ponadto oczekuje się, że rosnące wykorzystanie cyberbezpieczeństwa opartego na sztucznej inteligencji w ochronie systemów wojskowych doprowadzi do dalszej integracji sztucznej inteligencji w sektorze militarnym, zwiększając jej rolę zarówno w szkoleniu, jak i obronie przed ewoluującymi cyberzagrożeniami. Pomimo rosnącego zainteresowania wdrażaniem nowoczesnych technologii w sektorze obronnym bezrefleksyjne podejście technosolucjonizmu do

omawianej problematyki może generować liczne problemy, naruszając tym samym architekturę bezpieczeństwa globalnego i regionalnego.

Podsumowując rozważania, technosolucjoniści w swoich wizjach wykazują się zbytnią ignorancją wobec licznych kwestii o fundamentalnym znaczeniu dla naszej egzystencji. Prezentowane postawy mogą powodować, iż pomijamy wiele aspektów ludzkiego doświadczenia, ograniczając się do maszynowego, bazującego głównie na sztucznej inteligencji, sposobu percepcji otaczającej nas rzeczywistości. Adekwatna do zaprezentowanych przemyśleń okazuje się konstatacja Walkera Percy'ego: „Żyjesz w szalonych czasach – bardziej szalonych niż zwykle, bo mimo wielkiego postępu naukowego i technologicznego człowiek nie ma zielonego pojęcia, kim jest ani co robi".

Julia Anna Gawęcka

Artificial Intelligence In Military Market (2025–2030), https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-military-market-report (dostęp 28.01.2026); S. Kuruliszwili, *Technologie generatywnej sztucznej inteligencji – nowe perspektywy i nowe wyzwania edukacyjne*, „Forum Pedagogiczne" 2024, t. 14, nr 2.1; M. Lakomy, *Od „arabskiej wiosny" do powstania „lajków" w kontekście współpracy Federacji Rosyjskiej i Unii Europejskiej*, „Przegląd Polityczny" 2013, nr 2; E. Morozov, *The Net Delusion. How not to Liberate the World*, Penguin Books Ltd., Londyn 2012; E. Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, PublicAffairs, New York 2013; https://www.publicbooks.org/the-folly-of-technological-solutionism-an-interview-with-evgeny-morozov/ (dostęp 22.01.2026); W. Percy, *Lost in the Cosmos: The Last Self-Help Book*, Farrar, Straus & Giroux, New York 1983; N. Postman, *Technopol. Triumf techniki nad kulturą*, Muza, Warszawa 2004; A. Przegalińska, P. Oksanowicz, *Sztuczna inteligencja. Nieludzka, arcyludzka*, Społeczny Instytut Wydawniczy Znak, Kraków 2020; H. Rarot, *Technorealizm wobec społecznych konsekwencji techniki*, „Kultura i Wartości" 2024, nr 37; *Społeczny wymiar technologii. Repertuary ryzyka i emancypacyjne nadzieje*, https://sotechlab.agh.edu.pl/wp-content/uploads/2023/11/Raport-Spoleczny-wymiar-technologii-2.pdf (dostęp 27.01.2026).

TRAKTATY O OGRANICZENIU ZBROJEŃ STRATEGICZNYCH (ang. Strategic Arms Limitation Treaty, SALT) stanowiły pierwszy kompleksowy i skoordynowany wysiłek 2 supermocarstw: Stanów Zjednoczonych

i Związku Radzieckiego, mający na celu zahamowanie dynamiki wyścigu technologicznego i ilościowego w zakresie broni jądrowej oraz systemów jej przenoszenia. Wypracowane w czasie zimnej wojny, w warunkach głębokiej nieufności i wzajemnej rywalizacji, porozumienia SALT zapoczątkowały proces, który stopniowo przekształcił logikę militarnego konfrontowania się mocarstw w założenia strategicznej stabilizacji, przyczyniając się do stworzenia podstaw nowoczesnej architektury kontroli zbrojeń. Rozmowy SALT I i SALT II nie były traktatami *sensu stricto*, lecz wielostronnymi pakietami dokumentów obejmującymi zarówno umowy o charakterze prawnomiędzynarodowym, jak i porozumienia techniczne oraz polityczne deklaracje dotyczące zasad wzajemnych relacji.

Geneza inicjatywy sięga doświadczeń pierwszych dekad zimnej wojny, w szczególności kryzysu kubańskiego z 1962 r., który unaocznił obu stronom zimnowojennej rywalizacji realne ryzyko przypadkowej lub eskalacyjnej wojny nuklearnej zdolnej doprowadzić do globalnej katastrofy. Kryzys ten stał się przełomem nie tylko politycznym, lecz także psychologicznym. Przywódcy USA i ZSRR doszli do wniosku, że dalsze zwiększanie potencjału strategicznego bez wprowadzenia mechanizmów ograniczających prowadzi do sytuacji niekontrolowanej, a każdy kolejny krok w wyścigu zbrojeń zwiększa prawdopodobieństwo błędnej interpretacji działań przeciwnika. W latach 60. pojawiły się dodatkowe czynniki sprzyjające negocjacjom w postaci zwiększenia przejrzystości zapewnianej przez rozwój satelitarnych środków rozpoznania, zmiany klimatu politycznego w kierunku odprężenia oraz rosnących kosztów utrzymania strategicznych programów zbrojeniowych.

Rozmowy SALT I rozpoczęły się 17 listopada 1969 r. w Helsinkach, dając początek kilkuletniemu procesowi negocjacyjnemu, który objął 7 rund prowadzonych w Helsinkach i Wiedniu. Ich pierwszym wyzwaniem było ustalenie zakresu rozmów i wspólnego języka pojęć, ponieważ strony posługiwały się odmiennymi definicjami uzbrojenia strategicznego. Dla ZSRR pod terminem „broń strategiczna" rozumiano wszelkie środki ofensywne zdolne dosięgnąć terytorium przeciwnika, podczas gdy USA wiązały ją z międzykontynentalnymi systemami przenoszenia ładunków jądrowych. Różnica ta miała znaczenie praktyczne, ponieważ Amerykanie dysponowali wysuniętymi bazami i rakietami o zasięgu poniżej 5500 km

umieszczonymi w Europie, co dawało im istotną przewagę operacyjną, natomiast ZSRR opierał się głównie na rakietach lądowych ICBM o większym zasięgu. Już na tym etapie było jasne, że negocjacje będą obciążone asymetrią struktur sił obu stron.

Początkowe rozmowy dotyczyły 2 kluczowych obszarów, czyli ograniczenia systemów ofensywnych, obejmujących międzykontynentalne rakiety balistyczne (ICBM), rakiety balistyczne okrętów podwodnych (SLBM) oraz strategiczne lotnictwo bombowe, a także defensywnych – przede wszystkim obrony przeciwrakietowej (ABM). Strona amerykańska dążyła do wprowadzenia limitów ilościowych i zakazu konstruowania nowych form uzbrojenia, zwłaszcza rakiet wyposażonych w głowice MIRV, zdolnych do niszczenia wielu celów podczas 1 lotu. ZSRR koncentrował się natomiast na kwestii ograniczenia rozmieszczenia amerykańskiej broni nuklearnej w Europie oraz zagwarantowania sobie możliwości obrony kluczowych ośrodków politycznych, przede wszystkim Moskwy.

Znaczącym czynnikiem utrudniającym negocjacje była wzajemna nieufność, podsycana przez propagandę zimnowojenną, czego przykładem jest wystąpienie Leonida Breżniewa w Charkowie w 1970 r. Breżniew deklarował gotowość do porozumień, jednocześnie ostrzegając, że ZSRR odpowie zwiększeniem własnych sił na każdą próbę uzyskania przewagi militarnej przez USA. Te sprzeczne sygnały były charakterystyczne dla epoki, w której gesty polityczne nakładały się na równoległe działania zbrojeniowe, a negocjacje przebiegały w cieniu demonstracji siły.

W konsekwencji prowadzonych rozmów już w 1971 r. podpisano 2 pierwsze dokumenty towarzyszące SALT I, czyli Porozumienie w sprawie środków zmierzających do zmniejszenia niebezpieczeństwa wybuchu wojny nuklearnej oraz Porozumienie w sprawie udoskonalenia linii bezpośredniej łączności między USA a ZSRR. Miały one przede wszystkim charakter prewencyjny i techniczny – regulowały zasady powiadamiania o incydentach, testach rakietowych oraz sytuacjach potencjalnie prowadzących do eskalacji, a także rozwijały tzw. gorącą linię utworzoną w 1963 r., wzmacniając system szybkiej komunikacji między Moskwą a Waszyngtonem. Stanowiło to pierwszą próbę budowania zaufania między stronami, a jednocześnie krok w kierunku stabilizacji nuklearnej.

Kulminacja rozmów nastąpiła w maju 1972 r., podczas spotkania prezydenta Richarda Nixona z Breżniewem w Moskwie. Właśnie wtedy podpisano 2 kluczowe dokumenty, czyli Układ o ograniczeniu systemów obrony przeciwrakietowej (ABM Treaty) oraz Tymczasowe porozumienie o niektórych środkach dotyczących ograniczenia strategicznych zbrojeń ofensywnych. Oba te akty utworzyły fundament traktatowej architektury SALT I.

Układ o ograniczeniu systemów obrony przeciwrakietowej (ABM Treaty), podpisany 26 maja 1972 r., stanowił fundamentalny element SALT I i był pierwszym w historii prawnomiędzynarodowym dokumentem wprost ograniczającym rozwój technologii obronnych w interesie zachowania strategicznej stabilności. Jego główna zasada zakładała, że żadne z mocarstw nie może stworzyć systemu obrony przeciwrakietowej na tyle rozbudowanego, aby podważyć logikę wzajemnego gwarantowanego zniszczenia, czyli doktryny strategii wojskowej MAD. W myśl układu każda ze stron mogła utrzymywać jedynie **2** systemy ABM: chroniący stolicę i wybrane pole startowe rakiet strategicznych. W 1974 r. dodatkowy protokół ograniczył tę liczbę do **1** systemu, co wynikało zarówno z kosztów, jak i obaw o możliwe destabilizujące skutki wprowadzenia skutecznej obrony przeciwrakietowej. USA zdecydowały się utrzymywać system Safeguard służący ochronie wyrzutni ICBM w Grand Forks, natomiast ZSRR rozwinął system chroniący Moskwę. Obie konstrukcje miały znaczenie bardziej symboliczne niż militarne, podkreślając, że rdzeniem stabilności strategicznej pozostaje nie obrona, lecz odstraszanie.

Równolegle podpisane *Tymczasowe porozumienie o ograniczeniu strategicznych zbrojeń ofensywnych* (Interim Agreement) miało charakter czasowy i obowiązywało przez 5 lat; ograniczało liczbę rozmieszczonych rakiet strategicznych, a USA i ZSRR zobowiązały się do zamrożenia liczby wyrzutni ICBM na poziomie istniejącego stanu, a także ograniczenia rozwoju wyrzutni SLBM i ich nosicieli. Porozumienie nie obejmowało jednak kluczowej kwestii, czyli rozwijanej przez obie strony technologii MIRV. Było tak, ponieważ Stany Zjednoczone były w znacznie bardziej zaawansowanej fazie jej rozwoju, co oznaczało, że mimo ograniczeń ilościowych systemów przenoszenia ich potencjał rażenia mógł rosnąć niemal nieograniczenie. Tę asymetrię wskazywano w literaturze jako największą słabość

SALT I i 1 z powodów, dla których ZSRR dążył w późniejszych rozmowach do uzyskania formalnych limitów obejmujących także ładunki MIRV.

SALT I, choć przełomowy, miał charakter częściowy i otwierał drogę do dalszych, znacznie trudniejszych negocjacji, które miały doprowadzić do podpisania pełnego traktatu ograniczającego rozwój i rozmieszczanie strategicznych systemów ofensywnych. Rozmowy SALT II rozpoczęto w listopadzie 1972 r., niedługo po wejściu w życie SALT I. Atmosfera polityczna sprzyjała kontynuacji dialogu: okres odprężenia (*détente*) osiągnął apogeum, a obie strony wykazywały wolę ograniczenia kosztownych programów strategicznych. Niemniej technologiczna i doktrynalna ewolucja sił jądrowych znacznie skomplikowała negocjacje. W latach 70. oba państwa rozwijały nowe typy rakiet, bardziej precyzyjne systemy naprowadzania, zaawansowane głowice MIRV oraz nowoczesne platformy przenoszenia w postaci okrętów podwodnych klasy *Ohio*, radzieckich rakiet R-36M, bombowców Tu-22M, a to podważało dotychczasowe modele równowagi strategicznej.

Kluczowym problemem SALT II stało się więc nie tylko ograniczenie liczby wyrzutni, lecz także ujęcie w limitach *jakości* i *zdolności rażenia* systemów strategicznych. Negocjacje objęły m.in. ograniczenia liczby systemów MIRV, limity ogólnej liczby środków przenoszenia (ICBM, SLBM, bombowców strategicznych), zakaz budowy nowych typów rakiet balistycznych, ograniczenia w testowaniu mobilnych systemów rakietowych oraz konieczność ustalenia jednolitych zasad weryfikacji przestrzegania traktatu. Stany Zjednoczone szczególny nacisk kładły na wprowadzenie skutecznych mechanizmów kontroli, opartych na narodowych środkach technicznych (NST), takich jak satelity rozpoznawcze, co ZSRR początkowo kwestionował. Był to jednak warunek konieczny dla utrzymania przejrzystości strategicznej i zapobieżenia ryzyku ponownego wyścigu zbrojeń.

Sytuacja międzynarodowa istotnie wpłynęła na przebieg negocjacji. W drugiej połowie lat 70. relacje radziecko-amerykańskie zaczęły ulegać pogorszeniu. Z jednej strony, wynikało to z ogólnych napięć geopolitycznych (m.in. kwestii praw człowieka, sytuacji w Afryce, rosnącej aktywności radzieckiej floty), z drugiej zaś – obaw administracji amerykańskiej dotyczących faktycznego zwiększania przez ZSRR potencjału

ofensywnego pomimo trwających rozmów. Niemniej jednak u stron wciąż istniało przekonanie, że całkowite zerwanie rozmów doprowadziłoby do powrotu niekontrolowanej eskalacji, co byłoby politycznie i ekonomicznie niekorzystne.

W 1979 r. zakończono prace nad traktatem SALT II, który miał stać się pierwszym trwałym, pełnym porozumieniem regulującym rozwój strategicznych systemów ofensywnych. Dokument podpisali 18 czerwca 1979 r. w Wiedniu prezydent Jimmy Carter i sekretarz generalny Leonid Breżniew. Układ przewidywał m.in. limit 2400 strategicznych środków przenoszenia dla każdej ze stron, ograniczenie liczby systemów MIRV do 1320 oraz zakaz tworzenia nowych typów rakiet balistycznych. Ograniczenia te miały charakter zarówno ilościowy, jak i jakościowy, a traktat po raz pierwszy odnosił się wprost do zaawansowanych technik przenoszenia głowic nuklearnych.

W momencie podpisania SALT II wydawał się ukoronowaniem dekady wysiłków dyplomatycznych i logiczną kontynuacją SALT I, jednak jego przyszłość została gwałtownie przekreślona przez wydarzenia międzynarodowe, a przede wszystkim radziecką interwencję w Afganistanie w grudniu 1979 r. Agresja ta doprowadziła do dramatycznego załamania *détente* i uniemożliwiła ratyfikację traktatu przez Senat USA. Stany Zjednoczone formalnie wycofały wniosek o ratyfikację, lecz obie strony przez kilka kolejnych lat deklarowały zamiar przestrzegania jego postanowień.

Znaczenie traktatów SALT dla systemu bezpieczeństwa międzynarodowego polegało przede wszystkim na tym, że po raz pierwszy w historii rywalizacji nuklearnej 2 supermocarstw udało się przejść od logiki nieograniczonej konkurencji do kontrolowanego ograniczania potencjałów strategicznych. Choć SALT I nie redukował realnie liczby głowic jądrowych, a SALT II nie wszedł formalnie w życie, obie inicjatywy doprowadziły do wprowadzenia liczbowych i jakościowych limitów, które ustabilizowały rywalizację i stworzyły przewidywalne ramy dla dalszych działań. Ich istota polegała nie tylko na ustanowieniu konkretnych pułapów ilościowych, lecz także uznaniu, że z punktu widzenia strategicznej stabilności całkowita swoboda zbrojeń jest nie tylko kosztowna, lecz wręcz niebezpieczna. W literaturze przedmiotu niejednokrotnie podkreśla się, że traktaty SALT I i SALT II zakotwiczyły w myśleniu elit politycznych

USA i ZSRR przekonanie, iż bezpieczeństwo może wynikać z *wzajemnego* ograniczenia, a nie wyłącznie jednostronnego dążenia do przewagi.

Wprowadzenie mechanizmów ograniczeń na systemy obrony przeciwrakietowej miało fundamentalne konsekwencje doktrynalne. Układ ABM formalnie utrwalił doktrynę wzajemnie gwarantowanego zniszczenia, czyli wspomnianej wcześniej doktryny MAD, jako podstawę stabilności nuklearnej. Ograniczenie możliwości stworzenia swoistej tarczy chroniącej przed odwetem przeciwnika oznaczało akceptację założenia, że bezpieczeństwo paradoksalnie wynika z *wzajemnej wrażliwości* na uderzenie nuklearne. W tym sensie SALT, a zwłaszcza ABM Treaty, nie tylko modyfikował strukturę sił, lecz także sankcjonował określony sposób myślenia o równowadze strategicznej. W konsekwencji traktaty te ograniczyły zapędy na przeprowadzenie pierwszego uderzenia (*first strike*), ponieważ żadna ze stron nie mogła liczyć na pełne zneutralizowanie odpowiedzi przeciwnika za pomocą rozwiniętego systemu obronnego.

Jednocześnie traktaty SALT ujawniły wiele problemów, które stały się przedmiotem krytyki. Po pierwsze, nie rozwiązywały kwestii jakościowej ewolucji uzbrojenia, a zwłaszcza rozwoju technologii MIRV oraz wzrostu precyzji rakiet balistycznych. Ograniczając nośniki, a nie liczbę głowic, otwierały pole do tzw. wyścigu w głąb, w którym każda rakieta stawała się nośnikiem z coraz większymi możliwościami uderzeniowej. Po drugie, SALT nie obejmował znacznej części arsenału średniego zasięgu, w tym systemów rozmieszczonych w Europie, co z punktu widzenia państw NATO oraz sojuszników ZSRR tworzyło wrażenie niepełności i asymetrii. Po trzecie, mechanizmy weryfikacji, oparte na narodowych środkach technicznych, choć przełomowe, pozostawiały margines niepewności co do dokładnych parametrów posiadanych przez przeciwnika systemów. Stąd w debacie strategicznej w USA pojawiały się okresowo głosy podważające wiarygodność zobowiązań radzieckich oraz sens dalszych ograniczeń.

Pomimo opisanych zastrzeżeń SALT wytworzył instytucjonalne i polityczne podłoże dla kolejnych etapów kontroli zbrojeń. Ustanowione w ramach SALT I formy dialogu, takie jak Stała Komisja Konsultacyjna ds. ABM czy regularne konsultacje na szczeblu eksperckim, stały się wzorem dla późniejszych mechanizmów weryfikacyjnych. Doświadczenia z negocjacji SALT II, choć formalnie niezakończonych ratyfikacją, dostarczyły

szczegółowej wiedzy o tym, jak konstruować kompleksowe porozumienia obejmujące zarówno ilościowe, jak i jakościowe parametry sił strategicznych. W praktyce wiele rozwiązań technicznych, definicyjnych i weryfikacyjnych, wypracowanych w trakcie SALT, zostało wprost przejętych i rozwiniętych w ramach traktatów START.

Przejście od SALT do START oznaczało ewolucję od *ograniczania wzrostu* potencjału do jego *realnej redukcji*. Podpisany w 1991 r. traktat START I przewidywał znaczące obniżenie liczby rozmieszczonych głowic i środków przenoszenia, a START II (1993) oraz późniejsze porozumienia, w tym New START (2010), kontynuowały ideę wcześniejszych porozumień. Nie byłoby to możliwe bez wcześniejszego oswojenia politycznych elit z ideą, że ogólny poziom uzbrojenia strategicznego może, a nawet powinien, podlegać wspólnie uzgodnionym ograniczeniom. W tym sensie SALT pełnił funkcję swoistego laboratorium kontroli zbrojeń, w którym testowano zarówno pojęcia, jak i mechanizmy polityczne konieczne do prowadzenia długotrwałego dialogu rozbrojeniowego.

Znaczącym wstrząsem dla dziedzictwa SALT była decyzja Stanów Zjednoczonych o wystąpieniu z układu ABM w 2002 r., motywowana potrzebą budowy nowego systemu obrony przeciwrakietowej przeciwko tzw. państwom zbójeckim i potencjalnym zagrożeniom asymetrycznym. Dla Federacji Rosyjskiej krok ten oznaczał podważenie 1 z filarów zimnowojennej stabilności. Choć realna skala nowego amerykańskiego systemu obronnego początkowo była ograniczona, Moskwa odebrała decyzję jako osłabienie logiki strategii MAD i sygnał możliwej rewizji dotychczasowego porządku. Mimo to struktury wywiedzione z tradycji SALT, takie jak limity ilościowe START czy praktyka obustronnych inspekcji, w dużej mierze przetrwały, a ich sens potwierdziły kolejne kryzysy w stosunkach rosyjsko-amerykańskich, kiedy to utrzymanie choćby minimalnej przejrzystości strategicznej okazywało się kluczowe.

Ocena SALT w naukach o bezpieczeństwie jest zasadniczo ambiwalentna, ale przeważają akcenty pozytywne. Z jednej strony, podkreśla się jego ograniczenia, takie jak brak redukcji arsenałów w fazie SALT I, niepełną implementację SALT II, pominięcie wielu istotnych kategorii broni, asymetrię w korzystaniu z technologii MIRV. Z drugiej – wskazuje się, że w warunkach bardzo wysokiego napięcia i głębokiej nieufności samo

ustanowienie ram ilościowych, kanałów komunikacji i zasad weryfikacji stanowiło przełom cywilizacyjny. Traktaty SALT zmieniły także sposób, w jaki społeczność międzynarodowa myśli o kontroli zbrojeń; zamiast abstrakcyjnych apeli o rozbrojenie pojawiła się praktyka stopniowego, technicznie precyzyjnego ograniczania najgroźniejszych kategorii broni.

Podsumowując, traktaty o ograniczeniu zbrojeń strategicznych (SALT) należy definiować jako zestaw powiązanych dokumentów rozbrojeniowych zawartych między Stanami Zjednoczonymi a Związkiem Radzieckim w latach 1972–1979, obejmujących zarówno Układ o ograniczeniu systemów obrony przeciwrakietowej oraz Tymczasowe porozumienie o ograniczeniu strategicznych zbrojeń ofensywnych (SALT I), jak i nieratyfikowany traktat SALT II. Ich wspólnym celem było zahamowanie dynamiki wyścigu zbrojeń strategicznych, ograniczenie potencjału nuklearnego w sposób gwarantujący zachowanie równowagi oraz stworzenie podstaw trwałego systemu kontroli zbrojeń, rozwijanego następnie w ramach układów START i innych instrumentów prawa międzynarodowego. Mimo upływu czasu i zmian geopolitycznych SALT pozostaje jednym z najważniejszych etapów w historii rozbrojenia nuklearnego i fundamentem współczesnych debat na temat kontroli zbrojeń.

Jarosław Indyk

L. Freedman, *The Evolution of Nuclear Strategy. New Updated and Completly Revised*, Palgrave Macmillan, London 2019; J.L. Gaddis, *Strategie powstrzymywania. Analiza polityki bezpieczeństwa narodowego Stanów Zjednoczonych w okresie zimnej wojny*, Książka i Wiedza, Warszawa 2007; R.L. Garthoff, *Détente and Confrontation. American–Soviet Relations from Nixon to Reagan*, Brookings Institution Press, Washington 1993; W. Multan, *Porozumienia rozbrojeniowe po II wojnie światowej, Państwowe Wydawnictwo Naukowe*, Warszawa 1985; M. Stempień, *Ewolucja międzynarodowej kontroli broni jądrowej i materiałów nuklearnych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2019, nr 9(2); S. Talbott, *Endgame: The Inside Story of SALT II*, Harper & Row, New York 1979.

TRAKTATY O REDUKCJI ZBROJEŃ STRATEGICZNYCH (ang. Strategic Arms Reduction Treaty, START) stanowią 1 z najważniejszych etapów w ewolucji kontroli zbrojeń nuklearnych po okresie zimnej wojny. O ile układy SALT zmierzały przede wszystkim do ograniczenia rozbudowy

potencjału strategicznego, START wprowadził jakościowo nowy model międzynarodowego reżimu rozbrojeniowego, którego istotą stała się realna redukcja strategicznych środków przenoszenia oraz głowic jądrowych. Zmiana ta wynikała z przeobrażeń geopolitycznych przełomu lat 80. i 90. XX w., w tym z końca dwubiegunowej konfrontacji oraz rosnącego przekonania wśród elit politycznych USA i ZSRR/Rosji o potrzebie zahamowania ekonomicznie wyniszczającego i technologicznie destabilizującego wyścigu zbrojeń. Pierwszy traktat START podpisano 31 lipca 1991 r., czyli zaledwie kilka miesięcy przed rozpadem Związku Radzieckiego, co przesądziło o konieczności dostosowania jego zapisów do nowych realiów międzynarodowych.

START I zapoczątkował nową filozofię redukcji strategicznych sił ofensywnych; jego podstawowe postanowienia dotyczyły obniżenia liczby rozmieszczonych środków przenoszenia broni jądrowej do 1600 oraz ograniczenia całkowitej liczby strategicznych głowic jądrowych do 6 tys. dla każdej ze stron. Układ określał także szczegółowe limity dotyczące kategorii uzbrojenia, m.in. maksymalną liczbę ciężkich międzykontynentalnych rakiet balistycznych (ICBM) oraz dopuszczalne konfiguracje systemów rakietowych wyposażonych w głowice MIRV. Jednocześnie traktat wprowadzał precyzyjne reguły tzw. „liczenia głowic" oraz regulował dopuszczalne formy modernizacji systemów przenoszenia. Celem było utrzymanie realnego balansu strategicznego przy jednoczesnym obniżeniu poziomu sił zdolnych do przeprowadzenia pierwszego masowego uderzenia jądrowego. Redukcja ta, w przeciwieństwie do poprzednich układów, była nie tylko ilościowa, ale również jakościowa, obejmując najbardziej destabilizujące elementy arsenałów ofensywnych.

Ważnym elementem START I były zaawansowane mechanizmy weryfikacji stanowiące 1 z największych osiągnięć dyplomacji rozbrojeniowej okresu powojennego. Traktat przewidywał szerokie wykorzystanie narodowych środków technicznych (NST), inspekcje na miejscu, monitoring produkcji systemów rakietowych, wymóg przekazywania danych telemetrycznych z testów rakietowych oraz stworzenie rozbudowanej infrastruktury kontrolnej. Zapisy te znacząco zwiększyły przejrzystość działań obu mocarstw, w teorii niwelując obawy przed ukrytym rozbudowywaniem potencjałów nuklearnych i pośrednio wzmacniając stabilność

strategiczną. START I był traktatem skrajnie technicznym i szczegółowym, a jego zapisy obejmowały setki stron załączników, definicji oraz instrukcji dotyczących weryfikacji, co czyniło go 1 z najbardziej złożonych układów kontroli zbrojeń w historii.

Podpisanie START I zbiegło się z procesem rozpadu ZSRR, co stworzyło potencjalne ryzyko niekontrolowanej proliferacji strategicznych systemów jądrowych. Z tego względu niezbędne stało się przyjęcie w 1992 r. protokołu lizbońskiego, który rozszerzał stronę traktatu o 4 państwa powstałe po rozpadzie ZSRR, czyli Rosję, Ukrainę, Białoruś i Kazachstan. Protokół nakładał na 3 ostatnie zobowiązanie do likwidacji broni nuklearnej znajdującej się na ich terytorium oraz przystąpienia do Traktatu o nierozprzestrzenianiu broni jądrowej (NPT) jako państwa nieatomowe. Proces ten, skomplikowany politycznie i logistycznie, został zakończony w połowie lat 90., przy istotnym wsparciu technicznym i finansowym USA.

Mimo trudności politycznych, w tym nieufności części elit rosyjskich wobec głębokich redukcji oraz sporów dotyczących kosztów modernizacji sił strategicznych, START I został w pełni wdrożony i funkcjonował aż do jego wygaśnięcia w grudniu 2009 r. W tym czasie Stany Zjednoczone oraz Federacja Rosyjska dokonały znaczących redukcji arsenałów, sprowadzając liczbę rozmieszczonych środków przenoszenia i głowic do poziomów niższych niż te przewidziane traktatem. START I stał się zatem fundamentem przejścia od ery nuklearnej konfrontacji do bardziej przewidywalnego modelu strategicznej stabilności, a jego dorobek instytucjonalny i techniczny został bezpośrednio przejęty przez kolejne układy, czyli traktaty START II, SORT oraz Nowy START.

Upadek Związku Radzieckiego oraz polityczna rekonstrukcja ładu międzynarodowego w latach 90. stworzyły warunki do podjęcia negocjacji nad drugim układem redukcyjnym, czyli START II, który został podpisany 3 stycznia 1993 r. Traktat ten miał stanowić kontynuację i pogłębienie reżimu ze START I, zakładając nie tylko dalsze cięcia ilościowe, ale przede wszystkim eliminację najbardziej destabilizujących kategorii uzbrojenia strategicznego. Kluczowym elementem START II była decyzja o całkowitym zakazie rozmieszczania międzykontynentalnych rakiet balistycznych uzbrojonych w głowice wielokrotnego niezależnego naprowadzania (MIRV) na stałych wyrzutniach lądowych, czyli broni

z kategorii możliwych do użycia jako ataku wyprzedzającego, zdolnej do obezwładnienia sił przeciwnika w krótkim czasie dzięki skoncentrowanej sile rażenia.

START II przewidywał redukcję rozmieszczonych głowic jądrowych do poziomu 3000–3500 dla każdej ze stron oraz znaczące obniżenie liczby ciężkich rakiet balistycznych. Szczególnie istotne było postanowienie dotyczące likwidacji radzieckich rakiet klasy SS-18 (RS-20), stanowiących trzon sił strategicznych ZSRR, zdolnych do przenoszenia nawet 10 głowic MIRV. Z punktu widzenia Moskwy był to wymóg dotkliwy, a zarazem kosztowny. Niejednokrotnie w literaturze przedmiotu stwierdza się, że START II faworyzował Stany Zjednoczone, których siły strategiczne opierały się w większym stopniu na komponentach morskich, uznawanych za stabilniejsze politycznie i bardziej odporne na ewentualne pierwsze uderzenie. Rosja natomiast traktowała ciężkie ICBM jako fundament odstraszania strategicznego, szczególnie w warunkach kryzysu gospodarczego i ograniczonej zdolności finansowej do rozwoju nowocześniejszego arsenału morskiego. W konsekwencji ratyfikacja START II w Rosji miała charakter przeciągający się i wysoce upolityczniony. Sytuację dodatkowo komplikowały równoległe spory dotyczące amerykańskich planów budowy systemów obrony przeciwrakietowej (National Missile Defense, NMD), postrzeganych w Rosji jako potencjalne naruszenie równowagi strategicznej opartej na wzajemnej podatności na odwet. Choć układ ABM z 1972 r. teoretycznie wciąż obowiązywał, debata w Waszyngtonie oraz pierwsze programy rozwojowe systemów antyrakietowych prowadziły rosyjskie elity wojskowe i polityczne do przekonania, że START II może pozbawić Rosję jej najbardziej efektywnego instrumentu nuklearnego odstraszania. Ostatecznie, choć USA ratyfikowały START II już w 1996 r., Rosja uczyniła to dopiero w 2000 r., uzależniając jego wejście w życie od dalszego obowiązywania układu ABM. Decyzja administracji George'a W. Busha o wycofaniu się z ABM w 2002 r. przekreśliła tę możliwość: w rezultacie Rosja formalnie odstąpiła od START II. Układ nigdy nie wszedł w życie, stając się jednym z najbardziej znaczących przykładów niewykorzystanej szansy na głęboką redukcję najbardziej destabilizujących elementów arsenałów strategicznych.

Upadek START II doprowadził do okresu strategicznej niepewności, obejmującego lata 2002–2009, w którym brakowało kompleksowego i prawnie wiążącego układu ograniczającego strategiczne siły ofensywne. Choć Stany Zjednoczone i Rosja deklarowały wolę utrzymania redukcji broni ofensywnej w postaci pocisków balistycznych, zabrakło ram weryfikacyjnych i kontrolnych charakterystycznych dla START I. W literaturze podkreśla się, że lata te były czasem erozji zaufania strategicznego, którą pogłębiały takie czynniki, jak rozszerzenie NATO, rosyjska modernizacja systemów rakietowych (m.in. RS-24 Jars, Topol-M), rozwój broni precyzyjnej dalekiego zasięgu w USA, a także rosnące napięcia geopolityczne. W tym kontekście poszukiwano sposobu na odbudowę stabilności strategicznej i przywrócenie instrumentów wzajemnej kontroli.

Przełom nastąpił wraz z administracją Baracka Obamy, która uczyniła kontrolę zbrojeń 1 z kluczowych elementów swej strategii bezpieczeństwa. W 2009 r. rozpoczęto negocjacje nad nowym układem, prowadzone w warunkach narastającej nieufności, lecz także świadomości, że brak formalnych mechanizmów redukcyjnych zagraża stabilności i transparentności w relacjach USA–Rosja. Owocem tych rozmów był podpisany 8 kwietnia 2010 r. w Pradze traktat New START, który zastąpił wygasły START I i przywrócił reżim prawnomiędzynarodowej kontroli strategicznych sił ofensywnych. New START ustalał limity 1550 rozmieszczonych głowic jądrowych oraz 700 środków przenoszenia (ICBM, SLBM, ciężkie bombowce), wprowadzając równocześnie uproszczony i bardziej elastyczny system weryfikacyjny. Choć redukcje w nim zapisane były mniejsze niż zakładane pierwotnie w ramach START II, sam fakt przywrócenia formalnego, przejrzystego reżimu kontroli był oceniany jako kluczowy element stabilizujący relacje USA–Rosja w pierwszej dekadzie XXI w.

Układy START odegrały kluczową rolę w kształtowaniu architektury bezpieczeństwa międzynarodowego po zakończeniu zimnej wojny. Ich znaczenie wykraczało poza aspekt militarny, wpływając na stabilność, dynamikę relacji USA–Rosja oraz mechanizmy kontroli zbrojeń w szerokim wymiarze politycznym. START I, a następnie New START, wprowadzały formalne limity, przejrzyste procedury weryfikacyjne oraz mechanizmy raportowania, które budowały zaufanie między rywalizującymi mocarstwami i zmniejszały prawdopodobieństwo przypadkowej

eskalacji. W literaturze podkreśla się, że skuteczność odstraszania jądrowego w dużej mierze zależy od wspólnego rozumienia zamiarów przeciwnika i jego realnych zdolności, a nie jedynie wielkości posiadanego arsenału.

Szczególnie istotny był rozwój i utrwalenie mechanizmów weryfikacji stanowiących fundament reżimu kontrolnego. Zarówno START I, jak i New START przewidywały inspekcje na miejscu, monitoring technologiczny oraz wymianę danych telemetrycznych, co wyraźnie odróżniało je od wcześniejszych porozumień SALT, w których weryfikacja była jeszcze ograniczona i pozostawiała duże pole do interpretacyjnych nadużyć. Według Zdzisława Lachowskiego traktaty te są jedną z najważniejszych gwarancji trwałości reżimu redukcyjnego, ponieważ bez dokładnych procedur kontrolnych nie dałoby się zapewnić ani wiarygodności, ani politycznej efektywności ograniczeń strategicznych. Z czasem technologie weryfikacyjne, oparte m.in. na satelitach rozpoznawczych, złożonych pomiarach telemetrycznych i analizach środowiskowych, stały się integralnym elementem globalnego systemu bezpieczeństwa.

Przeobrażenia technologiczne początku XXI w. zaczęły jednak stawiać pod znakiem zapytania dotychczasowy model architektury kontrolnej. Rozwój nowych typów broni, takich jak pociski hipersoniczne, systemy o częściowo niebalistycznej trajektorii lotu, konwencjonalnej broni dalekiego zasięgu o wysokiej precyzji rażenia oraz pojawienie się strategicznych dronów zwiększyły złożoność środowiska bezpieczeństwa. W literaturze przedmiotu wskazuje się również, że reżim START skoncentrowany na klasycznych systemach ICBM, SLBM i bombowcach może okazać się niewystarczający wobec modernizacji nuklearnych m.in. Rosji (Awangard, Sarmat, Posejdon) czy Chin, które dotąd nie uczestniczyły w porównywalnych mechanizmach kontroli zbrojeń. Rosnąca asymetria między mocarstwami, obejmująca nie tylko wielkość arsenałów, ale także różnice w doktrynach i strukturach sił, ograniczała możliwość łatwego przeniesienia dotychczasowego modelu redukcyjnego na nowe środowisko strategiczne.

W tym kontekście New START, choć szeroko oceniany jako sukces dyplomacji rozbrojeniowej, zaczął stopniowo funkcjonować w warunkach narastającej erozji geopolitycznej. Pogorszenie relacji na linii USA–Rosja po 2014 r., a następnie kolejne kryzysy, w tym napięcia

wokół INF, zbrojenia strategiczne, cyberzagrożenia i operacje hybrydowe, prowadziły do spadku wzajemnego zaufania. Mimo to układ przetrwał polityczne turbulencje, a administracja Joe Bidena w lutym 2021 r. doprowadziła do jego 5-letniego przedłużenia. Była to decyzja podkreślająca, że pomimo rosnących napięć brak formalnych ograniczeń strategicznych stwarzałby znacznie większe ryzyko destabilizacji niż utrzymanie dotychczasowych ram.

Po 2021 r. narastały jednak trudności związane z implementacją traktatu. Po pełnoskalowej agresji Rosji na Ukrainę w 2022 r. dialog strategiczny uległ faktycznemu zamrożeniu. W lutym 2023 r. Federacja Rosyjska ogłosiła zawieszenie udziału New START, argumentując to koniecznością reagowania na tzw. wrogie działania Zachodu. Choć Rosja zadeklarowała, że będzie przestrzegać podstawowych limitów traktatu, zawieszenie mechanizmów weryfikacyjnych oraz brak wymiany danych oznaczały, że skuteczność układu została poważnie naruszona.

Układy START w perspektywie historycznej stanowią zatem wielowymiarowy reżim kontroli zbrojeń, który przekształcił relacje na linii USA–Rosja oraz ukształtował podstawy współczesnych norm rozbrojeniowych. Po pierwsze, ukazały, że głębokie redukcje są możliwe wyłącznie w warunkach względnej stabilności politycznej i wzajemnej woli utrzymania przewidywalności strategicznej. Po drugie, potwierdziły, że reżim kontroli zbrojeń wymaga elastycznego dostosowywania do zmian technologicznych, zwłaszcza w okresie dynamicznego rozwoju systemów nienależących do klasycznych kategorii strategicznych. Po trzecie, doświadczenia START wskazują, że skuteczne porozumienia rozbrojeniowe muszą być wspierane szerokimi mechanizmami weryfikacji oraz politycznymi gwarancjami ich wdrażania. Wreszcie, ewolucja traktatów od sukcesu START I, przez niewykorzystany potencjał START II, aż po zagrożone funkcjonowanie New START odzwierciedla napięcie między dążeniem do stabilizacji a rywalizacyjną logiką polityki mocarstwowej.

Podsumowując, reżim START wytworzył historycznie bezprecedensowy poziom kontroli nad strategicznymi arsenałami nuklearnymi, przyczyniając się do redukcji liczby rozmieszczonych głowic o ponad 70% od początku lat 90. Jego przyszłość pozostaje jednak niepewna. Wobec nowych technologii, wzrostu znaczenia systemów taktycznych, modernizacji

arsenałów oraz erozji dialogu politycznego między światowymi mocarstwami przyszłe porozumienia będą wymagały szerszego zakresu, większej elastyczności i uwzględnienia nowych aktorów, zwłaszcza Chin. Niezależnie od wyzwań START pozostaje fundamentem historycznego dorobku kontroli zbrojeń i 1 z najważniejszych instrumentów ograniczania ryzyka wojny nuklearnej w epoce po zimnej wojnie.

Jarosław Indyk

D. Ellsberg, *The Doomsday Machine: confessions of a nuclear war planner*, Bloomsberg Publishing, London 2017; Z. Lachowski, *Nuklearne rozbrojenie i nieproliferacja: geneza, stan i perspektywy*, „Biuro Bezpieczeństwa Narodowego" 2013, nr 22; N. Sokov, *Russian Strategic Modernization: Past and Future*, Rowman & Littlefield Publishers, Lanham 2000; S. Talbott, *The Russia Hand: Shaping American–Russian Relations under Clinton*, Random House, New York 2002; C. Yeaw, G. Quester, P.J. Bolt, A.S. Willner, *Nuclear First Strike: Consequences of a Broken Taboo; China 's Nuclear Future*, „Naval War College Review" 2006, vol 29, no. 4; S. Zarychta, *Kontrola zbrojeń i traktaty rozbrojeniowe dotyczące broni jądrowej*, „Rocznik Bezpieczeństwa Morskiego" 2015, t. IX.

TRIPWIRE (dosłownie „drut potykacz") – specyficzny mechanizm organizowania obecności wojskowej, który ma służyć jako narzędzie odstraszania polityczno-strategicznego. Chodzi o sytuację, w której państwo lub sojusz świadomie rozmieszcza na zagrożonym kierunku stosunkowo niewielkie, często symbolicznie liczne siły, dobrze widoczne i jednoznacznie identyfikowalne. Taki kontyngent nie jest projektowany po to, aby samodzielnie wygrać kampanię obronną czy zatrzymać duże zgrupowanie przeciwnika. Jego zasadnicza rola polega na tym, że w razie agresji niemal na pewno będą ofiary wśród żołnierzy państwa-gwaranta lub całego sojuszu, a to z kolei ma w praktyce uruchomić mechanizm szerszej odpowiedzi politycznej, militarnej i sojuszniczej. W tym sensie *tripwire* stanowi swoiste sprzężenie między obecnością wojskową w terenie a decyzjami politycznymi w stolicach.

W klasycznym ujęciu *tripwire* wiąże się ściśle z rozszerzonym odstraszaniem. Państwo silniejsze deklaruje, że będzie bronić słabszych sojuszników, ale sama deklaracja może być kwestionowana jako niewystarczająco wiarygodna. Rozmieszczenie żołnierzy na obszarze zagrożonego

państwa ma przekształcić tę obietnicę w realne ryzyko dla potencjalnego agresora. Atak na partnera staje się automatycznie atakiem na ludzi, za których odpowiedzialność ponosi rząd mocarstwa. Polityczne i społeczne koszty zignorowania takiego faktu byłyby bardzo wysokie. Mechanizm *tripwire* ma więc przekształcić abstrakcyjne zobowiązania sojusznicze w coś konkretnego: obecność żołnierzy (czasami też ich rodzin), którzy w razie konfliktu będą pierwszymi ofiarami.

Geneza tego podejścia sięga okresu zimnej wojny; wówczas Stany Zjednoczone utrzymywały niewielkie, ale stałe kontyngenty w miejscach szczególnie narażonych na ewentualny nacisk ze strony Związku Radzieckiego i jego sojuszników. Klasycznym przykładem była obecność wojsk amerykańskich w Berlinie Zachodnim; sama ich liczebność nie pozwalała na realną obronę miasta przed hipotetycznym atakiem z zewnątrz, natomiast polityczny przekaz był oczywisty: każdy zbrojny ruch wymierzony w Berlin Zachodni oznaczałby niemal pewne ofiary wśród Amerykanów, a więc wciągnięcie USA w konflikt, który mógł szybko eskalować na poziom strategiczny. W podobny sposób działała obecność amerykańskich żołnierzy w Korei Południowej – nie mogła ona powstrzymać pełnoskalowej ofensywy Północy, ale gwarantowała, że agresja nie będzie incydentem „lokalnym", który można rozegrać z pominięciem Waszyngtonu.

Koncepcja ta wyrosła z bardzo konkretnego kontekstu: potrzeby połączenia bezpieczeństwa sojuszników z wiarygodnością zobowiązań mocarstwa nuklearnego. Z jednej strony, USA nie były skłonne rozmieszczać ogromnych armii w każdym strategicznie ważnym regionie świata, z drugiej – samo odwołanie do broni jądrowej jako ostatecznego środka odstraszania budziło wątpliwości sojuszników. *Tripwire* stawał się kompromisem: niewielka, ale trwała obecność wojskowa, która tworzy praktyczną więź między losem danego terytorium a decyzjami politycznymi w stolicy gwaranta.

