ENCYKLOPEDIA BEZPIECZEŃSTWA

TOM 2

ENCYKLOPEDIA
BEZPIECZEŃSTWA

TOM 2
D–K

REDAKCJA NAUKOWA
OLGA WASIUTA, SERGIUSZ WASIUTA

ENCYKLOPEDIA
BEZPIECZEŃSTWA

TOM 2
D–K

REDAKCJA NAUKOWA
OLGA WASIUTA, SERGIUSZ WASIUTA

ISBN 978-83-66269-52-1

Recenzenci:
prof. dr hab. Wojciech Jakubowski (Uniwersytet Warszawski)
prof. dr hab. Bogusław Pacek (Uniwersytet Jagielloński)

Redakcja:
Michał Pranke

Korekta:
Joanna Kłos

Projekt okładki i skład:
LIBRON

Publikacja sfinansowana przez Uniwersytet Pedagogiczny
im. 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

WYKAZ HASEŁ

TOM 1*

* Hasła na litery A–C i L–Ż znajdują się w osobnych tomach encyklopedii. Zob.: *Encyklopedia bezpieczeństwa*, O. Wasiuta, S. Wasiuta (red.), t. 1, 3, 4, Wydawnictwo Libron, Kraków 2021.

broń entomologiczna
broń genetyczna
broń geofizyczna
broń hipersoniczna
broń klimatyczna / broń meteorologiczna
broń masowego rażenia
broń nieśmiercionośna
broń nuklearna
broń radiologiczna
broń strzelecka
Bundeswehra
Business Process Management
Cambridge Analytica
casus belli
CENTO (Central Treaty Organization)
Centralne Biuro Antykorupcyjne
Centralne Biuro Śledcze Policji
Centrum Analiz Propagandy i Dezinformacji
Centrum Doskonalenia Obrony przed Cyberatakami
Centrum Eksperckie NATO ds. Komunikacji Strategicznej
centrum powiadamiania ratunkowego
cenzura
choroby informacyjne
cichociemni
crime mapping
Crime Prevention Through Environmental Design
cyberataki
cyberbezpieczeństwo
cyberbroń (broń cybernetyczna)
cybercenzura
cybergrupy
cyberkonflikt
cyberprzemoc
cyberprzestępczość
cyberprzestrzeń

TOM 2

TOM 3

międzynarodowe prawo humanitarne konfliktów zbrojnych
międzynarodowe stosunki wojskowe
Międzynarodowy Trybunał Karny
Międzynarodowy Trybunał Sprawiedliwości
militarne działania nieregularne
militarne i niemilitarne metody prowadzenia wojny hybrydowej
militaryzacja przestrzeni kosmicznej
misja pokojowa
mobilizacja
morale
nacjonalizm
NATO
nauki o bezpieczeństwie
nawalizm
nawoływanie do popełnienia przestępstwa
negocjacje międzynarodowe
neokonserwatyzm
neonazizm
neutralność międzynarodowa
Niebieska Karta
obrona cywilna
obrona narodowa
obrona totalna
ochrona ludności
ochrona własności intelektualnej w sieci
ochrona zdrowia (system opieki zdrowotnej, system ochrony zdrowia)
oddziały cybernetyczne w Wojsku Polskim
odstraszanie
okno Overtona
okręt wojenny
operacje dezinformacji wojskowej
operacje propagandowe
operacje psychologiczne
opinia publiczna
Organizacja ds. Współpracy w Zakresie Uzbrojenia

TOM 4

Służba Celno-Skarbowa
Służba Kontrwywiadu Wojskowego
Służba Ochrony Państwa
Służba Wywiadu Wojskowego
służby specjalne
Smart City
Social Media Intelligence
soft power
specjalistyczne uzbrojone formacje ochronne
społeczeństwo informacyjne
społeczeństwo nadzorowane
społeczeństwo obywatelskie
społeczeństwo ryzyka
społeczeństwo sieci
społeczne bezpieczeństwo informacyjne
stalinizm
standardy kompetencji informacyjnych
stany nadzwyczajne
stealth techniki
steganografia
stereotyp wroga
stopień wojskowy
strategia
strategia bezpieczeństwa narodowego
strategia cyberbezpieczeństwa USA
Strategiczny Przegląd Bezpieczeństwa Narodowego
Straż Miejska/Gminna
straż sąsiedzka
strefa zakazu lotów
suwerenność państwa
swatting
syndrom sztokholmski
system bezpieczeństwa narodowego
system HACCP
System Informacyjny Schengen

D

DARKNET (ciemna sieć) – część internetu najczęściej wiązana z pełną anonimowością i możliwością prowadzenia szeregu działań, w tym transakcji, które mają charakter nielegalny. W potocznych wyobrażeniach kojarzone z handlem bronią i narkotykami, pornografią dziecięcą i →przemocą [t. 3]*. Pojęcie darknetu zostało po raz pierwszy użyte w artykule P. Biddle'a, P. Englanda, M. Peinady i B. Willmana, pracowników korporacji Microsoft. W 2002 r. opublikowali opracowanie pt. *The Darknet and the Future of Content Distribution*, w którym przewidywali istnienie sieci typu darknet mających zwiększyć wygodę, przepustowość, wydajność i anonimowość w zakresie dzielenia się plikami. Choć wskazywali wówczas, że darknet może rodzić kontrowersje prawne, nie przewidzieli, w jakim kierunku będzie się rozwijać ten rodzaj aktywności w sieci.

W internecie – rozumianym jako globalny system sieci komputerowych, który obecnie rozszerzył się na inne urządzenia, takie jak smartfony i tablety – konieczne staje się wyróżnienie 2 warstw sieci: surface webu, zwanego też clearnetem, czyli internetu zindeksowanego lub inaczej

* Rozstrzelone słowa stanowią osobne hasła znajdujące się w *Encyklopedii bezpieczeństwa*. Oznaczenia „[t. 1]", „[t. 3]", „[t. 4]" informują, że hasło mieści się we wskazanych, odrębnych tomach encyklopedii.

powierzchniowego, oraz → d e e p w e b u, czyli ukrytej części sieci. Pierwsza z nich jest tym, co przeciętny użytkownik uważa za internet – zbiorem stron internetowych indeksowanych przez wyszukiwarki takie jak Google, Yahoo i Bing, do których to witryn można łatwo uzyskać dostęp za pomocą standardowych przeglądarek i protokołów internetowych. Choć można na nich odnaleźć ogromną ilość → i n f o r m a c j i, to surface web jest tylko wierzchołkiem góry lodowej. Główną jej częścią pozostaje deep web. Jest to druga warstwa sieci, zdefiniowana przez wymóg oddzielnego interfejsu potrzebnego do uzyskania dostępu do danych, ponieważ nie jest indeksowana. Wielu badaczy podkreśla, że ukryty internet jest znacznie większy niż internet zindeksowany. Z badań K. Finklei przeprowadzonych w 2017 r. wynika, że deep web jest większy ok. 4–5 tys. razy od internetu zindeksowanego. To właśnie w obszarze deep webu należy lokować → d a r k w e b oraz darknet, czyli ciemniejsze strony internetu.

W dyskusjach potocznych istnieje tendencja do traktowania pojęć „dark web" oraz „darknet" jako synonimów. Z technicznego punktu widzenia nie są one jednak tym samym. Cząstka „net" w wyrażeniu „darknet" pochodzi od słowa internet – globalnego systemu połączonych ze sobą sieci komputerowych. Z kolei słowo „web", skrót od World Wide Web, oznacza zestaw protokołów, które pozwalają korzystać z internetu, takich jak HTTP, TCP/IP czy UDP. Można je traktować jako rodzaj języka niezbędnego do tego, by wszystkie urządzenia mogły komunikować się ze sobą w ten sam sposób, aby proces przesyłania danych między nimi był skuteczny. Istnieje zatem wyraźna różnica pomiędzy darknetem a dark webem. Darknet to sieć komputerów, których zwykle nie można zobaczyć, a dark web to system, który pozwala na interakcję z nimi. Przykładami takich systemów są Tor lub Freenet, odpowiedniki usługi World Wide Web, umożliwiające korzystanie z ciemnej strony sieci.

Darknet jest niewielką częścią deep webu, do którego dostęp uzyskuje się za pomocą przeglądarek z maskowaniem tożsamości, takich jak The Onion Router (Tor), Freenet i I2P. Technologia zwiększająca poziom prywatności (ang. *privacy-enhancing technology*, PET) wykorzystywana przez te przeglądarki zawdzięcza swoje początki amerykańskiemu laboratorium badawczemu → m a r y n a r k i w o j e n n e j [t. 3] i Agencji Zaawansowanych Projektów Badawczych w Obszarze Obronności

(Defense Advanced Research Projects Agency, DARPA). PET i darknet zostały początkowo opracowane w celu ochrony internetowych komunikatów wywiadowczych USA przed zagranicznym nadzorem. Później zostały zmienione i wykorzystane przez The Tor Project do stworzenia platformy pozwalającej uniknąć monitorowania przez rządy i korporacje. Ze względu na silne szyfrowanie i wiele dostępnych technik maskowania tożsamości darknet jest używany przez cyberprzestępców.

Dostęp do darknetu może uzyskać każdy, kto zechce pobrać i zainstalować przeglądarkę Onion – np. Tor lub I2P. Jednak samo zainstalowanie przeglądarki typu Onion nie zapewnia anonimowości w darknecie. Usługodawca internetowy oraz instytucje nadzorujące korzystanie z sieci wiedzą, kiedy użytkownik korzysta z sieci takich jak Tor, chociaż niekoniecznie to, jakie treści przegląda. Właśnie dlatego niezbędne jest zwiększenie anonimowości użytkownika podczas korzystania z darknetu.

Wygląd przeglądarki typu Onion bazuje na popularnym, darmowym programie Mozilla Firefox. Cechą charakterystyczną adresów stron w tej sieci jest to, iż kończą się frazą *.onion*. Jako przykłady takich adresów można podać następujące strony, które w 2014 r. zostały zamknięte przez FBI:

- sklepy narkotykowe: Blue Sky (blueskyplzv4fsti.onion), Hydra (hy-drampvvnunildl.onion), Pandora (pandora3uym4z42b.onion), Cloud Nine (xvqrvtnn4pbcnxwt.onion);
- sklep z bronią: Executive Outcomes (http://iczyaan7hzkyjown.onion);
- sklep z kartami kredytowymi: Fake Real Plastic (http://igvmwp3544wp nd6u.onion);
- sklep z fałszywymi dowodami osobistymi: Fake ID (http://23swqgocas65z7xz.onion);
- sklepy z fałszywymi banknotami: Fast Cash (http://5oulvdsnka55buw6.onion), Super Notes Counter, (http://67yjqewxrd2ewbtp.onion).

W przeglądarce poza możliwościami przeglądania specjalnej, kodowanej treści istnieje też możliwość przeglądania zwykłych, ogólnodostępnych stron internetowych. Dostęp do treści szyfrowanych nie zawsze jest możliwy, gdyż uzależnione jest to od tego, czy serwer z daną zawartością pozostaje włączony. Nie zawsze tak jest, ponieważ węzły komunikacyjne

zakładane są w dużej mierze przez osoby prywatne, zaś ich utrzymanie wiąże się z wysokimi kosztami. Sieci typu darknet działają znacznie wolniej niż zwykły internet, ponieważ możliwości przesyłu danych są ograniczone. Jest to także powodem, dla którego wygląd stron jest na ogół bardzo skromny, oszczędny w grafiki czy pliki filmowe, niejednokrotnie ograniczony tylko do tekstu. Ponadto węzły komunikacyjne najczęściej są tak zaprogramowane, aby domyślnie blokowały te sposoby wymiany i dystrybucji plików, które powodują zbyt duży przesył danych.

Tor jest bardzo popularną przeglądarką, której liczbę aktywnych użytkowników w styczniu 2018 r. oszacowano na 4 mln. Najwięcej jest ich w USA (19%), następnie w Rosji (11,9%), Niemczech (9,9%) i Zjednoczonych Emiratach Arabskich (9,2%).

Darknet jest używany do szerokiej gamy działań społecznych. Obejmują one formy aktywności od wyraźnie moralnie akceptowalnych, poprzez uznane za niedozwolone przez niektórych, aż po wyraźnie przestępcze w oparciu o krajowe lub międzynarodowe normy prawne. Działania te można podzielić na 3 główne kategorie:

- aktywizm, dziennikarstwo i informowanie o nieprawidłowościach;
- działalność przestępcza na wirtualnych rynkach;
- generowanie → zagrożenia bezpieczeństwa [t. 4] cybernetycznego, w tym tworzenie → botnetów [t. 1], → złośliwego oprogramowania [t. 4] i oprogramowania → ransomware [t. 3].

Anonimowość zapewniana przez darknet jest wykorzystywana do celów społecznych i politycznych. Użytkownicy mogą otwarcie dzielić się swoimi przekonaniami i wyrażać niezgodę na działania rządów lub oczekiwania wobec nich bez obawy o odwet. Ta możliwość nieskrępowanej afirmacji postaw jest szczególnie cenna w państwach o silnej → cenzurze [t. 1] państwowej i inwigilacji wobec działaczy politycznych, bojowników o wolność i dziennikarzy. Reporterzy, aktywiści i demaskatorzy w takich państwach mogą wykorzystywać darknet do komunikowania się ze światem zewnętrznym, zachęcać do zmian społecznych i reform politycznych, nie ujawniając swojej tożsamości. Prawie wszystkie organizacje tego typu zmierzają do prowadzenia elektronicznej wymiany informacji w bezpiecznych miejscach. Korzystanie z Tora jest zalecane przez Reporterów bez Granic – międzynarodową

organizację pozarządową propagującą i monitorującą wolność prasy na całym świecie – jako jeden z warunków przetrwania dziennikarzy i aktywistów pracujących w represyjnych państwach. Dobrym przykładem zastosowania Tora mogą być zamieszki w Egipcie, w czasie których dziennikarzom i aktywistom z całego świata udało się dzięki przeglądarce ominąć cenzurę rządu i skutecznie informować o bieżącej sytuacji. Sygnalizm, czyli zgłaszanie nieprawidłowości w działaniu państwa, jest aktem polegającym na działaniu ukierunkowanym na wyciekanie prywatnych informacji rządów lub firm do wiadomości publicznej. Pozostaje to zgodne z założeniem, że społeczeństwo ma prawo do informacji o działaniach zarówno swoich rządów, jak i dużych przedsiębiorstw. Niezależnie od tego w niektórych krajach wyciek prywatnych informacji z plików rządowych jest uważany za szkodliwy. Co więcej, wyciek informacji z firm jest nielegalny w niektórych krajach, np. w USA. E. Snowden, jeden z najbardziej znanych informatorów, ujawnił poufne informacje rządu Stanów Zjednoczonych – większość z nich dotyczyła NSA i armii amerykańskiej – za co został oskarżony na podstawie ustawy o szpiegostwie z 1917 r. Najprawdopodobniej do wysłania do wielu dziennikarzy tajnej informacji o amerykańskim programie szpiegowskim PRISM wykorzystał Tora.

Duża liczba wirtualnych rynków darknetu specjalizuje się w handlu nielegalnymi narkotykami. Skradzione tożsamości, informacje o kartach kredytowych, broń i morderstwa na zlecenie to także popularne „towary i usługi" w tej sieci. Model biznesowy jest podobny do rynku online eBay. Użytkownicy mogą zostawiać informacje zwrotne na temat produktów, a w celu ochrony sprzedawców i kupujących oraz rozwiązywania ewentualnych sporów został utworzony system o nazwie „escrow". Najczęściej spotykaną i gwarantującą największą anonimowość metodą płatności są bitcoiny. Są one jedną z wielu istniejących kryptowalut, rozproszonego systemu księgowości, który przechowuje informacje o stanie posiadania użytkownika w umownych jednostkach. Waluta przechowywana jest w portfelach, do których dostęp mają tylko ich użytkownicy, można ją wymieniać na zwykłe waluty zarówno elektronicznie na odpowiednich serwisach, jak i na gotówkę w specjalnych bankomatach.

Darknet jest także miejscem → z a g r o ż e ń [t. 4] cybernetycznych. Na niektórych rynkach przedmiotem obrotu są narzędzia hakerskie, które

mogą być bezpośrednio lub pośrednio wykorzystywane do atakowania firm lub osób. Twórcy szkodliwego oprogramowania wykorzystują darknet do komunikacji i wymiany pomysłów. Szkodliwe oprogramowanie ChewBacca wykorzystuje infrastrukturę Tora do uzyskiwania adresów IP swoich ofiar i rejestrowania uderzeń klawiatury; z kolei złośliwe oprogramowanie i2Ninja jest znane z utrzymywania bezpiecznej komunikacji między zainfekowanymi urządzeniami a serwerem dowodzenia i kontroli poprzez ukrytą sieć I2P. Oprogramowanie ransomware uruchamia wirusy na zainfekowanych komputerach, szyfruje wszystkie dane, do których może uzyskać dostęp, a następnie żąda płatności w bitcoinach, aby uwolnić dane.

Ocena działania i funkcjonowania darknetu pozostaje niejednoznaczna. Anonimowe miejsce dyskusji, wymiany poglądów, protestów czy obywatelskiego buntu jawi się jako szczególnie wartościowe w dobie wszechobecnej kontroli państwa. Ciemna strona internetu jest jednak związana także z handlem ludźmi, bronią oraz pornografią dziecięcą. Z uwagi na anonimowość użytkowników darknetu ściganie działań niezgodnych z prawem jest tu o wiele trudniejsze niż w tradycyjnym internecie.

Jakub Idzik, Rafał Klepka

P. Biddle, P. England, M. Peinado i in., *The Darknet and the Future of Content Protection*, [w:] *Digital Rights Managment. DRM 2002*, J. Feigenbaum (ed.), Springer, Berlin–Heidelberg 2003; R. Broadhurst, D. Lord, D. Maxim i in., *Malware Trends on „Darknet" Crypto-markets: Research Review*, Australian National University, Cybercrime Observatory, Canberra 2018; J. Broséus, D. Rhumorbarbe, M. Morelato i in., *A Geographical Analysis of Trafficking on a Popular Darknet Market*, „Forensic Science International" 2017, vol. 277; K. Finklea, *Dark Web*, Congressional Research Service, 2017; L. Gayard, *Darknet: Geopolitics and Uses*, ISTE Ltd, Wiley, London–Hoboken 2018; J. Idzik, R. Klepka, *Darknet*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J. Kosiński, *Deepweb and Darknet – Police View*, referat wygłoszony na konferencji Archibald Reiss Days, Belgrad 2015; A. Krauz, *Mroczna strona internetu – TOR niebezpieczna forma cybertechnologii*, „Dydaktyka Informatyki" 2017, nr 12; M. Majorek, *Darknet. Ostatni bastion wolności w internecie?*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 4; M. Mirea, V. Wang, J. Jung, *The not so Dark Side of the Darknet: A Qualitative Study*, „Security Journal"

2019, vol. 32, no. 2; D. Moore, T. Rid, *Cryptopolitik and the Darknet*, „Survival Global Politics and Strategy" 2016, vol. 58, no. 1; H. Wojciechowski, *Darknet – wybrane aspekty kryminologiczne, kryminalistyczne i prawne szyfrowanych sieci komputerowych*, „Acta Universitatis Lodziensis. Folia Iuridica" 2018, nr 82.

DARK WEB (mroczna/ciemna sieć) – zbiór tysięcy stron internetowych, które istnieją w zaszyfrowanej sieci i nie można ich znaleźć lub odwiedzić przy użyciu tradycyjnych przeglądarek. Niektóre są publicznie widoczne, ale wykorzystują narzędzia anonimowości takie jak Tor i I2P, aby ukryć swój adres IP. Oznacza to, że każdy może odwiedzić witrynę sieci Web tego typu, ale ustalenie, gdzie jest ona hostowana – lub przez kogo – może być bardzo trudne. Dark web jest najczęściej używany do nielegalnych praktyk, np. sprzedaży narkotyków, broni palnej, pornografii dziecięcej, umożliwia jednak również anonimowe informowanie o nieprawidłowościach i chroni użytkowników przed inwigilacją i → c e n z u r ą [t. 1].

W 2015 r. Komitet ds. Zwalczania Fałszerstw – organ jednej z Podkomisji Kongresu USA – przygotował raport *Fałszerstwo w Ciemnej Sieci* (*Anticounterfeiting on the Dark Web*), który opisał 3 części sieci internetowej. Pierwsza z nich to *surface web* – jest to część sieci znana większości użytkowników, składają się na nią wszystkie strony internetowe, które mogą być indeksowane przez typowe wyszukiwarki. Jako drugą część wyróżniono → d e e p w e b (głęboką sieć), czyli część internetu ukrytą przed konwencjonalnymi wyszukiwarkami np. poprzez szyfrowanie; zbiór nieindeksowanych stron internetowych; zawiera wszystko, do czego nie ma dostępu wyszukiwarka. Jako trzecią wskazano dark web – to mała część deep webu, która jest celowo ukryta i niedostępna dla standardowych przeglądarek internetowych. Kiedy serwisy informacyjne błędnie opisują dark web jako 90% internetu, mylą go z deep webem – to ciemna sieć jest częścią głębokiej sieci. Deep web zawiera dark web, ale poza tym obejmuje również wszystkie bazy danych użytkowników, strony webmail, fora internetowe wymagające wcześniejszej rejestracji itp.

Większość stron dark webu korzysta z oprogramowania Tor, wywodzącego się z amerykańskich prac badawczych w zakresie technologii obronnych. Jest ono zbudowane w oparciu o kod źródłowy popularnej przeglądarki Firefox zmodyfikowany tak, aby umożliwić użytkownikom

anonimowe przeglądanie sieci, blokując lub odradzając użytkownikowi czynności, które mogą ujawnić jego tożsamość (np. zmianę rozmiaru okna przeglądarki).

Oprogramowanie Tor szyfruje ruch sieciowy w warstwach i przekierowuje ten ruch dookoła sieci przez losowo wybrane komputery na całym świecie, z których każdy usuwa pojedynczą warstwę szyfrowania przed przekazaniem danych do następnego komputera w sieci. Teoretycznie uniemożliwia to szpiegom – nawet tym, którzy kontrolują jeden z tych komputerów w zaszyfrowanym łańcuchu – dopasowanie pochodzenia ruchu do miejsca przeznaczenia. Kiedy internauci uruchamiają przeglądarkę Tor, odwiedzane przez nich strony nie mogą łatwo zidentyfikować adresu IP użytkownika sieci. Tor zapewnia anonimowość także samym stronom internetowym i serwerom. Serwery skonfigurowane do odbierania połączeń przychodzących tylko przez Tor są nazywane „ukrytymi usługami". Aby odwiedzić witrynę w dark webie, która używa szyfrowania Tor, użytkownik sieci musi używać oprogramowania Tor. Tak jak adres IP użytkownika końcowego jest odbijany przez kilka warstw szyfrowania, aby wyglądać na inny adres IP w sieci Tor, tak też działa adres IP witryny. Dzięki temu strony w ciemnej sieci mogą być odwiedzane przez każdego, ale bardzo trudno jest ustalić, kto stoi za tymi witrynami. Przeglądarka Tor i witryny dostępne tylko dla niej są wykorzystywane przez użytkowników → d a r k n e t u i mogą być identyfikowane poprzez domenę (pseudodomenę) „.onion". Dostęp do dark webu jest możliwy z poziomu sieci darknet, składającej się z wielu rozproszonych, anonimowych węzłów.

Tożsamości i lokalizacje użytkowników darknetu pozostają anonimowe i nie można ich śledzić z powodu warstwowego systemu szyfrowania. Technologia szyfrowania darknetu kieruje dane użytkowników przez dużą liczbę pośrednich serwerów, co chroni tożsamość użytkowników i gwarantuje anonimowość. Przesyłane → i n f o r m a c j e mogą zostać odszyfrowane tylko przez kolejny węzeł w schemacie, który prowadzi do węzła wyjściowego. Skomplikowany system uniemożliwia odtworzenie ścieżki węzła i odszyfrowanie informacji warstwa po warstwie. Ze względu na wysoki poziom szyfrowania strony internetowe nie są w stanie śledzić geolokalizacji i IP swoich użytkowników, a użytkownicy nie są w stanie uzyskać tych informacji o hoście. Komunikacja między użytkownikami

darknetu jest wysoce zaszyfrowana, co pozwala im na poufne porozumiewanie się, blogowanie i udostępnianie plików.

Gdy użytkownicy sieci uruchamiają Tora, wszystkie odwiedzane witryny nie mogą łatwo zobaczyć ich adresu IP. Ale strona internetowa, która sama uruchamia Tora – co jest znane jako usługa ukryta Tora – może być odwiedzana tylko przez użytkowników Tora. Fakt, że adresy IP tych witryn są ukryte, niekoniecznie oznacza jednak, że są one tajne. Ukryte usługi Tora, takie jak witryny sprzedaży narkotyków, miały setki tysięcy stałych użytkowników. W lipcu 2017 r. R. Dingledine, jeden z trzech założycieli projektu Tor, powiedział, że Facebook jest największą ukrytą usługą. Dark web zawiera tylko 3% ruchu w sieci Tor.

Nie wszystkie ciemne strony używają Tora. Niektóre korzystają z podobnego narzędzia o nazwie I2P (Invisible Internet Project), np. Silk Road (Jedwabny Szlak), który był globalnym rynkiem nielegalnych usług i przemytu, głównie narkotyków. Serwis został założony na początku 2011 r. i przez jakiś czas był najpopularniejszym spośród czarnorynkowych serwisów internetowych, z którym przez lata walczyły amerykańskie organy ścigania. Za jego pośrednictwem handlowano głównie narkotykami. Można było jednak kupić tam także broń czy zlecić zabójstwo. Z czasem Silk Road rozrósł się do ogromnych rozmiarów. Zaczęto go nazywać „narkotykowym Amazonem". Dostawcy nielegalnych substancji operowali w ponad 10 krajach na całym świecie. Od momentu uruchomienia witryny w styczniu 2011 r. ponad 100 tys. użytkowników wykorzystało ją do zakupu nielegalnych towarów, w tym narkotyków o wartości 1,2 mld USD. Szacuje się, że łączny przychód wyniósł 9,5 mln bitcoinów (wg średniego kursu z 2013 r. to równowartość ok. 3 mld USD). 2 października 2013 r., w bibliotece publicznej w San Francisco, agenci federalni zatrzymali administratora internetowego Silk Road, gdy był zalogowany do witryny za pośrednictwem tymczasowo zaszyfrowanego połączenia Tor, wykorzystując sieć WiFi biblioteki. Okazał się nim 29-letni R. Ulbricht, kryjący się pod pseudonimem DPR (Dread Pirate Roberts). Został oskarżony o pranie brudnych pieniędzy, piractwo komputerowe, umożliwienie handlu narkotykami oraz o zlecenie 6 zabójstw, w lutym 2015 r. został skazany na dożywocie w więzieniu za różne przestępstwa bez możliwości wcześniejszego zwolnienia.

W październiku 2013 r. została również zamknięta giełda, ale Silk Road (v. 2.0) reaktywowano w ciągu miesiąca od zamknięcia jego pierwszej odsłony. FBI potrzebowało kolejnego roku na odnalezienie kolejnego administratora i serwerów.

Na początku listopada 2014 r. skoordynowane działania FBI i → Europolu, znane jako operacja Onymous, zajęły dziesiątki ukrytych usług Tora, w tym 3 z 6 najpopularniejszych rynków narkotykowych w ciemnej sieci. Większość wymienianych towarów była nielegalna. Sposób, w jaki zlokalizowano te miejsca, pozostaje tajemnicą. Niektórzy analitycy → bezpieczeństwa spekulują, że rządowi → hakerzy wykorzystali tzw. ataki „odmowy usługi", które zalewają przekaźniki Tora niechcianymi danymi, aby zmusić witryny docelowe do korzystania z kontrolowanych przez nie przekaźników Tora, śledząc w ten sposób ich adresy IP. Mogli również zmienić administratorów w informatorów lub znaleźć inne podatne na atak luki w witrynach docelowych. Może to oznaczać, iż darknetowa implementacja sieci Tor zawiera kilka luk w zabezpieczeniach lub błędy w konfiguracji, które umożliwiają zdemaskowanie jej użytkowników. W 2016 r. specjaliści z firmy Intelliagg dokładniej sprawdzili, co kryje się w sieci Tor. Okazało się, że znajduje się tam maksymalnie 30 tys. stron o rozszerzeniu .onion (przypisanym do darknetu), ale tylko połowa z nich zawiera treści, które są zakazane prawem.

Dark web po raz pierwszy trafił na pierwsze strony gazet w sierpniu 2015 r., po tym jak doniesiono, że 10 GB danych skradzionych z Ashley Madison, serwisu randkowego i społecznościowego skierowanego do osób będących w związkach małżeńskich lub partnerskich, zostało umieszczonych w dark webie. Hakerzy ukradli dane i zagrozili, że przekażą je do sieci, jeśli witryna nie zostanie zamknięta. Później użytkownicy Ashley Madison otrzymali listy żądające zapłaty 2500 USD w bitcoinach lub ujawnienia niewierności. W ten sposób ciemna sieć wzbudziła ogromne zainteresowanie naukowców i rządów, starających się ujawnić tożsamość uczestników tych lukratywnych, ale nielegalnych rynków. Tradycyjne metodologie i techniki śledcze sprawdzające się w sieci okazały się nieudolne w demaskowaniu tych uczestników rynku.

W marcu 2015 r. rząd Wielkiej Brytanii uruchomił specjalną jednostkę ds. → cyberprzestępczości [t. 1], aby zająć się dark webem, ze

szczególnym naciskiem na zwalczanie poważnych przestępstw i pornografii dziecięcej. National Crime Agency (NCA) i brytyjski →wywiad [t. 4] Government Communications Headquarters (GCHQ) tworzą razem Joint Operations Cell (JOC).

Chociaż ciemna sieć jest najczęściej kojarzona ze sprzedażą narkotyków, broni, fałszywych dokumentów i pornografią dziecięcą – a wszystkie te mające swoich klientów branże rzeczywiście korzystają z usług Tora – nie wszystko w mrocznej sieci jest tak „ciemne". Dziennikarze korzystają z ciemnej sieci, aby chronić anonimowość swoich źródeł, a inni używają ciemnej sieci tylko dlatego, że mocno wierzą w swoje prawo do prywatności. Jedną z pierwszych wysokoprofilowych stron dark webu była usługa ukryta Tora stworzona przez WikiLeaks w celu akceptowania wycieków z anonimowych źródeł. Ten pomysł został od tego czasu dostosowany do narzędzia o nazwie SecureDrop, oprogramowania, które integruje się z ukrytymi usługami Tora, tak aby każda organizacja informacyjna mogła otrzymywać anonimowe zgłoszenia. Wielu aktywistów i dysydentów politycznych używa dark webu do swobodnego wyrażania swoich opinii lub jako sposób na wymianę i otrzymywanie informacji bez cenzury bądź kontroli. Sieć może służyć do ochrony urzędników przed identyfikacją i hakowaniem przez przeciwników. Może być też używana do prowadzenia tajnej lub ukrytej operacji sieci komputerowej, takiej jak likwidacja, atak typu „odmowa usługi" lub przechwycenie komunikacji. Nawet Facebook uruchomił wersję swojej strony w ciemnej sieci, aby „ułatwić dostęp do witryny z krajów, które ograniczają usługę, takich jak Chiny i Iran". Ma ona na celu lepszą obsługę użytkowników, którzy odwiedzają witrynę, używając Tora do unikania nadzoru i cenzury.

Olga Wasiuta

Anticounterfeiting Committee – U.S. Subcommittee Public Awareness Task Force, *Report: Anticounterfeiting on the Dark Web*, 13.04.2015, Inta.org (dostęp 31.07.2020); arma, *Did the FBI Pay a University to Attack Tor Users?*, 11.11.2015, Blog.TorProject.org (dostęp 31.07.2020); O. Catakoglu, M. Balduzzi, D. Balzarotti, *Attacks Landscape in the Dark Side of the Web*, [w:] *Proceedings of the Symposium on Applied Computing*, ACM, New York 2017; M. Egan, *What is the Dark Web, What's on it*

& How to Access it, 25.10.2019, TechAdvisor.co.uk (dostęp 31.07.2020); K. Finklea, *Dark Web*, Congressional Research Service, 2017; A. Greenberg, *Hacker Lexicon: What Is the Dark Web?*, 19.11.2014, Wired.com (dostęp 31.07.2020); D. Hayes, J. Cardon, F. Cappa, *A Framework for More Effective Dark Web Marketplace Investigations*, „Information (Switzerland)" 2018, vol. 9, no. 186; G.F. Hurlburt, *Shining Light on the Dark Web*, „Computer" 2017, no. 50 (4); R. Jansen, T. Vaidya, M. Sherr, *Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor*, [w:] *Proceedings of the 28th USENIX Security Symposium*, USENIX Association, Berkeley 2019; T. Leżoń, *Darknet i deep web. Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, 27.04.2015, TVN24.pl (dostęp 31.07.2020); A. Nastiti, A. Wimmer, *Darknet, Social Media and Extremism: Addressing Indonesian Counter terrorism on the Internet*, „Deutsches Asienforschungszentrum Asian Series Commentaries" 2015, vol. 30; O. Wasiuta, *Dark Web*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J.M. Porup, *What is the Tor Browser? How It Works and how It Can Help You Protect Your Identity Online*, 12.07.2018, CSOOnline.com (dostęp 31.07.2020); T. Shim, *How to Access the Dark Web: Browsing Dark Web, TOR Browser, and .Onion Websites*, 10.04.2019,WebHostingSecretRevealed.net (dostęp 31.07.2020); J. Solomon, *The Deep Web Vs. The Dark Web*, 11.11.2015, Dictionary.com (dostęp 31.07.2020); M. Szpunar, *Imperializm kulturowy internetu*, Instytut Dziennikarstwa, Mediów i Komunikacji Społecznej Uniwersytetu Jagiellońskiego, Kraków 2017; M.P. Zillman, *Deep Web Research and Discovery Resources 2019*, 21.01.2019, LLRX.com (dostęp 31.07.2020).

DEBUNK (ang. demaskować, witryny: Debunk.eu, Demaskuok.lt w jęz. lit.) – to unikalna ogólnokrajowa litewska inicjatywa, która powstała w 2015 r., a jej celem jest monitorowanie i dementowanie → d e z i n f o r m a c j i. Debunk łączy litewskie jednostki → k o m u n i k a c j i s t r a t e g i c z n e j i podmioty → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4] – w tym media, dziennikarzy i wolontariuszy, a także podmioty biznesowe i medialne – w jednym celu: aby społeczeństwo było bardziej odporne na zorganizowane kampanie dezinformacyjne i ich obalanie, zanim fałszywe, wprowadzające w błąd lub niszczące zaufanie do państwa i jego demokratycznych instytucji informacje rozprzestrzenią się w kraju. Z inicjatywą współpracuje także litewska społeczność → e l f ó w, naukowcy oraz doświadczeni informatycy. Wg organizatorów docierają one do 90% mieszkańców Litwy. Platforma jest krokiem w kierunku zwalczania wyzwań dezinformacyjnych z zagranicy,

jednak obserwatorzy twierdzą, że pomaga ona społeczeństwu radzić sobie z rosnącym strumieniem → i n f o r m a c j i z samego kraju. Inicjatywa została sfinansowana i zrealizowana w ramach projektu Digital Innovation Foundation firmy Google oraz redakcji największego w regionie portalu informacyjnego Delfi Baltic. Na czele Debunk.eu stoi V. Daukšas.

Strona wykorzystuje zautomatyzowany system → s z t u c z n e j i n t e l i g e n c j i [t. 4] do skanowania i analizy ok. 20 tys. artykułów dziennie w 3 językach w ciągu 2 minut od ich publikacji, w tym w mediach rosyjskich i litewskich, korzysta z ponad 1 tys. źródeł prasowych, biorąc pod uwagę podejrzane słowa kluczowe, zgłasza artykuły z określonymi słowami kluczowymi i wskazuje potencjalne źródło rozprzestrzeniania się dezinformacji, w tym również takich, że Litwa jest krajem upadłym lub jest ponownie zajęta przez → N A T O [t. 3]. Wolontariusze filtrują treści oznaczone przez system, odczytują materiały i oceniają potencjalne → z a g r o ż e n i e [t. 4]. Zgłoszone informacje docierają do dziennikarzy wraz z konkretnymi komentarzami i wiedzą wolontariuszy, którzy posiadają wiedzę na tematy poruszane przez → p r o p a g a n d ę [t. 3], takie jak technologia, polityka lokalna i konflikt w Ukrainie. Inicjatywa Debunk.eu obnażyła np. nieprawdziwość doniesień o testach → b r o n i b i o l o g i c z n e j [t. 1] w krajach bałtyckich, obiektach pozaziemskich zestrzelonych na Litwie czy też fikcyjność historii → ż o ł n i e r z a [t. 4] NATO, który zabił rowerzystę.

Litewscy dziennikarze publikują analizy obnażające wyprodukowane przez rosyjskie media → f a k e n e w s y. Inicjatywa ta jest również otwarta dla czytelników portalu Delfi. Na głównej podstronie działu znajduje się formularz, w którym można zgłosić dany problem dziennikarzom lub poinformować o nowym fake newsie. Każdy użytkownik strony może sprawdzić, czy news, na który natknął się w sieci, został uznany za manipulację lub fake. Działanie witryny skupia się przede wszystkim na fake newsach istotnych z punktu widzenia państwa (a nie np. komercyjnych). Przykładami takich istotnych wiadomości mogą być fałszywe twierdzenia rosyjskich mediów państwowych o porwaniu 6 rosyjskich dzieci przez litewskie siły specjalne, aby zmusić rodziców do współpracy przeciwko Rosji, lub całkowicie nieprawdziwe informacje, wg których Łotwa wzniosła obozy koncentracyjne dla etnicznych Rosjan.

Liczba ludności rosyjskojęzycznej na Litwie wynosi zaledwie 6% ogółu, mniej niż w Estonii i na Łotwie. Jednak 8% ankietowanych Litwinów twierdzi, że poparło → a n e k s j ę [t. 1] Krymu. Ok. 97% ludzi ogląda telewizję codziennie; z tej liczby 14% to odbiorcy rosyjskich stacji, z których wiele jest faktycznie zarejestrowanych w krajach europejskich i podlega przepisom UE dotyczącym transmisji. Popularność mediów rosyjskich jest większa wśród starszych pokoleń Litwinów, którzy dorastali z sowieckimi mediami i czują się lepiej, będąc informowani w swoim podstawowym języku. T. Kvedaras, attaché prasowy w litewskim Ministerstwie Spraw Zagranicznych, powiedział, że jego 85-letnia babcia nadal woli NTV lub Channel One od jakiejkolwiek stacji w języku litewskim.

Litwini starają się na różne wydarzenia reagować natychmiast. Kiedy na Litwie rosyjską firmę Lukoil przemianowano na Vijada, żeby zmylić społeczeństwo, w odpowiedzi natychmiast opublikowano i rozpowszechniono w → m e d i a c h s p o ł e c z n o ś c i o w y c h [t. 3] zdjęcia z podpisem „To ta sama kakaszka, tylko z drugiej strony". Skuteczność takich memów była dość wysoka: dzięki humorowi można wiele przekazać społeczeństwu. Kiedy firma Adidas zaczęła produkować koszulki z symbolami ZSRR, Litwini uruchomili kampanię „Stop! Adidas", która okazała się bardzo udana, także w globalnej skali. W 19 krajach opublikowano 116 artykułów na ten temat, w tym 55 artykułów na Ukrainie, co zmusiło przedsiębiorstwo do oficjalnego zaprzestania takiej produkcji.

We wrześniu 2018 r. litewską inicjatywę Demaskuok.lt po raz pierwszy przedstawiono instytucjom i państwom członkowskim UE. Spotkanie z Europejską Służbą Działań Zewnętrznych i zagranicznymi dyplomatami odbyło się w Stałym Przedstawicielstwie Litwy przy UE w Brukseli. Skala problemu dezinformacji została również omówiona z europejską komisarz ds. gospodarki cyfrowej i społeczeństwa M. Gabriel. Podczas konferencji prasowej dla zagranicznych mediów lider inicjatywy Daukšas przedstawił inicjatywę Demaskuok.lt oraz możliwości zastosowania tego narzędzia w UE lub w poszczególnych krajach UE. Inicjatywa wzbudziła duże zainteresowanie instytucji UE i międzynarodowych mediów. We wnioskach uznano, że tylko wspólne media, działania pozarządowe i sektor publiczny tworzą dobrze poinformowane społeczeństwo, które może odnosić sukcesy w walce z dezinformacją.

Wykorzystując zasady niezależności, przejrzystości i skuteczności, Demaskuok.lt jest unikalną inicjatywą tego rodzaju nie tylko na Litwie, ale także prawdopodobnie na świecie. Inicjatywa krajowa Demaskuok.lt znalazła się w gronie finalistów konkursu zorganizowanego przez → Centrum Eksperckie NATO ds. Komunikacji Strategicznej [t. 1] i ambasadę USA pod koniec grudnia 2018 r. Debunk oferuje rozwiązania, które pomagają identyfikować szkodliwą zawartość wideo i zdjęć używanych do rozpowszechniania dezinformacji w sieci. Do tej pory inicjatywa została już zaprezentowana w Brukseli dyplomatom państw UE, przedstawicielom biur Komisji Europejskiej i przedstawicielom NATO, została przedstawiona także w USA w 2018 r. przy okazji spotkań Rady Atlantyckiej.

Z pomocą elfów i unikalnych narzędzi opartych na algorytmach media mogą reagować na dezinformację i manipulację w czasie rzeczywistym i skutecznie. Rozwiązania stosowane przez Debunk.eu można aplikować zarówno w instytucjach litewskich, jak i międzynarodowych, automatyzując monitorowanie mediów, zmieniając fałszywe narracje i oceniając zakres rozpowszechnienia się dezinformacji, np. w kontekście nadchodzących wyborów do Parlamentu Europejskiego czy wyborów do parlamentów krajowych.

Litwa, podobnie jak inni sąsiedzi, ukształtowana przez komunistyczną dominację w czasach sowieckich, od dawna dążyła do twardego podejścia do dezinformacji zarówno w kraju, jak i na poziomie UE. → Strategia [t. 4] Wilna jest godna uwagi ze względu na sposób, w jaki opiera się na bliskiej współpracy między różnymi grupami w społeczeństwie, takimi jak media i wojsko.

Komisja Europejska zaproponowała przyjęcie wspólnego unijnego kodu dezinformacji, wsparcie dla niezależnej sieci weryfikatorów faktograficznych i promowanie wysokiej jakości dziennikarstwa poprzez podniesienie umiejętności korzystania z mediów.

Sergiusz Wasiuta

Debunk, *Disinformation*, Debunk.eu (dostęp 10.03.2019); Embassy of the Republic of Lithuania to the United States of America and to the United Mexican States, *Lithuania shares its experience in countering disinformation*, 9.10.2018, USA.MFA.lt

(dostęp 10.03.2019); B. Gerdziunas, *Lithuania hits back at Russian disinformation*, 27.09.2018, DW.com (dostęp 10.03.2019); Lrytas, *„Demaskuok.lt" – NATO konkurso finale*, 28.11.2018, Lrytas.lt (dostęp 10.03.2019); ciż, *Demaskuok.lt pristatyta Europos Komisijos atstovybėje*, 26.09.2018, Lrytas.lt (dostęp 10.03.2019); A. Kendall-Taylor, R. Rizzo, V. Daukšas, Giedrius, *Combatting Disinformation in Lithuania*, 19.10.2018, CNAS.org (dostęp 10.03.2019); S. Wasiuta, *Debunk*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

DEEPFAKE (generowane komputerowo treści wideo, zbitka od ang. *deep learning* – głębokie uczenie – oraz *fake* – fałszywy) – to technika obróbki obrazów twarzy ludzkich oparta na działaniu →sztucznej inteligencji [t. 4]. Służy do zautomatyzowanego przez program komputerowy łączenia istniejących obrazów lub filmów oraz nakładania na siebie treści tak, aby w rezultacie wytworzyć przekonujące fotomontaże lub nagrania ze zmienionymi obrazami twarzy bohaterów. Technologia deepfake wykorzystuje sztuczną inteligencję do tworzenia lub modyfikowania odwzorowania twarzy, do tworzenia ultrarealistycznych fałszywych filmów, na których ludzie mówią i robią rzeczy, które w rzeczywistości nie się zdarzyły. Oprogramowanie do edycji zdjęć takie jak Photoshop od dawna było używane do fałszowania obrazów statycznych, jednak do niedawna trudno było edytować treści wideo bez użycia specjalistycznego oprogramowania, wysokich umiejętności i dużej ilości czasu. W związku z tym nagrania wideo często były uważane za dowód, że coś faktycznie się wydarzyło. Od innych technik manipulacji treściami wideo odróżnia deepfake jego potencjał do uzyskania wysoce realistycznych, przekonujących rezultatów.

Termin został utworzony od nazwy anonimowego użytkownika portalu Reddit o pseudonimie deepfakes, który w grudniu 2017 r. opublikował kilka filmów pornograficznych, na których twarze aktorek zostały podmienione na twarze celebrytek. Filmy typu deepfake są tworzone przez załadowanie do komputera złożonego zestawu instrukcji wraz z dużą ilością zdjęć i nagrań dźwiękowych. Następnie program komputerowy uczy się, jak naśladować i odtwarzać mimikę danej osoby, jej głos, ruchy, indywidualne maniery, intonację oraz rodzaj używanego słownictwa. Wystarczająca liczba filmów i zapisów dźwiękowych danej osoby umożliwia systemowi stworzenie nagrania z tą osobą. Bardzo często oszuści tworzący

materiały typu deepfake wykorzystują autentyczne nagrania, które łączą ze sztucznie wygenerowanym obrazem.

Nowa technologia pozwala każdemu stworzyć materiał wideo, w którym pojawiają się znane postaci, np. prezydent USA D. Trump czy wysocy rangą dyplomaci, wypowiadający się na kontrowersyjne tematy w sposób podburzający → o p i n i ę p u b l i c z n ą [t. 3]. Filmy typu deepfake zostały wykorzystane do fałszywego przedstawienia znanych polityków na portalach gromadzących treści wideo lub na czatach, np. twarz argentyńskiego prezydenta M. Macriego zastąpiła twarz A. Hitlera, w innym nagraniu twarz A. Merkel została zastąpiona twarzą Trumpa. W lipcu 2017 r. świat obiegł filmik, w którym B. Obama obrażał Trumpa. Okazało się, że byłego prezydenta USA wygenerowano w całości w aplikacji → F a k e A p p, a głosu użyczył mu komik J. Peele. Akcja miała na celu zwrócenie uwagi na problem fake newsów. W kwietniu 2018 r. Peele i J. Peretti stworzyli podróbkę, używając wizerunku Obamy do publicznego ogłoszenia o → z a g r o ż e n i a c h [t. 4] związanych z podróbkami.

W ostatnich latach technologia przetwarzania obrazu (aparaty cyfrowe, telefony komórkowe itp.) stała się wszechobecna, umożliwiając ludziom na całym świecie natychmiastowe wykonywanie zdjęć i tworzenie nagrań wideo. Odzwierciedleniem tego wzrostu liczby obrazów cyfrowych jest zdolność nawet stosunkowo niewykwalifikowanych użytkowników do manipulowania i zniekształcania przekazu mediów wizualnych. Podczas gdy wiele manipulacji jest wykonywane dla zabawy lub dla wartości artystycznej, inne służą celom takim jak → p r o p a g a n d a [t. 3] lub → d e z - i n f o r m a c j a. Ta manipulacja multimediami wizualnymi jest możliwa dzięki szerokiej dostępności zaawansowanych aplikacji do edycji obrazu i wideo, a także dzięki zautomatyzowanym algorytmom umożliwiającym edycję w sposób bardzo trudny do wykrycia nieuzbrojonym okiem lub nawet poprzez analizę z wykorzystaniem specjalistycznych narzędzi. Słowo deepfake określa wykorzystanie algorytmów uczenia maszynowego i technologii mapowania twarzy do cyfrowej manipulacji głosami, ciałami i twarzami ludzi. Technologia rozwija się w tak dużym tempie, że coraz trudniej jest stwierdzić, co jest fałszywe. Z czasem, bez odpowiedniego sprzętu, filmy deepfake staną się nie do odróżnienia od prawdziwych zdjęć czy filmów. Deepfake'i mogą być wykorzystywane również

do tworzenia fałszywych wiadomości i złośliwych oszustw. Dysponując wystarczającą ilością obrazów obu aktorów i wystarczającą ilością czasu na szkolenie komputerowe, rezultaty mogą być niezwykle przekonujące. Filmy deepfake można zidentyfikować na podstawie braku sygnałów fizjologicznych właściwych człowiekowi: oddychania, mrugania oczami, braku widocznego pulsu.

Liderzy państw demokratycznych doceniają obecnie wagę problemu, jaki niesie ze sobą możliwość tworzenia treści, w których generowane komputerowo obrazy znanych postaci życia publicznego wypowiadają bulwersujące stwierdzenia i są nie do odróżnienia od prawdziwych osób. Materiały wideo tego rodzaju są potencjalnym zagrożeniem dla →bezpieczeństwa wewnętrznego [t. 1] każdego państwa, a także mogą stać się narzędziem wpływu na wybory. Kolejny sfabrykowany skandal może zagrozić →bezpieczeństwu narodowemu [t. 1] lub wpłynąć na opinię publiczną, to pole do działania dla oszustów chcących ingerować np. w nastroje polityczne w społeczeństwie, a także nowa broń w→wojnie informacyjnej [t. 4]. Technologia ta będzie narzędziem wykorzystywanym przez państwa w celu manipulowania opinią publiczną i przeprowadzania kampanii dezinformujących, a także podkopywania wiary w obecnie istniejące instytucje.

Masowa dostępność oprogramowania do tworzenia materiałów typu deepfake ma wiele niepokojących implikacji, które trudno ignorować. Dzięki tej technologii coraz trudniejsze będzie odróżnienie prawdy od kłamstwa. Technologia deepfake jest już szeroko stosowana w fałszywych filmach pornograficznych i komediowych. Szybki postęp technologiczny może oznaczać jednak poważne konsekwencje. Realistyczne filmy deepfake można również wykorzystywać przy próbach szantażu, linkach →phishingowych [t. 3] i oszustwach służących wymuszeniu. Przy minimalnym nakładzie pracy mogą także dostarczać przestępcom narzędzi do tworzenia realistycznych, trudnych do weryfikacji, przynajmniej bez dogłębnej analizy, nagrań wideo, na których osoby mogą podszywać się pod kogoś innego, prowadząc do oszustwa i unikając wyegzekwowania prawa. Mogłyby one zostać wykorzystane np. do wplątania niewinnych ludzi w zbrodnie, a w postępowaniu cywilnym te sfałszowane filmy mogą być wykorzystywane do przeprowadzania wszelkiego rodzaju oszukańczych roszczeń.

To narzędzie ma jednak znacznie większe możliwości, co właśnie wykorzystują Chińczycy. W listopadzie 2018 r. chińska państwowa telewizja Agencji Informacyjnej Xinhua stworzyła wygenerowanego komputerowo prezentera, który poprowadzi wieczorne wiadomości (jego sylwetka była wzorowana na pracowniku agencji, Z. Zhao). Xinhua planuje stworzenie mediów, które będą prowadzone na okrągło przez komputerowych prezenterów, a wiadomości widz będzie mógł usłyszeć w dowolnym języku. Treści, które ma przedstawiać cyfrowy prezenter, wprowadzane są do pamięci oprogramowania deepfake, a ruch jego warg jest synchronizowany ze słowami wypowiadanymi przez syntezator mowy. Stało się to, czego wielu obawiało się od dawna. Pierwszy raz w historii telewizji wiadomości ze świata relacjonuje prezenter, który został sztucznie wytworzony za pomocą technologii deepfake.

Technologia tworzenia zmanipulowanych wideo nie jest jeszcze doskonała i wytrawne oko dostrzeże modyfikacje. Mechanizm konstruowania nagrań typu deepfake jednak cały czas się rozwija i za chwilę odbiorca być może nie zauważy, że materiał filmowy jest fałszywy.

W USA aktywnie rozwijana jest technologia służąca identyfikacji filmów typu deepfake. Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (Defense Advanced Research Projects Agency, DARPA) rozpoczęła w 2016 r. projekt MediFor (ang. Media Forensics, media śledcze), którego celem jest opracowanie technologii do automatycznej oceny integralności zdjęć lub filmów i uczynienie jej częścią platformy wymiany materiałów pomiędzy użytkownikami końcowymi. W założeniach platforma MediFor automatycznie będzie wykrywać manipulacje, podawać szczegółowe informacje o tym, jak owe manipulacje zostały wykonane, a także oceniać ogólną integralność obrazów wizualnych, ułatwiając użytkownikom podjęcie decyzji o wykorzystaniu jakichkolwiek wątpliwych zdjęć lub filmów.

Opracowaniem oprogramowania do weryfikacji autentyczności mediów zajmuje się także utworzona w 2017 r. amerykańska → A I F o u n d a t i o n [t. 1]. Celem pierwszego produktu firmy o nazwie Reality Defender jest identyfikowanie oszustw i złośliwej zawartości poprzez wykorzystanie uczenia maszynowego oraz ludzkiego umiarkowania i rozsądku. Naukowcy zapraszają użytkowników do wysyłania im fałszywych materiałów do

tworzenia spersonalizowanej sztucznej inteligencji, z której mogą korzystać wszyscy ludzie. W tym celu firma utworzyła własną Globalną Radę ds. Sztucznej Inteligencji (Global AI Council), która stara się przewidywać i przeciwdziałać negatywnym skutkom wykorzystania sztucznej inteligencji.