Logika działania *tripwire* opiera się na kilku warstwach. Po pierwsze, ma on zadziałać psychologicznie na potencjalnego agresora; ten, planując operację wojskową, musi wziąć pod uwagę, że pierwszymi ofiarami będą obywatele państw, z którymi niekoniecznie chciałby wejść w otwarty konflikt. Po drugie, mechanizm ten ma wymiar wewnątrzpolityczny: przywódcy państw-gwarantów wiedzą, że śmierć własnych żołnierzy

na terytorium sojusznika generuje ogromną presję opinii publicznej i elit na udzielenie zdecydowanej odpowiedzi. Po trzecie, obecność *tripwire* wzmacnia morale państw przyjmujących, które zyskują nie tylko symboliczne, ale bardzo namacalne potwierdzenie, że nie są same w obliczu zagrożenia.

W przeciwieństwie do klasycznych koncepcji rozmieszczenia dużych zgrupowań, *tripwire* z definicji zakłada dysproporcję sił. Kontyngent jest na tyle mały, że samodzielnie nie zdoła powstrzymać agresji, ale na tyle widoczny, że nie da się go pominąć w trakcie działań. Nie chodzi o stworzenie nieprzekraczalnej linii obrony, lecz o skonstruowanie „wyłącznika", po dotknięciu którego uruchamia się inny poziom gry. W wielu planach operacyjnych zakłada się, że oddziały tego typu będą prowadzić walkę opóźniającą, wycofywać się na kolejne linie, a przede wszystkim dokumentować naruszenie terytorium i obecność przeciwnika, tak aby nie było żadnych wątpliwości co do tego, kto jest agresorem.

W debacie na temat wschodniej flanki NATO po 2014 r. koncepcja *tripwire* pojawiła się bardzo szybko, gdy zaczęto rozmieszczać w państwach bałtyckich i w Polsce wielonarodowe grupy bojowe. Ich struktura i liczebność sprawiały, że nie można było ich traktować jako pełnowymiarowej obrony liniowej, zdolnej samodzielnie zatrzymać duże rosyjskie zgrupowanie. Jednocześnie ich znaczenie polityczne było ogromne: w razie konfliktu w Estonii, Łotwie, Litwie czy Polsce pierwsze ofiary padłyby również wśród żołnierzy Kanady, Niemiec, Wielkiej Brytanii czy Stanów Zjednoczonych. Oznaczałoby to automatyczne upolitycznienie konfliktu na poziomie całego Sojuszu i bardzo silną presję na uruchomienie mechanizmów kolektywnej obrony przewidzianych w art. 5.

W polskim kontekście mechanizm *tripwire* bardzo wyraźnie wiąże się z funkcjonowaniem NATO na wschodniej flance i rolą Polski jako państwa-gospodarza sojuszniczej obecności wojskowej. Z jednej strony, Polska sama korzysta z odstraszania rozszerzonego opartego na art. 5, który – jak już ustalono – ma charakter klasycznego *deterrence by punishment*: potencjalny agresor musi liczyć się z tym, że atak na terytorium Rzeczypospolitej uruchomi reakcję całego Sojuszu. Z drugiej strony, obecność na polskim terytorium wojsk amerykańskich i innych sojuszników tworzy realny „drut potykacz": każda poważniejsza operacja militarna

przeciwko Polsce oznaczałaby automatyczne uderzenie także w żołnierzy USA, Wielkiej Brytanii, Kanady czy innych państw, co radykalnie zwiększa prawdopodobieństwo odpowiedzi zbiorowej. W tym sensie polska część systemu obronnego NATO łączy klasyczne odstraszanie przez karę (obietnica wielkoskalowego odwetu sojuszniczego) z elementem *tripwire*, ponieważ potencjalny agresor nie mógłby ograniczyć konfliktu do „lokalnego incydentu" z 1 państwem.

Po 2014 r., a szczególnie po 2022 r., gdy Rosja dokonała pełnoskalowej agresji na Ukrainę, ten wymiar polskiej roli jeszcze wyraźniej się zaznaczył. Decyzje szczytu NATO w Warszawie i późniejsze rozmieszczenie w Polsce wielonarodowej grupy bojowej w ramach tzw. *enhanced Forward Presence* były wprost opisywane jako siła o charakterze *tripwire*: formacja sama w sobie nie była projektowana do prowadzenia długotrwałej, samodzielnej obrony, lecz miała sygnalizować solidarność sojuszniczą i w praktyce demonstrować działanie artykułu 5. Kolejne decyzje, w tym zapowiedziane na szczycie madryckim przekształcenie wysuniętej obecności w bardziej rozbudowaną obronę, możliwość rozwinięcia batalionów do struktur brygadowych i trwała lokalizacja amerykańskiego dowództwa V Korpusu w Polsce, pokazują, że Warszawa pełni funkcję kluczowego „węzła" tej logiki: to tutaj przecinają się linie odstraszania nuklearnego, konwencjonalnego, mechanizmu art. 5 i fizycznej obecności sił sojuszniczych. Polska jest zatem jednocześnie beneficjentem i współtwórcą systemu *tripwire*: udostępniając terytorium i infrastrukturę dla wojsk sojuszniczych, wzmacnia wiarygodność własnego bezpieczeństwa, ale też staje się przestrzenią, w której ewentualny atak natychmiast przybiera wymiar konfliktu NATO–agresor, a nie wyłącznie sporu bilateralnego.

W najnowszej debacie w ramach Sojuszu coraz częściej podkreśla się, że ów „cienki drut potykacz" musi być w Polsce i w innych państwach wschodniej flanki wzmocniony szerszą obroną wysuniętą. Madrid Strategic Concept i późniejsze decyzje o zwiększaniu liczebności zgrupowań oraz skracaniu czasu przybycia wzmocnień wskazują na przejście od modelu czysto symbolicznego *tripwire* ku konstrukcji, w której wysunięte siły mają nie tylko wywołać efekt polityczny, ale również realnie utrudnić przełamanie obrony od pierwszego dnia konfliktu. W polskiej perspektywie oznacza to, że rola państwa w systemie odstraszania ewoluuje:

wciąż opiera się na groźbie kary zakotwiczonej w art. 5, ale staje się coraz bardziej powiązana z własnymi zdolnościami obronnymi i obecnością sojuszniczych jednostek, które pełnią równocześnie funkcję *tripwire* i realnego komponentu obrony. Dzięki temu sama groźba kary, będąca istotą *deterrence by punishment*, zostaje wzmocniona poprzez fakt, że agresor od pierwszego dnia miałby do czynienia nie tylko z deklaracjami, ale i konkretną wielonarodową strukturą wojskową, z którą musiałby się fizycznie zmierzyć na polskim terytorium.

Właśnie w tym miejscu dobrze widać różnicę między tradycyjną obecnością sojusznika a modelem *tripwire*. Klasyczna baza wojskowa z dużym garnizonem może pełnić zarówno funkcję operacyjną, jak i odstraszającą. Siły *tripwire* z kolei konstruuje się z założenia jako niewystarczające operacyjnie, ich zadaniem nie jest wygranie wojny „tu i teraz", lecz zmiana kalkulacji politycznej. Z perspektywy agresora oznacza to, że przeprowadzenie szybkiej, lokalnej operacji mającej na celu stworzenie faktów dokonanych staje się znacznie trudniejsze do zaplanowania. Atak na państwo, w którym stacjonują żołnierze kilku czy kilkunastu sojuszniczych armii, bardzo trudno przedstawić później na arenie międzynarodowej jako „wewnętrzny spór" czy ograniczoną akcję.

Warto przy tym zaznaczyć, że mechanizm *tripwire* nie działa tylko na linii państwo–mocarstwo; można go dostrzec także w relacjach wewnątrzsojuszniczych, gdy silniejsi partnerzy rozlokowują swoje kontyngenty na terytorium słabszych, choć formalnie wszyscy mają ten sam status. W przypadku NATO obecność żołnierzy państw zachodnioeuropejskich i północnoamerykańskich na wschodniej flance jest sygnałem zarówno wobec potencjalnego agresora, jak i społeczeństw lokalnych, że bezpieczeństwo regionu traktowane jest jako integralna część bezpieczeństwa całego Sojuszu.

Z czasem wokół koncepcji *tripwire* narosła jednak istotna krytyka; część analityków argumentuje, że opieranie się na bardzo małych, symbolicznych kontyngentach nie odpowiada na realne wyzwania związane z możliwością szybkiej operacji ofensywnej. W scenariuszu, w którym przeciwnik podejmuje skoordynowane działania militarne, cybernetyczne i informacyjne, niewielka liczba żołnierzy może zostać szybko zneutralizowana, zanim opinia publiczna i elity polityczne zdążą w pełni zareagować.

W takim ujęciu *tripwire* może okazać się bardziej deklaracją polityczną niż rzeczywistym środkiem wpływającym na zachowanie agresora.

Inny wątek krytyczny dotyczy woli politycznej państw-gwarantów. Przeciwnicy przeceniania *tripwire* zwracają uwagę, że sama obecność ofiar wśród żołnierzy nie przesądza automatycznie o decyzji o eskalacji. Odwołują się przy tym do doświadczeń z konfliktów asymetrycznych, w których państwa zachodnie ponosiły straty wśród swoich kontyngentów, a mimo to ich społeczeństwa były coraz mniej skłonne akceptować dalsze zaangażowanie militarne. Jeśli opinia publiczna jest zmęczona konfliktami zagranicznymi, samo ryzyko utraty kilkuset żołnierzy nie musi wystarczyć, by wygenerować poparcie dla dużej operacji odwetowej.

Współczesne NATO ewoluuje więc w kierunku łączenia mechanizmu *tripwire* z bardziej rozbudowaną koncepcją obrony wysuniętej. Po rosyjskiej agresji na Ukrainę w 2022 r. w dokumentach sojuszniczych coraz częściej mówi się nie tylko o wysuniętej obecności, lecz i obronie. Oznacza to odejście od schematu, w którym zadaniem sił rozmieszczonych na wschodniej flance jest przede wszystkim sygnalizowanie determinacji, w kierunku modelu, gdzie mają one realnie utrudnić przeciwnikowi osiągnięcie celów w pierwszej fazie konfliktu. *Tripwire* nie znika, ale zostaje wkomponowany w szerszą strukturę obronną: nadal ważne jest, by w razie ataku ucierpieli także żołnierze państw zachodnich, lecz równie istotne staje się to, aby siły te były zdolne do prowadzenia działań o większej skali.

W ostatnich latach coraz częściej wskazuje się, że klasycznie pojmowany *tripwire* musi dostosować się do zmian w środowisku działań zbrojnych. Rozwój broni precyzyjnej dalekiego zasięgu, systemów rozpoznania satelitarnego oraz środków rażenia o wysokiej dokładności sprawia, że niewielkie, skoncentrowane kontyngenty mogą stać się stosunkowo łatwym celem uderzeń w pierwszych minutach konfliktu. Dla części analityków oznacza to potrzebę odejścia od statycznego modelu rozmieszczenia w stronę bardziej rozproszonej, mobilnej obecności, która nadal pełni funkcję politycznego „wyłącznika", ale jest mniej podatna na natychmiastowe zniszczenie. Taki sposób myślenia wpisuje się w szerszy trend przechodzenia od symbolicznych garnizonów do sieci rozproszonych punktów obecności, zdolnych do szybkiego rozwinięcia i integracji z siłami państwa-gospodarza.

Kolejnym wymiarem tej ewolucji jest uwzględnienie wojny hybrydowej i działań poniżej progu otwartej agresji. Tradycyjnie zakładano, że *tripwire* zadziała w momencie jednoznacznego przekroczenia granicy terytorialnej i rozpoczęcia operacji wojskowej. W realiach zorganizowanych kampanii presji, sabotażu, cyberataków i operacji informacyjnych trudno jednak wskazać jeden moment, który „uruchamia" cały sojuszniczy mechanizm. Z tego powodu część koncepcji rozwija ideę „*tripwire* rozszerzonego" o elementy niekinetyczne: stałą obecność oficerów łącznikowych, wspólne centra analiz, podłączanie państwa-gospodarza do systemów wczesnego ostrzegania oraz ścisłą integrację w domenach cybernetycznej i informacyjnej. W zamyśle ma to utrudnić agresorowi przeprowadzanie długotrwałej kampanii hybrydowej bez ryzyka, że poszczególne incydenty zostaną powiązane w spójny obraz i potraktowane jako przygotowanie do agresji.

Odrębnym, rzadziej omawianym aspektem jest ryzyko, że siły *tripwire* mogą zostać wykorzystane w charakterze swoistego „zakładnika strategicznego". Przeciwnik, mając świadomość, że zachodni kontyngent nie zostanie łatwo wycofany w obawie przed utratą wiarygodności, może próbować stopniowo podnosić napięcie, licząc na to, że strona sojusznicza będzie unikała ostrych reakcji, by nie narażać własnych żołnierzy. Ten paradoks – polegający na tym, że obecność mająca odstraszać może w pewnych warunkach stać się czynnikiem ograniczającym swobodę działania – również pojawia się w literaturze. Odpowiedzią na tego typu obawy jest większy nacisk na planowanie ewakuacji, rotacji, maskowania oraz elastycznego użycia rozmieszczonych sił, tak aby nie były one postrzegane jako bierny, „przywiązany" do miejsca symbol, ale realny, dynamiczny element całościowej postawy obronnej.

W miarę jak rośnie znaczenie nowych domen działań – cyberprzestrzeni, przestrzeni kosmicznej, walki informacyjnej – samo fizyczne rozmieszczenie oddziałów przestaje wystarczać jako jedyny nośnik sygnału odstraszającego. W odpowiedzi rozwija się myślenie o „wielowymiarowym *tripwire*", w którym symboliczna obecność wojskowa jest uzupełniana przez widoczne formy współpracy technologicznej, wspólne projekty w obszarze rozpoznania satelitarnego, wzajemne wsparcie w odpieraniu cyberataków czy skoordynowane kampanie informacyjne. Z perspektywy potencjalnego agresora oznacza to, że przekroczenie progu agresji wobec państwa, na

którego terytorium stacjonują sojusznicze siły, pociąga za sobą nie tylko zagrożenie stratami militarnymi, ale także konsekwencje w sferze technologicznej, informacyjnej i gospodarczej, co czyni kalkulację ryzyka jeszcze bardziej niekorzystną.

Mechanizm ten ma również swoje zastosowania w sferze polityczno-prawnej; obecność żołnierzy państwa trzeciego na terytorium sojusznika ułatwia jednoznaczne zdefiniowanie sytuacji jako zbrojnego ataku w rozumieniu prawa międzynarodowego. Jeżeli giną lub zostają ranni żołnierze kilku państw, trudniej podważać fakt, że doszło do agresji, a nie serii niejasnych incydentów. W świecie, w którym stosuje się często działania „pod progiem wojny", to właśnie wyraźna, fizyczna obecność wojskowa paradoksalnie bywa jednym z nielicznych elementów, które pozwalają jasno nazwać sytuację.

W sensie symbolicznym *tripwire* odgrywa jeszcze jedną rolę: ma wymiar komunikatu skierowanego do społeczeństw państw przyjmujących. Obecność sojuszniczych żołnierzy buduje poczucie, że potencjalny agresor nie będzie mógł „rozgrywać" danego kraju w izolacji, a jego bezpieczeństwo jest realnie współdzielone, co sprzyja odporności psychologicznej wobec presji zewnętrznej, szantażu czy kampanii dezinformacyjnych. W pewnym sensie jest to „widoczna twarz" sojuszu – bardziej przemawiająca do wyobraźni niż abstrakcyjne zapisy traktatów.

Nie oznacza to jednak, że *tripwire* jest rozwiązaniem uniwersalnym. Funkcjonuje najlepiej tam, gdzie istnieje stosunkowo wyraźna linia potencjalnego kontaktu z przeciwnikiem, rozwinięta infrastruktura zdolna przyjąć kontyngenty oraz dojrzałe mechanizmy polityczne po obu stronach. W regionach o bardzo niestabilnej sytuacji wewnętrznej, w państwach z silnymi napięciami wewnętrznymi czy w sytuacji braku zgody co do kierunków polityki zagranicznej rozmieszczanie *tripwire* może generować dodatkowe ryzyko, stając się przedmiotem sporów wewnętrznych lub prowokacji.

Mechanizm *tripwire* jest jedną z technik budowania wiarygodności sojuszniczej w polityce bezpieczeństwa; łączy w sobie aspekty czysto wojskowe z wyraźnym wymiarem psychologicznym, komunikacyjnym i prawnym. Jego skuteczność zależy od tego, na ile potencjalny agresor wierzy, że śmierć lub zranienie niewielkiego, ale symbolicznego kontyngentu rzeczywiście uruchomi szeroką reakcję polityczną i militarną.

W epoce, w której granice między wojną a pokojem, konfliktem lokalnym a globalnym stają się coraz mniej wyraźne, *tripwire* pozostaje narzędziem przydatnym, ale sam w sobie nie wystarcza, musi być osadzony w szerszej strategii obronnej i wsparty realnymi zdolnościami militarnymi oraz stabilnymi mechanizmami decyzyjnymi.

Fabian Kobalczyk-Gruda

Australian Strategic Policy Institute, Australian tripwire forces: an idea whose time has come?, „The Strategist" 2023, https://www.aspistrategist.org.au/australian-tripwire-forces-an-idea-whose-time-has-come/ (dostęp 29.11.2025); *eFP Battle Group Poland – Combined Arms, Combined Strength*, 2022, https://www.vcorps.army.mil/Newsroom/Articles/Article-Display/Article/3238976/efp-battle-group-poland-combined-arms-combined-strength/ (dostęp 29.11.2025); A. Lanoszka, *Evaluating the Enhanced Forward Presence After Five Years*, „The RUSI Journal" 2023, https://www.tandfonline.com/doi/abs/10.1080/03071847.2023.2190352 (dostęp 29.11.2025); A. Lanoszka, *Poland in a time of geopolitical flux, Sasakawa Peace Foundation*, „JPUS Insights" 2025, https://www.spf.org/jpus-insights/spf-worldviews-on-the-united-states-en/woldviews-on-the-united-states006.html (dostęp 29.11.2025); D.Y. Lee, *Strategies of Extended Deterrence: How States Provide the Security Umbrella*, „Security Studies" 2021, https://www.tandfonline.com/doi/full/10.1080/09636412.2021.2010887 (dostęp 29.11.2025); S. Lee, *Prospects for the ROK's Nuclear Policy – Sharing or Redeployment?*, 2025, https://www.spf.org/iina/en/articles/sanghoe_lee_02.html (dostęp 29.11.2025); *Lessons from the Enhanced Forward Presence, 2017–2020*, A. Lanoszka, C. Leuprecht, A. Moens (eds.), NATO Defense College, Rome 2020, https://www.ndc.nato.int/download/lessons-from-the-enhanced-forward-presence-2017-2020/ (dostęp 29.11.2025); *Ministry of Foreign Affairs of Latvia, NATO Enhanced Forward Presence*, 2025, https://www.mfa.gov.lv/en/nato-enhanced-forward-presence (dostęp 29.11.2025); K.D. Motacki, *Znaczenie wzmocnionej Wysuniętej Obecności NATO dla bezpieczeństwa Polski i państw wschodniej flanki,* „Bezpieczeństwo Narodowe" 2024, https://www.bbn.gov.pl/download/1/30804/KwartalnikBN2024-44ZnaczeniewzmocnionejWysunietejObecnosciNATOdlabezpieczenstwaP.pdf (dostęp 29.11.2025); *NATO is moving towards a new generation of forward defence*, Swedish Defence Research Agency, Sztokholm 2025, https://www.foi.se/en/foi/news-and-pressroom/news/2025-06-26-nato-is-moving-towards-a-new-generation-of-forward-defence.html (dostęp 29.11.2025); *NATO's Enhanced Forward Presence*, Factsheet, Bruksela 2017, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/1705-factsheet-efp.pdf (dostęp 29.11.2025); D. Palavenis, *NATO enhanced forward presence*

in the Baltics: The nexus between the host and the framework nation, „Security and Defence Quarterly" 2025, https://securityanddefence.pl/NATO-enhanced-forward-presence-in-the-Baltics-The-nexus-between-the-host-and-the,193734,0,2.html (dostęp 29.11.2025); S.S. Reed, *The Korean Security Dilemma: Shifting Strategies Offer a Way*, Air University, Maxwell AFB 2018, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/reed.pdf (dostęp 29.11.2025); D. Reiter, P. Poast, *The Truth About Tripwires: Why Small Force Deployments Do Not Deter Aggression*, „Texas National Security Review" 2021, https://tnsr.org/2021/06/the-truth-about-tripwires-why-small-force-deployments-do-not-deter-aggression/ (dostęp 29.11.2025); T. Romar, C. Guerout, *The Evolving 'Tripwire' on NATO's Eastern Flank*, 2024, https://www.wilsoncenter.org/article/evolving-tripwire-natos-eastern-flank (dostęp 29.11.2025); *Rozbudowa wschodniej flanki NATO w świetle koncepcji odstraszania*, Instytut Nowej Europy, Warszawa 2024, https://ine.org.pl/rozbudowa-wschodniej-flanki-nato-w-swietle-koncepcji-odstraszania/ (dostęp 29.11.2025); *Strengthening NATO's eastern flank*, „NATO Topics" 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/strengthening-natos-eastern-flank (dostęp 29.11.2025); C. Work, *What's in a Tripwire: The Post-Cold War Transformation of the US Military Presence in Korea*, 2022, https://www.stimson.org/2022/whats-in-a-tripwire-the-post-cold-war-transformation-of-the-us-military-presence-in-korea/ (dostęp 29.11.2025); M. Zima, *NATO's Enhanced Forward Presence: Assets and Limits of Conventional Deterrence*, IRSEM, Research Paper No. 131, Paryż 2022, https://www.irsem.fr/storage/file_manager_files/2025/03/rp-irsem-131-zima-nato-en.pdf (dostęp 29.11.2025).

TURNING POINT USA (TPUSA) to amerykańska organizacja pozarządowa, z główną siedzibą w Phoenix, w Arizonie, propagująca respektowanie konserwatywnych wartości w życiu publicznym i prywatnym. Współcześnie uznawana za 1 z największych i najlepiej zorganizowanych tego typu inicjatyw w Stanach Zjednoczonych. Obecna na ponad 900 uniwersytetach i w niemal 2 tys. szkół średnich na terenie całego kraju zrzesza niemal 830 tys. młodych ludzi. Jej głównym celem jest przekształcenie amerykańskiej polityki, gospodarki i kultury w duchu tradycyjnych wartości, co w założeniu ma nie tylko umożliwić harmonijny i stabilny rozwój społeczny, ale także bezpośrednio przyczynić się do znacznego wzrostu satysfakcji i szczęścia obywateli. W swojej narracji akcentuje przywiązanie do chrześcijaństwa, podkreślając jego fundamentalne znaczenie dla powstania

cywilizacji zachodnioeuropejskiej. Promuje zasadę ograniczonego rządu, własność prywatną oraz wolny rynek.

Organizacja została założona 5 czerwca 2012 r. przez młodzieżowego aktywistę z Chicago Charliego Kirka. Początkowo jej działalność koncentrowała się na inicjowaniu debat politycznych na kampusach uniwersyteckich powszechnie postrzeganych jako bastiony liberalnego czy też lewicowego światopoglądu. Ich celem była dyskusja na tematy społecznie istotne, mająca na celu nie tylko wyłożenie słuchaczom konserwatywnej oceny rzeczywistości, ale także walkę z utrwalonymi i najczęściej formułowanymi przez środowiska liberalne argumentami. Opowiadając się jednoznacznie za zakazem aborcji, przeciwko nielegalnej imigracji oraz popierając prawo do posiadania broni, Kirk wzbudzał kontrowersje, co przekładało się na duże zainteresowanie organizowanymi przez niego spotkaniami oraz znaczącą liczbą studentów podejmujących z nim dialog.

Zaangażowanie i niewątpliwa charyzma Kirka skutkowały rozbudową organizacji oraz większymi możliwościami pozyskania środków finansowych na jej działalność. W kolejnych latach inicjatywa była wspierana przez zamożnych konserwatywnych przedsiębiorców i filantropów, polityków Partii Republikańskiej, a także tysiące obywateli amerykańskich podzielających głoszone przez nią poglądy, co skutkowało rozbudową struktury oraz zwiększeniem liczby wolontariuszy działających w stowarzyszeniu. Jego liderzy wspierali finansowo i merytorycznie konserwatywną młodzież ubiegającą się o miejsce w organach samorządu studenckiego, a także wskazali zadania kluczowe dla rozwijającego się ruchu. Były nimi identyfikacja, edukacja, szkolenie i organizacja studentów w celu promowania wolności.

Na czele organizacji stoi dyrektor generalny wraz z radą nadzorczą, zaś organem wpierającym te podmioty jest rada doradcza. Ponadto w ramach struktury Turning Point USA obok jednostek zapewniających obsługę organizacji (departament zasobów ludzkich, marketingu czy dystrybucji i zarządzania aktywami) funkcjonują oddziały o charakterze zadaniowym odpowiedzialne m.in. za tworzenie programów nauczania, projektowanie merytoryczne i graficzne rozpowszechnianych materiałów czy organizację szczytów i konferencji. Dodatkowo praca niektórych sekcji koncentruje się wokół określonych grup społecznych, np. uczniów szkół

średnich, studentów czy członków mniejszości rasowych oraz etnicznych takich jak Afroamerykanie, Azjaci czy Latynosi. Co więcej, specjalny dział wiary (*faith*) zajmuje się jednoczeniem chrześcijan oraz ich mobilizacją w głoszeniu prawd ewangelicznych i zgodnym z nimi trybem życia.

Szersze zadania ma natomiast powołana w 2019 r. stowarzyszona z TPUSA Turning Point Action; jej celem jest agregacja poparcia wyborczego dla kandydatów o prawicowych poglądach oraz wsparcie konserwatystów, którzy zdecydują się na start w elekcji organów lokalnych. Organizacja była zaangażowana w mobilizację elektoratu na rzecz Donalda Trumpa w trakcie kampanii poprzedzającej wybory prezydenckie w 2025 r., a także republikańskiego gubernatora Florydy Rona DeSantisa, który powtórnie objął urząd w 2022 r. Charakter wspierający ma również powołany w 2018 r. fundusz powierniczy (Turning Point Endowment) odpowiedzialny za stabilność finansową TPUSA oraz możliwość realizowania działalności statutowej, w tym także charytatywnej, co jest odpowiedzialnym zadaniem, biorąc pod uwagę, że całkowite przychody organizacji w 2024 r. wyniosły 85 mln dolarów, a można przypuszczać, że w kolejnych latach przekroczą tę kwotę.

Do rozpowszechniania swojej agendy Turning Point USA szeroko wykorzystuje nowoczesne media: ma konta na wszystkich istotnych platformach komunikacyjnych (Facebook, Instagram, X), nagrywa filmy oraz prowadzi podcasty. Najbardziej popularnymi z nich są poświęcony zagadnieniom politycznym i społecznym Charlie Kirk Show oraz traktujący o konserwatywnym spojrzeniu na kwestie zdrowotne Culture Apothecary prowadzony przez Alexa Clarka. Liderzy organizacji na bieżąco publikują nagrania i treści związane ze swoją działalnością, codziennie wchodząc w interakcje z odbiorcami oraz komentują najważniejsze wydarzenia w kraju i na świecie, zapraszając do rozmów czołowych polityków i ekspertów. Organizacja posiada również własną platformę streamingową, gdzie regularnie prowadzi transmisje na żywo, oraz kilka aplikacji umożliwiających szybki kontakt z odbiorcami.

Ponadto Turning Point USA kilka razy w roku organizuje ogólnokrajowe spotkania mające na celu zachęcenie młodych ludzi do podjęcia działań w obronie konserwatywnych wartości. Ich uczestnicy słuchają przemówień i biorą udział w warsztatach, ucząc się przywództwa, organizacji

oraz efektywnej komunikacji. Co istotne, omawiane wydarzenia zwykle są skierowane do konkretnego odbiorcy: kobiet, mężczyzn, studentów, przedstawicieli mniejszości etnicznych. Organizowane z dużym rozmachem, koncentrują uwagę mediów i opinii publicznej. Wśród zaproszonych mówców są konserwatywni politycy i specjaliści z pierwszych stron gazet, a prowadzone zajęcia są sprofilowane i oparte na praktyce.

Jednym z narzędzi służących realizacji wyznaczonych przez organizację celów stała się założona w 2016 r. strona internetowa Professor Watchlist zawierająca nazwiska akademików, którzy według Turning Point USA „dyskryminują studentów o konserwatywnych poglądach, promują antyamerykańskie wartości oraz wykorzystują sale wykładowe do głoszenia lewicowej propagandy". Podobny charakter ma witryna Dean's List recenzująca uniwersytety m.in. na podstawie dominujących na nich wartości. Analizując takie czynniki jak stopień uprzedzeń rasowych, poparcie lub jego brak dla aktywistów kultury *woke* oraz ewentualna działalność konserwatywnych zrzeszeń studenckich, algorytm strony ocenia uczelnie, przyznając im noty, co ma umożliwić młodzieży chcącej kontynuować edukację podjęcie świadomej decyzji odnośnie do wyboru szkoły wyższej.

Do recenzowania szkół podstawowych i średnich stworzono portal School Board Watchlist wskazujący okręgi szkolne, w których w ramach lekcji prowadzi się kursy o transpłciowości, organizuje spotkania z *drag queen* lub stosuje politykę neutralnych płciowo toalet. Wskazano, że objętym systemem powszechnej edukacji dzieciom przekazuje się treści nieakceptowane, a nawet wyraźne negowane przez ich rodziców. Argumentowano, że bez wiedzy i zgody tych ostatnich do programu nauczania wprowadza się materiały o treściach seksualnych lub nowych koncepcjach postrzegania historii i rzeczywistości społeczno-politycznej. Chodzi m.in. o krytyczną teorię rasy zakładającą istnienie rasizmu systemowego czy o Projekt 1619 przyjmujący negatywną ocenę tradycyjnie podziwianych postaci i wydarzeń w historii Stanów Zjednoczonych. Strona identyfikuje stojące na czele okręgów rady szkolne wspierające implementację takich teorii, nagłaśnia ich działania oraz zachęca rodziców do zwalczania tego typu przedsięwzięć.

Co więcej, organizacja podjęła współpracę z innymi podmiotami reprezentującymi konserwatystów, takimi jak walcząca z nadmierną

ingerencją rządu i stająca w obronie wolności nauczania Freedom Foundation czy skoncentrowana na mniejszości afroamerykańskiej Blexit Foundation. Celem tej ostatniej jest zmiana tradycyjnego przywiązania mniejszości rasowej do Partii Demokratycznej na rzecz bardziej prawicowych poglądów, zwłaszcza w kontekście gospodarczym oraz politycznym. Popularność TPUSA – spotkania z Kirkiem odbyły się również na najlepszych brytyjskich uniwersytetach, takich jak Oxford czy Cambridge – zaowocowała również powołaniem w 2019 r. analogicznego stowarzyszenia w Wielkiej Brytanii (Turning Point UK), którego przedstawicielstwa działają na ponad 30 brytyjskich uniwersytetach, zwracając uwagę na konieczność powrotu współczesnych młodych ludzi do tradycyjnych wartości, takich jak patriotyzm czy rodzina nuklearna.

Jak dotychczas największym wstrząsem dla Turning Point USA okazała się śmierć jej założyciela – Kirk został zamordowany strzałem z broni palnej 10 września 2025 r., podczas spotkania ze studentami na Utah Valley University. To wydarzenie wywołało wielkie poruszenie opinii publicznej i było szeroko komentowane przez przedstawicieli wielu środowisk politycznych. W uroczystościach żałobnych, które odbyły się 21 września w Glendale, w Arizonie uczestniczyło blisko 100 tys. osób, w tym prezydent Stanów Zjednoczonych Donald Trump, wiceprezydent James David Vance, minister obrony Pete Hegseth, minister zdrowia i opieki społecznej Robert F. Kennedy Jr. oraz wielu innych. Współpracownicy Kirka zobowiązali się kontynuować jego działalność, mianując dyrektorem generalnym organizacji jego żonę – Ericę Kirk.

Środowiska republikańskie i konserwatywne pozytywnie oceniają inicjatywy podejmowane przez Turning Point USA, wskazując, że stanowi ona nową jakość w dyskusji o sprawach państwa. Docenia się przede wszystkim merytoryczną i rzeczową argumentację oraz fakt, że przedstawiciele organizacji wchodzą w bezpośrednie interakcje z młodymi ludźmi. Podkreśla się zaangażowanie i oddanie liderów dbających o formę, zróżnicowanie i znaczną liczbę podejmowanych przedsięwzięć, od formułowania internetowych komunikatów, poprzez opracowanie profesjonalnych materiałów informacyjnych, aż po organizację ogólnokrajowych spotkań i konferencji. Z uznaniem mówi się, o jego wpływie na wspólnoty akademickie, które w wielu przypadkach na nowo z większą

intensywnością zaczęły prowadzić dialog o istotnych społecznie kwestiach, co zmobilizowało i zachęciło do działania studentów i studentki.

Organizacja była jednak również wielokrotnie krytykowana; oskarżano ją m.in. o przekraczanie granic i naruszanie standardów moralnych. Chodzi tu głównie o doniesienia mówiące o płaceniu nastolatkom za umieszczanie postów w social mediach wspierających stanowisko Turning Point USA (np. dotyczących rzekomego zawyżania przez władze danych dotyczących zachorowań na COVID). Podnosi się także, iż tworzenie list uniwersytetów i wykładowców akademickich o poglądach lewicowych może prowadzić do zastraszania akademików oraz ograniczenia wolności wypowiedzi. Zarzuty dotyczą również manipulacji emocjami młodzieży oraz jej polaryzacji poprzez formułowanie uznawanej niejednokrotnie za agresywną retoryki bazującej niekiedy na uproszczonej wizji świata, zwłaszcza w odniesieniu do gospodarki czy polityki. Przeciwnicy TPUSA znajdują w rozpowszechnianych przez nią materiałach treści nacjonalistyczne i ksenofobiczne, które antagonizują młodzież, utrudniając jej przyjęcie innego niż własny punktu widzenia.

Elżbieta Sadowska-Wieciech

A. Binder, J.L. Kidder, *The Channels of Student Activism How the Left and Right Are Winning (and Losing) in Campus Politics Today*, University of Chicago Press, Chicago 2022; M. Boedy, *Guns and Freedom: The Second Amendment Rhetoric of Turning Point USA*, [w:] *Rethoric and Guns*, L. Wilkes, G. Kreuter, R. Skinnell (eds.), University Press of Colorado, Louisville 2022; A. Fucci, T. Catalano, *Missing the (Turning) point: The erosion of democracy at an American University*, „Journal of Language and Politics" 2019, vol. 18, no. 3; Ch. Kirk, *Right Wing Revolution: How to Beat the Woke and Save the West*, Winning Team Publishing, Lafayette 2024.

U

USTAWA CXL Z 2021 R. O OBRONIE NARODOWEJ ORAZ WĘGIERSKICH SIŁACH ZBROJNYCH (węg. 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről) to obowiązujący od 22 grudnia 2021 r. dokument określający podstawy, cele, zasady obronne państwa oraz funkcjonowania armii węgierskiej. Wśród najważniejszych cech ustawy należy wymienić wdrożenie mechanizmów reagowania na sytuacje w razie kryzysu obronnego, zasady natychmiastowego działania państwa w razie ataku, jak również regulacji statusu prawnego, struktury organizacyjnej oraz systemu dowodzenia węgierskich sił zbrojnych. Ten obszerny dokument składa się ze 118 paragrafów zawartych w 17 rozdziałach. Rozdział 1 poprzedza preambuła, w której wskazano, że ustawa została uchwalona w celu ochrony niepodległości, ludności, integralności terytorialnej, granic. Ponadto ma na celu wzmocnienie świadomości obronnej obywateli przy jednoczesnym oparciu działań obronnych na zasadach powstrzymywania się od użycia siły, a także podjęcia starań do prowadzenia pokojowego rozwiązywania sporów. Uwzględniając wprowadzony podział na 4 części, przytoczyć można następujące zapisy ustawy:

1. Część 1 (*Podstawy obrony ojczyzny*) rozpoczyna rozdział 1 zatytułowany *Przepisy ogólne*, zgodnie z którym obrona ojczyzny stanowi sprawę narodową, a przygotowanie obywateli do zadań obronnych w czasie pokoju powinno mieć charakter dobrowolny. Ponadto uzasadniono podstawowe zasady organizacji i wykonywania zadań obronnych, a także zawarto katalog definicji, które obejmują kluczowe pojęcia wykorzystywane w ustawie. Rozdział 2 odwołuje się do zasad zarządzania obroną narodową, określając podział kompetencji pomiędzy kluczowymi organami władzy publicznej, takimi jak Zgromadzenie Narodowe, prezydent Republiki Węgier, rząd oraz minister obrony narodowej. Ponadto zawarto tam regulacje zasad podejmowania decyzji dotyczących operacji wojskowych – w szczególności tych, które wymagają użycia i stacjonowania wojsk obcych na terytorium kraju oraz użycia węgierskich sił zbrojnych poza granicami Węgier. *Obowiązki obronne i zwolnienia* to tytuł rozdziału 3, który kompleksowo reguluje zadania służby wojskowej, informacyjnej, a także szczególnych zasad wykonywania obowiązków obrony cywilnej w okresie konfliktu zbrojnego. Umożliwia to wskazanie katalogu zadań zaliczanych do danej dziedziny, takich jak alarmowanie, ewakuacja, ratownictwo, utrzymanie porządku oraz zabezpieczenie infrastruktury krytycznej. W rozdziale 4 poruszono problematykę administracyjnej kary obronnej i postępowań specjalistycznych, które zgodnie z treścią ustawy nakładane są przez organy administracji rządowej w przypadku naruszenia obowiązków wynikających z przepisów o obronności. Ponadto uregulowana została procedura uprawnień do udziału w projektach realizowanych w ramach NATO Security Investment Programme. Rozdział 5 reguluje określone zasady dotyczące personelu organizacji obronnych, a także określa obowiązek stałego podnoszenia kwalifikacji oraz uzupełnienia wiedzy obronnej przez pracowników cywilnych struktur obronnych. Wskazuje również możliwość umarzania należności wobec zmarłych pracowników organizacji obronnych w zależności od oceny przebiegu służby. W rozdziale 6 odwołano się do zasad

gospodarowania nieruchomościami przeznaczonymi na potrzeby obronności, a także uregulowano zasady służebności.

2. Część 2 ustawy, którą zatytułowano *Siły zbrojne*, rozpoczyna rozdział 7 określający status prawny węgierskich sił zbrojnych. Wskazano, iż stanowią one hierarchicznie zorganizowaną formację, która w czasie pokoju oparta jest na zasadzie dobrowolności, a w czasie wojny także na powszechnym obowiązku obrony. Ponadto uregulowane zostały zasady udostępniania sprzętu i środków technicznych sił zbrojnych, a także określono uprawnienia żołnierzy delegowanych do zadań wspierających. Przedstawiony został także zakres stosowania środków przymusu oraz zasady jego legalności. W rozdziale 8 określono zasady tworzenia, reorganizacji i znoszenia węgierskich struktur organizacji sił zbrojnych, a także sprecyzowano zadania centralnego organu administracji wojskowej. Rozdział 9 ustawy porusza kwestie zasad naboru personelu sił zbrojnych, regulując skład osobowy, obowiązek złożenia przysięgi wojskowej przy rozpoczęciu służby, a także system rezerw wojskowych opartych na elementach dobrowolnych lub obowiązkowych. Ponadto wskazano kategorie osób wchodzących w skład rezerwy oraz określono tryb wydawania kart powołania do pełnienia służby. Rozdział 10 koncentruje się na systemie zależności służbowych opartych na hierarchii kierowania i dowodzeń sił zbrojnych Węgier. Uregulowane zostały zasady przyznawania awansów, a także kierowania jednostkami podporządkowanymi wspólnym dowództwom. Ponadto wskazano, jakie podmioty posiadają prawo wydawania poleceń służbowych, a także określono zasady odpowiedzialności za rozkaz wykonywanych poleceń przez żołnierzy na służbie. Rozdział 11 zatytułowany *Wybrane środki bezpieczeństwa* zwraca uwagę na zasady ochrony i zabezpieczenia obiektów, mienia oraz personelu organizacji obronnych. Ponadto reguluje uprawnienia posiadane przez wojskowe służby porządkowe, środki ograniczenia wolności osobistej, a także przypadków uprawniających do zatrzymania i doprowadzenia wobec żołnierzy oraz osób przebywających na terenie obiektów wojskowych. *Użycie broni i innych środków przymusu* to tytuł rozdziału 12, który m.in.

określa zasadę konieczności i proporcjonalności przy użyciu broni, a także reguluje szczególne sytuacje dopuszczające użycie broni palnej oraz sekwencję czynności poprzedzających. Ponadto uregulowany został tryb wnoszenia i rozpatrywania skarg związanych z użyciem broni – zarówno przez siły powietrzne, jak i żołnierzy pełniących służbę za granicą. W rozdziale 13 zwrócono uwagę na zasady prowadzenia ćwiczeń wojskowych, zakładając, że krajowe szkolenia z użyciem broni powinny być realizowane zasadniczo na terenie nieruchomości, które pozostają w zarządzaniu przez resort obrony. Rozdział 14 określił symbole oraz oznaczenia wojskowe, gdzie odwołano się m.in. do sztandarów naczelnego dowódcy, jednostek, wstęg, bander, znaków historycznych oraz oznaczeń węgierskich (państwowych) sił zbrojnych. W dalszych częściach wskazano zasady oznaczania pojazdów wojskowych, stworzono katalog oznaczeń służących identyfikacji personelu, zasad noszenia munduru, a także przewidziano możliwość nadawania honorowych stopni wojskowych osobom wspierającym cele obronne państwa węgierskiego.

3. Część 3 zatytułowaną *Zarządzanie kryzysami wojskowymi* rozpoczyna rozdział 15 zwracający szczególną uwagę na funkcjonowanie tzw. instytucji sytuacji kryzysu obronnego, które w ustawie określone zostały jako zespoły skoordynowanych działań defensywnych zarządzanych na wniosek ministra właściwego do spraw obronnych przez węgierski rząd. Ponadto uregulowano reguły obowiązywania sytuacji kryzysu obronnego oraz stanów nadzwyczajnych, a także określony został katalog środków możliwych do zastosowania w czasie sytuacji kryzysu defensywnego (np. podwyższenie gotowości struktur obronnych, intensyfikacja działań rozpoznawczych i cybernetycznych, a także wspólne działania wojska i policji w celu ochrony obiektów i ludności). Rozdział 16 zwraca uwagę na potrzebę podjęcia natychmiastowego działania rządu Węgier poprzez odparcie nagłego ataku jeszcze przed formalnym wprowadzeniem stanu wojennego lub wyjątkowego w celu ochrony terytorium państwa lub porządku konstytucyjnego. Ponadto wskazano, że w takim przypadku żołnierze będą zobowiązani

do użycia broni oraz uzbrojenia, które zostało powierzone, wobec członków zewnętrznych grup przebywających nielegalnie na terytorium państwa i podejmujących działania zbrojne zagrażające bezpieczeństwu Węgier.

4. Część 4 poświęcona została przepisom końcowym, które rozpoczyna rozdział 17. Wskazano w nim obowiązek przygotowania oraz okresowego przeglądu regulacji dotyczących statusu poborowego, a także obowiązkowej pracy w zakresie obronności w czasie pokoju, co ma przyczynić się do stałego zapewniania gotowość legislacyjnej państwa węgierskiego. W końcowych przepisach ustawy zwrócono również uwagę na szeroki katalog delegacji ustawowych dla rządu oraz ministra właściwego do spraw obronnych. Te dotyczą m.in. kwestii kierowania obroną i siłami zbrojnymi, realizacją międzynarodowej strategii NATO, zarządzania systemami alarmowymi, działalnością administracji publicznej w sektorze obronnym, inwestycji infrastrukturalnych, cyberobrony, a także szkoleń. Ustawa posiada 2 załączniki: pierwszy to wykaz stanowisk i podmiotów skategoryzowanych w ramach instytucjonalizacji *meghagyás*, zgodnie z którą kategoria I dotyczy najwyższych organów państwa oraz osób pełniących kluczowe funkcje konstytucyjne, a II obejmuje centralne i terenowe organy władzy, sądy, bank centralny, media publiczne, organizacje obronne, służby porządkowe, podmioty infrastruktury krytycznej oraz związki wyznaniowe. Do kategorii III zakwalifikowano podmioty indywidualne wyznaczane decyzją terytorialnych komisji obronnych. Załącznik 2 określa z kolei treść przysięgi wojskowej, która jest odrębna dla żołnierzy odbywających służbę z bronią, bez broni oraz w węgierskiej straży koronnej (Honvéd Koronaőrség).

Wprowadzenie w życie Ustawy CXL z 2021 r. o obronie narodowej oraz węgierskich siłach zbrojnych z całą pewnością przyczyniło się do aktualizacji regulacji administracji obronnej i bezpieczeństwa Węgier względem dynamicznie ewoluujących zagrożeń. Wśród opinii zawartych w analizach naukowych oraz publicystyce odwołującej się do węgierskiej ustawy można dostrzec przychylność w związku z zasadnością utworzenia ram planowania obronnego, a także wprowadzenia przyspieszonej

procedury decyzyjnej, co w przyszłości może istotnie przyczynić się do zwiększenia odporności Węgier na ewentualne zagrożenia.

Artur Jach-Chrząszcz

2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről, https://njt.hu/jogszabaly/2021-140-00-00 (dostęp 25.11.2025); *A honvédelmi szempontból fontos infrastruktúrák drónvédelmének kérdéseiIssues of Countering Unmanned Aerial Vehicles in Relation to Critical Infrastructure from a National Defence Perspective*, „Műszaki Katonai Közlöny" 2025, no. 35(2), 10.32562/mkk.2025.2.3 (dostęp 30.12.2025); A. Bencsik, M. Karpiuk, M. Kelemen, *The Status of the Armed Forces in Hungary, Poland and Slovakia*, „Ius et Securitas"2024, vol. 2, https://iusetsecuritas.pl/wp-content/uploads/2025/04/1_Andras-Bencsik-Miroslaw-Karpiuk-Miroslav-Kelemen.pdf?utm_source=chatgpt.com (dostęp 25.11.2025); T. Benkő, *A sikeres haderőfejlesztés záloga (2.)*, https://real.mtak.hu/161865/1/01_BenkoTiborny.vezerezredes_3-16.pdf (dostęp 30.12.2025); P. Kádár, *A magyar védelem és biztonság szabályozás reformjának rövid áttekintése / A short overview of the reform of Hungarian defence and security regulations*, „Hadtudomány" 2022, vol. 1, https://doi.org/10.17047/HADTUD.2022.32.1.61 (dostęp 25.11.2025); V. Krisztián, C. Sarkadi-Illyés, *A kormány hamarosan dönthet a katonai műveletekről*, https://www.economx.hu/belfold/honvedseg-haboru-fegyverek-katonak-honvedelmi-miniszterium.796360.html (dostęp 25.11.2025); S.P. Till, *A Magyar Honvédség feladatrendszerének újraszabályozása az új honvédelmi törvény tükrében*, https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20MT_2023_6_TILL_Szabolcs_A%20Magyar%20Honvédség%20feladatrendszerének%20újraszabályozása%20az%20új%20honvédelmi%20törvény%20tükrében%20.pdf html (dostęp 25.11.2025).

USTAWA LXIX Z 2024 R. O WĘGIERSKIM CYBERBEZPIECZEŃSTWIE (węg. 2024. évi LXIX. törvény Magyarország kiberbiztonságáról) to obowiązujący od 1 stycznia 2025 r. dokument stanowiący pełną implementację unijnej dyrektywy NIS2 oraz konsolidację wcześniejszych rozporoszonych regulacji (ustawa o bezpieczeństwie informacji organów państwowych z 2013 r. oraz ustawa o certyfikacji i nadzorze cyberbezpieczeństwa z 2023 r.) bezpośrednio związanych z węgierskim sektorem cyberbezpieczeństwa. Ustawa ta, mając na celu podniesienie poziomu ochrony krajowej infrastruktury cyfrowej, nakłada szeroki katalog obowiązków na podmioty publiczne oraz prywatne, tj. obowiązki rejestracyjne, wdrożenia systemów zarządzania ryzykiem oraz procedur reagowania

na incydenty, zabezpieczania techniczne oraz regularne audyty. W 2025 r. celem przesunięcia kluczowych terminów realizacji obowiązków w zakresie cyberbezpieczeństwa ustawa została znowelizowana, a zmiany weszły w życie 31 maja 2025 r. Ten obszerny dokument składa się 10 rozdziałów oraz 92 paragrafów. Uwzględniając wprowadzony podział, przytoczyć można następujące zapisy Ustawy LXIX z 2024 r. o węgierskim cyberbezpieczeństwie:

1. W rozdziale 1 odwołano się do przepisów ogólnych, precyzując, które systemy informacji elektronicznej oraz jakie rodzaje działalności podlegają obowiązkom państwa, gospodarki i bezpieczeństwa kraju. Rozdział ten zawiera również definicje kluczowych pojęć, takich jak system informacji elektronicznej, bezpieczeństwo informacji, incydent cyberbezpieczeństwa, a także określa ogólne zasady stosowania ustawy, w tym relacje do innych aktów prawnych oraz podstawowych obowiązków organizacji w zakresie zapewnienia bezpieczeństwa systemów informatycznych.
2. Rozdział 2 odwołuje się do obowiązków organizacji oraz wymagań wobec systemów informacji elektronicznej. Dokument m.in. wprowadza wymóg wdrożenia i utrzymywania systemu zarządzania ryzykiem, stosowania środków ochrony proporcjonalnych do klasy bezpieczeństwa systemu oraz ich regularnej aktualizacji. Ponadto ustanawia obowiązki sprawozdawcze wobec krajowego organu ds. cyberbezpieczeństwa, nakłada obowiązek wyznaczenia osoby odpowiedzialnej za bezpieczeństwo systemów informacyjnych, wprowadza obowiązek przeprowadzania cyklicznych audytów cyberbezpieczeństwa oraz określa zasady ochrony systemów wsparcia. Rozdział zawiera także regulacje dotyczące centralnego rejestru nazw domen najwyższego poziomu, w tym zasad gromadzenia, przetwarzania oraz udostępniania danych właściwym organom.
3. W kolejnym rozdziale ustawy można zapoznać się z regulacjami nadzoru cyberbezpieczeństwa, które wprowadzają m.in. zasady audytów, procedur dopuszczalności do uzyskania wpisów rejestrowych, a także zakresu badań, tj. testy penetracyjne, analiza kodu czy kryptografia. Rozdział określa właściwość organów nadzorczych, wskazując, że nadzór nad systemami informacji elektronicznej

organizacji sprawować będzie krajowy organ ds. cyberbezpieczeństwa oraz SZTFH, natomiast w przypadku systemów służących celom obronności właściwym jest niezależny organ ds. cyberbezpieczeństwa w sektorze obronnym, który działa na podstawie prawa i nie podlega poleceniom w zakresie spraw urzędowych. SZTFH wykonuje analogiczne zadania wobec organizacji z określonych grup, może nakazywać dodatkowe środki, żądać dokumentów i danych, a także przeprowadzać nadzwyczajne kontrole i audyty. W przypadku istotnych zagrożeń bezpieczeństwa powstałych w następstwie przeprowadzonych audytów w rozdziale wskazuje się na obowiązek niezwłocznego informowania organów państwowych. Przewiduje się także szeroki katalog środków nadzorczych i sankcji, w tym ostrzeżenia, nakazy usunięcia naruszeń, wyznaczenie inspektora ds. bezpieczeństwa informacji oraz dochodzenie kosztów działań zapobiegawczych.

4. Certyfikację bezpieczeństwa w rozdziale 4 określają procedury dotyczące ochrony danych, zapewnienia poufności, integralności oraz zdolności do szybkiego odtwarzania systemów bezpieczeństwa w następstwie cyberataków. W tej części ustawy wprowadzono także 3 poziomy niezawodności: podstawowy, znaczący i wysoki, które zostały powiązane z rodzajem ryzyka, a także charakterem zagrożeń określających minimalne działania oceniające dla każdego poziomu (przegląd dokumentacji technicznej, weryfikację braku znanych luk, testy funkcji bezpieczeństwa, a także testy penetracyjne). Ponadto określone zostały zasady wydawania węgierskich cyfrowych certyfikatów deklaracji zgodności, a także omówiono zasady oznaczania cyfrowych produktów, usług i procesów. Przewidziano też zasady postępowania przed organem certyfikującym, w tym termin rozpatrywania spraw, procedurę zgłaszania jednostek oceniających zgodność do Komisji Europejskiej oraz warunki udzielania zezwoleń jednostkom oceniającym zgodność na wydawanie certyfikatów o „wysokim" poziomie niezawodności.
5. Rozdział 5 wprowadza szczegółowe przepisy dotyczące zobowiązania do stosowania postkwantowego szyfrowania. Ustawa w tej części zobowiązuje podmioty oferujące tego rodzaju rozwiązania

szyfrowe do zapewniania poufności, integralności i dostępności danych, a także systemów informacyjnych z wykorzystaniem kryptografii odpornej na zagrożenia, które mogłyby wynikać z rozwoju komputerów kwantowych. Zgodność z tymi wymogami podlega certyfikacji przez uprawnione podmioty wpisane do rejestru SZTFH, które w myśl ustawy będą wydawać specjalistyczne rekomendacje, a także informować organ nadzorczy o zagrożeniach dla ciągłości działania lub powstałych naruszeniach prawa.

6. Kolejny rozdział wyznacza podmioty uprawnione do prowadzenia badań podatności systemów informacji elektronicznej – organy państwowe, centrum zarządzania incydentami w obszarze obronności cybernetycznej, a także certyfikowane podmioty gospodarcze wpisane do rejestru SZTFH. Wskazano, iż osoby przeprowadzające badania podatności muszą przejść kontrolę bezpieczeństwa narodowego, posiadać wiedzę specjalistyczną, co najmniej 2-letnie doświadczenie zawodowe oraz zostać wpisane do rejestru osób uprawnionych, przy czym warunkiem jest zatrudnianie co najmniej 2 takich ekspertów. W rozdziale omówiona została także rola krajowego organu ds. cyberbezpieczeństwa w zakresie kontroli (nakaz wykonania badania podatności na dowolny podmiot), a także kompetencje dotyczące możliwości nakładania kar finansowych.
7. Rozdział 7 ustanawia kompleksowy system zarządzania przepisami związanymi z incydentami cyberbezpieczeństwa. Wyszczególnia się krajowe centrum zarządzania incydentami (KC) dla systemów cywilnych oraz odrębne centrum dla systemów obronnych (CO). Do głównych zadań KC należą monitorowanie zagrożeń, wczesne ostrzeganie, zapobieganie oraz reagowanie na incydenty, zarządzanie sytuacjami kryzysowymi, działania informacyjne, a także współpraca międzynarodowa. CO z kolei analizuje ruch sieciowy, wykrywa ataki i koordynuje sposoby podejmowania reakcji na zagrożenia. Rozdział wdraża także możliwość stosowania nadzwyczajnych środków służących przerwaniu ataku z cyberprzestrzeni na podstawie decyzji organów rządowych, z uwzględnieniem interesów bezpieczeństwa narodowego. §69 ustawy przewiduje także środki służące przerwaniu ataku z cyberprzestrzeni, podjęte na

podstawie decyzji osoby wyznaczonej przez rząd, które muszą być proporcjonalne i uwzględniać interesy bezpieczeństwa narodowego, obrony, ścigania przestępstw oraz polityki zagranicznej.

8. Organizacja systemu koordynacji zadań związanych z cyberbezpieczeństwem ustanawia w rozdziale 8 funkcję komisarza ds. cyberbezpieczeństwa, który odpowiada za realizację krajowej strategii bezpieczeństwa cybernetycznego oraz krajowego planu zarządzania kryzysowego w zakresie cyberbezpieczeństwa. Ponadto w tej części dokumentu ustanowione zostaje Krajowe Centrum Koordynacyjne (KCK) jako punkt kontaktowy dla wspólnoty kompetencji w zakresie cyberbezpieczeństwa określające zakres danych gromadzonych o organizacjach ubiegających się o członkostwo w UE oraz organy, którym dane mogą być przekazywane – w szczególności Europejskiemu Centrum Kompetencji, organom ds. cyberbezpieczeństwa i krajowemu centrum reagowania na incydenty. Rozdział ponadto szczegółowo uregulował zasady zarządzania sytuacjami kryzysowymi w cyberprzestrzeni, np. w przypadku ogłoszenia kryzysu rząd może wprowadzać nadzwyczajne środki, takie jak podwyższanie gotowości wybranych organów, ograniczanie usług łączności, korzystanie z zasobów podmiotów prywatnych, gromadzenie narzędzi istotnych dla cyberbezpieczeństwa, a także informowanie struktur unijnych i sojuszniczych.
9. Przedostatni rozdział reguluje przepisy dotyczące przetwarzania i ochrony danych przez organy ds. cyberbezpieczeństwa. Ustawa wprowadza także ścisły obowiązek zachowania poufności danych przez organy i ich pracowników, a dla systemów związanych z obronnością narodową przewidziano ograniczenia w zakresie ujawniania informacji. Jednocześnie dopuszczono publikowanie anonimowych statystyk dotyczących stanu cyberprzestrzeni, incydentów i trendów, pod warunkiem, że nie pozwalają one na identyfikację konkretnych podatności systemów. Rozdział precyzuje również zasady przekazywania informacji innym organom krajowym, a także instytucjom unijnym – powinno przebiegać w zgodzie z przepisami o ochronie informacji niejawnych i danych

osobowych, a także nie może naruszać interesów bezpieczeństwa narodowego, publicznego oraz obronnego państwa.

10. Ostatni rozdział zawiera przepisy upoważniające, przejściowe oraz regulacje dotyczące zgodności z konstytucją i prawem UE. Dokument przyznaje szerokie kompetencje regulacyjne rządowi, ministrom i prezesowi SZTFH, które obejmują m.in. doprecyzowanie obowiązków organizacji, zasad klasyfikacji systemów danych, wymogów bezpieczeństwa, nadzoru, audytów, badań podatności, obsługi incydentów, ćwiczeń, zarządzania kryzysowego, certyfikacji cyberbezpieczeństwa, szyfrowania postkwantowego oraz prowadzenia rejestrów. Przepisy przewidują także stopniowe wdrażanie nowych środków ochronnych, powiązanie dawnych klas bezpieczeństwa z nowymi regulacjami oraz uznanie niektórych organizacji za krytyczne do czasu zakończenia procedur umożliwiających wyznaczenie nowych regulacji. Rozdział potwierdza także zgodność ustawy z konstytucją i wskazuje, że implementuje ona kluczowe akty UE – w tym dyrektywę NIS2.

Wprowadzenie ustawy LXIX z 2024 r. węgierskie kancelarie w analizach oraz komentarzach określają jako „nową erę zgodności z przepisami cyberbezpieczeństwa", która z jednej strony, oceniana jest jako krok w stronę uporządkowania przepisów prawnych i ich konsystencji przy dynamicznej zmienności zagrożeń w cyberprzestrzeni, a z drugiej – stanowi dla mniejszych podmiotów wyzwanie organizacyjne oraz kosztowe z uwagi na konieczność audytów, klasyfikacji systemów, a także brakujące wytyczne i interpretacje w przypadkach niektórych dostawców usług IT (np. centra danych czy usługodawców chmurowych), co może w najbliższym czasie prowadzić do niepewności legislacyjnych w tym zakresie.

Artur Jach-Chrząszcz

2024. évi LXIX. törvény – Magyarország kiberbiztonságáról, https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/HU_ACT_ON_CYBERSECURITY_2024_hu.pdf (dostęp 25.11.2025); Z. Balogh, *NIS2: New Cybersecurity Act and Important Changes*, https://www.rsm.hu/blogs/nis2-new-cybersecurity-act-and-important-changes? (dostęp 25.11.2025); K. Horváth, *Hungary extends cybersecurity registration obligations for entities falling under NIS2*, https://

cms-lawnow.com/en/ealerts/2025/08/hungary-extends-cybersecurity-registration-obligations-for-entities-falling-under-nis2? (dostęp 25.11.2025); G. Katona, *NIS 2 in Hungary: A New Era of Cybersecurity Compliance*, https://www.lexology.com/library/detail.aspx?g=b53f7c60-fa25-4f99-bed2-1a5c178e24de&utm, (dostęp 25.11.2025); A. Menczelesz, *The digital defence line: Hungary adopts comprehensive cybersecurity law*, https://www.schoenherr.eu/content/the-digital-defence-line-hungary-adopts-comprehensive-cybersecurity-law? (dostęp 25.11.2025); C. Vári, *Hungary: New framework for cybersecurity regulation*, https://insightplus.bakermckenzie.com/bm/data-technology/hungary-new-framework-for-cybersecurity-regulation? (dostęp 25.11.2025).

V

VIGINUM (Francuska Służba Czujności i Ochrony przed Zagranicznymi Zakłóceniami Cyfrowym) – służba techniczna i operacyjna odpowiedzialna za monitorowanie i ochronę przed zagraniczną ingerencją cyfrową, działająca przy Sekretariacie Generalnym ds. Obrony i Bezpieczeństwa Narodowego. Agencja rządowa odpowiada za wykrywanie i zwalczanie zagranicznych ingerencji cyfrowych, takich jak dezinformacja i manipulacja informacją w sieci. Agencja została utworzona 13 lipca 2021 r. w odpowiedzi na zagrożenie ze strony działań zewnętrznych, analizując treści publikowane online i identyfikując ich źródła. Powstanie agencji było odpowiedzią na incydent z 2017 r., kiedy to wykradziono i opublikowano e-maile francuskiego prezydenta Emmanuela Macrona w trakcie kampanii wyborczej, co przypisano rosyjskim służbom specjalnym.

Podczas posiedzenia Rady Obrony Narodowej i Bezpieczeństwa 12 stycznia 2021 r. Macron podjął decyzję o utworzeniu takiego podmiotu. Nową służbę narodową stworzono na mocy dekretu nr 2021-922 z dnia 13 lipca 2021 r. Francuska agencja VIGINUM rozpoczęła działalność 7 grudnia 2021 r., po tym jak dekret upoważnił ją do gromadzenia informacji w sieciach społecznościowych i ich przechowywania. W przypadku

wyborów prezydenckich we Francji w 2022 r. agencja monitorowała możliwe interwencje zagraniczne mające na celu promowanie lub zniechęcanie obywateli do pójścia na wybory.

VIGINUM ma za zadanie wykrywać, analizować i charakteryzować zagraniczne operacje ingerencji cyfrowej oraz identyfikować manipulacje informacjami pochodzącymi z zagranicy, których celem jest destabilizacja państwa i zaszkodzenia interesom Francji. Agencja monitoruje treści dostępne publicznie na platformach internetowych, aby identyfikować i analizować kampanie dezinformacyjne prowadzone przez obce państwa. Nie chodzi o ukazanie prawdy, ale o wykrycie, czy masowe przepływy informacji są wynikiem ingerencji zagranicznej. Według Stéphane'a Bouillona, sekretarza generalnego ds. obrony i bezpieczeństwa narodowego Francji, usługa powinna umożliwiać „politykom, dyplomatom, przedstawicielom wymiaru sprawiedliwości i prasie sprawdzenie, czy spośród 400 tys. tweetów powtarzających daną informację 200 tys. pochodzi z farmy botów z regionu poza Francją lub czy dana debata ma swoje źródło w rosyjskiej farmie trolli".

Zgodnie z treścią dekretu opublikowanego w Dzienniku Urzędowym VIGINUM „jest upoważniona do wdrażania komputerowego i zautomatyzowanego przetwarzania danych osobowych". Przetwarzanie to ma na celu wykrywanie i charakteryzowanie operacji, w których bezpośrednio lub pośrednio uczestniczy państwo obce lub zagraniczny podmiot niebędący państwem, mające na celu sztuczne lub zautomatyzowane, masowe i celowe, rozpowszechnianie ewidentnie niedokładnych lub wprowadzających w błąd twierdzeń lub zarzutów dotyczących faktów, które mogą zaszkodzić podstawowym interesom Francji.

Dekret stanowi, że zebrane dane są przechowywane maksymalnie przez 6 miesięcy, a usługa VIGINUM działa na platformach wymagających rejestracji, których liczba odwiedzających we Francji przekracza 5 mln użytkowników miesięcznie. Usługa nie analizuje treści prywatnych komunikatorów, takich jak WhatsApp, Facebook czy Messenger.

Bouillon oświadczył podczas przesłuchania przed Komisją Obrony Narodowej i Sił Zbrojnych Zgromadzenia Narodowego w czerwcu 2021 r.: „Powiedzmy sobie jasno, absolutnie nie wolno nam mówić, że taka a taka informacja jest prawdziwa, a taka a taka nie. To jest rola polityków, mediów

i to jest rola wymiaru sprawiedliwości. Nie może to być rola administracji i nie powinna być to jej rola".

VIGINUM podlega sekretarzowi generalnemu ds. obrony i bezpieczeństwa narodowego, organowi odpowiedzialnemu za wspieranie premiera w wykonywaniu jego obowiązków w zakresie obrony i bezpieczeństwa narodowego.

Pierwszym szefem VIGINUM został Gabriel Ferriol, inżynier i sędzia specjalizujący się w inżynierii informacyjnej, komunikacyjnej i kognitywnej. Na jego zastępcę został wyznaczony podpułkownik Marc-Antoine Brillant.

VIGINUM ma za zadanie chronić Francję i jej podstawowe interesy przed zagranicznymi operacjami manipulacji informacjami na platformach cyfrowych.

Główne działania VIGINUM obejmują:

- wykrywanie i charakteryzowanie kampanii manipulacji informacjami prowadzonych przez zagranicznych aktorów;
- monitorowanie i analizowanie treści, które mogą szkodzić francuskim interesom narodowym, w tym w kontekście ważnych wydarzeń (np. igrzyska olimpijskie w Paryżu 2024, wybory);
- publikowanie raportów technicznych dotyczących zidentyfikowanych zagrożeń i operacji wpływu, często przypisywanych konkretnym państwom, takim jak Rosja czy Azerbejdżan;
- współpracę z partnerami krajowymi (takimi jak France Télévisions, PEReN) i międzynarodowymi w celu zwalczania dezinformacji;
- badanie wykorzystania nowych technologii, takich jak generatywna sztuczna inteligencja (GenAI), do celów manipulacji informacjami.

Działalność VIGINUM koncentruje się na ochronie debaty publicznej i przestrzeni informacyjnej przed skoordynowanymi, masowymi i celowymi działaniami dezinformacyjnymi, które mają na celu destabilizację społeczeństwa lub wpływanie na politykę kraju.

W 2022 r. w VIGINUM pracowało 42 agentów, z czego 62% stanowiły kobiety. Obecnie to 65 osób, głównie specjalistów w dziedzinie nauki o danych, wywiadu opartego na otwartych źródłach, nauk politycznych

i geopolityki. Budżet startowy szacowano na 5 mln euro, a następnie 12 mln euro rocznie.

Od końca 2023 r. VIGINUM obserwuje i dokumentuje złośliwą kampanię, która może wpłynąć na francuskojęzyczną debatę publiczną w internecie. Operacja ta, przywoływana w raportach pod nazwą „Matrioszka", jest aktywna co najmniej od września 2023 r.

W lutym 2024 r. francuski urząd ds. ochrony cyberprzestrzeni VIGINUM zidentyfikował rosyjską siatkę 193 portali internetowych prowadzących w sposób skoordynowany akcję dezinformacyjną wymierzoną w kraje europejskie, w tym Polskę, które propagują rosyjską narrację w sprawie wojny w Ukrainie. Celem było przedstawienie rosyjskiej inwazji w korzystny sposób, a także ataki na ukraińskich liderów politycznych i wojskowych. Portale nie tworzyły własnych treści, jedynie przekazywały publikacje rosyjskich serwisów informacyjnych i oficjalnych stron administracji rosyjskiej.

VIGINUM publikuje wyniki swoich śledztw i stosowane metody, aby promować transparentność i umożliwić niezależną weryfikację przez dziennikarzy i społeczeństwo. Śledztwa VIGINUM wykazały, że większość treści została pierwotnie opublikowana na rosyjskojęzycznych kanałach Telegram, które zostały już zidentyfikowane w operacjach informacyjnych. Najbardziej znany jest raport agencji z 5 lutego 2025 r. na temat rosyjskiej kampanii dezinformacyjnej „Matrioszka" obejmującej zakłócenia cyfrowe, które manipulowały informacjami skierowanymi do europejskich mediów i organizacji factcheckingowych. VIGINUM uważa, że jej celem jest dyskredytacja mediów, osób publicznych i organizacji zajmujących się weryfikacją faktów oraz promowanie treści prorosyjskich.

Szczególną uwagę w raporcie zwrócono na rażące przypadki manipulacji informacjami, zaobserwowane podczas wyborów prezydenckich w Rumunii w 2024 r. Przeanalizowano metody stosowane na TikToku do sztucznego promowania określonych treści i wykorzystywania influencerów oraz oceniono ryzyko stosowania takich metod we Francji.

„Skuteczność złośliwych operacji wpływu zagranicznego jest determinowana wsparciem, jakie otrzymują od ludności będącej celem. Jedną z pułapek, na jakie możemy się natknąć, jest przecenianie ich wpływu" – stwierdzili senatorowie francuscy we wstępie do swojego 369-stronicowego

raportu. Oprócz Rosji komisja śledcza zidentyfikowała Chiny, Turcję i Azerbejdżan jako kluczowych „konkurentów" prowadzących wojnę o wpływy przeciwko Francji.

Między wrześniem a grudniem 2023 r. agencja VIGINUM analizowała działalność sieci cyfrowych „portali informacyjnych", które rozpowszechniają prorosyjskie treści wśród międzynarodowych odbiorców – znalazła co najmniej 193 strony internetowe, które rozpowszechniają fałszywe twierdzenia, że wojna Rosji w Ukrainie jest legalną operacją wojskową, i krytykują Zachód. Głównym celem tych portali jest relacjonowanie wojny rosyjsko-ukraińskiej poprzez pozytywne przedstawienie „specjalnej operacji wojskowej" oraz oczernianie Ukrainy i jej przywódców – stwierdza raport francuski. Silnie ideologicznie zorientowana treść ujawnia wyraźnie nieścisłe lub wprowadzające w błąd narracje, które dotyczą portalu skierowanego do Francji, *Prawda-fr(.)com*, bezpośrednio uczestnicząc w polaryzowaniu francuskojęzycznej cyfrowej debaty publicznej.

Raport wskazuje, że tego rodzaju strony internetowe skierowane są również do krajów zachodnich wspierających Ukrainę i jej ludność, takich jak Francja, Niemcy, Austria, Szwajcaria, Polska, Hiszpania, Wielka Brytania i USA. W większości domen znajduje się słowo „prawda", a wygląd stron przypomina wcześniej zidentyfikowane serwisy, które docierają do rosyjskojęzycznych odbiorców w Ukrainie.

Francuskie śledztwo wykazało również powiązania z adresami IP o podobnych cechach, które są skierowane do rosyjskiej i ukraińskiej publiczności. Strony często zawierały teksty skopiowane z prorosyjskich kont w mediach społecznościowych, witryn rosyjskich agencji prasowych oraz lokalnych serwisów. Na kontach w mediach społecznościowych, takich jak Telegram, stosowały „masową automatyzację udostępniania treści", jak podali francuscy eksperci. Również tematyka była kontrowersyjna – „przyczyniała się do podziału francuskojęzycznej debaty publicznej".

Agencja VIGINUM ujawniła działalność rosyjskiej sieci dezinformacyjnej o nazwie „Portal Kombat", składającej się z cyfrowych „portali informacyjnych" rozpowszechniających prorosyjskie treści, pozytywnie relacjonujących rosyjską inwazję na Ukrainę i oczerniających władze kijowskie, a także szerzących prokremlowską propagandę w celu wywierania wpływu na opinię publiczną, szczególnie we Francji. Strony tej

sieci nie produkują żadnych oryginalnych treści, lecz masowo przekazują publikacje głównie z 3 typów źródeł: kont i platform społecznościowych rosyjskich lub prorosyjskich społeczności, rosyjskich agencji prasowych oraz oficjalnych stron instytucji.

W próbie dotarcia do szerokiej publiczności sieć ta stosuje kilka technik, takich jak staranny wybór źródeł prorosyjskiej propagandy zgodnie z lokalizacją docelową, masowa automatyzacja dystrybucji treści czy optymalizacja cytowania w wyszukiwarkach dla wpływania na zachodnią opinię publiczną i rozpowszechniania określonych narracji i manipulacji.

Agencja VIGINUM w raporcie oskarżyła Rosjan o podszywanie się pod rząd i media w celu szerzenia dezinformacji oraz rozpoczęcie „kampanii manipulacji cyfrową informacją przeciwko Francji" przy wsparciu rosyjskich podmiotów państwowych. Kampania, którą organizacja monitorowała przez ponad rok, polegała na tworzeniu fałszywych stron internetowych podszywających się pod francuskie departamenty rządowe i 4 najpopularniejsze francuskie dzienniki: „20 Minutes", „Le Monde", „Le Parisien" i „Le Figaro", obok fałszywych kont w mediach społecznościowych.

Oficjalny raport o operacji wpływu, opublikowany na stronie Sekretariatu Generalnego ds. Obrony i Bezpieczeństwa Narodowego Francji, ostrzega, że kampania próbowała szerzyć wiele fałszywych narracji mających na celu podważenie francuskiego wsparcia dla Ukrainy. Sugerowały one, że sankcje wymierzone w Rosję są nieskuteczne i szkodliwe dla krajów europejskich; państwa zachodnie wykazują rusofobię; ukraińskie siły zbrojne przejawiają cechy barbarzyńskie i mają powiazania z neonazistami, a przyjmowanie ukraińskich uchodźców ma negatywny wpływ na kraje goszczące.

Olga Wasiuta

P. Alonso, *Amaelle Guiton, Les dessous de «Viginum», la future agence contre les manipulations de l'information*, 30.06.2021, https://www.liberation.fr/societe/police-justice/les-dessous-de-viginum-la-future-agence-contre-les-manipulations-de-linformation-20210630_NFTB6CNJ6ZGDDFBMZRZKBBANYA/ (dostęp 20.11.2025); *Foreign digital interference – Publication of the VIGINUM report on information manipulation*, 5.02.2025, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/

foreign-digital-interference-publication-of-the-viginum-report-on-information (dostęp 18.11.2025); *Francja odkryła sieć blisko 200 portali z rosyjską propagandą wymierzoną w europejskie kraje. Na liście jest Polska*, https://wyborcza.biz/biznes/7,177150,30693902,francja-odkryla-siec-blisko-200-portali-z-rosyjska-propaganda.html?disableRedirects=true (dostęp 20.11.2025); *French agency uncovers pro-Russian propaganda network*, 13.02.2024 , https://www.euronews.com/next/2024/02/13/french-agency-uncovers-pro-russian-propaganda-network (dostęp 18.11.2025); Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide – Rapport. RAPPORTS DE COMMISSION D'ENQUÊTE. Rapport n° 739 (2023–2024), tome I, déposé le 23 juillet 2024, https://www.senat.fr/rap/r23-739-1/r23-739-10.html (dostęp 20.11.2025); A. Martin, *France accuses Russians of impersonating French government and media to spread disinformation*, 13.06.2023, https://therecord.media/france-accuses-russians-of-impersonating-french-government-media-misinformation (dostęp 18.11.2025); *Projet de loi de finances pour*, 2022, https://www.budget.gouv.fr/files/files/plf/plf2022/PLF_2022-I.pdf (dostęp 20.11.2025); *ПОРТАЛ КОМБАТ Структурированная и скоординированная сеть пророссийской пропаганды*, 12.02.2024, https://www.sgdsn.gouv.fr/files/files/Publications/20240212_NP_SGDSN_VIGINUM_RAPPORT-RESEAU-PORTAL-KOMBAT_RU_VF.pdf (dostęp 20.11.2025).

W

WERBUNEK – termin związany z czynnościami operacyjno-rozpoznawczymi i metodą agenturalną (→ agentura). To wymagające, wieloetapowe przedsięwzięcie, którego celem jest nakłonienie uprzednio rozpracowanej i wyselekcjonowanej osoby fizycznej do podjęcia współpracy z policją, organami o uprawnieniach policji czy służbami specjalnymi, zaś jego finałem jest rozmowa werbunkowa. W przypadku powodzenia nakłoniony zostaje agentem, który następnie dostarcza informacje oraz realizuje przydzielone mu zadania. Werbunek może być realizowany zarówno przez funkcjonariuszy, jak i pozyskaną uprzednio agenturę. Nakłanianym do podjęcia współpracy może być obywatel państwa obcego, co jest zwłaszcza charakterystyczne dla działań służb specjalnych i to zarówno tych o charakterze wywiadowczym, jak i kontrwywiadowczym. W przypadku werbunku realizowanego na potrzeby policji czy organów o uprawnieniach policji w praktyce będzie on przeważnie ukierunkowany na obywateli własnego państwa; wynika to bowiem ze specyfiki zadań, jakie są stawiane przez ustawodawcę. W przypadku zamierzeń werbunkowych realizowanych przez policję czy organy o uprawnieniach policji uprzednie konflikty

z prawem, przynależność do środowisk przestępczych osoby werbowanej mogą być jej zaletą, a nie przeciwskazaniem do pozyskania.

Bezwzględnym wymogiem werbunku jest dochowanie zasad konspiracji działań. Docelowa współpraca zwerbowanej osoby ma bowiem mieć charakter niejawny. Niepowodzenie werbunku rodzi nieuniknione niebezpieczeństwo zdekonspirowania policji, organów o uprawnieniach policji czy służb specjalnych. Ponadto może za sobą pociągać dekonspirację osób dokonujących werbunku; tym samym szczególne znaczenie ma staranne przygotowanie do podjętych działań, co wymaga skrupulatności, przewidywania scenariuszy rozwoju sytuacji operacyjnej (→ sytuacja operacyjna) i jest ze swej natury długotrwałe.

Wyróżnia się werbunek:

- jednorazowy;
- stopniowy;
- dla pozornie innego celu;
- pod → obcą flagą.

Werbunek jednorazowy ma miejsce, gdy pozyskanie do współpracy jest wynikiem 1 rozmowy. Stopniowy realizowany jest na przestrzeni czasu poprzez konsekwentne wciąganie osoby do pełnej współpracy. Dla pozornie innego celu wykorzystywany jest, gdy samo osiągnięcie zgody na współpracę nie jest tak wymagające jak uzyskanie ukierunkowanego jej celu; wówczas nie od razu ujawnia się faktyczny cel współpracy, ale czyni się to po przyzwyczajeniu agenta do realizacji zadań, które dopiero z czasem nakierowuje się na pierwotny cel. Werbunek pod obcą flagą jest metodą z zakresu czynności operacyjno-rozpoznawczych służb specjalnych o charakterze wywiadowczym; polega na podawaniu się podczas działań werbunkowych za przedstawiciela służby wywiadu pochodzącego z kraju ojczystego potencjalnego agenta lub sojuszniczego czy też darzonego przez niego sympatią. Po dokonaniu w ten sposób skutecznego werbunku zasadne jest niewyprowadzanie zwerbowanego agenta z błędu, by uniknąć powzięcia przez niego wiedzy, dla kogo w istocie pracuje, co mogłoby skutkować zakończeniem współpracy.

Zanim dojdzie do werbunku, konieczne jest wytypowanie kandydatów do potencjalnej współpracy. W tym celu, w pierwszym kroku, dokonuje się określenia kręgu osób mających określoną wiedzę lub też możliwość

dotarcia do określnej jednostki będącej przedmiotem zainteresowania (czyli tzw. figuranta). W drugim kroku z tak określonego kręgu osób wybiera się potencjalnego kandydata do zwerbowania – odbywa się to w drodze selekcji i bierze się w niej pod uwagę praktyczne możliwości pozyskania danych osób do współpracy. Konieczne jest zatem jak najszersze, oczywiście niejawne, poznanie ich profili osobistych, zawodowych, majątkowych czy społecznych. Ważne będzie też zidentyfikowanie ewentualnie posiadanych talentów czy słabości – realizuje się zatem operacyjne rozpracowanie potencjalnych kandydatów do zwerbowania, by wyłonić z nich tego, wobec którego podjęty zostanie werbunek. Oprócz weryfikacji w stosownych bazach danych jest to realizowane przy użyciu różnorakich metod z zakresu czynności operacyjno-rozpoznawczych, takich jak w szczególności analiza operacyjna, wywiad operacyjny, eksperyment operacyjny czy → kombinacja operacyjna. Wszelkie czynności na tym etapie rzutują bezpośrednio na skuteczność podejmowanego werbunku.

Po rozpracowaniu kandydatów i wyselekcjonowaniu kandydata do zwerbowania opracowuje się taktykę działań werbunkowych. Kluczowe znaczenie ma tu identyfikacja podstawy werbunku i opracowanie sposobu jego przeprowadzenia. Zagadnienia te są ściśle związane z psychologicznymi uwarunkowaniami uzyskania trwałej zgody na współpracę. Zakładając trafną potencjalną motywację do podjęcia współpracy, taktyka działań werbunkowych polegać będzie na przekonaniu werbowanego, iż podjęcie przez niego współpracy zaspokoi jego niezrealizowane potrzeby, przy jednoczesnym zapewnieniu mu bezpieczeństwa. Potencjalne ryzyko, jakie będzie brać pod uwagę werbowany, musi być zarysowane jako odległe lub przyćmione otwierającymi się możliwościami.

W literaturze, mimo różnorakich zastrzeżeń, w zakresie motywacji do współpracy wskazuje się w szczególności na koncepcję MICE (akronim od angielskich słów: *money*, *ideology*, *coercion*, *ego* – pieniądze, ideologia, przymus, ego). Zakłada ona, że podstawy werbunku, a co za tym idzie – sposoby jego przeprowadzenia, zawierać się będą w 4 segmentach potencjalnych motywacji podjęcia współpracy przez wskazanego kandydata. Mogą one występować nie tylko samodzielnie, ale i w połączeniu z pozostałymi, lub też ewoluować w trakcie współpracy.

Pierwszy segment w koncepcji MICE to korzyści finansowe: pieniądze mogą zrównoważyć poczucie zagrożenia w związku z podjętą współpracą i zapewnić bezpieczeństwo na przyszłość. Powszechnie uznaje się, że najczęściej motywem podjęcia współpracy przez werbowanego jest chęć uzyskania przez niego właśnie takich korzyści. Trudno jednoznacznie orzec, czy tak będzie w odniesieniu do policji i organów o uprawnieniach policji, ale jeśli chodzi o służby specjalne, warto w tym kontekście przywołać amerykańskie opracowania Centrum Badań nad Personelem Obronnym i Bezpieczeństwem (The Defense Personnel and Security Research Center, PERSEREC). Od 1992 r. podmiot ten analizuje ujawnione przypadki współpracy obywateli amerykańskich z obcymi służbami wywiadowczymi. I tak w opracowaniu obejmujących lata 1947–2015 porównano dane dotyczące 3 grup osób w oparciu o moment rozpoczęcia działalności szpiegowskiej: 1947–1979 (wczesna faza zimnej wojny), 1980–1989 (późna faza zimnej wojny) oraz 1990–2015 (okres postsowiecki). W pierwszej grupie zbadano 68 osób, w drugiej – 74, w trzeciej natomiast – 67. Odpowiedzi ostatniej puli respondentów dostarczają najbardziej przydatne dane; wśród motywacji Amerykanów, którzy po 1990 r. popełnili przestępstwa związane z podjęciem współpracy z obcymi służbami specjalnymi, korzyści finansowe nadal były jedyną lub najważniejszą podstawą werbunku (37%). Widać tu jednak wyraźny spadek z 44% i 63%, odpowiednio w pierwszej i drugiej grupie badanych, przy czym dla 10% był to jedyny motyw podjęcia współpracy, a dla 27% – główny. Podobne wyniki uzyskano podczas badania realizowanego na Uniwersytecie w Malmo pod nazwą *Podatność Europy na rosyjskie działania szpiegowskie. Co motywuje Europejczyków do szpiegowania na rzecz Rosji?* (*Europe's susceptibility to Russian espionage operations. What motivates Europeans to spy for Russia*?), które obejmowało ujawnione przypadki współpracy ze służbami specjalnymi Federacji Rosyjskiej w latach 2012–2024; korzyści finansowe były najczęstszym czynnikiem motywacyjnym (40% wskazań).

Odnosząc się do kolejnej motywacji w koncepcji MICE, tj. ideologii, można stwierdzić, że osoby zwerbowane na tej podstawie są najbardziej pożądane. Już w polskim międzywojennym opracowaniu pn. *Służba wywiadowcza i ochrona przeciwszpiegowska* wskazywano na przewagę agentów ideowych nad „płatnymi". Ci pierwsi mieli mieć lepsze wyniki pracy,

jak również nie wymagali szczególnej kontroli, przejawiając mniejszą skłonność do zdrady. Również chociażby i instrukcja werbunkowa OSS (Office of Strategic Services – Biuro Służb Strategicznych) podkreślała, by „nie kupować ludzi". Historia zna liczne przypadki werbunków na podstawie motywacji ideologicznej; oprócz szeroko opisywanych przypadków, chociażby Harolda „Kima" Philby'ego, Donalda Macleana, Guya Burgessa, Anthony'ego Blunta, Johna Cairncrossa czy Ryszarda Kuklińskiego, warto tu dla zobrazowania zagadnienia przywołać postać Any Belén Montes. Ta urodzona w 1957 r. obywatelka Stanów Zjednoczonych, pochodzenia hiszpańskiego, w 1979 r. podjęła pracę w Departamencie Sprawiedliwości, najpierw jako sekretarka, a potem – asystent prawny. Jej werbunek przez kubańskie służby specjalne miał miejsce w 1984 r. – zwrócił się wówczas do niej jej kolega ze studiów, znający jej krytyczny stosunek do amerykańskiej polityki zagranicznej w państwach Ameryki Łacińskiej. Poprosił ją o spotkanie z przyjaciółmi, którzy szukali kogoś, kto mógłby przetłumaczyć artykuły na temat Nikaragui z języka hiszpańskiego na angielski. Pod tą → legendą w rzeczywistości zorganizowano spotkanie z funkcjonariuszami kubańskiego wywiadu DGI (Direccion General de Inteligencia – Główny Zarząd Wywiadu) pracującymi pod przykrywką dyplomatyczną. Podczas spotkania doszło do skutecznego werbunku Montes, która zgodziła się pomóc Nikaragui za pośrednictwem Kubańczyków – 3 miesiące później niejawnie udała się na Kubę, by następnie podjąć wysiłki w uzyskaniu pracy mogącej rozszerzyć jej dostęp do amerykańskich tajemnic państwowych. Wstąpiła do DIA (Defense Intelligence Agency – Agencji Wywiadu Obronnego Stanów Zjednoczonych), gdzie podczas swojej 16-letniej kariery jako analityk otrzymywała awanse, certyfikaty dostępu do tajnych informacji, jak również wielokrotnie była nagradzana za wydajną służbę. Dopiero w 2001 r. została zatrzymana i postawiono je zarzuty szpiegostwa na rzecz Kuby. W 2002 r. w ramach ugody częściowo przyznała się do winy; w tym samym roku skazano ją na 25 lat pozbawienia wolności. W przeciwieństwie do Aldricha Amesa czy Roberta Hansena motywacje Montes do podjęcia współpracy z kubańskim wywiadem miały podłoże ideologiczne: prawdopodobnie przez cały okres długoletniej współpracy nie uzyskała z tego tytułu jakichkolwiek korzyści materialnych. Jak później wyjaśniła, jej decyzja, by podjąć działalność na rzecz Kuby, wynikała z jej negatywnej

oceny działań Stanów Zjednoczonych, zwłaszcza w kontekście wsparcia dla partyzantów Contras w Nikaragui. Miała też przeświadczenie o błędności polityki amerykańskiej wobec Kuby; w jej ocenie rząd w Hawanie nie tylko nie stanowił dla Stanów Zjednoczonych zagrożenia, ale w istocie nie był im wrogi. Sądziła, że ewentualny upadek Związku Sowieckiego zwiększy prawdopodobieństwo amerykańskiej inwazji na wyspę. Mimo iż zaprzeczała, jakoby miała komunistyczne poglądy, przejawiała sympatię dla polityki władz w Hawanie i sandinistów w Managui. W rezultacie jej przekonania ułatwiły werbunek, choć Montes konsekwentnie twierdziła, że nie pracowała „dla" kubańskiego wywiadu, ale „z" kubańskim wywiadem.