Olga Wasiuta, Sergiusz Wasiuta

J. Booth, A. Roussos, A. Ponniah i in., *Large Scale 3D Morphable Models*, „International Journal of Computer Vision" 2018, vol. 126, no. 2; A. Dodge, L. House, E. Johnstone, *Using Fake Video Technology To Perpetrate Intimate Partner Abuse*, 25.04.2018, WithoutMyConsent.org (dostęp 15.03.2019); W. Gogołek, *Komunikacja sieciowa. Uwarunkowania, kategorie i paradoksy*, ASPRA-JR, Warszawa 2010; R. Heartfield, G. Loukas, *Protection Against Semantic Social Engineering Attacks*, [w:] *Versatile Cybersecurity. Advances in Information Security*, M. Conti, G. Somani, R. Poovendran (eds.), Springer, Cham 2018; H. Kim, P. Garrido, A. Tewari i in., *Deep Video Portraits*, „ACM Transactions on Graphics" 2018, vol. 37, no. 4; D. Rivera, A. García, M.L. Martín-Ruiz i in., *Secure Communications and Protected Data for a Internet of Things Smart Toy Platform*, „IEEE Internet of Things Journal" 2019, vol. 6, no. 2; S. Suwajanakorn, S.M. Seitz, I. Kemelmacher-Shlizerman, *Synthesizing Obama: Learning Lip Sync from Audio*, „ACM Transactions on Graphics" 2017, vol. 36, no 4; A. Tewari, M. Zollhöfer, H. Kim i in., *MoFA: Model-based Deep Convolutional Face Autoencoder for Unsupervised Monocular Reconstruction*, [w:] *2017 IEEE International Conference on Computer Vision (ICCV)*, Wenecja 2017; J. Thies, M. Zollhöfer, M. Stamminger i in., *FaceVR: Real-Time Facial Reenactment and Eye Gaze Control in Virtual Reality*, „ACM Transactions on Graphics" 2018, vol. 37, iss. 2; O. Wasiuta, *Deepfake*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 3; Y. Zhu, R. Bridson, D.M. Kaufman, *Blended cured quasi-newton for distortion optimization*, „ACM Transactions on Graphics" 2018, vol. 37, iss. 4.

DEEP WEB (także ang. *invisible web* – niewidzialna sieć, ang. *hidden web* – ukryta sieć), ukryty internet, głęboka sieć – obszar globalnej sieci, który nie jest indeksowany, a więc także nie jest wyszukiwany przez standardowe wyszukiwarki internetowe (ang. *search engines*); to część sieci ukryta przed konwencjonalnymi wyszukiwarkami, np. poprzez szyfrowanie; zbiór nieindeksowanych stron internetowych.

Termin *invisible web* („niewidzialna sieć") po raz pierwszy został użyty przez J. Ellsworth w 1994 r. na określenie tych zasobów sieciowych, których wyszukiwarki nie mogą lub nie chcą indeksować i które ostatecznie są dla użytkowników niewidzialne i niedostępne. Duży wkład w rozwój badań nad zagadnieniem wniósł G. Price – bibliotekarz i szef Online Information Resources w serwisie Ask.com. Stworzył również bezpłatną, dostępną online listę zawierającą wykaz rankingów firm, wybitnych ludzi i ich zawodowych osiągnięć, prowadzoną od 1998 r. Za pośrednictwem jego serwisu DirectSearch można było dotrzeć do wielu zasobów deep webu. Co ważne, ok. 95% głębokiej sieci stanowią zasoby, do których dostęp jest bezpłatny, a blisko połowa to specjalistyczne, dziedzinowe bazy danych – niezwykle cenne w poszukiwaniach bibliograficznych.

Deep web to pojęcie złożone. Można w nim wyróżnić 2 kategorie zasobów.

- Pierwsza kategoria to każda → i n f o r m a c j a trudna do uzyskania poprzez standardowe wyszukiwanie. Może to obejmować posty na Twitterze lub Facebooku, linki „schowane" w wielu warstwach lub wyniki, które znajdują się tak daleko w standardowych wynikach wyszukiwania, że typowi użytkownicy nigdy ich nie znajdą.
- Druga kategoria to ogromne repozytorium informacji, które nie są dostępne dla standardowych wyszukiwarek. Składa się z treści znalezionych na stronach internetowych, w bazach danych i innych źródłach. Często są one dostępne tylko za pośrednictwem niestandardowego zapytania skierowanego do poszczególnych stron internetowych, do których nie można dotrzeć za pomocą prostego wyszukiwania powierzchniowego. Deep web nie znajduje się w jednym miejscu. Składa się zarówno z treści ustrukturyzowanych, jak i niestrukturalnych, których ogromna ilość znajduje się w bazach danych.

Zawartość głębokiej sieci jest ogromna – jak szacuje firma Bright Planet, ok. 500 razy większa niż ta widoczna dla konwencjonalnych wyszukiwarek – i o znacznie wyższej jakości niż sieć powierzchniowa. Ukryty internet w dużej mierze składa się z niezwykle cennych i użytecznych źródeł informacji praktycznej i naukowej. Jak podkreśla N. Pamuła-Cieslak, mają one tę przewagę nad dokumentami widzialnego internetu

(ang. *surface web*), że w dużej części pozostają pod stałą kontrolą merytoryczną, faktograficzną, językową oraz bibliograficzną. Dzieje się tak dlatego, że powstają z inicjatywy lub przy współudziale ekspertów dziedzinowych. Gwarantuje to użytkownikom wiarygodność zdobytych w ten sposób informacji i danych. Aby dotrzeć do zasobów ukrytego internetu, należy zastosować pewne → s t r a t e g i e [t. 4] wyszukiwawcze – nie wystarczy tu skorzystać z jednego prostego narzędzia, jakim jest wyszukiwarka. Aby zastosować owe strategie, należy wiedzieć, że są one ściśle związane z rodzajem poszukiwanych źródeł.

Korzystając z internetu, mamy do dyspozycji ok. 1,5 mld zindeksowanych stron internetowych. Ta liczba robi wrażenie, ale to tylko wierzchołek góry lodowej – ok. 3–4% zawartości całej sieci. Reszta internetu kryje się pod powierzchnią na dynamicznie generowanych stronach, których nie można znaleźć poprzez standardowe wyszukiwarki. Są one dla nich po prostu niewidoczne, ponieważ stanowią sieć niezindeksowaną. Roboty wyszukiwarek nie docierają do większości zasobów zamieszczonych w głębokiej sieci, chociaż ok. 95% z nich to publicznie dostępne informacje. Zasoby sieci, które nie są indeksowane, powiększają się gwałtownie i przyjmują przeważnie postać baz danych – ponad połowa niewidocznej sieci znajduje się w bazach danych specjalistycznych. Warto dodać, że twórcy wyszukiwarek opracowują coraz lepsze algorytmy wyszukiwania, co powoduje, że zasoby widzialnego internetu i głębokiej sieci coraz bardziej się przenikają. Obecnie jesteśmy jednak dopiero na początku tej drogi, która ma na celu zindeksowanie jak największej części zasobów.

Deep web nie jest jednorodny, jego zawartość można łatwo zdefiniować. Zasoby te, ze względu na swoją rozległość, treść i uwarunkowania techniczne, są bardzo heterogeniczne. C. Sherman i G. Price proponują następującą typologię wg kryteriów podobnego typu i formatu dokumentów, podobnych problemów związanych z dotarciem do nich, podobnych sposobów ich znajdowania (strategii wyszukiwawczych):

- sieć nieprzezroczysta (ang. *the opaque web*) – zaliczają się do niej te zasoby internetowe, które bez trudu mogą być indeksowane przez wyszukiwarki, ale z kilku powodów indeksowane nie są i dlatego znajdują się w obszarze deep webu; tymi powodami są: „głębokość" ich znajdowania się w Internecie, częstotliwość przeszukiwania

sieci, maksymalna liczba rezultatów wyszukiwania w rankingu odpowiedzi, nieobecne w hipertekście adresy URL;

- sieć zasobów prywatnych (ang. *the private web*) – zasoby prywatne mogą być zaindeksowane przez wyszukiwarki, coś jednak sprawia, że indeksowane nie są; przyczynami tego mogą być: hasło zabezpieczające stronę (w tym przypadku mechanizm skanujący nie ma do niej dostępu i nie może zindeksować jej zawartości), użycie przez autora strony pliku o nazwie robots.txt w katalogu, w którym witrynę fizycznie umieszczono na serwerze (taki plik umieszcza się celowo, by określić, które strony i pliki mogą być indeksowane przez wyszukiwarki); zasoby znajdujące się w sieci prywatnej zwykle zawierają treści, które interesują osoby znające zarówno hasło, jak i adres konkretnej witryny;
- sieć zastrzeżona (ang. *the proprietary web*) – zasoby internetu dostępne tylko dla tych użytkowników, którzy uzyskali zgodę na ich przeglądanie i wykorzystywanie; tego typu witryny wymagają rejestracji użytkownika, można mówić o bezpłatnej i komercyjnej części sieci zastrzeżonej, nawet zasoby bezpłatne są jednak niedostępne dla wyszukiwarek (roboty nie mają możliwości technicznych przejścia przez proces rejestracyjny, polegający zwykle na odpowiadaniu na pytania zawarte w formularzu – podaniu danych osobowych niezbędnych do identyfikacji użytkownika, określeniu własnych preferencji); najrozleglejszą częścią sieci zastrzeżonej są komercyjne systemy płatnej rejestracji, oferujące dostęp do baz danych, które w większości zostały stworzone jeszcze przed powstaniem sieci WWW, potencjalnie udostępniane odbiorcom;
- prawdziwie ukryty internet (ang. *truly invisible web*) – zasoby, które nie są skanowane i indeksowane przez wyszukiwarki z powodów technicznych i technologicznych. Takie postawienie problemu jest jednak nie do końca słuszne, gdyż na bieżąco powstają nowe, coraz bardziej zaawansowane technicznie wyszukiwarki, starające się indeksować choć część zasobów należących dotychczas do prawdziwie ukrytego internetu, a i te istniejące dotychczas starają się nadążać w tym względzie za konkurencją.

Z punktu widzenia przeciętnego użytkownika w deep webie znajduje się wszystko to, co nie pojawia się na pierwszej stronie rezultatów wyszukiwania wiodących serwisów (Google), czego nie ma w newsfeedzie na portalach społecznościowych (Facebook). Cały ruch sieciowy, czyli wszystkie dane, jest wielokrotnie szyfrowany w momencie przejścia przez poszczególne węzły. Ponadto żaden węzeł sieciowy nie zna ani źródła ruchu, ani jego punktu docelowego, ani zawartości. Sprawia to, że anonimowość jest na wysokim poziomie oraz w typowych warunkach niemal niemożliwe jest stwierdzenie, kto w rzeczywistości stoi za daną aktywnością sieciową. Cała zawartość jest przechowywana w różnych systemach o różnych strukturach. Deep web zawiera mnóstwo danych oraz bogactwo możliwości, m.in.:

- zasoby nieindeksowane przez uniwersalne wyszukiwarki, zwłaszcza Google – z różnych powodów, w tym technicznych (błędne metadane, czas działania, nietypowe formaty itp.), ale też związanych z polityką wyszukiwarek lub właścicieli serwisów WWW;
- zasoby indeksowane, do których nie tak łatwo dotrzeć, których odnalezienie i wykorzystanie wymaga rozwiniętej strategii wyszukiwawczej;
- wewnętrzne strony największych firm, stowarzyszeń i organizacji handlowych;
- dokumenty w nietypowych formatach, np. skompresowane;
- serwisy WWW zabezpieczone hasłem, np. fora, intranety (szkół, uczelni i uniwersytetów);
- listy dyskusyjne wymagające zalogowania się;
- serwisy WWW, do których nie prowadzą odsyłacze z innych witryn;
- strony wyłączone z procesu indeksacji przez twórców, czyli takie, których autorzy zabronili robotom indeksowania ich treści;
- treści generowane dynamicznie, w czasie rzeczywistym, np. w odpowiedzi na zapytanie użytkownika;
- zasoby *de facto* indeksowane przez wyszukiwarki uniwersalne, ale pojawiające się na odległych miejscach na liście wyników wyszukiwania (aspekt algorytmów rankingowych) albo takie, których odnalezienie wymaga zaawansowanej strategii wyszukiwawczej;

- zawartość komercyjnych baz danych, czasopism, wypożyczalni online itd., wymagających dokonania rejestracji albo subskrypcji;
- zawartość publicznie dostępnych baz danych, archiwów i repozytoriów typu Open Access, bibliotek cyfrowych, katalogów bibliotecznych itp.;
- źródła, do których dociera się dzięki poleceniom innych;
- bazy danych tworzone z reguły przez podmioty rządowe lub naukowe, w których wyszukiwanie za pomocą ich własnych interfejsów (a nie interfejsu Google czy innej wyszukiwarki globalnej) jest o wiele bardziej efektywne i których zawartość jest uważana za wiarygodną;
- dane – badawcze, statystyczne i in. oraz zbiory takich danych;
- grafiki, multimedia – a właściwie ich zawartość;
- pełne teksty artykułów i książek;
- zawartość portali społecznościowych.

Wspólne jest to, że informacje w nich zawarte nie są przeznaczone do konsumpcji publicznej. Właściciele treści mogą dołożyć wszelkich starań, aby były niedostępne, a także zapewnić, że nie pojawią one się w wynikach wyszukiwania.

Przyczyny istnienia deep webu to:

- polityka i sposób działania wiodących serwisów WWW, zwłaszcza wyszukiwarek globalnych;
- postępowanie dostawców treści/zasobów informacyjnych – dostęp restrykcyjny, w tym komercyjny;
- brak kompetencji cyfrowych/informacyjnych użytkowników (ang. *digital literacy*/*information literacy*);
- zasoby nieindeksowane i/lub nieudostępniane przez Google.

Warto zauważyć, że zawartość deep webu nie zawsze jest nielegalna, w jego obszarze istnieje wiele działań pozostających całkowicie w ramach prawa. Można tu wyróżnić np.:

- → media społecznościowe [t. 3], blogi, czaty głosowe;
- międzynarodowe gry w stylu turniejowym, takie jak szachy i backgammon (tryktrak);
- grupy typu „koniec świata”;
- kluby książki, fankluby, kluby gier wideo;

- ukryte odpowiedzi – popularna wersja Yahoo Answers;
- rejestry publiczne i certyfikaty, indeksy systemu bibliotecznego;
- komunikacja za pomocą szyfrowanego użycia w celu zapewnienia prywatności i ochrony;
- konkursy karaoke i śpiewu;
- grupy teoretyków spisku;
- kursy z zakresu obsługi komputera i technologii.

Tradycyjne wyszukiwarki tworzą swoje indeksy przez przeglądanie lub indeksowanie powierzchniowych stron internetowych. Aby zostać odkryta, strona musi być statyczna i połączona z innymi stronami. Głębokie witryny sieci Web otrzymują średnio o 50% większy ruch miesięczny niż strony powierzchniowe i są bardziej powiązane z witrynami na powierzchni. Typowa (wg mediany) głęboka strona internetowa nie jest jednak dobrze znana użytkownikom sieci. Ponad połowa głębokich stron znajduje się w bazach tematycznych.

Deep web charakteryzuje się rozrostem, różnorodnością domen i licznymi ustrukturyzowanymi bazami danych. Rośnie w tak dużym tempie, że skuteczne oszacowanie jego wielkości może być trudne lub wręcz niemożliwe.

Olga Wasiuta, Sergiusz Wasiuta

P. Biddle, P. England, M. Peinado, *The Darknet and the Future of Content Distribution*, 2003; M.K. Bergman, *The Deep Web: Surfacing Hidden Value*, „The Journal of Electronic Publishing" 2001, vol. 7, iss. 1; E. Dilipraj, *Cyber Enigma: Unravelling the Terror in the Cyber World*, Routledge, Milton 2019; K. Król, *Deep Web i Dark Web: niewidoczne zasoby internetu*, 9.05.2019, HomeProject.pl (dostęp 18.05.2019); T. Leżoń, *Darknet i deep web. Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, 27.04.2015, TVN24.pl (dostęp 31.07.2020); D. Mider, *Mappa mundi ukrytego internetu. Próba kategoryzacji kanałów komunikacji i treści*, „Praktyka i Teoria Informacji Naukowej" 2015, t. 23, nr 1; E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs, New York 2011; W. Orliński, *Internet. Czas się bać*, Wydawnictwo Agora, Warszawa 2013; N. Pamuła-Cieslak, *Typologia zasobów ukrytego internetu*, „Przegląd Biblioteczny" 2006, z. 2; taż, *Ukryty internet jako przedmiot edukacji informacyjnej*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2015; C. Sheils, *The Dark Web & Deep Web: How To Access The Hidden Internet Today*, 27.02.2019, Digital.com (dostęp 27.02.2019); Ch. Sherman,

G. Price, *The Invisible Web. Uncovering Information Sources Search Engines Can't See*, Information Today, Medford, New Jersey 2003; M. Szpunar, *Imperializm kulturowy internetu*, Instytut Dziennikarstwa, Mediów i Komunikacji Społecznej Uniwersytetu Jagiellońskiego, Kraków 2017; taż, *Sieć ukryta a sieć widzialna. O zasobach WWW nieindeksowanych przez wyszukiwarki*. „Przegląd Kulturoznawczy" 2014, nr 1 (19); D. Szumilas, *Kop głębiej! Google to nie wszystko*, „Magazyn Internet" 2005, nr 8; B. Świderski, *Najciemniejszy zakątek internetu naprawdę istnieje. Ukryta sieć TOR: Lewe papiery, pedofilia, przekręty i narkotyki*, 21.09.2012, NaTemat.pl (dostęp 18.05.2019); O. Wasiuta, *Deep web,* [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron Kraków 2019; O. Wasiuta, S. Wasiuta, *FakeApp jako nowe zagrożenie bezpieczeństwa politycznego i informacyjnego*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 3; J.A. Wood, *The Darknet: a Digital Copyright Revolution*, „Richmond Journal of Law & Technology" 2010, vol. 16, iss. 4.

DEGRADACJA WOJSKOWA – polega na odebraniu posiadanego → s t o p n i a w o j s k o w e g o [t. 4], co bywa dokonywane często w ceremonialny sposób, aby dodatkowo ukarać i upokorzyć degradowanego. Ceremonia taka odbywa się publicznie – na widoku wszystkich zgromadzonych odbiera się degradowanemu wszelkie odznaczenia i emblematy, zrywa się guziki i epolety, strąca czapkę i łamie białą broń przyboczną. Degradacji wojskowej dokonywano za różne czyny, przy czym zwykle była to kara za działania haniebne i uważane za niehonorowe i niegodne → ż o ł n i e r z a [t. 4]. Wśród znanych zdegradowanych wymienia się m.in. F. Mitchella (1621 r.), T. Cochrane'a (1814 r.), A. Dreyfusa (1894 r.), P. Pétaina (1945 r.), R. Kuklińskiego (1984 r.).

Obecnie w Polsce, zgodnie z art. 324 § 1 pkt. 3 kk, degradacja jest jednym ze środków karnych. Definicja legalna degradacji zawarta została w art. 327 § 1 kk, zgodnie z nią degradacja obejmuje utratę posiadanego stopnia wojskowego i powrót do stopnia szeregowego. Degradacja godzi w istotny sposób w prestiż ukaranego, a także pociąga za sobą restrykcje natury ekonomicznej takie jak utrata pracy, brak możliwości uzyskania dodatkowego uposażenia rocznego czy odprawy, a także odebranie prawa do zaopatrzenia emerytalnego.

Sąd może orzec degradację w razie skazania za przestępstwo umyślne, jeżeli rodzaj czynu, sposób i okoliczności jego popełnienia pozwalają

przyjąć, że sprawca utracił właściwości wymagane do posiadania stopnia wojskowego, a zwłaszcza w wypadku działania w celu osiągnięcia korzyści majątkowej. Oznacza to, że degradacja może zostać orzeczona w odniesieniu do każdego skazanego żołnierza, niezależnie od typu czynu, jaki popełnił. Sąd może orzec degradację tylko wobec osoby, która w chwili popełnienia → c z y n u z a b r o n i o n e g o [t. 1] była żołnierzem, chociażby przestała nim być w chwili orzekania.

Ostatnim publicznie zdegradowanym angielskim rycerzem królestwa był Mitchell – został pozbawiony rycerstwa po uznaniu go winnym wyłudzania pieniędzy od licencjobiorców po tym, jak otrzymał monopol na licencjonowanie zajazdów przez G. Villiersa, pierwszego księcia Buckingham, i króla Jakuba I Stuarta. Z kolei Cochrane, brytyjski arystokrata, polityk i wojskowy, adm. Royal Navy, uczestnik wojen napoleońskich, został zdegradowany za udział w spekulacjach giełdowych. Marszałek Pétain został zdegradowany za zdradę narodową i kolaborację na rzecz hitlerowskich Niemiec.

Jednym z najbardziej znanych w historii zdegradowanych żołnierzy był kpt. Dreyfus, którego historia wywołała skandal polityczny we Francji pod koniec XIX wieku. Dreyfus był niezależnym, zamożnym Żydem pochodzenia niemieckiego, służył w Sztabie Generalnym Armii Francuskiej. Został oskarżony o szpiegostwo na rzecz Niemiec na podstawie dokumentu znanego jako „Bordereau" (fr. *bordereau*, wykaz, notka) znalezionego w niemieckiej ambasadzie. Wyraźnie antysemicki Sztab Generalny odmówił Dreyfusowi dostępu do dokumentacji użytej do osądzenia go w procesie przed sądem wojskowym w październiku 1894 r. Dreyfus został uznany za winnego i skazany na degradację i uwięzienie na Diabelskiej Wyspie. Płk G. Picquart wkrótce po procesie zdał sobie sprawę, że dokument „Bordereau" został napisany przez mjra F. Walsina Esterhazy'ego, którego pismo odpowiadało innym obciążającym dowodom. Picquarta szybko zastąpił komendant H.-J. Henry, który sfałszował dokumenty obciążające Dreyfusa, a gdy zostało to odkryte, popełnił samobójstwo. Sąd wojenny zwolnił Esterhazy'ego ze wszystkich stawianych mu zarzutów. W sprawę niesłusznie oskarżonego i zdegradowanego Dreyfusa zaangażował się pisarz Emil Zola, który 13 stycznia 1898 r. opublikował list otwarty *J'Accuse…!* (*Oskrażam…!*), pod którym podpisało się wielu francuskich intelektualistów. M.in. za sprawą

listu miał miejsce nowy proces w Rennes 3 czerwca 1899 r., w którym Dreyfus ponownie został uznany za winnego, ale z okolicznościami łagodzącymi. W 1903 r. Sąd Najwyższy stwierdził, że wyrok sądu wojskowego był błędny. Dopiero jednak 22 lipca 1906 r. przywrócono Dreyfusowi stopień kapitana, awansowano go na majora oraz odznaczono Legią Honorową.

Kontrowersje wywołuje niejednokrotnie pytanie o to, za co można ukarać żołnierza degradacją, aby kara odpowiadała popełnionemu czynowi. W 2012 r. ze stopnia sierż. sztab. piechoty morskiej USA do stopnia szeregowego został zdegradowany F. Wuterich. Dowodził on oddziałem, który dokonał masakry w Al-Hadisie w Iraku 19 listopada 2005 r. Wówczas to amerykańscy żołnierze brutalnie zamordowali 24 Irakijczyków, w tym kobiety i dzieci. Przyczyną wydarzenia był wybuch bomby pułapki, która zabiła jednego z żołnierzy marines. Koledzy zabitego w akcie desperacji zastrzelili cywilów w taksówce, a następnie wtargnęli do domów w pobliżu miejsca eksplozji. Tam zastrzelili kilkanaście kolejnych osób. Wśród 24 zabitych było 8 kobiet i 5 dzieci. Ciała zamordowanych nosiły ślady strzałów w głowę, jedno zaś było spalone. Świadkowie wydarzeń podkreślali, że nie było powodów dla tak brutalnego działania. Lokalna ludność żądała ukarania śmiercią żołnierzy, którzy dopuścili się masakry. Postępowanie wobec zdegradowanego następnie Wutericha trwało 6 lat.

Proces degradacji może być nie tylko następstwem wyroku sądowego, ale także konsekwencją decyzji politycznej. W Polsce w 2018 r. pojawił się projekt ustawy degradacyjnej, której założeniem było pozbawienie stopni wojskowych żołnierzy i oficerów służących w Wojsku Polskim w czasie PRL, w tym przede wszystkim odebranie stopni generalskich W. Jaruzelskiemu i C. Kiszczakowi. Zgodnie z projektem ustawy degradacja miała objąć oficerów wskazanych przez ministra obrony narodowej, który będzie mógł wszcząć stosowne postępowanie z inicjatywy własnej lub po uzyskaniu → i n f o r m a c j i od Instytutu Pamięci Narodowej, Wojskowego Biura Historycznego oraz organizacji społecznych. Ustawa nie weszła jednak w życie w związku z odmową jej podpisania przez Prezydenta RP.

W 1984 r. zdegradowany ze stopnia pułkownika został Kukliński. Pozycja Kuklińskiego w Sztabie Generalnym Polskiej Armii Ludowej i jego rola jako oficera łącznikowego między Polską Armią Ludową a oddziałami Układu Warszawskiego dała mu dostęp do najtajniejszych dokumentów

wojskowych. W 1971 r. rozpoczął współpracę z CIA, która wg niektórych źródeł historycznych dostarczyła Amerykanom ok. 35 tys. stron ściśle tajnych materiałów, od specyfikacji technicznych najnowszej radzieckiej broni po plany operacyjne Układu Warszawskiego. W 1981 r, tuż przed ogłoszeniem przez gen. Jaruzelskiego stanu wojennego, kiedy ujawnienie Kuklińskiego było bliskie, wraz z rodziną z pomocą CIA opuścił PRL. Następnie mieszkał w USA pod zmienioną tożsamością. Zaocznie Kukliński został zdegradowany i skazany na śmierć przez polski sąd wojskowy, ale wyrok został uchylony w 1996 r. po upadku → k o m u n i z m u w Polsce.

Jakub Idzik

S. Cenckiewicz, *Atomowy szpieg. Ryszard Kukliński i wojna wywiadów*, Zysk i S-ka, Poznań 2014; G. Chapman, *The Dreyfus Case: A Reassessment*, Reynal, New York 1972; *Encyclopedia of Violence, Peace & Conflict*, L.R. Kurtz (red.), Elsevier, Oxford 2008; *Handbook of the Sociology of the Military*, G. Caforio, M. Nuciari (red.), Springer International Publishing, Cham 2018; M. Horoszewicz, *Sprawa Dreyfusa: ostrzeżenie sprzed wieku*, Bellona, Warszawa 2017; A. King, *The Combat Soldier. Infantry Tactics and Cohesion in the Twentieth and Twenty-First Centuries*, Oxford University Press, Oxford 2013; A. Richardson, *Dreyfus Affair (1894–1906)*, [w:] *Ground Warfare: An International Encyclopedia*, S. Sandler (ed.), ABC-CLIO, Santa Barbara–Denver–Oxford 2002; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 2019.1950 t.j.; B. Weiser, *Ryszard Kukliński. Życie ściśle tajne*, Świat Książki, Warszawa 2009.

DEMILITARYZACJA – w wąskim rozumieniu oznacza zobowiązanie do usunięcia wszelkich obiektów militarnych, broni oraz sił zbrojnych z danego terenu oraz zakaz ich lokowania, budowania czy utrzymywania na nim w przyszłości, wynikające z umów międzynarodowych i stanowiące jeden z typów ograniczenia zwierzchnictwa terytorialnego państwa. Takie ujęcie terminu zostało zawarte w załączniku XIII do traktatu pokojowego z Włochami, podpisanego w Paryżu dnia 10 lutego 1947 r. Zgodnie z dokumentem demilitaryzacja powinna być rozumiana jako:

> zakaz, na danym terenie i na danych wodach terytorialnych, wszelkich urządzeń lub fortyfikacji morskich, wojskowych i lotniczo-wojskowych, jak również ich zbrojenia, sztucznych zapór

wojskowych, morskich i powietrznych; korzystania z baz przez jednostki wojskowe, morskie i lotnictwa wojskowego lub stacjonowania stałego, jak również tymczasowego tych jednostek; szkolenia wojskowego w jakiejkolwiek bądź formie oraz fabrykacji sprzętu wojennego.

W I protokole dodatkowym do konwencji genewskich użyto natomiast terminu strefa zdemilitaryzowana, która spełnia następujące warunki:

a) wszyscy kombatanci, jak też broń i ruchomy sprzęt wojskowy powinni zostać z niej usunięci;
b) w strefie nie należy czynić użytku ze stałych urządzeń i obiektów wojskowych na szkodę nieprzyjaciela;
c) władza i ludność danego obszaru nie będą podejmować działań na szkodę nieprzyjaciela oraz
d) nie może być prowadzona żadna działalność na rzecz wsparcia wysiłku wojskowego.

Wyróżnia się demilitaryzację całkowitą i częściową. W pierwszym przypadku dany teren ma być wyłączony z wykorzystania w celach militarnych pod jakimkolwiek względem, w drugim zobowiązanie polega jedynie na ograniczeniu wykorzystania danego terenu do celów militarnych. Szczególnym przykładem częściowej demilitaryzacji jest denuklearyzacja, czyli zakaz utrzymywania → b r o n i n u k l e a r n e j [t. 1] na określonym obszarze. Status stref wolnych od broni jądrowej ustanowiono np. w Ameryce Łacińskiej i na Karaibach (traktat z Tlatelolco z 1967 r.), na Południowym Pacyfiku (traktat z Rarotonga 1985 r.), w Azji Południowo-Wschodniej (traktat z Bangkoku z 1995 r.), w Afryce (traktat z Pelindaba z 1996 r.) i w Azji Środkowej (traktat z Semipałatyńska z 2006 r.).

Termin demilitaryzacja używany jest także w znaczeniu szerszym – jako dążenie do ograniczenia potencjału militarnego państw, przy czym nie oznacza całkowitego usunięcia z ich terytorium wszelkich obiektów czy sił militarnych, a jedynie ograniczenie liczebności sił zbrojnych czy arsenału posiadanego uzbrojenia. Przykładami może być demilitaryzacja Niemiec, Austrii i Japonii po II wojnie światowej.

Dążenie do wyłączenia określonych obszarów z wykorzystania w celach wojskowych jest zjawiskiem znanym od wieków, by wspomnieć np. tego rodzaju zapisy w traktatach pokojowych zawartych w Westfalii w 1648 r. czy w Utrechcie w 1713 r. Postanowienia tego rodzaju coraz częściej ujmowano w traktatach zawieranych od końca XIX wieku – demilitaryzacja Kanału Kilońskiego, Kanału Panamskiego, Kanału Sueskiego, demilitaryzacja Nadrenii, cieśniny Magellana, Dardanele, Bosfor, Gibraltarskiej. Status obszarów zdemilitaryzowanych mają także: Antarktyka (traktat antarktyczny z 1959 r.), dno morskie (traktat o dnie morza z 1971 r.), Wyspy Alandzkie (traktat paryski z 1856 r., potwierdzony w 1921 i ponownie w 1947 r.), koreańska strefa zdemilitaryzowana oddzielająca Koreę Północną i Koreę Południową (ustalona przez ONZ w 1953 r.).

Przestrzeń kosmiczną można uznać za przynajmniej częściowo zdemilitaryzowaną. Traktat o przestrzeni kosmicznej z 1967 r. przewiduje, że państwa-strony

> zobowiązują się nie wprowadzać na orbitę wokół Ziemi jakichkolwiek obiektów przenoszących broń nuklearną lub jakichkolwiek innych rodzajów broni masowego zniszczenia ani nie umieszczać tego rodzaju broni na ciałach niebieskich lub w przestrzeni kosmicznej w jakikolwiek inny sposób. […] Zakazuje się zakładania wojskowych baz, instalacji oraz fortyfikacji na ciałach niebieskich, dokonywania na nich prób z jakimikolwiek typami broni oraz przeprowadzania manewrów wojskowych. Korzystanie z personelu wojskowego w celu badań naukowych lub w jakichkolwiek innych celach pokojowych nie jest zabronione.

Analogicznego statusu nie nadano natomiast morzom i oceanom. Artykuł 88 Konwencji Narodów Zjednoczonych o prawie morza z 1982 r. wskazuje jedynie, że *morze pełne jest wykorzystywane wyłącznie do celów pokojowych*. Konwencja nie wprowadza więc ani częściowej, ani całkowitej demilitaryzacji czy też denuklearyzacji morza pełnego, nie zakazuje również działalności nawigacji wojskowej.

Anna Pacholska

T. Brańka, *Demilitarization and Neutralization – the Case of the Åland Islands*, „Przegląd Politologiczny" 2017, nr 4; R. Klepka, *Parlament w państwie federalnym na przykładzie Austrii, Belgii, Niemiec i Szwajcarii*, Wydawnictwo Sejmowe, Warszawa 2013; A. Makowski, *Konwencja o prawie morza – implikacje dla bezpieczeństwa polski*, „Prawo Morskie", t. XXVII; A. Pacholska, *Demilitaryzacja*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; J. Polit, *Kapitulacja i okupacja Japonii*, [w:] *Historia polityczna świata XX wieku*, M. Bankowicz (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2004; Protokół dodatkowy do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I), sporządzony w Genewie dnia 8 czerwca 1977 r., Dz. U. 1992, nr 41, poz. 175.

DEMOBILIZACJA – w szerszym znaczeniu to szereg działań, które mają miejsce w państwie w przypadku zmiany jego sytuacji politycznej z wojennej na pokojową. W tym zakresie pojęcie jest przeciwstawne do mobilizacji oznaczającej zmianę sposobu funkcjonowania państwa w przypadku zmiany sytuacji pokojowej na wojenną. Zmiana demobilizacyjna polega na podjęciu szeregu działań odnoszących się do funkcjonowania armii, gospodarki, systemu ekonomicznego, przemysłu, rolnictwa, transportu, łączności oraz innych sfer. W węższym sensie demobilizacja wojskowa jest procesem rozumianym jako jeden z aspektów działania obejmującego rozbrojenie, demobilizację i reintegrację byłych → ż o ł n i e r z y [t. 4] oraz przemysłu nastawionego na prowadzenie działań wojennych. Odgrywa kluczową rolę w przechodzeniu od → w o j n y [t. 4] do pokoju. Powodzenie lub niepowodzenie tego przedsięwzięcia bezpośrednio wpływa na długoterminowe perspektywy budowania pokoju w każdym społeczeństwie po zakończeniu konfliktu. Procesy demobilizacji przyczyniają się do zaspokojenia natychmiastowych potrzeb w zakresie → b e z p i e c z e ń s t w a [t. 1] i umożliwiają rozwój silnych instytucji politycznych, dobrze funkcjonujących gospodarek oraz reintegrację społeczną i gospodarczą byłych uczestników walk w celu przyczynienia się do racjonalnych rządów, pojednania społeczeństwa, długofalowego rozwoju i trwałego pokoju.

Demobilizacja wojskowa jest zarówno procesem fizycznym, jak i mentalnym. Aspekt fizyczny polega na oddzieleniu elementu uzbrojonego, a więc żołnierza, od systematycznej struktury dowodzenia i kontroli sił zbrojnych lub grupy, zmniejszając w ten sposób liczbę walczących w siłach

zbrojnych albo rozwiązując grupy w całości. Mentalny aspekt procesu demobilizacji polega na przygotowaniu danej osoby lub grupy do znalezienia swojego miejsca w → społeczeństwie obywatelskim [t. 4]. Wojsko ma do odegrania ważną rolę zarówno w rozbrojeniu, jak i demobilizacji, jednakże równie istotny jest komponent cywilny – rozbrojenie jest przede wszystkim odpowiedzialnością wojska, zaś w pozostałych czynnościach, zwłaszcza w programie reintegracji, uczestniczy głównie ten drugi, przy czym strony udzielają sobie wzajemnego wsparcia. Współpraca cywilno-wojskowa jest kluczem do wydajności w tej części operacji.

Demobilizacja wojskowa odnosi się do szeregu interwencji w procesie → demilitaryzacji oficjalnych i nieoficjalnych grup zbrojnych poprzez rozbrajanie i rozwiązywanie grup niepaństwowych oraz ewentualnie zmniejszanie sił zbrojnych. Tradycyjnie alternatywą dla rozwiązania pokonanej grupy zbrojnej jest włączenie jej częściowo do zwycięskich sił zbrojnych. Polityczne i społeczne motywy demobilizacji obejmują poprawę jakości i efektywności sił zbrojnych, zapewnienie politycznej legitymizacji sił zbrojnych, co wiąże się z przesunięciem lojalności grupy zbrojnej z określonego podmiotu (politycznego), modernizację wojska, utrzymanie dokładnej reprezentacji mniejszości w grupie zbrojnej oraz zagwarantowanie bezpieczeństwa ludzi. Należy podkreślić, że demobilizacja jest przede wszystkim procesem cywilnym, choć wkład wojska ma kluczowe znaczenie dla decyzji metodologicznych i organizacyjnych.

W praktyce programy demobilizacyjne pomagają byłym uczestnikom walk odchodzić od ról i stanowisk, które określały ich w czasie konfliktu, aby identyfikowali się jako obywatele i członkowie lokalnych społeczności. Zakłada się, że doszło do rozbrojenia oraz że broń została zebrana, zmagazynowana lub w ostateczności zniszczona. Zorganizowanie zgrupowania byłych walczących jest zazwyczaj pierwszym krokiem dającym możliwość odzyskania kontroli nad wcześniej rozproszonymi oddziałami i ich bronią. Oprócz usunięcia symboli życia wojskowego walczących, takich jak broń, mundur i stopień, byli żołnierze są rejestrowani, liczeni i monitorowani przy użyciu dokumentów identyfikacyjnych, a jednocześnie zbierane są → informacje niezbędne do ich integracji ze społecznością. Osobom, które wcześniej brały udział w konfliktach, oferuje się medyczne badania przesiewowe i pomoc, zaopatrzenie i transport w celu powrotu do ich

rodzinnych regionów. Udzielanie pomocy materialnej lub finansowej rodzinom byłych uczestników walk jest również uważane za kluczowe w tym procesie, ponieważ ułatwia akceptację długo nieobecnych członków społeczeństwa przez ich macierzyste społeczności.

Po przeniesieniu się do społeczności lokalnych byli uczestnicy walk otrzymują szkolenie zawodowe do pracy poza dziedziną bezpieczeństwa, kredyty, stypendia, dystrybucję własności ziemi, a czasami znajdują zatrudnienie w nowej → p o l i c j i [t. 3] lub służbie bezpieczeństwa. Jednakże aby proces powrotu zakończył się sukcesem, społeczność lokalna, do której były żołnierz i jego rodzina są ponownie wprowadzani, musi być na to przygotowana. Jednocześnie byli uczestnicy walk muszą znać swoje obowiązki zgodne z prawem i zwyczajami panującymi w ich państwie oraz być świadomi zmian politycznych, które miały lub mają miejsce.

Demobilizacja może prowadzić do trwałej reintegracji z życiem obywatelskim w dłuższej perspektywie czasowej, jeżeli istnieje odpowiednia perspektywa ekonomiczna, funkcjonują instytucje państwowe zdolne do świadczenia podstawowych usług, ramy prawne i ścisła koordynacja ze społeczeństwem obywatelskim w celu zapewnienia, że byli żołnierze znajdą realne źródła utrzymania i nowy cel w życiu.

Doświadczenia międzynarodowe ilustrują wyzwania związane z wdrażaniem procesu demobilizacji, a także jej polityczny i złożony charakter. Proces ten w dużej mierze koncentruje się na byłych walczących i ogranicza się do stosunkowo krótkiego okresu po zakończeniu wojny. Proces reintegracji musi być jednak postrzegany jako zadanie długoterminowe, które wymaga gotowości podmiotów międzynarodowych do utrzymania politycznego rozmachu tego programu. W zależności od charakteru wojny społeczności mogą zdecydowanie sprzeciwiać się powrotowi walczących. Mogą upłynąć lata, zanim część z nich wróci do domu, tak jak np. w Rwandzie, gdzie w czasie konfliktu zaszły drastyczne zmiany prawne i polityczne. Ponadto, aby poradzić sobie z brakiem zaufania do zmian politycznych lub poczuciem marginalizacji, demobilizacja jest prowadzona w połączeniu z innymi działaniami reformującymi sektor bezpieczeństwa.

Dodatkowym problemem pozostaje kwestia tego, ilu byłych walczących trzeba zdemobilizować. Liczby pochodzące z list dowódców są często przeszacowane i w związku z tym muszą być zweryfikowane innymi

sposobami. Co więcej, byli żołnierze mogą nie chcieć oddać całej swojej broni, a wówczas może dojść do wzrostu → przemocy [t. 3] i → przestępczości [t. 3]. W niektórych przypadkach dawni walczący nie chcą wrócić do swoich domów lub mogą obawiać się dezaprobaty bądź odrzucenia, a tym samym próbować zatrzymać proces.

Istnieje również duża trudność w ustaleniu tego, kto jest byłym walczącym i kto powinien kwalifikować się do wsparcia demobilizacyjnego. Zdefiniowanie osoby biorącej udział w konflikcie jako noszącej broń często prowadziło do wykluczenia z procesów demobilizacyjnych kobiet i dziewcząt. Nierzadko związane z siłami zbrojnymi, napotykają również szczególne trudności w ponownej integracji ze społeczeństwem, w którym podporządkowują się tradycyjnym poglądom na swoją rolę w społeczeństwie.

Demobilizacja może być postrzegana jako nowa umowa społeczna pomiędzy byłymi uczestnikami walk a ich środowiskiem po zakończeniu konfliktu. Od 1989 r. kompleksowe rozwiązania polityczne mające na celu zakończenie długotrwałych konfliktów wewnętrznych w Ameryce Środkowej, różnych częściach Afryki, Azji Południowo-Wschodniej i na Bałkanach Zachodnich zawierały szczegółowe przepisy dotyczące rozbrojenia i demobilizacji rebeliantów i sił rządowych. W tym kontekście kraje OECD uzgodniły wytyczne polityczne dotyczące pomocy rozwojowej, a Departament Operacji Pokojowych ONZ opublikował zasady i wytyczne dotyczące właściwych programów, które od tego czasu stały się obowiązkowym elementem operacji utrzymywania i egzekwowania pokoju. Oprócz zaangażowania ONZ Bank Światowy finansuje i pomaga w prowadzeniu i ocenie tego rodzaju programów, podczas gdy Unia Europejska od dawna wspiera procesy rozbrojenia, demobilizacji i reintegracji poprzez programy wspólnotowe, fundusze dwustronne państw członkowskich, a od 2005 r. poprzez misje w ramach Europejskiej Polityki Bezpieczeństwa i Obrony (EPBiO). Coraz częściej organizacje pozarządowe działające w lokalnych społecznościach otrzymują fundusze na prowadzenie pomocy reintegracyjnej oraz świadczenie usług socjalnych i szkoleń.

Jakub Idzik

K.M. Clark, *Fostering a Farewell to Arms: Preliminary Lessons Learned in the Demobilization and Reintegration of Combatants*, United States Agency for International Development, Washington 1996; G.A. Dzinesa, *Disarmament, Demobilization and Reintegration in Southern Africa: Swords into Ploughshares?*, Palgrave Macmillan, Johannesburg 2017; A. Giustozzi, *Introduction*, [w:] *Post-conflict Disarmament, Demobilization and Reintegration: Bringing State-building Back In*, A. Giustozzi (ed.), Routledge, New York–London 2016; T. Kmiecik, *Problemy demobilizacji i przejścia Wojska Polskiego na stopę pokojową w latach 1945–1947*, „Słupskie Studia Historyczne" 2004, z. 11; M. Knight, A. Özerdem, *Guns, Camps and Cash: Disarmament, Demobilization and Reinsertion of Former Combatants in Transitions from War to Peace*, „Journal of Peace Research" 2004, vol. 41 (4); tenże, *Disarmament, Demobilization and Reintegration of Former Combatants in Afghanistan: Lessons Learned from a Cross-Cultural Perspective*, „Third World Quarterly" 2002, vol. 23 (5); J. Rak, *From Mobilization to Demobilization: Dynamics of Contention in the Austerity-driven Slovenia*, „Środkowoeuropejskie Studia Polityczne" 2018, nr 3; The World Bank, *Demobilization and Reintegration Programming in the World Bank*, Conflict Prevention and Reconstruction Unit, The World Bank, Washington 2003; N. Young, *Demobilisation after War*, [w:] *The International Encyclopedia of Peace*, Oxford University Press, Oxford 2009.

DEMONOPOLIZACJA BEZPIECZEŃSTWA – proces tworzenia →społeczeństwa obywatelskiego [t. 4] nierozerwalnie związany jest z decentralizacją władzy i przekazaniem części kompetencji, a co za tym idzie także odpowiedzialności, samorządom. Bardzo ważną kompetencją uzyskaną przez władze samorządowe stało się zapewnianie →bezpieczeństwa publicznego [t. 1]. Odbywało się to w sytuacji, gdy zmiany ustrojowe o charakterze ekonomiczno-politycznym, jakie rozpoczęły się w Polsce na początku lat 90. XX w., spowodowały nie tylko akcelerację procesów gospodarczych i cywilizacyjnych zapewniających dynamiczny rozwój w różnych dziedzinach życia, ale także gwałtowny wzrost →przestępczości [t. 3] i towarzyszących jej →patologii społecznych [t. 3]. To właśnie wtedy pojawiły się nieznane wcześniej rodzaje przestępstw, w tym te o charakterze zorganizowanym i międzynarodowym. Jednocześnie kontrola nad aktywnością obywateli uległa ze strony państwa osłabieniu, tworzyły się pierwsze prywatne fortuny, dając początek powstawaniu rodzimego kapitału. Nastąpił też międzynarodowy transfer aktywów finansowych, a granice stały się bardziej otwarte, także dla świata

przestępczego. Społeczeństwo zaczęło też, głównie dzięki przekazom medialnym, odczuwać zwiększony stan →zagrożenia [t. 4] przestępczością, którą uznało za poważną przeszkodę w osiągnięciu satysfakcjonującego poziomu życia. Państwo nie było już zdolne do zapewnienia szeroko rozumianego →bezpieczeństwa [t. 1], a to z kolei zapoczątkowało trwałą zmianę, jaką jest demonopolizacja bezpieczeństwa. Paradoksalnie kolejną determinantą zagrożenia stało się wejście Polski do koalicji antyterrorystycznej i udział Sił Zbrojnych RP zarówno w misjach stabilizacyjnych, jak i operacjach wojskowych poza granicami kraju, stworzyły one dla kraju realne zagrożenie ze strony ekstremistów. Przed organami państwa pojawił się wówczas problem skutecznego przeciwstawiania się nowym wyzwaniom skutkującym wzrostem dynamiki →zagrożenia bezpieczeństwa [t. 4].

W nowej sytuacji państwo szybko zorientowało się, że dotychczas scentralizowane zarządzanie bezpieczeństwem jest nieefektywne, gdyż nie zapewnia właściwej reakcji na nieznane dotąd w Polsce determinanty zagrożeń. Tak więc podzielenie się odpowiedzialnością za stan →bezpieczeństwa publicznego [t. 1] z innymi niż rządowe podmiotami wynikało z jednej strony z procesów demokratyzacji państwa, a z drugiej z niemożności samodzielnego zwalczania występujących zagrożeń. W ten sposób następowała stopniowa demonopolizacja bezpieczeństwa.

Słownik języka polskiego PWN słowo „monopol" definiuje jako „czyjeś wyłączne prawo do czegoś". Demonopolizacja oznacza więc likwidowanie istniejącego monopolu w określonej dziedzinie. Przez wiele lat sferą całkowicie zmonopolizowaną przez państwo było bezpieczeństwo. Jest ono powszechnie uznawane za jedną z podstawowych potrzeb człowieka, której zaspokojenie umożliwia mu korzystanie z innych wartości, dając możliwość przetrwania i rozwoju. Termin „bezpieczeństwo" pojawił się w piśmiennictwie polskim już w XIX w., a jednym z jego prekursorów był, w okresie międzywojennym, W. Kawka, który definiował je jako stan, w którym ogół społeczeństwa, jak również państwo ze swoimi celami, mają zagwarantowaną ochronę od szkód zagrażających im z jakiegokolwiek źródła. J. Zaborowski za bezpieczeństwo publiczne uważa taki realny stan wewnętrzny państwa, który pozwala mu, bez narażenia na szkody (spowodowane zarówno działaniem sił natury, techniki jak i zachowaniem

ludzkim), na prawidłowe funkcjonowanie organizacji państwowej i zapewnienie jej interesów, zachowanie życia i zdrowia obywateli oraz korzystanie przez nich z praw i swobód zagwarantowanych im konstytucją i innymi uregulowaniami prawnymi. Kwestią bezpieczeństwa publicznego zajął się także Sąd Najwyższy, który w uchwale z dnia 22 grudnia 1993 r. określił je jako *całość porządku i urządzeń społecznych, chroniących obywateli przed zjawiskami groźnymi dla życia, zdrowia lub grożącymi poważnymi stratami w gospodarce narodowej*.

Biorąc pod uwagę przedstawione wyżej definicje, można przyjąć, że demonopolizacja bezpieczeństwa to udzielenie przez państwo zgody oraz stworzenie odpowiednich warunków do zapewniania bezpieczeństwa także przez inne niż państwowe podmioty. To podzielenie się przez państwo kompetencjami, zadaniami i odpowiedzialnością w zapewnianiu bezpieczeństwa z podmiotami, które ustawodawca wyposażył w tym celu w określone uprawnienia i narzędzia, pozwalające im na prowadzenie efektywnych działań.

Zapewnianiu bezpieczeństwa publicznego służy system będący zorganizowanym zbiorem podsystemów współdziałających ze sobą i tworzących spójną całość, ukierunkowanych na realizację wspólnego celu, jakim jest uzyskanie i utrzymanie pożądanego stanu w państwie, rozumianego jako brak zagrożenia w życiu społeczeństwa i poszczególnych jego członków, umożliwiającego im stały i →zrównoważony rozwój [t. 4]. Podsystemy te funkcjonują na podstawie przyznanych im kompetencji, realizując różne zadania zmierzające do skutecznego przeciwdziałania wszelkim determinantom zagrożeń oraz zapobiegające czynom godzącym w dobro państwa, jego porządek publiczny, życie, zdrowie i mienie obywateli. Za stworzenie i sprawne funkcjonowanie systemu bezpieczeństwa publicznego odpowiada państwo, dla którego zapewnienie bezpieczeństwa jest jednym z podstawowych i najważniejszych zadań. Do czasu transformacji ustrojowo-politycznej państwa system bezpieczeństwa opierał się na organach administracji państwowej, a szczególna rola przypadała w nim tzw. służbom mundurowym do których zaliczamy: →Policję [t. 3], →Agencję Bezpieczeństwa Wewnętrznego [t. 1], →Agencję Wywiadu [t. 1], →Służbę Kontrwywiadu Wojskowego [t. 4], →Służbę Wywiadu Wojskowego [t. 4], →Centralne Biuro

Antykorupcyjne [t. 1], →Straż Graniczną [t. 4], →Służbę Ochrony Państwa [t. 4], →Państwową Straż Pożarną [t. 4] oraz →Służbę Więzienną [t. 4]. Także obecnie dział administracji rządowej „sprawy wewnętrzne" obejmuje zadania realizowane przez te formacje, z których najważniejsze to: ochrona bezpieczeństwa i porządku publicznego, ochrona granicy państwowej, →zarządzanie kryzysowe [t. 4], →obrona cywilna [t. 3], ochrona przeciwpożarowa, przeciwdziałanie skutkom klęsk żywiołowych, nadzór nad ratownictwem górskim i wodnym.

Demonopolizacja bezpieczeństwa implikowała wprowadzenie do systemu bezpieczeństwa, który do tej pory tworzyły organy administracji państwowej, 2 nowych podsystemów: samorządowego i prywatnego.

Podsystem prywatny tworzą firmy ochrony osób i mienia. Wspólna inicjatywa podjęta przez organy państwowe oraz samorząd gospodarczy prywatnego sektora bezpieczeństwa doprowadziła do uchwalenia przez Sejm 22 sierpnia 1997 r. długo oczekiwanej ustawy o ochronie osób i mienia. Tym samym administracja państwowa, odpowiedzialna za system bezpieczeństwa państwa, uznała, że jej partnerem na poziomie lokalnym będą przedsiębiorcy prowadzący koncesjonowaną działalność gospodarczą, spełniający wysokie, ściśle określone wymagania i zatrudniający pracowników mających odpowiednie kwalifikacje zawodowe. W ramach demonopolizacji bezpieczeństwa rozpoczął się także proces jego komercjalizacji.

Jednak najważniejszym skutkiem demonopolizacji bezpieczeństwa było powstanie podsystemu samorządowego, który stał się ważnym ogniwem w zapewnianiu porządku i bezpieczeństwa publicznego. By mogło to nastąpić, ustawodawca wprowadził nowe regulacje prawne. Kluczowa była Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, która w art. 7 uznała, że zaspokajanie zbiorowych potrzeb wspólnoty mieszkańców należy do zadań własnych gminy. Jako szczególnie ważne zadanie własne wskazała sprawy porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, w tym wyposażenia i utrzymania gminnego magazynu przeciwpowodziowego. Wiodącym partnerem Policji w realizacji zadań z zakresu poprawy stanu bezpieczeństwa i porządku publicznego w mieście stała się →straż miejska [t. 4].