W koncepcji MICE kolejną motywacją do współpracy jest przymus, nierzadko rozumiany jako szantaż. Podczas tego rodzaju werbunku często wykorzystuje się materiały kompromitujące bądź obciążające; te pierwsze należy dobrać z rozwagą, gdyż to, co jest moralnie naganne dla jednych, nie musi być tak postrzegane przez kandydata do werbunku. Drugie z kolei pozwalają na wystosowanie groźby (uniknięcie ewentualnych konsekwencji prawnych, odpowiedzialności w zamian za współpracę). Błędne jest twierdzenie, że przymus to metoda typowa dla werbunków realizowanych przez funkcjonariuszy państw totalitarnych czy autorytarnych. Przykładowo w podręcznikach Służby Bezpieczeństwa wykazywano, że rodzi to opór, tym samym bardziej wskazane było szukanie motywacji pozytywnych dla zamierzeń werbunkowych. Współczesne badania, jak chociażby Davida Charneya i Johna Irvina, dowodzą, iż osoba przymuszona do współpracy będzie ją realizować jedynie w niezbędnym zakresie, dążąc do jej zerwania tak szybko, jak to tylko możliwe. Niemniej jednak po dziś dzień, wobec braku innych możliwości, werbunek wykorzystujący jako motywację przymus jest realizowany; nic nie stoi bowiem na przeszkodzie, by w dalszych fazach współpracy szukać innych motywacji do jej kontynuowania. Znamiennym może być tu przypadek Denissa Metsavasa, majora estońskich sił zbrojnych zwerbowanego do współpracy przez rosyjski wywiad wojskowy GRU (Gławnoje Razwiedywatielnoje Uprawlenije – Główny Zarząd Wywiadowczy) w 2007 r., podczas pobytu w Smoleńsku. W ramach kombinacji operacyjnej nagrano jego stosunek seksualny z nowo poznaną kobietą, by następnie zagrozić mu odpowiedzialnością karną za rzekome przestępstwo gwałtu. Metsavas zgodził się na współpracę – na

przestrzeni kolejnych lat, aż do 2018 r., przekazywał Rosjanom informacje objęte tajemnicą wojskową, a z czasem zaczął uzyskiwać z tego tytułu wynagrodzenie. Rolę kuriera pełnił jego ojciec, który będąc z pochodzenia etnicznym Rosjaninem, przejawiał motywacje natury ideologicznej, co nie pozostawało bez wpływu na postawę Metsavasa.

W koncepcji MICE ostatnią motywacją do współpracy jest ego – mowa zatem o czynnikach natury egoistycznej, wynikających zwłaszcza z niedowartościowania lub potrzeby wzmocnienia poczucia własnej wartości poprzez podjętą współpracę. Ta motywacja będzie zasadna wobec jednostek mających przeświadczenie, że są pomijane, niezauważane w swoim środowisku, zwłaszcza zawodowym. Werbunek ma je dowartościować, unaocznić, że są ważne, a to, co mają do przekazania, ma znaczenie. Być może również umożliwić odwet na „prześladowcach". Można też stwierdzić, że zarówno korzyści finansowe, jak i ideologiczne w istocie także są formą wyrażenia własnego ego. Szczególnie podatne na tego rodzaju werbunek są osobowości narcystyczne. Dobrym przykładem jest sprawa Jonathana Pollarda – mimo czytelnych oznak zaburzeń osobowości i fałszywych twierdzeń na temat swoich rzekomych zdolności przyjęto go do służby jako analityka amerykańskiej marynarki wojennej, zaś w 1984 r. podjął współpracę z izraelskimi służbami specjalnymi. Wyrazem jego cech charakterologicznych może być list, jaki wysłał z zakładu karnego już po swoim skazaniu za szpiegostwo na rzecz Izraela: twierdził w nim, że jego działalność faktycznie służyła wzmocnieniu długoterminowych interesów bezpieczeństwa Stanów Zjednoczonych na Bliskim Wschodzie. Wykazując cechy narcystyczne, przedstawiał siebie jako lidera sprawy narodowej.

W kontekście polskim nie sposób nie zauważyć, iż obecne uwarunkowania prawne zabraniają polskim służbom specjalnym (art. 37 Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 41 Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 26 Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym) korzystania z tajnej współpracy swoich obywateli, jeśli pełnią oni funkcję:

1. Posłów i senatorów.

2. Osób zajmujących kierownicze stanowiska państwowe, o których mowa w art. 2 Ustawy z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe.
3. Dyrektorów generalnych w ministerstwach, urzędach centralnych lub urzędach wojewódzkich.
4. Sędziów, asesorów sądowych, prokuratorów, adwokatów i radców prawnych.
5. Członków rady nadzorczej, członków zarządu oraz dyrektorów programów Telewizji Polskiej – Spółka Akcyjna, i Polskiego Radia – Spółka Akcyjna, a także dyrektorów terenowych oddziałów Telewizji Polskiej – Spółka Akcyjna.
6. Dyrektora generalnego, dyrektorów biur oraz kierowników oddziałów regionalnych Polskiej Agencji Prasowej – Spółka Akcyjna.
7. Nadawców w rozumieniu art. 4 pkt 5 Ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji.
8. Redaktorów naczelnych, dziennikarzy lub osób prowadzących działalność wydawniczą, o których mowa w Ustawie z dnia 26 stycznia 1984 r. – Prawo prasowe.
9. Rektorów.
10. Członków Rady Głównej Nauki i Szkolnictwa Wyższego, Polskiej Komisji Akredytacyjnej i Rady Doskonałości Naukowej.

Jeżeli jest to jednak uzasadnione względami bezpieczeństwa państwa, możliwe staje się za zgodą w szczególności prezesa Rady Ministrów korzystanie z tajnej współpracy z osobami wymienionymi w pkt 7 i 8. Brakuje analogicznych zakazów w ustawach o Policji czy Straży Granicznej; w praktyce oznacza to niemożność werbunku przez polskie służby specjalne agentury pośród wymienionych już osób pełniących najważniejsze funkcje państwowe. W rezultacie wręcz uniemożliwia skuteczne operacyjne rozpoznanie środowisk, które winny być przecież w obszarze ich szczególnego zainteresowania; jest jednocześnie wręcz zaproszeniem obcych służb specjalnych do ich infiltracji. Swobodny wyjazd w maju 2024 r. sędziego Wojewódzkiego Sądu Administracyjnego w Warszawie Tomasza Szmydta na terytorium Białorusi, gdzie poprosił o „opiekę i ochronę", zrzekając się jednocześnie funkcji sędziego jako

wyraz protestu przeciwko „niesprawiedliwej i krzywdzącej" polityce Rzeczypospolitej wobec Republiki Białorusi i Federacji Rosyjskiej, jest tego wymowną konsekwencją.

Jakub Purchla

R. Burket, *Rethinking an Old Approach. An Alternative Framework for Agent Recruitment: From MICE to RASCLS*, „Studies in Intelligence" 2013, vol. 57, no. 1; D.L. Charney, J.A. Irvin, *The Psychology of Espionage*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2016; K. Horosiewicz, *Wybrane elementy taktyki werbowania i współpracy z osobowymi źródłami informacji*, Wyższa Szkoła Policji w Szczytnie, Szczytno 2019; *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989)*, T. Ruzikowski (red.), Instytut Pamięci Narodowej, Warszawa 2004; D. Koreś, *Instrukcja Oddziału II Sztabu Głównego WP o prowadzeniu ewidencji agentów i raportów organizacyjnych z 1931 r.*, [w:] *Studia nad wywiadem i kontrwywiadem Polski w XX wieku*, t. 2, W. Skóra, P. Skubisz (red.), Instytut Pamięci Narodowej, Szczecin 2015; J.H. Larecki, *Wielki leksykon tajnych służb świata*, Rytm, Warszawa 2017; F. Musiał, *Podręcznik bezpieki. Teoria pracy operacyjnej Służby Bezpieczeństwa w świetle wydawnictw resortowych Ministerstwa Spraw Wewnętrznych PRL (1970–1989)*, Instytut Pamięci Narodowej, Warszawa–Kraków 2018; *Review of the Actions Taken to Deter, Detect and Investigate the Espionage Activities of Ana Belen Montes*, Office of the Inspector General of the Department of Defence – United States, Arlington 2005; *The Expanding Spectrum of Espionage by Americans, 1947–2015*, Departament of Defence – United States, PERSEREC, Seaside 2017; U.M. Wilder, *Why Spy? The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2; www.youtube.com/watch?v=52-wgeRoWX4 (dostęp 5.12.2025); Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. 2002, nr 74, poz. 676 ze zm.; Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz.U. 2006, nr 104, poz. 708 ze zm.; Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. 2006, nr 104, poz. 709 ze zm.

WĘGIERSKA STRATEGIA CYBERBEZPIECZEŃSTWA 2025–2030 (węg. Magyarország kiberbiztonsági stratégiája) to obowiązujący od 1 kwietnia 2025 r. dokument przyjęty zgodnie z Rozporządzeniem rządu Węgier numer 1089/2025 (III.31). Strategia zakładająca przygotowanie krajowego planu działań na lata 2025–2030 tworzy kompleksowe i wiążące ramy zgodnie z dyrektywą NIS2 oraz ustawą o cyberbezpieczeństwie

Węgier z 2024 r. Przedstawiona na początku dokumentu wizja ukazuje konieczność kompleksowego wzmocnienia i utrzymania poziomu krajowego cyberbezpieczeństwa oraz cyfrowego dobrostanu poprzez budowę odpornego na zagrożenia systemu bezpieczeństwa, stałego podnoszenia świadomości społecznej, skuteczną cyfryzację administracji publicznej, podmiotów gospodarczych, rozwój współpracy w obszarze bezpieczeństwa, a także pogłębianie partnerstwa państwa ze społeczeństwem w zakresie obrony oraz bezpieczeństwa. Struktura strategii obok przedstawionej już wizji obejmuje wprowadzenie, 7 rozdziałów oraz postanowienia końcowe. Uwzględniając wprowadzony podział, przytoczyć można następujące zapisy Węgierskiej strategii cyberbezpieczeństwa 2025–2030:

- we wprowadzeniu zaznaczono, iż funkcjonujące dotychczas strategie cyberbezpieczeństwa na Węgrzech przyczyniły się do wzrostu odporności na cyberzagrożenia, jednak dynamiczny rozwój cyfryzacji i narastająca liczba cyberataków wymagają dalszego doskonalenia systemu ochrony, rozwoju ram prawnych, zdolności obronnych oraz podnoszenia świadomości społecznej. Cyfryzacja, wspierana przez Krajową strategię cyfryzacji, Program cyfrowego obywatelstwa i odpowiednie ustawy, stanowi jednocześnie szansę rozwojową i źródło nowych zagrożeń, dlatego zapewnienie bezpiecznej cyberprzestrzeni zostało uznane za wspólną odpowiedzialność państwa, instytucji, gospodarki, nauki i obywateli, która może być realizowana we współpracy międzynarodowej – zgodnie z zobowiązaniami UE i NATO, przy jednoczesnej ochronie suwerenności państwa i infrastruktury krytycznej;
- w kolejnym rozdziale zatytułowanym *Największe wyzwania w cyberprzestrzeni* przedstawiono dynamicznie narastające ryzyko wynikające z burzliwego otoczenia bezpieczeństwa, w którym tradycyjne i nowe zagrożenia współwystępują, a aktywność podmiotów państwowych oraz niepaństwowych w sieci zwiększa podatność państw na ataki. Podrozdział 3.1 odwołuje się do wojen XXI w., które zgodnie z koncepcją autorów unaoczniły bezpośredni wpływ cyberataków na procesy polityczne, gospodarcze i społeczne, a także na bezpieczeństwo narodowe.

Podrozdział 3.2 wskazuje na zakłócenie równowagi między jednostką a społeczeństwem, wzmocnione przez pandemię oraz rozwój cyfrowych kampanii dezinformacyjnych osłabiających zaufanie publiczne. Podrozdział 3.3 akcentuje rosnące uzależnienie od technologii, szczególnie wśród nieletnich, co poszerza powierzchnię ataku. Podrozdział 3.4 identyfikuje zagrożenia dla łańcuchów dostaw, a 3.5 – gwałtowny wzrost naruszeń bezpieczeństwa danych, w tym ataków *ransomware*. Dodatkowo podkreślono niedoskonałość regulacji, szybkie tempo rozwoju technologii (AI, IoT, 5G), potrzebę wzmacniania świadomości i kompetencji oraz konieczność międzynarodowej współpracy wobec transgranicznej natury cyberzagrożeń;

– w rozdziale 4 dokonano identyfikacji kluczowych podmiotów, wskazując, że cyberbezpieczeństwo jest wspólną odpowiedzialnością państwa, gospodarki i społeczeństwa, a jego wzmocnienie wymaga zarówno skutecznej identyfikacji zagrożeń, jak i ochrony obywateli oraz ich danych w internecie. Wskazano, że ramy organizacyjne cyberobrony wyznaczają przepisy unijne oraz węgierska ustawa o cyberbezpieczeństwie, które porządkują system zarządzania, odpowiedzialność instytucji i koordynację działań na poziomie strategicznym i operacyjnym. Szczególną rolę przypisano podmiotom strategicznym, takim jak system zarządzania obronnością, Krajowa Grupa Robocza ds. Cyberbezpieczeństwa czy Krajowe Forum Cyberbezpieczeństwa, a także kluczowym podmiotom operacyjnym: zespołom CSIRT (centra reagowania na incydenty związane z cyberbezpieczeństwem), organom ds. cyberbezpieczeństwa, policji, siłom cyberobrony, ośrodkom SOC oraz instytucjom naukowym. Zwrócono uwagę na priorytetową ochronę infrastruktury krytycznej, znaczenie kadr specjalistycznych, edukacji oraz rosnącą rolę dostawców usług cyfrowych i sektora informacyjno-komunikacyjnego dla bezpieczeństwa państwa i gospodarki;
– kolejna część strategii dotyczy wzmocnienia pozycji Węgier w międzynarodowej przestrzeni cybernetycznej i zaangażowania

państwa w rozwój oraz przestrzeganie międzynarodowych norm odpowiedzialnego postępowania w cyberprzestrzeni w ramach ONZ, OBWE, Unii Europejskiej i NATO. Ważną regułą jest przestrzeganie stosowania prawa międzynarodowego oraz znaczenia globalnego, otwartego i bezpiecznego internetu. Rozdział 5 wskazuje na aktywną współpracę z państwami członkowskimi UE i NATO w zakresie cyberobrony, wspólnego rozpoznania sytuacji, wzajemnej pomocy oraz rozwoju zdolności obronnych. Zwrócono uwagę na udział Węgier w projektach budowy potencjału, innowacjach europejskich, ćwiczeniach międzynarodowych oraz zwalczaniu cyberprzestępczości we współpracy z Europolem, Interpolem i w ramach konwencji budapeszteńskiej. Podkreślono także znaczenie współpracy z podmiotami rynkowymi, koncepcji Rule-based Order oraz odpowiedzialności kierownictwa instytucji za realizację celów międzynarodowej strategii cyberbezpieczeństwa;

– w oparciu o konstytucję Węgier, Strategię bezpieczeństwa narodowego oraz Strategię wojskową z 2021 r. ogólne ustalenia strategiczne określają, że celem Węgierskiej strategii cyberbezpieczeństwa 2025–2030 jest wyznaczenie krajowych celów, kierunków i narzędzi działań państwa w cyberprzestrzeni jako części przestrzeni globalnej. Podkreślono, że cyberbezpieczeństwo jest nie tylko zadaniem obronnym, lecz także szansą gospodarczą, która wymaga rozwoju badań, innowacji oraz zdolności analitycznych. Wskazano na wspólną odpowiedzialność państwa, sektora prywatnego i społeczeństwa, konieczność wzmacniania odporności sieci, budowy zdolności operacyjnych, przejrzystych regulacji oraz kształtowania świadomości i cyberhigieny. Zwrócono uwagę na zasadę *security-by-design*, potrzebę nowoczesnych zamówień publicznych, utrzymanie krajowych zdolności cyberbezpieczeństwa oraz priorytetową ochronę infrastruktury krytycznej, w szczególności sektorów finansowego i energetycznego;
– w kolejnym rozdziale zatytułowanym *Kwestie obronności i bezpieczeństwa* wskazano, że cyberbezpieczeństwo Węgier służy

zarówno wzmocnieniu zdolności obronnych państwa, jak i budowie skutecznej siły odstraszania poprzez identyfikację, wykrywanie i pociąganie do odpowiedzialności podmiotów zagrażających suwerenności. Podkreślono, że działania w zakresie cyberobrony stanowią element skoordynowanych działań obronnych i bezpieczeństwa, realizowanych głównie w ramach kompetencji krajowych, przy jednoczesnym wsparciu sojuszników z Unii Europejskiej i NATO. Zwrócono uwagę na trudności w jednoznacznym przypisywaniu sprawstwa cyberataków oraz konieczność ostrożnych decyzji dotyczących reakcji odwetowych w oparciu o prawo krajowe i międzynarodowe. Wskazano także, że skumulowane wrogie działania w cyberprzestrzeni mogą osiągnąć próg ataku zbrojnego, a kluczowym zadaniem pozostaje strategiczna koordynacja procesów w nowym środowisku operacyjnym obrony i bezpieczeństwa;

– w rozdziale 7 dokonano sformułowania celów szczegółowych i priorytetów, zauważając, że wobec rosnącej skali i wyrafinowania zagrożeń cybernetycznych opracowana strategia opiera się na 4 filarach: wzmocnieniu krajowego systemu organizacji cyberbezpieczeństwa, intensyfikacji współpracy i innowacji, podnoszeniu świadomości oraz promowaniu certyfikacji. Podkreślono konieczność rozwoju forów współpracy, skutecznej koordynacji działań, budowy zdolności prewencyjnych, sprawnego reagowania na incydenty oraz wzmacniania zaufania do usług e-administracji i projektów inteligentnych miast. Wskazano na kluczową rolę wymiany informacji, rozwiązań opartych na sztucznej inteligencji, zaangażowania małych i średnich przedsiębiorstw, środowiska naukowego oraz wsparcia badań w obszarze nowych technologii. Szczególny nacisk położono na edukację, program *bug bounty* premiujący znalezienie i zgłoszenie luk czy błędów w infrastrukturze IT oraz rozwój kadr. Podkreślono również znaczenie certyfikacji produktów oraz usług informacyjno-komunikacyjnych, bezpiecznego wykorzystania chmury, wzmacniania suwerenności danych oraz

tworzenia stabilnych warunków regulacyjnych i finansowych dla rozwoju krajowych podmiotów rynkowych;

– w przedostatnim rozdziale poświęconym celom i priorytetom sektorowym wskazano, że cyberbezpieczeństwo powinno być wzmacniane we wszystkich najważniejszych obszarach funkcjonowania państwa. W sektorze administracji publicznej jako priorytet wskazano ochronę państwowych zasobów danych, niezawodność usług cyfrowych oraz rozwój krajowych i obronnych centrów zarządzania incydentami cyberbezpieczeństwa. W sektorze obrony narodowej strategia akcentuje rozwój zdolności cyberobronnych, współpracę z podmiotami gospodarczymi, ćwiczenia i budowę kultury bezpieczeństwa, w tym w przestrzeni kognitywnej. W sektorze informacyjno-komunikacyjnym oraz infrastruktury cyfrowej jako kluczowe elementy wskazano konsolidację infrastruktury państwowej, podnoszenie standardów technologicznych, zarządzanie ryzykiem łańcucha dostaw, a także wymianę informacji o incydentach. Jako ważną część opieki zdrowotnej wskazano ochronę danych i systemów e-zdrowia, w tym rozwiązań opartych na sztucznej inteligencji, IoT i IoMT. Podobnie istotnym elementem wrażliwości danych jest sektor rolniczy na wszystkich poziomach – od zintegrowanych czujników po przechowywane parametry w chmurach (Cloud Computing), co może przyczyniać się do ryzyka uzależnienia od globalnych dostawców usług. W sektorze kosmicznym podkreślono konieczność kompleksowej ochrony łańcucha wartości usług kosmicznych. Ostatnie sektory wymienione w rozdziale 7 dotyczą energetyki, wodociągów i gospodarki odpadami, które – jak zaznaczono w strategii – wymagają przede wszystkim wzmocnienia zabezpieczeń sieci, systemów sterowania i procesów logistycznych wobec rosnącej cyfryzacji i automatyzacji;

– w postanowieniach końcowych wskazano, że skuteczna realizacja strategii cyberbezpieczeństwa wymaga zapewnienia stabilnego i wieloźródłowego finansowania obejmującego zarówno środki z budżetu państwa, fundusze Unii Europejskiej, jak

również mechanizmy współpracy sektora publicznego i prywatnego. Podkreślono konieczność zagwarantowania odpowiednich zasobów dla wszystkich podmiotów odpowiedzialnych za cyberbezpieczeństwo, w tym na utrzymanie wykwalifikowanych specjalistów oraz ochronę kluczowych danych i systemów informacyjnych. Zwrócono również uwagę na potrzebę dostarczania decydentom rzetelnych informacji o ryzykach i ich skutkach społeczno-gospodarczych w celu racjonalnej alokacji środków. W części dotyczącej realizacji podkreślono, że wdrożenie strategii wymaga opracowania spójnego planu działania opartego na współpracy, ukierunkowanego na ograniczanie zagrożeń, wzmacnianie odporności, rozwój kadr, pogłębianie współpracy oraz stałą aktualizację programów szkoleniowych, przy jednoczesnym monitorowaniu zmian w środowisku cyberprzestrzeni i okresowym przeglądzie strategii.

W analizach oraz komentarzach węgierskich ekspertów ds. bezpieczeństwa powstałych po wprowadzeniu strategii podkreśla się, że dynamiczny wzrost zróżnicowania cyberzagrożeń, a także narastająca skala dezinformacji determinują potrzebę powołania jednolitego organu ds. cyberbezpieczeństwa. Podmiot ten mógłby pełnić funkcję koordynacyjną w zakresie działań edukacyjnych, przyczyniających się do podnoszenia poziomu świadomości społecznej. Jest to szczególnie istotne z uwagi na fakt, iż celem cyberataków mogą być nie tylko instytucje państwowe i duże podmioty gospodarcze, lecz również indywidualni obywatele.

Artur Jach-Chrząszcz

1089/2025 (III.31). *Korm. határozat Magyarország kiberbiztonsági stratégiájáról*, https://njt.hu/jogszabaly/2025-1089-30-22 (dostęp 25.11.2025); V.C. Balázs, *Kiberbiztonsági szakértő: Az edukáció szükséges, mert a tudatlanság sebezhetővé tesz*, https://mandiner.hu/belfold/2025/05/kiberstrategia (dostęp 25.11.2025); J. Bálint, B. Czakó, *Hungary extends cybersecurity registration obligations for entities falling under NIS2*, https://cms-lawnow.com/en/ealerts/2025/08/hungary-extends-cybersecurity-registration-obligations-for-entities-falling-under-nis2 (dostęp 25.11.2025); T. Bereczki, A. Liber, *Hungary's New Cybersecurity Strategy*, https://ceelegalmatters.com/briefings/29288-hungary-s-new-cybersecurity-strategy (dostęp 25.11.2025).

WĘGIERSKI PROGRAM ROZWOJU OBRONY NARODOWEJ I SIŁ ZBROJNYCH ZRÍNYI (węg. Zrínyi Honvédelmi és Haderőfejlesztési Program) to największy po transformacji ustrojowej rządowy projekt mający na celu modernizację węgierskich sił zbrojnych. Powstał 20 grudnia 2016 r., kiedy to István Simicskó (ówczesny minister obrony narodowej Węgier) zapowiedział w Budapeszcie uruchomienie programu Zrínyi 2026. Pierwotna koncepcja obejmowała 10-letnie przedsięwzięcie rozwojowe o wartości inwestycyjnej wynoszącej około 3500 mld forintów (około 9 mld euro) mające na celu bezpośrednie wsparcie założeń zawartych w Nowej strategii bezpieczeństwa narodowego Węgier (NBS). W związku z dynamicznie zmieniającą się sytuacją bezpieczeństwa w Europie po 2020 r. węgierskie władze postanowiły kontynuować rozwój programu co najmniej do roku 2030.

Węgry w latach 1989–2016 prowadziły w sektorze zbrojnym politykę częściowych zakupów oraz remontów przede wszystkim poradzieckiego sprzętu pozostającego na wyposażeniu armii: miało to bezpośrednie przełożenie na stosunkowo niski (jak na drugą dekadę XXI w.) poziom technologiczny sprzętu należącego wówczas do węgierskich sił zbrojnych. Długotrwałe utrzymanie wydatków obronnych przez Budapeszt utrzymujących się na poziomie poniżej 1% PKB pogłębiał światowy kryzys finansowy z 2008 r. Wśród wydarzeń, które mogły mieć bezpośrednie przełożenie na polityczne decyzje o uznaniu obronności za priorytet strategiczny, a tym samym o uruchomieniu Węgierskiego programu rozwoju obrony narodowej i sił zbrojnych Zrínyi, wskazuje się przede wszystkim zmianę środowiska bezpieczeństwa w Europie po 2011 r. (m.in. Arabska Wiosna, konflikt rosyjsko-ukraiński, kryzys migracyjny), a także presję polityczną na państwa członkowskie NATO w zakresie sprawiedliwego podziału obciążeń.

To właśnie zmieniające się środowisko bezpieczeństwa międzynarodowego, a także zobowiązania sojusznicze ustalone podczas szczytu NATO w Walii (2014), zgodnie z którymi państwa członkowskie zwiększą wydatki obronne do poziomu co najmniej 2% PKB, miały bezpośredni wpływ na dynamikę zmian wysokości finansowania obronności Węgier. W chwili rozpoczęcia programu (2016) wydatki tego kraju na obronność wynosiły 1,289 mld dolarów (przekładało się to na 1,003% PKB). Przyjęty

wówczas mechanizm corocznego wzrostu budżetu obronnego o 0,1% PKB miał umożliwić do 2026 r. osiągnięcie wymaganego poziomu 2% PKB. W kolejnych latach wydatki zwiększano: w 2017 r. – do 1,463 mld dolarów (1,027% PKB), w 2018 r. – do 1,792 mld dolarów (1,117% PKB), w 2019 r. – do 2,051 mld dolarów (1,254% PKB), w 2020 r. – do 2,41 mld dolarów (1,614% PKB), a w 2021 r. – do 3,060 mld dolarów (1,7% PKB). Wyjątek stanowił jedynie rok 2022, kiedy to odnotowano spadek nominalny do wydatków na poziomie 2,572 mld dolarów (1,5% PKB), jednak rok później zauważalnie zwiększono wydatki do wysokości 4,3 mld dolarów, co umożliwiło osiągnięcie poziomu przeznaczania środków na poziomie 2% PKB w 2023 r. Tendencja ta została podtrzymana w kolejnych latach, odpowiednio 2024 oraz 2025.

Jednym z pierwszych elementów przyczyniających się do modernizacji węgierskich wojsk lądowych było sformowanie nowoczesnej brygady ciężkiej. Filarem tej struktury stała się 1 Brygada Pancerna MH im. Klapka György stacjonująca w Tata (MH Klapka György 1. Páncélosdandár – Tata). W grudniu 2018 r. ogłoszono zakup 44 nowych czołgów Leopard 2A7HU oraz 24 samobieżnych haubic PzH 2000. Z końcem 2020 r. państwo węgierskie zakupiło dla celów szkoleniowych 12 zmodernizowanych czołgów Leopard 2A4HU, uzupełnieniem technicznym były z kolei pojazdy wsparcia WiSENT 2 oraz mosty towarzyszące Leguan 2. Pierwsze Leopardy 2A7HU dotarły na Węgry w roku 2023, a pełne wyposażenie batalionu osiągnięto w 2025 r. Celem zwiększenia interoperacyjności i gotowości bojowej około 800 żołnierzy węgierskich w dniach 6–24 czerwca 2025 r. uczestniczyło w międzynarodowych ćwiczeniach NATO odbywających się w ramach DEFENDER 25. Szkolenie to było szczególnie ważne dla węgierskiego personelu arteryjnego, któremu od końca 2024 r. przyszło obsługiwać zakupione w ramach programu Zrínyi 2026 samobieżne haubicoarmaty Panzerhaubitze 2000 (PzH 2000).

Modernizacji uległy ciężkie i zmechanizowane jednostki, jak również pojazdy wsparcia oraz mobilności. W sierpniu 2020 r. węgierski rząd podpisał umowę na zakup 218 gąsienicowych wozów bojowych Rheinmetall Lynx KF41, z czego 172 miały zostać wyprodukowane w nowo powstałej fabryce w węgierskim Zalaegerszeg. Produkcję krajową rozpoczęto w 2023 r., a pierwsze wozy Lynx otrzymała 30 Brygada Zmechanizowana MH im.

Kinizsi Pál (MH Kinizsi Pál 30. Páncélozott Gyalogdandár). W ramach współpracy węgiersko-tureckiej wprowadzono do użytku armii wyposażone w zdalnie sterowane wieże uzbrojenia i systemy detekcji ostrzału pojazdy Gidrán 4 × 4 oraz Nomád (Yörük).

Produkcja krajowa przemysłu obronnego była integralną częścią programu Zrínyi 2026. Od 2016 r. można zaobserwować systematyczny wzrost liczby przedsiębiorstw, których profil działalności związany jest z produkcją uzbrojenia oraz sprzętu wojskowego. Kluczowe znaczenie mają inwestycje realizowane przy współpracy z partnerami zagranicznymi, jak również budowa nowych zakładów produkcyjnych, takich jak fabryka amunicji w Várpalota (*Várpalotai lőszergyár*). W tym czasie rozpoczęto także licencyjną produkcję broni strzeleckiej, co związane było z podjętą w 2016 r. decyzją o przeprowadzeniu modernizacji umundurowania oraz wyposażenia indywidualnego węgierskich żołnierzy. Tym samym stałym elementem uzbrojenia węgierskiego wojska pozostały karabinki, pistolety, granatniki, a także będąca elementem przeciwpancernych środków rażenia amunicja krążąca. W grudniu 2022 r. węgierski holding zbrojeniowy N7 stworzył z czeską grupą Colt CZ spółkę, której głównym celem jest produkcja broni krótkiej w węgierskim zakładzie MH Arzenál Zrt. i bezpośrednie zaopatrywanie w nią węgierskich sił zbrojnych. W tym samym czasie N7 Holding Zrt. utworzył spółkę z niemiecko-izraelskim Dynamit Nobel Defence (DND), którego celem jest produkcja na Węgrzech broni przeciwpancernej RGW 110. W dobie rosnącego stosowania dronów wielozadaniowych węgierskie siły zbrojne zamówiły także bezzałogowe statki HERO produkowane przez zależną od niemieckiego koncernu Rheinmetall izraelską spółkę UVision. Zgodnie z przewidywaniami Siły Obronne Węgier zakupią około 120 sztuk dronów, z czego część prawdopodobnie zostanie wyprodukowana na Węgrzech.

Węgierski program Zrínyi od 2020 r. objął również filary obrony powietrznej, systemów rozpoznania oraz rozbudowy sił powietrznych. W listopadzie 2020 r. węgierski rząd ogłosił decyzję o zakupie 7 jednostek amerykańsko-norweskiego systemu rakietowej obrony powietrznej NASAMS-3 (2 jednostki dostarczono na Węgry w 2023 r., pozostałe 5 – rok później). Z kolei do 2028 r. powinno zakończyć się kompletowanie 11 naziemnych, mobilnych

radarów wielozadaniowych ELM-2084. Program Zrínyi 2026 charakteryzuje się również kompleksową odbudową zdolności lotniczych, która obejmuje zwiększenie floty oraz modernizację myśliwców wielozadaniowych Saab JAS 39 Gripen. Zgodnie z porozumieniem, jakie zawarto w lutym 2024 r., Węgry przedłużą wsparcie techniczne dla 14 samolotów wydzierżawionych od szwedzkiego producenta, a do 2026 r. kolejne 4 myśliwce powinny powiększyć węgierską flotę Gripenów do 18 sztuk; te po zakończonym okresie leasingu (2036) staną się własnością państwa węgierskiego. Ponadto węgierskie siły zbrojne w ramach programu Zrínyi 2026 zakupiły samoloty transportowe KC-390 (pierwszy do bazy w Kecskemét został dostarczony we wrześniu 2024 r., drugi – w listopadzie 2025 r.), a także jednostki szkoleniowo-bojowe Aero L-39 Skyfox, Zlin Z-242L i Zlin Z-143LSi.

Z końcem sierpnia 2025 r. odbyła się ceremonia przekazania węgierskiej armii łodzi SOC-R (Special Operations Craft Riverine), która na co dzień używana jest przez Marynarkę Wojenną Stanów Zjednoczonych (United States Navy). Obecny na uroczystości minister obrony Węgier Kristóf Szalay-Bobrovniczky podkreślił, że wydarzenie to uzupełnia szeroką transformację rozwoju węgierskich sił zbrojnych o ostatni (po lądzie i powietrzu), wodny filar jej działalności. Jak zaznaczył, wybór amerykańskiej jednostki poparty był nie tylko niezawodnością, ale także szeroką ofertą programu szkoleniowego realizowanego przy współpracy z amerykańskimi siłami zbrojnymi. Generał Ferenc Kajári jako istotną zaletę łodzi SOC-R wskazał wysokie zdolności umożliwiające szybkie przemieszczanie sił oraz potencjału ewakuacji Zespołów Zadaniowych Operacji Specjalnych (SOTU) w środowisku wodnym, nawet pod ostrzałem. Ponadto zauważono, że jednostki te mogą zapewniać wsparcie ogniowe, prowadzić rozpoznanie, misje wywiadowcze oraz dostarczać zaopatrzenie medyczne.

Jak zauważa László Pásztor, istotnym elementem programu Zrínyi 2026 jest także wdrażanie rozwiązań mogących przyczyniać się do stałego wzrostu uznania społecznego, wynagrodzeń oraz możliwości planowania kariery obecnych oraz przyszłych żołnierzy węgierskich sił zbrojnych. Tym samym w okresie rozpoczynającym wdrożenie programu Zrínyi 2026 do 2019 r. osiągnięto 38-procentowy wzrost płacy nominalnej węgierskich żołnierzy przy jednoczesnym oferowaniu licznych dodatkowych świadczeń, takich jak nieoprocentowane pożyczki, wsparcie mieszkaniowe czy dofinansowanie

komunikacji miejskiej. W roku 2025 węgierskie siły zbrojne kandydatom w trakcie szkolenia podstawowego zaoferowały minimalne miesięczne wynagrodzenie powyżej średniej krajowej brutto, a także premię za podpisanie kontraktu, jak również świadczenia dodatkowe, m.in. zwrot kosztów podróży, bezpłatne zakwaterowanie w koszarach lub dodatek mieszkaniowy, opiekę zdrowotną oraz dobrowolne składki na fundusz emerytalny.

Istotną rolę w procesie rekrutacyjnym do węgierskich sił zbrojnych odgrywa uruchomiony niedługo po Zrínyi 2026 Program kadetów obrony narodowej. Zgodnie z danymi w roku szkolnym 2018/2019 w programie partnerskim uczestniczyły 54 szkoły (1723 kadetów), natomiast w roku szkolnym 2024/2025 było to 155 szkół i blisko 11 tys. kadetów. Ponadto w węgierskich szkołach podstawowych wprowadzono edukacyjno-wychowawczy program Hadapród, którego celem jest kształtowanie postaw proobronnych, obywatelskich i patriotycznych wśród najmłodszych. Podobne cele wdrożone zostały również w kolejnych etapach szkolnictwa, np. w szkołach średnich utworzono przedmiot obrona narodowa, a w szkolnictwie wyższym – stypendium im. Lázára Mészárosa.

10 lat funkcjonowania programu Zrínyi 2026 miało także bezpośrednie przełożenie na węgierską gospodarkę w kontekście utrzymania istniejących i tworzenia nowych miejsc pracy. Z uwagi na obecną sytuację geopolityczną oraz umiejscowienie terytorialne Węgier w dającej się przewidzieć przyszłości procesy modernizacji sił zbrojnych z dużym prawdopodobieństwem będą kontynuowane i zgodnie z szacunkami obejmą prawdopodobnie przede wszystkim węgierski sprzęt naziemny oraz środki obrony przeciwlotniczej. Równie istotnym filarem modernizacji węgierskiego sektora obronnego jest umowa o współpracy obronnej (DCA) z USA z 2019 r., przy jednoczesnym przesunięciu Niemiec na pozycję kluczowego partnera strategicznego w Narodowej Strategii Bezpieczeństwa z 2020 r., co oznacza formalne usytuowanie Berlina powyżej dotychczasowego priorytetu relacji z Waszyngtonem. To właśnie rządy tych 2 państw wymienia się jako potencjalnych inwestorów mogących zapoczątkować wieloletni proces rekonstrukcji węgierskiej infrastruktury wojskowej w miejscowościach Kecskemét, Pápa, Tata oraz Várpalota.

Artur Jach-Chrząszcz

Agreement Between the United States of America and Hungary 19-821, https://www.state.gov/wp-content/uploads/2019/10/19-821-Hungary-Defense-TIM-S-61984-Frank.pdf (dostęp 30.12.2025); O. Balogh, *Węgierski program rozwoju armii i obronności „Zrínyi 2026" jako odpowiedź na nowe zagrożenia w regionie*, „Studia Bezpieczeństwa Narodowego" 2019, t. 15(1), https://doi.org/10.37055/sbn/132160; G. Baranyai, *Made in Hungary – átadták az első magyar gyártású Hiúz páncélost*, https://magyarnemzet.hu/belfold/2024/07/made-in-hungary-atadtak-az-elso-magyar-gyartasu-hiuz-pancelost (dostęp 30.12.2025); G. Baranyai, *Nemzeti haderő épül*, https://magyarnemzet.hu/belfold/2025/06/nemzeti-hadero-honvedelem-honvedseg-magyar-fejlesztes-gdp-nato (dostęp 30.12.2025); *Hungary's armed forces are expanded with a unique, new capability*, https://defence.hu/news/hungary-s-armed-forces-are-expanded-with-a-unique-new-capability.html (dostęp 30.12.2025); M. Hypś, *Zrínyi 2026. Węgierska modernizacja pod sztandarem Zrinskiego*, https://www.konflikty.pl/technika-wojskowa/na-ladzie/zrinyi-2026-wegierska-modernizacja/ (dostęp 30.12.2025); G. Kormány, *Megérkezett a Magyar Honvédség második KC-390 Millennium szállító repülőgépe*, https://honvedelem.hu/hirek/megerkezett-a-magyar-honvedseg-masodik-kc-390-millennium-szallito-repulogepe.html (dostęp 30.12.2025); D. Nagy, *Zrínyi 2026: Hungary's Large-scale Military Force Development Programme*, https://www.hungarianconservative.com/articles/current/zrinyi-2026-hungarys-large-scale-military-force-development-programme/ (dostęp 30.12.2025); S. Nyulas, *Új fegyverek a magyar katonáknak*, https://honvedelem.hu/media/aktualis-videok/uj-fegyverek-a-magyar-katonaknak.html (dostęp 30.12.2025); J. Padanyi, L. Foldi, *Military Technical Developments in Hungary in the Frame of ZRINYI 2026 Program*, 2019 International Conference on Military Technologies (ICMT), Brno, 10.1109/MILTECHS.2019.8870061; L. Pásztor, *Comprehensive Revitalization Program of Hungarian Defence Forces „Zrinyi 2026" and His Impact on the Security Environment of Central Europe*, https://real.mtak.hu/218857/1/PPT_13_Comprehensive_Revitalization.pdf (dostęp 30.12.2025).

WIEDEŃSKIE CENTRUM DS. ROZBROJENIA I NIEPROLIFERACJI (ang. VCDNP Vienna Center for Disarmament and Non-Proliferation) pełni funkcję kluczowego forum badawczego, dedykowanego inkubacji rozwiązań w obszarze kontroli zbrojeń. Poprzez synergię działań edukacyjnych i naukowych ośrodek aktywnie wspiera międzynarodowe wysiłki na rzecz ograniczenia zbrojeń jądrowych. Ośrodek dostarcza również odpowiednim decydentom praktycznych rekomendacji politycznych, organizuje wydarzenia publiczne oraz wspiera spójny dialog o charakterze społecznym. Organizacja zajmuje się także szkoleniem dyplomatów, jak

i praktyków w obszarze tematyki nierozprzestrzeniania broni jądrowej oraz rozbrojenia. Instytucja założona 25 lutego 2010 r. jest niezależna i powstała z inicjatywy Federalnego Ministerstwa Spraw Europejskich i Międzynarodowych Austrii i Centrum Studiów nad Nierozprzestrzenianiem Broni Jądrowej im. Jamesa Martina w Instytucie Studiów Międzynarodowych Middlebury, w Monterey. Organizacja jest również członkiem Konsorcjum UE ds. Nierozprzestrzeniania Broni Jądrowej i Rozbrojenia, której zadaniem jest (przy wsparciu UE) koordynacja ogólnoeuropejskiej sieci ośrodków analitycznych i instytutów badawczych.

Praca organizacji skupia się na kilku obszarach. Instytut prowadzi badania i analizy, które wykorzystywane są przy kształtowaniu polityki nuklearnej i podejmowaniu odpowiednich korków przez decydentów. Statut organizacji wskazuje strukturę organizacyjną: składa się ona z organów kierowniczych, z dyrektorem wykonawczym na czele, którego zadaniem jest kierowanie organizacją, ale również administracją czy też procesem wdrażania. Dyrektor upoważniony jest do współpracy z osobami trzecimi za zgodą organów, którym podlega (JMCNS, MIIS); powoływany jest przez dyrektora JMCNS (James Martin Center for Nonproliferation Studies). Należy zauważyć też ścisłą zależność pomiędzy VCDNP i JMCNS, który pełni centralne kierownictwo i nadzór strukturalny. W takim układzie dyrektor odpowiada nie tylko za organizację pracy, ale również raportowanie finansowe i administracyjne przed instytucjami założycielskimi. Obowiązek ten dotyczy również sprawozdań budżetowych i raportów nt. realizacji projektów. Innym ważnym organem organizacji jest rada doradcza, do zadań której należą wsparcie programowe i merytoryczne oraz przygotowywanie rekomendacji działalności inicjatyw badawczych, które muszą odpowiadać misji organizacji. Rada doradcza składa się z przedstawicieli m.in. instytucji założycielskich i akademickich. Dyrektor wykonawczy uczestniczy w pracach rady doradczej, co zapewnia ciągły kontakt pomiędzy zarządem wykonawczym a organem doradczym. Statut określa również sposób zatrudnienia i finansowanie: każdy pracownik oraz stażysta jest formalnie zatrudniony w Middlebury College, a nie VCDNP. Zasady te obowiązują według regulacji Stanów Zjednoczonych i Austrii ze względu na lokalizację biura organizacji. Dokument jasno wskazuje także, że organizacja ma charakter non profit. Drugi aspekt

statutu – finansowanie organizacji – odbywa się zgodnie z jej charakterem non profit.

Fundusze pozyskiwane są z różnych źródeł m.in. dotacji, darowizn, organizacji międzynarodowych, państw, osób prywatnych. W statucie jasno wskazano, że wszystkie otrzymane fundusze mają służyć działalności niekomercyjnej organizacji. Na jego podstawie określony został również cel, którym jest rozwój międzyjądrowego dialogu, edukacji, ale również szkoleń w tematyce rozbrojenia i nierozprzestrzeniania broni.

Misją organizacji jest wspieranie globalnego bezpieczeństwa poprzez rozwój polityki w obszarze nierozprzestrzeniania oraz kontroli zbrojeń, a także zagrożeń z obszaru broni masowego rażenia. Dodatkowo organizacja opracowuje praktyczne rekomendacje na podstawie spójnych i wiarygodnych analiz; zrzesza wielu ekspertów z takich obszarów, jak broń jądrowa, nierozprzestrzenianie broni jądrowej, bezpieczeństwo jądrowe, zarządzanie energetyką jądrową, zabezpieczenia MAEA, kontrola zbrojeń, rozbrojenie i bezpieczeństwo międzynarodowe, polityka zagraniczna, teorie oraz praktyki reżimów międzynarodowych, relacje między mocarstwami, zarządzanie. Specjaliści dzielą się swoimi spostrzeżeniami na konferencjach poprzez renomowane publikacje czy też za pomocą międzynarodowych mediów.

Obszary badawcze organizacji to rozbrojenie, nierozprzestrzenianie i zabezpieczenia broni jądrowej, kontrola zbrojeń, zarządzanie energią jądrową i reżimy międzynarodowe, pokojowe stosowanie technologii jądrowych. Organizacja stale proponuje wydarzenia publiczne, które pozwalają na uświadomienie społeczeństwu najpilniejszych problemów związanych z bronią jądrową i jej wykorzystywaniem. VCDNP gromadzi podczas organizowanych wydarzeń decydentów, badaczy, ale również przedstawicieli społeczeństwa z różnych środowisk w celach omówienia istniejących wyzwań. Priorytetowym działaniem organizacji jest prezentacja szerokiego spektrum perspektyw, ale również zachęcanie do wspólnego dialogu na rzecz bezpieczeństwa. Działania VCDNP to także stałe budowanie potencjału dotyczące zgłębienia tematyki nierozprzestrzeniania broni jądrowej, rozbrojenia, bezpieczeństwa jądrowego oraz zabezpieczeń. Eksperci prowadzą kursy, które mają na celu chociażby doszkolenie dyplomatów, urzędników (również wysokiego szczebla) w zakresie zagadnień

związanych z nierozprzestrzenianiem broni jądrowej i rozbrojeniem. Są one okazją do nabrania doświadczenia edukacyjnego, a także nawiązywania kontaktów międzynarodowych. Organizacja VCDNP prezentuje również liczne publikacje w obszarze badań, takich jak kontrola zbrojeń, rozbrojenie, bezpieczeństwo nuklearne, zabezpieczenie nuklearne, nowe technologie, nierozprzestrzenianie broni jądrowej. Opisywany ośrodek ekspercki staje się kluczowym elementem dokonywanych zmian na tle międzynarodowym, które obejmują bezpieczeństwo.