Lokalne → s t r a t e g i e [t. 4] i programy bezpieczeństwa były przyjmowane w gminach, zarówno mających charakter wielkomiejskich aglomeracji, jak i w małych miejscowościach, których mieszkańcy i przedstawiciele samorządów uznali, że sama Policja nie zapewni im bezpieczeństwa. W wielu gminach zaczęły więc funkcjonować komisje ds. porządku i bezpieczeństwa publicznego. Podlegają one radzie gminy, które przedkładają plan pracy oraz okresowe sprawozdania ze swej działalności (art. 21 ustawy o samorządzie gminnym). W zakresie spraw nieuregulowanych w odrębnych ustawach lub innych przepisach powszechnie obowiązujących, rada gminy uzyskała również uprawnienia o charakterze legislacyjnym. Prawo wydawania przepisów porządkowych ma zastosowanie w sytuacji, gdy jest to niezbędne dla ochrony życia lub zdrowia obywateli oraz dla zapewnienia porządku, spokoju i bezpieczeństwa publicznego (art. 40 ust. 3 ustawy o samorządzie gminnym). Kolejnym etapem demonopolizacji bezpieczeństwa było uchwalenie przez Sejm w dniu 5 czerwca 1998 r. kolejnej ustawy rozszerzającej prerogatywy samorządowe w tym obszarze na poziom powiatowy. Powiatom powierzono wykonywanie określonych ustawami zadań publicznych, także w zakresie porządku publicznego i bezpieczeństwa obywateli (art. 4 ust. 1 pkt 15 ustawy o samorządzie powiatowym). Ważną prerogatywą rady powiatu jest uchwalanie powiatowego programu zapobiegania przestępczości oraz ochrony bezpieczeństwa obywateli i porządku publicznego. Do kompetencji komisji należy: ocena zagrożeń porządku publicznego i bezpieczeństwa obywateli na terenie powiatu; opiniowanie pracy Policji i innych powiatowych służb, inspekcji i straży, a także jednostek organizacyjnych wykonujących na terenie powiatu zadania z zakresu porządku publicznego i bezpieczeństwa obywateli; przygotowywanie projektu powiatowego programu zapobiegania przestępczości oraz porządku publicznego i bezpieczeństwa obywateli; opiniowanie projektów programów współdziałania Policji i innych powiatowych służb, inspekcji i straży oraz jednostek organizacyjnych wykonujących na terenie powiatu zadania z zakresu porządku publicznego i bezpieczeństwa obywateli.

W ramach demonopolizacji bezpieczeństwa państwo przyznało prawo administrowania porządkiem i bezpieczeństwem publicznym organom samorządowym, co jednak nie oznacza pozbawienia organów rządowych kompetencji w zakresie realizacji tych zadań. Nadal utrzymywanie

bezpieczeństwa pozostaje przede wszystkim w gestii służb i formacji należących do administracji rządowej, które wykonują podstawowe zadania w tym obszarze. Działalność podmiotów samorządowych i → specjalistycznych uzbrojonych formacji ochronnych [t. 4] należących głównie do sektora prywatnego, komercyjnego ma jedynie charakter uzupełniający i pomocniczy. Jest to spowodowane tym, że samorządy terytorialne, a tym bardziej prywatne firmy ochrony osób i mienia nie posiadają takich uprawnień jak organy rządowe. Stąd koncentrują one swoją uwagę głównie na działaniach o charakterze ochronnym. Najszerszy zakres uprawnień w zakresie bezpieczeństwa został przekazany na szczebel gminy, która realizuje te zadania głównie poprzez tworzenie straży gminnych (miejskich).

Andrzej Czop

A. Czop, *Prywatny sektor ochrony niedocenianym elementem w zarządzaniu bezpieczeństwem wewnętrznym w Polsce*, [w:] *Współczesne uwarunkowania zarządzania bezpieczeństwem wewnętrznym państwa*, J. Falecki, R. Kochańczyk, P. Sowizdraniuk (red.), Szkoła Policji w Katowicach, Katowice 2018; tenże, *System bezpieczeństwa publicznego w Polsce*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2012, nr 12; tenże, *Udział firm ochrony osób i mienia w zapewnianiu bezpieczeństwa publicznego w Polsce*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Katowice 2014; M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, AON, Warszawa 2014; W. Kawka, *Policja w ujęciu historycznym i współczesnym*, Drukarnia „Zorza", Wilno 1939.

DEPORTACJA (łac. *deportatio* – zesłanie) – przymusowe przeniesienie lub wydalenie osoby lub grupy osób ze stałego miejsca zamieszkania do innego państwa lub innej miejscowości, zwykle pod nadzorem; wygnanie przestępców, przeciwników politycznych lub całych grup etnicznych z → przemocą [t. 3] państwową w odległe miejsca na długie lub dożywotnie przymusowe pobyty. Deportacja całych grup etnicznych może mieć charakter „czystki etnicznej", mającej na celu ujednolicenie narodowościowe (lub wyznaniowe) danego terytorium.

Termin „deportacja" wywodzi się z ustawodawstwa karnego Francji w XVIII–XIX w. i odnosi się do określonych rodzajów wygnania. Po raz

pierwszy deportacja niewiarygodnych politycznie w Gujanie została ustanowiona na mocy ustawy o podejrzanych z 1791 r. Deportacja, w tym deportacja na całe życie, była przewidziana w kodeksie karnym z 1810 r. i polegała na wygnaniu i życiu poza terytoriami kontynentalnymi, w miejscach deportacji określonych ustawą z 23 marca 1872 r. Prawo to przewidywało utworzenie centralnego obozu deportacyjnego na wyspie Well oraz umocnionego miejsca (fortecy) dla deportowanych na półwyspie Duco w Nowej Kaledonii. Deportacja służyła nie tylko do karania przestępców i recydywistów po odbyciu kary w więzieniach metropolitalnych, ale także do radzenia sobie z rewolucjonistami (w 1872 r. schwytani komuniści zostali deportowani na wyspy archipelagu Nowej Kaledonii).

Deportacja jako forma kary była stosowana od czasów starożytnych w różnych kulturach i jest dobrze opisana, szczególnie w starożytnej Mezopotamii. Z ściśle historycznego punktu widzenia Biblia w kilku fragmentach odnosi się do masowych deportacji, obecnie uznawanych za historyczne: przeniesienie dużej części ludności Izraela do Babilonu, najwyraźniej wbrew ich woli i w celach niewolniczych. W czasach cesarstwa rzymskiego różne plemiona były zmuszane do przemieszczania się w kierunku imperium (Traków, Dalmacji) lub poza nie (Niemcy, Celtowie, Madziarowie), z woli armii rzymskiej lub aby uciec przed naporem swoich wrogów. W późnym średniowieczu całe populacje greckie, albańskie i starożytne imperium bizantyjskie zostały zmuszone do wycofania się ze swoich naturalnych granic w kierunku północno-wschodniej Europy ze względu na spotkania armii krzyżowców z Turkami.

Deportacje można podzielić na następujące rodzaje:

- Deportacja więźniów do kolonii karnych – ma długą historię, więźniowie w koloniach mogli w pewnym zakresie swobodnie się przemieszczać. W czasach współczesnych były w dużym stopniu wykorzystywane przez Wielką Brytanię, Australię, Związek Radziecki z obozami karnymi (Gułag), Rosję, Francję, Włochy. W Rosji deportacja więźniów politycznych lub osób po prostu niewygodnych na Syberię była powszechną praktyką od czasów Iwana IV Groźnego i trwa w praktyce nadal, nawet w XXI wieku.
- Deportacja niechcianych osób – obejmuje osoby, które nie popełniły żadnych przestępstw, ale nie chcą pozostać na miejscu.

Takie deportacje były przeprowadzane w różnym stopniu przez właściwie wszystkie → d y k t a t u r y.

- Deportacja grup osób – w latach 1863–1880 miały miejsce masowe deportacje z Polski na Syberię. Konflikty narodowościowe dawały częste okazje do deportacji mniejszości.
- Deportacje na podstawie umów – np. deportacje rdzennych Amerykanów oparte o ustawę o przeprowadzkach z 1830 r. oraz umowy o ich transporcie zawarte między USA a poszczególnymi plemionami indiańskimi, w szczególności przymusowe przesiedlenia z żyznych lasów południowo-wschodnich USA na dość jałowe ziemie mieszczące się w granicach współczesnej Oklahomy. Innymi przykładami mogą być: wymiana ludności między Grecją a Turcją na podstawie traktatu z Lozanny z 24 lipca 1923 r.; porozumienie w sprawie przesiedlenia Południowych Tyrolczyków między Niemcami a Włochami z czerwca 1939 r.; niemiecko-sowiecki traktat o granicy i przyjaźni po podziale Polski, kiedy uzgodniono wymianę mniejszości między Niemcami a Związkiem Radzieckim. Dotknęło to grup etnicznie niemieckich, a także Ukraińców i Białorusinów mieszkających w Niemczech i okupowanej przez Niemcy Polsce. Największym przesiedleniem z udziałem ok. 20 mln osób był podział Indii. W ramach negocjacji niepodległościowych uzgodniono przeprowadzenie relokacji z perspektywy religijnej. Muzułmanie powinni byli przenieść się do nowo powstającego Pakistanu, a Hindusi do Indii. Niewłaściwe przygotowanie, nieodpowiednie wsparcie i niesprawiedliwości związane z przesiedleniem doprowadziły do ataków, zamieszek, gwałtownego przesiedlenia i ucieczek, co poskutkowało około milionem ofiar śmiertelnych.
- Deportacje z przyczyn ekonomicznych – przykładem deportacji z przyczyn ekonomicznych, ale również politycznych są tzw. *Highland Clearances* w Szkocji w XVIII i XIX wieku. W 1707 r. doszło do zawarcia unii pomiędzy Anglią i Szkocją i powstania Królestwa Wielkiej Brytanii. W latach 1715 i 1746 wybuchły krwawo stłumione powstania jakobitów, będące ostatnimi znaczącymi przejawami oporu Szkotów przeciwko dominacji angielskiej. Anglicy, obawiając się kolejnych zamieszek, rozpoczęli egzekucje i deportacje

mieszkańców regionu Highlands; przystąpili do likwidacji struktury klanów, zabronili również przestrzegania tradycyjnych obyczajów. Chłopi, pozbawieni ziemi, emigrowali do Ameryki. Na wyludnionych terenach Anglicy zakładali hodowle owiec. Dopiero wprowadzony w 1886 r. Crofters' Holding Act, który chronił prawa drobnych posiadaczy ziemi, zakończył okres wyludnienia regionu.

- Deportacje grup ludzi do pracy przymusowej – dotknęły obywateli we wszystkich krajach okupowanych przez nazistowskie Niemcy podczas II wojny światowej (niem. *Ostarbeiter* – robotnicy ze wschodu). Od grudnia 1944 r. radzieckie tajne służby NKWD deportowały setki tysięcy niemieckich cywilów do pracy przymusowej w obozie Związku Radzieckiego (Gułag), głównie kobiet. Te cywilne deportacje zostały uznane przez aliantów na konferencji w Jałcie jako reparacje w naturze. Około 1/3 deportowanych zmarło w wyniku uwięzienia z głodu, chorób i zimna lub podczas transportu w wagonach dla bydła. Szacuje się, że 1,7–2 mln ludzi w Kambodży zostało deportowanych do obozów śmierci z powodów polityczno-ideologicznych w czasach Czerwonych Khmerów pod rządami komunistycznego → r e ż i m u [t. 3] Mao Pol Pota, gdzie zostali zamordowani lub umarli podczas pracy przymusowej na polach ryżowych.
- Deportacje jako sankcja – deportacja duńskich funkcjonariuszy → p o l i c j i [t. 3] do niemieckich obozów koncentracyjnych miała miejsce w 1944 r. podczas II wojny światowej po rozbrojeniu i rozwiązaniu duńskiej policji (operacja Möwe). Zatrzymani policjanci zostali najpierw deportowani do obozu koncentracyjnego Neuengamme, a następnie do obozu koncentracyjnego Buchenwald. Natomiast w ZSRR Koreańczykom nie wolno było podróżować poza Azję Środkową i służyć w wojsku, ale poza tym zachowali oni prawa obywateli radzieckich. Mniejszość koreańska to ok. 200 tys. mieszkańców Dalekiego Wschodu, którzy padli ofiarą represji państwowych w 1937 r. Podczas deportacji Koreańczycy zostali załadowani do wagonów bydlęcych, a także przetransportowani do Kazachstanu lub Uzbekistanu. W specjalnych lokalizacjach osadniczych byli wykorzystywani do pracy przymusowej i mieszkali w warunkach

ograniczonych praw i wolności. Większość z nich była wcześniej rolnikami i rybakami i miała trudności z przystosowaniem się do jałowego środowiska Azji Środkowej. Szacuje się, że w pierwszych latach po deportacji zmarło do 40 tys. Koreańczyków. Deportowani Koreańczycy etniczni nie mogli wrócić do domu. Szkoły koreańskie i używanie języka koreańskiego zostały zakazane.

- Deportacje przeciwników politycznych – wiele osób, które oparło się nazistom, zostało deportowanych po dekrecie z 7 grudnia 1941 r., jeżeli nie zostali zabici. Z powodu złych warunków transportu (brak wody, brak powietrza itp.) duża część więźniów zginęła w pociągach w trakcie przewozu.
- Deportacje ze względów religijnych – do XVIII w. deportacje z powodów religijnych miały miejsce w Szwajcarii: menonici zostali wydaleni, zwłaszcza w kantonie Berno, z pomocą państwowych anabaptystów w celu ochrzczenia terytorium. W XX w. w ZSRR w czasach Stalina deportowano na Syberię rosyjsko-niemieckich menonitów oraz Świadków Jehowy i członków ich rodzin.
- Deportacje narodów – były szeroko stosowane w ZSRR, będąc formą represji, stanowiąc rodzaj narzędzia radzieckiej polityki demograficznej i narodowej. Zarówno jednostki, jak i całe narody, uznane przez oficjalne władze za społecznie niebezpieczne, zostały poddane przymusowej migracji do odległych części kraju. Deportacja ludności była przymusową relokacją obywateli z przyczyn narodowych i społecznych do różnych regionów ZSRR. W zależności od przyczyn przesiedlenia i potrzeb ekonomicznych państwa docelowe miejsca deportacji były różne – Syberia, miasta Uralu, Kazachstan, Azja Środkowa i in.
- Deportacja osób – wszystkie kraje zastrzegają sobie prawo do deportacji osób bez prawa pobytu, nawet tych, które są rezydentami długoterminowymi lub posiadają stałe miejsce zamieszkania. Zasadniczo cudzoziemcy, którzy popełnili poważne przestępstwa, nielegalnie wjechali do kraju, przedłużyli lub złamali warunki wizy lub w inny sposób utracili status prawny umożliwiający pozostanie w kraju, mogą zostać administracyjnie wydaleni lub deportowani. W niektórych przypadkach nawet obywatele mogą

być deportowani. Niektóre kraje zachodnie mają również możliwość deportacji obywateli, jeśli mają inną narodowość lub nabywają obywatelstwo w wyniku oszustwa. Np. w latach 30. XX w., podczas Wielkiego Kryzysu, bardziej rygorystyczne egzekwowanie przepisów imigracyjnych doprowadziło do wydalenia nawet 2 mln obywateli Meksyku z USA. Deportacja często wymaga określonego procesu, który musi zostać zatwierdzony przez sąd, lub uprawnień wyższego urzędnika państwowego.

Począwszy od lat 20. XX wieku, deportacje osiągnęły szczyt w pierwszej połowie lat 30. XX wieku, kiedy to miliony chłopów z Ukrainy, Białorusi i Korei zostały deportowane na Syberię i na daleką północ ZSRR. Pierwsza deportacja w historii ZSRR, która miała miejsce ze względu na narodowość, dotyczyła Finów. W 1935 r. podjęto decyzję o wydaleniu ludności fińskiej z obszarów przygranicznych na północnym zachodzie. Kilkadziesiąt tysięcy Finów z Petersburga przeniesiono do obwodu wołogodzkiego. Była to jedna z pierwszych z serii operacji mających na celu „oczyszczenie" granic i przygotowanie się do działań wojennych.

Wraz z wybuchem II wojny światowej deportacja mniejszości etnicznych osiągnęła największy zasięg. Całe ludy zostały wspólnie „ukarane". Oskarżenie o „zdradę" sowieckiego systemu było regularnie podawane jako oficjalny powód deportacji. W wyniku przymusowych eksmisji w latach 1939–1940 ucierpiała ludność zachodniej Ukrainy, zachodniej Białorusi i państw bałtyckich. W czasie → w o j n y [t. 4] w latach 1941–1944 Niemcy zostali deportowani na odległe obszary Syberii, podobnie przedstawiciele narodów, których kraje były członkami koalicji hitlerowskiej (Węgrzy, Bułgarzy, Finowie).

Najbardziej brutalne były deportacje wojenne. W latach 1942–1945 Kałmucy, Niemcy, Finowie, Tatarzy krymscy, Karaczajowie, Czeczeni, Bałkani, Turcy meschetyńscy i inne ludy, mieszkańcy terytoriów radzieckich pod okupacją niemiecką, obywatele Europy Wschodniej, w tym rosyjscy emigranci, zostali deportowani. Po sowietyzacji Mandżurii w sierpniu i wrześniu 1945 r. chińscy, japońscy i rosyjscy emigranci również zostali deportowani. W 1944 r. pod zarzutem współpracy z Niemcami przymusowo zostali zmuszeni do eksmisji Tatarzy krymscy, Kałmucy, Inguszowie, Czeczeni, Karaczajowie, Bałkarzy, Nogajowie, Turcy meschetyńscy.

Szacuje się, że wewnętrzne przymusowe migracje w ZSRR dotknęły ok. 6 mln ludzi. Spośród nich zginęło ok. 1–1,5 mln osób. Deportacjom towarzyszyła likwidacja ich autonomii.

W wyniku deportacji narodów etnicznych z Kaukazu Północnego i Krymu ok. 870 tys. osób musiało opuścić swoje domy. Wraz z Niemcami liczba deportowanych obywateli w latach wojny 1941–1945 wynosiła ok. 2,3 mln osób. Opuszczone obszary zostały ponownie zaludnione przez rosyjskojęzycznych obywateli. Łącznie daje to ok. 3 mln ofiar całkowitej deportacji etnicznej.

Rehabilitacja deportowanych ludów w ZSRR rozpoczęła się w latach 1957–1958, a ograniczenia zostały ostatecznie zniesione 14 listopada 1989 r. Deklaracją Rady Najwyższej ZSRR.

Po „przymusowej emigracji" i wydaleniu Żydów z Niemiec po rozpoczęciu wojny niemiecko-radzieckiej 22 czerwca 1941 r. zaczęła się systematyczna deportacja i mordowanie wszystkich europejskich Żydów w obozach koncentracyjnych. Z tzw. względów higieny rasowej naziści zmuszali zarówno żydowskich Niemców, jak i żydowskich mieszkańców terenów okupowanych i kontrolowanych przez Niemcy w czasie II wojny światowej w Europie Zachodniej, a zwłaszcza w Europie Wschodniej (w tym w Belgii, Danii, Francji, Grecji, Luksemburgu, Holandii, Norwegii, Polsce i Węgrach).

Proces przymusowego wysiedlenia niemieckiej ludności krajów Europy Wschodniej do Niemiec i Austrii miał miejsce w latach 1945–1950 po klęsce Niemiec w II wojnie światowej. W sumie ok. 12–14 mln Niemców zostało poddanych przymusowej eksmisji. Procesowi wydalenia Niemców z Europy Wschodniej towarzyszyła zorganizowana przemoc o ogromnych rozmiarach, w tym konfiskata całej własności, umieszczanie niemieckich cywilów w obozach koncentracyjnych, pomimo uznania deportacji za →zbrodnię przeciwko ludzkości [t. 4] podczas trybunału wojskowego w Norymberdze w sierpniu 1945 r.

W przeciwieństwie do terminu deportacji istnieje definicja przymusowego wygnania, która opiera się głównie na ograniczeniach swobodnego rozwoju jednostki w pierwotnym miejscu zamieszkania. W nowo wybranym miejscu docelowym państwo odpowiedzialne za wygnanie nie nakłada ograniczeń ani sankcji na wolność osobistą. Termin „migracja

przymusowa", który obejmuje także przesiedlenia, dominował w latach 80. XX w., ponieważ miał zastosowanie do różnych rodzajów przemieszczeń ludności w XX w. i określał masową przemoc jako główną ich przyczynę.

Ochronę prawną przed deportacjami zapewnia Powszechna Deklaracja Praw Człowieka ONZ (art. 9 i 12) w czasach pokoju oraz art. 49 IV Konwencji genewskiej z 12 sierpnia 1949 r. w czasie wojny lub okupacji wojskowej. Jeżeli deportacja wiąże się z pracą przymusową, narusza ona art. 4 Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności (ETPC), zgodnie z którym nikt nie może zostać wydalony z terytorium państwa, którego jest obywatelem, i żadnemu obywatelowi nie może być zakazany wjazd na jego terytorium. Zgodnie z art. 7 Rzymskiego Statutu Międzynarodowego Trybunału Karnego z 17 lipca 1998 r. „deportacja lub przymusowe przemieszczanie ludności" odnosi się do zbrodni przeciwko ludzkości i pociąga za sobą międzynarodową odpowiedzialność karną. Deportacje są ścigane przez →Międzynarodowy Trybunał Karny [t. 3] w Hadze jako zbrodnie przeciwko ludzkości (w czasie pokoju) lub jako →zbrodnie wojenne [t. 4]. Już w prawie naturalnym XVIII w. filozofowie zgodzili się, że wydalenie narodu z terytorium, w którym historycznie zamieszkuje, jest niedopuszczalne. Pod koniec XX wieku Organizacja Narodów Zjednoczonych opracowała kodeks dotyczący zbrodni przeciwko ludzkości. Art. 18 kodeksu zbrodni przeciwko pokojowi i →bezpieczeństwu [t. 1] ludzkości określa arbitralną lub przymusową deportację na dużą skalę jako zbrodnię przeciwko ludzkości.

Obecnie termin deportacja jest równoznaczny z wydaleniem administracyjnym i oznacza rodzaj kary administracyjnej stosowanej wyłącznie wobec cudzoziemców lub bezpaństwowców, polegający na ich kontrolowanym, dobrowolnym wyjeździe lub przymusowym wydaleniu (w tym pod eskortą) z kraju przyjmującego.

Olga Wasiuta

S. Ciesielski, G. Hryciuk, A. Srebrakowski, *Masowe deportacje ludności w Związku Radzieckim*, Wydawnictwo Adam Marszałek, Toruń 2003; ciż, *Masowe deportacje radzieckie w okresie II wojny światowej. Prace Historyczne*, Instytut Historyczny Uniwersytetu Wrocławskiego, Wrocław 1994; S. Ciesielski, W. Materski,

A. Paczkowski, *Represje sowieckie wobec Polaków i obywateli polskich*, Ośrodek Karta, Warszawa 2000; P. Christensen, *The Decline of Iranshahr: Irrigation and Environments in the History of the Middle East, 500 B.C. to A.D. 1500*, Museum Tusculanum Press, Copenhagen 1993; R. Conquest, *The Nation Killers*, Macmillan, New York 1970; S. Coutin, *Exiled by Law: Deportation and the Inviolability of Life*, [w:] *The Deportation Regime: Sovereignty, Space, and the Freedom of Movement*, N. De Genova, N. Peutz (ed.), Duke University Press Books, Durham 2010; R. Daniels, *Coming to America: A History of Immigration and Ethnicity in American Life*, HarperCollins, New York 2002; R. Fischer, J.C. Leggett, *Stalin and German Communism: A Study in the Origins of the State Party*, Transaction Publishers, New York 2006; A.T. Fragomen, S.C. Bell, *Immigration Fundamentals: A Guide to Law and Practice*, Practising Law Institute, New York 1996; A. Gil, *Deportacja Ukraińców z Polski w latach 1944–1946 jako problem we współczesnych relacjach polsko-ukraińskich*, Instytut Europy Środkowo-Wschodniej, Warszawa 2004; B.O. Hing, *Defining America Through Immigration Policy*, Temple University Press, Philadelphia 2004; A.M. Jaimoukha, *The Chechens: A Handbook*, Routledge, Florence 2005; E. Mawdsley, *The Stalin Years: The Soviet Union 1929–1953*, Manchester University Press, Manchester 2003; A. Radziwinowiczówna, *Doświadczenie deportacji: przemoc orężem suwerenności*, „Praktyka Teoretyczna" 2016, nr 3 (21).

DETEKTYWISTYKA – to regulowana działalność gospodarcza prowadzona przez przedsiębiorcę posiadającego wpis do rejestru prowadzonego przez ministra właściwego do spraw wewnętrznych, polegająca na świadczeniu usług detektywistycznych.

Podstawowym aktem prawnym, który traktuje o prowadzeniu działalności gospodarczej, jest Konstytucja Rzeczypospolitej Polskiej, która w art. 20 stanowi, że społeczna gospodarka rynkowa jest oparta na wolności działalności gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych, będąc podstawą ustroju gospodarczego RP. Ograniczenie wolności działalności gospodarczej jest dopuszczalne wyjątkowo i może nastąpić jedynie w drodze ustawy, o ile wymaga tego ważny interes publiczny.

Definicja działalności gospodarczej określona w Ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej wskazuje, że jest to: zarobkowa działalność wytwórcza, budowlana, handlowa, usługowa oraz poszukiwanie, rozpoznawanie i wydobywanie kopalin ze złóż, a także działalność zawodowa, wykonywana w sposób zorganizowany i ciągły.

Ważnym desygnatem tej działalności jest jej charakter zarobkowy, co oznacza, że przedsiębiorca winien w swej aktywności dążyć do odniesienia zysku. Przedsiębiorcą może być osoba fizyczna, osoba prawna i jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznaje zdolność prawną – wykonująca we własnym imieniu działalność gospodarczą. *Expressis verbis* ustawodawca wskazuje, że dany podmiot, aby mógł zostać uznany za przedsiębiorcę, musi posiadać zdolność prawną. Przedsiębiorca prowadzi działalność gospodarczą w imieniu własnym, co świadczy o jego autonomii prawnej i nabywaniu bezpośrednim praw i obowiązków w stosunkach cywilnoprawnych.

Przedsiębiorca prowadzący firmę detektywistyczną świadczy usługi polegające na uzyskiwaniu, przetwarzaniu i przekazywaniu →informacji o osobach, przedmiotach i zdarzeniach. Są one realizowane na podstawie umowy zawartej ze zleceniodawcą, w formach i w zakresach niezastrzeżonych dla organów i instytucji państwowych. W szczególności działania te obejmują sprawy wynikające ze stosunków prawnych dotyczących osób fizycznych oraz sprawy wynikające ze stosunków gospodarczych. W tym obszarze mogą dotyczyć wykonania zobowiązań majątkowych, zdolności płatniczych lub wiarygodności w tych stosunkach, a także bezprawnego wykorzystywania nazw handlowych lub znaków towarowych. Przedmiotem usług detektywistycznych mogą być też przejawy nieuczciwej konkurencji lub kwestie ujawnienia wiadomości stanowiących tajemnicę przedsiębiorstwa lub tajemnicę handlową. Usługi mogą też dotyczyć wiarygodności informacji o szkodach zgłaszanych zakładom ubezpieczeniowym.

Osobnym obszarem aktywności detektywistycznej jest poszukiwanie osób zaginionych lub ukrywających się oraz poszukiwanie mienia. Detektywi mogą również zbierać informacje w sprawie, w której toczy się postępowanie karne, postępowanie w sprawach o przestępstwa skarbowe lub wykroczenia skarbowe, ale zleceniodawcą tych czynności nie mogą być organy prowadzące lub nadzorujące postępowania w tych sprawach. Wykonywanie działalności gospodarczej w zakresie usług detektywistycznych jest działalnością regulowaną w rozumieniu przepisów Ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej i wymaga uzyskania wpisu do rejestru działalności detektywistycznej. Działalność

regulowana to taka działalność gospodarcza, której wykonywanie wymaga posiadania określonych kwalifikacji i dozwolona jest dopiero po uzyskaniu zezwolenia, które można zdobyć po spełnieniu wymogów określonych przepisami prawnymi danego państwa.

Wg Dyrektywy 2005/36/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. zawód regulowany to działalność zawodowa lub zespół działalności zawodowych, których podjęcie, wykonywanie lub jeden ze sposobów wykonywania wymaga posiadania specjalnych kwalifikacji zawodowych. W szczególności używanie tytułu zawodowego zastrzeżone jest na mocy przepisów ustawowych, wykonawczych i administracyjnych dla osób posiadających odpowiednie kwalifikacje zawodowe.

Polskie prawo stanowi, że tytułu zawodowego „detektyw" może używać wyłącznie osoba posiadająca licencję. Przedsiębiorca będący osobą fizyczną może wykonywać działalność detektywistyczną, o ile posiada licencję detektywa lub ustanowił pełnomocnika, który ma taką licencję. W przypadku przedsiębiorcy niebędącego osobą fizyczną licencję musi posiadać co najmniej jedna osoba uprawniona do reprezentowania firmy lub pełnomocnik ustanowiony przez przedsiębiorcę do kierowania działalnością detektywistyczną. Przedsiębiorca ten nie może być wpisany do rejestru dłużników niewypłacalnych Krajowego Rejestru Sądowego. Osoby nieposiadające licencji, wchodzące w skład organu zarządzającego przedsiębiorcy oraz ustanowieni przez ten organ prokurenci i przedsiębiorca będący osobą fizyczną nie mogą być osobami wcześniej karanymi za przestępstwa umyślne lub umyślne przestępstwa skarbowe. Organem prowadzącym rejestr firm detektywistycznych jest minister właściwy do spraw wewnętrznych.

Przedsiębiorca jest zobowiązany do zachowania formy pisemnej umów w zakresie usług detektywistycznych. Musi też prowadzić oraz przechowywać dokumentację dotyczącą zatrudnianych detektywów oraz zawieranych i realizowanych umów. Jest zobowiązany do przedstawiania tej dokumentacji, na żądanie upoważnionego do kontroli organu. Ponadto ma zachować w tajemnicy źródła informacji oraz okoliczności sprawy, o których dowiedział się w związku z wykonywaniem zlecenia. Ponosi również, na zasadach określonych w kodeksie cywilnym, odpowiedzialność za wszelkie szkody wyrządzone podczas wykonywania usług

detektywistycznych oraz wskutek podania nieprawdziwych informacji. W związku z tym na przedsiębiorcy ciąży też obowiązek zawarcia umowy ubezpieczenia od odpowiedzialności cywilnej za takie właśnie szkody. Przedsiębiorca może sam wykonywać czynności detektywistyczne, o ile posiada licencję detektywa lub może przekazać ich realizację zatrudnionym pracownikom, którzy uzyskali takie licencje.

O wydanie licencji detektywa może ubiegać się osoba, która posiada obywatelstwo polskie lub obywatelstwo innego państwa członkowskiego Unii Europejskiej lub przysługuje jej, na podstawie umów międzynarodowych lub przepisów prawa UE, prawo do podjęcia zatrudnienia lub wykonywania działalności gospodarczej na terytorium RP. Musi mieć ukończone 21 lat i posiadać wykształcenie co najmniej średnie. Koniecznym warunkiem jest także pełna zdolność kandydata do czynności prawnych. Nie może toczyć się przeciwko niemu postępowanie o umyślne przestępstwo lub umyślne przestępstwo skarbowe. Nie może to być osoba skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe ani też zwolniona dyscyplinarnie z → Policji [t. 3], → Straży Granicznej [t. 4], → Agencji Bezpieczeństwa Wewnętrznego [t. 1], → Agencji Wywiadu [t. 1], → Służby Ochrony Państwa [t. 4], wojska, → prokuratury [t. 3], sądu lub z innego urzędu administracji publicznej w RP lub innym państwie, w okresie ostatnich 5 lat. Konieczne jest posiadanie pozytywnej opinii wydawanej przez komendanta powiatowego (rejonowego, miejskiego) Policji właściwego ze względu na miejsce zamieszkania kandydata. W toku badań lekarskich stwierdzana jest jego zdolność fizyczna i psychiczna do wykonywania czynności detektywa.

Przyszły detektyw musi legitymować się dokumentem potwierdzającym odbycie szkolenia w zakresie: zagadnień ochrony danych osobowych, ochrony → informacji niejawnych, przepisów regulujących prawa i obowiązki detektywa oraz zasad wykonywania działalności gospodarczej w zakresie usług detektywistycznych. Licencję w drodze decyzji administracyjnej wydaje lub odmawia jej wydania komendant wojewódzki Policji właściwy ze względu na miejsce zamieszkania osoby ubiegającej się o wydanie licencji. W przypadku osoby niemającej miejsca zamieszkania na terytorium RP organem właściwym jest Komendant Stołeczny Policji.

Wprawdzie licencję wydaje się na czas nieoznaczony, ale jej posiadacz jest obowiązany poddawać się okresowym badaniom lekarskim i psychologicznym. Detektyw powinien przy wykonywaniu czynności kierować się zasadami etyki, lojalnością wobec zlecającego usługę i szczególną starannością, aby nie naruszyć wolności i → p r a w c z ł o w i e k a [t. 3] i obywatela. Wykonuje bowiem zawód zaufania publicznego. Trybunał Konstytucyjny w orzeczeniu z 7 maja 2002 r. (w sprawie SK 20/00) orzekł, że

> „zawód zaufania publicznego" to zawód polegający na obsłudze osobistych potrzeb ludzkich, wiążący się z przyjmowaniem informacji dotyczących życia osobistego i zorganizowany w sposób uzasadniający przekonanie społeczne o właściwym dla interesów jednostki wykorzystywaniu tych informacji przez świadczących usługi.

Nie ma żadnych wątpliwości, że detektyw spełnia wskazane w tym wyroku warunki.

W trakcie wykonywania czynności detektyw może uzyskiwać informacje zarówno od osób fizycznych i przedsiębiorców, jak i od instytucji, a także organów administracji rządowej lub samorządowej. Detektyw podczas pracy jest obowiązany do przestrzegania przepisów prawa oraz odmowy wykonania czynności niezgodnej z prawem lub nieetycznej. Musi także zachować należytą staranność i rzetelność, a zwłaszcza sprawdzać zgodność z prawdą uzyskanych informacji. Ma obowiązek zachować w tajemnicy źródła informacji oraz okoliczności sprawy, o których dowiedział się w trakcie wykonywania zleconych czynności. Ten obowiązek ciąży na nim także po zaprzestaniu pracy w zawodzie detektywa. Wykonując powierzone mu czynności, musi mieć przy sobie licencję oraz okazywać ją na żądanie osoby, której czynności dotyczą. Detektyw nie może stosować środków technicznych oraz metod i → c z y n n o ś c i o p e r a c y j n o - r o z p o z n a w c z y c h [t. 1] zastrzeżonych dla upoważnionych organów na mocy odrębnych przepisów. Oznacza to, że nie wolno mu stosować → p o d s ł u c h ó w [t. 3], gdyż naraża się wówczas na odpowiedzialność karną określoną w art. 267 kk § 3. Przepis ten przewiduje karę za uzyskiwanie informacji poprzez zakładanie lub posługiwanie się

urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

23 marca 2011 r. SN odmówił odpowiedzi na pytanie prawne sądu w sprawie detektywa – oskarżonego przez pewną kobietę o umieszczenie lokalizatora GPS w jej aucie – ale zarazem wypowiedział się co do istoty sprawy. Sąd pytał, czy takie zainstalowanie GPS dopuszcza ustawa o usługach detektywistycznych, czy też jest ono czynnością operacyjno-rozpoznawczą zastrzeżoną dla „upoważnionych organów". Sędzia SN A. Ryński mówił, że ustawa o usługach detektywistycznych nie ogranicza rodzaju informacji zdobywanych przez detektywów, ale ogranicza środki ich uzyskiwania. Detektyw może zatem zdobywać informacje wkraczające np. w kwestie relacji małżeńskich – uznano. Ale już środki techniczne niejawnego zdobywania informacji są zastrzeżone dla organów państwa. SN powołał się m.in. na wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu, który w 2010 r. uznał, że użycie lokalizatora GPS może prowadzić do naruszenia prawa do prywatności, także przez organy władzy. Ryński podkreślił, że w Niemczech zgodę na użycie GPS przez służby wydaje prokurator generalny. Jedyne szczególne uprawnienie nadane detektywowi – szersze niż wynikające z uprawnień obywatelskich – to prawo do przetwarzania danych osobowych zebranych w toku wykonywanej usługi bez zgody osób, których informacje dotyczą. Jednak ustawodawca zastrzegł, że nie może być to czynione dla innego podmiotu, a sam proces powinien być zgodny z przepisami ustawy o ochronie danych osobowych z wyłączeniem przepisów dotyczących konieczności uzyskania zgody. Można zatem powiedzieć, że profesja detektywa jest związana z dużym ryzykiem prawnym.

Andrzej Czop

M. Berent, W.J. Modrakowski, *Etyka zawodu detektywa w kontekście standardu minimalnego Internationale Kommission der Detektiv-Verbände*, „Krytyka Prawa" 2016, nr 1, t. 8; D. Brakoniecki, *Detektywistyka – prawne i funkcjonalne aspekty działalności detektywistycznej w Polsce i na świecie*, Difin, Warszawa 2016; G. Gozdór, *Usługi detektywistyczne. Komentarz*, Wydawnictwo C.H.Beck, Warszawa 2014; J. Konieczny, T. Aleksandrowicz, A. Konik, *Podstawy detektywistyki. Usługi detektywistyczne*, *prawo, taktyka, moralność*, Wydawnictwa Akademickie i Profesjonalne,

Warszawa 2008; K. Turaliński, *Wywiad Gospodarczy i Polityczny – podręcznik dla specjalistów ds. bezpieczeństwa, detektywów i doradców gospodarczych*, Wydawnictwo ARTEFAKT.edu.pl, Warszawa 2015; Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych, Dz. U. 2002, nr 12, poz. 110.

DEZERCJA – ucieczka, zbiegostwo →żołnierzy [t. 4] z armii, porzucenie pełnionej służby, samowolne oddalenie się z pola walki, samowolne opuszczenie wojska w czasie pokoju lub w czasie →wojny [t. 4] lub inne zachowanie cechujące się rezygnacją z czegoś z powodu braku odwagi, by stawić czoła trudnościom.

Pojęcie dezercji znane jest polskiemu prawu karnemu – przestępstwo to polega na opuszczeniu jednostki lub wyznaczonego miejsca przebywania lub pozostaniu w takim miejscu – może ono zostać popełnione zarówno przez działanie, jak i przez zaniechanie. Jest to przestępstwo indywidualne, czyli takie, które popełnić może wyłącznie osoba pełniąca czynną służbę wojskową, z wyjątkiem terytorialnej służby wojskowej pełnionej dyspozycyjnie. Definicja legalna żołnierza ujęta została w z art. 115 § 17 kk. Dalsze doprecyzowanie tego pojęcia zawiera ustawa o służbie wojskowej żołnierzy zawodowych (art. 3 ust. 1 i 1a oraz art. 124) oraz ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (art. 59).

Jednostką wojskową jest natomiast wyodrębniony administracyjnie i gospodarczo oddział lub instytucja wojskowa rozlokowana w wyraźnie wskazanym rejonie lub miejscu. Wyznaczone miejsce przebywania definiuje się jako znajdujący się poza jednostką wojskową rejon (np. szpital, warsztat, plac ćwiczeń, poligon, magazyn, areszt dyscyplinarny, sąd, żandarmeria czy →prokuratura [t. 3]), do którego żołnierz jest oddelegowany w celu wykonywania określonych zadań związanych ze służbą.

Od dezercji odróżnić należy samowolne opuszczenie przez żołnierza jednostki lub wyznaczonego miejsca przebywania albo samowolne poza nimi pozostawanie w wymiarze nieprzekraczającym jednorazowo 48 godzin, które stanowi odrębne przestępstwo zgodnie z art. 338 § 1 kk, jeżeli miało miejsce przynajmniej 2-krotnie w okresie 3 miesięcy. Sposób popełnienia przestępstwa w obu przypadkach jest zbliżony, różnią się one jednak zamiarem przyświecającym sprawcy. W obu przypadkach żołnierz świadomie łamie zasady →dyscypliny wojskowej, jednak

dla uznania jego absencji za dezercję konieczne jest nie tylko stwierdzenie, że trwała ona dłużej niż 48 godzin, ale też że jego celem było trwałe uchylanie się od służby wojskowej.

Typy kwalifikowane przestępstwa dezercji dotyczą sytuacji, gdy wystąpiła przynajmniej jedna z następujących okoliczności: dezerter działał wspólnie z innymi żołnierzami lub dokonał zaboru broni albo dezerter podjął ucieczkę za granicę bądź też uchylał się od powrotu do kraju z zagranicy. Każdy z tych przypadków zagrożony jest wyższą karą niż popełnienie przestępstwa w typie podstawowym.

Kodeks wprowadza karalność czynności przygotowawczych do wszystkich odmian przestępstwa dezercji, także do odmiany podstawowej.

Aktualnie obowiązujący kodeks karny z 1997 r. przyniósł złagodzenie podejścia ustawodawcy do przestępstwa dezercji. Warto zauważyć, że wszystkie typy przestępstwa dezercji stanowią występki, a nie zbrodnie. Odmiennie natomiast kwestia ta była uregulowana w poprzednio obowiązującym kodeksie karnym z 1969 r., w którym typy kwalifikowane dezercji, z uwagi na wymiar grożącej za nie kary, stanowiły zbrodnie. Zmiany zaszły także w sposobie ujęcia typów kwalifikowanych: kodeks z 1969 r. zawierał sformułowanie „dopuszcza się dezercji z zamiarem ucieczki za granicę lub urzeczywistnia taki zamiar w czasie trwania dezercji", co potencjalnie dawało szersze możliwości surowego ukarania poprzez relatywnie łatwą możliwość przypisania zamiaru ucieczki za granicę. Ponadto wydatnie złagodzono sankcje, różnicując równocześnie surowość ustawowego → z a g r o ż e n i a [t. 4] w zależności od tego, czy chodzi o dezercję zbiorową lub dezercję łączącą się z zabraniem broni, czy też dezercję połączoną z ucieczką za granicę lub uchylaniem się od powrotu do kraju – wcześniej groziła za to jednakowa sankcja: kara pozbawienia wolności od lat 3 do 15. Kodeks Karny Wojska Polskiego z 1957 r. za dezercję w czasie wojny połączoną z zaborem broni oraz za dezercję zbiorową w czasie wojny przewidywał obok kary więzienia także karę śmierci. Dla porównania, wojskowy kodeks karny z 1932 r. za opuszczenie jednostki lub stanowiska służbowego wbrew obowiązkowi służbowemu groził więzieniem do lat 2, w czasie wojny do lat 3. W przypadku, gdy sprawca działał w zamiarze trwałego uchylenia się od obowiązku wojskowego bądź gdy nieobecność w jednostce trwała dłużej niż 6 miesięcy, czyn był zagrożony karą pozbawienia wolności do

lat 10, jego popełnienie w czasie wojny skutkowało podniesieniem dolnego pułapu kary od 1 roku pozbawienia wolności. Dopuszczenie się dezercji w obliczu nieprzyjaciela karane było śmiercią.

Problematyka dezercji nie jest szeroko ujmowana w prawie międzynarodowym. Przyjmuje się, że dezerterom przysługuje status jeńców wojennych.

Anna Pacholska

J. Majewski, *Art. 338*, [w:] *Kodeks Karny. Część szczególna. Tom III. Komentarz do art. 278–363,* A. Zoll (red.), Wolters Kluwer Polska, Warszawa 2016; A. Pacholska, *Dezercja*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; S.M. Pryjemski, M. Rogacka-Rzewnicka, *Przestępstwa przeciwko obowiązkowi pełnienia służby wojskowej i przeciwko zasadom pełnienia służby*, [w:] *System Prawa Karnego. Tom 11. Szczególne dziedziny prawa karnego. Prawo karne wojskowe, skarbowe i pozakodeksowe*, M. Bojarski (red.), Wydawnictwa C.H.Beck, Instytut Nauk Prawnych PAN, Warszawa 2018; Ustawa z dnia 6 czerwca 1997 r., Kodeks karny, Dz. U. 2019.1950 t.j.

DEZERCJA W ARMIACH EUROPEJSKICH – zjawisko →dezercji jest znane od starożytności, zawsze stanowiły one jedno z najpoważniejszych →zagrożeń [t. 4] dla stabilnego funkcjonowania każdej armii. W kodeksach wojskowych dezercje traktowano jako poważne przestępstwo. Do XIX w. dezercje prawie zawsze były karane wyrokiem śmierci. Rozstrzelanie dezerterów orzekały sądy wojskowe, często sądy doraźne, a wykonywały specjalne plutony egzekucyjne. XIX w. przyniósł jednak zmiany w ocenie dezercji. Zaczęto rozróżniać długotrwałą ucieczkę z armii, czyli dezercję, i krótkotrwałe tzw. samowolne oddalenie się, po którym →żołnierze [t. 4] dobrowolnie powracali do macierzystych jednostek wojskowych. W wielu państwach zaczęto zupełnie odmiennie traktować zbiegostwo w czasie pokoju i w czasie walki. W większości kodeksów wojskowych dezercje z pola walki były znacznie bardziej surowo karane niż ucieczki w czasie pokoju, a nawet z miejsca bazowania pułku znacznie oddalonego od linii frontu. W porównaniu z dezercjami spowodowanymi tęsknotą za bliskimi czy też złym traktowaniem przez przełożonych większa odpowiedzialność karna czekała sprawców

tzw. zbiorowych ucieczek, dezerterów dopuszczających się szpiegostwa i zdrady na rzecz wroga lub obcego państwa w czasie pokoju. Poważnych konsekwencji karnych mogli spodziewać się także wszyscy dezerterzy, którzy dopuścili się przestępstw tak na szkodę wojska, jak i osób cywilnych. Kary dla zbiegłych z armii oficerów, żołnierzy szeregowych, a także kary za niestawiennictwo do służby wojskowej regulowały różnego rodzaju rozporządzenia, ustawy i kodeksy wojskowe. Do czasu wybuchu I wojny światowej w Europie był to m.in. francuski wojskowy kodeks karny z 1857 r., uproszczony przez Napoleona III w 1875 r., a także kolejne ustawy z 1893, 1899 i 1909 r., w carskiej Rosji ustawy z 1867 i 1874 r., w Austro-Węgrzech ustawy z 1889 i 1912 r., w Niemczech Niemiecki Kodeks Karny Wojskowy z 1872 r.

Liczba dezercji w wielu armiach europejskich wzrastała jeszcze przed I wojną światową. Przykładowo w 1911 r. w armii rosyjskiej za ucieczki ukarano 8027 żołnierzy, a w 1912 r. już 13358 dezerterów, w 1911 r. we Francji poszukiwano zaś 60 tys. dezerterów i ukrywających się przed służbą wojskową poborowych, co było znacznym wzrostem w stosunku do kilku wcześniejszych lat. Gigantyczną skalę dezercji ukazała dopiero I wojna światowa. Dezercje były jedną z przyczyn rozpadu armii austro-węgierskiej, w której wg węgierskich źródeł wojskowych we wrześniu osiągnęły 800 tys. żołnierzy. Wzrost dezercji notowano już w latach 1914–1915, które ukazały niechęć do służby w cesarsko-królewskiej (c.k.) armii żołnierzy narodowości słowiańskich. Jesienią 1914 r. prym w ucieczkach z pułków austro-węgierskich wiedli Czesi, Słowacy, Serbowie, Chorwaci i Słoweńcy. Pierwszej poważnej dezercji doświadczył 9 Korpus c.k. Armii, z którego tylko w listopadzie 1914 r. zbiegło 5500 żołnierzy, głównie Czechów, najchętniej uciekających na stronę Rosjan, których traktowali jak przyjaciół, wyzwolicieli spod jarzma Habsburgów. Symboliczny był tutaj 3 kwietnia 1915 r. i postawa praskiego 28 Pułku Piechoty, kiedy po kolejnym rosyjskim ataku z praskiego pułku na stronę rosyjską zdezerterowało tysiące oficerów i żołnierzy czeskich. Na stronę wroga nie przeszło jedynie 20 oficerów i 236 żołnierzy, którzy powrócili do zdekompletowanej jednostki. Największych rozmiarów dezercji w czasie I wojny światowej doświadczyła jednak armia rosyjska. Tylko w latach 1915–1916 rosyjska żandarmeria miała zatrzymać 420 tys. dezerterów, choć nie brak również

opinii, że w tym czasie zdezerterowało nawet 1,5 mln żołnierzy. Wzrost liczby dezercji w armii rosyjskiej wynikał z kilku przyczyn:

- niejednolitego składu narodowościowego armii;
- między żołnierzami szeregowymi a oficerami panowały feudalne relacje;
- przedłużająca się → w o j n a [t. 4], a zwłaszcza kolejne klęski militarne działały zniechęcająco na armię, w której przewagę mieli niepiśmienni i zastraszeni chłopi;
- rozkład armii przyspieszał obalenie caratu.

Dezercje w latach 1914–1918 były zjawiskiem nie tylko wstydliwym dla krajów, które przegrały wojnę, ale również dla państw zwycięskich. Po zakończeniu pierwszej wojny światowej w zwycięskiej Francji zwlekano z przedstawieniem faktycznej liczby zbiegłych żołnierzy. Dopiero w 1920 r. francuska → p o l i c j a [t. 3] poinformowała społeczeństwo, że w latach 1914–1918 aresztowano 66 678 francuskich dezerterów. Współcześnie ocenia się, że liczba francuskich dezerterów w czasie Wielkiej Wojny wahała się od 80 do 90 tys. żołnierzy. Bardzo zbliżona liczba dezercji wydarzyła się w armii brytyjskiej. Wielu dezerterów z różnych armii, które walczyły na frontach I wojny światowej, szukało schronienia nie tylko w rodzinnych stronach. Celem ucieczek były neutralne w tej wojnie kraje, takie jak Hiszpania, Portugalia, Dania, Szwecja, a przede wszystkim Holandia i Szwajcaria. Tylko od połowy września 1918 r. do końca grudnia 1918 r. w samej Holandii zarejestrowano aż 4 tys. uciekinierów z armii niemieckiej. Wg jednego z raportów → w y w i a d u [t. 4] armii francuskiej w Genewie w styczniu 1918 r. przebywało 4800 dezerterów z francuskiej armii.

W Rosji na początku 1918 r. bolszewicy stworzyli własne siły zbrojne. 28 stycznia została utworzona Рабоче-крестьянская Красная армия (Rabocze-kresť janskaja Krasnaja armija), powszechnie znana jako Armia Czerwona. Armia bolszewików początkowo składała się z ochotników, ale 29 maja 1918 r. wprowadzono pobór. Dezercje, które były jednym z czynników rozkładu carskiej armii, dały tu o sobie znać niedługo po pierwszym poborze, kiedy z wysłanych przeciwko Korpusowi Czechosłowackiemu 50 tys. żołnierzy w rejonie koncentracji stawiło się jedynie 7 tys. żołnierzy. Większym problem militarno-politycznym dla bolszewików

było pojawienie się tzw. Zielonej Kadry (ZK), żołnierzy zbiegłych z Armii Czerwonej i organizującej własne oddziały. Rosyjskie ZK stworzyły *de facto* groźny, choć niewspółpracujący ze sobą ruch partyzancki, którego ideą była obrona chłopskiej, lokalnej rewolucji. Największe akcje rosyjskie ZK przeprowadzały w rejonie Woroneża, Saratowa, Riazania, Tuły, Niżnego Nowogrodu i Tweru. Zieloni walczyli również z oddziałami Białych, tj. oddziałami wojska opowiadającymi się za przedrewolucyjnym politycznym i ekonomicznym porządkiem, najczęściej jednak atakowały żołnierzy Armii Czerwonej. Kulminacja działań ZK przypadła na wiosnę 1919 r. W końcowej fazie istnienia Austro-Węgier, a także tuż po rozpadzie monarchii Habsburgów oddziały ZK pojawiły się również na terenach Chorwacji, Moraw, Słowacji oraz Galicji. W porównaniu z Chorwacją, a przede wszystkim Morawami Południowymi i Słowacją, działające na terenie Rosji oddziały Zielonych były nie tylko znacznie liczniejsze, ale i zdecydowanie bardziej wrogo nastawione do → k o m u n i z m u.

W międzywojniu żołnierze dezerterowali we wszystkich armiach na świecie. Szczególnie głośne były zagraniczne dezercje oficerów, którzy niejednokrotnie dostarczali wrogim krajom cennych → i n f o r m a c j i. Dla państw takich jak Francja, która przed 1939 r. uchodziła za jedną z militarno-politycznych potęg, dezercja kpt. J. Sadoula wywoływała w latach 20. i 30. XX wieku nie mniejsze emocje niż słynna sprawa Dreyffusa. Kpt. Sadoul został wysłany wraz z francuską misją wojskową do ogarniętej rewolucją Rosji. We wrześniu 1917 r. przeszedł na stronę bolszewików, za co we Francji otrzymał zaoczną karę śmierci. Jego powrót do Francji w 1924 r. zbulwersował → o p i n i ę p u b l i c z n ą [t. 3]. Po procesie Sadoul został uniewinniony i z powodzeniem reprezentował sowieckie interesy we Francji. Duży wstrząs w Rumunii wywołała dezercja por. E. Bodnăraşa który w lutym 1932 r. zbiegł z 12 Pułku Artylerii w Czerniowcach. Już w 1936 r. przerzucono go do ojczyzny jako sowieckiego agenta. W 1942 r. Bodnăraş został na krótko aresztowany. Jego błyskotliwa kariera polityczna rozpoczęła się po objęciu władzy przez komunistów, był m.in. rumuńskim ministrem obrony narodowej. Znacznie bardziej szokowały w latach 30. dezercje oficerów, do których doszło w Niemczech i w Związku Sowieckim. Dla Hitlera z pewnością kłopotem było to, że do Szwajcarii w lipcu 1935 r. uciekło 15 oficerów Reichswehry, którzy pozostawali

do dyspozycji Wehrmachtu. O fakcie tym nie bez satysfakcji informowały francuskie i polskie gazety. Furię Stalina wywoływał fakt, że tylko w maju i czerwcu 1938 r. zbiegło do zajmowanej przez Japończyków Mandżurii 2 wysokich rangą oficerów. Byli to mjr Francewicz i gen. Gienrich Luszkow. Do kilkudziesięciu tysięcy dezercji doszło także w latach 1936–1939, czyli w czasie → w o j n y d o m o w e j [t. 4] w Hiszpanii. Dezerterów nie brakowało tak wśród zwolenników gen. Franco, jak i Republiki.

Świadectwem pokaźnej liczby dezercji są fronty II wojny światowej. W czerwcu 1940 r. Niemcy pokonały jednego z najgroźniejszych politycznych i militarnych przeciwników, czyli Francję. Niebagatelny wpływ na pojawienie się wielu przypadków dezercji we Francji miała agitacja Francuskiej Partii Komunistycznej, która po podpisaniu paktu Ribbentrop–Mołotow wzywała francuskich żołnierzy do porzucenia szeregów armii. Największa skala dezercji nastąpiła w Armii Czerwonej, kiedy 22 czerwca 1941 r. Niemcy uderzyły na swojego niedawnego polityczno-wojskowego sojusznika – Związek Radziecki. Szacuje się, że w pierwszych tygodniach niemieckiej → i n w a z j i na ZSRR zbiegło nawet 700 tys. czerwonoarmistów. Jedni z dezerterów poddawali się Niemcom, inni spieszyli w rodzinne strony. Wyłapywaniem i bardzo często niemal natychmiastowym rozstrzeliwaniem sowieckich dezerterów zajmowały się specjalnie powstałe tzw. oddziały zaporowe Armii Czerwonej, co w jakiś sposób powstrzymywało wzrost liczby dezercji. Na początku 1942 r. Niemcy z jeńców i dezerterów Armii Czerwonej rozpoczęli formowanie tzw. Legionów Wschodnich, w których znaleźli się Ormianie, Azerowie, Czeczeni, Gruzini, Tatarzy i Turkmeni. We wrześniu 1943 r. oddziały sformowane ze wspomnianych grup ludnościowych liczyły 500 tys. żołnierzy. Wiosną 1945 r. nastąpił natomiast gwałtowny wzrost liczby dezercji w Wehrmachcie. W kwietniu 1945 r. jedynie w oblężonym przez Armię Czerwoną Berlinie ukrywało się ok. 50 tys. dezerterów. W latach 1944–1945 niemieccy żołnierze najchętniej dezerterowali do Brytyjczyków i Amerykanów. Znacznie mniejsze dezercje charakteryzowały siły zbrojne aliantów, przykładowo w czasie II wojny światowej w armii brytyjskiej nie przekroczyły one 50 tys. przypadków.

Po 1945 r. do dezercji dochodziło we wszystkich wojskach świecie, włączywszy w to chyba najsilniejszą armię na świecie, czyli siły zbrojne

Stanów Zjednoczonych. Wg danych Pentagonu po wybuchu wojny koreańskiej z armii amerykańskiej zdezerterowało 46 tys. żołnierzy, z czego 35 tys. albo powróciło w szeregi wojska z własnej woli, albo zostało zatrzymanych na skutek działań żandarmerii. Dezercje w czasie wojny w Korei nie wywołały w amerykańskim dowództwie obaw, ponieważ w porównaniu z II wojną światową (ok. 100 tys. dezercji amerykańskich żołnierzy) były znacznie mniejsze. Więcej niepokoju wywoływała wojna w Wietnamie. W 1968 r. raportowano o podwojeniu się dezercji w siłach lądowych i lotniczych USA, nieco mniejszy wzrost tego zjawiska dotyczył jedynie → marynarki wojennej [t. 3]. W 1970 r. dowództwo armii amerykańskiej poinformowało o 65 643 dezerterach, jak podkreślono w meldunku, liczbie żołnierzy odpowiadających 4 amerykańskim dywizjom. Szacuje się, że po otrzymaniu rozkazu wyjazdu do Wietnamu ok. 7 tys. żołnierzy zbiegło ze Stanów Zjednoczonych do Kanady. W obawie przed przerzuceniem do Wietnamu żołnierze amerykańscy uciekali również z → baz wojskowych [t. 1] w Japonii i Niemczech. Z Japonii szukano azylu we wspomnianej Kanadzie, a z Niemiec w Szwecji. Do Kanady zbiegło również ok. 50 tys. młodych przedpoborowych, a także poborowych obawiających się wyjazdu do Wietnamu. Większość z nich deklarowała się jako obdżektorzy. Przyjęcie statusu obdżektora, tj. osoby, która ze względu na sprzeciw sumienia odmawia wojskowej powinności, stało się popularnym sposobem unikania służby wojskowej podczas I wojny w Zatoce Perskiej. W latach 1990–1991 liczba obdżektorów wśród żołnierzy amerykańskich gwałtownie wzrosła, warto przypomnieć, że ponad 2500 żołnierzy amerykańskich, którzy ogłosili się obdżektorami, zostało aresztowanych. Był to w historii USA największy wzrost liczby żołnierzy, którzy ogłosili, że ze względu na sprzeciw sumienia nie mogą dalej pełnić służby wojskowej. We wspomnianych latach ponad 1 tys. rezerwistów amerykańskiej armii powiadomiło władze wojskowe, że są obdżektorami. Wielu weteranów I wojny w Zatoce Perskiej, takich jak sierż. C. Mejia i K. Benderman, publicznie potępiło udział USA w tej wojnie. Trudno stwierdzić, czy takie wypowiedzi zdemotywowały wielu amerykańskich żołnierzy do udziału w II wojnie w Zatoce Perskiej. Z raportu armii amerykańskiej z maja 2005 r. wynikało, że w tym czasie liczba dezercji w wojsku amerykańskim sięgnęła blisko

6 tys. żołnierzy. W latach 1997–2004 w armii amerykańskiej odnotowano łącznie 21 187 dezercji.

Remigiusz Kasprzycki

Armeen und ihre Deserteure. Vernachlässigte Kapitel einer Militärgeschichte der Neuzeit, U. Bröckling, M. Sikora (hg.), Vandenhoeck & Ruprecht, Göttingen 1998; Ch. Glass, *Dezerterzy. Ostatnia nieopowiedziana historia II wojny światowej*, tłum. T. Fiedorek, Dom Wydawniczy Rebis, Poznań 2014; R. Fantina, *Desertion and American soldier 1776–2006*, Algora Publishing, New York 2006; C. Jahr, *Gewöhnliche Soldaten: Desertion und Deserteure im deutschen und britischen Heer 1914–1918*, Vandenhoeck & Ruprecht, Göttingen 1998; R. Kasprzycki, *Ucieczki do Polski żołnierzy z krajów sąsiednich w latach 1920–1939*, „Przegląd Nauk Historycznych" 2017, r. 16, nr 1; L. Milewski, *Dezercja cudzoziemca*, „Wojskowy Przegląd Prawniczy" 1936, r. IX, nr 2; A. Smoliński, *Dezercje z Robotniczo-Chłopskiej Armii Czerwonej w latach 1918– 1922. Wojna z Polską i wojna domowa w Rosji*, „Przegląd Wschodni" 2007, t. 10, z. 3 (39).

DEZERCJE W WOJSKU POLSKIM W XX WIEKU – pierwsze →dezercje [t. 1] w Wojsku Polskim (WP) miały miejsce już w końcu 1918 r., ale dopiero w latach 1918–1921 ucieczki z wojska stały się dość poważnym problemem. Szacuje się, że w czasie wojny polsko-bolszewickiej (1919–1920) z polskiej armii zbiegło lub nie stawiło się w jej szeregi od 100 do 150 tys. dezerterów i poborowych. Dezerterzy porzucali szeregi frontu po zaciętych →bitwach [t. 1], opuszczali także bataliony zapasowe, które stacjonowały w głębi kraju. Przyczyny dezercji były bardzo różne, podobne do występujących w innych walczących armiach na całym świecie; powodowane strachem przed cierpieniem po odniesionych ranach, kalectwem i bezsensowną śmiercią. Były również sposobem zakończenia →przemocy [t. 3], której →żołnierze [t. 4] doświadczyli od przełożonych, niekiedy daleko od linii frontu. To ostatnie spotykało zwłaszcza rekrutów albo ideowo i patriotycznie nastawionych ochotników. Niestety, różne formy psychicznego oraz fizycznego znęcania się nad najmłodszymi stopniem i z najkrótszym stażem służby żołnierzami były smutnym dziedzictwem armii zaborczych, w największym stopniu pozostałością po armii carskiej. Takie problemy starali się wykorzystać komuniści, którzy z początku liczyli, że wywołają rewolucję w polskiej armii

i podporządkują sobie większość oddziałów. Okazało się to niewykonalne, więc wzywano do dezercji. W praktykach tych przodowała →propaganda [t. 3] bolszewicka. Oczekiwania bolszewików, że dezerterzy z WP masowo zasilą Armię Czerwoną, nie sprawdziły się, a nadzieja, że zbiegli polscy żołnierze stworzą silny „czerwony" pułk złożony z ochotników, również okazała się płonna. Ostatnią rzeczą, jakiej pragnęli ukrywający się przed poborem albo dezerterzy z WP, był udział w →wojnie [t. 4] po którejkolwiek ze stron. Najlepszym dowodem tego były tysiące poborowych i dezerterów, którzy w latach 1918–1921 w większości uciekali do Niemiec, a nie do Rosji bolszewickiej. Niestawiennictwo poborowych i dezercje charakteryzowały w tych latach zwłaszcza ludność pochodzącą z polskich wsi wchodzących w skład byłego zaboru rosyjskiego, a także narodowość żydowską. W czasie wojny polsko-bolszewickiej władze wojskowe starały się walczyć ze zjawiskiem dezercji w różny sposób. W miastach i na wyznaczonych obszarach stosowano niespodziewane obławy, a w garnizonach edukowano żołnierzy o negatywnych skutkach dezercji. Latem 1920 r. podjęto szeroką akcję propagandową skierowaną do →ludności cywilnej [t. 3], która miała zniechęcić do jakiejkolwiek pomocy dla dezerterów. Zaostrzający się kurs wobec dezerterów był widoczny w rozkazie Ministerstwa Spraw Wojskowych z 25 lipca 1920 r. Gen. br. K. Sosnkowski, wiceminister spraw wojskowych, od 9 sierpnia 1920 r. minister spraw wojskowych, wskazywał, że sądy doraźne rozpatrujące sprawy dezerterów miały funkcjonować energicznie i odpowiedzialnie. Orzeczenia miały być pozbawione zbędnej biurokracji, a wyroki wydawane niemal ekspresowo. Zalecał, aby prawo łaski było stosowane jedynie w wyjątkowych przypadkach. Surowe słowa gen. Sosnkowskiego nie oznaczały jeszcze, że wszyscy schwytani dezerterzy byli natychmiast rozstrzeliwani. O wiele ważniejsza była świadomość nieuchronności kary. W trakcie wojny polsko-bolszewickiej funkcjonowały wojskowe sądy doraźne, które decydowały o losach dezerterów. W czasie tej wojny liczba postawionych przed sądami polowymi dezerterów, którzy często popełniali różne kryminalne przestępstwa, sięgnęła w 1920 r. 11 tys., z czego 3 tys. skazano na karę śmierci; w zdecydowanej większości przypadków wykonanie kary śmierci zostało wstrzymane. W 1920 r. wojenne sądy doraźne orzekły 333 wyroki śmierci, spośród których dezerterami było

125 skazanych. W 1921 r. na mocy wyroków tych sądów wykonano jedynie 22 wyroki śmierci.

W latach 1921–1939 dezercje dalej stanowiły wciąż poważny problem WP. Wynikało to z kilku powodów:

- Służba w polskiej armii była powszechna i obowiązkowa.
- Warunki socjalno-bytowe codziennej służby (zwłaszcza w latach 20.) w wielu pułkach wymagały znacznej poprawy.
- Działalność destrukcyjną przeciwko armii polskiej nieprzerwanie prowadzili nie tylko komuniści polscy (w latach 1918–1925 pod nazwą Komunistycznej Partii Robotniczej Polski, od 1925–1938 jako Komunistyczna Partia Polski), ale także komuniści białoruscy (Komunistyczna Partia Zachodniej Białorusi) i ukraińscy (Komunistyczna Partia Zachodniej Ukrainy).
- WP miało charakter wielonarodowościowy, poza żołnierzami polskiej narodowości, którzy zawsze stanowili w armii polskiej zdecydowaną większość (w latach 1922–1939 zazwyczaj ponad 75% wcielonych rekrutów do armii polskiej było Polakami), w międzywojennych siłach zbrojnych II RP służyli również Żydzi, Białorusini, Ukraińcy, Litwini, Rosjanie, Niemcy i Czesi, a także przedstawiciele innych narodowości. Bardzo rozbieżne dane (choćby → p o l i c j i [t. 3] i żandarmerii wojskowej) wskazują, że od 1921 do 1939 r. z WP zdezerterowało lub (w większości) dokonało krótkotrwałego samowolnego oddalenia się od 30 do 60 tys. żołnierzy.

Poza żołnierzami polskiej narodowości największą liczbę dezercji popełnili w latach 1923–1928 Ukraińcy (5–8 tys. dezercji) i Białorusini (4–6 tys. dezercji) oraz Żydzi (2–3 tys. dezercji). Dezerterzy, a także poborowi ukrywali się na terenie kraju, lecz również decydowali się na ucieczki za granicę. Nadal najbardziej popularnym kierunkiem ucieczek były Niemcy. Najzamożniejszy sąsiad II RP przyciągał nie tylko perspektywą poprawy materialnego bytu, ale i wizją przedostania się do innych krajów Europy Zachodniej, a także wyjazdu do USA. W 1923 r. tylko z województwa stanisławowskiego do odległych Niemiec zbiegło aż 150 poborowych, do Czechosłowacji 103, do ZSRR 98, a do Rumunii 50. Podobna tendencja „emigracyjna" utrzymała się w latach 30. W 1936 r. 81 dezerterów dotarło do Niemiec, 69 do ZSRR, 23 do Czechosłowacji,

23 na Litwę, 1 do Rumunii, a 1, jak ustalono, trafił aż do Hiszpanii. W przeważającej liczbie dezerterzy z WP, którzy znaleźli się za granicami kraju, doświadczyli poważnego rozczarowania. Po zatrzymaniu i dokładnych przesłuchaniach przez przedstawicieli obcych → w y w i a d ó w [t. 4] nie okazywali się „cennym źródłem" → i n f o r m a c j i. Ze względu na niski poziom wykształcenia, nierzadki analfabetyzm i półanalfabetyzm (przewaga żołnierzy służby zasadniczej z obszarów wiejskich) dezerterów z armii polskiej przeważnie nie przygotowywano do zadań szpiegowskich. W Niemczech i ZSRR uciekinierzy z WP stanowili zazwyczaj tanią siłę roboczą, jednak często rozczarowani powracali do Polski, gdzie osądzeni trafiali do więzień. Bardziej niebezpieczne były dezercje oficerów w międzywojennej Polsce, które były jednak nieliczne. Do najbardziej znanych należała ucieczka mjr. dypl. S. Kraussa, szefa wyszkolenia w Dowództwie Okręgu Korpusu Nr VI we Lwowie, który w połowie października 1930 r. nie powrócił z miesięcznego urlopu. Po przeprowadzonym śledztwie okazało się, że mjr Krauss nie tylko przywłaszczył od różnych oficerów i instytucji wojskowych 35 tys. złotych, ale i w swoim domu przechowywał kopię akt związanych z obronnością kraju. W latach 1932–1933 strona polska bezskutecznie starała się o ekstradycję Kraussa z Belgii i Francji. Francuzi informowali wręcz, że nic nie wiedzą o losie poszukiwanego. Nie przeszkodziło to jednak tamtejszemu wywiadowi zatrzymać wiosną 1934 r. Kraussa, który był niemieckim agentem działającym jako George Teworyt vel Sybert.

W latach 1921–1939 poważnym problemem były nie tylko dezercje, ale również niechęć do służby w WP. Największe zainteresowanie uniknięciem służby wojskowej wykazywali Żydzi, oceniani przez Samodzielne Referaty Informacji (SRI) WP jako najmniej „wartościowy materiał żołnierski" spośród wszystkich służących w polskiej armii mniejszości narodowych żołnierzy. Przykładowo wśród żołnierzy żydowskich notowano w trakcie służby największą liczbę symulowania różnego rodzaju chorób, a także wywrotowej komunistycznej agitacji. Dla porównania SRI wysoko ceniła kwalifikacje żołnierskie Niemców, choć poważnie obawiała się lojalności tej narodowości. Nieufność polskiego → k o n t r w y w i a d u budzili także Litwini, a zwłaszcza Ukraińcy pozostający pod wpływem Organizacji Ukraińskich Nacjonalistów (OUN), która przekonywała młodzież

ukraińską, że nie powinna dezerterować z WP, a czas służby w polskiej armii wykorzystać do zdobycia przydatnych umiejętności wojskowych. Władze WP znacznie mniej obawiały się postaw Białorusinów i Rosjan, wysoko natomiast ceniły lojalność nielicznie służących w polskiej armii Czechów.

W 1939 r. obawy władz wojskowych o postawę żołnierzy reprezentujących mniejszości narodowe częściowo okazały się uzasadnione. Sygnałem ostrzegawczym były masowe ucieczki niemieckich poborowych, które rozpoczęły się wiosną 1939 r. Prawdopodobnie do wybuchu wojny, tj. do września 1939 r., z II RP do III Rzeszy zbiegło ok. 10 tys. poborowych narodowości niemieckiej, w tym z samej Wielkopolski blisko 2500 niemieckiej młodzieży. Dezercje w szeregach WP miały miejsce od początku wybuchu II wojny światowej, ale dopiero 10 września 1939 r. niepokojące informacje zaczęły napływać z Małopolski Wschodniej, w której pojawiały się zbrojne grupy ukraińskich dezerterów z WP. Działania te inspirowała OUN. Wzrost dezercji w WP, w tym żołnierzy polskich, nastąpił dopiero w drugiej połowie września 1939 r., kiedy stało się jasne, że państwo i armia II RP zmierza ku klęsce. Zwrotnym momentem był 17 września 1939 r., zaatakowanie Polski przez ZSRR. W niektórych miejscach dezercje przybrały masowy charakter. Np. w nocy z 19 na 20 września 1939 r. z 3 Dywizjonu Taborów w Lidzie zdezerterowali wszyscy służący w nim Białorusini i Żydzi. Kategorycznie należy jednak zaprzeczyć, że wszyscy żołnierze białoruscy, niemieccy, ukraińscy i żydowscy, którzy służyli we wrześniu 1939 r., wykazali się nielojalnością wobec II RP. Znaczne męstwo charakteryzowało wielu Białorusinów, którzy dzielnie walczyli w oddziałach wchodzących w skład 20 Dywizji Piechoty (DP), która w dniach 1–4 września 1939 r. stoczyła ciężką bitwę pod Mławą. 10% obrońców Helu, który skapitulował dopiero 2 października 1939 r. stanowili Białorusini. We wrześniu 1939 r., walecznością wyróżnili się ukraińscy ułani służący w 2 i 7 Pułku Strzelców Konnych. Wielu z nich otrzymało za odwagę i poświęcenie na polu walki wysokie odznaczenia.

W sierpniu 1941 r. na mocy porozumień emigracyjnego rządu londyńskiego i rządu sowieckiego w ZSRR rozpoczęto formowanie Polskich Sił Zbrojnych (PSZ), potocznie nazywanych Armią Andersa. Od marca do listopada 1942 r. ze Związku Sowieckiego ewakuowano do Iranu ponad

78 tys. żołnierzy i 35 tys. cywilów. Ewakuacji odmówiła jednak pewna grupa oficerów współpracująca z sowieckimi władzami – byli to ppłk Z. Berling, ppłk L. Bukojemski i por. T. Wicherkiewicz – współtwórcy podporządkowanej Stalinowi i utworzonej przez komunistów w 1943 r. w ZSRR komunistycznej armii polskiej, którą w latach 60. i 70. w Polsce Ludowej nazywano Ludowym Wojskiem Polskim (LWP). W 1943 r. sąd wojenny przy 2 Korpusie WP uznał postępowanie Berlinga i wspomnianych oficerów za zdradę i dezercję. Innym problemem były dezercje żołnierzy narodowości żydowskiej, którzy ewakuowali się wraz z Armią Andersa. Do pierwszych ucieczek żołnierzy narodowości żydowskiej służących w PSZ doszło jeszcze w czasie pobytu w Iranie. W sierpniu i wrześniu 1942 r. zdezerterowało 193 żydowskich żołnierzy. Kolejne dezercje miały miejsce już w Palestynie, gdzie żydowscy dezerterzy z PSZ zasilali miejscowe podziemie zbrojne, walczące o niepodległość Izraela.

Najliczniejsze dezercje w wojsku polskim w ostatnich latach II wojny światowej wydarzyły się w LWP. Tuż przed końcem wojny, to jest w 1944 r., z 2 Armii LWP zdezerterował prawie cały 31 Pułk Piechoty (PP) – dokładnie 636 żołnierzy i 2 oficerów, którzy przyłączyli się do antykomunistycznej partyzantki. W marcu 1945 r. ze szkoły oficerskiej w Chełmie jednej nocy zbiegło ok. 300 podchorążych. Niemal wszystkie bataliony i kompanie drezdeńskiej 9 DP latem 1945 r. porzuciły koszary. Władze komunistyczne najpierw zreorganizowały, a następnie rozwiązały 3 Brygadę Korpusu Bezpieczeństwa Wewnętrznego. Powodem tej decyzji nie były straty poniesione w walce – całe bataliony tej jednostki znikały z bronią. Dezerterzy z LWP zasilali oddziały zbrojnego podziemia. Często w ten sposób tworzyły się także zalążki nowych oddziałów leśnych i siatek konspiracyjnych. W maju 1945 r. dotarła do 5 Wileńskiej Brygady AK 70-osobowa grupa dezerterów z 6 Zapasowego PP 2 Armii LWP z Torunia i poprosiła o wcielenie w szeregi formacji. Trzy dni później przybyło kolejnych 25 żołnierzy z Samodzielnego Batalionu Ochrony Lasów Państwowych z Hajnówki. W 1945 z LWP zdezerterowało 14 tys. żołnierzy, a w 1948 jeszcze więcej, bo 24 tys. Jednak tylko część z nich kierowała się do leśnych oddziałów „żołnierzy wyklętych" i tam docierała. W kolejnych latach przechodzenie żołnierzy LWP na stronę zbrojnego podziemia niepodległościowego wyraźnie zmalało. Miało to

ścisły związek z zewnętrzną i wewnętrzną sytuacją polityczno-militarną w Polsce i na świecie.

W latach 1944–1989 jednym z najważniejszych powodów dezercji z LWP był wzrost przemocy psychicznej i fizycznej, którego doświadczali młodzi rekruci od starszych stażem kolegów. Różne formy znęcania się stosowali również podoficerowie, a nawet oficerowie, za co często nie ponosili żadnej odpowiedzialności karnej. W latach 1952–1955 doszło do 2954 pojedynczych i 278 zbiorowych przypadków dezercji z LWP. Wśród dezerterów Polski Ludowej dominowali młodzi żołnierze, którzy nie wytrzymywali trudów i prymitywnych rytuałów służby wojskowej – przeniesionych głównie z wzorów Armii Czerwonej, a wcześniej carskiej Rosji. W PRL kwestie samowolnych oddaleń z wojska i dezercji regulowały kolejne kodeksy karne, m.in. z 1944, 1957 i 1969 r., a także dekret o stanie wojennym z 13 grudnia 1981 r., który wprowadzał postępowanie doraźne przed sądami wojskowymi za przestępstwa powszechne i wojskowe. Za samowolne oddalenie się i dezercję dekret przewidywał 3 kary główne: karę śmierci, karę 25 lat pozbawienia wolności lub karę pozbawienia wolności na czas nie krótszy od 3 lat. 23 maja 1984 r. sąd wojskowy PRL skazał zaocznie płk. R. Kuklińskiego, który do czasu ucieczki w listopadzie 1981 r. pełnił obowiązki w Sztabie Generalnym WP. Kara została wymierzona za dezercję i zdradę państwa.

Po 1989 r. dezercje nie skończyły się, ale dzięki zniesieniu → c e n z u r y [t. 1] i wprowadzeniu jawności życia społecznego Polacy dowiadywali się znacznie więcej o problemach wojska. Wiele informacji mogło być jednak szokujących, np. jak ta związana z szer. pchor. J. Ochnikiem z Wyższej Szkoły Oficerskiej Wojsk Łączności (WSOWŁ) w Zegrzu. W maju 1990 r. Ochnik zastrzelił dowódcę warty i 3 swoich kolegów, którzy znęcali się nad nim psychicznie. Dezerter z WSOWŁ kilkanaście dni ukrywał się w okolicznych lasach. W 1999 r. Naczelna Izba Kontroli (NIK) skontrolowała warunki pełnionej zasadniczej służby wojskowej. Z raportu NIK wynikało, że w kontrolowanych jednostkach wojskowych wymierzono łącznie 2715 kar dyscyplinarnych, z czego aż 1724 związanych było z nieobecnością żołnierzy na służbie lub z samowolnym oddaleniem się.

Remigiusz Kasprzycki

J. Grzybowski, *Białorusini w polskich regularnych formacjach wojskowych w latach 1918–1945*, Wydawnictwo ISP PAN, Warszawa 2006; D. Jarosz, G. Miernik, *Pobór, wcielenie, „pruska dyscyplina", dezercje. Wstęp do badań nad historią społeczną służby wojskowej w stalinowskiej Polsce (1950–1955)*, „Polska 1944/45–1989. Studia i Materiały" 2018, nr 16; R. Kasprzycki, *Dezercje i unikanie służby w Wojsku Polskim w latach 1918–1939*, „Dzieje Najnowsze" 2016, r. 48, nr 3; tenże, *Miraże Czerwonego Raju. Losy dezerterów z Wojska Polskiego w Związku Radzieckim*, „Niepodległość i Pamięć" 2017, nr 1 (57); tenże, *Niespełnione marzenia naiwnych. Losy dezerterów z Wojska Polskiego w Niemczech w latach 1921–1939*, „Niepodległość i Pamięć" 2019, nr 1 (65); P. Stawecki, *Z badań nad dyscypliną i moralnością wojska Drugiej Rzeczypospolitej*, Wydawnictwo PAW, Warszawa 2000; T. Szczygieł, *Wojskowe postępowanie karne w II Rzeczypospolitej (1918–1939)*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2017.

DEZINFORMACJA – metoda oddziaływania psychologicznego, która wprowadza w błąd osobę/grupę osób co do rzeczywistego stanu rzeczy, świadomie przekazuje nieprawdziwe → i n f o r m a c j e w celu skuteczniejszego prowadzenia działań wojennych, sprawdzania wycieków informacji i kierunku ich wycieku, a także procesu manipulowania informacjami, wprowadzania w błąd przez podanie niepełnych lub kompletnych, ale już nie niezbędnych informacji, tworząc zniekształcony obraz rzeczywistości. Rozpowszechnianie zniekształconych, niepełnych lub świadomie fałszywych informacji do celów propagandowych, wojskowych (wprowadzających w błąd), handlowych lub innych.

Dezinformacja jest utożsamiana z procesem mylnego informowania, sytuacją, w której brakuje informacji rzetelnych, także z przekazem treści zamierzonych. Niektórzy uważają, że dezinformacja znajduje się między wprowadzaniem w błąd a wpływaniem. Strategiczna dezinformacja jest instrumentem rosyjskiej polityki zarówno w czasie → w o j n y [t. 4], jak i pokoju. Wyspecjalizowanymi organami realizującymi zadania z zakresu dezinformacji są organy → w o j n y p s y c h o l o g i c z n e j [t. 4], taką rolę odgrywają również cywilne i wojskowe → s ł u ż b y s p e c j a l n e [t. 4]. Dezinformacja obejmuje czynności podejmowane z zaangażowaniem poważnych środków, jest prowadzona w sposób systematyczny i fachowy, zawsze za pośrednictwem mass mediów i jest adresowana do → o p i n i i p u b l i c z n e j [t. 3].

Wyróżnia się następujące poziomy manipulacji:

- wzmocnienie istniejących w umysłach ludzi wartości, które są korzystne dla manipulatora (idee, postawy itp.);
- częściowa zmiana poglądów na temat konkretnego wydarzenia lub okoliczności;
- podejmowanie przez odbiorcę błędnych decyzji;
- kardynalna zmiana postaw.

Rodzaje dezinformacji:

- wprowadzanie w błąd konkretnej osoby lub grupy osób, czyli podawanie fałszywych informacji;
- manipulowanie działaniami (jednej osoby lub grupy osób);
- tworzenie opinii publicznej na temat problemu lub przedmiotu;
- „półprawda" lub „fałszywe zaniedbanie". W szczególności totalitarne → reżimy [t. 3] polityczne pragną otrzymywać od władz niższego szczebla jedynie pozytywne informacje, ukrywając niepowodzenia i błędy. „Fałsz milczenia" przenika także do mediów, tworząc iluzję „udanego postępu", podczas gdy w rzeczywistości dochodzi do regresji. Ostatnio aktywnie wykorzystywana jest technologia dezinformacji znana jako „biały szum informacyjny". Oznacza to, że jeśli nie jest możliwe ukrycie „niewygodnej" informacji, jest ona zróżnicowana, tj. tworzy się pewien zestaw wersji, które są w równym stopniu potwierdzone, mocując je w masowej świadomości.

Rozwój internetu, → mediów społecznościowych [t. 3] oraz nowoczesnych technologii sprawił, że znacznie wrosło → zagrożenie [t. 4] dezinformacją. Obecnie fałszywe informacje rozprzestrzeniają się na nieosiągalną wcześniej skalę, a ich zasięg stał się na tyle duży, że może wpłynąć na funkcjonowanie całego kraju. Tym samym dezinformacja stała się dla państwa wyzwaniem. O dezinformacji możemy mówić, gdy rozpowszechniane informacje:

- są całkowicie lub częściowo fałszywe, zmanipulowane lub wprowadzające w błąd;
- dotyczą kwestii ważnych z punktu widzenia interesu publicznego;
- mają wywołać niepewność lub wrogość, doprowadzić do polaryzacji albo zakłócenia procesów demokratycznych;

- są rozpowszechniane lub wzmacniane za pomocą zautomatyzowanych i agresywnych technik, takich jak boty społeczne, → sztuczna inteligencja [t. 4] (AI), mikrotargeting lub trollowanie.

Istnieją różne metody dezinformacji, z których każda ma swoje pozytywne i negatywne cechy. Konkretny wybór tej czy innej metody zależy bezpośrednio od sytuacji operacyjnej, która jest opracowana w określonym obszarze służby wywiadowczej, zadań, które są przed nią ustalane, itd. Metody dezinformacji:

- tendencyjne opowiadanie faktów: to rodzaj dezinformacji, która obejmuje stronnicze przedstawianie pewnych faktów lub innych informacji o zdarzeniach przy użyciu specjalnie wybranych prawdziwych danych w określonych odstępach czasu – z reguły w tej metodzie informacja jest dozowana do stale rosnącego napięcia, a taki stan społeczeństwa/grupy jest utrzymywany przez ciągłe „podrzucanie" nowych części ściśle ograniczonych i mierzonych danych w środowisku deficytu informacji;
- odwrotna dezinformacja: dzieje się to poprzez przekazywanie prawdziwych informacji w perwersyjny sposób lub w sytuacji, gdy cel postrzega je jako fałszywe – zastosowanie takich środków stwarza sytuację, w której odbiorca faktycznie zna prawdziwą informację o zamiarach lub konkretnych działaniach strony przeciwnej, ale postrzega ją w taki sposób, że nie jest gotowy do wytrzymania negatywnego wpływu;
- terminologiczne „minowanie": jest wypaczeniem pierwotnej poprawnej istoty fundamentalnie ważnych, podstawowych terminów i interpretacji o ogólnym charakterze ideologicznym i operacyjnie stosowanym;
- pochlebstwo: wykorzystanie przyjemnych interpelacji, czasami nieumiejętnie, w celu przekonania odbiorcy (np. „Jesteś bardzo inteligentny, powinieneś zgodzić się z tym, co mówię");
- apel do autorytetu: cytuje się ważne postacie, aby poprzeć pomysł, argument lub linię postępowania, a nie inne opinie;
- apel do strachu: przerażona publiczność znajduje się w sytuacji biernej otwartości i łatwiej ulega jakiejkolwiek indoktrynacji lub idei, którą chce się jej wpoić;

- kozioł ofiarny: demonizując osobę lub grupę osób i oskarżając o bycie odpowiedzialnym za rzeczywisty lub rzekomy problem, propagandysta może uniknąć mówienia o prawdziwych sprawcach i pogłębić sam problem;
- żądanie dezaprobaty lub wkładanie słów w usta: ma sugerować, że pomysł lub działanie jest przyjmowane przez grupę przeciwną, skłania to innych do zmiany zdania;
- efekt skumulowany: próba przekonania publiczności do przyjęcia pomysłu sugerującego, że ruch masowy jest już zaangażowany w podtrzymywanie danej idei, chociaż jest to nieprawda – niestety, większość woli być zawsze po stronie zwycięzców, owa taktyka pozwala przygotować społeczeństwo do → p r o p a g a n d y [t. 3]; łatwiej jest gromadzić ludzi w grupach, aby wyeliminować indywidualne sprzeciwy i stosować większy przymus, przekonanie lub zasady marketingowe stosowane przez sprzedawców;
- używanie haseł: krótkie frazy, łatwe do zapamiętania i rozpoznania, zdolne do pozostawienia śladu u wszystkich odbiorców, pozytywnie lub ironicznie (np. „Jan P. jest uczciwym człowiekiem");
- stereotypowanie lub etykietowanie: ta technika wykorzystuje uprzedzenia i stereotypy odbiorców, aby coś odrzucić;
- eufemizm lub semantyczny poślizg: zamiana jednego wyrażenia na inne, aby zmienić treść emocjonalną i znaczenie (np. „czystki etniczne" w przypadku umotywowanych rasizmem mordów, „solidarność" zamiast podatku);
- celowa niedokładność: dotyczy powoływania się na statystyki lub odwoływania się do faktów je deformujących bez wskazywania źródeł lub wszystkich danych – zamiarem jest nadanie treści wypowiedzi pozorów charakteru naukowego i unieważnienie analizy jego przydatności bądź prawdziwości;
- przyciemnienie: aby nie zgłaszać czegoś nieprzyjemnego dla władzy, treść zostaje przeformułowana (np. zamiast powiedzieć, że bezrobocie wzrosło do 4 mln, można powiedzieć, że stopa bezrobocia wzrosła w mniejszym stopniu niż w tym samym miesiącu ubiegłego roku);
- poziom językowy oraz wygląd „zwykłego człowieka" dla zdobycia zaufania publiczności: z powodu psychologicznego mechanizmu

projekcji odbiorcy są bardziej skłonni zaakceptować przedstawione im pomysły, ponieważ ktoś, kto je przedstawia, jest podobny do samej publiczności;
- redefinicja i rewizjonizm: polega na redefiniowaniu słów lub fałszowaniu historii w sposób stronniczy, aby stworzyć iluzję spójności;
- przesadne uproszczenie: ogólniki używane do kontekstualizacji złożonych problemów społecznych, politycznych, ekonomicznych lub wojskowych;
- świadectwo: podawanie konkretnych przypadków zamiast ogólnych sytuacji, aby podtrzymać daną politykę (np. szanowana osobowość wchodzi do partii politycznej oskarżonej o → k o r u p c j ę, aby wykorzystać swoją reputację i przeciwdziałać złemu wizerunkowi partii);
- transfer: technika służąca projekcji pozytywnych lub negatywnych cech osoby, bytu, przedmiotu lub wartości (jednostki, grupy, organizacji, narodu, rasy, patriotyzmu) na coś, co uczyni to bardziej (lub mniej) akceptowalnym;
- używanie ogólnych i prestiżowych słów, które mogą powodować intensywne emocje na widowni: miłość do kraju i pragnienie pokoju, wolności, chwały, sprawiedliwości, honoru i czystości itp. pozwalają zabić krytycznego ducha publiczności, ponieważ znaczenie tych słów różni się w zależności od interpretacji każdej osoby, ale ich ogólnie znaczenie jest pozytywne, w związku z czym wykorzystujące takie słowa koncepcje i programy propagandystów same będą postrzegane jako wielkie, dobre, pożądane i cnotliwe.

Dezinformacja jest integralną częścią → w o j n y i n f o r m a c y j n e j [t. 4], która obejmuje:
- → o p e r a c j e p s y c h o l o g i c z n e [t. 3] (wykorzystanie informacji do psychologicznego oddziaływania na → ż o ł n i e r z y [t. 4] wroga);
- wojnę elektroniczną (nie pozwala wrogowi na uzyskanie dokładnych informacji);
- środki bezpieczeństwa (chęć uniknięcia wiedzy wroga o możliwościach i zamiarach strony przeciwnej);

- bezpośrednie ataki informacyjne (zniekształcenie informacji bez widocznej zmiany jej istoty).

Aby skuteczniej manipulować opinią publiczną, dezinformacja może rozprzestrzeniać się jednocześnie za pośrednictwem mediów drukowanych i elektronicznych, telewizji, internetu, plotek, a także poprzez wykorzystanie ulotek w lokalnych konfliktach i wojnach.

W szerokim sensie wojna informacyjna jest jedną z metod konfrontacji między dwoma państwami, która ma miejsce głównie w czasie pokoju, gdzie przedmiotem wpływów wraz z siłami zbrojnymi i →ludnością cywilną [t. 3] jest społeczeństwo jako całość, jego państwowe systemy administracyjne, struktury zarządzania produkcją, nauka, kultura itp. W wąskim znaczeniu jest to jedna z metod operacji bojowych lub bezpośredniego przygotowania się do nich w celu uzyskania przewagi nad wrogiem w procesie przyjmowania, przetwarzania i wykorzystania informacji.

Do prowadzenia operacji informacyjnych i psychologicznych z wykorzystaniem dezinformacji aktywnie angażuje się telewizja, która we współczesnym świecie jest najważniejszym narzędziem masowego wpływu na społeczeństwo. Istnieje kilka metod manipulowania świadomością indywidualną i masową wykorzystywanych przez media:

- →przeciążenie informacyjne [t. 3] – odbiorca otrzymuje nadmierną ilość niepotrzebnych informacji (abstrakcyjne rozumowanie, niepotrzebne szczegóły itp.), co uniemożliwia mu zrozumienie prawdziwej istoty problemu;
- dozowanie informacji – tylko część informacji jest przekazywana do odbiorcy, a reszta jest starannie ukryta, co prowadzi do zniekształcenia rzeczywistego obrazu w określonym kierunku;
- wielkie kłamstwo – społeczeństwu podaje się możliwie poważnie najbardziej nieprawdopodobne kłamstwo, które wydaje się szczególnie przekonujące;
- mieszanie faktów – fakty są mieszane ze wszelkiego rodzaju założeniami, hipotezami i plotkami; społeczeństwu niezwykle trudno jest odróżnić prawdę od fikcji;
- opóźnienie czasu informacji – pod różnymi pretekstami opóźnia się podanie naprawdę ważnych informacji, aż do momentu, gdy będzie za późno, aby odbiorca coś zmienił;

- ukryte uderzenie – fikcyjna informacja jest przekazywana przez manipulatora do odbiorcy przez neutralnych, ale podstawionych ludzi;
- rzeczywiste kłamstwo – społeczeństwu podaje się całkowicie fałszywą, ale niezwykle oczekiwaną w danej chwili informację (z czasem oszustwo zostaje ujawnione, ale dotkliwość sytuacji nie ustępuje lub pewien proces nabiera nieodwracalnego charakteru).

Celem działań dezinformacyjnych jest destabilizacja innych państw. Liberalne demokracje nie mają symetrycznej odpowiedzi na takie działania, które mogą być prowadzone jedynie przez agresywne, autorytarne państwa.

Podczas Warsaw Security Forum 8 listopada 2017 r. odbył się panel pt. „Polityka w erze post-prawdy: Zwalczanie dezinformacji i fake newsów w Europie Centralnej i Wschodniej", gdzie zaprezentowano raport *Rosyjska wojna dezinformacyjna przeciwko Polsce*. Został wydany przez Fundację im. Kazimierza Pułaskiego we współpracy merytorycznej z → Centrum Analiz Propagandy i Dezinformacji [t. 1] oraz Studium Europy Wschodniej Uniwersytetu Warszawskiego.

W styczniu 2018 r. Komisja Europejska powołała grupę ekspertów wysokiego szczebla ds. nieprawdziwych informacji i dezinformacji w internecie (High-Level Expert Group on Fake News and Disinformation spread online, HLEG). Jej zadaniem jest doradzanie przy inicjatywach związanych z przeciwdziałaniem → fake newsom i dezinformacji w sieci. Efektem jej prac były sprawozdanie i raport, opublikowane 12 marca 2018 r., w których grupa analizuje problemy związane z dezinformacją w sieci, a w mniejszym stopniu fałszywych informacji, podkreślając, że dezinformacja może zagrażać demokratycznym procesom i wartościom. Grupa zaleciła m.in.: rozwój umiejętności korzystania z mediów w celu → przeciwdziałania dezinformacji [t. 3], opracowanie narzędzi, które pomogą użytkownikom i dziennikarzom zwalczać dezinformację, zachowanie różnorodności i stabilności europejskich mediów informacyjnych oraz dalsze badania wpływu dezinformacji na społeczeństwo w Europie.

Dezinformacja może destabilizować sytuację w państwie, wywierać destrukcyjny wpływ na jego struktury administracyjne i decyzyjne, a także

podważać podstawy społeczne, ekonomiczne oraz kulturowe. Wg raportu *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy* coraz więcej krajów na świecie wykorzystuje media społecznościowe do działań dezinformacyjnych – zarówno do kształtowania swojej wewnętrznej polityki, jak i do wpływania na inne państwa. Przeciwdziałanie dezinformacji staje się wyzwaniem nie tylko dla pojedynczych państw, ale też instytucji i organizacji międzynarodowych.

Jak zaznaczają autorzy publikacji z września 2019 r. *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, konieczność przeciwdziałania kampaniom dezinformacyjnym w Europie podkreśliła po raz pierwszy Rada Europejska w marcu 2015 r. Od tego czasu w strukturach Europejskiej Służby Działań Zewnętrznych (European External Action Service) powstało kilka zespołów zajmujących się analizowaniem dezinformacji w Unii Europejskiej oraz krajach sąsiadujących ze wspólnotą. Wg Komórki UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych to dezinformacja ze strony Federacji Rosyjskiej miała stanowić największe zagrożenie przed przeprowadzonymi w maju 2019 r. wyborami do Parlamentu Europejskiego. Niepokojące doniesienia o skali i wpływie kampanii dezinformacyjnych sprawiły, że 2018 r. był w UE czasem wyjątkowo wytężonej pracy w tym zakresie. Opublikowano łącznie 4 istotne dokumenty, które podejmowały zagadnienie dezinformacji.

Olga Wasiuta

J. Darczewska, *Między jawną dezinformacją a niejawną praktyką gry rosyjskich służb*, Ośrodek Studiów Wschodnich im. Marka Karpia, Warszawa 2019; A. Januszko-Szakiel, *Dezinformacja jako narzędzie medialnej manipulacji świadomością*, [w:] *Manipulacja pedagogiczno-społeczne aspekty. Część I. Interdyscyplinarne aspekty manipulacji*, J. Aksman (red.), Oficyna Wydawnicza AFM, Kraków 2010; T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2 (24); NASK Cyber Policy, *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, NASK Państwowy Instytut Badawczy, Warszawa 2019; P. Pogorzelski, *Zagrożenie rosyjską dezinformacją w Polsce i formy przeciwdziałania*, Kolegium Europy Wschodniej im. Jana Nowaka-Jeziorańskiego we Wrocławiu, Wrocław 2017; M. Świerczek *„System matrioszek", czyli dezinformacja doskonała. Wstęp do zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19; V. Volkoff,

Dezinformacja – oręż wojny, Delikon, Warszawa 1991; M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnych*, AON, Warszawa 2005.

DEZINFORMACJA WOJSKOWA – proces prowadzący do powstania →informacji fałszywej bądź też kłamliwej, mający na celu wprowadzenie odbiorcy w błąd i wytworzenie u przeciwnika fałszywego obrazu rzeczywistości. Rozwój →środowiska informacyjnego [t. 4] doprowadził do znaczącego poszerzenia pojęcia znaczenia od tradycyjnie rozumianej →propagandy [t. 3] o nową kategorię →fake newsów. W procesie →dezinformacji główny nacisk kładziony jest na cel przekazywania nieprawdziwej informacji, stosując ją jako narzędzie do osiągnięcia wymiernych korzyści. Podmiot dezinformujący oczekuje, że przekazanie nieprawdziwej informacji spowoduje podjęcie nieprawidłowych decyzji przez odbiorców, prowadząc tym samym do zamierzonego celu.

Dezinformacja to szereg działań konsekwentnie wprowadzany, skupiony na szerszej grupie społecznej, a nie tylko na pojedynczej jednostce. Dezinformacja może obejmować różne dziedziny, takie jak polityka, ekonomia, nauka, technika, wojskowość. Dezinformacja poza utrzymywaniem podmiotu dezinformowanego w niepewności i błędzie może pomóc w uzyskaniu efektów zaskoczenia niezwykle istotnych na płaszczyźnie operacyjno-strategicznej. Opiera się ona m.in. na blokowaniu kanałów wzajemnej komunikacji.

Środki dezinformacji wojskowej powinny być skoordynowane z →operacjami psychologicznymi [t. 3] gwarantującymi korzystne nastawienie →ludności cywilnej [t. 3] i kierownictwa wojskowego sił wielonarodowych. Zaniedbanie tej okoliczności może prowadzić do kompromisu w sprawie oszustwa. →Wywiad [t. 4] i →kontrwywiad również są niezwykle ważne dla organizacji dezinformacji wojskowej, szczególnie przy planowaniu, realizacji i zakończeniu każdej operacji.

Dezinformacja wojskowa to szczególny rodzaj dezinformacji skupiony na płaszczyźnie wojskowej. Podmiot dezinformujący wprowadza nieprawdziwe informacje dotyczące zamierzeń i planów, a także siły i proporcji o znaczeniu militarnym. Skutecznie zrealizowana dezinformacja wojskowa przynosi zwycięstwo. Proces ten jest przeprowadzany przez wyspecjalizowane jednostki posiadające odpowiednie zasoby, podstawą

których jest rozpoznanie podmiotu. Konieczne jest właściwe przygotowanie kanałów informacyjnych, pozbawiających podmiot dezinformowany możliwości weryfikacji.

Dezinformacja wojskowa jest prowadzona nie tylko w trakcie → w o j n y [t. 4], lecz również w trakcie pokoju. Prowadzona jest na poziomach: strategicznym, operacyjnym i taktycznym, zarówno w formie działań ofensywnych, jak i defensywnych. Dezinformacja wykorzystuje różne kanały, m.in. polityczne, dyplomatyczne, ekonomiczne, naukowo-techniczne, wojskowe i specjalne.

M. Świerczek przytacza kilka zróżnicowanych określeń dezinformacji wojskowej, wskazując, że jest ona:

- wyjątkowo złożoną metodą pracy operacyjnej, będącą sposobem oddziaływania na aktualnego czy potencjalnego przeciwnika, wrogie → s ł u ż b y s p e c j a l n e [t. 4] bądź określone grupy czy warstwy społeczne w innym, ale niekiedy też i własnym kraju. Termin wymyślony przez niemieckie służby specjalne w czasie I wojny światowej; przy sztabie armii niemieckiej do końca działań wojennych istniała komórka dezinformacyjna sterowana przez wojskową służbę wywiadowczą. Później służby specjalne innych państw wprowadziły tę formę działania jako metodologiczny sposób oddziaływania na przeciwnika, podejmowany z zamiarem wykreowania celowego, ukierunkowanego wpływu na kształtowanie opinii i bieg możliwych do przewidzenia zdarzeń;
- celowo fałszywą informacją, która ma wpłynąć na określoną grupę ludzi lub całą populację – jest to jedna z podstawowych metod pracy operacyjnej wywiadu, służąca wpłynięciu na postępowanie przeciwnika, by zachował się korzystnie dla służby wywiadowczej;
- tworzeniem i rozprzestrzenianiem mylącej lub fałszywej informacji w celu zniekształcenia obrazu przeciwnika;
- celowym przekazywaniem przeciwnikowi, za pomocą środków i metod pracy operacyjnej, nieprawdziwych informacji w celu wprowadzenia go w błąd i uzyskania zaplanowanych rezultatów;
- prowokacją, a nie kłamstwem państwa używającym swych wywiadów do malowania obrazu prowokującego przeciwnika do podejmowania błędnych ocen;

- działaniem stawiającym sobie za cel realizację konsekwentnego programu zmierzającego do zastąpienia w świadomości, a przede wszystkim podświadomości, mas będących przedmiotem działań poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie;
- systematycznymi wysiłkami zmierzającymi do rozprzestrzenienia nieprawdziwych informacji i do zafałszowania lub zablokowania informacji dotyczących rzeczywistej sytuacji i polityki.

Procesy dezinformacyjne muszą podlegać ciągłym zmianom, unikanie wcześniej używanych technik, różnorodność i nieszablonowość są charakterystyczne dla działań. Manipulacja jako jedna z form dezinformacji polega na przekazywaniu nieprawdziwych danych, pomijaniu ważnych danych a przekazywaniu mniej istotnych, zmniejszaniu rangi danych istotnych, przekazywaniu informacji wieloznacznych, co utrudnia ich właściwe zrozumienie, tworzeniu i przekazywaniu nadmiaru danych, prowadząc do powstania szumu informacyjnego. Dezinformacja jest niezwykle istotnym elementem prowadzenia walki informacyjnej, jej działania odbywają się m.in. poprzez paraliż procesu decyzyjnego, rozłam pomiędzy sojusznikami, wzbudzanie strachu, a także →trolling [t. 4], →dywersję ideologiczną czy też manipulowanie →mediami społecznościowymi [t. 3].

Zgodnie z terminologią przyjętą w rosyjskich siłach zbrojnych dezinformacja wojskowa jest elementem maskowania operacyjnego lub strategicznego. W ściśle tajnym słowniku KGB z 1972 r. zdefiniowano „dane dezinformacyjne" jako „specjalnie przygotowane dane, wykorzystywane do tworzenia w umyśle wroga niepoprawnych lub wyimaginowanych obrazów rzeczywistości, na podstawie których wróg podejmowałby korzystne decyzje" dla Związku Radzieckiego. Stosowanie dezinformacji wojskowej jako broni przez KGB, wcześniej GPU (Państwowy Zarząd Polityczny przy Ludowym Komisariacie Spraw Wewnętrznych Rosyjskiej Federacyjnej Socjalistycznej Republiki Radzieckiej) rozpoczęło się w 1923 r., kiedy I.S. Unszlicht, wiceprezes GPU, zaproponował utworzenie „specjalnego biura dezinformacji do prowadzenia aktywnych operacji wywiadowczych i wojskowych". Wg ostatniego tomu historii rosyjskiego wywiadu, opublikowanego w Rosji pod redakcją J. Primakowa, w różnych

okresach „radzieckie operacje dezinformacyjne przeciwko specjalnym służbom wroga miały kilka oznaczeń: «działania wpływowe», «dezinformacja operacyjna», «aktywne środki», «gry operacyjne» oraz «środki pomocy»". Pomimo różnic w kategoriach wszystkie były i są konkretnymi, ukierunkowanymi działaniami mającymi na celu dezinformowanie wojskowe faktycznego lub potencjalnego przeciwnika w stosunku do prawdziwych zamiarów lub możliwości oraz służącymi uzyskaniu korzystnej reakcji „celu działania", która byłaby praktycznie nieosiągalna za pomocą otwartych środków.

Wojskowe operacje dezinformacyjne stawiają sobie zwykle za cel doprowadzenie wroga do tego, by pozyskał informacje i uwierzył w to, że ofensywa lub atak planowane są w określonym czasie, przeciwnik posiada lub nie posiada określonego typu broni, mimo że jest dokładnie odwrotnie. Archetypem dezinformowania wojskowego może być przypadek wojny trojańskiej. Ofiarowany Trojanom koń, w którym znajdowali się greccy wojownicy, został przekazany wrogom jako prezent sygnalizujący rezygnację z oblężenia miasta. Prezent został w Troi przyjęty z ulgą. Dezinformacja, wg mitów greckich przypisywania Odyseuszowi, udała się bezbłędnie, ponieważ zarówno Odyseusz, kreując treść dezinformującego komunikatu, w pełni osiągnął swój cel, jak i Trojanie całkowicie poddali się informacji dotyczącej otrzymania podarunku i wycofania się wojsk greckich.

Dezinformacja wojskowa była także stosowana w czasie → z i m n e j w o j n y [t. 4]. Na początku 1952 r. za sprawą działań Związku Radzieckiego prowadzono znaczącą kampanię dezinformacyjną, w której twierdzono, że USA wykorzystują broń biologiczną w Korei. Niedawno ujawnione dokumenty z radzieckich archiwów dowodzą, że KGB (wówczas pn. MGB – Ministerstwo Bezpieczeństwa Państwowego ZSRR) było głęboko zaangażowane w rozpowszechnianie fałszywej historii „w celu oskarżenia Amerykanów o użycie broni bakteriologicznej w Korei i Chinach". W. Burchett, australijski dziennikarz i członek Partii Komunistycznej, ściśle współpracował z chińskimi urzędnikami i był niezwykle aktywny w rozpowszechnianiu fałszywej opowieści wśród dziennikarzy na Dalekim Wschodzie. Później w 1957 r., gdy Burchett był w Moskwie, został agentem KGB. Dokument znaleziony w rosyjskich archiwach ujawnia, że w lipcu

1957 r. KGB poinformowało Komitet Centralny Partii Komunistycznej, że ich agent Burchett, który został wyznaczony „do penetracji amerykańskiej i zachodnioeuropejskiej prasy burżuazyjnej", został moskiewskim korespondentem prokomunistycznej amerykańskiej gazety „National Guardian".