Organizacja poprzez łączenie wielu przestrzeni działalności wpływa na debatę polityczną, a także stanowiska państw dotyczące chociażby nieproliferacji broni masowego rażenia. Przykładami realnych działań organizacji budujących międzynarodowe środowisko bezpieczeństwa są:

- utworzenie raportu dotyczącego sztucznej inteligencji i zarządzania bezpieczeństwem nuklearnym (dotyczy radzenia sobie z zagrożeniami związanymi z pionierską sztuczną inteligencją, koncentruje się także na pytaniu, czy pionierska sztuczna inteligencja może pomóc atakującemu w naruszeniu bezpieczeństwa materiałów jądrowych i obiektów na arenie międzynarodowej). Raport skupia się na 3 fazach działania przeciwnika: cel ataku, plan ataku, budowanie umiejętności wraz z wykonaniem działania. Rozważa, czy sztuczna inteligencja może obecnie wzmocnić przeciwnika;
- organizowanie wydarzenia dotyczącego kluczowych obszarów działań w kwestii późniejszych dyskusji dotyczących wejścia w życie Traktatu o całkowitym zakazie prób z bronią jądrową (CTBT). Spotkanie Grupy Roboczej B Komisji Przygotowawczej CTBTO pozwoliło na omówienie sposobów utrzymania globalnej normy zakazującej prób jądrowych, a także uzyskania ratyfikacji. Dodatkowo wydarzenie pozwoliło na wymianę argumentów panelistów w sprawie wartości Międzynarodowego Systemu Monitorowania (IMS) oraz znaczenia przestrzegania CTBT w nowoczesnym świecie;
- wspieranie działań młodych badaczy w obszarze kontroli zbrojeń, rozbrojeń czy też nierozprzestrzeniania broni jądrowej. VCDNP jest organizatorem spotkań młodych specjalistów

i badaczy, dając im możliwości pogłębienia nie tylko wiedzy, ale i budowania kariery w obszarze kontroli zbrojeń, rozbrojeń i nierozprzestrzeniania broni. Dzięki wydarzeniu uczestnicy mogli skorzystać nie tylko z doświadczenia starszych specjalistów, ale również podjęcia inicjatyw np. w sieci zrzeszającej młodych i utalentowanych badaczy – Emerging Voices Network of the British American Security Information Council (BASIC), programu POIN dla początkujących ekspertów w celu zagłębienia zagadnień związanych z energią jądrową – Project on Nuclear Issues of the Center for Strategic and International Studies (CSIS). Działania na rzecz inkluzji młodego pokolenia w obszar studiów nad zbrojeniami nuklearnymi wykraczają poza doraźne inicjatywy. Ich systemowym przejawem są m.in. cykliczne spotkania multimedialne z cyklu »Środy YGLN«. Gromadzą one członków Sieci Liderów Młodego Pokolenia (Younger Generation Leaders Network – YGLN), działającej pod egidą E*uropean Leadership Network (ELN).* Ta licząca ponad 150 ekspertów platforma umożliwia dynamiczną wymianę myśli strategicznej oraz budowanie kapitału relacyjnego między przyszłymi decydentami. Wiedeńskie Centrum ds. Rozbrojenia Nieproliferacji jest niezależną organizacją, która działa na rzecz międzynarodowego pokoju oraz bezpieczeństwa, promując zagadnienia dotyczące nierozprzestrzeniania broni jądrowej oraz rozbrojenia.

Organizacja non profit stanowi kompleksowy ośrodek wiedzy połączony z promowaniem młodych badaczy. Prowadzi kompleksową działalność badawczą, ekspercką i edukacyjną w środowisku bezpieczeństwa międzynarodowego. Poprzez swoje zaangażowanie i inicjatywy edukacyjne przyczynia się do budowy odpowiednich zasad dotyczących nierozprzestrzeniania broni jądrowej i rozbrojenia.

Natalia Borodziuk

Govering Statute of the Vienna Center for Disarmament and Non-Proliferation (VCDNP) (2025); Vienna Center for Disarmament and Non-Proliferation, https://vcdnp.org/about-us/ (dostęp 11.12.2025).

WOJNA CYBERNETYCZNA, zwana także cyberwojną, polega na wykorzystaniu komputerów, internetu oraz innych środków do przeprowadzania ataków na systemy informatyczne przeciwnika, które odbywają się w cyberprzestrzeni mającej wiele definicji. Przyjmuje się, iż cyberprzestrzeń to interaktywna domena tworzona przez sieci cyfrowe, wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji. Internet jest jej integralną częścią, ale występują w niej również inne systemy informacyjne obsługujące gospodarkę, sektor finansowy, infrastrukturę krytyczną oraz wspomagające świadczenie usług. Lapidarna i uproszczona definicja cyberprzestrzeni wskazuje, że jest to komunikacyjna przestrzeń stworzona przez globalne połączenie sprzętu służącego do automatycznego przetwarzania danych cyfrowych.

Departament Obrony Stanów Zjednoczonych wypracował własną definicję, według której cyberprzestrzeń to „globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesy oraz kontrolery".

Z kolei polskie ustawodawstwo przyjmuje, iż jest to obszar przetwarzania i wymiany informacji tworzony przez systemy teleinformatyczne, określone w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Negatywne zjawiska w cyberprzestrzeni mają wymiar działalności zewnętrznej i wewnętrznej; mogą to być ataki przeprowadzane w sieci na infrastrukturę krytyczną państwa, jego system obronny, lub o charakterze dezinformacyjnym czy cyberprzestępczym; działania godzące w międzynarodową pozycję i prestiż danego państwa realizowane przy użyciu wirusów, robaków i trojanów. Istotą zagrożeń w cyberprzestrzeni jest zatem działanie w przestrzeni komunikacyjnej podejmowane przy wykorzystaniu szerokiego spektrum instrumentów wpływających destrukcyjnie na podmioty korzystające z sieci komputerowych. Najważniejszymi zagrożeniami bezpieczeństwa informacyjnego są:

- wojna informacyjna;
- szantaż;
- szpiegostwo;

– działania grup hakerskich.

James A. Green w swojej definicji cyberwojny przyjął, że jest ona kontynuacją polityki za pomocą działań inicjowanych w cyberprzestrzeni zarówno przez podmioty państwowe, jak i niepaństwowe, generujące zagrożenie dla bezpieczeństwa innych podmiotów lub też działania będące reakcją na zagrożenie dla bezpieczeństwa danego państwa. Wojna ta paraliżuje infrastrukturę: mechanizmy komunikacyjne czy gospodarcze, które w nowoczesnych państwach bazują na systemach komputerowych. Obecnie takimi konfliktami, w których strony prowadzą działania w cyberprzestrzeni, są wojna w Ukrainie oraz konflikt izraelsko-palestyński.

James A. Lewis zauważył, że decyzja o tym, czy dany konflikt stanowi akt wojny, jest zawsze polityczna. Wskazał, iż występuje tu szara strefa „zjawisk między irytacją a działaniami, które mają na celu zniszczenie państwa". Ważne jest więc stwierdzenie, czy cyberatak spowodował lub miał spowodować ofiary, bowiem to one (lub poważne zniszczenia) dają podstawę politykom do podjęcia decyzji, czy był to akt wojny usprawiedliwiający zastosowanie przemocy jako adekwatnej reakcji. Tym samym destrukcję danych i sieci można uznać za akt wojny, ale trzeba uwzględnić skalę zniszczenia oraz wrażliwość informacji, które zostały utracone. Również sam agresor może wpływać na decyzję, czy taki zamach był aktem wojny.

Krzysztof Liedl podał tu przykład niestabilnego psychicznie angielskiego aktywisty, który w proteście przeciwko wojnie w Iraku włamał się na publiczne strony Pentagonu, powodując szkody w sieci. Ten zamach został potraktowany jako przestępstwo, a nie akt wojny. Jeśli w takie działanie byłoby zaangażowane państwo albo gdyby działał tu pośrednik, a fakt zlecenia mu wrogiego działania zostałby udowodniony, sprawie mógłby zostać nadany dużo większy ciężar. Globalny charakter internetowych połączeń powoduje, iż aktywności w cyberprzestrzeni likwidują dużą część tradycyjnej ochrony, którą stanowiły granice, obronne mury i oceany. W przeciwieństwie do lądu, morza i powietrza internet został stworzony przez człowieka i opiera się na wspólnej własności, obsłudze i ochronie sektora publicznego i prywatnego.

Research And Development Corporation (RAND) – amerykański think tank i organizacja badawcza non profit – swoimi badaniami objął

cyberwojnę. Analitycy wskazali, że wojna cybernetyczna to sposób prowadzenia operacji wojskowych zgodnie z zasadami związanymi z informacją jako zasobem strategicznym. Celem głównym jest zakłócenie działania bądź destrukcja systemów komunikacyjnych i informacyjnych wroga oraz uzyskanie przewagi poprzez zgromadzenie odpowiedniej wiedzy dotyczącej przeciwnika, przy jednoczesnym zapobieganiu uzyskania przez niego jakichkolwiek danych.

Uzyskanie wskazanej przewagi informacyjnej widoczne jest w oddziaływaniu na systemy informacyjne i komunikacyjne wroga, wpływające na jego wiedzę np. z zakresu:

- identyfikacji własnych oddziałów;
- ich lokalizacji oraz możliwości;
- terminu przeprowadzenia akcji;
- kolejności zwalczania zagrożeń.

RAND uważa, iż wojna cybernetyczna to konflikt o wysokim stopniu intensywności. Eksperci wskazują, że angażuje ona wiele różnych technologii, takich jak dowodzenia i kontroli, gromadzenia informacji wywiadowczych, przetwarzania i dystrybucji informacji, identyfikacji „przyjaciel–wróg", broni „inteligentnej". W cyberwojnie mogą występować takie działania ofensywne, jak „oślepianie" przeciwnika, przeciążanie jego systemów, infiltracja systemów komunikacyjnych i informacyjnych. Tak więc rewolucja informacyjna implikuje konieczność stosowania we współczesnych armiach wielu zmian organizacyjnych. Poszczególne komponenty muszą działać bardziej jako powiązane ze sobą sieci, a nie wyalienowane struktury hierarchiczne. Proces ten szczególnie oddziałuje na armie współczesnych państw, które adaptując się do nowych form konfliktu, muszą dokonywać głębokich przemian organizacyjno-funkcjonalnych.

Tym samym wojna cybernetyczna wprowadza wiele istotnych zmian dla bezpieczeństwa współczesnych państw oraz doktryn militarnych wpływających na współczesne bezpieczeństwo. Obserwujemy, że następuje zmiana w postrzeganiu samego pola walki, gdyż cyberwojna nie jest już związana z geograficznymi wyznacznikami pola walki, ale raczej – architekturą cyberprzestrzeni. Cyberwojna zmieniła także postrzeganie tego, czym jest atak – obecnie wcale nie musi oznaczać fizycznej eliminacji przeciwnika, a jedynie uderzenie w elementy krytyczne jego systemu

komunikacyjnego i informacyjnego. Cyberwojna na strategicznym poziomie może skutkować realizacją zasady centralizacji strategicznej i taktycznej decentralizacji. Podczas konfliktu w cyberprzestrzeni może wystąpić zalew informacją i dezinformacją. Uwzględniając tempo, w jakim są podejmowane działania w cyberprzestrzeni, może to oznaczać, iż hierarchiczne dowodzenie będzie niemożliwe. Decydowanie o każdej kwestii taktycznej stanowiącej problem na polu walki przez dowódcę szczebla centralnego będzie niemożliwe w krótkim czasie, dostępnym na wypracowanie takiej decyzji, co spowoduje dalsze usamodzielnianie jednostek wojskowych prowadzących działania bojowe w cyberprzestrzeni. Zjawisko to wynika z konieczności przekształcania struktur hierarchicznych w sieciowe, w których dowodzenie i kontrola ustępują miejsca konsultacji i koordynacji. To procesy będące podstawą działania organizacji sieciowych.

Analiza dotychczas zidentyfikowanych ataków w cyberprzestrzeni ujawniła, że na tym cyfrowym froncie celami są zarówno infrastruktura państwowa, jak i cywilna, a także systemy krytyczne. Jeszcze zanim Rosja dokonała pełnoskalowej inwazji, wielokrotnie atakowała cele w Ukrainie, zaś po 24 lutego 2022 r. grupy hakerów mające powiązania z rosyjskimi służbami specjalnymi (GRU, SWR i FSB) znacznie zintensyfikowały swoją aktywność: cały czas utrzymują intensywność ataków, wykorzystując nowe taktyki oraz modyfikując stosowane wcześniej oprogramowanie. Zwiększenie aktywności działań w cyberprzestrzeni związanej z obecną agresją nie rozpoczęło się dokładnie w dniu lub nawet w przeddzień inwazji; zgodnie z rosyjskimi założeniami doktrynalnymi jest to ciągły proces mający prowadzić do maksymalnego osłabienia oraz dezintegracji społeczeństwa i struktur państwowych Ukrainy.

Już od 2014 r., czyli od momentu zajęcia Półwyspu Krymskiego oraz wschodniej części Donbasu, Federacja Rosyjska starała się wpływać na sytuację w Ukrainie, wykorzystując aktora proxy – grupę CyberBerkut (atrybucja wykazała powiązania grupy z APT 28) i próbując aktywnie przeszkodzić w wyborach prezydenckich. Implikowało to późniejsze ataki na sieć energetyczną w 2015 i 2016 r., kampanię NotPetya, której straty oszacowano na 10 mld dolarów, czy też atak na stację uzdatniania wody w 2018 r. Przez cały ten czas (2014–2022) Rosjanie z różnym natężeniem atakowali Ukrainę, traktując ją jako swoiste laboratorium testowania

środków ofensywnych w cyberprzestrzeni. Z tego też powodu Rosja rozpoczęła swoją zbrojną agresję od ataku pocisku manewrującego na ukraińskie rządowe centrum danych, a inne lokalne serwery zostały zaatakowane przy użyciu broni konwencjonalnej.

Inwazja rosyjska wykorzystuje cyberstrategię obejmującą przynajmniej 3 odrębne, a niekiedy skoordynowane, działania; są to niszczycielskie cyberataki na terenie Ukrainy, penetracja sieci i szpiegostwo prowadzone poza granicami Ukrainy oraz cyberoperacje wywierania wpływu informacyjnego wymierzone w społeczeństwa na całym świecie. Rosja skierowała destrukcyjne ataki za pomocą oprogramowania typu *wiper* na lokalne sieci komputerowe. Obserwatorzy zauważają, iż ataki w okresie poprzedzającym rozpoczęcie fazy pełnoskalowej wojny przeciw Ukrainie oraz te, które nastąpiły już po 24 lutego 2022 r. nie były „innowacyjnym przełomem" co do użytych technik i procedur, jednak nastąpiło nowe podejście w zakresie stosowanej taktyki związanej z powszechnym użyciem ataków typu DDoS; miały one ogniskować siły i środki ukraińskiego zespołu CERT. Skutkowały one częściowym ograniczeniem dostępności usług, ale głównie były elementem obfuskacyjnym, czyli maskująco-dezorientującym.

Analizy wykazały, iż najbardziej powszechnym rodzajem złośliwego oprogramowania stosowanym w tym okresie był *wiper*, który w obszarze logiki działania i zaimplementowanych rozwiązań jest pochodną ataków *ransomware*. Analitycy i eksperci z Cert Ukraina wskazali następujące cyberataki zrealizowane przez Rosję tylko w pierwszych miesiącach wojennych działań: Spear Phishing Email – wobec pracowników strategicznego sektora energetycznego, Cobalt Strike, GrimPlant i GraphSteel stanowiące element plików aktualizacyjnych. Powszechnie stosowano zmasowane ataki DDoS, wysyłanie wiadomości SMS oraz prowadzono kampanię dezinformacyjną. Atakowano przy wykorzystaniu *malware* HermeticWiper oraz *ransomware*, a także *malware* IsaacWiper oraz phishingowe dostarczające *malware* SunSeed. Odnotowano również atak na elementy infrastruktury teleinformatycznej VIASAT z zastosowaniem *malware* AcidRain oraz na punkt kontroli granicznej (Ukraina–Rumunia), a także kompromitujący strony wybranych uczelni wyższych. Dużą skoordynowaną akcją była dezinformacja przeprowadzona na portalu Facebook; Rosjanie pozyskali także dane uwierzytelniające dla kont pracowników

koncernów medialnych; zastosowali FormBook Spam w ramach kampanii adresowanej do obywateli Ukrainy; dokonali ataku na systemy sterowania ruchem i zasobami logistycznymi w zachodniej Ukrainie, operatora telekomunikacyjnego Ukrtelecom, konta komunikatora Telegram, ukraińskie media i dostawcę energii. Poważnym zagrożeniem była też dystrybucja trojana IcedID oraz atak DDoS na zasoby ukraińskiej poczty.

Pomimo tych zmasowanych i różnorodnych cyberzamachów ukraiński rząd zdołał podtrzymać operacje cywilne i wojskowe, podejmując sprawne i szybkie działania niezbędne, by rozproszyć swoją cyfrową infrastrukturę w chmurze publicznej, w której jest hostowana w centrach danych w całej Europie. Tym samym Ukraina odniosła względny sukces w stosowaniu mechanizmów cyberobrony. Chociaż nie są one jeszcze doskonałe, wykazują przewagę nad możliwościami cyberoperacji ofensywnych Rosji, co odzwierciedla obserwowane od pewnego czasu trendy. Po pierwsze, postęp w analizowaniu zagrożeń, m.in. przy zastosowaniu sztucznej inteligencji (AI), umożliwił efektywniejsze wykrywanie ataków. Po drugie, ochrona punktu końcowego połączonego z internetem pozwala na szybkie rozpowszechnianie kodu oprogramowania zabezpieczającego zarówno do usług w chmurze, jak i innych połączonych urządzeń przetwarzających dane. Umożliwia to szybkie identyfikowanie i wyłączanie złośliwego oprogramowania.

Firma Microsoft zidentyfikowała rosyjskie próby włamań do sieci, które dotyczą aż 128 organizacji w 42 krajach. Obok Stanów Zjednoczonych, które stanowią dla Rosji cel priorytetowy, ważnym obszarem tych wrogich działań jest także Polska, na której terenie jest koordynowana znaczna część logistyki dostaw w ramach pomocy humanitarnej i wsparcia wojskowego dla walczącej Ukrainy.

Cyberofensywa Rosji jest także wymierzona w państwa bałtyckie, ale widoczny jest również wzrost takiej aktywności wobec sieci komputerowych w Danii, Norwegii, Finlandii, Szwecji i Turcji. Zestawienie celów tych zamachów jest stosunkowo szerokie i obejmuje takie podmioty, jak think tanki, organizacje humanitarne, firmy z branży IT oraz dostawców energii i pozostałej infrastruktury krytycznej. Od rozpoczęcia wojny zidentyfikowane wrogie ataki Rosji powiodły się w 29% przypadków. Z kolei 25% tych udanych włamań doprowadziło do potwierdzonej eksfiltracji danych

różnych organizacji. Ekspertów z Microsoft najbardziej niepokoją rządowe komputery, które nadal zbyt często działają lokalnie zamiast w chmurze. To obrazuje aktualny, globalny stan ofensywnego cyberszpiegostwa i defensywnej cyberochrony.

W grudniu 2020 r. rosyjscy hakerzy włamali się do infrastruktury SolarWinds, firmy produkującej platformę do monitorowania sieci, i aplikacji o nazwie Orion; następnie wykorzystali ten dostęp do tworzenia i rozpowszechniania trojanizowanych aktualizacji wśród użytkowników oprogramowania. Aktualizacje dla wersji Orion od 2019.4 HF 5 do 2020.2.1, które zostały wydane między marcem 2020 a czerwcem 2020 r., mogły zawierać złośliwe komponenty. Na swojej stronie internetowej SolarWinds poinformował, iż wśród jego klientów było 425 osób z listy Fortune 500, 10 największych amerykańskich firm telekomunikacyjnych, 5 wiodących amerykańskich firm księgowych, wszystkie oddziały sił zbrojnych USA, Pentagon, Departament Stanu, a także setki uniwersytetów i szkół wyższych na całym świecie. Jak pokazało zdarzenie SolarWinds, rosyjskie agencje wywiadowcze mają niezwykle wyrafinowane metody zagnieżdżania kodu i działania jako zaawansowane stałe zagrożenie (APT), które może na bieżąco pozyskiwać i eksfiltrować poufne informacje z sieci. Wprawdzie od tamtego czasu nastąpił znaczący rozwój w zakresie ochrony defensywnej, ale stopień wdrażania tych postępów przez europejskie rządy wciąż pozostaje niewystarczający.

Wraz z rozwojem wojny w Ukrainie rosyjskie agencje koncentrują swoje cyberoperacje w obszarze wywierania wpływu informacyjnego wobec 4 grup adresatów. Ich celem jest podtrzymanie wsparcia ludności rosyjskiej dla działań wojennych i osłabienie zaufania ukraińskiego społeczeństwa w możliwości skutecznego odparcia rosyjskich ataków. Są także skierowane w społeczeństwa Ameryki i Europy celem zachwiania jedności Zachodu i odpierania krytyki zbrodni wojennych dokonywanych przez rosyjską armię, a także w społeczeństwa krajów nienależących do koalicji, tak by zapewnić sobie ich poparcie w Organizacji Narodów Zjednoczonych i na innych międzynarodowych forach. Rosyjskie cyberoperacje w zakresie wywierania wpływu informacyjnego opierają się na taktykach, które powstały na potrzeby innych aktywności w cyberprzestrzeni i są z nimi ściśle powiązane. Zespoły zaawansowanej stałej manipulacji APM (Advance Persistent

Manipulator) są powiązane z rosyjskimi agencjami rządowymi i działają przy wykorzystaniu mediów społecznościowych oraz platform cyfrowych. Rozpowszechniają fałszywą narrację w sposób podobny do złośliwego oprogramowania; prowadzą na szeroką skalę równoczesne „relacjonowanie" oparte na narracji zarządzanych i inspirowanych przez rząd witryn internetowych i wzmacniają ten przekaz, wykorzystując narzędzia technologiczne przeznaczone do wykorzystywania luk w serwisach społecznościowych.

Agresja Rosji na Ukrainę zdynamizowała ilość cyberataków; intensyfikacja działań spowodowała powstanie wielu nowych grup lub „emanacji" działających już podmiotów, których aktywność jest śledzona i kwalifikowana. Przedłużająca się eskalacja konfliktu kinetycznego połączona z postępującą izolacją polityczną Rosji, a także kolejnymi nakładanymi na nią sankcjami może implikować zwiększenie intensywności wrogich działań w cyberprzestrzeni, w szczególności wobec sektorów objętych sankcjami i mających wysoką wartość gospodarczą lub znaczący wpływ na bezpieczeństwo narodowe.

Dotychczasowe wektory zagrożeń wskazują, iż najbardziej zagrożone będą sektory usług finansowych, przemysłu zbrojeniowego, energetycznego oraz obiekty stanowiące infrastrukturę krytyczną, stąd konieczne jest zintensyfikowanie zarówno przez Ukrainę, jak i państwa członkowskie NATO wysiłków zmierzających do zwiększenia zdolności obrony kluczowych zasobów oraz rozbudowy tych ofensywnych, pozwalających na operacje w cyberprzestrzeni i stanowiących komponent działań wielodomenowych.

Andrzej Czop

J.A. Green, *Routledge Studies in Conflict, Security and Technology, Cyber warfare a multidisciplinary analysis*, Routledge, London 2016; J.A. Lewis, *Tresholds for Cyberwar*, http://csis.org/fi les/publication/101001_ ieee_insert.pdf (dostęp 10.09.2025); K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1; A. Rogozińska, *Zagrożenia jako główna determinanta bezpieczeństwa międzynarodowego*, „Rocznik Nauk Społecznych" 2021, nr 2; Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. 2002, nr 113, poz. 985; J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

WOJNA KOGNITYWNA (ang. *cognitive warfare*) albo poznawcza – wszelkie wrogie działania mające na celu wpływanie na postawy i zachowania; forma współczesnego konfliktu, w której przedmiotem ataku jest ludzki umysł, a celem – wpływanie na procesy poznawcze, w tym ocenę sytuacji, myślenie, percepcję rzeczywistości, podejmowanie decyzji oraz system wartości i tożsamość. Jest to rodzaj wojny hybrydowej stanowiącej rozszerzenie informacyjnej i wykorzystującej m.in. propagandę i dezinformację. W odróżnieniu od wojny informacyjnej, która koncentruje się na treści informacji, kognitywna skupia się na mechanizmach przetwarzania danych przez człowieka. Główne wyzwanie stanowi to, że jest ona zasadniczo niewidoczna; dostrzegalne są tylko jej skutki, a wtedy często jest już za późno. Generał NATO Paolo Ruggiero wyróżnia ją spośród innych działań związanych z informacją: „Jej celem nie jest to, co myślą jednostki, ale raczej sposób, w jaki myślą".

Koncepcja wojny kognitywnej oficjalnie weszła do słowników wojskowości i nauk politycznych w 2017 r., kiedy to została spopularyzowana na Zachodzie przez generała Sił Powietrznych Stanów Zjednoczonych Davida Goldfeina, ale początki tej formy konfliktu są znacznie starsze i można znaleźć prace prekursorskie na ten temat już od końca lat 90. Uważa się, że podwaliny przejścia od wojny psychologicznej do poznawczej zostały położone w czasie II wojny światowej, w okresie eksperymentów z kontrolą umysłu przeprowadzanych przez Kurta Plonera w nazistowskich Niemczech, a następnie wzmocnione w okresie bezpośrednio powojennym wraz z równoczesnym rozpoczęciem w Stanach Zjednoczonych i Związku Radzieckim badań nad funkcjonowaniem ludzkiego umysłu w celach wojskowych i politycznych.

W 2021 r. NATO rozpoczęło opracowywanie własnej koncepcji wojny kognitywnej, wzywając jednocześnie państwa członkowskie do wyposażenia się w niezbędny personel, zaplecze i narzędzia umożliwiające badanie i przeciwdziałanie temu zjawisku.

Oliver Backes i Andrew Swab z Centrum Belfera na Uniwersytecie Harvarda definiują wojnę poznawczą jako strategię mającą na celu zmianę sposobu myślenia grupy docelowej, co doprowadzi do modyfikacji sposobu jej działania, a tym samym – zmiany jej zachowania.

Alonso Bernal z Uniwersytetu Johnsa Hopkinsa w artykule z 2020 r. twierdzi, że wojna kognitywna polega na wykorzystywaniu opinii publicznej jako broni i jej celem jest nie tylko kontrolowanie przepływu informacji, ale także sposobu, w jaki jednostki lub grupy docelowe reagują na te informacje jako „uzbrajanie opinii publicznej przez podmioty zewnętrzne w celu wpłynięcia na politykę publiczną i/lub rządową lub podważenia działań rządu i/lub stabilności instytucji rządowych".

Koncepcja wojny kognitywnej rozwinęła się na styku psychologii poznawczej, neuronauki, sztucznej inteligencji, big data i mediów cyfrowych. Lin Zhengrong z Tajwańskiego Uniwersytetu Obrony Narodowej stwierdził, że termin „wojna kognitywna" pojawił się po raz pierwszy w raporcie NATO, gdzie został zdefiniowany jako nowa dziedzina konkurencji, wykraczająca poza tradycyjne domeny, takie jak ląd, morze i powietrze. To niekonwencjonalny sposób prowadzenia wojny, który wykorzystuje indywidualne uprzedzenia psychologiczne i myślenie refleksyjne, używając sieci technologicznych do manipulowania ludzkim poznaniem, wywoływania zmian w myśleniu i tym samym powodowania negatywnych skutków.

Według istniejącej literatury i koncepcji NATO wojna kognitywna jest definiowana jako *„taktyka łącząca tradycyjne i nowe technologie, a także środki wykraczające poza granice wojny w celu osiągnięcia efektów poznawczych u ludności przeciwnika, a także u jego przywódców politycznych i wojskowych*".

Ataki kognitywne nie są niczym nowym, jednak koncepcja ta definiuje je jako celowe manewry ofensywne mające na celu wpływanie na percepcję, przekonania, interesy, decyzje i zachowania poprzez bezpośrednie oddziaływanie na ludzki umysł. Zakłada się, że innowacja tkwi w zdolności przeciwników do szybkiego i anonimowego przeprowadzania ataków poznawczych w środowisku informacyjnym z wykorzystaniem platform cyfrowych i nowych technologii przełomowych (EDT).

Koncepcja wojny kognitywnej, badana przez NATO i innych analityków ds. bezpieczeństwa, obejmuje wykorzystanie taktyk technologicznych do manipulowania ludzkim poznaniem, wpływania na proces decyzyjny i zmiany zachowania. Ostatecznym celem przeciwnika stosującego te

taktyki jest często sianie niezgody, podważanie zaufania i „wpływanie na wolę walki" ludności i personelu wojskowego państwa docelowego.

Organizacja Traktatu Północnoatlantyckiego bada wojnę kognitywną jako nową dziedzinę działań wojennych. „Sojusz stoi przed szeregiem wyzwań w nowych dziedzinach konfliktów. Domeny te mogą wynikać z wprowadzania nowych i przełomowych technologii. Na przykład dziedziny kosmosu i cyberprzestrzeni wyrosły z rozwoju technologii rakietowych, satelitarnych, komputerowych, telekomunikacyjnych i sieciowych. Coraz powszechniejsze wykorzystanie mediów społecznościowych, sieci społecznościowych, komunikatorów społecznościowych i technologii urządzeń mobilnych stwarza obecnie nową dziedzinę: wojnę poznawczą".

Jednocześnie NATO uważa wojnę kognitywną za ewolucję psychologicznej, integrującą cybernetykę, informatykę, psychologię i inżynierię społeczną, aby wpływać na przekonania i działania, traktując umysł jako domenę konfliktu. Podało na swojej stronie internetowej następującą definicję: wojna kognitywna to działania prowadzone w synchronizacji z innymi instrumentami władzy, mające na celu oddziaływanie na postawy i zachowania poprzez oddziaływanie, ochronę lub zakłócanie procesów poznawczych na poziomie jednostki, grupy lub populacji w celu uzyskania przewagi nad przeciwnikiem. Natomiast wspólnie opublikowana w 2020 r. praca badaczy z NATO i Uniwersytetu Johnsa Hopkinsa definiuje wojnę kognitywną w następujący sposób: ma ona na celu doprowadzenie do tego, by wrogowie zniszczyli się od wewnątrz.

NATO określa taki konflikt *„szóstą domeną prowadzenia wojny"* (obok lądu, morza, powietrza, kosmosu i cyberprzestrzeni). Koncepcja wojny poznawczej jest stosunkowo nowa i nie osiągnęła jeszcze pełnego konsensusu co do jej dokładnej definicji.

W ramach doktryny NATO wojna kognitywna spełnia swoją funkcję jako koncepcja wojskowa niższego szczebla. Biorąc pod uwagę jej koncentrację na szybko ewoluujących nowych technologiach przełomowych (*Emerging and Disruptive Technologies,* EDT), prawdopodobnie będzie wymagała częstych modyfikacji, aby zachować skuteczność i aktualność. Ta potrzeba ciągłej adaptacji odzwierciedla dynamiczny charakter wojny kognitywnej i środowisko technologiczne, w którym funkcjonuje. Biorąc pod uwagę te aspekty, staje się oczywiste, że choć wojna kognitywna jest

potężną i ewoluującą koncepcją, jej skuteczne wdrożenie i użyteczność zależą od starannego rozważenia jej zakresu i kontekstu, w jakim jest stosowana.

Wojna kognitywna nie jest środkiem, którym walczymy, ale właśnie samą walką. Mózg jest zarówno celem, jak i bronią w zmaganiach o przewagę poznawczą. Rywalizacja w tym środowisku obejmuje celowe, zsynchronizowane działania wojskowe i niemilitarne w całym kontinuum rywalizacji, mające na celu uzyskanie, utrzymanie i ochronę przewagi poznawczej.

Wojna kognitywna koncentruje się na atakowaniu i degradacji racjonalności, co może prowadzić do wykorzystywania słabości i systemowego osłabienia, jednak sytuacja staje się bardziej skomplikowana, gdy w grę wchodzą cele niemilitarne. Przykład: rosyjskie media społecznościowe i operacje informacyjne wymierzone były w dużą część społeczności międzynarodowej, próbując wskazać Ukrainę jako winną wojny. Poprzez połączenie technologii komunikacyjnych, fałszywych wiadomości i manipulacji percepcją Rosja dąży do wpływania na opinię publiczną oraz osłabianie zaufania publicznego do otwartych źródeł informacji. Te narracje mają szeroki zasięg i często obejmują zarówno ofensywne, jak i defensywne postawy.

Artykuł *Zwalczanie wojny kognitywnej: świadomość i odporność* w „NATO Review" (2021) wyjaśnia, jak przeciwnicy wykorzystują technologię (media społecznościowe, sztuczną inteligencję), aby przekształcić ludzki umysł w pole bitwy, wpływając na zachowania poprzez dezinformację i psychomanipulację. Świadomość i odporność odgrywają kluczową rolę w obronie, wymagając nowych strategii, takich jak zespoły obrony poznawczej i edukacja medialna, aby chronić społeczeństwa i wojsko. Takim polem bitwy stają się media społecznościowe, komunikatory i technologie mobilne jako kluczowe narzędzia umożliwiające ataki na percepcję, zaufanie i wolę oporu ludności cywilnej oraz wojskowej. Natomiast techniki tej wojny obejmują manipulowanie informacjami, rozpowszechnianie dezinformacji i wykorzystywanie słabości psychicznych w celu osiągnięcia celów strategicznych.

W 2023 r. Dowództwo Sojusznicze NATO ds. Transformacji opublikowało artykuł *Wpływ na wolę walki* (*Impact the Will to Fight*), w którym

opisało główny cel lub zamierzony efekt taktyk wojny kognitywnej, podkreślając, że skuteczna wojna kognitywna wymaga płynnej synchronizacji i koordynacji, aby manipulować ludzkim poznaniem, wpływając na rozumienie środowiska informacyjnego przez decydentów i ich determinację do angażowania się w konflikt.

Głównym celem wojny kognitywnej nie jest zmiana tego, co myśli wrogi cel, ale sposobu, w jaki myśli. W odróżnieniu od działań kinetycznych wojna kognitywna nie dąży do fizycznego zniszczenia, lecz przekształcenia świadomości jednostek i zbiorowości. W tym kontekście stosuje się wielowarstwowe techniki, aby zniekształcić percepcję celu, osłabić jego racjonalne rozumowanie, zniszczyć wspólny grunt prawdy i złamać odporność społeczną. Cele wojny kognitywnej obejmują przejęcie kontroli nad procesami myślowymi, emocjami i decyzjami przeciwnika. To forma konfliktu, w której nie liczy się terytorium, siła militarna, a kluczowe znaczenie ma umysł człowieka.

Istnieją różnorodne cele wojny kognitywnej:

1. Nadrzędne (strategiczne) – trwały wpływ na sposób myślenia przeciwnika, tak aby:
   - podejmował decyzje korzystne dla agresora;
   - działał wbrew własnym interesom;
   - tracił zdolność racjonalnej oceny sytuacji;
   - samodzielnie ograniczał swoją wolę oporu.
2. Polityczne:
   - paraliż decyzyjny elit władzy;
   - wprowadzanie chaosu informacyjnego;
   - wywoływanie sprzecznych ocen sytuacji;
   - podważanie kompetencji decydentów;
   - opóźnianie lub blokowanie decyzji strategicznych;
   - delegitymizacja władzy;
   - podważanie zaufania do instytucji państwowych;
   - kreowanie narracji o „nieudolnym" lub „nielegalnym" rządzie;
   - wzmacnianie poczucia niesprawiedliwości i krzywdy.
3. Społeczne:
   - rozbicie spójności społecznej;
   - polaryzacja opinii publicznej;

- antagonizowanie grup społecznych;
- eskalacja konfliktów kulturowych i ideologicznych;
- osłabienie tożsamości i odporności zbiorowej;
- relatywizacja historii i wartości;
- podważanie symboli narodowych;
- promowanie postaw nihilistycznych i apatii obywatelskiej.

4. Psychologiczne:
   - demoralizacja;
   - wywoływanie strachu, poczucia bezsensu i bezradności;
   - wzmacnianie narracji o „nieuchronnej porażce";
   - manipulacja emocjami;
   - sterowanie gniewem, lękiem, poczuciem krzywdy;
   - wykorzystywanie traum i kryzysów (wojna, pandemia, migracje).
5. Informacyjne:
   - zniszczenie pojęcia prawdy;
   - zatarcie granicy między faktem a opinią;
   - masowa produkcja sprzecznych narracji;
   - wzmacnianie relatywizmu poznawczego („każdy ma swoją prawdę");
   - przeciążenie informacyjne;
   - zalew informacji niemożliwych do zweryfikowania;
   - osłabienie zdolności krytycznego myślenia.
6. Ekonomiczne:
   - wywołanie nieufności wobec systemu gospodarczego;
   - destabilizacja rynków poprzez panikę informacyjną;
   - osłabienie wiary w stabilność waluty i instytucji finansowych.
7. Militarne:
   - osłabienie zdolności obronnych: demotywowanie żołnierzy i rezerwistów, podważanie sensu obrony państwa, rozbijanie morale sił zbrojnych;
   - ułatwienie działań kinetycznych: przygotowanie „miękkiego gruntu" przed konfliktem zbrojnym, zmniejszenie oporu społecznego wobec agresji.
8. Długofalowe (strategiczne):

- trwała zmiana postaw: kształtowanie pokoleń podatnych na manipulację, normalizacja wrogich narracji;
- samodestrukcja przeciwnika: skłonienie społeczeństwa do konfliktów wewnętrznych, osłabienie państwa bez formalnej wojny.

Największym sukcesem wojny kognitywnej jest sytuacja, w której ofiara nie zdaje sobie sprawy, że jest atakowana, a jej cele są trudne do jednoznacznego zidentyfikowania, rozproszone w czasie i często realizowane poniżej progu wojny.

Metody stosowane w wojnie kognitywnej:

- kampanie dezinformacyjne;
- zanieczyszczenie informacyjne i przeciążenie informacyjne;
- manipulacja algorytmami mediów społecznościowych;
- treści *deepfake*;
- sieci botów i fałszywe profile użytkowników;
- techniki wojny psychologicznej.

Wojna kognitywna uderza bezpośrednio w czynnik ludzki, co utrudnia jej wykrycie i przeciwdziałanie, potencjalnie podważając społeczeństwa od wewnątrz. Natomiast generatywna sztuczna inteligencja zaostrza te zagrożenia, wymagając innowacyjnych środków zaradczych, przy jednoczesnym zachowaniu równowagi między prawami podstawowymi, co omówiono w powiązanych analizach bezpieczeństwa.

Wojna kognitywna polega na wykorzystaniu procesów związanych z wiedzą w kontekście konfliktu. Działania te realizowane są za pomocą różnych instrumentów władzy, które działają harmonijnie i synchronicznie i mają na celu modyfikację postrzegania rzeczywistości docelowych jednostek, grup lub społeczności, a tym samym – zmianę ich zachowania.

Wykorzystują one narzędzia dostarczane przez różne nauki związane z wiedzą i jej procesami: psychologię, lingwistykę, neurobiologię itp. Działania te wykraczają poza sferę militarną i znajdują zastosowanie w obszarze polityki, gospodarki, społeczeństwa i kultury. Każdy użytkownik obecnych technologii informacyjno-komunikacyjnych może być potencjalnym celem. Działania w ramach wojny poznawczej ze względu na swoją wirtualną naturę zacierają granice między celami cywilnymi i wojskowymi.

Chiny, jako strategiczny konkurent NATO, opisują wojnę kognitywną jako wykorzystanie opinii publicznej, operacji psychologicznych

i wpływów prawnych w celu osiągnięcia zwycięstwa. Psychologia walki ma istotny wpływ na zdolność żołnierza do funkcjonowania. Poza polem bitwy może również oddziaływać na prawo, rządy porządku i konstrukty cywilne. W 2014 r. wojskowe instytucje badawcze Chin wprowadziły koncepcję „dominacji poznawczej", kładąc nacisk na manipulację ideologiczną, operacje wpływu i strategiczną wojnę informacyjną; dowiodło to, że stosowanie przez KPCh taktyk poznawczych i psychologicznych wobec mieszkańców Tajwanu opiera się na pewnych ramach teoretycznych.

Naukowcy uważają, że „wojna kognitywna" jest pojęciem podrzędnym w ramach wojny szarej strefy lub hybrydowej, jednocześnie jest elementem wojny informacyjnej. Niektórzy naukowcy twierdzą wręcz przeciwnie, że wojna informacyjna jest pojęciem podrzędnym w stosunku do wojny poznawczej. Działania te są definiowane w literaturze przedmiotu jako operacje w domenie kognitywnej, choć równie często określa się je mianem oddziaływania paradygmatycznego lub wielowymiarowych operacji wpływu.

Wojna kognitywna może obejmować wiele dziedzin, w tym tradycyjną wojnę propagandową, psychologiczną, ideologiczną i prawną. W porównaniu do „wojny informacyjnej", która może być skierowana do decydentów za pośrednictwem mediów społecznościowych online i sieci interpersonalnych, a także zniekształcać i manipulować poznaniem i emocjami wyborców, „wojna kognitywna" koncentruje się nie tylko na manipulacji mediami, ale rozciąga się również na obszar neuronauki , mając na celu wpływanie na funkcje mózgu poza konwencjonalnymi kanałami mediów masowych. Spośród różnych powiązanych ze sobą koncepcji obecnie jedynie „wojna kognitywna" wykorzystuje neuronaukę jako broń w zastosowaniach praktycznych, a konkretnie – ukierunkowanie i wpływanie na funkcje poznawcze mózgu.

W wojnie kognitywnej informacja służy jako broń bojowa: może być prawdziwa lub częściowo prawdziwa i częściowo fałszywa; nie musi to być całkowicie *fake news*. Obejmuje wykorzystanie różnych środków, takich jak zwykłe media, media społecznościowe, kultura i polityka, aby manipulować i wpływać zarówno na opinię publiczną, jak i świadomość przeciwnika. „Wojna informacyjna" jako składnik wojny poznawczej koncentruje się na wykorzystaniu informacji i technologii, takich jak media,

media społecznościowe, internet oraz technologie elektroniczne i cyfrowe w celu wpłynięcia na świadomość i zachowanie przeciwnika.

Skutki wojny kognitywnej można podzielić na 3 grupy:

- społeczne: utrata zaufania do instytucji, dezintegracja społeczeństwa, radykalizacja postaw;
- polityczne: paraliż decyzyjny państwa, osłabienie demokracji, manipulacja wyborami;
- militarne: demoralizacja wojska, błędne decyzje strategiczne, osłabienie zdolności obronnych.

Przykładami współcześnie wykorzystanej wojny kognitywnej mogą być:

- działania informacyjno-kognitywne Rosji wobec państw Zachodu, w tym przeciwko USA. Kampania wpływu kognitywnego przed wyborami, zaczynając od kampanii prezydenckiej 2015 r., nadzorowana i wdrażana przez rosyjską Agencję Badań Internetowych, odbywała się w internecie, głównie na Facebooku i Twitterze, gdzie influencerzy, blogerzy, trolle, rosyjskie media państwowe i punkty kontrinformacji zajmowały się nieustanną produkcją i rozpowszechnianiem oszustw i postprawd mających na celu pogłębianie podziałów w społeczeństwie amerykańskim. To przyczyniło się do zaostrzenia polaryzacji między grupami politycznymi, w szczególności demokratami i republikanami, oraz podsycania procesów radykalizacji wśród niektórych mniejszości, zwłaszcza Afroamerykanów. Potwierdzono, że Rosja nie tylko oczerniała Partię Demokratyczną, aby zapewnić zwycięstwo Donalda Trumpa, ale także emitowała reklamy polityczne na Facebooku i innych platformach, poruszające kontrowersyjne tematy w amerykańskim społeczeństwie, takie jak rasizm, imigracja, prawa do posiadania broni i homoseksualizm. Reklamy krytykujące i oczerniające obu kandydatów w tych kwestiach ostatecznie zaostrzyły konflikt między konserwatystami a liberałami, zgodnie z zamierzeniami Rosji. Za te działania, które określono jako próbę ingerencji w „wybory i procesy polityczne w USA", Agencja Badań Internetowych

została ukarana, a 13 obywateli Rosji – oskarżonych przez Departament Sprawiedliwości USA w 2018 r.;
- nieustanne działania Chińskiej Republiki Ludowej (ChRL) w celu zjednoczenia z Tajwanem. Chińska Armia Ludowo-Wyzwoleńcza prowadzi specjalistyczną jednostkę i szkolenia do „3 wojen" (opinii publicznej, psychologicznej i prawnej) oraz rozpowszechnia informacje, podszywając się pod prywatne media;
- zdolność TikToka (platformy do udostępniania filmów stworzonej przez chińską firmę ByteDance) do ogłupiania użytkowników, promowania antyspołecznych wartości, a w skrajnych przypadkach nakłaniania osób najbardziej podatnych do popełnienia samobójstwa. Powyższe powody, które według niektórych ekspertów miałyby uczynić z aplikacji „superoperację psychologiczną", skłaniają coraz więcej krajów do ograniczenia lub całkowitego zakazu dostępu do niej;
- produkowanie od drugiej dekady XXI w. w Turcji filmów, oper mydlanych i seriali telewizyjnych o tematyce historycznej i religijnej, których akcja toczy się głównie w epoce osmańskiej, co w niektórych krajach, takich jak Egipt i Arabia Saudyjska, wywołało kontrowersje ze względu na silny wpływ psychologiczny, jaki wywierały na widzów. Specjaliści określili to mianem „otomanii", która może objawiać się na różne sposoby: nagłą fascynacją kulturą turecką, poparciem dla polityki Recepa Tayyipa Erdoğana, a w skrajnych przypadkach – przejściem na islam;
- rosyjska inwazja na Ukrainę w lutym 2022 r. – wyciągając wnioski z wydarzeń na Krymie, Ukraińcy stali się bardziej sceptyczni wobec informacji w mediach społecznościowych. Według brytyjskiego think tanku Dossier rząd rosyjski rozesłał do państwowych mediów podręcznik zawierający instrukcje, takie jak „Ważne jest, aby nadal twierdzić, że Stany Zjednoczone i ich sojusznicy opracowują broń nuklearną i biologiczną w Ukrainie".

NATO współpracuje z różnymi organizacjami w celu zwalczania wojny kognitywnej, a mianowicie:

- wdraża międzynarodowe środki współpracy: działa z ponad 20 państwami członkowskimi, licznymi zespołami NATO, środowiskiem akademickim i ekspertami przemysłowymi;
- dzieli się wiedzą: tworzy forum wymiany badań i informacji między państwami członkowskimi i partnerskimi;
- opracowuje koncepcje: eksperci z wielu dyscyplin w Dowództwie Transformacji NATO opracowują koncepcje mające na celu ochronę Sojuszu przed zagrożeniami wynikającymi z wojny kognitywnej;
- współpracuje z sektorem prywatnym poprzez angażowanie ekspertów branżowych w opracowywanie koncepcji i strategii; organizowanie wspólnych grup roboczych i warsztatów; tworzenie mechanizmów wymiany informacji i synchronizacji zdolności, które mogą zmniejszyć ryzyko militarne i zwiększyć prawdopodobieństwo powodzenia misji;
- współpracuje ze środowiskiem akademickim poprzez opracowywanie koncepcji (praca z ekspertami interdyscyplinarnymi mająca na celu ochronę NATO przed zagrożeniami związanymi z wojną kognitywną); organizowanie wydarzeń edukacyjnych i szkoleń; udzielanie wskazówek w kwestiach świadomości, współpracy cywilno-wojskowej, odporności społecznej i wymiany danych; promowanie badań naukowych.

W wojnie kognitywnej szczególny nacisk kładzie się na wykorzystanie nowych technologii przełomowych (EDT) i wynikające z nich efekty poznawcze. Ta innowacja podkreśla znaczenie koncepcji we współczesnej wojnie, w której postęp technologiczny odgrywa kluczową rolę. Jednak analiza empiryczna wojny kognitywnej jest obecnie utrudniona przez brak przykładów w terenie i trudności związane z pomiarami. Pomimo to koncepcja ta ma duży potencjał.

Wojna kognitywna jest 1 z najbardziej niebezpiecznych form współczesnego konfliktu, ponieważ:

- nie ma formalnego początku ani końca;
- nie wymaga użycia broni;
- jest trudna do przypisania konkretnemu sprawcy;
- działa długofalowo i podprogowo.

Wojna kognitywna jest ważną formą propagandy opinii publicznej, perswazji psychologicznej i walki ideologicznej opartej na współczesnych teoriach i nauce, mającej na celu przejęcie inicjatywy nad myślami, przekonaniami i wartościami ludzi. Nie dąży do zniszczenia przeciwnika fizycznie, lecz zmiany sposobu, w jaki myśli, postrzega rzeczywistość i podejmuje decyzje.

Działania z zakresu wojny kognitywnej budzą kontrowersje etyczne i spotykają się z krytyką za ingerencję w sprawy wewnętrzne społeczeństw docelowych, naruszanie wolności słowa i podważanie procesów demokratycznych.

Koncepcja wojny kognitywnej, opracowana przez NATO ACT, jest z natury zorientowana na przyszłość. Współczesna myśl strategiczna wskazuje na wyraźną konwergencję wojny kognitywnej z takimi zjawiskami jak zagraniczne operacje manipulacji informacją (FIMI) czy szeroko rozumiane zagrożenia hybrydowe. Granice między tymi pojęciami są płynne, gdyż wszystkie one zmierzają do destabilizacji przeciwnika poprzez instrumentalizację domeny informacyjnej. Wojna kognitywna mogłaby zatem zostać skutecznie zintegrowana jako element taktyczny w ramach szerszych strategii zagrożeń hybrydowych.

Olga Wasiuta

B. Claverie, F. du Cluzel, *The Cognitive Warfare Concept*, https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf (dostęp 16.12.2025); *Cognitive Warfare Focus for September 2025. NATO Cogwar Perception*, „Applied Cognitive Effects Newsletter Perception" 09.2025, vol. 1, no. 1, https://www.act.nato.int/wp-content/uploads/2025/10/20250819_CogWar-Newsletter-September.pdf (dostęp 15.12.2025); *Cognitive Warfare*, „Applied Cognitive Effects Newsletter Perception" 11.2025, no. 3, https://www.act.nato.int/wp-content/uploads/2025/11/20251105_CogWar-Newsletter_November.pdf (dostęp 15.12.2025); *Cognitive Warfare*, „Applied Cognitive Effects Newsletter Perception" 12.2025, no. 4, https://www.act.nato.int/wp-content/uploads/2025/12/20251219_CogWar-Newsletter-December.pdf (dostęp 16.12.2025); *Cognitive Warfare*, https://www.act.nato.int/activities/cognitive-warfare/ (dostęp 15.12.2025); *Countering Cognitive Warfare: Awareness and Resilience*, *„NATO Review" 2021,* https://www.scribd.com/document/838634646/NATO-Review-Countering-cognitive-warfare-awareness-and-resilience-2021 (dostęp 16.12.2025); C. Deppe, G.S. Schaal, *Cognitive*

warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept, „Front Big Data" 1.11.2024, vol. 7, 10.3389/fdata.2024.1452129; M. Karwowski, *Wojna już trwa, a polem bitwy są ludzkie umysły*, 10.07.2024, https://biznesalert.pl/wojna-kognitywna-dezinformacja-manipulacja-bezpieczenstwo/ (dostęp 15.12.2025); R. Reczkowski, A. Lis, *Cognitive Warfare: what is our actual knowledge and how to build state resilience?*, „Bezpieczeństwo. Teoria i Praktyka. Security. Theory and Practice" 2022, no. 3(XLVIII); *The Role of NATO and its Strategic Commands. Two Strategic Commands*, https://www.act.nato.int/activities/act-20th-anniversary/ (dostęp 16.12.2025); H.D. Thoreau, *Cognitive Warfare, "It's not what you look at that matters, it's what you see"*, „Applied Cognitive Effects Newsletter Perception" 10.2025, vol. 1, no. 2, https://www.act.nato.int/wp-content/uploads/2025/10/20251001_CogWar-Newsletter-October.pdf (dostęp 15.12.2025).

WOJNA KULTUROWA – konflikt ideologiczny między grupami społecznymi i walka o dominację nad ich wartościami, przekonaniami i praktykami. Zazwyczaj ogranicza się do palących problemów, w których występuje powszechna niezgodność społeczna i widoczna jest polaryzacja wartości. W sytuacjach nierównowagi sił konflikt ten przestaje opierać się na słusznych argumentach, a nabiera konotacji nadużywania władzy i propagandy mającej na celu ustanowienie historycznego rewizjonizmu.

Pojęcie „wojny kulturowej" często pojawia się w debacie publicznej, lecz jego znaczenie bywa niejednorodne. W ujęciu politologicznym i socjologicznym termin ten można zdefiniować jako długotrwały konflikt o wartości, normy i tożsamość, który toczy się w przestrzeni symbolicznej; nie dotyczy bezpośrednio zasobów materialnych ani terytorium, zamiast tego obejmuje spory o interpretację świata, granice wolności, role społeczne, prawa mniejszości czy sposób organizacji życia publicznego.

Współczesne wojny kulturowe rozgrywają się za pomocą narracji; strony sporu formułują opowieści o społeczeństwie, historii, tradycji oraz przyszłości, konkurując o to, która z nich stanie się dominująca. W tym sensie wojna kulturowa łączy się bezpośrednio z funkcjonowaniem mediów i popkultury, które dostarczają symboli i wzorów interpretacyjnych. Obrazy, memy, slogany i historie stają się narzędziem walki o znaczenia. Narracje budowane w przestrzeni publicznej mogą polaryzować społeczeństwa, ponieważ przedstawiają świat w formie uproszczonych opozycji: „my kontra oni", „wartości tradycyjne kontra nowoczesność", „patriotyzm

kontra kosmopolityzm". Ten dualizm sprzyja eskalacji konfliktu, ponieważ utrudnia dialog i kompromis.

Wojna kulturowa dotyczy również konfliktów o rolę instytucji publicznych, takich jak szkoła, uniwersytet, media, kościoły czy system prawny. Każda ze stron sporu dąży do tego, by owe instytucje odzwierciedlały określoną wizję społeczeństwa. Ten typ konfliktu wiąże się silnie z polityką tożsamości; ludzie bronią określonych wartości, ponieważ są one częścią ich osobistego i zbiorowego „ja", a to sprawia, że wojny kulturowe mają intensywny ładunek emocjonalny i nie wygasają wraz z kompromisami politycznymi. W odróżnieniu od sporów o zasoby, konflikty symboliczne nie mają jednego rozwiązania, które satysfakcjonuje wszystkie strony, dlatego wojna kulturowa może trwać latami, wciąż odtwarzana przez nowe pokolenia.

Pojęcie wojny kulturowej ma złożoną genezę sięgającą sporów polityczno-religijnych XIX w., a następnie zostało przekształcone w nowoczesną kategorię opisu konfliktów dotyczących wartości, norm i tożsamości zbiorowych. W ujęciu historycznym za jeden z najwcześniejszych i najbardziej znaczących przykładów konfliktu o charakterze kulturowym uznaje się niemiecki *Kulturkampf* – spór między państwem pruskim a Kościołem katolickim na przełomie lat 60. i 70. XIX w. Toczył się on m.in. o kontrolę nad edukacją, regulacje dotyczące małżeństwa oraz obsadę stanowisk kościelnych, ujawniając starcie odmiennych wizji ładu politycznego i społecznego. W literaturze wskazuje się, że właśnie w tym okresie termin ten zaczął funkcjonować szerzej jako określenie walki o dominację określonego systemu wartości. W kontekście Stanów Zjednoczonych zwraca się uwagę, że spory o charakterze kulturowym pojawiały się już pod koniec XIX i na początku XX w., m.in. w debatach dotyczących edukacji, moralności publicznej, języka nauczania czy prohibicji. Jednak współczesne, szeroko akceptowane znaczenie pojęcia *culture war* ukształtowało się dopiero w drugiej połowie XX w. W analizach podkreśla się, że konflikty te dotyczą nie tylko zagadnień politycznych, lecz przede wszystkim wyobrażeń o tym, jakie wartości powinny określać wspólnotę oraz jakie normy moralne mają stanowić fundament ładu społecznego.

W literaturze przedmiotu wojna kulturowa jest opisywana jako długotrwały i strukturalny konflikt o wartości, normy i tożsamość zbiorową,

w którym strony mobilizują zasoby symboliczne – historyczne, religijne, edukacyjne i medialne – aby nadać dominujące znaczenie określonym interpretacjom rzeczywistości społecznej. Elżbieta Wiącek podkreśla, że wojna kulturowa oznacza konflikt prowadzony w sposób pokojowy, ale mający wyraźnie polityczny, ideologiczny i cywilizacyjny charakter. Spór ten zachodzi pomiędzy różnymi grupami społecznymi, szczególnie środowiskami o poglądach konserwatywnych i zwolennikami nurtów liberalno-lewicowych. Jego istotą jest dążenie uczestników do narzucenia pozostałym członkom społeczeństwa własnej wizji świata oraz reprezentowanej ideologii obejmującej przekonania moralne, wartości i normy dotyczące funkcjonowania życia społecznego. W efekcie walka ta dotyczy sposobu interpretowania rzeczywistości oraz prób jej przeobrażenia poprzez zmianę powszechnie obowiązujących zasad i prawa.

Współczesne wojny kulturowe obejmują szeroki zakres konfliktów dotyczących wartości, norm społecznych oraz symbolicznych definicji tożsamości zbiorowej. W wymiarze moralnym szczególnie widoczne są spory o prawa mniejszości, w tym seksualnych i etnicznych, które w wielu państwach stały się jednym z głównych obszarów polaryzacji. Debaty te często przybierają formę napięcia między orientacją liberalną, akcentującą autonomię jednostki i równość wobec prawa, a konserwatywną odwołującą się do znaczenia tradycji, religii i dziedzictwa kulturowego. Podobne konflikty dotyczą roli religii w życiu publicznym, zwłaszcza w kontekście świeckości państwa, edukacji seksualnej czy praw reprodukcyjnych. Szczególną rolę odgrywa tu szkoła jako instytucja socjalizacyjna, stanowiąca kluczowe pole rywalizacji o to, jakie normy i wzorce społeczno-kulturowe mają zostać przekazane kolejnym pokoleniom. Równolegle rozwijają się konflikty polityczne i geopolityczne, w których narracje kulturowe pełnią funkcję istotnego narzędzia oddziaływania.

Jednym z najczęściej analizowanych przykładów jest rywalizacja narracyjna związana z agresją Federacji Rosyjskiej na Ukrainę. W licznych badaniach podkreśla się, że Rosja wykorzystuje reinterpretacje historii, symbole walki z faszyzmem oraz retorykę „obrony tradycyjnych wartości", aby legitymizować swoje działania. Z kolei Ukraina przedstawiana jest w wielu analizach jako państwo broniące suwerenności, integralności terytorialnej i zasad prawa międzynarodowego, a także aktor odwołujący

się do wartości demokratycznych oraz solidarności międzynarodowej. W tym sensie konflikt rosyjsko-ukraiński stanowi przykład, w którym wojna kulturowa i narracyjna splatają się z rywalizacją polityczną i militarną. Podobnie relacje USA–Chiny coraz częściej interpretowane są nie tylko jako konkurencja gospodarcza czy technologiczna, lecz również spór o dominujące modele kulturowo-polityczne. W dyskursie pojawia się opozycja między liberalnym porządkiem demokratycznym a modelem autorytarnego kapitalizmu, co wpływa na sposób, w jaki opinia publiczna i instytucje międzynarodowe interpretują działania obu stron. Narracje te przenikają nie tylko do debat eksperckich, lecz także globalnej kultury masowej.

Wojny kulturowe są również widoczne w sferze popkultury, która stała się jednym z kluczowych pól sporów o reprezentacje i znaczenia symboliczne. W przestrzeni popkultury konflikty te często przybierają formę kampanii konsumenckich, bojkotów, wiralowych sporów w mediach społecznościowych oraz długotrwałych dyskusji o tym, jakie narracje kulturowe powinny dominować w globalnym obiegu.

Choć pojęcie wojny kulturowej jest stosunkowo nowe, samo zjawisko w historii społeczeństw pojawiało się wielokrotnie. Narodziło się w Stanach Zjednoczonych, kiedy socjolog James Davison Hunter spopularyzował je w 1991 r., opisując narastające konflikty między grupami o odmiennych wartościach i wizjach społeczeństwa. Jednak samo zjawisko jest znacznie starsze i wynika z przemian społecznych lat 60. XX w., kiedy to ruchy praw obywatelskich, feminizm, protesty studenckie oraz rewolucja obyczajowa zaczęły głęboko dzielić społeczeństwo. Politycy szybko zauważyli, że spory dotyczące moralności, religii czy obyczajów mobilizują wyborców do opowiedzenia się po jednej „stronie", dlatego zaczęli wykorzystywać je jako narzędzia walki politycznej. Media wzmocniły te podziały, nagłaśniając konflikty i tworząc przestrzeń, w której różne grupy coraz bardziej zamykały się w swoich przekonaniach.

Wraz z rozwojem internetu i mediów społecznościowych zjawisko to przeniosło się także do innych krajów, w tym europejskich, gdzie wojny kulturowe zaczęły toczyć się wokół takich kwestii, jak religia w życiu publicznym, migracja, prawa mniejszości czy rola tradycji. W ten sposób współczesne wojny kulturowe stały się globalnym problemem

wynikającym z szybkich zmian społecznych, politycznego wykorzystania sporów i rosnącej roli mediów. Wojna kulturowa prowadzi do polaryzacji, która wykracza poza zwykłe różnice poglądów, a prowadzi do tego, że ludzie przestają postrzegać drugą stronę jako osobę o odmiennym zdaniu, a zaczynają traktować ją jako „kogoś gorszego" lub wręcz zagrożenie. Proces ten jest wzmacniany przez selekcję informacji, co oznacza, że ludzie szukają wiadomości potwierdzających ich przekonania i unikają tych, które mogłyby je podważać. Dodatkowo emocjonalizacja dyskursu sprawia, że spory stają się bardziej gwałtowne czy osobiste. Istotne jest też utożsamianie poglądów z przynależnością do grupy, krytyka czyjegoś zdania często jest odbierana jako atak na całą społeczność, do której się należy. Polaryzację wzmacniają również działania partii politycznych, które wykorzystują konflikty kulturowe do mobilizacji poparcia i budowania własnej pozycji. Ostatecznie społeczeństwo dzieli się coraz bardziej, a komunikacja między grupami staje się trudniejsza i niejednokrotnie nacechowana wrogością. Wojna kulturowa to zjawisko społeczne charakteryzujące się konfliktem pomiędzy różnymi grupami, których wartości, przekonania, ideologie czy styl życia są diametralnie odmienne. W najogólniejszym ujęciu dotyczy ona sporu o to, jakie normy i praktyki powinny dominować w danej społeczności.

Pojęcie „wojny kulturowej" zyskało szczególną prominencję w dyskursie publicznym pod koniec XX w. Wzrost wpływów ruchów konserwatywnych w latach 80. zapoczątkował istotną reorientację w amerykańskiej polityce, która z czasem oddziaływała również na inne demokracje zachodnie. Termin ten odnosi się do starcia na polu tożsamości, religii, tradycji, a także kwestii związanych z prawami człowieka, edukacją, mediami czy kulturą popularną.

Wojny kulturowe mogą mieć charakter lokalny, narodowy lub globalny, a ich katalizatorami bywają procesy globalizacyjne, rozwój technologii czy zmiany demograficzne. W kontekście historycznym wojny kulturowe pojawiały się w różnych epokach jako reakcja na zmiany społeczne, lecz we współczesnym świecie są one szczególnie widoczne ze względu na szybkie tempo transformacji społecznych i medialnych. Zjawisko to ma swoje korzenie w długiej historii ludzkości, a współczesne spory wokół takich

kwestii jak prawa kobiet, wolność słowa, religia czy prawa mniejszości są jedynie najnowszym przejawem tego fenomenu.

Wojny kulturowe nie są wynalazkiem współczesności; już w starożytności obserwowano starcia cywilizacji, które nie dotyczyły jedynie podbojów terytorialnych, ale również dominacji kulturowej. Jednym z pierwszych wyraźnych przykładów wojny kulturowej był konflikt między starożytną Grecją a Persją. Wojny perskie w V w. p.n.e. były nie tylko starciem militarnym, ale również ideologicznym – Grecy reprezentowali idee demokracji i wolności jednostki, podczas gdy Persowie symbolizowali scentralizowaną monarchię i teokratyczną dominację. Podobnie starcia kulturowe były widoczne w średniowieczu, kiedy chrześcijaństwo konkurowało z islamem o dominację w regionie Morza Śródziemnego. Wyprawy krzyżowe, które rozpoczęły się w XI w., były nie tylko konfliktem religijnym, ale również starciem 2 odmiennych światopoglądów i systemów wartości. Obie strony próbowały narzucić swoją wizję ładu światowego, co prowadziło do licznych wojen, migracji i przemian kulturowych.

Pojęcie „wojna kulturowa" stało się popularne w latach 90. XX w. Społeczeństwo amerykańskie zostało podzielone na 2 obozy: konserwatywny, który opowiada się za tradycyjnymi wartościami, takimi jak religia chrześcijańska, rodzina nuklearna, patriotyzm i zachowanie istniejącego porządku społecznego, oraz liberalny, promujący sekularyzację, prawa mniejszości (na przykład LGBT, osób czarnoskórych, kobiet), pluralizm kulturowy, równość społeczną oraz progresywne podejście do zmian społecznych.

Zasadnicza cecha wojny kulturowej tkwi w jej długoterminowym charakterze, wykraczającym poza cykliczność kampanii wyborczych. Przedmiotem rywalizacji są fundamentalne idee i wartości determinujące społeczny, moralny, duchowy i ekonomiczny rozwój zbiorowości. Konflikt ten transcenduje zatem czysto utylitarne rozważania nad efektywnością ekonomiczną poszczególnych systemów społeczno-politycznych, obejmując również normatywne pytania o sprawiedliwość, wartości moralne i duchowe fundamenty trwałego rozwoju społecznego. Wojna kulturowa operuje przez złożoną sieć instytucji i mediów społecznych. Do jej nośników należą: uniwersyteckie sale wykładowe, podręczniki edukacyjne, instytucje oświatowe wszystkich szczebli, sztuka, media audiowizualne

(telewizja, kino, platformy streamingowe), radio, muzyka popularna, literatura, prasa drukowana i cyfrowa, media społecznościowe, fundacje i organizacje pozarządowe, rodzina jako instytucja socjalizacyjna, wspólnoty religijne oraz sport. Co istotne, również symbolika przestrzeni publicznej, taka jak pomniki, nazewnictwo ulic i obiektów infrastrukturalnych, funkcjonuje jako narzędzie propagacji określonych narracji historycznych i wartości.

Wojna kulturowa pokazuje, że informacja nigdy nie jest neutralna: zawsze niesie ze sobą konsekwencje. Media, które miały jedynie informować, stały się również narzędziem wpływu, wpływając na myśli i emocje. W świecie natłoku treści trudno odróżnić prawdę od manipulacji, a granice między wiedzą a opinią zacierają się. To, co czytamy i oglądamy, kształtuje nasze postrzeganie rzeczywistości, niejednokrotnie bez naszej świadomości. Jednocześnie każdy z nas ma dziś możliwość wyboru, weryfikacji i krytycznego spojrzenia na świat, choć wymaga to wysiłku i refleksji. Pytanie brzmi: czy wykorzystamy tę szansę, czy pozwolimy mediom decydować za nas?

Wojna kulturowa nie toczy się tylko w debatach publicznych, ale w naszych własnych umysłach i codziennym życiu. Jako świadoma jednostka musimy nauczyć się myśleć samodzielnie i odpowiedzialnie wybierać źródła informacji. W cyfrowej rzeczywistości nasza świadomość staje się najpotężniejszym narzędziem, a jej brak – zagrożeniem. Ostatecznie to od nas zależy, czy media będą dla nas szansą, dodatkiem, sposobem porozumienia czy murem, który dzieli nas jako społeczeństwo. Wojna kulturowa jest jednym z najważniejszych wyzwań współczesnych społeczeństw; choć nie ma jednoznacznych rozwiązań dla wszystkich kwestii, które się w niej pojawiają, to zrozumienie i akceptacja odmiennych poglądów mogą pomóc w tworzeniu bardziej harmonijnych społeczności. Ostatecznie wojna kulturowa nie polega na „wygraniu" jednej strony, ale znalezieniu wspólnego gruntu i umiejętności współżycia w różnorodności.

Żanna Osikowicz

J. Baranowski, *Dlaczego kultura jest ważna dla naszej tożsamości i wspólnoty*, 2025, https://starenowemapy.pl/dlaczego-kultura-jest-wazna-dla-naszej-tozsamosci-i-wspolnoty (dostęp 24.01.2026); W.J. Burszta, *Wojny kulturowe jako fenomen*

antropologiczny, https://nck.pl/upload/archiwum_kw_files/artykuly/2._ wojciech_j._burszta_-_wojny_kulturowe_jako_fenomen_antropologiczny.pdf (dostęp 24.01.2026); D. Dziwisz, *Wojna na media społecznościowe. (Selektywna) polityka informacyjna Facebooka a wojna w Ukrainie*, „Komentarz KBN" 2022, nr 14(103); W. Jóźwicki, *Wojna kultur w Ameryce i na świecie. Moralność mieszczańska czy etos rycerski remedium na kontrkulturę? Oraz kilka innych uwag na marginesie książki Gertrude Himmelfarb „Jeden naród, dwie kultury"*, „*Civitas. Studia z Filozofii Polityki*" 2010, nr 12; J. Koperek, *Nowe demokracje a kulturowa jedność Europy*, „Seminare. Poszukiwania naukowe" 2004, nr 20; W. Możgin, *Wojna kulturowa między Rosją a Ukrainą. Sposób na osłabienie rosyjskiego kulturowego imperializmu*, „POLITEJA" 2022, nr 3(78); T. Mróz, *Polska wojna kulturowa: pole bitwy i strona konfliktu*, „Kultura Popularna" 2015, nr 2; P. Przybysz, *Wojny kulturowe*, [w:] *Kulturowe konteksty wojny*, M. Ciesielski, P. Pawlak, S. Szykowna (red.), Wydawnictwo Rys, Poznań–Gniezno 2023; M. Staniszewski, *Polska wojna kulturowa*, Wydawnictwo WEI, Warszawa 2022.

WOJSKA AEROMOBILNE – rodzaj wojsk wchodzący w skład Wojsk Lądowych Sił Zbrojnych RP, w którego strukturze znajdują się związki taktyczne, oddziały i pododdziały zdolne zarówno do manewrowania w powietrzu, jak i prowadzenia walki z powietrza oraz lądu i powietrza. Wojska aeromobilne mogą – ale nie muszą – etatowo posiadać statki powietrzne.

Celem działań wojsk aeromobilnych zgodnie z Regulaminem ogólnym Wojsk Lądowych jest zwiększenie możliwości bojowych przez przeniesienie działań w głąb ugrupowania przeciwnika (tworzenie nowych ognisk walki) i wspieranie ich w przejęciu inicjatywy i uzyskaniu swobody działania. Do zadań szczegółowych realizowanych przez wojska aeromobilne należą: opanowanie i utrzymanie kluczowego terenu; możliwość wykonania manewru pionowego; przeprowadzanie rajdów; prowadzenie działań rozpoznawczych; izolacja obszaru (rejonu) działań; wspieranie działań mających na celu zmylenie przeciwnika; przeciwdziałanie rozpoznaniu przeciwnika; wzmocnienie okrążonych sił.

W skład wojsk aeromobilnych wchodzą jednostki powietrzno-desantowe, kawalerii powietrznej, desantowo-szturmowe i lotnictwa wojsk lądowych.

Regulamin działań Wojsk Lądowych mówi, iż wojska powietrznodesantowe stanowią siły, które są wyszkolone i wyposażone do wykonania zadań po desantowaniu sposobem spadochronowym. Wykonują one przede wszystkim działania na obiekty położone w głębi ugrupowania przeciwnika, samodzielnie lub we współdziałaniu z innymi siłami. Używane są także w działaniach stabilizacyjnych, w tym w celu rozdzielenia stron konfliktu, opanowania ważnych obiektów, wzmocnienia sił stabilizacyjnych, demonstracji siły czy prewencyjnego rozmieszczenia sił. Są także wykorzystywane w sytuacjach kryzysowych, np. gdy istnieje potrzeba dostarczenia sił i środków metodą zrzutu spadochronowego. Prowadzą również operacje ewakuacji osób niezaangażowanych, szczególnie gdy wymaga to użycia siły.

Z kolei kawaleria powietrzna to siły przeznaczone do wykonania zadań po desantowaniu przy wykorzystaniu śmigłowców.

Krystian Frącik, Grzegorz Plaskota i Arkadiusz Skrzek definiują wojska desantowo-szturmowe jako siły przeznaczone do realizacji zadań w wymiarze powietrzno-lądowym, gdzie zasadniczym celem organizacyjnym jest uzyskanie synergii wynikającej z połączenia potencjału komponentu lądowego i śmigłowców realizujących zadania zarówno transportowe jak i wsparcia bezpośredniego działań.

Lotnictwo wojsk lądowych w ujęciu tych autorów obejmuje pododdziały, oddziały i związki taktyczne śmigłowców, a czasem lekkich samolotów. Jest ono przeznaczone do wsparcia ogniowego; osłony wojsk lądowych przed rozpoznaniem i uderzeniami z powietrza przez wolno latające aparaty powietrzne przeciwnika; prowadzenia działań powietrzno-szturmowych (powietrzno-manewrowych), rozpoznania powietrznego; zabezpieczenia działań tych wojsk.

Już pod koniec I wojny światowej, w połowie 1918 r., z pomysłem wykorzystania wojsk spadochronowych do przełamania frontu zachodniego wystąpił amerykański generał William B. Mitchell. Zaproponował on sformowanie w strukturach wojsk alianckich batalionów spadochroniarzy i przerzucenie ich na tyły wojsk niemieckich.

Do koncepcji „pionowego uderzenia" wrócili na przełomie lat 20. i 30. XX w. Sowieci. 2 sierpnia 1930 r., w czasie doświadczalno-pokazowych ćwiczeń sił lotniczych Moskiewskiego Okręgu Wojskowego przeprowadzono

pod Woroneżem pierwszy w historii desant spadochronowy z udziałem 12 skoczków. Zwolennikiem rozbudowy formacji spadochronowych był marszałek Michaił Tuchaczewski, który proponował utworzenie zmotoryzowanej dywizji lotniczej i przeprowadzenia z jej udziałem operacji kombinowanej. Jego zdaniem skoczkowie mieli być rzucani na nieprzyjacielskie lotniska lub inne dogodne do lądowania miejsca i przejmować nad nimi kontrolę, a następnie czekać na siły główne obejmujące piechotę desantową, pojazdy i sprzęt ciężki. W 1932 r. w rejonie Kijowa, w obecności zachodnich obserwatorów, Sowieci przeprowadzili ćwiczenia połączone z desantem prawie 1200 spadochroniarzy. Wojska powietrznodesantowe stały się wkrótce elementem nowej sowieckiej doktryny głębokiej operacji.

Współczesne Wojska Powietrznodesantowe Federacji Rosyjskiej są osobnym rodzajem sił, które nie podlegają dowódcom okręgów wojskowych, a jedynie dowództwu WPD w Moskwie. W 2022 r. liczyły one około 33 tys. żołnierzy, a ich struktura opierała się na: Dowództwie WPD w Moskwie; Centrum Dowodzenia WPD w Moskwie; 7 Dywizji Desantowo-Szturmowej; 76 Dywizji Desantowo-Szturmowej; 98 Dywizji Powietrznodesantowej; 106 Dywizji Powietrznodesantowej; 11 Samodzielnej Brygadzie Desantowo-Szturmowej; 31 Samodzielnej Brygadzie Desantowo-Szturmowej; 83 Samodzielnej Brygadzie Desantowo-Szturmowej; 45 Samodzielnej Brygadzie Specjalnego Przeznaczenia; 38 Samodzielnej Brygadzie Dowodzenia; 150 Samodzielnym Batalionie Remontowym; szkołach i ośrodkach szkolenia. Na ich wyposażeniu znajdował się sprzęt ciężki, w tym czołgi, bojowe wozy desantowe czy transportery opancerzone.

W trakcie rosyjskiej wojny przeciwko Ukrainie spadochroniarze walczą przede wszystkim jako piechota lub piechota zmechanizowana. Najważniejszym przykładem użycia WPD w tym konflikcie był dokonany już pierwszego dnia desant śmigłowcowy na lotnisko Antonowa w Hostomelu. Najpewniej celem desantu było opanowanie lotniska i umożliwienie lądowania samolotów transportowych ze wzmocnieniem w postaci komponentu zmechanizowanego. Skuteczna obrona lotniska przez siły ukraińskie doprowadziła do porażki Rosjan.

Wojska aeromobilne niepodległej Ukrainy od początku wchodziły w skład wojsk lądowych. W 2012 r. zostały przemianowane na wysoko mobilne wojska desantowe. Doświadczenia związane z walkami przeciwko

rosyjskiej agresji w 2014 r. i aneksji Krymu doprowadziły do przekształcenia ich w 2016 r. w osobny rodzaj wojsk. W 2018 r. uchwałą Rady Najwyższej zmieniono ich nazwę na wojska desantowo-szturmowe.

W momencie agresji rosyjskiej na Ukrainę w 2022 r. Dowództwu Wojsk Desantowo-Szturmowych w Żytomierzu podlegały: 25 Samodzielna Siczesławska Brygada Powietrznodesantowa w m. Hwardijske, 79 Samodzielna Brygada Desantowo-Szturmowa w m. Mikołajów, 80 Samodzielna Brygada Desantowo-Szturmowa we Lwowie, 81 Samodzielna Brygada Aeromobilna w m. Drużkiwka, 95 Samodzielna Brygada Desantowo-Szturmowa w Żytomierzu, 132 Samodzielny Batalion Rozpoznawczy w Żytomierzu, 135 Samodzielny Batalion Dowodzenia w Żytomierzu, 148 Samodzielny Dywizjon Samobieżnych Haubic w Żytomierzu, 199 Centrum Szkolenia Wojsk Desantowo-Szturmowych w m. Teteriwka, jednostki logistyczne. Doświadczenia wojenne spowodowały odejście od doktryny lekkich wojsk aeromobilnych na rzecz zmechanizowanych wojsk rajdowych, również z komponentem pancernym. Sformowano również dowództwo szczebla korpusu w postaci 7 Korpusu Desantowo-Szturmowego. Dodatkowo już w czasie wojny utworzono 3 nowe brygady desantowo-szturmowe – 46, 77 i 82. W skład Wojsk Desantowo-Szturmowych wszedł także 78 Pułk Szturmowy Herc.

Początki polskich wojsk aeromobilnych wiążą się z historią działającej w ramach Polskich Sił Zbrojnych na Zachodzie 1 Samodzielnej Brygady Spadochronowej dowodzonej przez gen. Stanisława Sosabowskiego. Powstała ona w 1941 r. na bazie 4 Brygady Kadrowej Strzelców i pierwotnie miała wziąć udział w powstaniu zbrojnym na terenie okupowanej Polski, do czego ostatecznie nie doszło. Uczestniczyła we wrześniu 1944 r. w Market Garden, największej operacji powietrznodesantowej podczas II wojny światowej. Została rozformowana w 1947 r.

W 1957 r. przeformowano 6 Pomorską Dywizję Piechoty na 6 Pomorską Dywizję Powietrznodesantową z dowództwem w Krakowie. Ze względu na swoje wyszkolenie i wyposażenie uważana była od początku za formację elitarną. W 1973 r. wystawiła Polską Jednostkę Specjalną Pokojowych Sił ONZ w Egipcie. W 1986 r. przeformowano ją w 6 Pomorską Brygadę Powietrznodesantową, a w 1989 r. – w 6 Pomorską Brygadę Desantowo–Szturmową. W latach 1991–2009 funkcjonowała jako 6 Brygada

Desantowo-Szturmowa. W 2009 r. przemianowana została na 6 Brygadę Powietrznodesantową, równocześnie odzyskując pierwotny charakter związku taktycznego wojsk powietrznodesantowych.

Obecnie strukturę wojsk aeromobilnych Sił Zbrojnych RP stanowią:

- 6 Brygada Powietrznodesantowa;
- 25 Brygada Kawalerii Powietrznej;
- 1 Brygada Lotnictwa Wojsk Lądowych.

Strukturę 6 Brygady Powietrznodesantowej stanowią: dowództwo i sztab brygady w Krakowie, 6 Batalion Dowodzenia, 6 Batalion Powietrznodesantowy, 16 Batalion Powietrznodesantowy, 18 Bielski Batalion Powietrznodesantowy, 6 Batalion Logistyczny.

Do podstawowych zadań 6 Brygady Powietrznodesantowej zalicza się: uchwycenie oraz utrzymanie do czasu nadejścia sił głównych kluczowych punktów terenowych i rejonów położonych w głębi ugrupowania operacyjnego przeciwnika; atakowanie i niszczenie lotnisk, lądowisk, baz, składów, magazynów i innych ważnych obiektów na głębokim zapleczu przeciwnika; odblokowanie i wspieranie wojsk własnych, które znalazły się w okrążeniu; dezorganizację i niszczenie systemów dowodzenia, łączności, komunikacji, logistyki oraz odwodów zgrupowanych na tyłach przeciwnika; prowadzenie działań opóźniających; wsparcie operacji specjalnych; prowadzenie ewakuacji personelu niewojskowego w warunkach wymagających użycia siły.

Z kolei 25 Brygada Kawalerii Powietrznej z dowództwem w Tomaszowie Mazowieckim powstała w 1999 r. w wyniku przeformowania istniejącej od 1995 r. 25 Dywizji Kawalerii Powietrznej. Jednostka jest związkiem taktycznym przeznaczonym do prowadzenia działań powietrzno-szturmowych i desantowo-szturmowych. Jej strukturę stanowią obecnie: dowództwo i sztab, 25 Batalion Dowodzenia, 1 Batalion Kawalerii Powietrznej, 7 Batalion Kawalerii Powietrznej, 1 Dywizjon Lotniczy, 7 Dywizjon Lotniczy, 25 Batalion Logistyczny, Powietrzna Jednostka Ewakuacji Medycznej, Ośrodek Szkolenia Aeromobilno-Spadochronowego oraz 22 Karpacki Batalion Piechoty Górskiej.

1 Brygada Lotnictwa Wojsk Lądowych z dowództwem w Inowrocławiu powstała w 2011 r. Podlegają jej bazy lotnicze 49 i 56. Jest przeznaczona do wsparcia związków taktycznych i jednostek (pododdziałów) na polu walki;

zabezpieczenia dowodzenia, realizacji zadań transportowo-łącznikowych; rozpoznania; korygowania ognia artylerii; zabezpieczenia przerzutu grup dalekiego rozpoznania i grup specjalnych; prowadzenia operacji bojowego poszukiwania i ratownictwa we wszystkich warunkach atmosferycznych w dzień i w nocy. Ma również zadania w zakresie reagowania kryzysowego, w tym działania antyterrorystyczne i utrzymanie porządku publicznego; izolowanie zagrożonego obszaru, działania zabezpieczające, ratownicze i ewakuacyjne przy zagrożonych obiektach budowlanych i zabytkach; monitorowanie i ocena skutków zagrożeń niemilitarnych; akcje poszukiwawczo-ratownicze; ewakuacja poszkodowanej ludności i mienia; udział w zwalczaniu skutków powodzi i zatorów lodowych oraz prowadzenie prac wymagających użycia materiałów wybuchowych.

Zgodnie z Regulaminem działań Wojsk Lądowych wojska aeromobilne mogą być używane w obronie, natarciu, działaniach opóźniających; żołnierze wraz z ich wyposażeniem wykonują manewr na polu walki przy użyciu statków powietrznych w celu zaangażowania się we wspólną walkę lądowo-powietrzną. Podstawą koncepcji tych działań jest użycie śmigłowców (samolotów) w celu zwiększenia siły ognia i ruchliwości pododdziałów wojsk lądowych w ramach zintegrowanego systemu walki powietrzno-lądowej. Zasadniczym celem prowadzenia działań aeromobilnych jest zwiększenie możliwości bojowych wojsk lądowych przez przeniesienie działań w głąb ugrupowania przeciwnika (tworzenie nowych ognisk walki) i wspieranie ich w przejęciu inicjatywy i uzyskaniu swobody działania. Ich szczegółowymi zadaniami są opanowanie i utrzymanie kluczowego terenu; możliwość wykonania manewru pionowego; przeprowadzanie rajdów; prowadzenie działań rozpoznawczych; izolacja obszaru (rejonu) działań; wspieranie działań mających na celu zmylenie przeciwnika; przeciwdziałanie rozpoznaniu przeciwnika; wzmocnienie okrążonych sił.

Wojska aeromobilne uważane są – ze względu na dobór kadry i żołnierzy, ich wyszkolenie i wyposażenie – za elitarny element sił zbrojnych. Odgrywają przy tym niejednokrotnie rolę sił szybkiego reagowania.

Przemysław Wywiał, Żaneta Zając

P. Chmielowiec, *Najkrótszą drogą do kraju: 1 Samodzielna Brygada Spadochronowa*, Instytut Pamięci Narodowej, Warszawa 2025; R. Cyniak, *Siły aeromobilne w działaniach opóźniających*, „Przegląd Sił Zbrojnych" 2014, nr 5; K. Frącik, G. Plaskota, A. Skrzek, *Rola i miejsce kawalerii powietrznej w systemie wojsk aeromobilnych Sił Zbrojnych Rzeczypospolitej Polskiej*, Akademia Sztuki Wojennej, Warszawa 2019; H. Królikowski, *6 Pomorska Dywizja Powietrznodesantowa*, Ajaks, Pruszków 1997; Regulamin działań Wojsk Lądowych, Dowództwo Wojsk Lądowych – Pion Szkolenia, DWLąd Wewn. 115/2008, Warszawa 2008; K. Witulski, *Połączyła nas czasza spadochronu i esprit de corps*, Polskie Towarzystwo Geopolityczne, Kraków 2022; S. Zaloga, *Berety z gwiazdami: radzieckie wojska powietrznodesantowe*, Rytm–Bellona, Warszawa 2003.

WOJSKOWE SYSTEMY RATOWNICZE – wyspecjalizowane formacje i procedury Sił Zbrojnych RP (takie jak wojska inżynieryjne, chemiczne czy Wojska Obrony Terytorialnej), które wykorzystują swój potencjał ludzki, organizacyjny oraz specjalistyczny sprzęt do reagowania na zagrożenia niemilitarne. Ich znaczenie dla ludności cywilnej jest kluczowe w sytuacjach nadzwyczajnych, gdy siły i środki cywilne są niewystarczające do likwidacji pojawiających się zagrożeń. Wojskowe systemy ratownicze zapewniają bezpośrednią ochronę ludzi i mienia, prowadzą ewakuacje oraz dostarczają niezbędną pomoc medyczną, żywność i wodę do obszarów zagrożonych. Odgrywają kluczową rolę w systemie ochrony życia i zdrowia ludzi. Ponadto siły zbrojne pełnią kluczową funkcję w zakresie usuwania skażeń, neutralizacji materiałów niebezpiecznych oraz odbudowy zniszczonej infrastruktury, co znacząco przyspiesza proces przywracania normalnego funkcjonowania lokalnych społeczności po wystąpieniu katastrof.

Obowiązkiem państwa jest zapewnienie bezpieczeństwa obywatelom, dlatego jest ono głównym organizatorem działań ratowniczych. Poprzez utrzymanie odpowiednich zasobów kadrowych i sprzętowych, a także stosowanie efektywnych metod pracy państwo odpowiada za przygotowanie i działanie ratownictwa publicznego, w ramach którego można wyróżnić różne jego podtypy. W niektórych sytuacjach, determinowanych wielkością zdarzenia, konieczna jest integracja dziedzin i działań podmiotów ratowniczych dla powodzenia prowadzonych czynności ratowniczych. Czasem podstawowe podmioty ratownicze, takie jak Krajowy

System Ratowniczo-Gaśniczy oraz Państwowe Ratownictwo Medyczne, są niewystarczające i tutaj wsparciem dla ich działań są siły zbrojne.

Udział wojska w przeciwdziałaniu zagrożeniom niemilitarnym w Polsce ma wieloletnią tradycję, jednak jego charakter uległ znaczącym przeobrażeniom wraz ze zmianami ustrojowymi i rozwojem wyspecjalizowanych służb cywilnych. Przed 1989 r. Siły Zbrojne RP stanowiły główny filar działań ratowniczych, realizując niemal wszystkie kluczowe zadania, od usuwania zatorów lodowych po kompleksową likwidację skutków powodzi. Po transformacji ustrojowej ciężar ten przesunął się w stronę formacji cywilnych, w tym przede wszystkim Państwowej Straży Pożarnej. Sytuacje, jakie wydarzyły się w historii Polski, pokazały jednak, że całkowita rezygnacja z potencjału militarnego w sytuacjach kryzysowych jest niemożliwa. Często podaje się za przykład „powódź tysiąclecia" z 1997 r., która obnażyła słabości techniczne i organizacyjne sił cywilnych. W tamtym czasie wojsko zostało ocenione jako formacja w pełni mobilna i odpowiedzialna, zdolna do bezpośredniej ochrony ludzi i mienia w warunkach nadzwyczajnych – m.in. właśnie to doświadczenie z powodzi stało się fundamentem pod budowę nowoczesnych ram prawnych współpracy cywilno-wojskowej.