Cel wojskowej operacji dezinformacyjnej jest postrzegany jako pożądany rezultat oszustwa, wyrażony jako to, co wróg powinien lub czego nie powinien robić w kluczowym czasie i/lub miejscu. Oznacza to, że w przypadku każdej operacji i potencjalnie na każdym jej etapie cele oszustwa będą różne, w zależności od konkretnych warunków bieżącej sytuacji.

Dezinformacja wojskowa jest przeprowadzana w celu wsparcia wspólnych operacji w celu wywarcia wpływu na dowództwo i kwaterę główną wroga, zmniejszając jego zdolność do zarządzania i kontroli.

W dzisiejszym środowisku postępującej informatyzacji, digitalizacji oraz rozwoju środowiska → b i g d a t a, w którym informacja podlega dynamicznym zmianom i każdy może być jej nadawcą, procesy związane z dezinformacją są ułatwione. Kreowanie wizji świata stało się jednym ze sposobów prowadzenia polityki, co prowadzi do wielu niebezpieczeństw zarówno dla jednostki, jak i dla całego społeczeństwa.

Edyta Sadowska, Jakub Idzik

R. Brzeski, *Dezinformacja*, Warszawa 2011; L. Ciborowski, *Mechanizmy i przestrzenie walki informacyjnej*, [w:] *Informacja w walce zbrojnej*, G. Nowacki (red.), AON, Warszawa 2002; E. Sadowska, *Big data*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J. Janczak, *Zakłócenia informacyjne*, AON, Warszawa 2001; H. Lewandowski, *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, Wydawnictwo UOP, Warszawa 2000; S. Lewandowsky, W.G.K. Stritzke, A.M. Freund i in., *Misinformation, Disinformation, and Violent Conflict: From Iraq and the „War on Terror" to Future Threats to Peace*, „American Psychologist" 2013, vol. 68 (7); NASK Cyber Policy, *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, NASK Państwowy Instytut Badawczy, Warszawa 2019; H. Romerstein, *Disinformation as a KGB Weapon in the Cold War*, „Journal of Intelligence History" 2001, vol. 1; M. Świerczek *„System matrioszek", czyli dezinformacja doskonała. Wstęp do zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19; V. Volkoff,

Dezinformacja – oręż wojny, Wydawnictwo Delikon, Warszawa 1991; M. Wrzosek, *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2 (87); A. Żebrowski, *Ewolucja polskich służb specjalnych: wybrane obszary walki informacyjnej: wywiad i kontrwywiad w latach 1989–2003*, Oficyna Wydawnicza Abrys, Kraków 2005.

DOBRA KULTURY – OCHRONA W WARUNKACH KONFLIKTU ZBROJNEGO – pierwszymi dokumentami chroniącym dobra kultury były postanowienia konwencji haskich z lat 1899 i 1907. Później treści dotyczące ochrony dóbr kultury zawarto w traktacie wersalskim z 1919 r. W okresie międzywojennym rozwijało się prawo w tej dziedzinie, nie ochroniło ono jednak dóbr kultury przed zniszczeniami w trakcie II wojny światowej. Doświadczenia →wojny [t. 4] doprowadziły do prac nad całościową konwencją. Ukoronowaniem tych prac było przyjęcie w Hadze w 1954 r. Konwencji o ochronie dóbr kulturalnych w wypadku konfliktu zbrojnego (zob. →dobra kultury – ochrona w warunkach konfliktu zbrojnego).

Konwencja haska z 1954 w art. 1 podaje definicję dóbr kulturalnych, są to:

a) dobra ruchome lub nieruchome, które posiadają wielką wagę dla dziedzictwa kulturalnego narodu, na przykład zabytki architektury, sztuki lub historii, zarówno religijne, jak świeckie; stanowiska archeologiczne; zespoły budowlane posiadające jako takie znaczenie historyczne lub artystyczne; dzieła sztuki, rękopisy, książki i inne przedmioty o znaczeniu artystycznym, historycznym lub archeologicznym, jak również zbiory naukowe i zbiory książek, archiwaliów oraz reprodukcji wyżej określonych dóbr;
b) gmachy, których zasadniczym i stosowanym w praktyce przeznaczeniem jest przechowywanie lub wystawianie dóbr kulturalnych ruchomych, określonych pod lit. a), takie jak muzea, wielkie biblioteki, składnice archiwalne, jak również schrony mające na celu przechowywanie w razie konfliktu zbrojnego dóbr kulturalnych ruchomych, określonych pod lit. a);

c) ośrodki obejmujące znaczną ilość dóbr kulturalnych określonych powyżej, a zwanych w tekście Konwencji „ośrodkami zabytkowymi".

Elementem konwencji, który od początku budził istotne wątpliwości, była kwestia tzw. konieczności wojskowej, umożliwiającej uchylenie się od wymogu ochrony dóbr kulturalnych w wypadku zaistnienia kategorycznej konieczności wojskowej (art. 4.2 Konwencji).

Konwencja przewiduje możliwość przyznania niektórym dobrom kulturalnym tzw. ochrony specjalnej. Zgodnie z treścią art. 8 konwencji:

> Ochroną specjalną może być objęta ograniczona ilość schronów przeznaczonych do przechowywania dóbr kulturalnych ruchomych w razie konfliktu zbrojnego oraz ośrodków zabytkowych i innych dóbr kulturalnych nieruchomych o bardzo wielkim znaczeniu, pod warunkiem, że:
> a) znajdują się w dostatecznej odległości od wielkich ośrodków przemysłowych oraz od wszelkich ważnych obiektów wojskowych stanowiących punkty wrażliwe, jak na przykład lotnisk, radiowych stacji nadawczych, zakładów pracujących na rzecz obrony narodowej, portów lub dworców kolejowych o pewnym znaczeniu, jak również wielkich linii komunikacyjnych;
> b) nie są użytkowane do celów wojskowych.
>
> Schron dla dóbr kulturalnych ruchomych może być objęty ochroną specjalną bez względu na swoje położenie, jeżeli jest zbudowany w taki sposób, że według wszelkiego prawdopodobieństwa nie może ponieść szkody w bombardowaniu.
>
> Ośrodek zabytkowy uważa się za użytkowany do celów wojskowych, jeżeli służy do przemieszczania, chociażby tylko tranzytowego, osób wojskowych lub materiału wojskowego, jak również jeżeli jest terenem czynności bezpośrednio związanych z działaniami wojskowymi, z kwaterunkiem osób wojskowych lub z produkcją materiału wojennego.
>
> Natomiast nie jest uważane za użytkowanie do celów wojskowych strzeżenie dóbr kulturalnych wymienionych w ust. 1 przez uzbrojonych strażników specjalnie powołanych do tego zadania

> ani obecność w pobliżu dóbr kulturalnych sił policyjnych, do których stałego zakresu działania należy zapewnienie porządku publicznego.
>
> Dobro kulturalne, wymienione w ust. 1 niniejszego artykułu, położone w pobliżu ważnego obiektu wojskowego w rozumieniu tegoż ustępu, może być jednak objęte ochroną specjalną. Jeżeli Wysoka Umawiająca się Strona, która składa o to wniosek, zobowiąże się, że w razie konfliktu zbrojnego zaniecha wszelkiego użytkowania odnośnego obiektu, a w szczególności, gdy chodzi o port, dworzec kolejowy lub lotnisko – wyłączy go z wszelkiego ruchu komunikacyjnego. Wyłączenie takie powinno być przygotowane już w czasie pokoju.
>
> Ochrona specjalna zostaje przyznana dobru kulturalnemu przez wpisanie go do „Międzynarodowego Rejestru Dóbr Kulturalnych Objętych Ochroną Specjalną".

Co istotne z punktu widzenia → e d u k a c j i o b y w a t e l s k i e j i prawnej sił zbrojnych, konwencja zobowiązuje, by włączyć jej nauczanie

> do programów szkolenia wojskowego, a w miarę możliwości również cywilnego tak, aby […] zasady [konwencji – przyp. aut.] mogły być znane całej ludzkości, a zwłaszcza siłom zbrojnym i personelowi przydzielonemu do ochrony dóbr kulturalnych.

Konwencja została rozwinięta tekstem Protokołu drugiego do konwencji haskiej z 1954 r. o ochronie dóbr kulturalnych w razie konfliktu zbrojnego. Protokół podkreślił m.in. znaczenie prowadzenia specjalnych programów edukacyjnych i informacyjnych. Ponadto protokół w miejsce ochrony specjalnej wprowadził tzw. ochronę wzmocnioną (art. 10 i nast.). Zgodnie z postanowieniami Protokołu drugiego ochroną wzmocnioną może zostać objęte dobro kulturalne, pod warunkiem, że spełnia ono 3 następujące warunki:

a) jest dziedzictwem kulturalnym o największym znaczeniu dla ludzkości;

b) jest chronione na mocy odpowiednich krajowych środków prawnych i administracyjnych, uznających jego wyjątkową wartość kulturową i historyczną oraz zapewniającą ochronę w najwyższym stopniu;
c) nie jest wykorzystywane do celów wojskowych lub dla osłony miejsc wojskowych i Strona, która sprawuje władzę nad tym dobrem kulturalnym, złożyła deklarację potwierdzającą, że nie zostanie ono w ten sposób wykorzystane.

Regulacje Konwencji haskiej wraz z protokołami uzupełniają postanowienia norm →międzynarodowego prawa humanitarnego konfliktów zbrojnych [t. 3]. Również Statut →Międzynarodowego Trybunału Karnego [t. 3] chroni kulturę, penalizując działania skierowane przeciwko dobrom kulturalnym.

Piotr Łubiński

R. Abi-Saab, *Humanitarian Law and Internal Conflicts: The Evolution of Legal Concern*, [w:] *Humanitarian Law of Armed Conflict: Challenges Ahead – Essays in Honour of Frits Kalshoven*, A.J.M. Delissen, G.J. Tanja (eds.), Nijhoff Publishers, Dodrecht–Boston–London 1991; Art. 8 Konwencji o ochronie dóbr kulturalnych w razie konfliktu zbrojnego wraz z regulaminem wykonawczym do tej konwencji oraz Protokół o ochronie dóbr kulturalnych w razie konfliktu zbrojnego, podpisane w Hadze dnia 14 maja 1954, Dz. U. 1957 nr 46, poz. 212; Art. 10 drugiego Protokołu do Konwencji o ochronie dóbr kulturalnych w razie konfliktu zbrojnego, podpisanej w Hadze dnia 14 maja 1954 r., sporządzony w Hadze dnia 26 marca 1999 r., Dz. U. 2012, poz. 248; R. Bierzanek, *Wojna a prawo międzynarodowe*, Wydawnictwo Ministerstwa Obrony Narodowej, Warszawa 1982; W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe publiczne*, Wydawnictwo C.H.Beck, Warszawa 2004.

DOKTRYNA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ – dokument opracowany przez →Biuro Bezpieczeństwa Narodowego [t. 1] w konsultacji z organizacjami sektora publicznego (instytucji administracji, środowiska akademickiego) oraz prywatnego. Został zatwierdzony przez →Radę Bezpieczeństwa Narodowego [t. 3] 12 stycznia 2015 r. Ma charakter wykonawczy w stosunku do →Strategii Bezpieczeństwa Narodowego [t. 4].

Doktryna jest oficjalną podstawą koncepcyjną organów państwa Rzeczypospolitej Polskiej, mającą zapewnić strategiczny cel, którym jest →bezpieczeństwo [t. 1] funkcjonowania →cyberprzestrzeni [t. 1] w kontekście transsektorowym – w ujęciu praktycznym stanowi rekomendacje dla państwowych podmiotów odpowiedzialnych za teleinformatyczną →infrastrukturę krytyczną państwa oraz prywatnych podmiotów gospodarczych. Określa cele w dziedzinie →cyberbezpieczeństwa [t. 1], opisuje środowisko, wskazując na →zagrożenia [t. 4], ryzyka i szanse, a także wskazuje najważniejsze zadania, jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa.

Jego osiągnięciu ma służyć realizacja celów o charakterze operacyjnym i preparacyjnym. Do pierwszych zaliczono: ocenę warunków cyberbezpieczeństwa, w tym rozpoznanie zagrożeń, szacowanie ryzyka i identyfikowanie szans, zapobieganie zagrożeniom, redukowanie ryzyka i wykorzystanie szans, obronę i ochronę własnych systemów i ich zasobów, zwalczanie źródeł zagrożeń, odtwarzanie sprawności i funkcjonalności systemów cyberprzestrzeni po ewentualnym ataku. Warto zwrócić uwagę na wymienione zagadnienie „zwalczania źródeł zagrożeń", która precyzuje dopuszczalne odpowiedzi państwa w postaci działań ofensywnych i defensywnych, takich jak dezorganizacja, zakłócanie oraz niszczenie.

Cele preparacyjne sprowadzono do zbudowania, utrzymania i doskonalenia systemu cyberbezpieczeństwa obejmującego podsystemy kierowania (czyli organizowania skoordynowanych działań podmiotów państwowych i niepaństwowych), operacyjne i wsparcia (czyli posiadające rzeczywiste zdolności ofensywne i defensywne oraz możliwość wsparcia sojuszników). Dokument wskazuje Radę Ministrów jako organ, który ma być odpowiedzialny za koordynację działań w cyberprzestrzeni na poziomie strategicznym. Praktycznym posunięciem, które mogłoby przybliżyć realizację tego celu, jest pkt 38 doktryny rekomendujący tworzenie podporządkowanych właściwym ministrom odrębnych technicznych centrów kompetencyjnych.

Duże znaczenie ma umieszczony we wprowadzeniu wykaz pojęć, którymi posługuje się dokument, dotyczą one terminów w większości niezdefiniowanych w przepisach prawa polskiego, co w pewien sposób zawęża dalszą dyskusję i rozwiązuje dotychczasowe dylematy w naukach

społecznych i prawnych. Autorzy przybliżają m.in. definicję cyberbezpieczeństwa RP, bezpieczeństwa cyberprzestrzeni RP, →środowiska cyberbezpieczeństwa [t. 4], wyzwania cyberbezpieczeństwa, ryzyka cyberbezpieczeństwa, zagrożenia cyberbezpieczeństwa. Na uwagę zasługuje zdefiniowanie pojęcia cyberprzestrzeni w sposób odmienny od definicji legalnej zawartej m.in. w ustawach o stanie wojennym i o stanie wyjątkowym.

Zwrócono uwagę na podnoszenie świadomości obywatelskiej w zakresie cyberbezpieczeństwa oraz cyberobrony i cyberochrony kraju. Wiele miejsca poświęcono współpracy sektora publicznego i prywatnego, wspieraniu podmiotów sektora prywatnego.

W drugim rozdziale dokumentu podjęto analizę środowiska cyberbezpieczeństwa, które zdefiniowano jako ogół warunków funkcjonowania danego podmiotu w cyberprzestrzeni, scharakteryzowanego w doktrynie przez wskazanie wyzwań (szanse i ryzyka) oraz zagrożeń dla osiągania przyjętych celów, na 2 płaszczyznach – w wymiarze wewnętrznym i zewnętrznym.

Wśród najważniejszych wymienionych ryzyk wymiaru wewnętrznego są poruszone takie zagadnienia jak zakup infrastruktury technicznej systemowej z zagranicy oraz związany z tym brak dostępu do kodów źródłowych oprogramowania; problem dotyczący współpracy organów państwa z prywatnymi operatorami i dostawcami usług teleinformatycznych, których zarządy decyzyjne znajdują się poza granicami kraju; uwzględnienie ochrony →praw człowieka [t. 3] i obywatela w działaniach legislacyjnych i bezpośrednich, zwłaszcza z poszanowaniem prawa do wolności słowa oraz prywatności. W dokumencie zasugerowano rozwiązanie poprzez podniesienie wagi dialogu i znaczenia konsultacji społecznych, podniesienie stanu →edukacji obywatelskiej poprzez samokształcenie w zakresie cyberbezpieczeństwa – także poprzez wykorzystanie potencjału obywateli w społecznych inicjatywach wspierających cyberbezpieczeństwo RP w formie wolontariatu. Wsparcie dla tej inicjatywy miałoby powstać dzięki współpracy na linii obywatele – sektor prywatny – sektor publiczny.

Wśród poruszonych tematów związanych z szansami wymiaru wewnętrznego doktryna odwołuje się do rozwoju dziedziny nauk

informatycznych i podkreśla wyraźnie korelację między poziomem innowacyjności, posiadanej technologii, wiedzy i specjalistów a oddziaływaniem na → b e z p i e c z e ń s t w o n a r o d o w e [t. 1] państwa.

Doktryna zawiera zbiór zadań operacyjnych i preparacyjnych w dziedzinie cyberbezpieczeństwa państwa, które są skierowane do sektora publicznego w wymiarze krajowym i międzynarodowym, sektora prywatnego i obywatelskiego, wyznacza także zadania transsektorowe. Zadania operacyjne sektora publicznego w wymiarze krajowym obejmują m.in. rozpoznawanie źródeł zagrożeń, prowadzenie analiz ryzyka, działania w obszarze kryptografii i kryptoanalizy, bieżące monitorowanie zagrożeń z wykorzystaniem zespołów CERT (Computer Emergency Response Team), prowadzenie audytów cyberbezpieczeństwa. Podkreślono potrzebę przygotowania i wdrażania scenariuszy postępowania w warunkach → c y b e r a t a k ó w [t. 1] i planów reagowania kryzysowego. Zaakcentowano konieczność prowadzenia aktywnej cyberobrony oraz utrzymania gotowości do → c y b e r w o j n y [t. 1], ochrony i obrony własnych systemów teleinformatycznych, przeciwdziałania i zwalczania → c y b e r p r z e s t ę p c z o ś c i [t. 1]. Do zadań sektora publicznego w wymiarze międzynarodowym zaliczono w szczególności współpracę w ramach systemów reagowania → N A T O [t. 3] i UE. Zadania sektora prywatnego to współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom cybernetycznym, prowadzenie audytu środków i mechanizmów cyberbezpieczeństwa, współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni. Wśród zadań sektora obywatelskiego wymieniono na pierwszym miejscu dbałość o użytkowane systemy i urządzenia teleinformatyczne jako formę pomocy w zapewnieniu bezpieczeństwa państwa. Jedynym zadaniem transsektorowym jest koordynacja współpracy podmiotów sektora prywatnego i publicznego oraz tworzenie mechanizmów wymiany → i n f o r m a c j i, a także standardów i dobrych praktyk w obszarze cyberbezpieczeństwa.

Najważniejszym zadaniem preparacyjnym jest wdrożenie i rozwój systemowego podejścia do cyberbezpieczeństwa w wymiarze prawnym, w tym przyjęcie nowych rozwiązań prawnych, organizacyjnych i technicznych. Rozwiązania przyjmowane w tym zakresie powinny być zgodne z dokumentami UE i NATO oraz innymi inicjatywami międzynarodowymi.

Twórcy doktryny zakładają wykorzystanie i rozszerzenie jej treści w pracach nad innymi dokumentami, takimi jak Polityczno-Strategiczna Dyrektywa Obronna, w planach →zarządzania kryzysowego [t. 4], programach rozwoju sił zbrojnych oraz programach pozamilitarnych przygotowań obronnych.

Wojciech Cendrowski

M. Adamczuk, K. Liedel, *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12; W. Cendrowski, *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2015; J. Kowalewski, M. Kowalewski, *Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017; Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz. U. 2002, nr 156, poz. 1301; Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz. U. 2002, nr 11, poz. 985.

DOKTRYNA MILITARNA (właśc. wojskowa) – oficjalnie przyjęty przez państwo system naukowo uzasadnionych poglądów dotyczących sposobu przygotowania obrony kraju w sytuacjach →zagrożenia [t. 4] zewnętrznego oraz prowadzenia działań wojennych z zastosowaniem metod i środków będących w dyspozycji państwa lub koalicji państw. Za sprawą powyższej definicji doktryna militarna często jest utożsamiana z doktryną wojenną, która jest pojęciem nieco szerszym i stanowi zbiór poglądów i idei związanych z przygotowaniem i prowadzeniem →wojny [t. 4] jako całości z uwzględnieniem takich czynników jak ustrój państwa, sytuacja polityczna (wewnętrzna i międzynarodowa), zasoby kraju, potencjał gospodarczy, poziom naukowo-techniczny, doświadczenie prowadzenia wojny, położenie geograficzne.

Doktryna militarna wywodzi się ze →sztuki wojennej [t. 4] będącej dziedziną wiedzy i umiejętności dotyczącą form i sposobów przygotowania oraz prowadzenia działań wojennych. Sztuka wojenna już w starożytności zaliczana była, podobnie jak większość dziedzin nauki,

do filozofii, a jako pierwszy opisał ją żyjący na przełomie VI i V w. p.n.e. chiński generał i filozof Sun Zi (Sun Tzu).

Polityka wojskowa jest integralną częścią działań każdego państwa, a jej głównym celem jest zagwarantowanie →bezpieczeństwa [t. 1] wojskowego kraju. Skoncentrowane rozumienie polityki wojskowej znajduje się w państwowej doktrynie wojskowej/militarnej, czyli deklaracji polityki państwa w dziedzinie bezpieczeństwa wojskowego (obronnego) określającej system oficjalnych poglądów i przepisów wyznaczających kierunki budowy wojsk, warunki przygotowania państwa i sił zbrojnych do wojny, środki i formy prowadzenia wojny. Podstawowe postanowienia doktryny militarnej są opracowywane i zmieniane w zależności od polityki i porządku społecznego, poziomu rozwoju sił produkcyjnych, nowych osiągnięć naukowych i charakteru spodziewanej wojny.

W rzeczywistości doktryna militarna stanowi ideologiczny rdzeń wszelkiej militarno-politycznej działalności państwa (polityki wojskowej) jako jeden z kierunków ogólnej polityki państwa, partii politycznych, organizacji pozarządowych i instytucji. Dotyczy interesów społeczeństwa i wszystkich struktur państwowych. W dokumentach tego rodzaju intencje państwa są głoszone otwarcie, więc doktryna wojskowa nie powinna zawierać żadnych zamkniętych rozdziałów, nie może jej opracowywać konkretna grupa osób, niezależnie od publicznych i wojskowych środowisk akademickich. Podstawowe elementy doktryny wojskowej mogą w zależności od formy rządu zostać określone przez odpowiednie władze państwowe na określony czas.

Doktryna militarna uwzględnia aspekty polityczne i wojskowo-techniczne. Podstawowe założenia doktryny są określane przez kierownictwo polityczne i wojskowe państwa w zależności od ustroju społeczno-politycznego i poziomu rozwoju gospodarczego, naukowego i technicznego oraz wyposażenia sił zbrojnych kraju. Doktryna militarna jest wyrazem tego, w jaki sposób siły wojskowe przyczyniają się do kampanii, dużych operacji, bitew i walk, jednocześnie oznacza zbiór zasad, którymi siły zbrojne kierują się w działaniach, prowadząc swoje operacje. Obejmuje elementy →obrony narodowej [t. 3] i sojuszniczej zarówno z perspektywy społeczno-politycznej, jak i wojskowo-technicznej.

W XX w. zasadniczo wykształciły się 3 typy doktryn wojennych, mające charakter defensywny (obronny), ofensywny i mieszany. Zasadnicza

różnica pomiędzy nimi polega na tym, że podstawowe założenia doktryny wojennej formułują najwyższe organy władzy państwowej (parlament, prezydent), a doktrynę militarną – naczelne dowództwo armii danego państwa albo sojuszu wojskowego.

Swoje doktryny w XX w. posiadał każdy rodzaj sił zbrojnych – wojska powietrzne, → w o j s k a l ą d o w e [t. 4], → m a r y n a r k a w o j e n n a [t. 3]. Wszystkie zawierały podstawowe normy postępowania i ogólne procedury pozwalające na maksymalne skoordynowanie działań tych formacji. Jest to przewodnik po działaniu, a nie twarde i skodyfikowane zasady postępowania. Doktryna zapewnia wspólne ramy odniesienia dla całej armii. Pomaga ustandaryzować operacje, ułatwiając gotowość, ustanawiając wspólne sposoby wykonywania zadań wojskowych. Doktryna łączy teorię, historię, eksperymenty i praktykę. Jej celem jest wspieranie inicjatywy i kreatywnego myślenia. Doktryna dostarcza armii zbiór oświadczeń na temat tego, jak siły wojskowe prowadzą operacje, i zapewnia wspólny leksykon do wykorzystania przez planistów i dowódców wojskowych.

W wielu krajach termin doktryna militarna traktuje się jako politykę → b e z p i e c z e ń s t w a [t. 1], która reprezentuje system poglądów oficjalnie przyjętych i wiążących przez pewien czas w danym państwie (koalicji wojskowej), opisując charakter możliwych konfliktów zbrojnych oraz przygotowanie i wdrożenie zbrojnej zewnętrznej ochrony państwa. Dlatego doktryna militarna działa głównie jako dokument konstytutywny. Opracowanie szczegółów wdrożenia w wojskowej praktyce politycznej jest zwykle obowiązkiem kolejnych dokumentów lub kompetencji organów władzy państwowej.

Jednocześnie doktryna nie jest → s t r a t e g i ą [t. 4], operacją ani taktyką, służy jako ramy koncepcyjne łączące wszystkie 3 poziomy działań wojennych. Doktryna różni się również od teorii, ponieważ jest instytucjonalna, ma charakter poznawczy, ponieważ jest zarówno częścią, jak i wynikiem procesu zdobywania, oceny i rozpowszechniania wiedzy. Doktryna jest z natury subiektywna, ponieważ jej treść odzwierciedla system przekonań. Ale doktryna to coś więcej niż tylko zasady. Jest to refleksja nad tym, w jaki sposób siły armii zamierzają działać jako część wspólnych sił, oraz stwierdzenie, w jaki sposób armia zamierza walczyć. Ustanawia wspólne ramy odniesienia, w tym narzędzia intelektualne, których

przywódcy armii używają do rozwiązywania problemów wojskowych. Ma skupiać się na tym, „jak" myśleć, a nie na tym, „co" myśleć.

Definicja doktryny →NATO [t. 3], stosowana przez wiele państw członkowskich w niezmienionej formie, brzmi: „Podstawowe zasady, zgodnie z którymi siły zbrojne wykonują swoje zadania z zamiarem osiągnięcia określonych celów. Odgrywa ona rolę nadrzędną, ale wymaga oceny zasadności wykorzystania jej w praktyce". Do niedawna większość doktryn NATO była odzwierciedlona przez równoważne, ale różne narodowe doktryny. Często powodowało to dylemat dla sił zbrojnych różnych państw zaangażowanych w operacje w ramach koalicji.

Współczesne doktryny amerykańskie opierają się na koncepcji operacji pełnego spektrum, które łączą operacje ofensywne, defensywne i stabilności lub wsparcia cywilnego, jednocześnie w ramach współzależnych lub połączonych sił w celu przejęcia, utrzymania i wykorzystania inicjatywy. Stosują zsynchronizowane działania – śmiercionośne i nieśmiercionośne – proporcjonalne do misji i oparte na dokładnym zrozumieniu wszystkich wymiarów środowiska operacyjnego. Operacje ofensywne pokonują i niszczą siły wroga oraz zajmują teren, zasoby i centra ludności, narzucają wrogowi wolę dowódcy. Operacje obronne pokonują atak wroga, zyskują czas, oszczędzają siły i rozwijają warunki sprzyjające operacjom ofensywnym lub stabilności. Operacje stabilności obejmują różne misje wojskowe, zadania i działania prowadzone za granicą w celu utrzymania lub przywrócenia bezpiecznego środowiska, odbudowy infrastruktury w→sytuacjach kryzysowych [t. 4] i pomocy humanitarnej. Operacje wsparcia cywilnego to zadania i misje wspierające cywilów na wypadek sytuacji kryzysowych w kraju i innych działań dotyczących skutków klęsk żywiołowych lub katastrof spowodowanych przez człowieka.

Wojsko USA potrzebuje wspólnej doktryny, która poprowadzi wszystkie służby w kierunku skoordynowanego podejścia do operacji obejmujących wiele dziedzin i zapewni odpowiednie inwestycje w dowodzenie i kontrolę, tworzenie sieci i podejmowanie decyzji. Ostatnia wspólna doktryna (JP-1) została opublikowana w 2013 r. a zmieniona w 2017 r. Nawet wraz z aktualizacją nie odzwierciedla ona nowych wyzwań strategicznych stawianych przez wschodzące wielkie mocarstwa, takie jak Rosja i Chiny, ani wzmocnionych regionalnych przeciwników,

takich jak Iran i Korea Północna. Nie odnosi się także do podstawowych założeń nowych strategii →bezpieczeństwa narodowego [t. 1] lub obrony narodowej, nie odzwierciedla charakteru rywalizacji między mocarstwami, zasięgu i złożoności zagrożeń dla bezpieczeństwa USA i Zachodu, zmian technologicznych dotyczących sposobu prowadzenia operacji wojskowych.

Armia kanadyjska ma swoją definicję doktryny militarnej:

> Doktryna militarna jest formalnym wyrazem wiedzy i myśli wojskowej, którą armia uznaje za istotne w danym czasie, która obejmuje charakter konfliktu, przygotowanie armii do konfliktu oraz metodę angażowania się w konflikt, aby osiągnąć sukces […]. Ma charakter opisowy, a nie nakazowy, wymaga przemyślenia w zastosowaniu. Nie ustanawia dogmatów ani nie zapewnia listy kontrolnej procedur, ale jest nadrzędnym przewodnikiem opisującym to, jak wojsko myśli o walce, a nie jak powinno walczyć. Stara się być wystarczająco definitywną, aby pokierować działaniami wojskowymi, a jednocześnie wystarczająco wszechstronną, aby uwzględnić wiele różnych sytuacji.

Przez ok. 280 lat armia brytyjska osiągała znaczące sukcesy bez formalnej doktryny wojskowej, chociaż powstało wiele publikacji dotyczących taktyki, operacji i administracji. Jednak podczas pełnienia funkcji szefa sztabu generalnego (1985–1989) gen. N. Bagnall zlecił przygotowanie brytyjskiej doktryny wojskowej płk. (późniejszemu gen.) T. Granville'owi-Chapmanowi (oficerowi →artylerii [t. 1], który był jego asystentem wojskowym w 1. Korpusie Brytyjskim). Pierwsze wydanie *British Military Doctrine* (BMD) zostało opublikowane w 1988 r., a w 1996 r. stała się ona brytyjską doktryną obronną (*British Defence Doctrine*, BDD) obowiązującą we wszystkich siłach zbrojnych. Czwarta edycja BDD została opublikowana w 2011 r., wykorzystując definicję doktryny NATO.

Radzieckie znaczenie doktryny wojskowej bardzo różniło się od użycia tego terminu przez wojsko USA. A. Grieczko, minister obrony ZSRR, marszałek Związku Radzieckiego, naczelny dowódca Wojsk Lądowych Armii Radzieckiej, naczelny dowódca Zjednoczonych Sił

Zbrojnych Państw Stron Układu Warszawskiego, zdefiniował ją w 1975 r. jako „system poglądów na temat natury wojny i metod jej prowadzenia oraz na temat przygotowania kraju i armii do wojny, oficjalnie przyjętych w danym państwie i jego siłach zbrojnych". W czasach radzieckich teoretycy podkreślali zarówno polityczną, jak i wojskowo-techniczną stronę doktryny wojskowej, podczas gdy z punktu widzenia ZSRR ludzie Zachodu ignorowali stronę polityczną. Doktryna radziecka (i współczesna rosyjska) podkreśla rozpoczęcie działań wojennych w wybranym przez siebie czasie i miejscu, zgodnie z wyborem i obszernym przygotowaniem pola bitwy do operacji.

Doktryna wojskowa Federacji Rosyjskiej jest dokumentem planowania strategicznego i stanowi system oficjalnie przyjętych poglądów na stan przygotowań do obrony zbrojnej Rosji. Najnowsza wersja doktryny wojskowej została zatwierdzona w 2014 r. Liczne kolejne rewizje doktryny wojskowej były ogłaszane w listopadzie 1993 r. po wydarzeniach w Naddniestrzu 1993 r.; w kwietniu 2000 r. po wojnie w Czeczenii w 1999 r.; w lutym 2010 r. po wojnie rosyjsko-gruzińskiej w 2008 r. oraz w grudniu 2014 r. po → a n e k s j i [t. 1] Krymu i początku wojny na wschodzie Ukrainy w 2014 r. Doktryna w ujęciu rosyjskim wykracza poza dyskusję o potencjalnych zagrożeniach. Chronologia wydarzeń, które ją poprzedzały, i odsłony doktryny FR w nowych wydaniach pokazują, jak rosyjscy przywódcy próbują za każdym razem zalegalizować swoje przestępcze działania, wybielić je, a co najważniejsze, dać na przyszłość podobnym przestępstwom podstawę prawną. Doktryna wojskowa Rosji wyraźnie stwierdza, że 3/4 doktryny to komponent informacyjny albo wpływ ekonomiczny i tylko 1/4 to wykorzystanie siły fizycznej.

Doktryna militarna jest podstawową koncepcją bezpieczeństwa państwa, dąży również do sformułowania celów i zadań polityki wojskowej państwa oraz określenia priorytetowych interesów, a także do wyrażenia swojego stanowiska w kwestiach wojennych i zagadnieniach związanych z obszarami użytkowania sił zbrojnych oraz przygotowywaniem misji bojowych przydzielonych siłom państwa w czasie wojny lub pokoju. Jest również diagnozą charakteru faktycznych i potencjalnych → z a g r o ż e ń m i l i t a r n y c h [t. 4] wobec państwa, stara się określić charakter przyszłej wojny oraz metody, za pomocą których można odeprzeć wszelką

→agresję [t. 1] środkami militarnymi i opracować nowe koncepcje strategii wojskowych oraz wytyczne dotyczące przygotowania państwa w celu obrony terytorium państwa i jego bezpieczeństwa.

Doktryna składa się z podstawowych zasad, taktyki, technik, procedur oraz terminów i symboli. Przede wszystkim doktryna zawiera podstawowe zasady. Odzwierciedlają one poglądy armii na temat działań wojennych na podstawie jej dawnych doświadczeń, porażek i sukcesów, określają zasady ognia, manewrów i wspólnych operacji sił zbrojnych. Co ważne, doktryna nie zawsze ma charakter nakazowy, ale jest nadrzędna i stanowi punkt wyjścia do rozwiązywania nowych problemów. Zasady powinny wspierać inicjatywę, by →żołnierze [t. 4] byli zdolni do adaptacji i kreatywni w rozwiązywaniu trudności, są podstawą wprowadzania nowych technologii i projektów organizacyjnych.

Taktyki, techniki i procedury wykorzystują wiedzę i doświadczenie armii, wspierają i wdrażają podstawowe zasady, obejmują różne metody i procesy. Taktyka polega na uporządkowanym rozmieszczeniu sił względem siebie. Techniki to nie nakazowe sposoby lub metody wykorzystywane do wykonywania misji, funkcji lub zadań, są one podstawowym sposobem przekazywania wyciągniętych wniosków, które jednostki zdobywają podczas operacji. Procedury to standardowe metody postępowania, zwykle składają się z szeregu kroków w ustalonej kolejności. Procedury są nakazowe, niezależnie od okoliczności są one wykonywane w ten sam sposób. Wspólny zestaw procedur w wojsku obejmuje standardową procedurę operacyjną dla poszczególnych jednostek. Wreszcie doktryna zapewnia wspólny język komunikacji wojskowych. Jest to szczególnie ważne podczas konfliktu zbrojnego, gdy →informacje muszą być szybko i dokładnie przekazywane oraz powszechnie zrozumiałe.

Terminy i definicje stanowią większą część wspólnego języka armii, zrozumiałego dla wszystkich jej jednostek tak, aby jasne były zadania, które należy wykonać. Symbole wojskowe są sposobem zapewnienia wspólnego graficznego zrozumienia niezliczonej ilości informacji i zapewniają inny sposób szybkiego przesyłania informacji. Ustanawianie i używanie słów i symboli o wspólnych znaczeniach wojskowych usprawnia komunikację i umożliwia wspólne rozumienie doktryny, szybką identyfikację zaangażowanych jednostek, dokładną identyfikację zadań do wykonania.

Znaczenie tego wspólnego języka jest nieprzecenione. Pozwala osobom z zupełnie różnych środowisk na szybką naukę uniwersalnego języka. Umożliwia armii szybkie komunikowanie się, nawet gdy istnieje bariera językowa.

Fryderyk II Wielki (Friedrich II von Hohenzollern) – król Prus w latach 1740–1786, pod rządami którego Prusy stały się jednym z najpotężniejszych państw europejskich, powiedział: „Wojna nie jest przypadkiem. Aby dobrze ją prowadzić, niezbędna jest ogromna wiedza, nauka i medytacja".

Olga Wasiuta

AAP-06 Edition 2019. NATO glossary of terms and definitions (English and French), NATO Standardization Office, 2019; *AAP-6. Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO*, NATO Standardization Office, 2017; I.T. Brown, *A New Conception of War: John Boyd, the U.S. Marines, and Maneuver Warfare*, Marine Corps University Press, Quantico, Virginia 2018; Canada Department of National Defence, *Conduct Of Land Operations – Operational Level Doctrine For The Canadian Army (English)*, Department of National Defence, 1998; R.M. Cassidy, *Peacekeeping in the Abyss: British and American Peacekeeping Doctrine and Practice after the Cold War*, Praeger, London 2004; B. Chapman, *Military Doctrine: A Reference Handbook*, ABC-CLIO, Santa Barbara 2009; R. Frank, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907–1960*, Air University Press, 1989; A.P. Jackson, *The Roots of Military Doctrine: Change and Continuity in Understanding the Practice of Warfare. Combat Studies Institute Press*, Fort Leavenworth, KA 2013; E. Kier, *Imagining War: French and British Military Doctrine between the Wars*, Princeton University Press, Princeton 1998; A. Long, *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the US and UK*, Cornell University Press, London 2016; G. Sheffield, *Doctrine & Command in the British Army, A Historical Overview*, Army Doctrine Publication Land Operations, DGD&D, British Army, 2005; Ch.P. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations*, Cornell University Press, London 2010.

DOKTRYNA ONZ „ODPOWIEDZIALNOŚĆ ZA OCHRONĘ" (ang. *Responsibility to Protect*, R2P, RtoP) – doktryna, która proponuje szereg kompleksowych rozwiązań – od prewencji, poprzez reakcję, do odbudowy – stosowanych w celu → o c h r o n y l u d n o ś c i [t. 3] przed najdotkliwszymi

następstwami konfliktu. Doktryna ma ważną ogólną wartość teoretyczną, ponieważ dotyczy bezpośrednio podstawowych kategorii prawnych, w szczególności →prawa człowieka [t. 3] i →suwerenności państwa [t. 4]. Jak podkreśla A.-M. Slaughter:

> doktryna odpowiedzialności za ochronę jest najważniejszą doktryną w koncepcji suwerenności państwa od czasu pokoju westfalskiego 1648 r. Zakłada ona fundament ładu międzynarodowego, który uznaje prawa i obowiązki jednostek i narodów.

Współczesne procesy transformacji stosunków międzynarodowych i myślenia geopolitycznego mają znaczący wpływ na kształtowanie nowego podejścia do →bezpieczeństwa narodowego [t. 1] jako jednego z głównych problemów geopolitycznych państwa. Znacznie zwiększa się rola czynników niemilitarnych bezpieczeństwa narodowego, jak stanu systemów informacyjnych, rozwoju strategicznie ważnych gałęzi nauki, ogólnego poziomu wykształcenia ludności itp.

Wydarzenia społeczne i polityczne ostatnich lat stały się trudnym sprawdzianem właściwości regulacyjnych i efektywności prawa międzynarodowego oraz zaktualizowały nowe problemy współczesnych badań. W tym samym czasie, gdy społeczeństwo staje w obliczu →zagrożenia [t. 4] →zbrodniami przeciwko ludzkości [t. 4], →ludobójstwem [t. 3], czystkami etnicznymi i innymi masowymi i rażącymi naruszeniami praw człowieka, a konkretne państwo najwyraźniej nie jest w stanie im przeciwdziałać, wtedy zobowiązania podtrzymania →bezpieczeństwa [t. 1] opierają się na społeczności międzynarodowej. Te idee zawiera doktryna „odpowiedzialność za ochronę".

We wrześniu 2000 r. z inicjatywy Kanady powstała Międzynarodowa Komisja ds. Interwencji i Suwerenności Państwa przy Organizacji Narodów Zjednoczonych (International Commission on Intervention and State Sovereignty, ICISS). W jej skład weszli wybitni specjaliści w zakresie międzynarodowego prawa człowieka, na czele z byłym ministrem spraw zagranicznych Australii G. Evansem i specjalnym doradcą sekretarza generalnego ONZ M. Sakhnunem. W 2001 r. grupa przedstawiła sekretarzowi generalnemu i państwom członkowskim ONZ dobrze

znany w prawie międzynarodowym raport *The Responsibility to Protect* (R2P), w którym zaproponowano alternatywę dla tzw. prawa do humanitarnej interwencji, zastępując je „odpowiedzialnością za ochronę". W doktrynie podkreślono transformację międzynarodowego rozumienia ochrony ludności i praw człowieka, przewidując międzynarodową interwencję w przypadku ludobójstwa czy innych masowych zbrodni i redefiniując pojęcie suwerenności. W raporcie komisji opublikowanym w grudniu 2001 r. bez odpowiedzi pozostało pytanie, czy i pod jakimi warunkami →interwencja humanitarna byłaby legalna w przypadku braku autoryzacji ze strony →Rady Bezpieczeństwa ONZ [t. 3] lub Zgromadzenia Ogólnego ONZ.

Odpowiedzialność za ochronę jest koncepcją prawa międzynarodowego, nową zasadą miękkiego prawa międzynarodowego, która została podtrzymana przez ONZ w 2005 r. Składa się ona z kilku reguł, opartych na idei suwerenności nie jako przywileju państwa, a jako przede wszystkim obowiązku, historycznie wynikających z idei pokoju westfalskiego i norm nieinterwencji. Ogólnie doktryna R2P stwierdza, że „suwerenne państwa mają obowiązek chronić swoich obywateli przed możliwością uniknięcia katastrofy", a „społeczność międzynarodowa ma obowiązek promowania i wspierania państw w wypełnianiu tego obowiązku".

Jej źródłem jest koncepcja interwencji humanitarnej, odrzucona przez społeczność międzynarodową po akcji →NATO [t. 3] przeciw Jugosławii, w związku z konfliktem w Kosowie. Nowa doktryna koncentruje się na zapobieganiu międzynarodowym zbrodniom ludobójstwa, →zbrodniom wojennym [t. 4], zbrodniom przeciwko ludzkości i czystkom etnicznym. Zastosowanie R2P w przypadku innych przestępstw lub katastrof humanitarnych jest wykluczone. Interwencja humanitarna sama w sobie jest konceptualną hybrydą znajdującą się na skrzyżowaniu praw człowieka, prawa międzynarodowego i stosunków międzynarodowych. Przede wszystkim istnieje wyraźna potrzeba normatywnego ujęcia zasad i ich politycznego egzekwowania.

W wyniku wydarzeń z lat 90. XX w. doszło do poważnej i bardzo nagłośnionej międzynarodowej debaty oraz rewizji zasady nieinterwencji, w wyniku czego społeczność międzynarodowa zaczęła dopuszczać interwencje zbrojne jako prawnie i moralnie uzasadnione

w wyjątkowych okolicznościach oraz po wyczerpaniu się możliwości zastosowania innych środków. Do przypadków takich zaliczono akty ludobójstwa, upadek państwa skutkujący przewlekłym →kryzysem wewnętrznym i anarchią, łamanie praw człowieka i zagrożenia dla pokoju międzynarodowego.

Zgodnie z koncepcją podstawowym obowiązkiem państwa jest ochrona ludności na terytorium własnego państwa. Zakłada ona, że każde państwo ma obowiązek chronić swoją ludność przed ludobójstwem, zbrodniami wojennymi, czystkami etnicznymi oraz zbrodniami przeciwko ludzkości. Kiedy państwa nie mogą lub nie chcą wypełniać tego obowiązku – czy to z powodu braku możliwości, czy z przyczyn związanych z wolą polityczną – odpowiedzialność za ochronę przenosi się na wspólnotę międzynarodową, nawet wbrew władzom danego państwa. Wspomniana idea stała się m.in. podstawą interwencji w Libii w 2011 r. Odpowiedzialność za ochronę jest przemyśleniem koncepcji interwencji humanitarnej, ale w odróżnieniu od niej wykorzystuje działania zbrojne jako obowiązek społeczności międzynarodowej, a nie jako prawo państwa lub grupy państw.

Jednak w końcowym dokumencie Światowego Szczytu ONZ z 2005 r., przyjętym przez Zgromadzenie Ogólne (rezolucja nr 60/1), wykluczono możliwość podejmowania działań przez poszczególne państwa na podstawie doktryny R2P bez zezwolenia Rady Bezpieczeństwa ONZ. Pierwszą rezolucją Rady autoryzującą użycie siły w odwołaniu do koncepcji R2P była rezolucja nr 1973, na podstawie której miała miejsce interwencja w Libii w 2011 r. (Rosja i Chiny wstrzymały się wtedy od głosu). Rosja poparła interwencję w Libii (pierwsze właściwe zastosowanie R2P), wstrzymując się od głosowania w Radzie Bezpieczeństwa ONZ, ale wniosła swój wkład w impas w Syrii, nie zgadzając się nawet na przyjęcie rezolucji potępiającej okrucieństwa →reżimu [t. 3] Assada. Potępiła natomiast wdrożenie decyzji Rady Bezpieczeństwa w sprawie Libii jako wykraczającej daleko poza zakres rezolucji. Decyzja o ochronie ludności cywilnej została zastąpiona zmianą reżimu. Interweniując w celu ochrony ludności cywilnej, siły NATO ukierunkowały swoje działania także na obalenie reżimu Kaddafiego. Ta szeroka interpretacja mandatu Rady miała istotny wpływ na niechęć Rosji i Chin do wdrażania jakichkolwiek sankcji

przeciwko Syrii. Przypadek Libii pokazuje więc, jak istotne jest, aby R2P jako bardzo młoda doktryna, niemająca charakteru prawnie wiążącego, była stosowana rygorystycznie i w sposób neutralny.

Istnieją poglądy, że doktryna R2P może być wykorzystywana także w innych sytuacjach. Jest ona normą, nie prawem, choć wiąże się z prawem międzynarodowym. Przez długi czas ta doktryna była potężnym narzędziem oddziaływania zachodniej społeczności poprzez negocjacje, →sankcje [t. 4] ekonomiczne, przy wsparciu organizacji pozarządowych, państw i instytucji międzynarodowych. Innym przykładem może być, pomijając nawet wydarzenia z sierpnia 2008 r., kiedy sytuacja była nieco inna i Rosja rozpoczęła operację militarną przeciwko Gruzji, →aneksja [t. 1] Krymu i rozmieszczenie wojsk rosyjskich w Ukrainie, przez rosyjskich analityków uznawane za zgodne z zachodnimi koncepcjami „interwencji humanitarnej" i doktryny R2P.

R2P opiera się na 3 filarach:

- obowiązku każdego państwa do ochrony swojej ludności przed wymienionymi zbrodniami,
- zobowiązaniu się społeczności międzynarodowej do pomocy państwom w wypełnianiu swoich obowiązków w tym zakresie,
- gotowości państw do kolektywnego działania w ramach zasad Karty Narodów Zjednoczonych, kiedy państwo nie jest w stanie ochronić swojej ludności.

Różne ujęcia R2P odnoszą się do 5 kryteriów wspomagających ocenę legalności ewentualnej interwencji:

- kryterium stopnia zagrożenia,
- celu – przeciwdziałanie ludzkiemu cierpieniu,
- ostateczności – inne możliwe i dostępne pokojowe rozwiązania zawiodły,
- proporcjonalności środków – działania wojskowe powinny być ograniczone do minimum koniecznego do osiągnięcia celu,
- bilansu skutków – korzyści z interwencji powinny przewyższać skutki zaniechania działania.

R2P jest ważną oraz zyskującą na znaczeniu zasadą, jednak podważa pkt. 7 art. 2 Karty Narodów Zjednoczonych (KNZ). Ów mówi o tym, że żadne postanowienie KNZ nie upoważnia ONZ do ingerencji w sprawy,

które ze swojej istoty należą do kompetencji wewnętrznych któregokolwiek państwa.

Chociaż R2P została przyjęta przez społeczność międzynarodową w 2005 r., wciąż jest słabo rozpoznawalna przez państwa członkowskie ONZ, jeśli chodzi o jej praktyczne zastosowanie. R2P nie jest jeszcze powszechnie akceptowaną zasadą, ale stała się ważną normą, dzięki której Zachód ma nadzieję na zbudowanie globalnej opieki nad naruszeniem praw człowieka. W kontekście prawa międzynarodowego R2P koncentruje się na ochronie ludności, a nie na interwencji w celu zmiany stylu rządzenia suwerennym państwem. Od kiedy norma została wprowadzona do społeczności międzynarodowej, narracja R2P była stosowana przez Radę Bezpieczeństwa ONZ w kilku rezolucjach. Jednak w przypadku interwencji w Libii i Republice Środkowoafrykańskiej R2P była wyraźnie cytowana tylko w odniesieniu do legalnej siły militarnej. R2P należy odróżniać od interwencji humanitarnej, ponieważ interwencja humanitarna jest tylko jedną z dostępnych odpowiedzi związanych z zasadą R2P.

Naukowcy twierdzą, że interwencja humanitarna jest uzasadniona, gdy:

- system Rady Bezpieczeństwa ONZ nie działa, a rezolucja jest niedostępna,
- trwa kryzys humanitarny związany ze zbrodniami wojennymi, zbrodniami przeciwko ludzkości, ludobójstwem, czystkami etnicznymi, występują dowody skrajnego nieszczęścia humanitarnego wymagającego natychmiastowej pomocy, kryzys humanitarny zakłóca porządek międzynarodowy (art. 51 KNZ – prawo państwa do samoobrony),
- używanie siły powinno być dozwolone tylko po to, aby powstrzymać działania niezgodne z prawem i musi być konieczne, proporcjonalne i ukierunkowane na pomoc humanitarną, wyłącznie w celu położenia kresu zbrodniom i przywróceniu praw człowieka,
- musi być jasne, że nie ma praktycznej alternatywy poza interwencją, a żadne pokojowe rozwiązanie nie jest możliwe,
- żadne państwo nie powinno jednostronnie podejmować działań.

Te starannie przemyślane zasady zawiodły w przypadku → w o j n y d o m o w e j [t. 4] w Syrii. Chociaż w Radzie Bezpieczeństwa ONZ nie osiągnięto konsensusu co do tego, jakie działania należy podjąć, ale

większość zgadza się, że interwencja humanitarna jest uzasadniona faktem, że Baszar Al-Asad użył → b r o n i c h e m i c z n e j [t. 1] przeciwko swojej ludności. Po drugiej stronie medalu znajduje się Rosja, która dokonała aneksji Krymu, części terytorium innego państwa, twierdząc, że zrobiła to, ponieważ miała „obowiązek ochrony":

- tych, którzy sprzeciwiają się → „ p u c z o w i w o j s k o w e m u" [t. 3] Euromajdanu, i tych, którzy byli „zagrożeni represjami", a także ogólnie mniejszość rosyjskojęzyczną,
- przed nacjonalistami (zob. → n a c j o n a l i z m [t. 3]), neonazistami (zob. → n e o n a z i m [t. 3]), rusofobami i antysemitami, którzy dokonali nielegalnego i niekonstytucyjnego zamachu stanu i pozostają u władzy,
- ponadto Rosja legitymizowała użycie siły (→ i n w a z j a i aneksja Krymu) za zgodą parlamentu, a prezydent Ukrainy W. Janukowycz i premier Krymu wezwali Rosję do użycia siły militarnej w celu „ochrony ich życia i praw".

Takie argumenty nie mogły być podstawą ani jednostronnej → s e c e s j i [t. 4], ani jednostronnej interwencji humanitarnej. W tym czasie etniczni Rosjanie nie byli zabijani ani prześladowani. Represje, o których mówił W. Putin, nie uzasadniają interwencji Rosji, a interwencja oparta na zainteresowaniach jest współczesną wersją imperializmu.

Putin posunął się za daleko – aneksja, → a g r e s j a [t. 1] i interwencja, gdy nie ma kryzysu humanitarnego, są tak samo szkodliwe dla koncepcji R2P, jak brak działania, gdy kryzys humanitarny jest jawnie oczywisty. Jakkolwiek trudna jest równowaga pomiędzy pomocą humanitarną a interesami państwa, ważne jest, aby ludzie nie cierpieli, nie zważając na wszystkie inne czynniki. Wola polityczna (pod wpływem interesów państwa) niestety zwycięża nad względami humanitarnymi i widzimy groteskowe tego przykłady w Ukrainie i Syrii. W Ukrainie rosyjska wola polityczna doprowadziła do interwencji bez legitymizacji, a w Syrii warunki zostały spełnione, lecz nie było woli politycznej (ze strony Rosji i Chin) do działania w obliczu kryzysu. Dlatego dobrze byłoby wziąć pod uwagę – lub przynajmniej nie całkowicie odrzucić – wolę polityczną i interesy państwa w rozważaniu stosowania zasady R2P. Zasadą jest, aby ta doktryna działała niezależnie od interesów państwowych, ale niestety

jest ona i tak napędzana wolą polityczną, która musi być uwzględniana przy każdej ocenie zastosowania tej doktryny, inaczej niezbędna byłaby zmiana praktycznie całej koncepcji. Ukraina i Syria to bardzo dobre przykłady konsekwencji działania i bezczynności.