Wszystkie służby działają w określonym porządku prawnym, wykonując swoje zadania zgodnie z wyznaczonymi w ustawach i innych aktach prawnych zadaniami, obowiązkami i uprawnieniami. W przypadku działalności wojsk możemy wyróżnić kilka kluczowych dokumentów regulujących ich działanie i już wspomnianą współpracę. Podstawowym dokumentem jest Ustawa z dnia 11 marca 2022 r. o obronie ojczyzny – to główny akt normatywny regulujący organizację, zadania i użycie wojska do realizacji zadań niemilitarnych. Artykuł 11 wskazuje, że siły zbrojne mogą brać udział w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działaniach antyterrorystycznych, ochronie mienia, a także w akcjach poszukiwawczo-ratowniczych. Ustawa kładzie duży nacisk na Wojska Obrony Terytorialnej, które mają za zadanie m.in. współdziałanie ze służbami cywilnymi w sytuacjach kryzysowych. Dokument stanowi nadrzędną regulację dotyczącą funkcjonowania SZ RP i wprost odnosi się do wsparcia administracji publicznej. Innym ważnym dokumentem jest Strategia

bezpieczeństwa narodowego RP, która definiuje odporność państwa jako zdolność do ochrony ludności przy współudziale komponentów siłowych.

Zasady udziału SZ RP w działaniach ratowniczych opierają się na zasadzie pomocniczości (subsydiarności). Oznacza to, że wojsko jest angażowane tylko wtedy, gdy użycie innych sił i środków jest niemożliwe lub niewystarczające. Kluczowymi dokumentami regulującymi ten proces są ustawa o stanie klęski żywiołowej z 2002 r. pozwalająca ministrowi obrony narodowej przekazać oddziały do dyspozycji wojewody w celu zapobiegania skutkom katastrof oraz ustawa o zarządzaniu kryzysowym z 2007 r. określająca procedurę użycia wojska, stosownie od ich przygotowania specjalistycznego, na wniosek wojewody i definiująca katalog 15 kluczowych zadań (współudział w monitorowaniu zagrożeń; wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń; wykonywanie zadań poszukiwawczo-ratowniczych; ewakuowanie poszkodowanej ludności i mienia; wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach; współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń; izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej; wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych i zabytkach; prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach SZ RP; usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących na wyposażeniu Sił Zbrojnych Rzeczypospolitej Polskiej; likwidowanie skażeń chemicznych oraz skażeń i zakażeń biologicznych; usuwanie skażeń promieniotwórczych; wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej; współudział w zapewnieniu przejezdności szlaków komunikacyjnych oraz udzielanie pomocy medycznej i wykonywanie zadań sanitarnohigienicznych i przeciwepidemicznych).

Istotne kwestie zawiera także najnowsza Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej. Akt prawny określa zasady organizacji systemu ochrony ludności cywilnej w Polsce oraz reguluje m.in. zadania i obowiązki organów państwa, jednostek samorządu

terytorialnego i podmiotów włączonych w system reagowania kryzysowego, w tym współdziałanie sił zbrojnych i pomocy wojskowej wobec zagrożeń niemilitarnych. Dokument ten integruje zadania ochrony ludności z obroną cywilną w czasie wojny. Zgodnie z nią ochrona ludności to system organów administracji i podmiotów, w tym SZ RP, współpracujących w celu ochrony życia, zdrowia i mienia.

Wojsko nie tylko wspiera logistycznie, lecz także realizuje zadania wymagające specjalistycznych kompetencji. Z tego powodu w strukturach sił zbrojnych za prowadzenie akcji ratowniczych odpowiadają wyspecjalizowane jednostki, m.in. Centralny Ośrodek Analizy Skażeń (CAZ SZ), który pełni funkcję centrum dyspozycyjnego MON w zakresie alarmowania, wykrywania i analizowania skażeń chemicznych, biologicznych i radiacyjnych, będąc częścią Krajowego Systemu Wykrywania Skażeń i Alarmowania. Następnie Wojska Chemiczne i Zespoły CHiRZ – specjalistyczne jednostki przeznaczone do likwidacji skutków awarii chemicznych i radiacyjnych, prowadzące odkażanie terenu oraz transport materiałów niebezpiecznych; Wojska Inżynieryjne, które dysponują batalionami ratownictwa inżynieryjnego uformowanymi po 1997 r. i wykorzystują m.in. transportery pływające oraz mosty do ewakuacji ludności i naprawy wałów przeciwpowodziowych. Zadania z zakresu ratownictwa realizuje jeszcze Wojskowa Ochrona Przeciwpożarowa (WOP), wspierająca swoją działalnością przede wszystkim PSP oraz Wojska Obrony Terytorialnej, które odgrywają specyficzną rolę dzięki lokalnemu charakterowi działania. WOT są zaangażowane we wszystkie fazy zarządzania kryzysowego: od zapobiegania (ocena ryzyka) po odbudowę. Natomiast dowódcy brygad OT są przedstawicielami wojsk w kontakcie z wojewodami w zakresie planowania użycia sił, wsparcia logistycznego czy ratowniczego.

Nowa ustawa o ochronie ludności i obronie cywilnej wprowadza synergię między militarnymi i niemilitarnymi działaniami. Wojsko staje się użytkownikiem Systemu Bezpiecznej Łączności Państwowej (SBŁP), co zapewnia interoperacyjność ze służbami cywilnymi. Co istotne, finasowanie ochrony ludności jest powiązane z budżetem obronnym – 0,15% PKB na ten cel pochodzi z limitu wydatków na potrzeby obronne. W czasie wojny personel ochrony ludności z nadanymi przydziałami mobilizacyjnymi staje

się personelem obrony cywilnej, przy czym obowiązek służby wojskowej ma pierwszeństwo.

Inne kluczowe dokumenty odnoszące się do działalności wojsk w ratownictwie to Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. *w* sprawie szczegółowych zasad udziału pododdziałów SZ RP w zapobieganiu skutkom klęski żywiołowej, w którym doprecyzowano techniczne aspekty współpracy. Ponadto Krajowy Plan Zarządzania Kryzysowego, który jest dokumentem operacyjnym określającym sposób użycia zasobów państwa, w tym wojska, w konkretnych zdarzeniach, oraz doktryny i wytyczne NATO (np. AJP-3.4.9) dotyczące współpracy cywilno-wojskowej (CIMIC), które polskie siły zbrojne implementują w celu zachowania standardów sojuszniczych podczas operacji ratunkowych.

Podsumowując, głównym zadaniem wojskowych systemów ratowniczych jest dbanie o bezpieczeństwo publiczne. Jego istota polega na szybkim, skutecznym i skoordynowanym działaniu, które pozwala minimalizować skutki zdarzeń nadzwyczajnych. Siły Zbrojne RP mogą wspierać działania w czasie klęsk żywiołowych i innych kryzysów, m.in. poprzez wykrywanie zagrożeń, ostrzeganie, akcje przeciwpowodziowe, usuwanie skażeń, gaszenie pożarów, odśnieżanie, oczyszczanie terenów z materiałów wybuchowych, zabezpieczanie obszarów katastrof czy pomoc humanitarną. Efektywność ich działania zależy od kwalifikacji, przygotowania i przeszkolenia żołnierzy w reagowaniu na różne scenariusze. Siły Zbrojne RP ewoluowały z głównego ratownika w okresie PRL do roli specjalistycznego wsparcia opartego na zasadzie subsydiarności w XXI w. Najnowsze przepisy z 2024 r. jeszcze silniej integrują wojsko z cywilnym systemem ochrony ludności: dzięki swoim zasobom i zdolnościom inżynieryjnym i chemicznym pozostaje odwodem państwa gwarantującym bezpieczeństwo obywateli w sytuacjach przekraczających możliwości służb cywilnych. Współpraca wojska i cywilnych służb ratowniczych jest niezbędna, aby ratownictwo mogło skutecznie działać i odpowiadać na współczesne zagrożenia, również hybrydowe.

Żaneta Mrożek

M. Biniak-Pieróg, Z. Zamiar, *Organizacja systemów ratownictwa*, Wydawnictwo Uniwersytetu Przyrodniczego, Wrocław 2013; Krajowy Plan Zarządzania Kryzysowego, https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego (dostęp 22.01.2026); A. Kukuła, *Wojska Obrony Terytorialnej w systemie zarządzania kryzysowego*, „Zeszyty Naukowe Pro Publico Bono" 2024, nr 1(1); B. Michailiuk, *Zasady funkcjonowania systemu wykrywania zagrożeń, ostrzegania, powiadamiania i alarmowania ludności o zagrożeniach*, „Wiedza Obronna" 2025, t. 290, nr 1; Rozporządzenie Rady Ministrów z dnia 23 lutego 2024 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach, Dz.U. 2024, poz. 290; A. Skrabacz, *Ratownictwo w III RP. Ogólna charakterystyka*, AON, Warszawa 2004; A. Skrabacz, M. Domasiewicz, *Numer alarmowy 112. Organizacja i funkcjonowanie systemu powiadamiania ratunkowego w zintegrowanym regionalnie systemie ratowniczym*, ELIPSA, Warszawa 2019; Strategia bezpieczeństwa narodowego RP 2015–2025; Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad udziału pododdziałów SZ RP w zapobieganiu skutkom klęski żywiołowej, Dz.U. 2003, nr 41, poz. 347; T. Szczurek, *Resort obrony narodowej w systemie zarządzania kryzysowego*, „Roczniki Nauk Społecznych" 2023, t. 15(51) nr 2; Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej, Dz.U. 1991, nr 88, poz. 400; Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz.U. 2025, poz. 112; Ustawa z dnia 26 kwietnia 2006 r. o zarządzaniu kryzysowym, Dz.U. 2007, nr 89, poz. 590; Ustawa z dnia 11 marca 2022 r. o obronie ojczyzny, Dz.U. 2022, poz. 655; Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. 2024, poz. 1907; M. Wojciszko, G. Lewandowski, *Współdziałanie (współpraca) Sił Zbrojnych RP z administracją publiczną podczas reagowania obronnego*, „Wiedza Obronna" 2023, t. 284, nr 3.

WSPARCIE PRZEZ PAŃSTWO GOSPODARZA (ang. Host Nation Support, HNS) to w ujęciu NATO zorganizowane wsparcie cywilne i wojskowe, którego tzw. państwo-gospodarz udziela w czasie pokoju, kryzysu oraz wojny sojuszniczym siłom zbrojnym i organizacjom rozmieszczonym na jego terytorium, realizującym tam zadania lub przemieszczającym się przez jego obszar. Udzielanie takiej pomocy odbywa się na podstawie porozumień zawieranych między właściwymi władzami państwa-gospodarza, władzami państw wysyłających a właściwymi organami NATO.

Państwo wysyłające odpowiada za przerzut swoich wojsk, ich zaopatrzenie oraz uzupełnianie potrzebnych zasobów, natomiast na państwie przyjmującym spoczywa odpowiedzialność za organizację transportu

na swoim terytorium, kierowanie ruchem, obsługę techniczną i serwis, magazynowanie, a także zapewnienie dostaw wody, paliwa i żywności. Dodatkowo państwo przyjmujące, w zależności od wymogów operacyjnych, wyznacza obcym wojskom miejsca składowania, rejony stacjonowania bądź obszary odpowiedzialności.

Zgodnie z zapisami *NATO Logistics Handbook* państwo przyjmujące powinno:

- zachować zasadniczą kontrolę nad zasobami przeznaczonymi na HNS, chyba że formalnie zrzeknie się tej kontroli;
- aktywnie uczestniczyć w planowaniu i realizacji działań, aby wsparcie państwa-gospodarza było jak najbardziej skuteczne;
- na bieżąco informować właściwego dowódcę NATO o stanie i przebiegu negocjacji dotyczących HNS;
- ustalać jasne i jednolite standardy kosztów stanowiące podstawę kalkulacji wydatków związanych z HNS;
- w miarę możliwości dostosowywać swoje dwustronne ustalenia i plany w zakresie HNS do wymogów planowania operacyjnego NATO;
- zapewniać odpowiednią współpracę i koordynację między strukturami cywilnymi i wojskowymi, tak aby jak najefektywniej wykorzystywać ograniczone zasoby przeznaczone na wsparcie państwa-gospodarza.

Zagadnienia związane z funkcjonowaniem systemu wsparcia przez państwo-gospodarza są uregulowane zarówno w prawie międzynarodowym, jak i krajowym. W sferze prawa międzynarodowego rozwiązania dotyczące HNS wynikają z ratyfikowanych umów międzynarodowych, które zawierają postanowienia odnoszące się do sił zbrojnych państw-stron, ich żołnierzy oraz personelu cywilnego. Umowy te stanowią podstawę i punkt odniesienia dla dwu- i wielostronnych porozumień przygotowywanych na potrzeby konkretnych operacji NATO.

Podstawy tworzenia warunków do realizacji zadań wsparcia przez państwo-gospodarza wynikają z art. 3 Traktatu Północnoatlantyckiego, który nakłada na każde państwo członkowskie obowiązek utrzymywania i rozwijania własnych zdolności w celu przyjęcia i udzielenia zbiorowej pomocy na wypadek zbrojnej agresji. Miarą sprawności państwa w tym

obszarze jest osiągnięcie interoperacyjności sojuszniczej, rozumianej jako zdolność do skutecznego współdziałania z sojusznikami dzięki znajomości, implementacji i stosowaniu dorobku prawnego oraz doktrynalnego NATO. Oznacza to również konieczność właściwego zorganizowania i ciągłego doskonalenia narodowego systemu wsparcia poprzez wyznaczenie adekwatnych sił i środków, określenie relacji między nimi, nadanie im spójnych kierunków działania oraz skoordynowanie przedsięwzięć administracji publicznej z aktywnością sił zbrojnych. Dodatkowo istotne znaczenie ma umowa między państwami-stronami Traktatu Północnoatlantyckiego, dotycząca statusu ich sił zbrojnych, sporządzona w Londynie 19 czerwca 1951 r. (znana również jako NATO SOFA), która zawiera postanowienia dotyczące m.in. warunków i wymagań wobec sił zbrojnych państwa wysyłającego lub znajdujących się na terytorium państwa przyjmującego objętego obszarem Traktatu Północnoatlantyckiego, członków sił zbrojnych i personelu cywilnego oraz kompetencji i zasad postępowania organów wojskowych państwa wysyłającego i organów państwa przyjmującego.

Dokumentami, które mają zastosowanie w funkcjonowaniu systemu HNS, są doktryny sojusznicze określające procedury w zakresie przygotowania i realizacji HNS, np.

- Allied Joint Logistic Doctrine AJP-4(A);
- Allied Joint Doctrine for Host Nation Support AJP-4.5(B);
- Allied Joint Movement and Transportation Doctrine (AJP-4.4).

W dokumentach tych odniesiono się do sposobu określenia struktury organizacyjnej realizującej HNS, procedur zawierania porozumień i sposobu zapewnienia efektywnego wsparcia siłom zbrojnym NATO.

Dokumentem stosowanym przy realizacji i rozliczaniu HNS w ramach NATO jest porozumienie standaryzacyjne STANAG 2034 – Standard Procedures for Mutual Logistic Assistance (tzw. standardowe procedury wzajemnego wsparcia logistycznego w NATO). Wprowadza ono procedury udzielania oraz rozliczania wzajemnego wsparcia logistycznego w sytuacji, gdy siły zbrojne państwa NATO udzielają wsparcia logistycznego siłom zbrojnym innego państwa NATO, dowództwom lub formacjom wielonarodowym w czasie pokoju, kryzysu i wojny.

Ponadto dokumentami mającymi zastosowanie w określaniu wytycznych wsparcia cywilnego dla sił zbrojnych, w tym HNS, są m.in.

- Zobowiązanie do wzmocnienia odporności (ang. *Commitment to enhance resilience*) – przyjęte przez szefów państw i rządów na szczycie NATO w Warszawie w 2016 r.;
- Wytyczne do podnoszenia odporności, zaakceptowane przez ministrów obrony NATO w czerwcu 2016 r.;
- Wspólny komunikat do Parlamentu Europejskiego i Rady dotyczący Planu działania na rzecz mobilności wojskowej z 28 marca 2018 r. (ang. *Joint communication to the European Parliament and the Council on the Action Plan on Military Mobility*).

Współpraca pomiędzy NATO a Unią Europejską w tym zakresie jest rozwijana na podstawie Wspólnej deklaracji Przewodniczącego Rady Europejskiej, Przewodniczącego Komisji Europejskiej oraz Sekretarza Generalnego z dnia 8 lipca 2016 r.

Podstawą prawną w prawie polskim są przede wszystkim: Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Ustawa z dnia 11 marca 2022 r. o obronie ojczyzny (Dz.U. 2022, poz. 655), Ustawa z 17 grudnia 1998 r. o zasadach użycia lub pobytu Sił Zbrojnych Rzeczypospolitej Polskiej poza granicami państwa (Dz.U. 2021, poz. 396) oraz Ustawa z 23 września 1999 r. o zasadach pobytu wojsk obcych na terytorium Rzeczypospolitej Polskiej oraz zasadach ich przemieszczania się przez to terytorium (Dz.U. 2023, poz. 807).

W art. 23a Ustawy z 23 września 1999 r. o zasadach pobytu wojsk obcych na terytorium Rzeczypospolitej Polskiej oraz zasadach ich przemieszczania się przez to terytorium czytamy, że „wsparcie przez państwo -gospodarza, zwane dalej „HNS", jest realizowane w oparciu o priorytety obronne oraz rzeczywiste możliwości Rzeczypospolitej Polskiej i obejmuje:

1. Dostawy środków materiałowych i technicznych.
2. Dostęp do infrastruktury i urządzeń.
3. Dostarczanie usług, włączając ochronę rejonu działań.
4. Wsparcie administracyjne i prawne.
5. Inne świadczenia możliwe do zabezpieczenia przez państwo-gospodarza. Dodatkowo „HNS realizowane jest odpłatnie, bezpłatnie lub na zasadzie wzajemności, zgodnie z ustaleniami wynikającymi

> z międzynarodowych porozumień HNS […]. Finansowanie i rozliczanie HNS następuje na zasadach określonych w art. 137 Ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2024, poz. 1530 i 1572)".

Koordynację całokształtu przedsięwzięć wynikających z obowiązków państwa-gospodarza, zarówno w wymiarze narodowym, jak i sojuszniczym, sprawuje minister obrony narodowej poprzez pełnomocnika do spraw HNS, który jednocześnie pełni funkcję Centralnego Punktu Kontaktowego HNS współdziałającego z komórkami i jednostkami organizacyjnymi Ministerstwa Obrony Narodowej oraz, za pośrednictwem Departamentu Strategii i Planowania Obronnego w Ministerstwie Obrony Narodowej, z punktami kontaktowymi pozamilitarnych struktur obronnych państwa.

W celu dokonania nowelizacji zasad funkcjonowania HNS w Polsce w lutym 2018 r. powołany został – pod przewodnictwem pełnomocnika ministra obrony narodowej ds. HNS (szef zarządu logistyki – P4 SG WP) – międzyresortowy zespół do opracowania koncepcji funkcjonowania narodowego systemu wsparcia przez państwo-gospodarza (HNS). W jego skład weszli przedstawiciele jednostek i komórek organizacyjnych kompetentnych ministerstw i agend rządowych, w tym również Rządowego Centrum Bezpieczeństwa. Zadaniem Zespołu było przygotowanie koncepcji działania krajowego systemu HNS, obejmującej zarówno sferę militarną, jak i niemilitarną.

Działania służące udzielaniu wsparcia w ramach obowiązków państwa-gospodarza zostały zaliczone do zadań obronnych Rzeczypospolitej Polskiej. W konsekwencji obejmują cały system obronny państwa – wszystkie jego struktury, a także poszczególne szczeble władzy i administracji publicznej oraz podmioty gospodarcze.

W dokumentach NATO HNS traktowane jest jako jeden z kluczowych „obszarów powiązanych z logistyką", obok wsparcia medycznego, inżynieryjnego, budżetowo-finansowego, współpracy cywilno-wojskowej czy wsparcia kontraktowego, co podkreśla jego przekrojowy charakter i konieczność ścisłej koordynacji z innymi funkcjami logistycznymi.

Agnieszka Warchoł

Koncepcja funkcjonowania narodowego systemu wsparcia przez państwo-gospodarza HNS obejmująca podsystem militarny i niemilitarny, Ministerstwo Obrony Narodowej, Warszawa 2018; A. Miler, *Organizacja Host Nation Support*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2010, nr 1(180); S. Łazarek, *Polska jako Państwo-Gospodarz w ramach Systemu HNS*, https://archiwum.rcb.gov.pl/polska-jako-panstwo-gospodarz-w-ramach-systemu-hns/ (dostęp 11.12.2025); *NATO Logistics Handbook*, https://www.forsvaret.no/en/organisation/nduc/nodefic/pre-study-packages/NATO%201.06%20-%20Vedlegg%20NATO%20Logistics%20Handbook%20(2012).pdf/_/attachment/inline/0e1ab045-8c67-4c02-8139-91ff98bbaa6c:25b16a41b2bdacd1dd5c47c0f37b754d2f70e7dc/NATO%201.06%20-%20Vedlegg%20NATO%20Logistics%20Handbook%20(2012).pdf (dostęp 28.11.2025); Ustawa z 23 września 1999 r. o zasadach pobytu wojsk obcych na terytorium Rzeczypospolitej Polskiej oraz zasadach ich przemieszczania się przez to terytorium, Dz.U. 1999, nr 93, poz. 1063; *Zasady HNS*, https://hns-polska.wp.mil.pl/o-nas-2017-01-16-r/zadania-2017-01-16-4/zasady-hns/ (dostęp 28.11.2025).

WYCHOWANIE NARODOWE – wszelkie koncepcje wychowawcze opierające się na określonych wzorcach i ideach przewodnich konstytuujących ich kształt, m.in. patriotyzmie, który legł u podstaw koncepcji wychowania narodowego na progu odzyskania przez Polskę niepodległości. Patriotyczne pragnienie zjednoczenia ziem polskich okupowanych przez zaborców przerodziło się w więź, bez której faktyczna jedność społeczna oraz państwowa i działanie na rzecz wspólnego interesu nie byłyby możliwe. Tego typu więzi i postawy mają jednak jeszcze jedno istotne znaczenie – uszlachetniające człowieka oraz hierarchizujące jego wartości (chociażby wyższość altruizmu ponad egoizmem). Paradoksalnie jednak egoizm może być elementem, który w sposób pozytywny będzie oddziaływał na jednoczące się społeczeństwo, jednakże musi to być egoizm narodowy, a więc postawa służąca potęgowaniu narodowej indywidualności w ramach wspólnoty i działalności na jej rzecz. Można to było osiągnąć poprzez wyzwolenie narodowego ducha jednostki i narodu będącego warunkiem przezwyciężenia narodowej bierności i skłaniania się ku wzrostowi twórczych sił w podzielonym zaborami społeczeństwie. Taki zamiar miała ówczesna, przedwojenna myśl polityczno-pedagogiczna, której głównymi wyrazicielami byli Stanisław

Prus-Szczepanowski, Zygmunt Balicki, Roman Dmowski i Lucjan Zarzecki – teoretycy koncepcji wychowania narodowego.

Jeśli chodzi o Prusa-Szczepanowskiego, to swój ideał „obywatela-bohatera" opierał na połączeniu podejścia tradycjonalistycznego z realistycznym; czerpał idee z przywiązania do tradycji narodowych, swoistego kultu polskiego narodu, jednakże zauważał też pewne ułomności natury ekonomicznej, które doprowadziły do niepowodzeń narodowych Polski i Polaków. Koncepcja wychowania narodowego Prusa-Szczepanowskiego była wynikiem praktycznego oraz interdyscyplinarnego podejścia do zagadnienia „odrodzenia narodowego", które to miało być możliwe poprzez szeroką działalność oświatową i społeczno-ekonomiczną. Myślicielowi bliskie było szczególnie pozytywistyczne podejście do kwestii wychowania narodowego – wzorem umysłowego. Jego zdaniem w tej materii należało dążyć do, po pierwsze, uznania doświadczenia życiowego człowieka i formy samokształcenia za podstawy tzw. „autodyktatyzmu" będącego warunkiem wszelkiego kształcenia; po drugie, kształtowania postaw obywatelskich, edukacyjnych i wychowawczych zbieżnych z linią prezentowaną przez ustrój polityczny całego państwa; po trzecie, zapewnienia przede wszystkim kształcenia dla warstw produkujących i zarabiających, a nie spożywających i egzystujących na „państwowym garnuszku"; po czwarte, kształcenia głównie w kierunkach matematyczno-przyrodniczych. Prusa-Szczepanowskiego zaliczano do postępowego nurtu pedagogiki narodowej w Polsce; postawa ta wynikała głównie z faktu jego inżynierskiego wykształcenia i braku zawodowej styczności z zagadnieniami czysto pedagogicznymi.

Balicki, nazwany przez Bogumiła Grotta „szermierzem pedagogiki narodowej", odniósł się do kwestii wychowawczych po raz pierwszy w tak doniosły sposób na Polskim Kongresie Pedagogicznym we Lwowie, który odbył się 1 listopada 1909 r. Wygłosił tam referat pt. *Zasady wychowania narodowego*, opublikowany również na łamach „Przeglądu Narodowego". Balicki wypowiedział tam następujące słowa: „Wychowanie narodowe wymaga od jednostki innego stosunku do ojczyzny niż jako do czegoś, co na zewnątrz duszy naszej istnieje, przy całem pragnieniu dobra tej ojczyzny i potępianiu wszystkiego, co w nią godzi".

W innym, wydanym w 1902 r. sztandarowym dziele Balicki pisze: „Altruizm wobec swego narodu i przejęcie się jego egoizmem składają się łącznie na uczucie patriotyzmu". Rozróżnienie egoizmu jednostkowego i narodowego jest kluczowe dla zrozumienia idei przyświecającej obowiązkowi patriotycznemu u Balickiego i jego koncepcji wychowania narodowego. To ostatnie powinno bowiem przejawiać się na różnych płaszczyznach narodowego życia i być odzwierciedleniem nieustannej walki o dobro własnego narodu i państwa. Słowa Balickiego trafnie oddają specyfikę dbałości o interes narodowy w duchu wspomnianego egoizmu narodowego: „Nie zadowalając się współudziałem w walkach o niepodległość obcych narodów, zapragnęliśmy mieszać się do ich wewnętrznych ruchów rewolucyjnych, w imię altruistycznej walki o wolność innych, jak gdybyśmy u siebie w domu nie potrzebowali wszystkich sił, aby ochronę własnej wolności należycie przygotować". Balicki postulował kształtowanie wśród najmłodszych pokoleń postaw wzmacniających poczucie własnej godności i tożsamości narodowej. Miały one być przede wszystkim aktywnym, czynnym owocem patriotycznych przekonań i wartości. Balicki stanowczo odrzucał ideę patriotyzmu biernego, nieprzebijającego się przez trudy życia codziennego; jego ideałem było wcielanie w życie idei wychowania narodowego uskuteczniającej koncepcję „człowieka działającego w zespole z myślą o jego celach zbiorowych, umiejącego funkcjonować ofiarnie w strukturach poddanych rygorom hierarchii i poczucia obowiązku". Obowiązkiem objęte miało być także kształcenie w zakresie historii, geografii, języka ojczystego i literatury służące formowaniu się „narodowego ducha" i przeciwstawiające się relatywizowaniu wartości. Ukształtowany na tych fundamentach człowiek miał być (emocjonalnie, intelektualnie i wolicjonalnie), zdaniem Balickiego, odzwierciedleniem modelu wychowawczego „żołnierza-obywatela", któremu przyświecał postulat twórczości. Balicki wyraźnie odróżniał proces edukacji od wychowania – jego zdaniem w tym ostatnim powinno górować przeżywanie dziejów narodu, poznawanie kraju, odczuwanie wspólnoty językowej, a nie nauka poprzez przyswajanie „suchej" wiedzy i faktów; w ten sposób miało odbywać się w koncepcji wychowania narodowego Balickiego kształtowanie charakteru narodowego. Pisał on bowiem: „Być kimś – sprowadza się we wszystkich dziedzinach życia do jednego: mieć charakter".

Dmowski, choć główna część jego pisarstwa i publicystyki opierała się na wątkach bardziej politycznych, społecznych i kulturowych niż pedagogicznych, w sposób mniej lub bardziej pośredni odwoływał się do kategorii wychowawczej i edukacyjnej przełomu XIX i XX w. Czynił to w szerokim kontekście „bierności powszechnej" polskiego społeczeństwa, której przyczyn dopatrywał się m.in. w szlacheckim charakterze narodu ukształtowanego na gruzach polskiej państwowości w czasie zaborów. Katarzyna Wrzesińska zauważa, że w momencie, w którym Rzeczpospolita utraciła swą niepodległość, zastopowaniu uległ rozwój społeczno-ekonomiczny kraju. W sytuacji nikłego znaczenia polskiego mieszczaństwa oraz biednej i zacofanej warstwy chłopskiej to właśnie szlachta (od której wzorce zachowania i postawy czerpało społeczeństwo) stanowiła warstwę dominującą, krzewiącą w narodzie nieobowiązkowość, zastój i wspomnianą bierność. W kontekście swoistego kultu czynu i aktywizacji Dmowski pisał w *Myślach nowoczesnego Polaka*: „Nienawidzę nauczycieli, którzy, mając z powołania swego obowiązek uczyć i wychowywać młodzież, znęcają się nad nią, zabijając jej siły fizyczne w zarodku, znieprawiają ją moralnie, powstrzymują lub wypaczają jej rozwój umysłowy". Zatem dla Dmowskiego kwestia „emancypacji" narodowego pierwiastka ponad bierne jego otoczenie, ułożenie moralne czyniące człowieka godnym następcą minionych pokoleń oraz rozwój umysłowy urosły do rangi czynnika decydującego również o sile charakteru to nieodzowne elementy wychowania narodowego, których pielęgnacja doprowadzić miała do ukształtowania ideału człowieka zdolnego, zdaniem Dmowskiego, do bezwzględnej walki o swe prawa. Franciszek Filipowicz pisze: „Dmowski wskazywał na konieczność kształtowania od najmłodszych lat takich cech, jak odwaga do samodzielnego życia, zdolność do podejmowania inicjatyw, do szukania lepszych perspektyw […]. Winą za wzrastanie kolejnego pokolenia «niedołęgów» [Dmowski – przyp. PŁ] nie obarcza szkół, podlegających polityce zaborców, a samo społeczeństwo polskie, które przez lata po tragedii powstania styczniowego nie potrafiło znaleźć własnych dróg kształtowania młodych charakterów i umysłów". Co ciekawe i warte odnotowania, Dmowski uważał, że nadmierny wpływ matki lub ojca na wychowanie dzieci może być (za sprawą nadopiekuńczości i niedostosowania młodego człowieka do wykonywania obowiązków oraz samoobrony przed zagrożeniami wynikającymi z kolei dorosłego życia)

szkodliwy dla ich psychiki i zachowania. Konsekwencją miała być niezaradność życiowa, brak zdolności do samodzielnego i odpowiedzialnego podejmowania decyzji, ustępliwość oraz strach przed rzeczywistością. A jest to jedna z kluczowych spraw dla wychowania narodowego, co potwierdzają słowa samego Dmowskiego: „Przyszła Polska […] będzie taka, jak wychowacie wasze dzieci".

Przedstawione postulaty i koncepcje teoretyków wychowania narodowego miały nieco odmienny charakter niż koncepcja pedagogiki narodowej i wychowania narodowego Zarzeckiego. Wspomniana odmienność wynikała z co najmniej 2 powodów: po pierwsze – żaden z wymienionych teoretyków (poza Zarzeckim) nie był z wykształcenia pedagogiem, a po drugie – wspomniana „trójka" dała pewne podstawy do ukonstytuowania się koncepcji Zarzeckiego, którego to określa się mianem głównego teoretyka wychowania narodowego, choć w pełni niedocenionego. Zarzecki, biorąc pod uwagę zasygnalizowane już ujęcia wychowania narodowego, zmodyfikował je, a jego ideał opierał się na modelu „robotnika-obywatela", człowieka, który odznaczał się silną wolą w dążeniu do celu i w całości poświęcał się własnej ojczyźnie. Kluczową kwestią myśli pedagogicznej Zarzeckiego jest refleksja nad aksjologicznym wymiarem wychowania narodowego i jego składowych, biorąc pod uwagę wartości zawierające się w owej koncepcji.

Praca, samowychowanie i wartości moralne będące osobowościowym wątkiem wychowania narodowego należy traktować łącznie, zwłaszcza że poza oczywistym walorem tożsamościowym i w pewnym sensie „emancypacyjnym" (wychodzenie narodu spod terytorialnej okupacji) stanowią one wykładnię narodowej koncepcji wychowania. Na osobowość składa się bowiem wiele czynników oddziałujących na człowieka na zewnątrz (praca na rzecz wspólnoty, a nie w ściśle indywidualnym tonie), od wewnątrz (potrzeba samokształcenia i samowychowania podstawą kształtowania świadomości) i w sensie uniwersalnym (wartości moralne). Tego typu zestawienie w ramach osobowości ludzkiej proponował także Zarzecki.

Jeśli chodzi o wartość pracy, a właściwie – pracowitości, to należy zaznaczyć, iż wyraża się ona w dokładności i staranności wykonania oraz systematyczności i wytrwałości w realizacji wytyczonych celów. Priorytetem wychowania narodowego jest kształcenie charakteru w kierunku otwarcia na dobro wspólnoty narodowej i przedsięwzięcie wszelkich czynności na rzecz

budowy silnej struktury społecznej i państwowej – także (a właściwie przede wszystkim) w sensie aksjologicznym. Praca w tym kontekście stanowi cenne źródło ludzkiej egzystencji (materialny aspekt pracy decydujący o poziomie stopy życiowej jednostki), współdziałania w ramach grup i większych zbiorowości (socjologiczny aspekt pracy) oraz rozwoju moralnego człowieka (realizacja i rozwój w duchu wartości moralnych).

W świetle badań okazuje się, że wysoki wskaźnik pracowitości osiąga się poprzez oddziaływanie międzypokoleniowe w podstawowej komórce wychowawczej (również w narodowej koncepcji), jaką jest rodzina. Sabina Bartel podaje, że wysoka pracowitość wynika m.in. z ścisłej współpracy na polu edukacyjno-wychowawczym zarówno ojca, jak i matki, w słowach i czynach których przejawia się model pracowitości stanowiący wzór dla dziecka; łącznego oddziaływania na dziecko systemu nagród i kar oraz argumentacji uzasadniającej wybór określonej wartości; przewagi nagród nad karami w procesie wychowawczym. Pisząc o pracy i pracowitości, autor ma na myśli ich różnorodny wymiar i charakter. Samowychowanie, które w literaturze przedmiotu często jest wartością pomijaną, odgrywa kluczową rolę w uświadamianiu sobie przez wychowanków wyników procesów wychowawczych decydujących o ich rozwoju (Zarzecki użyłby zapewne sformułowania „samowiedza").

Władysław Cichoń pisze, iż „niezbędną podstawą takich procesów samowychowawczych staje się wówczas akceptacja określonych zespołów wartości, które kształtują cel i ideał tak rozumianej autoedukacji. Samowychowanie jest zawsze samokształtowaniem, formowaniem własnego «aksjologicznego wnętrza», a przede wszystkim swego osobowego «ja»". Istotne jest także to, aby swój system wartości budować w oparciu o powszechnie uznany model wartości moralnych jako najbliższych naturalnej i teologicznej sferze godności ludzkiej. Porządek, zgodność czynów ze słowami i właśnie jakość ludzkiego współżycia we wspólnocie stanowią o randze wartości moralnych w kształtowaniu własnego „ja". Często podstawą etyczno-moralną w procesie wychowawczym staje się religia, którą teoretyk wychowania narodowego Zarzecki pragnął uczynić źródłem „zasad i norm moralnych".

Paweł Łubiński

Z. Balicki, *Egoizm narodowy – katechizm nacjonalisty* [fragment dzieła *Egoizm narodowy wobec etyki*, Lwów 1902], [w:] *Dusza społeczeństwa. Naród w polskiej myśli socjologicznej. Wybór tekstów*, J. Kurczewska (red.), Narodowe Centrum Kultury, Warszawa 2002; Z. Balicki, *Zasady wychowania narodowego*, „Przegląd Narodowy" 1909, nr 10; S. Bartel, *Pracowitość jako wartość w procesie edukacji w rodzinie*, [w:] *Świat wartości i wychowanie*, W. Szewczuk (red.), Wydawnictwo Fundacja Innowacja, Warszawa 1996; W. Cichoń, *Wartości – człowiek – wychowanie. Zarys problematyki aksjologiczno-wychowawczej*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 1996; D. Drynda, *Zarzecki Lucjan*, [w:] *Słownik pedagogów polskich*, W. Bobrowska-Nowak, D. Drynda (red.), Wydawnictwo Uniwersytetu Śląskiego, Katowice 1998; F. Filipowicz, *Myśl pedagogiczna Lucjana Zarzeckiego (1873–1925)*, Wydawnictwo Polskiej Akademii Nauk, Zakład Narodowy im. Ossolińskich, Wrocław–Warszawa–Kraków–Gdańsk 1974; B. Gawlina, *Potrzeba przemiany polskiego patriotyzmu*, [w:] *Świat wartości i wychowanie*, W. Szewczuk (red.), Wydawnictwo Fundacja Innowacja, Warszawa 1996; B. Grott, *Zygmunt Balicki ideolog Narodowej Demokracji*, Wydawnictwo Arcana, Kraków 1995; J. Kurczewska, *Zygmunt Balicki (1858–1916)*, [w:] *Dusza społeczeństwa. Naród w polskiej myśli socjologicznej. Wybór tekstów*, J. Kurczewska (red.), Narodowe Centrum Kultury, Warszawa 2002; J. Legowicz, *Intelektualizm tyczny i moralność*, [w:] *Świat wartości i wychowanie*, W. Szewczuk (red.), Wydawnictwo Fundacja Innowacja, Warszawa 1996; P. Łubiński, *Naród, nacjonalizm i ruch narodowy z perspektywy politologicznej*, Akademia Wychowania Fizycznego im. J. Kukuczki, Katowice 2018; M. Wójcik, *Szczepanowski-Prus Stanisław*, [w:] *Słownik pedagogów polskich*, W. Bobrowska-Nowak, D. Drynda (red.), Wydawnictwo Uniwersytetu Śląskiego, Katowice 1988; K. Wrzesińska, *Kultura i cywilizacja w myśli Narodowej Demokracji (1893–1918)*, Slawistyczny Ośrodek Wydawniczy, Warszawa 2012.

WYTŁUMACZALNOŚĆ (także „wyjaśnialność", ang. *explainability*) – zasada projektowania, rozwoju i wdrażania systemów sztucznej inteligencji (SI), której celem jest zapewnienie, że decyzje, działania lub wyniki tych systemów będą zrozumiałe dla użytkowników, a przesłanki wykorzystywane w procesie decyzyjnym – możliwe do wytłumaczenia. Często określana mianem „interpretowalności" (ang. *interoperability*) i łączona z pojęciem transparentności, choć nie zawsze te terminy są stosowane zamiennie. Katarzyna Filus (2023) wskazuje chociażby, iż „wyjaśnialność skupia się na zrozumiałych rezultatach metod, a interpretowalność – na rozumieniu modeli i ich procesu uzyskiwania rezultatów". Samą zasadę

wytłumaczalności, a często także systemy odznaczające się wytłumaczalnością, oznacza się akronimem xAI (ang. *explainable artificial intelligence*).

Jak wskazuje Mario González-Arencibia wraz z zespołem (2024), termin *explainability* został wprowadzony przez amerykańską Defense Advanced Research Projects Agency (DARPA) w 2016 r. i odnosił się wówczas przede wszystkim do militarnych zastosowań SI. Współcześnie jest postrzegany jako jedna z podstawowych zasad etycznych, a coraz częściej kodyfikowanych zasad prawnych w obszarze systemów SI.

Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji powołana przez Komisję Europejską wyróżniła wytłumaczalność jako jeden z wymogów projektowania systemów SI już w *Wytycznych w zakresie etyki dotyczącej godnej zaufania sztucznej inteligencji* z 2019 r. Następnie koncepcję rozwijano i dostosowywano do rosnących możliwości i skomplikowania technologii. W dokumencie z 2019 r. wskazano, iż „możliwość wyjaśnienia ma kluczowe znaczenie dla budowania i utrzymania zaufania użytkowników do systemów SI. Zasada ta oznacza, że procesy muszą być przejrzyste, możliwości i cele systemów SI – otwarcie komunikowane, a decyzje – w jak największym stopniu możliwe do wyjaśnienia osobom, na które mają one bezpośredni i pośredni wpływ".

Eksperci National Institute of Standards and Technology (NIST) pod kierunkiem Jonathona Phillipsa (2021) wymieniają 4 podzasady, które składają się na wytłumaczalność: wyjaśnienia (dowód lub uzasadnienie wyniku), znaczenia (wyjaśnienia są zrozumiałe dla docelowego odbiorcy), dokładności (wyjaśnienie prawidłowo odzwierciedla powód decyzji), ograniczenia wiedzy (system działa w warunkach, do których został zaprojektowany).

Wytłumaczalność odnosi się zatem zarówno do technicznej przejrzystości systemów SI, jak i ich zdolności do dostarczania zrozumiałych dla człowieka powodów swoich zachowań (w jaki sposób dane wejściowe są przekształcane w wyjściowe generowane przez system). W tym pierwszym aspekcie nacisk kładziony jest na interpretowalność funkcjonowania algorytmu i ma charakter techniczny, w drugim – na przyczyny podjętej decyzji i możliwość jej przekazania w formie zrozumiałej dla osób będących przedmiotem decyzji, co ma charakter semantyczny i logiczny. Ma to szczególne znaczenie w dziedzinach, w których błędne kalkulacje

mogą istotnie wpłynąć na rozstrzygnięcia administracyjne lub prawne (np. przyznawanie świadczeń, opieka zdrowotna, wyroki sądowe, udzielanie kredytów) bądź bezpieczeństwo (np. wykorzystanie SI w wojskowości i nadzór nad systemami odznaczającymi się wysokim poziomem autonomiczności). Unijna Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji podkreśliła (2019), iż wytłumaczenie powinno być każdorazowo dostosowane do poziomu wiedzy odbiorcy – przekazane w odpowiedniej, zrozumiałej i uproszczonej formie.

Wraz z rozwojem technologii wytłumaczalność nabrała znaczenia jako jedna z podstawowych zasad projektowania systemów SI, zwłaszcza złożonych i imitujących procesy wnioskowania charakterystyczne dla ludzi (np. oparte na głębokich sieciach neuronowych). Ze względu na skomplikowanie architektury systemów SI i trudności w analizie ich wnioskowań zachodzące wewnątrz systemów procesy są często określane mianem „czarnej skrzynki", a wręcz opisywane jako „niewytłumaczalne". Odznaczają się bowiem brakiem przejrzystości, przez co często nie są w pełni zrozumiałe nawet dla ich twórców.

Problem „czarnej skrzynki" stwarza zatem wiele wyzwań:

1. Brak możliwości ustalenia odpowiedzialności – jeśli nikt nie potrafi wyjaśnić, w jaki sposób system dochodzi do swoich wniosków, kwestionowanie jego decyzji lub przypisanie odpowiedzialności za szkodę staje się utrudnione lub wręcz niemożliwe.
2. Przeniesienie odpowiedzialności – wykorzystywanie systemów SI może w dorozumiany sposób zwalniać z odpowiedzialności człowieka nadzorującego wydanie decyzji i osłabiać mechanizmy kontroli następczej.
3. Ryzyko stronniczości i dyskryminacji – bez możliwości wglądu w wewnętrzne mechanizmy stojące za procesem decyzyjnym trudno jest wykryć, czy system kieruje się obiektywizmem i bierze pod uwagę wszystkie czynniki, czy też powiela lub wzmacnia szkodliwe uprzedzenia wynikające z błędnych lub niepełnych danych treningowych.
4. Wtórna dyskryminacja – stronniczość systemu SI może przyczyniać się do wykształcenia postaw dyskryminacyjnych wśród nadzorujących system ludzi.

5. Powielanie błędów – brak możliwości wytłumaczenia decyzji może skutkować osłabieniem autokontroli, brakiem weryfikacji poprawności procesu i jego automatycznym powielaniem przy kolejnych rozstrzygnięciach.
6. Erozja zaufania – osoby, na które wpływają decyzje SI (np. ubiegające się o pożyczkę, poszukujące pracy, pacjenci), mogą odrzucać lub kwestionować wyniki, szczególnie rozstrzygnięcia niekorzystne, których nie rozumieją lub które nie zostały im odpowiednio wytłumaczone, co prowadzi do spadku zaufania do instytucji.
7. Problem regulacyjny – ze względu na stopień skomplikowania algorytmów i brak odpowiedniej kontroli nad przebiegiem procesów decyzyjnych organy regulacyjne mogą mieć istotny problem z odpowiednim formułowaniem przepisów i procedur sprawdzających, a następnie z egzekwowalnością założeń wytłumaczalności w praktyce.
8. Utrudniona kontrola – organy nadzoru mogą mieć trudności z oceną zgodności z przepisami i standardami, gdy wyniki systemu nie mogą być w pełni zweryfikowane.
9. Zagrożenie dla bezpieczeństwa – brak zrozumienia funkcjonowania złożonych systemów SI utrudnia kontrolę nad ich rozwojem, w tym poziomem autonomiczności, jak również monitorowanie niewłaściwego funkcjonowania systemów odpowiedzialnych za (cyber)bezpieczeństwo.