Rosja była przekonana, że każda interwencja mająca na celu powstrzymanie cierpienia i →przemocy [t. 3] w Syrii musi zostać zatwierdzona przez Radę Bezpieczeństwa. Natomiast w 2014 r., w odpowiedzi na nieznane i niejasne groźby dla ukraińskich Rosjan, Kreml był chętny do jednostronnego odrzucenia suwerenności Ukrainy. Nie było zrozumiałe, w obliczu jakiego zagrożenia znajdowali się Rosjanie z Ukrainy: na Krymie nie było bezpośredniego zagrożenia ludobójstwem, zbrodniami przeciwko ludzkości ani czystkami etnicznymi, których dziś doświadcza naród tatarski. Używanie przez Rosję koncepcji R2P jest tym bardziej niepewne, że większość zagrożeń dla Ukraińców płynie z samej Rosji. Doktryna kategorycznie wyklucza możliwość jej wykorzystania przez jedno państwo przeciwko innemu państwu pod hasłem „ochrony obywateli" przed rzekomymi zagrożeniami, a w celu aneksji obcych terytoriów.

Inwazja na Ukrainę nie dotyczy koncepcji R2P, ponieważ jedynym prawowitym organem, który decyduje o zatwierdzeniu interwencji, jest Rada Bezpieczeństwa ONZ. Interwencja w imię odpowiedzialności za ochronę nie może być jednostronna. Poprzez sprzeniewierzenie i nadużywanie koncepcji R2P w celu usprawiedliwienia interwencji Rosja osłabia samą koncepcję R2P.

Gdy R2P została przywołana przez Radę Bezpieczeństwa ONZ w celu przerwania rozlewu krwi – i uzasadnienia interwencji NATO – w Libii, po upadku reżimu Muhammara al-Kaddafiego wspólnota międzynarodowa wykazała, że doktryna jest czymś więcej niż tylko retoryką. R2P powinna być narzędziem, do którego kraje mogą sięgać w tych przypadkach, kiedy trwa prawdziwy kryzys humanitarny, a ONZ lub inna międzynarodowa pomoc humanitarna zawodzi. Koncepcja R2P może pomóc w zapobieganiu →wojnom [t. 4] czy klęskom żywiołowym. Aby chronić integralność tej zasady, państwa muszą przeciwstawić się tym, którzy ją naruszają, jednak należy również uznać, że z samej swej natury R2P jest bardziej narzędziem politycznym.

Wojna rosyjsko-ukraińska udowodniła, jak kruchy jest współczesny pokój i jak szybko może rozpocząć się międzynarodowy konflikt zbrojny.

A. Eban, słynny izraelski minister spraw zagranicznych, powiedział kiedyś, że „prawo międzynarodowe – to prawo, którego przestępcy nie wykonują, a sprawiedliwi nie zmuszają ich go wykonywać". Niezaprzeczalne dowody zbrodni masowych w Syrii i agresja Rosji wobec Ukrainy wzmacniają przekonanie, że zbrodniarze nadal ignorują normy prawa międzynarodowego.

Olga Wasiuta, Sergiusz Wasiuta

G.J. Bass, *Freedom's Battle: The Origins of Humanitarian Intervention*, Alfred A. Knopf, New York 2008; A. Domagała, *Interwencja humanitarna w stosunkach międzynarodowych*, Wydawnictwo Branta, Bydgoszcz–Wrocław 2008; G. Evans, *The Responsibility to Protect: Ending Mass Atrocity Crimes Once and For All*, Brookings Institution Press, 2009; F. Francioni, Ch. Bakker, *Responsibility to Protect, Humanitarian Intervention and Human Rights: Lessons from Libya to Mali. The Transatlantic Relationship and the Future Global Governance*, „Working paper" 2013, no. 15; S.F. Gagro, *The Responsibility to Protect (R2P) Doctrine*, „International Journal of Social Sciences" 2014, no. 3 (1); S. De Geest, *Russian Intervention in Ukraine: R2P Limits and reclaiming the Concept and Narrative*, 11.04.2015, HSCentre.org (dostęp 19.02.2019); A. Hehir, *The Responsibility to Protect: Rhetoric, Reality and the Future of Humanitarian Intervention*, Palgrave Macmillan, Basingstoke 2012; Human Rights Watch, *Statement: Possible Intervention Syria, Human Rights Watch*, 28.08.2013, HRW.org (dostęp 15.02.2019); International Commission on Intervention and State Sovereignty *The Responsibility to Protect*, International Development Research Centre (Canada), Ottawa 2001; M. Kersten, *Does Russia have a „Responsibility to Protect" Ukraine? Don't buy it*, 4.03.2014, TheGlobeAndMail.com (dostęp 19.02.2019); A.S. Kolb, *The UN Security Council Members' Responsibility to Protect: A Legal Analysis*, Springer, New York 2017; D. Kuwali, *The Responsibility to Protect: Implementation of Article 4(h). Intervention*, Martinus Nijhoff Publishers, Leiden–Boston 2011; D. Kuwali, F. Viljoen, *Africa and the Responsibility to Protect: Article 4(h) of the African Union Constitutive Act*, Routledge, New York 2013; M. Martin, M. Kaldor, *The European Union and Human Security: External Interventions and Missions*, Routledge, London 2010; J. Pattison, *Humanitarian Intervention and Responsibility to Protect. Who Should Intervene*? Oxford University Press, Oxford 2012; *Responsibility to Protect. The Global Moral Compact for the 21st Century*, R.H. Cooper, J.V. Kohler (eds.), Palgrave Macmillan, London 2008; Rezolucja RB ONZ nr 1970 z 26 lutego 1970 roku; Rezolucja RB ONZ nr 2127 z 5 grudnia 2013 roku; N. Tsagourias, *Russia, Georgia and the Responsibility to Protect*, „Amsterdam Law Forum" 2019, vol. 1; C.B. Walling, *All the Necessary Measures: The United Nations and Humanitarian Intervention*, University

of Pennsylvania Press, Philadelphia 2013; O. Wasiuta, *Doktryna odpowiedzialności za ochronę*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Doktryna „Responsibility to protect" w praktyce politycznej Rosji*, „Przegląd Geopolityczny" 2019, nr 29; J. Welsh, *Implementing the „Responsibility To Protect"*, „Policy Brief" 2009, no. 1; I. Wrońska, *Zasada odpowiedzialności za ochronę w stosunkach międzynarodowych a działania NATO: uwagi na tle współczesnej koncepcji ochrony praw człowieka*, „Ante Portas. Studia nad Bezpieczeństwem" 2014, nr 1 (3).

DOKTRYNY (KONCEPCJE) OPERACYJNE – zespół poglądów dotyczących przygotowania poszczególnych rodzajów sił zbrojnych do konfrontacji militarnej z potencjalnym przeciwnikiem na określonym obszarze geograficznym. Pojęcie doktryn operacyjnych jest pojęciem węższym niż →doktryna wojskowa i doktryna wojenna. Jak podkreślił J. Solarz w książce *Doktryny militarne w XX wieku*, doktryną militarną będzie sposób przygotowania obrony kraju w sytuacji →zagrożenia [t. 4] zewnętrznego oraz prowadzenie działań wojennych z zastosowaniem metod i środków będących w dyspozycji państwa lub koalicji państw. Doktryną wojenną będzie z kolei zbiór poglądów i idei związanych z przygotowaniem i prowadzeniem →wojny [t. 4] jako całości, z uwzględnieniem takich czynników jak ustrój państwa, sytuacja polityczna (wewnętrzna i międzynarodowa), zasoby kraju, potencjał gospodarczy, poziom naukowo-techniczny, doświadczenia prowadzenia wojny i położenie geograficzne. Doktryny operacyjne zostają opracowane w praktyce przez wyspecjalizowane organy wojska lub organizacje pozarządowe (think tanki zajmujące się naukami strategicznymi lub →naukami o bezpieczeństwie [t. 3]), a następnie, po akceptacji na najwyższych szczeblach dowódczych sił zbrojnych, zostają przedstawione w oficjalnych dokumentach strategicznych lub podręcznikach polowych jako obowiązujące. Przykładem doktryn operacyjnych były 4 koncepcje, jakie pojawiły się w ciągu ostatnich kilkudziesięciu lat w siłach zbrojnych USA:

- koncepcja bitwy powietrzno-lądowej (AirLand Battle, ALB);
- koncepcja bitwy powietrzno-morskiej (AirSea Battle, ASB);
- koncepcja bitwy wielodomenowej (Multi-Domain Battle, MDB);
- koncepcja operacji wieloobszarowej (Multi-Domain Operation, MDO).

Doktryna bitwy powietrzno-lądowej została opracowana w latach 70. XX w. na potrzeby ewentualnej konfrontacji wojsk → NATO [t. 3] z wojskami Układu Warszawskiego na nizinach Europy Środkowej. Pierwszym dokumentem, w którym przedstawione zostały zasady ALB, była broszurka zatytułowana *The AirLand Battle and Corps 86, TRADOC Pamphlet 525-5* z 1981 r. W 1982 r. doktryna ta została opisana w podręczniku polowym *Field Mannual (FM) 100-5 Operations*. Przed pojawieniem się koncepcji bitwy powietrzno-lądowej, w 1976 r., w armii USA została opracowana doktryna aktywnej obrony. Była ona jedną z pierwszych propozycji zmiany doktryny militarnej po tzw. traumie wietnamskiej. Opierała się na doświadczeniach izraelskich wojny Jom Kippur w 1973 r. Zakładała ona „pogłębienie" pola walki, uderzenie na pierwszy rzut armii przeciwnika oraz niszczenie jego kolejnych rzutów za pomocą najnowocześniejszej broni. Jako przykład prowadzenia → bitwy [t. 1] z użyciem metod aktywnej obrony podawane było starcie izraelskich i syryjskich wojsk pod Al-Kunajtirą (Quneitra) w czasie wojny Jom Kippur. 6 października 1973 r. izraelska 7 Brygada Pancerna wyposażona w 100 czołgów stawiła czoło przeważającym siłom wroga i utraciła w ciągu 4 dni większość własnego sprzętu wojskowego. Pomimo strat → żołnierze [t. 4] 7 Brygady, wykorzystując kilkanaście naprawionych czołgów, przypuścili kontratak na pozycje syryjskie, zmuszając syryjskie wojska do odwrotu. Heroiczna postawa żołnierzy 7 Brygady umożliwiła wzmocnienie izraelskich sił na południu i przeprowadzenie przez dywizje gen. Lanera i Peleda 2 głębokich manewrów oskrzydlających. Był to kluczowy moment wojny Jom Kippur na odcinku syryjskim, który uświadomił obserwatorom, jak skuteczne mogą być działania opóźniające oraz niszczące, głęboko w regionie działań przeciwnika, prowadzone za pomocą → wojsk lądowych [t. 4] i sił powietrznych.

Sama koncepcja ALB została opisana w książce *Wojna i antywojna* autorstwa A. i H. Tofflerów. Zdaniem autorów, zgodnie z teorią 3 fal rozwoju cywilizacyjnego (agrarną, przemysłową i informacyjną), jest ona krokiem w kierunku transformacji sił zbrojnych USA z instytucji typu drugiej fali (masowej, zbiurokratyzowanej, hierarchicznego porządku) w kierunku instytucji trzeciej fali (nasyconej nowymi technologiami, elastycznej, sieciowej). Koncepcja ALB zakładała prowadzenie „głębokiej

bitwy", „rozszerzonego pola walki", „izolację pola walki" tak, aby zapobiec posuwaniu się wojska przeciwnika naprzód, zapewnić dostawy zaopatrzenia, dopływ → i n f o r m a c j i oraz umożliwić uderzenia oskrzydlające na przeciwnika i walkę na jego tyłach.

Za opracowaniem nowej koncepcji operacyjnej przemawiał również potencjał sił zbrojnych państw Układu Warszawskiego. Dowództwo armii USA zdawało sobie sprawę, iż NATO nie posiada przewagi ilościowej w jednostkach sprzętu wojskowego i ilości dywizji. Ponadto w latach 50. XX w. w Armii Radzieckiej pojawiły się nowe koncepcje operacyjne, przygotowujące tę armię do starcia konwencjonalnego z wojskami NATO w Europie. Jedną z nich była koncepcja Operacyjnych Grup Manewrowych (OGM), tj. jednostek składających się z 2 dywizji czołgów i 4 dywizji zmechanizowanych, przygotowanych do prowadzenia głębokich operacji na terytorium przeciwnika. Prowadzenie przez NATO walki przeciwko przeważającym siłom przeciwnika nie byłoby możliwe bez nowoczesnego uzbrojenia. Dlatego równolegle do zmian w obszarze teorii i doktryn militarnych na przełomie lat 70. i 80. XX w. pojawił się w armii USA szereg jednostek nowego sprzętu wojskowego, określanych jako tzw. wielka piątka – czołgi M1 Abrams, śmigłowce Apache, wozy bojowe Bradley, wieloprowadnicowe wyrzutnie pocisków rakietowych MRLS i samochody HMMWV (wielozadaniowe pojazdy kołowe).

Mimo że doktryna bitwy powietrzno-lądowej została opracowana na przełomie lat 70. i 80. XX wieku na potrzeby ewentualnej konfrontacji wojsk NATO z wojskami Układu Warszawskiego, jej założenia można nadal obserwować we współczesnych konfliktach zbrojnych. Jak zauważył M. Gawęda na łamach Defence24.pl, połączone operacje powietrzno-lądowe w duchu ALB prowadziła Rosja w Syrii w 2015 i 2016 r. Polegały one m.in. na współpracy niewielkich oddziałów komandosów z lotnictwem w celu naprowadzenia samolotów na cel, oceny skali zniszczenia, odparcia ataku sił przeciwnika, rażenia przeciwnika na całej głębokości (linia frontu, bliskie zaplecze, dalekie tyły). Przez lata armia rosyjska z powodu „luki technologicznej" w stosunku do państw zachodnich nie była w stanie prowadzić tego typu operacji. Wyposażenie wojska w systemy transmisji danych KRUS Strielec oraz pojawienie się w arsenale rosyjskiej armii bezzałogowych statków latających znacznie zwiększyło

jej możliwości. Skalę i efekty prowadzenia operacji bazującej na zasadach bitwy powietrzno-lądowej przedstawił pod koniec 2017 r. były dowódca wojsk rosyjskich w Syrii gen. S. Surowikin. Jego zdaniem w ciągu 227 dni zlikwidowano ponad 32 tys. terrorystów, zniszczono 394 czołgi oraz wyzwolono spod władzy → Państwa Islamskiego [t. 3] 67 tys. km^2 powierzchni Syrii.

Kolejna doktryna operacyjna, koncepcja bitwy powietrzno-morskiej, powstała w 2010 r. Wpływowy amerykański think tank Center for Strategic and Budgetary Assessments opublikował wówczas 2 raporty: *Why Air-Sea Battle?* oraz *Air-Sea Battle, a Point of Departure Operational Concept*. W 2012 r. z kolei ukazał się dokument Pentagonu *Joint Operational Access Concept* (JOAC), w którym opisane zostały założenia systemu Anti Access/Area Denial (A2/AD) i koncepcja bitwy powietrzno-morskiej. Obserwując rosnące zdolności Chin w izolowaniu pola walki na zachodnim Pacyfiku, pracownicy Center for Strategic and Budgetary Assessments zaproponowali przyjęcie przez Departament Obrony USA nowej koncepcji operacyjnej, przygotowującej amerykańskie siły zbrojne do konfrontacji militarnej z Chińską Armią Ludowo-Wyzwoleńczą (PLA). O ile w przypadku koncepcji bitwy powietrzno-lądowej miejscem konfrontacji miały być niziny Europy Środkowej, w przypadku koncepcji bitwy powietrzno-morskiej miałby to być zachodni Pacyfik. Głównymi obszarami konfrontacji byłyby morza, powietrze, ale także kosmos i → cyberprzestrzeń [t. 1]. Koncepcja zakłada konieczność obrony amerykańskich sojuszników – Japonii i Korei Południowej – oraz utrzymanie kontroli nad szlakami handlowymi, takimi jak Cieśnina Malakka. Zdaniem autorów dokumentów jednym z pierwszych posunięć strony chińskiej w czasie konfrontacji będzie użycie broni antysatelitarnej i cybernetycznej. W przypadku użycia broni cybernetycznej celem ataku będą amerykańskie systemy C2, radary znajdujące się na zachodnim Pacyfiku, jak również wszystkie naziemne i powietrzne obiekty tworzące obraz świadomości sytuacyjnej. Inną formą ataku będą rakiety mające na celu zniszczenie tzw. sanktuariów, czyli stałych lub rotacyjnych baz amerykańskich na zachodnim Pacyfiku. Do niedawna szereg baz amerykańskich znajdował się poza zasięgiem chińskich samolotów i pocisków balistycznych, jednak obecnie nawet jedna z największych baz amerykańskich na wyspie

Guam nie jest bezpieczna, jako że pociski typu DF-11, DF-15, DF-21 czy DF-4 osiągają dystans od kilkuset do 2500 mil morskich. Szczególnym zagrożeniem dla strony amerykańskiej jest rakieta balistyczna DF-21D, nazywana „zabójcą lotniskowców". DF-21D znacząco zmienia potencjał militarny obu stron w tym obszarze geograficznym, ponieważ naraża na zniszczenie lotniskowce już w pierwszej fazie konfliktu. Atutem po stronie USA jest z kolei dominacja w ilości okrętów podwodnych. Poza tym, jak podkreślają autorzy koncepcji, armia USA w pierwszych dniach bitwy powietrzno-morskiej skupi się na „oślepieniu" dowództw chińskiej armii w ramach „nowoczesnej bitwy zwiadowczej", niszcząc satelity oraz radary przeciwnika. Następnie, po zwycięskim starciu lotniczym nad Japonią, skupi się na eliminacji potencjału chińskiej floty, aby później przystąpić do blokady morskiej Państwa Środka.

W 2017 r. została przedstawiona kolejna koncepcja – →bitwa wieloobszarowa [t. 1] (Multi-Domain Battle). Jej założenia zostały opisane w dokumencie *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040* wydanym przez U.S. Army Training and Doctrine Command (TRADOC). Jak podkreślił były dowódca TRADOC gen. D. Perkins, konieczność opracowania doktryny bitwy wielodomenowej wynikała z kilku przyczyn. Po pierwsze, w przeciwieństwie do czasów →zimnej wojny [t. 4] i obowiązującej wówczas koncepcji bitwy powietrzno-lądowej, armia USA musi być przygotowana do konfrontacji nie z jednym, ale z kilkoma rodzajami przeciwników: mocarstwami międzynarodowymi, państwami upadłymi, ugrupowaniami terrorystycznymi itp. Po drugie, w latach 90. XX w. żaden z przeciwników nie był w stanie zagrozić USA w ani jednym obszarze (domenie) prowadzenia działań zbrojnych – na lądzie, w powietrzu, na morzu, w przestrzeni kosmicznej czy cyberprzestrzeni. USA posiadały wówczas niekwestionowaną przewagę w siłach powietrznych i →marynarce wojennej [t. 3]. Jedynym kwestionowanym obszarem dominacji Ameryki był ląd, gdzie za pomocą asymetrycznych metod prowadzenia walki nawet słabszy przeciwnik mógł zadać wojskom konwencjonalnym duże straty. Obecnie, biorąc pod uwagę zdolności chińskie na zachodnim Pacyfiku oraz możliwości armii rosyjskiej w wojnie na Ukrainie i wojnie w Syrii, należy się spodziewać, iż w przyszłych konfliktach zbrojnych dominacja amerykańska będzie

kwestionowana na wszystkich obszarach (domenach). Po trzecie, Stany Zjednoczone, aby wciąż posiadać status globalnego mocarstwa, muszą utrzymywać siły zbrojne w różnych odległych od siebie miejscach świata, narażając je tym samym w czasie ewentualnego konfliktu na odcięcie linii zaopatrzeniowych. Skutkuje to koniecznością przygotowania sił do operowania w warunkach dużej samodzielności, wystarczalności i zdolności prowadzenia operacji na wszystkich obszarach (domenach). Bitwa wielodomenowa zakłada tym samym powstanie nowych oddziałów, nazywanych oddziałami ICEW (ang. *intelligence, cyberwarfare and electronic warfare*), zdolnych prowadzić operacje w kilku obszarach jednocześnie. Na większą samodzielność wojska będą miały wpływ również nowe technologie medyczne, umożliwiające pomoc rannym na polu walki czy zastosowanie nowych części zamiennych do sprzętu wojskowego.

Najnowszą doktryną operacyjną rozwijaną w siłach zbrojnych USA jest koncepcja operacji wieloobszarowej. Jak podkreślił gen. E. Wesley, dyrektor U.S. Army Capabilities Integration Center (ARCIC), koncepcja operacji wieloobszarowej jest rozbudowaną wersją MDB. Zawiera o wiele więcej szczegółów opisujących to, jak powinny być prowadzone operacje w wielu domenach, weryfikowana jest ona także w cyklicznych ćwiczeniach wojskowych odbywających się w różnych miejscach na świecie, takich jak Joint Warfighting Assessment 18 w Niemczech czy Joint Warfighting Assessment 19 na Pacyfiku. TRADOC definiuje MDO jako metodę, za pomocą której siły zbrojne USA, będące częścią sił sojuszniczych, mogą powstrzymać i pokonać przeciwnika posiadającego zdolności kwestionujące dominację amerykańską we wszystkich obszarach (domenach) prowadzenia walki zbrojnej. Podobnie jak MBD, MDO wskazuje jako potencjalnego przeciwnika siły zbrojne Federacji Rosyjskiej i Chińskiej Republiki Ludowej oraz innych państw rozwijających zdolności antydostępowe (→ a n t y d o s t ę p o w e z d o l n o ś c i [t. 1]) (Iran, Korea Północna). Szczegóły koncepcji operacji wieloobszarowej przedstawione zostały w dokumencie TRADOC *The U.S. Army in Multi-Domain Operations 2028,* który ukazał się w 2018 r. Zdaniem autorów w przyszłości wojny prowadzone będą przez niewielkie siły zbrojne na dużych przestrzeniach. Ponadto, biorąc pod uwagę postępujące procesy urbanizacyjne, walka będzie się odbywać w terenie miejskim, gdzie przeciwnicy USA będą starali

się wykorzystać otoczenie do zminimalizowania przewagi amerykańskiej. Koncepcja dzieli aktywność wojskową na okres rywalizacji, okres walki zbrojnej oraz powrót do rywalizacji po zakończeniu konfliktu. W okresie rywalizacji podejmowane są działania dyplomatyczne i ekonomiczne, prowadzona jest →wojna informacyjna [t. 4] i działania nieregularne. Bardzo trudno jest określić, kiedy rywalizacja przechodzi w okres wojny, ponieważ →agresja [t. 1] ma charakter podprogowy (poniżej progu wojny). Walka zbrojna charakteryzuje się prowadzeniem operacji we wszystkich 5 domenach (lądowej, powietrznej, morskiej, kosmicznej i cyberprzestrzeni) na 7 obszarach:

- na strategicznym obszarze wsparcia położonym powyżej 5 tys. km poza miejscem prowadzonych walk,
- na operacyjnym obszarze wsparcia położonym powyżej 1,5 tys. km od miejsca prowadzonych walk,
- na taktycznym obszarze wsparcia położonym powyżej 500 km od miejsca prowadzonych walk,
- na bliskim obszarze i głębokim obszarze manewru położonym do 200 km od miejsca prowadzonych walk, zarówno w kierunku terytorium sojusznika, jak i wroga,
- na operacyjnym głębokim obszarze prowadzenia walk,
- na strategicznym głębokim obszarze prowadzenia walk położonych powyżej 500 km i 1 tys. km na terenie przeciwnika.

Zadaniem sił zbrojnych jest przełamanie zdolności antydostępowych wroga, uzyskanie swobody manewru, pokonanie jego sił zbrojnych, a następnie powrót do okresu rywalizacji.

Tomasz Wójtowicz

J. Bartosiak, *Pacyfik i Euroazja. O wojnie*, Jacek Bartosiak, Warszawa 2016; M. Gawęda, *Bitwa powietrzno-lądowa po rosyjsku. Przykład Syrii*, 11.02.2018, Defence24.pl (dostęp 22.12.2019); J. Judson, *From Multi-Domain Battle to Multi-Domain Operations: Army evolves its guiding concept*, 9.10.2018, DefenseNews.com (dostęp 20.12.2019); Ł. Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009; A.F. Krepinevich, *Why Air-Sea Battle?*, Center for Strategic and Budgetary Assessments, Washington 2010; A.H. Toffler, *Wojna*

i antywojna. Jak przetrwać na progu XXI wieku, Wydawnictwo Kurpisz S.A., Poznań 2006; J. van Tol, M. Gunzinger, A. Krepinevich, J. Thomas, *AirSea Battle. A Point-of-Departure Operational Concept*, Center for Strategic and Budgetary Assessments, Washington 2010; United States Army Training and Doctrine Command, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040*, United States Army Training and Doctrine Command, 2017; ciż, *The U.S. Army in Multi-Domain Operations 2028*, United States Army Training and Doctrine Command, 2018; U.S. Army Training and Doctrine Command's Joint Modernization Command, *Joint Warfighting Assessment 18*, 24.04.2018, Army.mil (dostęp 22.12.2019); K. Weinberger, *Russian Anti-Access and Area Denial*, 29.08.2016, UnderstandingWar.org (dostęp 22.12.2019); T. Wójtowicz, *Doktryny operacyjne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

DOKTRYNY OBRONNE RP – zbiór poglądów na →zagrożenie militarne [t. 4] kraju oraz zasad i wytycznych dotyczących przygotowania państwa, sił zbrojnych i społeczeństwa do prowadzenia →wojny [t. 4], wyrażających się w konkretnych przedsięwzięciach o charakterze militarnym i pozamilitarnym, realizowanych w czasie pokoju i ewentualnej wojny. Analizując doktryny obronne, należy jasno zaznaczyć, iż termin ten w polskich realiach zadomowił się na dobre po 1989 r., wcześniej, w czasach PRL, wydawano (głównie przez Sztab Generalny Wojska Polskiego, SGWP) dokumenty doktrynalne odnoszące się do powyższych zagadnień, lecz określano je częściej mianem doktryn wojennych. Owe doktryny we wspomnianym okresie były pod względem polityczno-ideologicznym tożsame z doktryną Układu Warszawskiego. Od 1967 r. wiele elementów doktryny wojennej można było odczytać z ustawy o powszechnym obowiązku obrony Polskiej Rzeczypospolitej Ludowej, będącej swoistą konstytucją obronności. W latach 60. XX w. ukształtowała się koncepcja organizacji systemu obronnego państwa na podstawie 3 układów:

- militarny (WP),
- funkcjonalny (resorty cywilne pogrupowane w szereg działów, np. polityczny, planowania i ekonomiki, →ochrony ludności [t. 3], komunikacji itp.),
- terytorialny (odpowiedniki działów układu funkcjonalnego na szczeblu województwa i powiatu).

Taka doktryna obronna (wojenna) z pewnymi modyfikacjami przetrwała aż do 1990 r. Zmiany polityczno-społeczne, które dokonały się w Polsce po 1989 r., niejako wymusiły nowe podejście do obronności państwa. Głównym wyzwaniem w pierwszej fazie było zerwanie z mentalnością „operatora", czyli wykonawcy zadań strategicznych przychodzących z zewnątrz, i zainicjowanie kreatywnej narodowej →kultury strategicznej, opartej na identyfikacji i uwzględnianiu własnych →interesów narodowych. Tak zrodziła się pierwsza doktryna obronna RP z 1990 r. Jak przyjęto w uchwale Komitetu Obrony Kraju (KOK), doktryna wytyczała generalne kierunki polityki obronnej obowiązujące organy państwowe, podmioty gospodarcze, organizacje społeczne i zawodowe oraz każdego obywatela. W myśl przedmiotowej doktryny polityka obronna została zdefiniowana jako podejmowanie działań na rzecz zapewnienia →bezpieczeństwa militarnego [t. 1] przy użyciu wszelkich dostępnych środków. System obrony państwa obejmował dziedzinę polityczno-społeczną, administracyjno-gospodarczą, militarną, ochrony państwa oraz →obronę cywilną [t. 3]. Treść doktryny utożsamiała →bezpieczeństwo narodowe [t. 1] z dziedziną obronną, a wspomniany i użyty w zapisach doktryny system obrony państwa stanowił główne narzędzie zapewnienia bezpieczeństwa narodowego. Nie należy się dziwić takiemu podejściu, biorąc pod uwagę istnienie jeszcze w tamtym okresie Układu Warszawskiego, RWPG, ZSRR i stacjonowania w Polsce Armii Radzieckiej. Kolejny dokument tego rodzaju pod nazwą Polityki Bezpieczeństwa i Strategii Obronnej RP został przyjęty w 1992 r. Co do podstawowych założeń nie różnił on się zbytnio od przyjętego 2 lata wcześniej. Nadal dominującą rolę w →systemie bezpieczeństwa narodowego [t. 4] odgrywał system obrony państwa, do tego stopnia, iż nawet kwestie ochrony ludności przed →katastrofami naturalnymi czy przemysłowymi przypisano podmiotom określonym jako pozamilitarne ogniwa obronne. Na kolejne tego typu opracowanie czekano 8 lat. W 2000 r. w ślad za przyjętą Strategią Bezpieczeństwa RP utworzono Strategię Obronności RP. Dokument ten nie okazał się rewolucyjny czy przełomowy. Warto jednak podkreślić, że dostrzeżono w nim →zagrożenia [t. 4] pozamilitarne, w reagowaniu na które państwo byłoby zmuszone zaangażować swój potencjał obronny. Kolejny tego typu dokument

ujrzał światło dzienne w 2009 r., czyli 2 lata po ukazaniu się → strategii bezpieczeństwa narodowego [t. 4]. Strategia Obronności RP, bo taki tytuł otrzymało to opracowanie, była niczym innym jak → strategią [t. 4] sektorową do tej pierwszej. W dokumencie obronność zdefiniowano jako dziedzinę bezpieczeństwa narodowego, stanowiącą sumę wszystkich cywilnych i wojskowych przedsięwzięć, mających na celu zapobieganie i przeciwstawianie się wszelkim potencjalnym → zagrożeniom bezpieczeństwa [t. 4] państwa, zarówno militarnym, jak i pozamilitarnym, mogącym doprowadzić do → kryzysu polityczno-militarnego. Innymi słowy, aby zapewnić zdolność do obrony, powinno się wykorzystywać wszystkie możliwe środki i podporządkować jej działania polityczne, gospodarcze, dyplomatyczne i wojskowe.

Z dokumentów doktrynalnych, a zwłaszcza tych z XXI w., wyłania się obraz → obrony narodowej [t. 3] jako jednego z podstawowych, elementarnych ogniw bezpieczeństwa narodowego, którą należy rozpatrywać o wiele szerzej aniżeli w aspekcie czysto militarnym.

Łukasz Szewczyk

W. Kitler, *Bezpieczeństwo Narodowe. Podstawowe kategorie. Uwarunkowania. System*, AON, Warszawa 2011; *Strategia Obronna RP*, MON, Warszawa 2000; *Strategia Obronności Rzeczypospolitej Polskiej*, Warszawa 2009; Uchwała Komitetu Obrony Kraju z dnia 21 lutego 1990 r. w sprawie doktryny obronnej Rzeczypospolitej Polskiej, M.P. 1990 nr 9, poz. 66; J. Wojnarowski, *System obronności państwa*, AON, Warszawa 2005; Z. Wilk-Woś, P. Kornacki, *Bezpieczeństwo i zarządzanie kryzysowe – bezpieczeństwo i obronność państwa*, Wydawnictwo Społecznej Akademii Nauk, Warszawa–Łódź 2016.

DOKUMENT Z MONTREUX (dokument z Montreux w sprawie istotnych międzynarodowych zobowiązań prawnych i dobrych praktyk państw związanych z operacjami prywatnych firm wojskowych i ochroniarskich w trakcie konfliktu zbrojnego z dnia 17 września 2008 r.) – pierwszy dokument o znaczeniu międzynarodowym, który określa, w jaki sposób prawo międzynarodowe stosuje się do działalności prywatnych firm wojskowych i ochroniarskich (ang. *private military and security companies*, PMSC), gdy działają one w strefie konfliktu zbrojnego. Przepisy zawarte w dokumencie

określają również obowiązki prawne spoczywające na samych prywatnych firmach ochroniarskich.

Dokument z Montreux jest wynikiem inicjatywy podjętej wspólnie przez Szwajcarię i Międzynarodowy Komitet Czerwonego Krzyża przy udziale ekspertów rządowych m.in. z Afganistanu, Angoli, Australii, Austrii, Kanady, Chin, Francji, Niemiec, Iraku, Polski, Szwajcarii, Wielkiej Brytanii, Ukrainy i USA. Prace prowadzone w latach 2006–2007 zaowocowały sformułowaniem treści tzw. dokumentu z Montreux. Opracowano go na podstawie wyników 4 spotkań międzyrządowych:

- Federalny Departament Spraw Zagranicznych – departament odpowiadający za prowadzenie polityki zagranicznej Szwajcarii – zorganizował pierwsze spotkanie rozpoznawcze w Zurychu w dniach 16–17 stycznia 2006 r., na którym zgromadzili się eksperci rządowi oraz przedstawiciele branż związanych z sektorem → bezpieczeństwa [t. 1], a także przedstawiciele organizacji działających na rzecz → społeczeństwa obywatelskiego [t. 4];
- drugie spotkanie o podobnej tematyce odbyło się w Montreux w dniach 13–14 listopada 2006 r. i zostało poświęcone omówieniu dobrych praktyk, które powinny być stosowane przez państwa: zawierające umowy z PMSC, na których terytorium działają PMSC oraz których obywatele działają w PMSC;
- trzecie spotkanie w dniach 14–16 kwietnia 2008 r. posłużyło konsolidacji opinii szerszego kręgu ekspertów rządowych, przedstawicieli organizacji działających na rzecz → praw człowieka [t. 3] i przedstawicieli branży na temat pierwszego projektu. Na podstawie tych dyskusji projekt został zmieniony i przekazany uczestniczącym w spotkaniach rządom do ostatecznych konsultacji;
- na czwartym (i końcowym) spotkaniu w sprawie inicjatywy w dniach 15–17 września 2008 r. prace nad dokumentem zostały sfinalizowane, a rządy uczestniczące przyjęły go w drodze konsensusu.

W październiku 2008 r. Stały Przedstawiciel Szwajcarii przy Organizacji Narodów Zjednoczonych przedstawił dokument Montreux Zgromadzeniu Ogólnemu i Radzie Bezpieczeństwa ONZ. Dokument

i towarzyszący mu list zostały przetłumaczone na 6 oficjalnych języków ONZ: angielski, arabski, chiński, francuski, hiszpański i rosyjski.

Dokument z Montreux określa obowiązki 3 głównych typów państw: 1. państw, które zatrudniają PMSC; 2. państw, na terytorium których działają PMSC, oraz 3. państw, w których zlokalizowane są siedziby PMSC. Chociaż dokument jest skierowany przede wszystkim do państw, dobre praktyki mogą być przydatne dla innych podmiotów, takich jak organizacje międzynarodowe, organizacje społeczne, firmy, które zawierają umowy z PMSC i same PMSC.

Przed przyjęciem dokumentu z Montreux panowało błędne przekonanie, że PMSC działają w próżni prawnej, albowiem nie można stosować względem nich reguł prawa międzynarodowego. Dokument ma praktyczne, realne znaczenie dla promowania poszanowania międzynarodowego prawa humanitarnego (MPH) i międzynarodowego prawa dotyczącego praw człowieka, a także zapewnia rządom plan skutecznego regulowania funkcjonowania PMSC. Zawiera on listę rekomendacji oraz dobrych praktyk, które państwa ratyfikujące dokument powinny implementować do swojego porządku prawnego. Do najważniejszych można zaliczyć następujące zasady:

- ugruntowane zasady prawa międzynarodowego mają zastosowanie do państw w ich relacjach z prywatnymi firmami wojskowymi i ochroniarskimi (PMSC);
- dokument zawiera katalog dobrych praktyk w zakresie promowania zgodności z MPH i prawami człowieka podczas konfliktu zbrojnego, które powinny być stosowane przez wszystkie państwa;
- dokument nie jest prawnie wiążącym instrumentem i nie wpływa na istniejące zobowiązania państw wynikające ze zwyczajowego prawa międzynarodowego lub umów międzynarodowych, których są stronami, w szczególności ich zobowiązania wynikające z Karty Narodów Zjednoczonych.

Dokument akcentuje obowiązki państw wynikające z prawa międzynarodowego, w szczególności MPH i międzynarodowego prawa dotyczącego praw człowieka, odnoszące się do działalności prywatnych firm wojskowych i ochroniarskich (PMSC) w sytuacjach konfliktu zbrojnego. Katalog dobrych praktyk i opcji regulacyjnych ma stanowić zbiór

praktycznych narzędzi, gotowych do zastosowania przez poszczególne państwa. Sprecyzowanie zagadnień dotychczas nieuregulowanych posłuży promowaniu poszanowania międzynarodowego prawa humanitarnego przez PMSC. Do chwili obecnej 54 państwa i 3 organizacje międzynarodowe poparły dokument z Montreux. Dokument zawiera 27 „oświadczeń" – fragmentów poświęconych różnym tematom, stanowiących przypomnienie głównych międzynarodowych zobowiązań prawnych państw w odniesieniu do operacji PMSC podczas konfliktów zbrojnych. Każde oświadczenie jest potwierdzeniem ogólnej zasady MPH, prawa międzynarodowego dotyczącego praw człowieka lub odpowiedzialności państwa, sformułowanym w sposób wyjaśniający ich zastosowanie w operacjach PMSC. Chociaż dokument został opracowany z myślą o tym, że PMSC działają w sytuacjach konfliktu zbrojnego, będzie mieć również znaczenie w sytuacjach pokonfliktowych i innych porównywalnych z konfliktem zbrojnym.

Dokument został podzielony na 2 części: 1. istotne międzynarodowe zobowiązania prawne dotyczące PMSC i 2. dobre praktyki dotyczące PMSC.

W pierwszej części przedstawiono obowiązki różnych podmiotów wynikające z międzynarodowego prawa humanitarnego i prawa międzynarodowego dotyczącego praw człowieka, przypomniane zostały również istotne zobowiązania prawne państw dotyczące PMSC. Obowiązki PMSC i ich personelu oraz odpowiedzialność przełożonych są również omówione w części pierwszej.

W drugiej części przedstawiono ok. 70 „najlepszych praktyk", które mają na celu zapewnienie wskazówek i pomocy państwom w regulowaniu działalności PMSC. Dobre praktyki służą ustaleniu, jakie usługi mogą być zlecane PMSC, a które wymagają odpowiedniego szkolenia, ustalania warunków udzielania licencji oraz przyjmowania środków w celu poprawy nadzoru, przejrzystości i rozliczalności PMSC.

We współczesnych konfliktach zbrojnych udział prywatnych firm wojskowych stał się coraz powszechniejszy. Początków nowożytnego najemnictwa należy szukać w okresie po II wojnie światowej. Wówczas setki byłych → ż o ł n i e r z y [t. 4] próbowały szczęścia, walcząc w różnych wojnach w Afryce. W późniejszym czasie, obok klasycznych najemników,

zaczęły działać coraz liczniejsze prywatne firmy ochroniarskie, których status w świetle prawa międzynarodowego był niejasny. Przełomowym wydarzeniem dla rozwoju tego rodzaju przedsięwzięć był konflikt w Iraku. Amerykańscy przywódcy liczyli na to, że uda im się przeprowadzić wojnę nowego typu, posługując się w tym celu znaczną liczbą prywatnych firm, które miały przejąć klasyczne zadania wojskowe takie jak → w y w i a d [t. 4] czy logistyka. Najbardziej znanym podmiotem prywatnym spośród działających w Iraku była Blackwater USA, występująca także pod nazwami Blackwater Worldwide, Xe Services LLC, obecnie Academi. Choć brak oficjalnych danych, szacuje się, że w samym Iraku działały tysiące najemników i rynek ich usług jest wyceniany w miliardach dolarów. Jednak rozwój rynku usług tego rodzaju, choć postrzegany pozytywnie przez państwa, rządy i samych przedsiębiorców, przyniósł szereg ważnych pytań dotyczących odpowiedzialności za działania w ramach konfliktu zbrojnego podmiotów niebędących państwami, których sytuacja nie została wprost uregulowana w aktach prawa międzynarodowego. Wątpliwości te stawały się obiektem zainteresowania → o p i n i i p u b l i c z n e j [t. 3] po każdym nagłośnionym przez media incydencie, a tylko sam konflikt iracki przyniósł ich wiele, by wymienić np. zabicie przez najemników 17 Irakijczyków w Bagdadzie, we wrześniu 2007 r. Wydarzenia te unaoczniły społeczności międzynarodowej, jak wielkie → z a g r o ż e n i e [t. 4] może wynikać z działania PMSC poza prawem lub na granicy prawa, i doprowadziły do szeregu inicjatyw mających na celu uregulowanie ich działalności.

Dokument z Montreux stanowi uzupełnienie projektu konwencji ONZ ws. PMSC (Draft International Convention On The Regulation, Oversight And Monitoring Of Private Military And Security Companies). Projekt konwencji proponuje wprowadzenie zakazu delegowania określonych uprawnień państw na podmioty prywatne, co ma dotyczyć w szczególności monopolu państwa na możliwość użycia siły w stosunkach międzynarodowych, którą należy rozumieć jako:

- bezpośredni udział w działaniach zbrojnych,
- prowadzenie wojny i operacji obejmujących walkę,
- branie jeńców,
- wywiad,
- transfer → i n f o r m a c j i wywiadowczych,

- użycie i działania powiązane z użyciem → broni masowego rażenia,
- działania o charakterze policyjnym, w tym aresztowanie, przetrzymywanie i przesłuchiwanie zatrzymanych (art. 2 ppkt. i) projektu konwencji).

Konwencja zakłada także, że każde państwo ponosi odpowiedzialność z tytułu działalności firm zarejestrowanych na terytorium danego państwa niezależnie od tego, czy dana firma działa na rzecz interesów tego państwa. Ponadto konwencja zakłada, że każde państwo powinno podjąć wszelkie konieczne kroki prawne w celu doprowadzenia do odpowiedzialności personelu takich firm z tytułu naruszenia prawa międzynarodowego lub krajowego.

W grudniu 2014 r. zostało utworzone Forum Dokumentu z Montreux (Montreux Document Forum) jako platforma, za pomocą której sygnatariusze i uczestnicy mogą dzielić się wskazówkami dot. dobrych praktyk w postępowaniu wobec PMSC i omawiać wyzwania dotyczące regulacji prywatnych firm wojskowych. Opracowano także uzupełniający globalny kodeks postępowania dla branży bezpieczeństwa.

Piotr Łubiński, Olga Wasiuta

S. Borelli, *Casting Light on the Legal Black Hole: International Law and Detentions Abroad in the War on Terror*, „International Review of the Red Cross" 2005, vol. 87; J. Cockayne, *Regulating Private Military and Security Companies: The Content, Negotiation, Weaknesses and Promise of the Montreux Document*, „Journal of Conflict and Security Law" 2008, vol. 13, iss. 3; P. Łubiński, *Status kombatanta, ochrona i uprawnienia jeńców wojennych i innych osób zatrzymanych,* [w:] *Międzynarodowe prawo humanitarne konfliktów zbrojnych. Materiał szkoleniowy dla oficerów*, Z. Falkowski (red.), Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014; M. Maxwell, M. Watts, *Unlawful Enemy Combatant: Status,Theory of Culpability, or Neither*?, „Journal of International Criminal Justice" 2007, vol. 5; D. Moeckli, *The US Supreme Court's 'enemy combatant' decisions: a 'major victory for the rule of law'?*, „Journal of Conflict and Security Law" 2005, vol. 10, iss. 1; *Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict: Montreux 17 September 2008*, „Journal of Conflict and Security Law" 2008, vol. 13, iss. 3; Report of the Working Group on the use of mercenaries

as a means of violating human rights and impeding the exercise of the right of peoples to self-determination (A/HRC/15/25), 2.07.2010; *The Montreux Document: On pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict*, International Committee of the Red Cross, 2009.

DOUBLESWITCH – nowa forma przejęcia kontroli nad kontami w portalach społecznościowych, wykorzystywana bardzo często w odniesieniu do kont w serwisie Twitter, ale możliwa do zastosowania także do kont na Facebooku i Instagramie. Jej specyfika polega na tym, że atak czyni standardowe mechanizmy odzyskiwania konta bezużytecznymi, co pozwala napastnikowi utrzymać kontrolę nad kontem ofiary przez dłuższy czas. Nowa forma ataku uwypukla nieprzewidziane luki w zasadach działania i funkcjach kont na Twitterze i w innych →mediach społecznościowych [t. 3], powinna stanowić ostrzeżenie dla osób korzystających z tych platform. Użytkownicy zagrożeni takimi atakami powinni stosować uwierzytelnianie wieloetapowe, aby w pierwszej kolejności zapobiec przejęciu kontroli nad kontem przez osoby niepowołane, zaś sam Twitter i platformy mediów społecznościowych z podobnymi funkcjami konta, takie jak Facebook i Instagram, powinny aktualizować swoje zabezpieczenia pod kątem ataków typu Doubleswitch.

Atak Doubleswitch polega na przejęciu konta w portalu społecznościowym w kilku krokach. Najbardziej narażeni na niego są użytkownicy, którzy nie włączyli dla swoich kont opcji uwierzytelniania wieloetapowego. Osoba atakująca może nakłonić użytkownika do ujawnienia hasła za pomocą →phishingu [t. 3]. Brak uwierzytelnienia wieloetapowego sprawia, że niewymagane jest kolejne działanie, by przejąć konto. Następnie możliwe staje się wysyłanie wiadomości, ale także subtelne zmienianie →informacji o koncie, w tym nazwy użytkownika. Oryginalna nazwa użytkownika dla tego konta staje się wówczas dostępna, co pozwala zainteresowanemu zarejestrować konto przy użyciu oryginalnej nazwy użytkownika, dysponując jednocześnie innymi danymi do logowania. Jeśli wówczas ofiara spróbuje odzyskać oryginalne konto poprzez zresetowanie hasła, wiadomość e-mail związana z tą procedurą zostanie wysłana bezpośrednio do atakującego. Taka forma przejmowania kont

ma poważne konsekwencje zwłaszcza w przypadku działaczy na rzecz →praw człowieka [t. 3], dziennikarzy lub osób, dla których ważna jest możliwość komunikowania się ze swoimi zwolennikami. Atakujący może wykorzystywać konto i wpływy swojej ofiary, a także niszczyć jej reputację. Niektóre ofiary ataku mogą nigdy nie odzyskać swojego konta, a nawet kiedy jest to możliwe, muszą poświęcić na to sporo czasu i wysiłku.

Znaczenie przejmowania kont społecznościowych przy wykorzystaniu techniki Doubleswitch wynika z faktu, że działacze polityczni, biznesmeni, dziennikarze i aktywiści na całym świecie wykorzystują platformy mediów społecznościowych, aby komunikować się z otoczeniem. Rządzący w represyjnych →reżimach [t. 3] politycznych czy zwykli przeciwnicy lub konkurenci czynią konta społecznościowe takich osób celami ataku. Zdobywając kontrolę nad kontami społecznościowymi, mogą uniemożliwić lub utrudnić ofierze komunikację, zawstydzić jej zwolenników, a także wywołać niepewność i szerzyć →dezinformację. Efekty takich działań można złagodzić za pomocą zautomatyzowanych procesów odzyskiwania kont opracowywanych przez samą platformę mediów społecznościowych, przy użyciu takich narzędzi jak formularze online do zgłaszania nieprawidłowości. Ataki typu Doubleswitch ewoluują i są coraz trudniejsze do zastosowania. Są szczególnie popularne w Wenezueli, Bahrajnie i Mjanmie. Aktywiści działający na rzecz demokracji i praw człowieka, którzy próbują odzyskać swoje konta w mediach społecznościowych za pomocą standardowych procesów odzyskiwania kont, często przez wiele miesięcy pozostają zablokowani. Za sprawą omawianej formy przejęcia konta ofiary nie tylko tracą kontrolę nad kontami w mediach społecznościowych, ale także trudniej im je odzyskać, a w wielu przypadkach nigdy ich już nie odzyskują.

Infolinia Digital Security przedsiębiorstwa Access Now, która pomaga osobom prywatnym i firmom na całym świecie w zakresie →bezpieczeństwa w sieci [t. 1], zidentyfikowała tę nową formę ataku poprzez pracę wspierającą aktywistów w Wenezueli, gdy kraj przechodził okres głębokich niepokojów politycznych. W tym okresie obowiązywał dekret prezydenta zezwalający na nadzór i →cenzurę [t. 1] online. 9 stycznia 2017 r. infolinia Digital Security otrzymała prośbę o pomoc od znanej dziennikarki M. Socorro, która poinformowała, że jej konto na Twitterze zostało przejęte. Miesiąc później zgłoszony został drugi wniosek o pomoc

od M. Pizarro, obrońcy praw człowieka i członka parlamentu Wenezueli. Wówczas pracownicy Access Now – firmy, która regularnie zajmuje się odzyskiwaniem kont mediów społecznościowych dla swoich klientów działających na rzecz →społeczeństwa obywatelskiego [t. 4] – zorientowali się, że nowe ataki były inne. W każdym przypadku atakujący uzyskiwali dostęp do konta na Twitterze ofiary, przy czym nie jest jasne, w jaki sposób. Następnie atakujący aktualizowali informacje o koncie, zmieniając hasło i powiązany adres e-mail, w efekcie blokując dostęp legalnego użytkownika do konta. W pierwszym przypadku porywacze zmienili nazwę użytkownika kont z @MilagrosSocorro na @DESAMORTOOT, a konto @Miguel_Pizarro na @PizarroPSUV, a następnie na @BuscoAsao. Po uzyskaniu pełnej kontroli nad zaatakowanym kontem wykorzystano funkcję, która pozwala Twitterowi nadawać po raz kolejny nieużywane nazwy użytkowników. Po zmianach atakujący zarejestrowali konta na Twitterze przy użyciu oryginalnych nazw użytkowników, które były teraz swobodnie dostępne, i podłączali konta do nowego adresu e-mail. Byli wtedy w stanie podszyć się pod Socorro i Pizarro. Gdy ofiary próbowały odzyskać swoje konta, wiadomości e-mail z potwierdzeniem na Twitterze trafiły do atakujących, którzy udawali, że problem został rozwiązany. Następnie atakujący usunęli jedno z oryginalnych kont, co jeszcze bardziej utrudniło ofierze jego odzyskanie. Pracownicy Twittera ściśle współpracowali z ofiarami, aby pomóc w przywróceniu kont, i ostatecznie udało się odnieść sukces. Niestety, atakujący zdążyli już rozpowszechnić fałszywe informacje przy użyciu przejętych kont, a także usuwać prawdziwe tweety.

Doubleswitch jest działaniem, którego sprawca może trwale zablokować lub wydłużyć okres, w którym kontroluje konto w serwisie społecznościowym, zmieniając nazwę użytkownika, a następnie usuwając oryginalne konto. Atak Doubleswitch myli potencjalnych obserwujących (followersów) i sprawia, że standardowe mechanizmy odzyskiwania są nieskuteczne. Platformy mediów społecznościowych zazwyczaj nie powiadamiają użytkowników o zmianach w nazwach użytkowników. Metodę można stosować także w innych serwisach społecznościowych, w tym na Facebooku i Instagramie.

Jakub Idzik, Rafał Klepka

A new social media attack called „Doubleswitch", 10.06.2017, LatestHackingNews.com (dostęp 20.01.2020); A.J. Dellinger, *DoubleSwitch Twitter Hack: New Attack Targets Activists On Twitter*, 6.09.2017, IBITimes.com (dostęp 20.01.2020); J. Idzik, R. Klepka, *Doubleswitch*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; G. Masters, *„Doubleswitch" targeting activists via social media, Access Now report*, 20.06.2017, SCMagazine.com (dostęp 20.01.2020); *The „Doubleswitch" social media attack: a threat to advocates in Venezuela and worldwide*, 9.06.2017, AccessNow.org (dostęp 20.01.2020); Q. Wong, *Twitter hack: Activists and journalists targeted in 'Doubleswitch' social media attack*, 9.06.2017, SiliconBeat.com (dostęp 30.04.2019).

DOWÓDZTWO EUROPEJSKIE STANÓW ZJEDNOCZONYCH (United States European Command, USEUCOM) – jest jednym z 11 połączonych dowództw Departamentu Obrony USA stacjonujących w Stuttgarcie (Niemcy), który odgrywa również rolę dowództwa operacyjnego →NATO [t. 3].

Prezydent H.S. Truman 14 grudnia 1946 r. zatwierdził pierwszy ujednolicony plan dowodzenia dla sił amerykańskich. Zunifikowana struktura dowodzenia zrodziła się w 1949 r. Pojawiły się pytania dotyczące zaangażowania USA w obronę Europy Zachodniej przed ZSRR. Zapewnienie wspólnej obrony było ważnym problemem, zwłaszcza po kryzysie berlińskim w latach 1948–1949, kiedy ZSRR zablokował dostęp do podzielonego miasta, w rezultacie czego w 1949 r. sojusznicy utworzyli Organizację Traktatu Północnoatlantyckiego (NATO).

USEUCOM zostało utworzone jako następca Sił Zbrojnych Stanów Zjednoczonych w Europie, które powstało po II wojnie światowej z siedzibą we Frankfurcie nad Menem. Przed 1 sierpnia 1952 r. Siły Powietrzne, Marynarka Wojenna i Armia Stanów Zjednoczonych w Europie prowadziły odrębne dowództwa, które podlegały bezpośrednio Połączonym Szefom Sztabów (Joint Chiefs of Staff). Taka sytuacja zaistniała na skutek stanowiska generała armii D.D. Eisenhowera, który nie chciał pełnić podwójnej funkcji dowódcy wszystkich sił amerykańskich w Europie oraz Naczelnego Dowódcy Sił Sojuszniczych Europy NATO. Jednak 19 maja 1952 r. poinformował Połączonych Szefów Sztabów, że obejmie bezpośrednie dowództwo sił amerykańskich w Europie i utworzy osobny sztab, który będzie prowadził wspólne sprawy wojskowe USA.

Pierwsze ujednolicone dowództwo na obszarze europejskim zostało ustanowione przez Połączonych Szefów Sztabów 1 sierpnia 1952 r. w celu zapewnienia „jednolitego dowództwa i władzy" nad wszystkimi siłami USA w Europie. W 1952 r. obszar odpowiedzialności USEUCOM obejmował Europę kontynentalną, Wielką Brytanię, Afrykę Północną i Turcję, następnie został rozszerzony na Azję Południowo-Zachodnią po Iran i na południu do Arabii Saudyjskiej.

W 1954 r. kwatera główna USEUCOM została przeniesiona do Camp-de-Loges na obrzeżach Paryża, aby być w pobliżu Naczelnego Dowództwa Sił Sojuszniczych Europy. Na początku lat 60. w NATO pojawiły się ostre spory polityczne, a w 1966 r. prezydent Francji Ch. de Gaulle zażądał usunięcia wszystkich kwater i sił zbrojnych USA i NATO z francuskiego terytorium. Od 14 marca 1967 r. siedziba znajduje się w Patch Barracks w Stuttgarcie-Vaihingen.

Dowództwo USEUCOM wykonuje pełen zakres operacji wielodomenowych we współpracy z sojusznikami i partnerami, aby „wspierać NATO, odstraszać Rosję, pomagać w obronie Izraela, umożliwiać operacje globalne i przeciwdziałać zagrożeniom transnarodowym, wzmacniać bezpieczeństwo euroatlantyckie".

Wraz z końcem → z i m n e j w o j n y [t. 4] Stany Zjednoczone zaczęły wycofywanie swoich wojsk z Europy. W 2004 r. prezydent G.W. Bush ogłosił nową doktrynę stacjonowania sił zamorskich, tzw. Global Posture Review. Była to najpoważniejsza zmiana od czasów zakończenia II wojny światowej. Bush nazwał nowy typ baz mianem *lily pad* (z ang. liść lilii wodnej). Zamiast stałych, gigantycznych baz miały powstawać w wielu regionach świata małe jednostki składające się najczęściej z lotniska, niewielkiej załogi, składów amunicji i paliw. Dzięki nim siły Stanów Zjednoczonych w razie potrzeby mogą w krótkim czasie uderzyć w każdym zakątku globu. Jeszcze w 2004 r. tylko amerykańskie siły lądowe liczyły w Europie 62 tys. wojskowych korzystających z 240 obiektów i zorganizowanych m.in. w ramach 2 dywizji (1 Dywizja Piechoty i 1 Dywizja Pancerna) oraz brygady powietrznodesantowej. W kolejnych latach kontynuowano proces konsolidacji jednostek, rozwiązywania zbędnych czy powrotu części z nich do Stanów Zjednoczonych (powrót dotyczył przede wszystkim obu wspomnianych dywizji). W 2006 r. U.S. Army utrzymywała w Europie

55 tys. → ż o ł n i e r z y [t. 4], chociaż istotnie zmieniła się struktura organizacyjna jednostek, w których służyli.

W 2007 r. pod dowództwem USEUCOM znajdowało się ok. 72 tys. żołnierzy. W 2010 r. Stany Zjednoczone obsługiwały ok. 737 amerykańskich baz rozsianych w blisko 150 krajach świata, w których na stałe stacjonowało prawie 400 tys. żołnierzy, 38 tys. spośród nich w miejscach o strategicznym znaczeniu dla lotnictwa i marynarki wojennej USA. Około 500 amerykańskich baz było w Europie, z czego nieco ponad 200 to lotniska wojskowe i powiązane obiekty. W 1990 r. w samej tylko Republice Federalnej Niemiec było 47 większych baz USA, w tym 10 baz sił powietrznych.

W połowie pierwszej kadencji B. Obamy rozpoczął on istotną redukcję amerykańskiego potencjału wojskowego w Europie. Decyzja ta miała wymiar strategiczny, USA dokonywały bowiem zmiany środka ciężkości swej globalnej obecności militarnej ze sfery atlantyckiej na Pacyfik. Dotyczyło to jednostek → m a r y n a r k i w o j e n n e j [t. 3], ale i w podobnym stopniu sił powietrznych, a nawet wojsk lądowych. Gdy USEUCOM pozostała w Europie z dwoma związkami taktycznymi o potencjale brygady, Rosjanie – inspirowani zmianami politycznymi w Ukrainie – w 2014 r. dokonali błyskawicznej → a n e k s j i [t. 1] Krymu i rozpoczęli ograniczony konflikt w Donbasie. W odpowiedzi amerykańskie siły zbrojne zwiększyły swą aktywność na wschodniej flance NATO.

Największe amerykańskie bazy zostały ulokowane wzdłuż gigantycznego półksiężyca niestabilności ciągnącego się od Karaibów poprzez Hawaje, Japonię, Koreę Południową, Guam aż po Zatokę Perską i kraje Europy Zachodniej. Tradycyjnie bazy USA mają spełnić 3 cele:

- powstrzymanie powiększania się wpływów największych rywali Stanów Zjednoczonych: Chin i Rosji;
- zapewnienie kontroli nad strategicznymi składami surowców, przede wszystkim ropy w Zatoce Perskiej;
- powstrzymanie gróźb islamskiego fundamentalizmu (zob. → f u n d a m e n t a l i z m r e l i g i j n y).

Obecnie w Europie stacjonuje ok. 60 tys. żołnierzy z 5 typów sił zbrojnych, natomiast w rekordowych pod tym względem latach 60. było ich 400 tys. Dowódcy sił amerykańskich w Europie podlegają gen. C. Scaparrottiemu, który jednocześnie pełni funkcję najwyższego dowódcy

wojskowego NATO. Generał w maju 2020 r. apelował do Kongresu, aby zwiększyć liczbę amerykańskich żołnierzy w Europie, bo tylko to zapewni skuteczne odstraszanie Moskwy. Kwatera główna sił USA w regionie znajduje się w Stuttgarcie. W Neapolu z kolei mieści się dowództwo VI Floty, która operuje na wschodnim Atlantyku i zachodniej części Oceanu Indyjskiego. Amerykanie mają w Europie również bomby atomowe pod postacią zwykłych, zrzucanych z bombowców ładunków. Szacuje się, że 150–200 sztuk takiego uzbrojenia znajduje się na wyposażeniu baz wojskowych w Holandii, Niemczech, Turcji i Wielkiej Brytanii. Amerykanie stacjonują w niemieckim Ramstein, włoskim Aviano, na japońskiej wyspie Okinawa, w tureckim İncirlik czy południowokoreańskim Kunsan – bazy tworzą zamknięte miasta, do których na kilka lat przyjeżdża wraz z rodzinami po kilkadziesiąt tysięcy amerykańskich żołnierzy i gdzie znajduje się najnowocześniejszy sprzęt wojskowy: we Włoszech stacjonuje 401 eskadra myśliwców F-16, w Niemczech czołgi M1A2 Abrams wyposażone w ultraprecyzyjne systemy naprowadzania, a w bazie Kleine Brogel w Belgii (80 km od Brukseli) Amerykanie mają pociski typu B-61 z głowicami atomowymi. Większość żołnierzy USEUCOM to 7 Armia Stanów Zjednoczonych, 6 Flota Stanów Zjednoczonych oraz 3 i 16 Brygada Sił Powietrznych.

Europejska inicjatywa odstraszania, ogłoszona w 2014 r., umożliwia Stanom Zjednoczonym wzmocnić odstraszającą postawę USA, zwiększyć gotowość i szybkość reakcji sił amerykańskich w Europie, wspierać obronę zbiorową oraz → b e z p i e c z e ń s t w o [t. 1] sojuszników NATO, a także wzmacniać bezpieczeństwo i potencjał sojuszników i partnerów USA.

W 2014 r. w związku z wydarzeniami w Ukrainie (aneksja Krymu przez Federację Rosyjską i konflikt zbrojny na wschodzie Ukrainy) USA rozpoczęły ćwiczenia militarno-polityczne w ramach operacji Atlantic Resolve. Zaczęto regularnie przeprowadzać rotację wojsk amerykańskich ze Stanów Zjednoczonych do Europy Wschodniej (do udziału w ćwiczeniach i wspólnym szkoleniu bojowym z siłami zbrojnymi państw tego regionu), po raz pierwszy w Polsce i krajach bałtyckich pojawiły się czołgi amerykańskie. Wielkość amerykańskich sił zbrojnych w Europie według „The Military Balance" w latach 2013–2016 zmniejszyła się z 70,1 do 67,1 tys. osób. Nie uwzględnia to jednak sił rotacyjnych, które

stacjonują w Europie przez określony czas. Ich średnioroczną liczbę można szacować na ok. 8 tys. osób. Od 2017 r. w Europie było więc ok. 75 tys. żołnierzy amerykańskich.

USA rozpoczęły w lutym 2017 r. wzmacnianie swych sił lądowych w Europie w ramach ciągłego rotacyjnego przenoszenia brygad pancernych, co zwiększyło obecność armii USA w Europie do 3 brygad. Według komunikatu dowództwa USEUCOM armia i przede wszystkim wojska lądowe USA rozpoczęły składowanie uzbrojenia w swych wysuniętych magazynach armijnych (Army Prepositioned Stocks, APS) na terenie Europy na potrzeby ewentualnych działań doraźnych. Chodzi o nieprzerwane rozmieszczenie w Europie Wschodniej brygady pancernej, bowiem rotacje wojsk będą przebiegały bez przerwy, co oznacza ciągłą obecność wojsk pancernych w tej części Europy. Ten plan rozmieszczenia armii jest kolejnym przejawem zdecydowanego i zrównoważonego podejścia do kwestii gwarancji dla sojuszników w obliczu agresywnej polityki Rosji w Europie Wschodniej. Według zapowiedzi USEUCOM uczestniczące w dziewięciomiesięcznych misjach rotacyjnych brygady zabiorą ze sobą z USA własne nowoczesne wyposażenie. Będzie to najnowocześniejsze wyposażenie, jakie armia ma do dyspozycji. Natomiast używane obecnie przez siły rotacyjne wyposażenie pozostanie w Europie, by po naprawach i unowocześnieniu stać się podstawowym elementem APS, które będą rozmieszczone w Belgii, Holandii i Niemczech. W razie potrzeby zmagazynowany w APS materiał zapewni wojskom dodatkowy potencjał bojowy.

Od końca 2017 r. w Europie znajdują się 3 w pełni wyposażone brygady armii USA – jedna pancerna (stacjonuje w Niemczech), jedna powietrznodesantowa (stacjonująca we Włoszech) i jedna typu Stryker – zmechanizowana brygada pancerna. Amerykańskie plany zakładają możliwość przerzucenia na wschodnie obrzeża NATO 4 brygad: 2 stacjonujących w Europie Zachodniej, kolejnej brygady ćwiczącej rotacyjnie w regionie, czwarta byłaby przerzucana z USA lub innej pozaeuropejskiej amerykańskiej bazy, sprzęt dla niej ma być składowany w Europie.

Pięć elementów europejskiego planu dowództwa USA dotyczącego wdrożenia EDI (ang. *Electronic Data Interchange*) składa się na opracowaną technikę wymiany danych wykorzystującą zasady działania poczty

elektronicznej, której cechą charakterystyczną jest niezależność od właściwości stosowanego sprzętu i oprogramowania (5910,6 mln USD na rok budżetowy 2020):

- Zwiększona obecność (2051 mln USD): Stany Zjednoczone będą nadal wspierać zwiększoną rotacyjną obecność wojskową USA w całej Europie, która jest w stanie odstraszać i – w razie potrzeby – reagować na regionalne → zagrożenia [t. 4].
- Ćwiczenia i szkolenie (609 mln USD): wzrost tempa szkolenia, które poprawia ogólną gotowość i interoperacyjność sojuszników NATO i partnerów, a także może służyć jako środek odstraszający wobec agresywnych podmiotów regionalnych.
- Lepsze pozycjonowanie wstępne (2359 mln USD): zwiększenie nowoczesnego sprzętu w całej Europie, który umożliwia jednocześnie szybkie rozmieszczenie sił zbrojnych według zapotrzebowania.
- Modernizacja infrastruktury (517 mln USD): kluczowe usprawnienia infrastruktury w całej Europie będą wspierać operacje wojskowe USA.
- Budowanie potencjału partnerstwa (374 mln USD): rozszerzone zaangażowanie i ćwiczenia wzmacniają zdolność sojuszników i partnerów do obrony i utrzymania → bezpieczeństwa europejskiego [t. 1].

USEUCOM utrzymuje operacyjne siły zbrojne do prowadzenia pełnych operacji samodzielnie lub we współpracy z partnerami koalicyjnymi i stawia przed sobą następujące zadania:

- zwiększenie bezpieczeństwa transatlantyckiego dzięki wsparciu NATO;
- zapewnienie stabilności regionalnej;
- powstrzymanie konfliktów, wojna z → terroryzmem [t. 4];
- przeciwdziałanie zagrożeniom transnarodowym w celu ochrony i obrony Stanów Zjednoczonych;
- reprezentacja interesów USA w regionie.

Aktualne obszary zainteresowania USA obejmują również:

- przegląd pozycji europejskich sił strategicznych;
- aktualizację problemów związanych z koronawirusem;
- międzynarodowe ćwiczenia sił morskich Northern.

Celem USEUCOM jest budowa bardziej efektywnych sił i utrzymanie współpracy z sojusznikami USA w Europie. Ma towarzyszyć temu optymalizacja amerykańskiej obecności militarnej na świecie, tj. lepsze ulokowanie sił i środków, zwiększenie ich efektywności w zmieniającym się współczesnym świecie.

Generalnie, zdaniem Szefa Pentagonu, przed USEUCOM stoi 5 kluczowych wyzwań:

- →strategia [t. 4] →odstraszania [t. 3] Rosji;
- wzmocnienie NATO;
- zagwarantowanie pewności sojusznikom;
- poprawa strategicznej elastyczności Stanów Zjednoczonych i operacyjnej elastyczności USEUCOM;
- zadbanie o wojskowych i ich rodziny.

W 2020 r. ok. 5,6 tys. wojskowych zostało przeniesionych z Niemiec do innych państw Sojuszu, ok. 6,4 tys. osób wraca do USA. Znaczna część żołnierzy jest zaangażowana w rotacyjną obecność w Europie. Amerykańskie dowództwa w Europie mają być przesunięte bliżej struktur dowodzenia NATO w Belgii oraz we Włoszech. Przesunięcia w systemie dowodzenia mogą objąć grupę nawet 2 tys. amerykańskich wojskowych.

Zgodnie z planami ogłoszonymi w lipcu 2020 r. przez Pentagon ze Stuttgartu w Niemczech do Mons w Belgii zostało przeniesione Dowództwo Europejskie Stanów Zjednoczonych oraz towarzyszące mu dowództwo amerykańskich sił operacji specjalnych w Europie. Z Niemiec – do jeszcze nieustalonej lokalizacji – przenieść mają się także dowództwa odpowiedzialne za amerykańskie siły zbrojne w Afryce oraz siły specjalne USA na tym kontynencie. Część mniejszych amerykańskich jednostek wojskowych ma zostać przesunięta z Niemiec do Belgii i Włoch.

Naczelny Dowódca Sił Sojuszniczych w Europie generał T.D. Wolters, udzielając wywiadu przedstawicielom NATO w październiku 2019 r. podkreślił, że:

> pierwszym priorytetem działalności EUCOM […] jest wspieranie NATO. Drugim priorytetem jest zwalczanie złośliwych wpływów Rosji. […] Trzecim dużym priorytetem są relacje i zaangażowanie […] dla wspierania gotowości naszych sił, aby były one

jak najbardziej responsywne, odporne i zabójcze, dotrzymując i promując te wartości demokratyczne, które są tak ważne dla NATO i USA.

Warto wskazać kilka ostatnich działań, które zostały przyjęte z perspektywy USEUCOM oraz z perspektywy SACEUR (Supreme Allied Commander Europe) – naczelnego dowódcy sojuszniczego w Europie, głównodowodzącego połączonych sił zbrojnych NATO w Europie, stojącego na czele Sojuszniczego Dowództwa Operacji (Allied Command Operations):

- adaptacja nowej strategii wojskowej NATO, która definiuje 2 podstawowe zagrożenia – jedno pochodzi z Rosji, a drugie dotyczy międzynarodowego terroryzmu;
- wstępna koncepcja odstraszania i obrony obszaru euroatlantyckiego NATO, którą muszą przyjąć wszystkie spośród 29 zaangażowanych krajów, żeby poprawić zdolność odstraszania w XXI w. i obrony w taki sposób, aby nigdy nie dochodziło do sytuacji, w której wyniknie konflikt kinetyczny i trzeba będzie się bronić;
- adaptacja struktury dowodzenia NATO – umieszczanie sił zbrojnych tam, gdzie muszą być, żeby były najlepiej dopasowane, we właściwym miejscu i czasie, żeby najskuteczniej odstraszać, tak aby niefortunny potencjał konfliktu nigdy się nie pojawił.

Od zakończenia II wojny światowej europejscy sojusznicy i partnerzy współpracują ze Stanami Zjednoczonymi, żeby osiągnąć bezpieczeństwo i stabilność, a Europa nadal ma kluczowe znaczenie dla → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1] USA. Obecnie Europejskie Dowództwo Stanów Zjednoczonych mierzy się z najgłębszymi negatywnymi zmianami w europejskim środowisku bezpieczeństwa od zakończenia zimnej wojny. Masowa migracja, terroryści, → w o j n a i n f o r m a c y j n a [t. 4] i hybrydowa, → c y b e r a t a k i [t. 1], utrzymujące się skutki światowego kryzysu finansowego i niedofinansowane budżety obronne państw sojuszników zagrażają bezpieczeństwu europejskiemu, USA oraz światowemu bezpieczeństwu i stabilności.

Szereg krajów Europy Wschodniej należy do regionów na obszarze EUCOM, w których pomimo ogólnej redukcji ma nastąpić wzrost

liczebności wojsk. Stany Zjednoczone stacjonowały już w Rumunii podczas II wojny w Zatoce Perskiej, ale wycofały się w 2003 r. W 2004 r. rząd rumuński zaoferował USA ponowne wykorzystanie lotniska wojskowego im. M. Kogălniceanu i pobliskich obiektów portowych w Konstancy, a także portu morskiego Mangalia i ośrodka szkoleniowego w Babadag. 6 grudnia 2005 r. oba państwa podpisały traktat o utworzeniu terminala operacyjnego. Kraje Europy Południowo-Wschodniej są szczególnie interesujące dla USA ze względu na ich bliskość do aktualnych punktów zapalnych na Bliskim Wschodzie. W najbliższym czasie do Europy Środkowo-Wschodniej zostanie wysłana brygada wojsk amerykańskich, brygada pancerna uzbrojona w najnowocześniejszy sprzęt.

Polski rząd starał się o ulokowanie baz amerykańskich na swoim terytorium od końca 2003 r. Pierwsi amerykańscy żołnierze (ok. 100 osób) na zaproszenie polskich władz przylecieli do Polski na poligon 16 Pomorsko-Warmińskiej Brygady Zmechanizowanej w Morągu na Mazurach samolotami transportowymi C-130 Herkules z 7 Brygady Obrony Powietrznej USA, stacjonującej w Kaiserslautern w Niemczech, latem 2010 r. Od 2012 r. na stałe są ulokowani w Polsce. W ten sposób po raz pierwszy od 17 września 1993 r., kiedy z polski wyjechała ostatnia jednostka armii ZSRR, w Polsce zaczęły stacjonować wojska innych państw – wojska amerykańskie.

Ponadto od maja 2014 r. w Bazie Lotniczej w Malborku odbywa się rotacja eskadr NATO, które wspierają patrolowanie przestrzeni powietrznej nad państwami bałtyckimi w ramach misji Baltic Air Policing. Wzmacnianie wschodniej flanki Sojuszu poprzez rotacyjne ćwiczenia kontynuowane były i w następnych latach, a większą dynamikę temu procesowi nadało utworzenie sił natychmiastowego reagowania NATO. Wdrożenie nowej strategii NATO, która może być przełomem m.in. dla Polski, jest konieczne dla zbudowania nowej architektury bezpieczeństwa w Europie i świecie.

Od 2017 r. w Polsce szkolą się amerykańskie brygady pancerne, które przyjeżdżają do naszego kraju na zasadzie misji rotacyjnych na 9 miesięcy. W Poznaniu zostało utworzone wysunięte stanowisko dowodzenia amerykańskiej dywizji.

Amerykanie budują w Polsce sieć dowództw przygotowaną do ewentualnego rozwinięcia w razie dużego zagrożenia. Pentagon planuje przerzucenie z USA do Polski na rotacyjnej zasadzie wysuniętego stanowiska

dowodzenia V Korpusu Sił Lądowych USA. To niedawno odtworzone dowództwo amerykańskie, które w czasach zimnej wojny znajdowało się w Niemczech Zachodnich i było odpowiedzialne za obronę kluczowego odcinka granicy, skąd wiodła najkrótsza droga z Niemieckiej Republiki Demokratycznej do Zagłębia Ruhry, będzie mogło koordynować duże siły po ich ewentualnym rozwinięciu, a w razie zagrożenia także nimi dowodzić.

Po wybuchu pandemii COVID-19 europejskie dowództwo USEUCOM zmniejszyło zakres i rozmiar prowadzonych przez USA wielonarodowych ćwiczeń DEFENDER-Europe 20, aby zminimalizować ryzyko dla uczestniczących sił i lokalnej ludności. Jest to jeden z przykładów współpracy sojuszników i partnerów w celu dostosowania się do tego kryzysu, przy jednoczesnym zachowaniu gotowości. Podczas gdy COVID-19 nieustannie stwarza wyzwania we wszystkich segmentach społeczeństwa, armia USA w Europie nadal pozostaje czujna. Około 72 tys. żołnierzy, którzy mieszkają i pracują na terenie całej Europy, utrzymuje gotowość bojową i środki odstraszające, podejmując jednocześnie odpowiednie kroki, żeby zapobiec dalszemu rozprzestrzenianiu się epidemii.

Ćwiczenia DEFENDER-Europe 20, chociaż zostały ograniczone pod względem zakresu i rozmiaru, wykazały mobilność wojskową. Ten wspólny wysiłek USA i innych uczestników wzmocnił również potrzebę wprowadzenia jednolitych wymogów dotyczących przekraczania granic między krajami partnerskimi UE. Ponadto wspólne wysiłki pokazały, jak ważne są długoterminowe inwestycje w niezawodną infrastrukturę podwójnego zastosowania w celu wspierania i umożliwiania mobilności wojskowej, która ma kluczowe znaczenie dla zapewnienia szybkiego rozmieszczenia wojsk i sprzętu w całej Europie.

Ćwiczenia powiązane z DEFENDER-Europe 20, a także szereg innych wydarzeń zaplanowanych na lato 2020 r., zostały odwołane, zmodyfikowane lub opóźnione w celu bezpiecznego przeprowadzenia zamierzonych szkoleń.

Olga Wasiuta

P.M. Breedlove, *United States European Command. Theater Strategy*, 2015, IEEE.es (dostęp 20.10.2020); M. Cielma, *Amerykańska obecność w Europie*, „Nowa Technika

Wojskowa" 2016, nr 3; S. Duke, *United States Military Forces and Installations in Europe*, Oxford University Press, SIPRI, Oxford 1989; *EUCOM: USA zwiększą swe siły lądowe w Europie do trzech brygad*, 30.03.2016, Bankier.pl (dostęp 20.10.2020); *EUCOM: Stany Zjednoczone zwiększą siły lądowe w Europie do trzech brygad*, 30.03.2016, wp.pl (dostęp 19.20.2020); *European Deterrence Initiative (EDI) Fact Sheet*, 1.02.2020, EUCOM.mil (dostęp 20.10.2020); B.W. Everstine, *Wolters Takes Command of EUCOM, NATO*, 2.05.2019, AirForceMag.com (dostęp 19.10.2020); *History of USEUCOM; Commander's Priorities; Current Focus Areas*, EUCOM.mil (dostęp 19.10.2020); *Jankesi w Polsce. Oto ich przyczółek*, 15.05.2010, Dziennik.pl (dostęp 19.10.2020); Ł. Kulesa, *Wzmocnienie obecności wojskowej USA w Polsce: perspektywa amerykańskich think tanków*, „Polski Przegląd Dyplomatyczny" 2019, nr 2; Z. Lachowski, *Foreign Military Bases in Eurasia*, „SIPRI Policy Paper" 2017, no 18; W. Malendowski, *Spory i konflikty międzynarodowe: aspekty prawne i polityczne*, Atla2, Wrocław 2000; M. Nowosielski, *Zimna wojna (1946–1989) i jej konsekwencje dla ładu międzynarodowego*, Instytut Zachodni, Poznań 2007; *Press Briefing on USEUCOM Priorities*, 3.10.2019, SHAPE.NATO.int (dostęp 18.10.2020); *United States European Command: Overview and Key Issues*, 4.08.2020, FAS.org (dostęp 20.10.2020); *U.S. European Command Remains Ready and Responsive During the Pandemic*, 8.04.2020, NATO.mil (dostęp 20.10.2020); J. Vandiver, *EUCOM Tests War Readiness with Classified Drill*, 23.10.2020, Stripes.com (dostęp 24.10.2020); *Wiemy, jakie jednostki wycofa USA z Niemiec. Co trafi do Polski?*, 29.07.2020, Defence24.pl (dostęp 18.10.2020).

DOWÓDZTWO PRZESTRZENI CYBERNETYCZNEJ I INFORMACYJNEJ NIEMIEC (niem. Kommando Cyber-und Informationsraum; KdoCIR, ang. Cyber and Information Domain Service, CIR) – cyberdowództwo w ramach →Bundeswehry [t. 1] ds. walki w wirtualnej przestrzeni. Siły zbrojne Niemiec powołały – obok →wojsk lądowych [t. 4] (Heer), lotnictwa (Luftwaffe), →marynarki wojennej [t. 3] (Marine), służby wsparcia (Streitkräftebasis) oraz służby medycznej Bundeswehry (Zentralen Sanitätsdienst der Bundeswehr) – szósty, nowy rodzaj wojsk, który jest najmłodszą częścią niemieckich sił zbrojnych. To zdecydowana odpowiedź Niemiec na →wojnę [t. 4] w →cyberprzestrzeni [t. 1].

W listopadzie 2015 r. niemieckie Ministerstwo Obrony powołało radę rozwoju KdoCIR, której zadaniem było opracowanie planów reorganizacji →cyberbezpieczeństwa [t. 1], IT, →wywiadu [t. 4]

wojskowego, geoinformacyjnych i operacyjnych jednostek komunikacyjnych w obszarze cyberprzestrzeni i →przestrzeni informacyjnej [t. 3] Bundeswehry. 26 kwietnia 2016 r. minister obrony U. von der Leyen przedstawiła →opinii publicznej [t. 3] plany nowego oddziału wojskowego, a 5 października 2016 r. personel dowództwa zaczął działać jako departament w Ministerstwie Obrony. 14 października 2016 r. minister obrony mianowała gen. L. Leinhosa na szefa dowództwa nowo utworzonego rodzaju sił zbrojnych. Na początku kwietnia 2017 r. został uruchomiony nowy rodzaj wojsk – KdoCIR z siedzibą w Bonn, które ma integrować zdolności w zakresie obrony cybernetycznej i prowadzenia operacji cybernetycznych w ramach Bundeswehry. Podczas inauguracji U. von der Leyen wspomniała o kamieniu milowym w niemieckim systemie obronnym, ponieważ →cyberataki [t. 1] stały się podstawowym →zagrożeniem bezpieczeństwa [t. 4].

U. von der Leyen twierdzi, że KdoCIR pozwala w przypadku ataku cybernetycznego na „ofensywną obronę". Gdy dojdzie do cybernetycznego ataku na niemiecką infrastrukturę, do działań włączone zostaną inne instytucje państwa niemieckiego. W skład cyberdowództwa weszło początkowo 260 pracowników z gen. Leinhosem na czele, którzy nadzorują →żołnierzy [t. 4] i cywilów w różnych jednostkach – od wywiadu wojskowego i →bezpieczeństwa [t. 1] IT po geoinformację. KdoCIR ma uzyskać pełną gotowość operacyjną do 2021 r. W ciągu najbliższych lat liczebność dowództwa wzrośnie do ok. 15 tys. osób, będzie to ok. 13,5 tys. żołnierzy i 1,5 tys. pracowników cywilnych.

Głównymi zadaniami cyberdowództwa są:

- ochrona wrażliwych systemów informatycznych Bundeswehry (należących do największych sieci komputerowych w Niemczech),
- utrzymanie bezpieczeństwa cybernetycznego,
- →rozpoznanie wojskowe [t. 3] i geoinformacja,
- prowadzenie działań psychologicznych na szczeblu operacyjnym i taktycznym.

KdoCIR ma za zadanie wzmacniać ochronę sieci informatycznych i systemów uzbrojenia Bundeswehry, ale też rozwijać zdolności do ofensywnych działań w cyberprzestrzeni oraz chronić państwo przed atakami →hakerów na cele wojskowe. Zadaniem KdoCIR będzie także:

- odpowiedź na →zagrożenia hybrydowe [t. 4],
- zapewnienie odpowiedniego poziomu bezpieczeństwa →infrastruktury krytycznej kraju,
- przeciwdziałanie →konfliktom międzynarodowym,
- wojskowe wykorzystanie cyberprzestrzeni,
- wsparcie komputerowe operacji konwencjonalnych i wykorzystanie zdolności cybernetycznych do wspierania operacji o charakterze konwencjonalnym.

Niemcy łączą w nowej strukturze szereg służb odpowiedzialnych za wykorzystanie →informacji w siłach zbrojnych, związanych ze strategicznym rozpoznaniem czy dowodzeniem. Nowo powstałemu dowództwu podlegają m.in.: Dowództwo Rozpoznania Strategicznego, Dowództwo ds. Technik Informacyjnych, Centrum Geoinformacji i podporządkowane im jednostki – wcześniej znajdujące się w strukturach Inspektoratu Wsparcia. KdoCIR jest rdzeniem →strategii [t. 3] cybernetycznej Bundeswehry. Oprócz wojska, lotnictwa, marynarki wojennej, służby wsparcia i służby medycznej, KdoCir jest teraz na równi z innymi wojskowymi jednostkami organizacyjnymi.

Cyberobrona leży w gestii Federalnego Ministerstwa Spraw Wewnętrznych, podczas gdy Federalne Ministerstwo Spraw Zagranicznych odpowiada za cybernetyczną i międzynarodową politykę bezpieczeństwa cybernetycznego. Zgodnie z białą księgą z 2016 r. aspekty obronne ogólnounijnej architektury bezpieczeństwa cybernetycznego zostały określone jako oryginalne zadania Federalnego Ministerstwa Obrony i jako konstytucyjny mandat Bundeswehry. Przestrzeń cybernetyczna i informacyjna stały się nowym wyzwaniem operacyjnym dla Bundeswehry.

Wyzwania dla bezpieczeństwa cybernetycznego i przestrzeni informacyjnej znalazły się na drugim miejscu na liście zagrożeń (po międzynarodowym →terroryzmie [t. 4]) w Białej księdze polityki bezpieczeństwa i przyszłości Bundeswehry z lipca 2016 r. Wg minister obrony U. von der Leyen Bundeswehra rejestruje ok. 4,5 tys. prób dostępu do swoich sieci codziennie. Utworzenie KdoCIR w Bundeswehrze odzwierciedla również tendencje w →NATO [t. 3]. Przestrzeń cybernetyczna została uznana w Sojuszu za sferę działań operacyjnych na szczycie w Warszawie w lipcu 2016 r.

W ostatnich latach Republika Federalna Niemiec była częstym celem ataków hakerskich: wg „Der Spiegel" za atakami w latach 2016–2017 na systemy informatyczne Bundestagu stała Federacja Rosyjska, w rezultacie czego władze były zmuszone do wymiany ponad 20 tys. urządzeń działających w tej sieci. Niemiecki resort obrony wydał oświadczenie, w którym stwierdzono, że od początku 2017 r. systemy informatyczne Bundeswehry były atakowane ponad 280 tys. razy.

Znaczenie KdoCIR dla niemieckiej obrony rośnie także na tle wyrafinowanych cyberataków na systemy rządowe, przemysłowe i infrastrukturalne. Wg raportu MSW z lipca 2017 r. w sprawie ochrony konstytucji, →cyberszpiegostwo [t. 1], sabotaż i →dezinformacja stały się standardowymi narzędziami zagranicznych służb wywiadowczych i hakerów, zwłaszcza z Rosji, Chin i Iranu. Gdy rząd stara się wzmocnić swoje systemy obronne, same siły zbrojne stają przed konkretnymi zagrożeniami. Wg Bundeswehry w 2017 r. było ok. 2 mln prób nieautoryzowanego dostępu do ich systemów, w tym 8 tys. prób, w których ingerencja w systemy informatyczne armii właśnie się nie powiodła, ponieważ działały zabezpieczenia takie jak zapory ogniowe.

Kluczowym punktem KdoCIR jest Cybersecurity Center, jednostka chroniąca systemy informatyczne Bundeswehry. Szef departamentu ppłk M. Krempel i jego zespół są odpowiedzialni za różne zadania, od technologii przeciwpancernych po prowadzenie szkoleń w zakresie cyberincydentów. Całodobowe centrum lokalizacyjne rejestruje zdarzenia i może wysyłać jednostki reagowania kryzysowego.

Ochrona i obrona oznaczają również znajdowanie słabych punktów w infrastrukturze bezpieczeństwa Bundeswehry, które mogą wykorzystać hakerzy. Jednak przypisanie ataku do konkretnego źródła nie jest głównym zadaniem jego jednostki.

W ramach obecnych rozwiązań prawnych Bundeswehra może wspierać inne organy administracji publicznej w przeciwdziałaniu atakom cybernetycznym. Znaczenie KdoCIR dla niemieckiej obrony wzrasta również w kontekście wyrafinowanych cyberataków na systemy rządowe, przemysłowe i infrastrukturalne. Wszyscy żołnierze mundurowi noszą ciemnoniebieski beret z nową odznaką – odznaką służby wojskowej KdoCIR.

Struktura KdoCIR: Dowództwo Cybernetyczne i Przestrzeni Informacyjnej, Dowództwo Rozpoznania Strategicznego, Centrum Geoinformacji, Dowództwo IT; którym podporządkowuje się: Centrum Operacji Cybernetycznych (od 2018 r.); Centrum Bezpieczeństwa Cybernetycznego; Centrum Operacyjne Systemów IT; Centrum Kompetencji Systemów IT (od 2019 r.); Centrum Rozpoznania Obrazowego; Centrum Komunikacji Operacyjnej; Centrum Ewaluacji Rozpoznania Elektronicznego; 4 bataliony → walki elektronicznej [t. 4]; 6 batalionów IT; Ośrodek Badań ds. Rozpoznania Technicznego; Szkoła Rozpoznania Strategicznego Bundeswehry; Szkoła IT Bundeswehry.

Oprócz tego istnieje Niemieckie Federalne Centrum Sił Zbrojnych ds. Bezpieczeństwa Cybernetycznego (ZCSBw), które zapewnia kompleksową ochronę interesów, usług IT i systemów informatycznych Bundeswehry w przestrzeni cybernetycznej i informacyjnej, realizując jednocześnie cele ochrony informacji w ramach cyberobrony. W koordynacji z KdoCIR oraz Głównym Urzędnikiem ds. Bezpieczeństwa Informacji w Niemieckich Siłach Zbrojnych (CISOBw) reprezentuje interesy bezpieczeństwa IT, cybernetycznego i informacyjnego Bundeswehry oraz partnerów zewnętrznych, krajowych i międzynarodowych w sprawach operacyjnych i technicznych.

Sergiusz Wasiuta

BMVg, *Abschlussbericht Aufbaustab Cyber- und Informationsraum Empfehlungen zur Neuorganisation von Verantwortlichkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung*, BMVg, 2016; *Bundeswehr: Gut gerüstet für den Cyberkrieg*?, DW.com (dostęp 18.04.2019); *Cyberangriffe auf die Bundeswehr*, 15.04.2017, BundeswehrJournal.de (dostęp 10.03.2019); J. Gotkowska, *Obszar cybernetyczno-informacyjny: nowa formacja w Bundeswehrze*, 12.04.2017, OSW.WAW.PL (dostęp 10.03.2019); C. Marischka, *Ein hybrides Kommando Der Organisationsbereich Cyber- und Informationsraum der Bundeswehr*, „Ausdruck" 2018, nr 5; A. Reiter, *Campus Für Cyber-Krieger*, 7.08.2017, Zeit.de (dostęp 18.04.2019); *Ursula von der Leyen: Bundeswehr startet neues Cyberkommando*, 5.04.2017, Zeit.de (dostęp 18.04.2019); *Zentrum Cyber-Operationen offiziell in Dienst gestellt*, 18.04.18, AugenGeradeaus.net (dostęp 10.03.2019).

DOXING (także „doxxing" lub „doxing") – rozpowszechnianie osobistych danych, np. imienia i nazwiska, adresu zamieszkania, identyfikatorów do rządowych rejestrów i usług (np. numerów ubezpieczeń społecznych w przypadku USA), rejestrów biznesowych, dokumentów oraz zdjęć osób i ich bliskich, za pośrednictwem internetu w łatwo dostępnej formie. →Informacje tego typu mogą być już publicznie dostępne, lecz trudno osiągalne lub rozproszone w różnych miejscach, co utrudnia ich przypadkowe odkrycie. Dane mogą być także informacjami dotyczącymi rządów, firm czy organizacji, które zostały zdobyte w wyniku naruszenia systemów →bezpieczeństwa [t. 1].

Doxing należy odróżnić od pokrewnych zjawisk, takich jak szantaż, zniesławienie czy plotki. W przeciwieństwie do szantażu, doxing nie wiąże się z żądaniami wobec podmiotu, których spełnienie miałoby zapobiec opublikowaniu informacji. Szantażysta publikuje dane tylko wtedy, gdy ofiara nie wypełni oczekiwań szantażysty. Podczas gdy groźba doxingu może służyć jako szantaż, sam atak nie jest szantażem. Zniesławienie obejmuje również publiczne udostępnianie informacji z zamiarem upokorzenia, zastraszenia lub ukarania podmiotu. Aby jednak informacje były zniesławiające, muszą ujawniać coś szkodliwego dla reputacji opisanej osoby. Doxing niekoniecznie musi ujawniać coś wątpliwego lub krępującego. Wreszcie doxing różni się od plotek tym, że polega na ujawnianiu faktów dotyczących tożsamości ofiary, a nie publikowaniu sugestii, pogłosek i insynuacji.

Termin „doxing" pochodzi od ang. wyrażenia *dropping documents* lub *dropping dox*, które w latach 90. XX w. były formą zemsty dokonywanej przez wyjętych spod prawa kultur →hakerów i obejmowały odkrywanie i ujawnianie tożsamości osób walczących o swoją anonimowość. *Oxford English Dictionary* definiuje doxing jako „wyszukiwanie i publikację prywatnych lub identyfikujących informacji na temat konkretnej osoby w internecie, zazwyczaj ze złośliwymi zamiarami". Istnieją różne motywy poddania kogoś doxingowi. Może to wynikać z chęci ujawnienia wyrządzonej przez zaatakowanego krzywdy i pociągnięcia go do odpowiedzialności. Atak może być wykorzystywany do poniżania, zastraszania, grożenia lub karania zidentyfikowanej osoby. Często jest to narzędzie cyberstalkingu, ponieważ publikowane informacje mogą

być sformułowane w sposób, który powodowałby, że ofiara zaczęłaby się obawiać o swoje życie. Ujawnienie tożsamości i danych osobowych ofiary, umożliwiające jej publiczne ośmieszenie, nękanie i oczernianie, może być wyrazem sprzeciwu wobec jakichś jej działań w ramach odwetu. Informacje udostępniane w internecie są łatwo dostępne i trudne do usunięcia: wprowadzenie nazwy ofiary doxingu w wyszukiwarce może ujawnić jej dane osobowe i nadużycia związane z atakiem przez lata. Potencjalne szkody są oczywiste, zwłaszcza gdy życie zawodowe i reputacja danej osoby zależy od jej widoczności w sieci.

Doxing może mieć druzgocący wpływ na jego ofiary. Pomaga w nękaniu i prześladowaniu, co może prowadzić do cierpienia psychicznego ofiar i zwiększa ryzyko obrażeń fizycznych, zwłaszcza jeśli dane osobowe są wykorzystywane do zachęcania innych do znęcania się nad ofiarą. Pomimo szkód doxing jest niekiedy przedstawiany jako narzędzie protestu i ujawniania wykroczeń. → K o r u p c j a urzędników państwowych ChRL jest często celem działań chińskich użytkowników internetu, którzy ujawniają dowody wykroczeń prywatnych i publicznych. Wszczęto np. dochodzenie w sprawie 2 chińskich urzędników samorządowych po tym, jak dokumenty zawierające informacje o wydatkach na podróże badawcze do USA i Kanady zostały anonimowo udostępnione w internecie. Dokumenty dostarczyły dowodów na to, że faktycznie środki publiczne zostały wykorzystane na opłacenie podróży o charakterze turystycznym.

Można wyróżnić 3 formy doxingu:

- deanonimizację,
- targetowanie,
- delegitymizację.

Doxing deanonimizujący uwalnia dane osobowe określające tożsamość osoby wcześniej anonimowej lub znanej pod pseudonimem. Doxing targetujący ujawnia informacje, które są zazwyczaj prywatne, niejawne i stawiają ofiarę w niekorzystnym świetle. Wreszcie doxing delegitymizujący ujawnia intymne informacje osobiste, które szkodzą wiarygodności celu. Wg niektórych badaczy w przypadkach, gdy ujawnienie wykroczenia leży w interesie publicznym, doxing deanonimizujący i delegitymizujący jest dopuszczalny tylko w zakresie niezbędnym do ujawnienia faktu naruszenia prawa, jednak używanie jakiejkolwiek formy doxingu do upokarzania

lub grożenia podmiotowi i ujawniania większej ilości informacji, niż jest to konieczne, jest nieuzasadnione.

Doxing można uznać za działanie o charakterze stopniowalnym. Np. zidentyfikowanie kogoś jako dorosłego mężczyznę, w dużym mieście nie zmniejsza jego anonimowości, ponieważ nie pozwala łatwo zdobyć o nim innej wiedzy. Jednak identyfikacja wg imienia i adresu zamieszkania utrudnia zachowanie anonimowości, ponieważ informacje te można łatwo wykorzystać do ustalenia innych faktów dotyczących tożsamości. Znajomość imienia pozwala na przeszukiwanie publicznie dostępnych rejestrów i baz danych w celu uzyskania dalszych informacji. Znajomość adresu pozwala poznać kogoś osobiście i obserwować jego ruchy, zwyczaje, wygląd fizyczny i cechy charakterystyczne. Weryfikowalność doxingu odróżnia go od innych form ekspozycji danych czy reklamy.

Różne rodzaje wiedzy o tożsamości są dokumentowane w różnych formach. Wiedza o tożsamości dotycząca danych osobowych wykorzystywanych w celach administracyjnych może być rejestrowana w oficjalnych dokumentach takich jak akty urodzenia, zeznania podatkowe czy rejestry zatrudnienia. Mogą one ujawniać nazwę, lokalizację i pseudonimy, które są powiązane z imieniem lub lokalizacją danej osoby. Dokumenty opisujące unikalne cechy posiadane przez osobę znaną pod pseudonimem (identyfikowaną także np. poprzez login czy adres e-mail), które nie mają związku z jej nazwiskiem lub lokalizacją, mogą ujawnić dalszą wiedzę o tożsamości, jeśli można ją powiązać z innymi informacjami. Ta możliwość istnieje np. wtedy, gdy dokumentacja medyczna nie jest wystarczająco anonimizowana.

Inne rodzaje wiedzy o tożsamości, takie jak wiedza o wzorcach i charakterystyka społeczna, są udokumentowane w inny sposób. Często aktualizowane informacje o lokalizacji, przechowywane np. przez urządzenia mobilne, mogą ujawniać codzienną rutynę danej osoby, a zatem gromadzić wiedzę na jej temat. Charakterystyka społeczna może zostać ustalona również na podstawie zdjęć i obrazów dotyczących osoby i jej zachowań. Taka charakterystyka często zależy od interpretacji obserwatora i może być myląca, jeśli obrazy są wyjęte z kontekstu lub przedstawione w stronniczy sposób. Dotyczy to zwłaszcza działań mających znaczenie społeczne lub symboliczne, podważających głęboko zakorzenione przekonania

i oczekiwania. Np. fotografie osoby wyrażającej za pomocą ubioru swoją seksualność mogą być przyczyną drwin, poniżania lub przemocy motywowanej nieprzestrzeganiem i kwestionowaniem konserwatywnych norm zachowania.

Jakub Idzik, Rafał Klepka

Q. Chen, K. Ling Chan, A. Shann Yue Cheung, *Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong*, „International Journal of Environmental Research and Public Health" 2018, vol. 15; D.K. Citron, *Hate Crimes in Cyberspace*, Harvard University Press, Cambridge 2014; D.M. Douglas, *Doxing: a Conceptual Analysis*, „Ethics and Information Technology" 2016, vol. 18, no. 3; L. Gao, J. Stanyer, *Hunting Corrupt Officials Online: The Human Flesh Search Engine and the Search for Justice in China*, „Information, Communication & Society" 2014, vol. 17, iss. 7; J. Idzik, R. Klepka, *Doxing*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; G.T. Marx, *What's in a Name? Some Reflections on the Sociology of Anonymity*, „The Information Society" 1999, vol. 15, iss. 2; D. Trottier, *Denunciation and Doxing: Towards a Conceptual Model of Digital Vigilantism*, „Global Crime" 2019.

DRONY ALBO BEZZAŁOGOWE STATKI POWIETRZNE (UAV) – powszechnie znane jako drony, można wyróżnić drony bojowe i drony konsumenckie.

Cambridge English Dictionary przedstawia 2 definicje dronów:

- statek powietrzny, który nie ma pilota, ale jest kontrolowany przez kogoś na ziemi i jest wykorzystywany przede wszystkim do zrzucania bomb lub nadzoru/obserwowania danego miejsca;
- samolot bez pilota, który jest kontrolowany przez kogoś na ziemi i jest używany w ramach czyjegoś hobby.

Definicje te są bardzo przydatne, ponieważ określają także główne zastosowania dronów. Drugą z nich można by poszerzyć o różne sposoby wykorzystania statków bezzałogowych, które pojawiły się niedawno, takie jak → b e z p i e c z e ń s t w o [t. 1], transport i dostawa itd. Nie ma jednego określenia nazwy samolotu bez pilota, w użyciu funkcjonują różne nazwy:

- UAV (ang. *Unmanned Aerial Vehicle*) – bezzałogowy statek powietrzny;

- UAS (ang. *Uninhabited Aircraft Systems*) – bezzałogowy system powietrzny;
- RPA (ang. *Remotely Piloted Aircraft*) – zdalnie sterowany samolot;
- RPAS (ang. *Remote Piloted Aircraft System)* – zdalnie sterowany system samolotowy.

Drony i UAV/UAS są powszechnie używane w zastosowaniach wojskowych, natomiast RPA/RPAS to drony użytkowane w celach cywilnych. Według raportów różnych organizacji zajmujących się analizą globalnego rynku dronów globalny rynek technologii UAS przekroczył wartość 2 mld USD w 2015 r.; 14 mld w 2018 r.; 22,5 mld USD w 2020 r., natomiast w latach 2024–2025 osiągnie ok. 43 mld USD. Ostatnie badania dotyczące przyszłości robotyki i → sztucznej inteligencji [t. 4] wykazały, że pojawienie się „inteligentnych maszyn" doprowadzi do kolejnej rewolucji przemysłowej. Szacuje się, że inteligentne maszyny i roboty będą wykonywać 45% całej produkcji do 2025 r. (w porównaniu do ok. 10% w 2016 r.). Globalne komercyjne wydatki na robotykę przemysłową sięgają ponad 43 mld USD rocznie. Ostatnie badanie przeprowadzone przez Bank of America szacuje, że całkowita wartość rynku robotyki przemysłowej wzrośnie do 127 mld USD do 2025 r.

Drony umożliwiają autonomiczne pozyskiwanie obrazów o wysokiej rozdzielczości przestrzennej (ang. *spatial resolution*) i czasowej (ang. *temporal resolution*), a także są bardzo tanie w porównaniu z innymi źródłami zdalnego gromadzenia takich obrazów (np. zdjęcia satelitarne lub załogowe zdjęcia lotnicze). Wysoka wydajność statków bezzałogowych jest wynikiem dywersyfikacji i miniaturyzacji czujników i kamer, w które mogą być wyposażone drony (np. globalny system pozycjonowania, inercyjny system nawigacji, cyfrowe RGB, kamery wielospektralne i hiperspektralne, czujniki temperatury, radar, LiDAR).

Drony komercyjne są obecnie wykorzystywane przez korporacje, rządy i środowisko akademickie do różnych celów (np. pomoc humanitarna, rolnictwo precyzyjne, ochrona biologiczna, archeologia, wydobycie, planowanie urbanistyczne, nadzór), pomimo obaw dotyczących etyki, bezpieczeństwa i prywatności.

Pierwszy patent na „Metodę i aparaturę do sterowania mechanizmem poruszających się statków lub pojazdów" (US Patent 0613809) został

złożony przez N. Teslę w 1898 r. Obecnie zgłaszane są różne patenty, takie jak drony bez śmigła lub drony zdolne do działania w środowisku wodnym, co pokazuje, jak interesująca może być branża dla nowych firm i jak ciekawe mogą być nowe pomysły biznesowe.

Autonomiczna broń była używana od czasów II wojny światowej (np. pasywny akustyczny celownik niemieckiej torpedy). Jeszcze w 1925 r. Brytyjczycy opracowali wyposażony w autopilota bezzałogowy samolot o nazwie Larynx (ang. *Long Range Gun with Lynx Engine*), który był bronią przeciwko jednostkom pływającym. Stosowane później w wojskowości latające bomby czy też pociski manewrujące także można zaliczać do bezzałogowych statków powietrznych. W kolejnych latach wysiłki skierowano na opracowanie możliwości zdalnego sterowania takimi jednostkami drogą radiową. Doskonalono konstrukcje dronów służących do szkolenia wojsk przeciwlotniczych. Doświadczenia te wykorzystano podczas II wojny światowej. W tym okresie podjęto prace nad dronami szpiegowskimi, które powszechnie zaczęto wykorzystywać w latach 60. i 70. XX wieku. Pod koniec lat 50. XX wieku firma Gyrodyne Company of America skonstruowała pierwszy bezzałogowy śmigłowiec QH-50 DASH, którego używano do celów bojowych jako niszczyciela łodzi podwodnych (ang. *Drone Anti-Submarine Helicopter*).

Nadzorowane przez człowieka zautomatyzowane systemy obronne istnieją od dziesięcioleci, a drony lotnicze zostały po raz pierwszy użyte ponad 20 lat temu. Dopiero po 11 września 2001 r. pojawiło się rosnące zainteresowanie wojska bezzałogowymi statkami powietrznymi. W ciągu zaledwie 10 lat liczba rodzajów samolotów bezzałogowych wzrosła ze 163 w 2003 r. do prawie 11 tys. w 2013 r. (w 2013 r. drony stanowiły 40% wszystkich samolotów). W XXI w. co najmniej 30 krajów zaczęło produkcję i wykorzystanie dużych dronów wojskowych. W związku z tym rośnie nacisk na opracowywanie nowych, bardziej autonomicznych systemów, które są lepiej przygotowane do przetrwania w przestrzeni powietrznej.

Według raportu firmy Tractica *Consumer Drones* sprzedaż dronów będzie rosła w ciągu najbliższych kilku lat, a globalne roczne zamówienia jednostkowe wzrosną ponad dziesięciokrotnie z 6,4 mln w 2015 r. do 67,9 mln w 2021 r. Podczas gdy średnie ceny sprzedaży dronów w tym okresie nadal będą gwałtownie spadać, łączne przychody wzrosną z 1,9 mld USD

w 2015 r. do 5 mld USD w 2021 r. Wiele czołowych firm inwestuje w technologie dronów klasy konsumenckiej, których możliwości sprzętowe i programowe z biegiem czasu stają się coraz bardziej niezawodne, umożliwiając nowe zastosowania dla konsumentów.

Wojsko znajduje się na zakręcie wielkiej rewolucji technologicznej, wkraczając w nowy wiek robotyzacji, gdy → w o j n y [t. 4] są prowadzone przez bezzałogowe i coraz bardziej autonomiczne systemy broni działające we wszystkich dziedzinach (powietrze, morze, ląd, przestrzeń kosmiczna) oraz w całym spektrum operacji wojskowych.

Bezzałogowe statki powietrzne to sektor lotnictwa, który rozwija się bardzo szybko i ma ogromny potencjał tworzenia wzrostu gospodarczego i nowych miejsc pracy w najbliższych latach: w USA przewiduje się utworzenie 100 tys. miejsc pracy do 2025 r., w Europie 150 tys. miejsc pracy do 2050 r. W określeniu „bezzałogowy statek powietrzny" zawierają się zarówno duże samoloty, podobne pod względem wielkości i złożoności do samolotów załogowych, jak i małe urządzenia elektroniczne do użytku osobistego. Technologie z użyciem dronów:

- służą ochronie granic, obiektów infrastruktury wrażliwej, takich jak kolej, kanały, linie energetyczne, rurociągi i autostrady;
- wspomagają ochronę morskich interesów ekonomicznych państwa;
- ułatwią monitoring lasów, miast czy skażeń środowiskowych;
- są wykorzystywane w gospodarstwach rolniczych do dokładnego, terminowego i efektywnego stosowania nawozów i pestycydów;
- są używane do monitorowania zasobów naturalnych, ochrony środowiska, badań atmosferycznych;
- są wykorzystywane w mediach i rozrywce, np. przy wykonywaniu fotografii, relacjonowaniu wiadomości czy robieniu zdjęć do filmów przyrodniczych itp.