Architekci systemów SI pracują nad różnymi technikami, które mają złagodzić efekt „czarnej skrzynki" i zwiększyć transparentność systemów SI. Jednocześnie, jak argumentuje González-Arencibia (2024), istotne jest wyważenie proporcji „między wyjaśnialnością a innymi wartościami, takimi jak wydajność czy prywatność", przez co niektórzy postulują bardziej elastyczne podejście. Nadmierne skoncentrowanie na wytłumaczalności może bowiem skutkować obniżeniem dokładności lub skuteczności rozwiązań. W literaturze wskazuje się również na wykorzystywanie systemów SI, które umożliwiają interpretowalność, jak drzewa decyzyjne, regresja liniowa czy metody wizualizacyjne. Mają one sprzyjać budowaniu systemów, których procesy określane są jako „biała skrzynka".

Odnotować należy również podejście *post hoc*, którego założeniem jest przedstawianie wyjaśnień dla podjętej decyzji w oparciu o analizę „cech lub zmiennych mających największy wpływ na proces decyzyjny modelu" bądź też „zachowania modelu w konkretnym przypadku" (Bernardo 2023).

Znaczenie wytłumaczalności ewoluowało równolegle z wysiłkami na rzecz opracowania ram etycznych i prawnych dla SI. Wczesne dokumenty, takie jak zbiory zasad dotyczące SI wydane przez OECD, G20, G7 czy wspomniane wytyczne UE, konsekwentnie podkreślały znaczenie transparentności i wytłumaczalności jako jednych z podstawowych zabezpieczeń systemów SI.

Po przyjęciu przez UE Aktu w sprawie sztucznej inteligencji, tzw. AI Act (2024), wytłumaczalność stała się unijnym wymogiem prawnym. Rozporządzenie wprowadza kategoryzację systemów SI i nakłada zróżnicowane obowiązki na ich twórców obejmujące m.in. konieczność prowadzenia dokumentacji umożliwiającej interpretowalność i przejrzystość. AI Act promuje wyjaśnialność jako jedną z kluczowych zasad sztucznej inteligencji godnej zaufania, posługując się nawet terminem „prawo do uzyskania wyjaśnienia". W art. 86 pkt 1 stwierdza wprost: „Każda osoba, na którą SI ma wpływ, będąca przedmiotem decyzji podjętej przez podmiot stosujący […], która to decyzja wywołuje skutki prawne lub w podobny sposób oddziałuje na tę osobę na tyle znacząco, że uważa ona, iż ma to niepożądany wpływ na jej zdrowie, bezpieczeństwo lub prawa podstawowe, ma prawo uzyskania od podmiotu stosującego jasnego i merytorycznego wyjaśnienia roli tego systemu SI w procedurze podejmowania decyzji oraz głównych elementów podjętej decyzji".

Wraz z dynamicznym rozwojem technologii SI wytłumaczalność powinna być postrzegana nie tylko jako cel techniczny, ale przede wszystkim filar odpowiedzialności twórców systemów SI; jest bowiem ściśle powiązana z prawami jednostki, sprawiedliwością proceduralną, nadzorem instytucjonalnym i wielowymiarowym bezpieczeństwem nowoczesnych systemów i ich stosowania. Wytłumaczalność staje się zatem kluczowym elementem odpowiedzialnego i wiarygodnego wdrażania technologii.

Mateusz Łabuz

V. Bernardo, *Explainable Artificial Intelligence*, Technology and Privacy Unit of the European Data Protection Supervisor, Bruksela 2023; K. Filus, *Wyjaśnialność i bezpieczeństwo systemów inteligentnych*, Instytut Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk, Gliwice 2023; B. Fischer, M. Sakowska-Baryła, *Wykorzystywanie otwartych danych… jako element zwiększenia wyjaśnialności AI*, „Prawo i Więź" 2024, nr 6(53); M. González-Arencibia, *Explainable Artificial Intelligence as an Ethical Principle*, „Ingenieria" 2024, no. 29(2); P. Kaźmierczyk, *Biała księga AI w praktyce klinicznej*, wZdrowiu, Warszawa 2022; I. Lipińska, *Etyka sztucznej inteligencji w dokumentach Unii Europejskiej w latach 2017–2020*, „Edukacja Filozoficzna" 2022, nr 73; D. Lubasz, *Przejrzystość i wyjaśnialność sztucznej inteligencji i ich funkcje w RODO i AI Act*, „Monitor Prawniczy" 2024, nr 11; J. Phillips, *Four Principles of Explainable Artificial Intelligence*, National Institute of Standards and Technology, Gaithersburg 2021; N. Smuha, *Wytyczne w zakresie etyki dotyczącej godnej zaufania sztucznej inteligencji*, Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, Bruksela 2019; D. Szostek, *Wyzwania i zagrożenia z zakresu cyberbezpieczeństwa podczas projektowania lub wykorzystywania AI*, [w:] *Cyberbezpieczeństwo AI. AI w cyberbezpieczeństwie*, NASK, Warszawa 2023.

WZMOCNIONA WYSUNIĘTA OBECNOŚĆ (ang. *enhanced Forward Presence*, eFP) – inicjatywa państw Sojuszu Północnoatlantyckiego dotycząca odstraszania i obrony, polegająca na stałej, rotacyjnej obecności wielonarodowych batalionowych grup bojowych na wschodniej flance NATO. Koncepcja została zatwierdzona na szczycie NATO w Warszawie w 2016 r. jako odpowiedź na nowe wyzwania i zagrożenia w środowisku bezpieczeństwa po rosyjskiej agresji na Ukrainę w 2014 r., w tym aneksji Krymu i destabilizacji Donbasu.

Podczas szczytu w Walii w 2014 r. NATO nie zgodziło się na żadną z proponowanych opcji rozmieszczenia sił bojowych na wschodniej flance NATO, jednak wraz z rozwojem sytuacji, a mianowicie – agresywnymi działaniami wojskowymi Rosji względem Ukrainy czy interwencji wojskowej w Syrii, ryzyko dla państw bałtyckich rosło, a już rozmieszczony amerykański kontyngent wojskowy był zbyt mały, aby stanowić środek odstraszający.

Przed szczytem NATO w Warszawie w 2016 r. odbyły się spotkania w formule ministrów spraw zagranicznych i ministrów obrony państw NATO. W trakcie lutowego spotkania uzgodniono ustanowienie

wzmocnionej wysuniętej sojuszniczej obecności, co miało spowodować wzmocnienie postawy obrony i odstraszania na wschodniej flance NATO. W czerwcu ministrowie zgodzili się co do tego, że eFP będzie realizowana w postaci 4 wielonarodowych, wzmocnionych batalionowych grup bojowych, rozmieszczonych w Polsce oraz w 3 państwach bałtyckich: Litwie, Łotwie i Estonii. Podczas szczytu NATO w Warszawie ustalenia ministrów zostały formalnie zatwierdzone przez przywódców państw i szefów rządów, a także rozszerzone o konkretne zobowiązania poszczególnych państw.

Inicjatywa została zawarta w Komunikacie ze szczytu NATO w Warszawie, w którym zapisano, że wzmocnienie obecności w Estonii, na Łotwie, Litwie oraz w Polsce ma na celu demonstrację solidarności, determinacji i gotowości sojuszników do natychmiastowej reakcji na każdy akt agresji. Zapisano również, że od początku 2017 r. eFP będzie opierała się na wielonarodowych siłach zapewnianych przez państwa ramowe oraz pozostałych sojuszników uczestniczących w tym przedsięwzięciu na zasadzie dobrowolności, ciągłości i rotacji. Siły te miały zostać zorganizowane wokół 4 batalionowych grup bojowych, zdolnych do współdziałania z jednostkami krajowymi stale rozmieszczonymi w państwach-gospodarzach oraz wspieranych przez realny plan wzmocnienia. Na samym początku do pełnienia roli państw ramowych zobowiązały się: Kanada, Niemcy, Wielka Brytania i USA. Polska zaproponowała udostępnienie istniejącej kwatery głównej dywizji jako podstawy do utworzenia wielonarodowej kwatery głównej dywizji. W pracach nad inicjatywną wewnątrz NATO konieczne było pogodzenie 2 kwestii: z jednej strony, zapewnienia państwom wschodniej flanki NATO realnych gwarancji wojskowych, a z drugiej – uniknięcie napięć poprzez rozmieszczenie zbyt licznych – potencjalnie postrzeganych jako ofensywne – grup. Konieczny do wypracowania był zatem konsensus, który pozwolił na pogodzenie tak odmiennych oczekiwań i problemów poszczególnych państw związanych z tą inicjatywą, np. Francja odmówiła bycia państwem przyjmującym, ale zgadzała się na udział w przedsięwzięciu zgodnie z prowadzoną polityką działań w tym regionie. Z kolei u genezy decyzji Kanady jako państwa ramowego leżały naciski wewnętrzne ze strony obywateli ukraińskich i środkowoeuropejskich. Dodatkowo nie wszyscy sojusznicy na etapie wdrażania inicjatywy

chcieli obecności wojsk NATO na swoim terytorium z uwagi na względy historyczne i prowadzoną politykę obronną i bezpieczeństwa, np. Słowacja. Jednak kilka lat później zbrojna inwazja Rosji na Ukrainę zmieniła perspektywę w Europie Środkowo-Wschodniej i ostatecznie doprowadziła do rozszerzenia inicjatywy.

W ramach realizacji inicjatywy rozmieszczono 4 wielonarodowe batalionowe grupy bojowe w Polsce, Estonii, na Łotwie i Litwie. Każda z nich liczyła około tysiąc żołnierzy i była tworzona przez tzw. państwo ramowe, które zapewniało trzon sił i dowodzenia, oraz państwa wspierające. Odpowiednio w Estonii rolę państwa ramowego objęła Wielka Brytania, na Łotwie – Kanada, na Litwie – Niemcy, a w Polsce – Stany Zjednoczone.

Po rosyjskiej pełnoskalowej inwazji na Ukrainę w 2022 r. koncepcja eFP została rozbudowana. Na nadzwyczajnym szczycie NATO w marcu 2022 r. i następnie na szczycie w Madrycie w czerwcu 2022 r. przywódcy zdecydowali o utworzeniu 4 kolejnych wielonarodowych grup bojowych w Bułgarii, Rumunii, na Węgrzech i Słowacji, co wydłużyło pas wysuniętej obecności od Morza Bałtyckiego po Morze Czarne. W kwietniu 2024 r. Niemcy rozpoczęły rozmieszczanie dodatkowych żołnierzy w dowodzonej przez siebie wielonarodowej grupie bojowej na Litwie, przygotowując grunt pod zwiększenie jej obecności z batalionu do brygady. Oddziały te tworzą stałą niemiecką bazę wojskową na Litwie. Brygada pod dowództwem niemieckim została zainaugurowana w maju 2025 r. Będzie ona nadal rozbudowywana i do 2027 r. osiągnie pełną zdolność operacyjną, licząc do 5 tys. żołnierzy. Natomiast w lipcu 2024 r. Łotwa stała się pierwszym krajem, który zwiększył swoją obecność w NATO do poziomu brygady. Docelowo Kanada planuje zakończyć pełne wdrażanie stale rozmieszczonych zdolności brygadowych na Łotwie do 2026 r., mając tam 2200 żołnierzy stacjonujących.

Obecnie wysunięte Siły Lądowe NATO składają się z 8 wielonarodowych grup bojowych rozmieszczonych w państwach członkowskich wzdłuż wschodniej flanki. Grupy bojowe różnią się wielkością i składem w zależności od potrzeb wojskowych. Rozmieszczone są w Bułgarii, Estonii, na Węgrzech, Łotwie, Litwie, w Polsce, Rumunii i Słowacji.

Tabela 1. Wielonarodowe grupy bojowe NATO

Państwo przyjmujące (gospodarz)	**Bułgaria**	**Estonia**	**Węgry**	**Łotwa**	**Litwa**	**Polska**	**Rumunia**	**Słowacja**
Państwo ramowe	Włochy	Wielka Brytania	Węgry	Kanada	Niemcy	USA	Francja	Hiszpania
Państwa delegujące	Albania Chorwacja Grecja Czarnogóra Macedonia Północna Turcja USA	Francja	Chorwacja Włochy Turcja USA	Albania Czechy Dania Islandia Włochy Czarnogóra Macedonia Północna Polska Słowacja Słowenia Hiszpania Szwecja	Belgia Czechy Luksemburg Holandia Norwegia	Chorwacja Rumunia Wielka Brytania	Belgia Luksemburg Hiszpania	Czechy Portugalia Rumunia Słowenia

Źródło: *Strengthening NATO's eastern flank*, https://www.nato.int/en/what-we-do/deterrence-and-defence/strengthening-natos-eastern-flank? (dostęp 11.12.2025).

Wszystkie osiem wielonarodowych grup bojowych zostało włączonych w system dowodzenia NATO, co pozwala utrzymać ich wysoki poziom gotowości i zapewnia możliwość szybkiego reagowania w razie potrzeby. 4 z nich, rozmieszczone w północno-wschodniej części Sojuszu – w Estonii, na Łotwie, Litwie i w Polsce – działają pod zwierzchnictwem NATO poprzez Kwaterę Główną Wielonarodowego Korpusu Północno-Wschodniego w Szczecinie. Za ich szkolenie i przygotowanie odpowiadają 2 dowództwa dywizyjne. Wielonarodowa Dywizja Północny-Wschód w Elblągu, która pełną zdolność operacyjną osiągnie w grudniu 2018 r., współpracuje z grupami rozmieszczonymi w Polsce i na Litwie, natomiast Wielonarodowa Dywizja Północ, powołana przez NATO w październiku 2020 r. i obecnie funkcjonująca w pełnym wymiarze, działa w oparciu

o wysunięte elementy w Ādaži, na Łotwie, oraz zasadnicze struktury w Karup, w Danii, koordynując grupy w Estonii i na Łotwie.

Pozostałe 4 grupy bojowe obsługiwane są przez dowództwa działające na południu wschodniej flanki; w ich skład wchodzą: Dowództwo Wielonarodowej Dywizji Centrum w Székesfehérvár, na Węgrzech, nadzorujące grupy na Węgrzech i Słowacji, a także 2 rumuńskie dowództwa – Korpus Południowo-Wschodni w Sybinie oraz Wielonarodowa Dywizja Południowo-Wschodnia w Bukareszcie, odpowiedzialne za koordynację działań grup bojowych w Rumunii i Bułgarii.

Grupy bojowe funkcjonują w porozumieniu z siłami zbrojnymi kraju przyjmującego i są przez cały czas obecne na jego terytorium. Dodatkowo formacje nie są identyczne – ich skład jest dostosowany m.in. do warunków geostrategicznych panujących w miejscu ich dyslokacji, co ma na celu maksymalne wzmocnienie ich skuteczności bojowej w danych warunkach operacyjnych.

Polska jest zarówno gospodarzem wzmocnionej Wysuniętej Obecności, jak i państwem kontrybuującym. Siły Zbrojne Rzeczypospolitej Polskiej delegują pododdział pancerny do wielonarodowej batalionowej grupy bojowej, sformułowanej przez Kanadę, która stacjonuje na Łotwie. Państwem ramowym eFP w Polsce są Stany Zjednoczone Ameryki; wojska sojusznicze stacjonują we wschodniej Polsce – ten amerykański kontyngent liczy ponad 800 żołnierzy i stanowi trzon „polskiej" wielonarodowej batalionowej grupy bojowej. W grupie służą także żołnierze z Chorwacji, Wielkiej Brytanii i Rumunii. Z kolei od lipca 2021 r. w ramach IX zmiany Polskiego Kontyngentu Wojskowego na Łotwie służą żołnierze z 9 Braniewskiej Brygady Kawalerii Pancernej, a cała grupa bojowa NATO liczy tam ponad tysiąc żołnierzy.

Agnieszka Warchoł

A. Matle, *From "Forward Presence" to –"Forward Defense"*, Germany Must Strengthen NATO's Northeastern Flank in Lithuania, https://dgap.org/en/research/publications/forward-presence-forward-defense (dostęp 11.12.2025); D. Palavenis, *NATO enhanced forward presence in the Baltics: The nexus between the host and the framework nation*, „Security & Defence" 2025; *Strengthening NATO's eastern flank*, https://www.nato.int/en/what-we-do/deterrence-and-defence/

strengthening-natos-eastern-flank (dostęp 11.12.2025); *Warsaw Summit Communiqué*, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique, (dostęp 11.12.2025); *Why the eFP? Some insights on the 2016 NATO*, Warsaw Summit, https://www.frstrategie.org/en/publications/nato-briefs-series/why-efp-some-insights-2016-nato-warsaw-summit-2021 (dostęp 12.12.2025); *Wzmocnienie wschodniej flanki NATO*, https://www.gov.pl/web/obrona-narodowa/wzmocniona-wysunieta-obecnoscc (dostęp 12.12.2025); Wzmocniona Wysunięta Obecność (enhanced Forward Presence, eFP), https://www.gov.pl/web/obrona-narodowa/batalionowa-grupa-bojowa (dostęp 12.12.2015).

Z

ZASADY ŚWIADCZENIA POMOCY HUMANITARNEJ. Pomoc humanitarna opiera się na 4 podstawowych zasadach określonych w rezolucjach Zgromadzenia Ogólnego nr 46/182 i 58/114, które włączono do Kodeksu postępowania obowiązującego w Międzynarodowym Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca i organizacjach pozarządowych w sytuacji reagowania na przypadki klęsk i katastrof, a także do Podstawowego standardu humanitarnego dotyczącego jakości i odpowiedzialności oraz Konsensusu europejskiego w sprawie pomocy humanitarnej. Są to:

- zasada humanitaryzmu nakazująca obowiązek reagowania na wszelkie formy ludzkiego cierpienia, zwłaszcza w odniesieniu do osób znajdujących się w najtrudniejszej sytuacji. Jej istotą jest poszanowanie i ochrona godności każdej osoby dotkniętej kryzysem;
- zasada neutralności stanowiąca zakaz faworyzowania którejkolwiek ze stron konfliktu zbrojnego lub sporu politycznego. Organizacje humanitarne działają wyłącznie na rzecz potrzebujących, bez angażowania się w działania o charakterze politycznym, militarnym lub ideologicznym;

- zasada bezstronności oznaczająca, że pomoc jest wolna od jakiejkolwiek dyskryminacji i musi być udzielana wyłącznie w oparciu o ocenę potrzeb, bez względu na różnice między społecznościami lub wewnątrz nich;
- zasada niezależności odnosząca się do autonomii celów i decyzji humanitarnych względem działań o charakterze politycznym, gospodarczym, wojskowym i innych, która gwarantuje, że jedynym celem pomocy pozostaje ochrona życia ludzkiego oraz łagodzenie cierpienia osób dotkniętych kryzysem i zapobieganie mu.

Zasady pomocy humanitarnej obejmują zarówno wymiar etyczny, jak i organizacyjny działań prowadzonych w sytuacjach kryzysowych. Zgodnie z Konsensusem europejskim w sprawie pomocy humanitarnej jednym z kluczowych aspektów jest konieczność stosowania zasady dobrej pomocy humanitarnej oraz ścisłej współpracy między wszystkimi podmiotami zaangażowanymi w niesienie pomocy. Zasada dobrej pomocy humanitarnej zakłada, że darczyńcy – państwa, organizacje międzynarodowe oraz instytucje prywatne – zobowiązują się do prowadzenia działań w sposób skoordynowany, przejrzysty i efektywny, z pełnym poszanowaniem zasad humanitaryzmu, bezstronności, neutralności i niezależności. Zasada współpracy między podmiotami europejskimi i międzynarodowymi ukierunkowana jest na dążenie do stosowania najlepszych praktyk w zakresie świadczenia pomocy humanitarnej. Współpraca ta obejmuje zarówno wymianę doświadczeń, jak i wspólne opracowywanie standardów jakości oraz mechanizmów oceny skuteczności działań pomocowych. Ponadto pomoc humanitarna powinna być udzielana proporcjonalnie do potrzeb (zasada adekwatności), w jak najkrótszym czasie (zasada szybkości), mając na uwadze, aby koszty świadczenia pomocy nie przewyższały jej wartości faktycznej (zasada możliwie niskich kosztów administracyjnych).

W 2003 r. rząd Szwecji zapoczątkował międzynarodową inicjatywę Dobre Donatorstwo Humanitarne (ang. Good Humanitarian Donorship, GHD) ukierunkowaną na ustanowienie wspólnych zasad i dobrych praktyk w zakresie udzielania pomocy humanitarnej. W spotkaniu inauguracyjnym wzięli udział przedstawiciele 16 państw-darczyńców, Komisji Europejskiej, Organizacji Współpracy Gospodarczej i Rozwoju,

Międzynarodowego Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca, organizacji pozarządowych oraz środowiska naukowego. W wyniku obrad opracowano *Zasady i dobre praktyki donatorstwa humanitarnego* (ang. *Principles and good practice of Humanitarian Donorship*), które obecnie (stan na 2026 r.) obejmują 24 reguły stanowiące kluczowy punkt odniesienia dla polityki darczyńców i organizacji międzynarodowych w zakresie świadczenia pomocy humanitarnej, odpowiedzialności darczyńców wobec beneficjentów i organizacji realizujących pomoc, oraz standardów dotyczących finansowania, koordynacji, monitorowania i ewaluacji działań humanitarnych.

Zasady i praktyki zdefiniowane przez GHD stanowią zarówno ramy dla oficjalnej pomocy humanitarnej, jak i mechanizm zachęcający do większej odpowiedzialności darczyńców. Zostały one opracowane w celu zwiększenia spójności i skuteczności działań darczyńców, a także ich odpowiedzialności wobec beneficjentów, organizacji wdrażających i podmiotów krajowych w zakresie finansowania, koordynacji, monitorowania i oceny tych działań. Ich stosowanie umożliwiają spójne, oparte na potrzebach i odpowiedzialne działania w pełnym cyklu zarządzania kryzysem humanitarnym: od prewencji i gotowości, przez reagowanie, po odbudowę i rozwój.

24 *Zasady i dobre praktyki donatorstwa humanitarnego* określają:

1. Cel działań humanitarnych, jakim jest ratowanie życia, łagodzenie cierpienia i zachowanie godności ludzkiej w trakcie i po kryzysach wywołanych przez człowieka i klęskach żywiołowych, zapobieganie takim sytuacjom oraz wzmacnianie gotowości na ich wystąpienie.
2. Zasady świadczenia pomocy humanitarnej: humanitaryzmu, bezstronności, neutralności i niezależności.
3. Zakres działań humanitarnych obejmujący ochronę ludności cywilnej i osób niebiorących już udziału w działaniach zbrojnych, oraz zapewnienie żywności, wody, środków sanitarnych, schronienia, usług medycznych i innych niezbędnych form pomocy podejmowanej na rzecz osób poszkodowanych celem umożliwienia im powrotu do normalnego życia i odbudowy źródeł utrzymania.

Zasady ogólne:

4. Prymat norm ochronnych. Należy szanować i promować wdrażanie międzynarodowego prawa humanitarnego, prawa uchodźczego oraz praw człowieka.
5. Odpowiedzialność państwa i solidarność międzynarodowa. Przy uznaniu podstawowej odpowiedzialności państw za ofiary kryzysów humanitarnych na ich terytorium dąży się do zapewnienia elastycznego i terminowego finansowania, opierając się na zbiorowym obowiązku zaspokajania potrzeb humanitarnych.
6. Oparcie pomocy humanitarnej na potrzebach. Środki na pomoc humanitarną przydziela się proporcjonalnie do udokumentowanych potrzeb, na podstawie przejrzystych ocen potrzeb.
7. Angażowanie beneficjentów. Organizacje humanitarne powinny najszerzej jak to możliwe angażować beneficjentów w projektowanie, wdrażanie, monitorowanie i ocenę działań humanitarnych.
8. Wzmacnianie zdolności lokalnych. Preferowane jest budowanie potencjału władz i społeczności dotkniętych kryzysem w zakresie prewencji, gotowości, łagodzenia skutków i reagowania na kryzysy humanitarne, aby umożliwić im wykonywanie obowiązków i skuteczną współpracę z partnerami humanitarnymi.
9. Powiązanie pomoc–odbudowa–rozwój. Pomoc humanitarną świadczy się w sposób sprzyjający odbudowie i długoterminowemu rozwojowi, w tym utrzymaniu/przywracaniu zrównoważonych źródeł utrzymania oraz płynnemu przejściu od świadczenia pomocy humanitarnej do działań związanych z odbudową i rozwojem.
10. Wspieranie podmiotów międzynarodowych. Wspiera się centralną rolę ONZ w przywództwie i koordynacji międzynarodowych akcji humanitarnych, szczególną rolę Międzynarodowego Komitetu Czerwonego Krzyża oraz kluczową rolę ONZ, Międzynarodowego Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca oraz organizacji pozarządowych w realizacji akcji humanitarnych.

Dobre praktyki w finansowaniu:

11. Brak wypierania kryzysów przewlekłych. Finansowanie działań humanitarnych w nowych kryzysach nie powinno ograniczać zaspokajania potrzeb w kryzysach trwających.

12. Przewidywalność i elastyczność. Zapewnia się przewidywalne, elastyczne finansowanie dla agencji, funduszy i programów ONZ oraz innych kluczowych organizacji humanitarnych, mając na uwadze konieczność dynamicznej i elastycznej reakcji na zmieniające się potrzeby w sytuacjach kryzysów humanitarnych,
13. Racjonalizacja przeznaczenia środków. Wspiera się przejrzyste, strategiczne priorytety i planowanie finansowe organizacji wdrażających; rozważa się możliwość ograniczenia lub zwiększenia elastyczności przeznaczania środków oraz wprowadzenia długoterminowych ustaleń dotyczących finansowania.
14. Podział obciążeń i instrumenty wspólne. Darczyńcy uczestniczą odpowiedzialnie w Skonsolidowanych Apelach Międzyagencyjnych ONZ i apelach Ruchu Czerwonego Krzyża/Czerwonego Półksiężyca, aktywnie wspierając Wspólne Plany Działań Humanitarnych (ang. Common Humanitarian Action Plan, CHAP) jako podstawowego narzędzia planowania, priorytetyzacji i koordynacji w złożonych sytuacjach kryzysowych.

Promowanie standardów i wdrażania:

15. Zgodność z dobrymi praktykami. Organizacje humanitarne w pełni stosują dobre praktyki i zobowiązują się do promowania odpowiedzialności, efektywności i skuteczności działań humanitarnych.
16. Wytyczne i kodeksy. Promuje się stosowanie wytycznych Stałego Komitetu Międzyagencyjnego, Przewodnich zasad przesiedleń wewnętrznych oraz Kodeksu postępowania Międzynarodowego Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca oraz organizacji pozarządowych w zakresie pomocy w przypadku klęsk żywiołowych z 1994 r.
17. Ułatwianie dostępu. Utrzymuje się gotowość do wspierania realizacji działań humanitarnych, w tym bezpiecznego dostępu do pomocy humanitarnej.
18. Planowanie awaryjne. Wspiera się mechanizmy planowania awaryjnego przez organizacje humanitarne, w razie potrzeby z dedykowanymi środkami finansowanymi na wzmocnienie zdolności reagowania.

19. Prymat cywilnego charakteru pomocy. Potwierdza się pierwszoplanową rolę organizacji cywilnych w realizacji działań humanitarnych – zwłaszcza w konfliktach zbrojnych. Wykorzystanie zasobów wojskowych do wspierania realizacji działań humanitarnych możliwe jest wyłącznie w zgodzie z międzynarodowym prawem humanitarnym i zasadami humanitarnymi, przy uznaniu wiodącej roli organizacji humanitarnych.
20. Wytyczne dotyczące zasobów wojskowych i cywilno-obronnych. Wspiera się wdrażanie Wytycznych z 1994 r. w sprawie wykorzystania zasobów obrony wojskowej i cywilnej w przypadku katastrof oraz Wytycznych z 2003 r. w sprawie wykorzystania zasobów obrony wojskowej i cywilnej w celu wspierania działań humanitarnych Organizacji Narodów Zjednoczonych w złożonych sytuacjach kryzysowych.

Uczenie się i odpowiedzialność:

21. Inicjatywy *learning & accountability*. Wspierane są programy uczenia się i odpowiedzialności służące skutecznemu i efektywnemu wdrażaniu działań humanitarnych.
22. Oceny reakcji międzynarodowych. Zachęca się do regularnych ewaluacji reakcji społeczności międzynarodowej na kryzysy humanitarne, w tym efektywności działań darczyńców.
23. Transparentna sprawozdawczość. Zapewnia się wysoką dokładność, terminowość i przejrzystość raportowania wydatków na oficjalną pomoc humanitarną darczyńców; promuje się standardowe formaty raportów.

Sposoby udzielania pomocy:

24. Transfery pieniężne. Systematycznie rozważa się wykorzystanie przekazów gotówkowych – samodzielnie lub w połączeniu z innymi formami – stosownie do kontekstu jako często najbardziej efektywnego i wydajnego sposobu zaspokajania potrzeb humanitarnych.

Klaudia Cenda-Miedzińska

Good Humanitarian Donorship, 24 Principles and Good Practice of Humanitarian Donorship, https://www.ghdinitiative.org/ghd/gns/principles-good-practice-of-ghd/principles-good-practice-ghd.html (dostęp 24.01.2026); Konsensus europejski w sprawie pomocy humanitarnej Rezolucja Parlamentu Europejskiego z dnia 18 stycznia 2011 r. w sprawie realizacji Konsensusu europejskiego w sprawie pomocy humanitarnej: przegląd śródokresowy planu działania i dalsze kroki, Dz.U. C 136E z 11.05.2012, s. 1–8; UN General Assembly, Resolution on Strengthening of the coordination of humanitarian emergency assistance of the United Nations, 19.12.1991, A/RES/46/182; UN General Assembly, Resolution on Strengthening of the coordination of emergency humanitarian assistance of the United Nations, 17.12.2003, A/RES/58/114; Wspólne oświadczenie Rady i przedstawicieli rządów państw członkowskich zebranych w Radzie, Parlamencie Europejskim i Komisji Europejskiej, Konsensus europejski w sprawie pomocy humanitarnej, Dz.U. C 25 z 30.01.2008, s. 1–12.

ZATRZYMANIE NIELETNIEGO – środek o charakterze procesowym polegający na czasowym pozbawieniu wolności osoby, która nie ukończyła 18 roku życia, podejmowany wyłącznie w przypadkach przewidzianych prawem. W ujęciu naukowym instytucja ta stanowi element systemu reagowania państwa na zachowania naruszające normy prawne, łącząc funkcję zabezpieczającą z wychowawczą i ochronną. Jej stosowanie podlega zasadzie proporcjonalności oraz szczególnym gwarancjom praw dziecka wynikającym z krajowych regulacji i standardów międzynarodowych. Celem zatrzymania nieletniego nie jest represja, lecz ochrona dobra małoletniego oraz prawidłowego toku postępowania.

Zatrzymanie jest środkiem przymusu polegającym na krótkotrwałym pozbawieniu wolności określonej osoby przez uprawnione organy państwowe. Zgodnie z art. 41 ust. 1 Konstytucji Rzeczypospolitej Polskiej pozbawienie lub ograniczenie wolności osobistej może nastąpić wyłącznie na zasadach i w trybie określonych w ustawie, z zachowaniem przewidzianych prawem gwarancji procesowych. Mimo swojej dolegliwości środek ten może być wyjątkowo niezbędny dla zabezpieczenia prawidłowego toku postępowania karnego, ochrony dóbr prawnie chronionych, w tym ochrony samego nieletniego bądź innych osób. W doktrynie i praktyce prawa wyróżnia się zatrzymanie procesowe oraz pozaprocesowe. To ostatnie zostało uregulowane w art. 15 ust. 1 pkt 2 i 3 ustawy o Policji i może być

stosowane wobec osób stwarzających w sposób oczywisty bezpośrednie zagrożenie dla życia lub zdrowia ludzkiego, a także dla mienia. Zatrzymanie procesowe normowane jest w rozdziale 27 Kodeksu postępowania karnego (dalej: k.p.k.). Zgodnie z art. 244 §1 k.p.k. Policja ma prawo zatrzymać osobę podejrzaną, jeżeli istnieje uzasadnione przypuszczenie, że popełniła ona przestępstwo, a jednocześnie zachodzi obawa jej ucieczki lub ukrycia się, zatarcia śladów przestępstwa, brak możliwości ustalenia tożsamości tej osoby albo istnieją przesłanki do prowadzenia wobec niej postępowania w trybie przyspieszonym.

W przypadku nieletnich zatrzymanie ma charakter wyjątkowy i powinno być stosowane tylko wtedy, gdy inne środki są niewystarczające, wynika to z zasad subsydiarności i minimalnej ingerencji.

Zasada subsydiarności polega na traktowaniu zatrzymania nieletniego jako środka ostatecznego (łac. *ultima ratio*). Oznacza to, że może ono zostać zastosowane wyłącznie wówczas, gdy inne, mniej dolegliwe nie są wystarczające do osiągnięcia zamierzonego celu, w szczególności zapewnienia bezpieczeństwa nieletniego lub prawidłowego toku postępowania. Organ stosujący prawo powinien każdorazowo rozważyć możliwość zastosowania alternatywnych form reakcji, takich jak oddanie nieletniego pod opiekę rodziców lub przedstawicieli ustawowych.

Zasada minimalnej ingerencji nakazuje natomiast ograniczenie stosowania zatrzymania do niezbędnego zakresu, zarówno pod względem czasu trwania, jak i intensywności oddziaływania. Zatrzymanie nieletniego powinno trwać możliwie najkrócej i być realizowane w sposób uwzględniający jego wiek, stopień rozwoju oraz potrzeby psychofizyczne. Zasada ta wyraża prymat dobra dziecka i wymaga, aby ingerencja organów państwa była proporcjonalna do zagrożenia oraz celu, jaki ma zostać osiągnięty.

Zasady subsydiarności i minimalnej ingerencji w sprawie zatrzymania nieletniego wynikają z kilku podstawowych przepisów prawa. Ich konstytucyjną podstawę stanowi art. 31 ust. 3 Konstytucji RP, wprowadzający zasadę proporcjonalności ograniczeń praw i wolności, oraz art. 41 ust. 1 Konstytucji RP, gwarantujący ochronę wolności osobistej. Na poziomie ustawowym zasady te wywodzone są z art. 3 ustawy o wspieraniu i resocjalizacji nieletnich, ustanawiającego nadrzędność dobra dziecka, oraz art.

5 tej ustawy, nakazującego stosowanie środków adekwatnych i możliwie najmniej dolegliwych. Ich międzynarodowym źródłem jest art. 37 lit. b Konwencji o prawach dziecka, zgodnie z którym pozbawienie wolności dziecka może być stosowane wyłącznie jako środek ostateczny i na możliwie najkrótszy czas.

Podstawę prawną zatrzymania nieletniego stanowi art. 48 ust. 1 Ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich, który określa przesłanki dopuszczalności zastosowania tego środka przez uprawnione organy:

– art. 48. 1. Policja może zatrzymać, a następnie umieścić w policyjnej izbie dziecka nieletniego, co do którego istnieje uzasadnione przypuszczenie, że dopuścił się czynu karalnego, o którym mowa w art. 1 ust. 2 pkt 2 lit. a, i zachodzi uzasadniona obawa ucieczki, ukrycia się nieletniego lub zatarcia śladów czynu karalnego albo nie można ustalić tożsamości nieletniego.

Uprawnienia do zatrzymania nieletniego przysługują określonym organom państwowym, w tym przede wszystkim Policji i Straży Granicznej, które w ramach swoich kompetencji mogą stosować ten środek w ściśle określonych prawem sytuacjach.

Przesłanki zatrzymania nieletniego stanowią warunki prawne, których spełnienie jest konieczne, aby organ uprawniony mógł zastosować środek ograniczający wolność osobistą osoby nieletniej:

– uzasadnione podejrzenie popełnienia czynu karalnego;
– uzasadniona obawa ucieczki lub ukrycia się nieletniego;
– uzasadniona obawa zatarcia śladów czynu zabronionego;
– brak możliwości ustalenia tożsamości nieletniego.

Uzasadnione podejrzenie popełnienia czynu karalnego oznacza istnienie informacji lub okoliczności wskazujących na wysokie prawdopodobieństwo, że nieletni dopuścił się czynu zabronionego. Nie wymaga ono całkowitej pewności, lecz musi opierać się na faktach, dowodach lub wiarygodnych poszlakach, a nie domysłach bądź pogłoskach. Przykładem mogą być obserwacje organów ścigania lub relacje świadków.

Uzasadniona obawa ucieczki lub ukrycia się nieletniego wynika z posiadanych informacji wskazujących, że osoba może próbować uniknąć

postępowania, np. poprzez zmiany miejsca pobytu, niestawiennictwo na wezwania czy przygotowanie fałszywych dokumentów. Sama deklaracja nieletniego o planowanym wyjeździe nie jest wystarczająca. Konieczne są okoliczności świadczące o realnym zamiarze uchylania się od nadzoru.

Obawa zatarcia śladów czynu zabronionego dotyczy działań nieletniego zmierzających do utrudnienia lub uniemożliwienia zabezpieczenia materiału dowodowego, np. ukrywania lub niszczenia przedmiotów związanych z przestępstwem.

Brak możliwości ustalenia tożsamości nieletniego występuje, gdy nieletni nie posiada dokumentów tożsamości lub podaje fałszywe dane, uniemożliwiając identyfikację w toku postępowania.

Czas zatrzymania nieletniego ma charakter ściśle ograniczony i służy wyłącznie realizacji niezbędnych czynności procesowych. Zatrzymanie może trwać do 48 godzin na polecenie sądu rodzinnego, natomiast pobyt nieletniego w Policyjnej Izbie Dziecka nie może przekroczyć 72 godzin i nie podlega przedłużeniu. W wyjątkowych sytuacjach dopuszczalne jest dalsze umieszczenie nieletniego w odpowiedniej placówce do 5 dni w celu oczekiwania na decyzję sądu lub przekazanie do właściwej instytucji.

Wobec nieletniego, który ukończył 18 rok życia i został zatrzymany w trakcie samowolnego pobytu poza zakładem poprawczym, może zostać zastosowany środek o charakterze zabezpieczającym polegający na jego czasowym umieszczeniu w jednostce organizacyjnej Policji. Umieszczenie to następuje w pomieszczeniu dla osób zatrzymanych lub doprowadzonych w celu wytrzeźwienia i ma charakter wyłącznie tymczasowy, ograniczony do okresu niezbędnego do przekazania nieletniego do właściwego zakładu poprawczego. Czas stosowania tego środka nie może przekroczyć 5 dni, wynika to z art. 49 ust. 2 ustawy o wspieraniu i resocjalizacji nieletnich.

Obowiązki Policji w związku z zatrzymaniem nieletniego obejmują zespół gwarancyjnych czynności procesowych, których celem jest ochrona praw dziecka oraz zapewnienie legalności zatrzymania. Policjant jest zobowiązany do niezwłocznego poinformowania nieletniego o przyczynach zatrzymania oraz pouczenia go o przysługujących prawach. Konieczne jest także bezzwłoczne przesłuchanie nieletniego i sporządzenie protokołu z tej czynności, przy czym czynność ta powinna odbywać się w obecności

rodzica, opiekuna lub obrońcy, a w razie niemożności ich udziału – innej uprawnionej osoby. Policja ma obowiązek sporządzić protokół zatrzymania zawierający okoliczności, czas i przyczyny pozbawienia wolności oraz doręczyć jego kopię nieletniemu wraz z pouczeniem. Ponadto Policja zobowiązana jest do niezwłocznego, nie później niż w ciągu 24 godzin, zawiadomienia właściwego sądu rodzinnego oraz rodziców lub opiekuna nieletniego o dokonanym zatrzymaniu, z udokumentowaniem faktu powiadomienia w protokole.

Prawa nieletniego w związku z zatrzymaniem stanowią zespół gwarancji procesowych mających na celu ochronę jego wolności osobistej oraz zapewnienie rzetelności postępowania. Nieletni ma prawo do niezwłocznej informacji o przyczynie zatrzymania oraz do rzetelnego pouczenia o przysługujących mu uprawnieniach, przy czym brak lub wadliwość pouczenia nie może rodzić dla niego negatywnych konsekwencji. Przysługuje mu prawo do korzystania z pomocy obrońcy, w tym do złożenia wniosku o wyznaczenie obrońcy z urzędu, a także do kontaktu z rodzicem, opiekunem lub obrońcą, przy czym kontakt z obrońcą powinien odbywać się bez udziału osób trzecich.

Nieletni ma prawo do składania wyjaśnień lub odmowy ich składania, do korzystania z bezpłatnej pomocy tłumacza, w tym tłumacza języka migowego, jeżeli wymaga tego jego sytuacja, oraz do dostępu do niezbędnej pomocy medycznej. Ponadto przysługuje mu prawo do otrzymania kopii protokołu zatrzymania oraz złożenia do niego oświadczenia. Zatrzymanemu nieletniemu, a także jego rodzicom lub opiekunowi, przysługuje prawo wniesienia zażalenia na zatrzymanie w celu zbadania jego legalności, zasadności i prawidłowości. Dodatkowo nieletni powinien być pouczony o możliwości zawiadomienia na swój wniosek, szkoły lub pracodawcy o zatrzymaniu oraz o prawie do kontaktu z właściwym urzędem konsularnym w przypadkach przewidzianych prawem.

Zwolnienie nieletniego stanowi obligatoryjną czynność procesową polegającą na niezwłocznym zakończeniu zatrzymania oraz przekazaniu nieletniego rodzicom albo opiekunowi prawnemu, jeżeli dalsze pozbawienie wolności traci podstawę prawną lub faktyczną. Zwolnienie to następuje w szczególności w przypadku:

– ustania przyczyny zatrzymania;

- wydania przez sąd rodzinny polecenia natychmiastowego zwolnienia;
- nieprzekazania przez Policję w terminie 24 godzin od chwili zatrzymania całości materiałów uzasadniających przypuszczenie popełnienia przez nieletniego czynu karalnego, o którym mowa w art. 1 ust. 2 pkt 2 lit. a ustawy o wspieraniu i resocjalizacji nieletnich;
- nieogłoszenia nieletniemu w terminie 24 godzin od przekazania tych materiałów sądowi rodzinnemu postanowienia o zastosowaniu środka tymczasowego, o którym mowa w art. 44 pkt 4–8 tej ustawy.

W konsekwencji zatrzymanie nieletniego powinno być traktowane jako instrument o ściśle wyjątkowym charakterze, stosowany jedynie w sytuacjach, w których zastosowanie łagodniejszych środków wychowawczych lub zabezpieczających nie zapewnia realizacji celów postępowania. Takie ujęcie pozostaje w zgodzie ze standardami wynikającymi z Konwencji o prawach dziecka, zgodnie z którymi pozbawienie wolności dziecka może być dopuszczone wyłącznie jako środek ostateczny i ograniczony do najkrótszego możliwego czasu.

Dariusz Hybś

T. Bojarski, e. Kruk, e. Skrętowicz, *postępowanie w sprawach nieletnich komentarz*, wydawnictwo wolters kluwer, warszawa 2016; konstytucja rzeczypospolitej polskiej z dnia 2 kwietnia 1997 r., dz.u. 2009, nr 114, poz. 946 z późn. Zm.; konwencja o prawach dziecka przyjęta przez zgromadzenie ogólne narodów zjednoczonych dnia 20 listopada 1989 r., dz.u. Nr 120, poz. 526 z późn. Zm.; j. Kudrelek, i. Wojciechowska, *postępowanie przygotowawcze. Wybrane zagadnienia, orzecznictwo, przykłady*, wydawnictwo wyższej szkoły policji, szczytno 2008; r. Nienałtowski, *przesłanki zatrzymania nieletniego sprawcy czynu karalnego*, „kwartalnik policyjny" 2022, nr 2; k. Nowakowska, p. Kuśka, p. Oleksiński, g. Waleczek, *procedury postępowania w sprawach nieletnich w świetle nowych przepisów prawnych*, szkoła policji w katowicach, katowice 2023; ustawa z dnia 6 kwietnia 1990 r. O policji, dz.u. 2025, poz. 636, 718 z późn. Zm.; ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, dz.u. 2025, poz. 46, 1178, 1420 z późn. Zm.; ustawa z dnia 12 sierpnia 2022 r. O wspieraniu i resocjalizacji nieletnich, dz.u. 2024, poz. 978, 1228 z późn. Zm.

ISBN 978-83-68637-15-1