W przyszłości drony mogłyby podnosić gigantyczne turbiny wiatrowe wytwarzające „zieloną" energię elektryczną. Inżynierowie pracują również nad mikrodronami, które mogłyby walczyć z lokalnymi wyciekami gazu i chemikaliów, a także mogłyby być zaprogramowane jako pszczoły w celu sztucznego zapylania roślin.

USA i Izrael dominują w sektorze bezzałogowych technologii militarnych. Chiny bezsprzecznie królują na rynku dronów rekreacyjnych

i zabawkowych. Unia Europejska stawia natomiast na cywilne i tzw. rządowe zastosowania bezzałogowców. To rolnictwo precyzyjne, geoinformacja, poszukiwanie i ratownictwo, inspekcja infrastruktury, ochrona środowiska czy też proces likwidacji szkód niezbędny do wypłaty odszkodowań. Łączy je pozyskiwanie danych i ich analiza.

Wraz z rozwojem nowych technologii zmieniały się możliwości wykorzystywania dronów. Siły zbrojne były głównym twórcą idei bezzałogowych statków powietrznych. Postęp technologiczny pozwala na wykorzystanie dronów podczas różnego typu akcji poszukiwawczo-ratowniczych, a także w czasie klęsk żywiołowych. Szybkość i niezawodność działań może w przyszłości skutkować zwiększeniem bezpieczeństwa oraz wzrostem liczby osób ocalałych w różnych zdarzeniach i wypadkach. Tak samo jak technologie internetowe na początku lat 90. XX w. doprowadziły do wypracowania ich wielu różnych zastosowań, technologie zdalnie sterowanych systemów awiacyjnych (ang. *Remotely Piloted Aircraft Systems*, RPAS) powinny skutkować w najbliższych latach wytworzeniem szerokiej gamy usług, w szczególności w połączeniu z innymi technologiami, takimi jak precyzyjne pozycjonowanie z wykorzystaniem systemu nawigacji satelitarnej Galileo, w powiązaniu z systemami telekomunikacyjnymi w celu zapobiegania i łagodzenia skutków klęsk żywiołowych, dynamicznego zwiększania przepustowości sieci komunikacyjnych. Chociaż dokładny charakter i zakres potencjalnego wykorzystania RPAS obecnie są trudne do przewidzenia, oczekuje się, że przemysł będzie generować przychody wystarczające do szybkiego rozwoju branży.

Szczególnie szybko rozwija się sektor małych dronów. W kwietniu 2014 r. Komisja Europejska przyjęła apel do Parlamentu Europejskiego i Rady *A New Era for Aviation. Opening the Aviation Market to the Civil Use of Remotely Piloted Aircraft Systems in a Safe and Sustainable Manner*. Jak stwierdzono w tym dokumencie, RPAS będą mogły oferować „mnóstwo nowych usług", znacząco zmieniając nasze codzienne życie. Należy podkreślić, że w ostatnim czasie zamiast drogich i wysokotechnologicznych dronów wykorzystuje się więcej tanich i uproszczonych, których strata podczas wykonywania zadań nie jest tak istotna przy ich pomyślnej realizacji. W przypadku awarii jednego lub więcej dronów są one zastępowane przez podobne z tego samego „roju" lub przez uruchomienie

dodatkowych urządzeń. Każdy z dronów w takim systemie utrzymuje połączenie z innymi UAV. Nie ma tam lidera lub dowódcy, pozwala się rojowi z powodzeniem przetrwać utratę niektórych dronów i nadal wykonywać skoordynowane działania, często opierające się na mapie neuronowej. Drony w takim systemie współpracują ze sobą w obrębie „roju" i nie powinny generować konfliktowych sytuacji, w których zadania jednostek w jakiś sposób kolidują ze sobą bądź w których utrata jednego statku uniemożliwia realizację działań. Każda grupa UAV (subrój) w „roju" wykonuje niezależne zadania (pomiar różnych parametrów, nagrywanie wideo, opryskiwanie poszczególnych części roślin itd.) i jest połączona tzw. umysłem zbiorowym (ang. *hive mind*). Przewiduje on skoordynowane działania wielu dronów, które lokalnie wchodzą w interakcje ze sobą i otoczeniem. Chociaż każdy dron działa wg prostych zasad, to system w całości demonstruje niezwykle złożone wspólne zachowanie. Działa jako jeden duży organizm.

Drony stają się integralną częścią życia, a sposoby ich wykorzystania będą determinować zarówno postęp, jak i → z a g r o ż e n i a [t. 4] dla społeczeństwa. Amerykański płk A. Tingle i pilot D. Tyree, autorzy publikacji dotyczącej wykorzystania dronów, twierdzą, że system małych bezzałogowych statków powietrznych jest destrukcyjną technologią komercyjną, która jest natrętna, niewykrywalna i potencjalnie śmiercionośna, a także naruszająca prywatność. UAV są unikalnym i obecnie niezidentyfikowanym zagrożeniem dla → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1], o czym świadczy raport amerykańskiej komisji senackiej ds. handlu, nauki i transportu na temat incydentów z udziałem dronów. Ostatnio Federalna Administracja Lotnictwa USA (Federal Aviation Administration, FAA) otrzymuje do 100 raportów miesięcznie o bezprawnych działaniach dronów.

UAV zakwestionowały istniejące doktryny obrony przeciwlotniczej i stworzyły precedens dla bardzo udanego zastosowania militarnego technologii komercyjnej. Chociaż – tak jak w przypadku każdej nowej technologii – możliwości związane z wykorzystaniem wojskowym nie zostały jeszcze w pełni odkryte, ostatnie wydarzenia wskazują na potencjalne niebezpieczeństwo. We wrześniu 2013 r. drony unosiły się w pobliżu twarzy niemieckiej kanclerz A. Merkel, gdy ta wygłaszała kampanijne przemówienie. W styczniu 2015 r. dron wylądował, początkowo niewykryty, na

trawniku przy Białym Domu. Warmińsko-Mazurski Oddział Straży Granicznej, odpowiedzialny za ochronę granicy polsko-rosyjskiej, informował o 5 wykrytych wzrokowo bezzałogowcach w 2016 r. – bezzałogowce pojawiały się w okolicy Grzechotek, Bezled i Gołdapi. Najgłębiej nad polskim terytorium był dron zauważony pod Bezledami, w odległości ok. 1 km. Pozostałe to przypadki naruszenia pasa granicznego na głębokość od 50 do 200 metrów. Patrole nie zawsze patrzą w niebo, drony mogą operować nocą, co utrudnia ich wykrycie wzrokowe – nawet w dzień niewielki obiekt lecący nisko nad lasem niełatwo wypatrzeć. Straż Graniczna ma na wyposażeniu radary, ale akurat nieprzeznaczone do dozoru przestrzeni powietrznej. Te zadania ma wykonywać wojsko, a zgodnie z ustawą strażnicy graniczni są tylko pośrednikami w przekazywaniu informacji o naruszeniach granicy powietrznej RP. Te przykłady podkreślają uciążliwość, niewykrywalność i potencjalną śmiercionośność dronów.

Podstawowa struktura fizyczna UAV (w tym wykorzystanie zaawansowanych materiałów) utrudnia działanie technologii radarowych, podstawowego składnika nowoczesnej obrony powietrznej. Radar działa poprzez odbijanie energii od obiektów znajdujących się w powietrzu i interpretację odbić powrotnych. Chociaż nowoczesna technologia radarowa ma zdolność śledzenia małych obiektów, trudno jest odróżnić drony od innych obiektów znajdujących się w powietrzu, zwłaszcza ptaków. Zastosowanie w obronie powietrznej tablic z akceleracją akustyczną i kamer elektrooptycznych wydaje się obiecujące, ale może wymagać połączenia wszystkich technologii śledzenia i identyfikacji w celu ochrony przed rosnącymi zagrożeniami dronów.

Przyszłe osiągnięcia w materiałoznawstwie i naukach komputerowych pozwolą UAV na samodzielne działanie, zwiększając ich skuteczność jako broni ofensywnej. Jedną z cech UAV jest to, że wyjątkowo dobrze nadają się one do zaawansowanych taktyk walki powietrznej. Wraz z dalszą automatyzacją pola bitwy siły zbrojne będą mogły wykorzystywać mnóstwo dronów w skoordynowanych formacjach znanych jako „roje dronów". Ta taktyka mogłaby utrudnić obronę, szczególnie w przypadku dużych lub nieruchomych obiektów.

Drony są aktywnie wykorzystywane w celach komercyjnych, nie potrzebują pasów startowych, wejście w atmosferę zajmuje kilka minut,

start może się odbyć w bezpośrednim sąsiedztwie obiektu. Bardzo ważne dla ochrony przed zagrożeniami ze strony dronów jest opracowanie skutecznego systemu wykrywania, śledzenia i identyfikacji.

Jak donosi „The Verge", powołując się na raport „USA Today", drony to narzędzie coraz częściej używane do przemytu różnego rodzaju nielegalnych towarów, m.in. na tereny więzień. Latające maszyny dostarczają tam towary zakazane – narkotyki, broń, telefony i pornografię. Biorąc pod uwagę fakt, że niewykrytych przemytów tą drogą jest zapewne znacznie więcej niż przypadków raportowanych, a namierzenie i złapanie przemytnika (osoby sterującej dronem) jest trudne, problem wydaje się bardzo poważny. W związku z tym Amerykanie pracują nad technologią, która będzie w stanie zapobiec tego typu procederom. Przemyt za pomocą dronów to problem nie tylko amerykańskich więzień. Przypadki takiej kontrabandy wykrywano również w Australii i Meksyku.

W związku z dynamicznym rozwojem niektórych rodzajów statków powietrznych, w szczególności w obszarze lotnictwa sportowego i rekreacyjnego, klasyfikacja statków powietrznych stała się nieaktualna i niekompletna. Nowe rozporządzenie w tej sprawie weszło w życie w 2012 r., a w 2017 r. pojawiła się nowa klasyfikacja, która umożliwi dokonywanie precyzyjnych zapisów w procesach sądowych i dokumentacji związanej z rejestracją lub ewidencjonowaniem statków powietrznych, określającej także ich zdatność do lotu oraz specyfikację techniczną.

Biorąc pod uwagę różnorodność UAV, ważne jest, aby je klasyfikować. Na podstawie znanych charakterystyk taktycznych i technicznych istniejących dronów można je porządkować wg głównych cech: wykorzystania; rodzaju systemu kontroli; zasady lotu; klasy; typu; typu skrzydła; sposobu startu/lądowania; typu silnika; układu paliwowego; rodzaju zbiornika paliwa; liczby zastosowań; kategorii (biorąc pod uwagę masę i maksymalny zakres działania); zakresu działania; osiągalnego pułapu wysokości; celu funkcjonalnego.

11 czerwca 2019 r. zostały opublikowane 2 rozporządzenia unijne dotyczące dronów, które ostatecznie ujednoliciły prawo na terenie Unii Europejskiej. Mowa o Rozporządzeniu delegowanym Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw

trzecich oraz o Rozporządzeniu wykonawczym Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych. Przepisy weszły w życie na początku lipca 2019 r., a państwa członkowskie będą miały rok na ich wdrożenie i wskazanie ew. odstępstw tak, aby do czerwca 2021 r. zunifikowane europejskie przepisy zaczęły obowiązywać w całej UE. Nadrzędnym celem wprowadzenia nowych regulacji jest zapewnienie wspólnego bezpieczeństwa operacji UAV oraz ochrona prywatności obywateli UE, a jednocześnie umożliwienie swobodnego dostępu do przestrzeni powietrznej dla dronów.

Rozporządzenie określa wspólne zasady bezpieczeństwa w lotnictwie cywilnym oraz zmienia mandat Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego (ang. European Union Aviation Safety Agency, EASA). Zgodnie z rozporządzeniem EASA nowe przepisy wprowadzają podstawowe zasady bezpieczeństwa, prywatności i ochrony danych osobowych. Mają też ograniczyć biurokrację i sprzyjać innowacyjności. Nowy dokument zastępuje ramy legislacyjne z 2008 r. Od 1 lipca 2020 r. przepisy nakładają obowiązek rejestracji dronów o masie powyżej 250 g. Pojawiły się 3 nowe kategorie zdefiniowane wg cech drona i celu jego użycia:

- „otwarta" (ang. *open*) – operacje wykonywane z użyciem bezzałogowego systemu powietrznego w tej kategorii nie będą wymagały uzyskania zezwolenia na lot ani posiadania licencji przez operatora; w tej kategorii znajdzie się większość dronów poniżej 250 g, wykorzystywanych do celów rekreacyjnych, które ze względu na charakter operacji nie będą wymagały oceny ryzyka;
- „szczególna" (ang. *specific*) – w tej kategorii operacje wykonywane z użyciem bezzałogowego systemu powietrznego będą wymagały uzyskania zezwolenia na lot wydanego przez właściwy organ; będzie wymagana ocena ryzyka; w tej kategorii najprawdopodobniej znajdą się wszystkie firmy usługowe, które wykonują płatne usługi na podstawie świadectwa kwalifikacji wydawanego przez Urząd Lotnictwa Cywilnego (ULC);
- „certyfikowana" (ang. *certified*) – w tej kategorii będzie wymagana certyfikacja bezzałogowego systemu powietrznego na podstawie rozporządzenia UE 2019/945 i certyfikacja operatora oraz,

w stosownych przypadkach, uzyskanie licencji przez pilota bezzałogowego statku powietrznego.

Zgodnie z prawem europejskim korzystanie z dronów nie powinno skutkować naruszeniem praw podstawowych, w tym poszanowania życia prywatnego i rodzinnego, a także ochrony danych osobowych. W USA wykorzystanie bezzałogowych samolotów jest regulowane przez FAA, zgodnie z kodeksem Code of Federal Regulations 14 CFR. W 2015 r. FAA przyjęła akt ustawodawczy, znany jako Part 107, nakładający obowiązek rejestracji wszystkich UAV. Zgodnie z kodeksem model lotniczy jest uznawany za dron, spełniając następujące kryteria:

- jest traktowany jako hobby lub do rozrywki;
- nie narusza lokalnych zasad bezpieczeństwa;
- waży nie więcej niż 55 funtów (25 kg) lub, w przypadku większej masy, przeszedł odpowiednią certyfikację;
- nie przeszkadza żadnemu załogowemu statkowi powietrznemu;
- w przypadku lotu w promieniu 5 mil (8 km) od portu lotniczego operator lotniska i wieża kontrolna muszą zostać ostrzeżone z wyprzedzeniem.

W UE przemysł UAV otrzymuje poważne wsparcie. Komisja Europejska wspiera rozwój rynku RPAS i konkurencyjnych rozwiązań w powiązanych sektorach przemysłu, w tym małych i średnich przedsiębiorstw oraz przedsiębiorstw rozpoczynających działalność. To szansa na zwiększenie dynamiki rozwoju rynku, jedno z wyzwań technologicznych mających ratować starą Europę w konkurencji globalnej, element → s t r a t e g i i [t. 4] Jednolitego Rynku Cyfrowego (Digital Single Market). Warto też zwrócić uwagę, że spora część unijnych programów badawczych, np. finansowanych w ramach programu Horyzont 2020, jest ukierunkowana na sektor militarny. Pokazuje to, że zastosowania wojskowe w dalszym ciągu napędzają rozwój technologiczny dronów. Strategiczny wymiar wyzwań dla rynku dronów oznacza, że firmy muszą wykazać przydatność nowej technologii zarówno przed potencjalnymi klientami, jak i inwestorami.

Obok USA i Izraela Polska jest jednym z trzech głównych ośrodków projektujących i produkujących drony. Wartość rynku produkcji dronów o zastosowaniu zarówno cywilnym, jak i wojskowym w Polsce szacuje się

na 201,31 mln złotych za 2016 r., co oznacza wzrost o 22,75% w stosunku do 2015 r. (o 164 mln złotych). Większość przychodów wygenerowała sprzedaż sprzętu rekreacyjnego i przeznaczonego dla profesjonalnej fotografii i filmu oraz usługi, w tym szkolenia na licencjonowanych operatorów bezzałogowców. Z → i n f o r m a c j i Komisji Europejskiej wynika, że już za 10 lat drony cywilne będą stanowić 10 proc. światowego rynku lotniczego, a jego wartość wzrośnie do 15 mld EUR. Firmy związane z tą branżą odnotowują liczne sukcesy.

Jednak przemysł systemów bezzałogowych to nie tylko maszyny latające. Ciekawym rozwiązaniem jest polski system antydronowy. SafeSky wykryje drona, a w razie potrzeby go zneutralizuje. Systemem są już zainteresowane duże firmy, lotniska, a także → s ł u ż b y s p e c j a l n e [t. 4]. SafeSky sprawdzi się w ochronie lotnisk, ale może mieć znacznie szersze zastosowanie. Już teraz szacuje się, że ok. 700 polskich firm realizuje różnego rodzaju oferty z wykorzystaniem dronów. Najczęściej są to usługi związane z robieniem zdjęć albo kręceniem filmów. Według danych ULC w Polsce na komercyjne użycie dronów zgodę posiada prawie 3 tys. osób. Drony stały się dostępne niemal dla każdego. Liczba tych maszyn powiększa się w lawinowym tempie – mówi się o przyroście nawet 30% w skali roku. Tylko w 2016 r. Polacy wydali 100 mln zł na lekkie modele rekreacyjne oraz półprofesjonalne, służące do robienia zdjęć. Z badań ankietowych ULC wynika, że wszystkich użytkowników dronów jest kilkadziesiąt tysięcy.

Znaczenie dronów jest już olbrzymie, a może być tylko większe. Jest to zupełnie nowa gałąź technologii, która może znacząco wzmocnić gospodarkę w wielu obszarach – w infrastrukturze, rolnictwie, budownictwie czy energetyce. Są to obszary, w których wydaje się największe pieniądze i gdzie znajduje się potencjał rozwojowy Polski na najbliższe lata. Co więcej, wskazane obszary mogą rozwijać się synergicznie wraz z technologią dronów.

Podsumowując, drony są coraz bardziej popularne. Zamiast o 2 segmentach ich wykorzystania – wojskowym i rekreacyjnym – można mówić o segmencie wojskowym, komercyjnym i rekreacyjnym. Chociaż główny udział w rynku ma pierwszy z nich, pozostałe 2 będą się rozszerzać w ciągu najbliższych lat.

Komisja Europejska przewiduje, że do 2035 r. europejski sektor dronów:

- będzie bezpośrednio zatrudniał ponad 100 tys. osób;
- będzie miał oddziaływanie ekonomiczne rzędu ponad 10 mld EUR rocznie, głównie w usługach.

Wraz z upowszechnianiem się dronów wzrośnie również konieczność odpowiedniego wyważenia korzyści i wyzwań, które ów sektor niesie. UAV mogą np. być przydatne do gromadzenia i interpretowania danych w różnych obszarach gospodarki, ale mogą też powodować problemy związane z ochroną danych, ochroną prywatności, hałasem i emisją CO_2.

Obecne nowoczesne możliwości UAV są wystarczająco groźne, a my jesteśmy na krawędzi postępu technologicznego, który uczyni z dronów bardziej zabójczą broń. Asymetryczny charakter ich działań, szczególnie w przypadku taktyki roju, sprawia, że obrona przed tą technologią jest trudna. UAV są stosunkowo niedrogie i wszechobecne (szacuje się, że tylko w USA jest ponad milion dronów). Zarazem większość systemów obronnych jest – przynajmniej na tym etapie rozwoju – zbyt kosztowna. Ponadto w miarę rozwoju najnowocześniejszych technologii, takich jak obecne komercyjne systemy operacyjne, niewielkie postępy w zakresie technologii wspomagających przyniosą ogromne skoki naprzód w zakresie technologii UAV, co dodatkowo pogłębi takie problemy obronne, jak wykrywanie i identyfikacja. Aby uchronić się przed tym zagrożeniem, należy opracować doktryny zarówno dotyczące ataku dronów, jak i obrony przed nimi.

W historii wojen istniało niewiele czysto komercyjnych technologii, które tak łatwo nadają się do natychmiastowego uzbrojenia jak drony. Zagrożenie leży nie tylko w samej technologii, ale także w stopniu, w jakim jest ona skuteczna i dostępna dla wszystkich potencjalnych aktorów. Właśnie komercyjna dostępność zaawansowanej technologii tworzy prawdziwe zagrożenie i ta nowa technologiczna granica może stanowić największe przyszłe wyzwanie dla bezpieczeństwa narodowego.

Olga Wasiuta

R. Clarke, L. Bennett Moses, *The Regulation of Civilian Drones Impacts on Public Safety*, „Computer Law & Security Review" 2014, vol. 30; *Drone Market Outlook: Industry Growth Trends, Market Stats and Forecast*, 3.03.2020, BuisnessInsider.com

(dostęp 5.08.2020); *Drony a prawo unijne*, SwiatDronow.pl (dostęp 25.02.2020); A. Ilachinski, *AI, Robots, and Swarms Issues, Questions, and Recommended Studies*, CNA, Washington 2017; K. Juszczyk, S. Kosieliński, P. Rutkowski, *Gdzie jesteśmy, dokąd idziemy*, [w:] *Rynek dronów w Polsce. Edycja 2017*, S. Kosieliński (red.), Instytut Mikromakro, Warszawa 2016; R. Kopeć, O. Wasiuta, T. Wójtowicz, *Wojna dronów. Militarne wykorzystanie bezzałogowych statków powietrznych*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2020; S. Kosieliński, *Świt w dolinie śmierci*, [w:] *Rynek dronów w Polsce. Edycja 2017*, S. Kosieliński (red.), Instytut Mikromakro Warszawa 2016; J. Merkisz, A. Nykaza, *Perspektywy rozwoju i wykorzystania bezzałogowych statków powietrznych w służbach ratowniczych*, „Bezpieczeństwo i Ekologia" 2016, nr 6; Rada Europejska, Rada Unii Europejskiej, *Drony: reforma unijnego bezpieczeństwa lotniczego*, Consillium.Europa.eu/pl; T. Rahman, M. Hariadi, S. Sumpeno, *NCP Striking Pattern in Combat Situation Using Boids Behaviour*, „Intelligent technology and its application": IEEE international seminar, Surabaya, Indonesia, 22–24 May, 2014; Rozporządzenie wykonawcze Komisji (UE) 2017/285 z dnia 15 lutego 2017 r. dotyczące klasyfikacji niektórych towarów według Nomenklatury scalonej. Dziennik Urzędowy Unii Europejskiej 18.2.2017 Pl; K. Siadkowska, *Prawne aspekty eksploatacji dronów*, „Studia Iuridica Lublinensia" 2017, vol. 26, nr 3; M. Szymczak, *Perspektywy rozwoju technologii i rynku dronów*, [w:] *E-mobliność: wizje i scenariusze rozwoju*, J. Gajewski, W. Paprocki, J. Pieriegud (red.), Centrum Myśli Strategicznych, Sopot 2017; *The Drone Market: Insights from Customers and Providers*, 2019, Comptia.org (dostęp 5.08.2020); *The Drone Market Report 2020–2025*, 4.05.2020, Droneii.com (dostęp 5.08.2020); *The US Drone Market Report 2019–2024*, 27.05.2019, Droneii.com (dostęp 5.08.2020); Urząd Lotnictwa Cywilnego, *Wdrażanie przepisów UE*, ULC.gov (dostęp 25.02.2020); R. Wallace, J. Loffi, *Examining Unmanned Aerial System Threats and Defenses: A Conceptual Analysis*, „International Journal of Aviation, Aeronautics, and Aerospace" 2015, no. 4; O. Wasiuta, *Drony*, [w:] *Vademecum bezpieczeństwa*, Wydawnictwo Libron, Kraków 2018.

DRONY ROZPOZNAWCZE – bezzałogowe statki powietrzne, których celem jest zbieranie i dostarczanie → i n f o r m a c j i przy wykorzystaniu zamontowanych urządzeń pokładowych. Kontrola nad nimi może odbywać się z dowolnego miejsca przy użyciu dostępnych technologii komunikacji (łączności radiowej, mikrofalowej, satelitarnej, optycznej i in.). Mogą poruszać się po zaplanowanej wcześniej trasie lub pomiędzy wyznaczonymi punktami z różnym poziomem autonomiczności (samodzielny wybór trasy, unikanie wyznaczonych obszarów, wykrywanie i unikanie

→zagrożeń [t. 4] zarówno naturalnych, jak i cywilizacyjnych i in.). W zależności od zamontowanego oprzyrządowania →drony mogą prowadzić rozpoznanie obrazowe (fotograficzne, wideo, w podczerwieni lub termowizji, radarowe), elektroniczne (nasłuch łączności radiowej), a zbierane informacje mogą być przekazywane w czasie rzeczywistym poprzez łącza bezprzewodowe do operatorów, sztabów oraz oddziałów operujących na danym obszarze. Drony zawsze są tylko częścią większego systemu, w skład którego wchodzi także system nawigacji i łączności oraz stacja naziemna (ang. *Ground Control Station*, GCS).

Samo określenie dron odnosi się do platformy latającej wraz z opcjonalnym wyposażeniem i może być zamiennie używane z określeniami takimi jak BSP (bezpilotowy statek powietrzny), UAV (ang. *Unmanned Aerial Vehicle*). Drony są klasyfikowane wg różnych kryteriów. Klasyfikacja używana przez →NATO [t. 3] została opracowana w oparciu o prace grupy JCGUAV (Joint Capability Group On Unmanned Aerial Vehicles), a jej celem było uproszczenie podziału BSP i uzyskanie zgodności dokumentacji w zakresie ruchu lotniczego pomiędzy krajami sojuszniczymi. Głównymi determinantami klas są promień działania i maksymalny pułap operacyjny, a dodatkowymi czynnikami są masa BSP i długotrwałość lotu:

- Klasa 1 obejmuje urządzenia o masie startowej do 150 kg, działające w zasięgu łącza (ang. *line-of-sight*) na poziomie plutonu/kompanii/batalionu. Są one na tyle małe, że mogą startować bezpośrednio z podłoża, z niewielkich wyrzutni pneumatycznych lub poprzez wyrzut z ręki operatora. Ich głównym zadaniem jest obserwacja i rozpoznanie realizowane w czasie rzeczywistym, dzięki czemu mogą wspomagać funkcjonowanie batalionu na jego obszarze działania.
- W klasie 2 zebrano taktyczne BSP, które służą do wsparcia działań na poziomie brygady. Ich masa startowa wynosi od 150 do 600 kg, dzięki czemu oprócz urządzeń do obrazowania w dzień i w nocy (radary SAR oraz I-SAR) mogą przenosić również uzbrojenie, czas ich lotu może wynieść do 24 godzin.
- W klasie 3 znajdują się BSP o największej masie startowej, a co za tym idzie największych możliwościach przenoszenia. Są to konstrukcje o masie ponad 600 kg i nieograniczonym promieniu

działania (ang. *beyond line-of-sight*). Ich zadania to obserwacja i rozpoznanie, ale również działania bojowe, czas ich przebywania w powietrzu może wynosić 24–48 godzin, a nawet dłużej (np. Zephyr – 336 godzin w powietrzu). W tej klasie możemy wyróżnić takie podklasy jak Medium Altitude Long Endurance (MALE), czyli BSP o średnim pułapie i dużej długotrwałości lotu, poruszające się na pułapie do 13 km, działające na szczeblu operacyjnym (korpus/dywizja), oraz High Altitude Long Endurance (HALE), czyli BSP o dużym pułapie i dużej długotrwałości lotu, których pułap operacyjny wynosi nawet 19,5 km i które działają na szczeblu strategicznym.

W Polsce BSP weszły do użytku militarnego stosunkowo niedawno – pierwsze z urządzeń zostały wprowadzone do użycia w 2005 r. Obecna klasyfikacja została stworzona na potrzeby Sztabu Generalnego Wojska Polskiego w 2012 r. na podstawie założeń zawartych w Programie operacyjnym do prowadzenia rozpoznania obrazowego w latach 2013–2022, a głównym parametrem był promień działania BSP:

- do klasy I, z racji nieograniczania masy startowej maszyn, zaliczamy zarówno takie urządzenia jak ważący 16 g i mieszczący się w kieszeni PD-100 Black Hornet produkcji Proxy Dynamics, jak i rodzimy produkt Drozd z Wojskowych Zakładów Lotniczych nr 2, ważący 25 kg i mający 3,8 metra rozpiętości skrzydeł. Klasa ta skupia wszystkie systemy o zasięgu do 30 km. Oczywisty rozdział ze względu na oznaczenie (mikro i mini) pozwala na dokładniejszą systematykę, dodatkowo wprowadza się jeszcze kategorię nanodronów;
- klasa II to BSP prowadzące rozpoznanie w promieniu do 200 km (kryptonimy Orlik i Gryf), co pozwala skutecznie koordynować ostrzał artyleryjski lub kontrolować strefy nadgraniczne. Wśród urządzeń spełniających te kryteria możemy wskazać wspólny projekt firm PIT-RADWAR oraz Eurotech, czyli E-310, a także Hermes-450 firmy Silver Arrow LP (Izrael), znacznie różniące się od siebie masą startową (od ok. 90 kg do ok. 550 kg);
- drony klasy III to nie tylko urządzenia służące do rozpoznania, ale również maszyny uzbrojone. Część urządzeń będzie wykorzystywana w ramach systemu NATO Alliance Ground Surveillance (AGS).

Historycznie, pierwszymi systemami rozpoznawczymi unoszącymi się w powietrzu były latawce i balony. Ich możliwości wykorzystywano m.in. w Chinach na przełomie III i II w. p.n.e. – były one używane m.in. jako rodzaj miary wypuszczanej w kierunku obleganej twierdzy, aby poprzez pomiar długości liny poznać długość koniecznego do wykopania tunelu, do mierzenia siły wiatru, a także jako metoda przekazywania widocznych z większej odległości sygnałów militarnych. Balonów rozpoznawczych z kolei używano począwszy od końca XVIII w. (w 1793 r. we Francji utworzono Pierwszą Kompanię Balonową), ale były to załogowe statki powietrzne. Balony bezzałogowe wykorzystywano za to, co prawda na niewielką skalę, do zadań uderzeniowych – balonów wypełnionych ładunkami wybuchowymi do ataków na formacje przeciwników użyto w czasie ataku Austrii na Wenecję w 1849 r. oraz podczas wojny secesyjnej (1861–1865).

Przełomem okazał się z jednej strony rozwój lotnictwa i powstanie pierwszych aerodyn (urządzeń cięższych od powietrza, w przeciwieństwie do aerostatów – balonów i sterowców) wyposażonych w napęd, a z drugiej rozwój technologii zdalnego sterowania (patent N. Tesli numer 613809 z 1898 r., wykorzystany początkowo do budowy zdalnie sterowanych jednostek pływających). Do rozwoju lotnictwa bezzałogowego przyczyniły się też wynalazki E.A. Sperry'ego, który opracował żyrokompas oraz mechanicznego autopilota. Pod koniec I wojny światowej Sperry wraz z C. Ketteringiem opracowali produkowany w niewielkich ilościach samolot zdalnie sterowany, nazywany Kettering Bug. Była to przeznaczona do celów uderzeniowych, przenosząca 81-kilogramową głowicę, „latająca bomba", a więc prekursor współczesnych pocisków manewrujących. Rozwój uderzeniowych bezpilotowych statków powietrznych przyspieszył podczas II wojny światowej, kiedy zastosowano bojowo konstrukcje takie jak amerykański TDR-1, używany w niewielkiej skali podczas walk na Pacyfiku w 1944 r., czy niemieckie zestawy Mistel, składające się z 2 samolotów, z których jeden pełnił funkcję stanowiska kierowania, a drugi bezzałogowej zdalnie sterowanej bomby latającej. Na dużą skalę używano niemieckich pocisków manewrujących V-1.

Początki zastosowania bezzałogowych statków powietrznych do zadań rozpoznawczych datują się na okres → z i m n e j w o j n y [t. 4]. Było to związane z rozwojem sensorów pokładowych, elektroniki i systemów

łączności i nawigacji. Podczas wojny w Wietnamie Amerykanie stosowali rozpoznawcze bezpilotowce rodziny Ryan 147, opracowane we wczesnych latach 60. jako rozwinięcie latających celów Firebee. W zależności od zabieranego wyposażenia były one wykorzystywane do celów rozpoznania fotograficznego z małej i dużej wysokości, rozpoznania elektronicznego i radioelektronicznego. Podczas konfliktu maszyny tego typu wykonały 3435 rozpoznawczych lotów bojowych. W 1963 r. do służby wprowadzono bezpilotowy śmigłowiec QH-50 DASH. Okazał się on jednak trudny w eksploatacji w pierwotnym zastosowaniu – jako operujący z pokładów okrętów nosiciel torped do zwalczania okrętów podwodnych – sprawdził się za to podczas konfliktu wietnamskiego w roli wyposażonego w kamerę telewizyjną aparatu rozpoznawczego (używanego m.in. do korygowania ognia → a r t y l e r i i [t. 1]).

Przełomem w rozwoju bezpilotowych statków powietrznych były doświadczenia izraelskie. W wojnie Jom Kippur w 1973 r. Izraelskie Siły Powietrzne poniosły znaczne straty, a oddziałom na lądzie brakowało efektywnego rozpoznania wizualnego. W rezultacie tych doświadczeń wypracowano spójną koncepcję zastosowania dronów w działaniach bojowych w synergii z lotnictwem załogowym, którą z powodzeniem wykorzystano podczas operacji Pokój dla Galilei w 1982 r. Izraelskie siły zbrojne wkroczyły do targanego wewnętrznymi konfliktami Libanu, a jednym z kluczowych zadań było zniszczenie ulokowanego w Dolinie Bekaa syryjskiego ugrupowania przeciwlotniczego, wspieranego przez syryjskie lotnictwo. Bezpilotowce Scout oraz Mastiff prowadziły rozpoznanie radiolokacyjne i elektrooptyczne z wysokości ok. 5 tys. m. Kolejnym stadium była pozoracja ruchu samolotów wykonywana przez BSP Samson z zamontowanymi odbijaczami radarowymi, co uaktywniało syryjskie stacje radarowe, które śledząc ruch Samsonów, zdradzały swoją pozycję, a ta była przekazywana przez Mastiffy do stanowisk dowodzenia. W efekcie siły izraelskie skutecznie poraziły wszystkie 19 syryjskich baterii rakiet przeciwlotniczych – 17 zostało zniszczonych, a 2 pozostałe poważnie uszkodzone. Trzeba zaznaczyć też, że izraelskie BSP, zwłaszcza Scout, na długie lata wyznaczyły standardy konstrukcyjne w tej klasie maszyn.

Izraelska taktyka i doświadczenia z użycia BSP zostały wykorzystane podczas operacji Pustynna Burza (1990–1991) – BSP Pioneer RQ-2

dostarczały informacje o rozmieszczeniu stanowisk irackiej artylerii i pól minowych, na ich podstawie dokonywano oceny skuteczności uderzeń własnej artylerii na obszarze do 30 km w głąb od linii walk. Również wprowadzone do służby BSL RQ-1 Predator pozwoliły na zwiększenie ilości informacji pozyskiwanych przez drony. RQ-1 Predator, wyposażany w system FLIR (Forward Looking Infrared), składający się m.in. z kamery termowizyjnej pozwalającej na operowanie w warunkach ograniczonej widoczności i przekazującej obraz z perspektywy pierwszej osoby (kamera dziobowa), mógł w czasie rzeczywistym przesyłać obraz wideo z miejsca operacji. Był także przystosowany do prowadzenia rozpoznania elektronicznego dzięki zastosowaniu czujników i wyposażenia pozwalającego na podsłuchiwanie łączności radiowej nieprzyjaciela. W trakcie operacji użyto również BSP FQM-151A Pointer, który służył do wykrywania umocnień oraz dostarczania wszelkich informacji na temat ruchu wrogich oraz własnych jednostek naziemnych. FQM-151A został wyprodukowany przez AeroVironment i rozpoczął służbę w Siłach Zbrojnych USA w 1990 r. Jego innowacyjność polegała na możliwości przesyłania obrazu w czasie rzeczywistym wprost do operatora. Napędzany 300-watowym silnikiem elektrycznym, miał możliwość pozostawania w powietrzu przez od 1 do 2 godzin w promieniu 5 km od operatora. Małe rozmiary BSP pozwalały na start z ręki operatora, a mała waga (ok. 22 kg, łącznie z osprzętem do sterowania) umożliwiała przenoszenie go przez oddział, dając szansę na użycie bezpośrednio na linii walk i dzięki temu dostarczając dowódcom lepszy ogląd sytuacji zarówno w dzień, jak i w nocy ze względu na przygotowanie do montażu kamery noktowizyjnej. Można go uznać za wzór dla m.in. maszyn Fly Eye, z których korzystają polskie jednostki → wojsk specjalnych [t. 4].

Konflikty lat 90. XX wieku na obszarze Bałkanów oraz w Czeczenii dały możliwość dalszego rozwoju BSP. Z węgierskiej bazy Taszar, 11. Ekspedycyjny Dywizjon Rozpoznawczy wyposażony w Predatory (RQ-1) wykonywał loty zwiadowcze na terenie Jugosławii. Oprócz Predatorów w konfliktach bałkańskich można było obserwować m.in. działania rosyjskiego BSP – Pczeła-1T (ros. Пчела-1Т). Zaprojektowana i produkowana w zakładach Jakowlewa konstrukcja była wystrzeliwana z platformy startowej ulokowanej na opancerzonym transporterze gąsienicowym BTR-D, a lądowała na

spadochronie po wykonaniu zadania, co uniemożliwiało szybkie przygotowanie do powtórnego lotu. W trakcie wojny w Czeczenii Pczeły-1T były wykorzystywane do rozpoznania dzięki zamontowanej kamerze wysokiej rozdzielczości oraz radiolinii pozwalającej przesyłać obraz w czasie rzeczywistym na odległość 30–50 km. Zdolność komunikacji warunkowała również promień działania BSP. Kolejnym ich zadaniem było podświetlanie celów, które były potem niszczone m.in. przez śmigłowce Mi-24P.

Przełom wieków przyniósł dalszy rozwój łączności na linii BSP – operator, a także wzrost częstotliwości wykorzystywania BSP nie tylko w celach zwiadowczych, ale również bojowych. W trakcie konfliktu w Kosowie (operacja Allied Force) w 1999 r. po raz pierwszy użyto łączy satelitarnych do przekazywania obrazu wideo, dzięki czemu centra dowodzenia mogły mieć stały wgląd w sytuację na teatrze działań. Podczas operacji Enduring Freedom w Afganistanie BSP stały się pełnoprawnymi uczestnikami działań w powietrzu. W trakcie swoich misji Predatory ściśle współpracowały zarówno z jednostkami naziemnymi, jak i powietrznymi, z jednej strony dostarczając niezbędnych informacji o działaniach przeciwnika, z drugiej podświetlając cele niszczone m.in. przez myśliwce F-14 i F-15. Nowością było przekazywanie danych lokalizacyjnych bezpośrednio z BSP do bombowców B-1B lub B-52 wyposażonych w bomby JDAM (Joint Direct Attack Munition) z układem naprowadzania GPS, co znacząco skróciło czas od wykrycia do zniszczenia celu przez bombowce.

Wszystkie te doświadczenia pozwoliły na stworzenie BSP RQ-4 Global Hawk przez inżynierów Northrop Grumman przy współpracy z DARPA (Defense Advanced Research Projects Agency). Jest to BSP klasy HALE, który wszedł do służby na przełomie 2002 i 2003 r. Obecnie w użyciu jest wersja Block 30, w której wprowadzono ulepszenia w zakresie urządzeń zwiadu elektronicznego, a także Block 40, w której wprowadzono radar MP-RTIP (jego głównym zadaniem jest poprawa śledzenia celów naziemnych). Zadania zwiadowcze są realizowane przy wykorzystaniu szeregu czujników, które razem tworzą EISS (Enhanced Integrated Sensor Suite – Rozszerzony Zintegrowany Pakiet Sensorów). EISS składa się z sensorów termowizyjnych i elektrooptycznych, a przede wszystkim radaru SAR, który dzięki wyposażeniu w funkcję GMTI (Ground Moving Target Indicator – Wskaźnik Ruchomych Celów Naziemnych) może również

odbierać sygnały od celów ruchomych. Na pokładzie zamontowano również system AN/APR-49 wykrywający i zakłócający sygnały radarowe. Global Hawk występuje również w innych wersjach. Pod nazwą Euro Hawk miał być wdrożony w niemieckiej Luftwaffe, lecz na drodze stanęły względy proceduralne – brak możliwości operowania w europejskiej przestrzeni powietrznej bez systemu zapobiegającego kolizjom z innymi statkami powietrznymi. Marynarka Wojenna Stanów Zjednoczonych (US Navy) zamówiła z kolei wersję MQ-4C Triton, która jest rozwinięciem Global Hawka do zadań patrolowych nad obszarami morskimi. Statki powietrzne tego typu zakupiła również Australia – 6 sztuk MQ-4C ma wejść do służby, począwszy od 2023 r. Global Hawk był używany m.in. w czasie operacji Enduring Freedom w Afganistanie (od 2002 r.) oraz Iraqi Freedom (od 2003 r.). Ich zadaniem, zgodnie z nowym trendem w lotnictwie, była stała obserwacja obszarów kluczowych dla prowadzonej operacji. W trakcie operacji Enduring Freedom zadania rozpoznawcze realizowały 2 maszyny, natomiast w trakcie Iraqi Freedom była to jedna maszyna. W Iraku zadania RQ-4 zostały rozszerzone i po raz pierwszy użyto go również do koordynacji działań i zabezpieczenia dowodzenia załogowymi platformami uderzeniowymi. Będzie on również wykorzystywany jako trzon systemu AGS NATO – 5 maszyn Global Hawk, wyposażonych w najnowsze radary MP-RTIP, a także pozostałe czujniki wchodzące w skład EISS, montowanego standardowo w RQ-4, będzie operowało z głównej bazy systemu we Włoszech.

Ciekawym przykładem drona rozpoznawczego jest Airbus Zephyr, określany również jako pseudosatelita. Jest on napędzany przez 2 silniki elektryczne zasilane przez akumulatory czerpiące energię z paneli słonecznych. Dzięki temu może teoretycznie przebywać w powietrzu przez dowolnie długi czas. Jedynym warunkiem jest odpowiednio długie przebywanie w zasięgu promieni słonecznych, które naładują akumulatory i pozwolą na dalszą podróż. Poruszając się z prędkością 55 km/h, na pułapie ponad 21 km, czyli poza zasięgiem zjawisk pogodowych, może patrolować obszar dziesiątek tysięcy kilometrów kwadratowych przez okres do 2 tygodni. Niestety, jego wątła budowa wymusza pewne ograniczenia – start i lądowanie muszą odbyć się przy względnie spokojnych warunkach pogodowych, a dotarcie na pułap operacyjny zajmuje ok. 2 dni,

natomiast zmiana miejsca dozorowania również wymaga dłuższego czasu niż w przypadku typowych BSP. Zadania wywiadowcze są realizowane poprzez lekkie kamery pracujące w świetle widzialnym i w podczerwieni, zaprojektowane specjalnie do użycia w Zephyrze, które mogą dostarczyć obrazy w rozdzielczości do 15 cm (1 piksel = 15 × 15 cm). Na etapie rozwoju jest obecnie radar, który ma zapewnić Zephyrowi możliwość zwiadu w każdych warunkach pogodowych i oświetleniowych. Program Zephyr znajduje się obecnie w fazie rozwojowej, a Wielka Brytania potwierdziła zakup 8 sztuk.

W kategorii mniejszych systemów klasy MALE dużą popularność zdobył izraelski Hermes 900 firmy Elbit Systems. Oblatany pod koniec 2009 r., wykorzystywany jest w siłach zbrojnych Izraela, Szwajcarii, Brazylii, Chile i Kolumbii. Hermes posiada autonomiczny system startu i lądowania, a jego wyposażenie rozpoznawcze składa się z głowicy elektrooptycznej, radaru SAR/ISAR, a także urządzeń do zwiadu elektronicznego. Ponieważ Hermes 900 jest zdecydowanie mniejszy niż BSP produkowane w USA (np. MQ-1C, MQ-9), jest tańszy w zakupie i eksploatacji, co przekłada się na jego popularność wśród mniej zamożnych państw.

Przykładem BSP klasy taktycznej jest poprzednik wspominanego Hermesa 900 – Hermes 450. System znajduje się na wyposażeniu m.in. Izraela, USA, Singapuru, Chorwacji, Azerbejdżanu, Gruzji, Brazylii i Wielkiej Brytanii (w wersji Watchkeeper WK450, zmodernizowanej i dostosowanej do operowania w warunkach europejskich, m.in. przez instalacje systemu zapobiegającego oblodzeniu w locie). Przykład Hermesa pokazuje też znaczenie posiadania narodowej kontroli nad systemem sterowania i kontroli nad BSP – wg niepotwierdzonych informacji Izraelczycy przekazali kody źródłowe gruzińskich Hermesów Rosjanom, co pozwoliło im niszczyć je poprzez zakłócanie systemów łączności.

Odrębną grupę stanowią drony rozpoznawcze przeznaczone do penetracji przestrzeni powietrznej państw dysponujących zaawansowanymi systemami przeciwlotniczymi. Wymaga to sprzętu o przeżywalności, jakiej nie mogą zapewnić najbardziej nawet wyrafinowane drony MALE i HALE, stosunkowo jednak powolne i łatwo wykrywalne. Rozwiązaniem są drony zbudowane z wykorzystaniem zaawansowanych → stealth technik [t. 4] (ograniczenia wykrywalności, przede wszystkim przez stacje

radiolokacyjne, a także systemy obserwacji w podczerwieni), niektóre konstrukcje charakteryzują się przy tym znaczną prędkością lotu. Najbardziej znanym przedstawicielem tej grupy jest amerykański Lockheed Martin RQ-170 Sentinel. Kolejną, znacznie większą konstrukcją należącą do tej kategorii, jest amerykański Northrop Grumman RQ-180. Dronów tej kategorii używa również Iran: to Shahed 171 Simorgh oraz Saegheh, będące lokalnymi odmianami Sentinela, który został przejęty przez Iran w stanie praktycznie nieuszkodzonym w 2011 r. podczas wykonywania lotu rozpoznawczego nad terytorium tego państwa. Nieco odmienną konstrukcją jest chiński WZ-8, który z uwagi na napęd rakietowy dysponuje bardzo dużą prędkością lotu (szacowaną na ok. 3,5 Ma).

Rafał Kopeć, Maciej Kulczycki

D. Becmer, D. Skorupka, A. Duchaczek, *Trendy rozwojowe bezzałogowych systemów latających*, „Problemy Techniki Uzbrojenia" 2015, nr 4, z. 136; J. Chojnacki, D. Pasek, *Historia wykorzystania bezzałogowych statków powietrznych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 1; R. Kopeć, *Drony rozpoznawcze*, [w:] *Vademecum bezpieczeństwa informacyjnego*, O. Wasiuta, R. Klepka (red.), t. 1: *A–M*, AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; R. Kopeć, O. Wasiuta, T. Wójtowicz, *Wojna dronów. Militarne wykorzystanie bezzałogowych statków powietrznych*, Wydawnictwo Uniwersytetu Pedagogicznego, Kraków 2020; T. Kwasek, *Klasyfikacja Bezzałogowych Statków Powietrznych*, „Dziennik Zbrojny" 2015, nr 1; W. Leśnikowski, *Drony. Bezzałogowe aparaty latające od starożytności do współczesności*, Wydawnictwo Adam Marszałek, Toruń 2016; A. Przekwas, R. Jaroszuk, *Bezzałogowe statki powietrzne w rozpoznaniu wojskowym*, „Przegląd Wojsk Lądowych" 2009, nr 7; B. Sajduk, *Amerykański i izraelski przemysł latających systemów bezzałogowych – porównanie wybranych platform*, [w:] *Przemysł zbrojeniowy. Tendencje, perspektywy, uwarunkowania, innowacje*, R. Kopeć (red.), Wydawnictwo Uniwersytetu Pedagogicznego, Kraków 2016; P.W. Singer, *Wired for War. The Robotic Revolution and Conflict in the 21st Century*, Penguin Press, New York 2009.

DYKTATURA (od łac. *dictare* – zalecać, dyktować) – forma wyłącznej, nieograniczonej i nadzwyczajnej, lecz ze swej istoty tymczasowej władzy politycznej jednostki lub grupy, ustanawianej w sytuacji poważnego →kryzysu politycznego bądź paraliżu zwyczajnych instytucji władzy

i → z a g r o ż e n i a [t. 4] ładu publicznego, zazwyczaj z wyraźnie określoną intencją unormowania położenia państwa i likwidacji istniejących zagrożeń oraz z założeniem, iż osiągnięcie takiego stanu rzeczy, tj. stabilizacji państwa, oznaczać winno zarazem kres trwania obowiązującej dyktatury. Źródła dyktatury sięgają starożytnego Rzymu z okresu republiki, w którym dyktatura była specjalnym urzędem, przewidzianym w razie zaistnienia stanu wyjątkowego.

W dyktaturze władza absolutna jest skoncentrowana w rękach lidera (powszechnie określanego jako dyktator), „małej kliki" lub „organizacji rządowej", a jej celem jest zniesienie pluralizmu politycznego, niezależnych partii politycznych lub mediów. Wraz z nadejściem XIX i XX w. dyktatury i demokracje konstytucyjne pojawiły się jako 2 główne formy rządów na świecie, stopniowo eliminując monarchię – jedną z tradycyjnych, szeroko rozpowszechnionych form rządzenia. Zazwyczaj w → r e ż i m i e [t. 3] dyktatorskim przywódca kraju jest utożsamiany z tytułem dyktatora, chociaż jego formalny tytuł może być zbliżony do „lidera". Powszechnym aspektem charakteryzującym dyktaturę jest wykorzystywanie silnej osobowości, zwykle poprzez tłumienie wolności myśli i wypowiedzi mas, w celu utrzymania całkowitej supremacji politycznej i społecznej oraz stabilności. Dyktatury i społeczeństwa totalitarne zazwyczaj stosują → p r o p a g a n d ę [t. 3] polityczną, aby zmniejszyć wpływ zwolenników alternatywnych systemów rządzenia. Opierają się na strukturach władzy i organach państwa, a nawet na bezpośredniej → p r z e m o c y [t. 3], represjach i terrorze. Chociaż często zdarza się, że dyktatury utrzymują pewne instytucje demokratyczne, ich rzeczywisty wpływ na politykę jest minimalizowany. Zazwyczaj reżimom dyktatorskim towarzyszą represje wobec przeciwników politycznych oraz surowe ograniczenia praw i wolności obywateli.

Skuteczność i optymalizacja tej formy sprawowania władzy zależy od wielu czynników, w szczególności od obiektywnej sytuacji, dostrzegania przez społeczeństwo potrzeby dyktatury, postawy społeczeństwa wobec niej oraz ideologicznego uzasadnienia władzy.

Forma rządu powszechnie powiązana z koncepcją dyktatury znana jest jako → t o t a l i t a r y z m [t. 4]. Nadejście totalitaryzmów zapoczątkowało nową erę polityczną w XX w. Ta forma rządzenia charakteryzuje się

obecnością jednej partii politycznej, a dokładniej potężnego lidera, który narzuca reszcie swoją osobistą i polityczną wizję rozwoju społeczeństwa. 2 podstawowe aspekty, które przyczyniają się do utrzymania władzy, to niezachwiana współpraca między rządem a → p o l i c j ą [t. 3] oraz wysoce rozwinięta ideologia. Rząd ma w takich przypadkach całkowitą kontrolę nad komunikacją masową oraz organizacjami społecznymi i gospodarczymi. Ideologia odgrywa wiodącą rolę w określaniu sposobu organizacji całego społeczeństwa. Najnowsze klasyfikacje nie ujmują jednak totalitaryzmu jako formy dyktatury.

Według B. Geddes rządy dyktatorskie można podzielić na 5 typów:

- → d y k t a t u r y w o j s k o w e – to reżimy, w których grupa oficerów sprawuje władzę, określa, kto będzie kierował krajem i wywiera wpływ na politykę. Elity wysokiego szczebla i przywódca są członkami dyktatury wojskowej; dyktatury wojskowe charakteryzują się rządami profesjonalizowanego wojska jako instytucji; elity wojskowe są nazywane członkami junty – są to zazwyczaj starsi oficerowie (i często inni oficerowie wysokiego szczebla) w wojsku;
- dyktatury jednopartyjne – to reżimy, w których jedna partia dominuje w polityce; w dyktaturach jednopartyjnych jedna partia ma dostęp do stanowisk politycznych i kontrolę nad polityką. Elity partyjne są zazwyczaj członkami organu rządzącego partii, czasem nazywanego komitetem centralnym, biurem politycznym lub sekretariatem – te grupy osób kontrolują wybór przedstawicieli partii i mobilizują obywateli do głosowania i popierania liderów partii;
- dyktatury personalistyczne – to reżimy, w których cała władza leży w rękach jednej osoby. Dyktatury personalistyczne różnią się od innych form dyktatur pod względem dostępu do kluczowych pozycji politycznych, znacznie bardziej zależą od uznania dyktatora personalistycznego. Personalistyczni dyktatorzy mogą być członkami wojska lub przywódcami partii politycznej. Jednak ani wojsko, ani partia nie sprawują władzy niezależnie od dyktatora. W personalistycznych dyktaturach elitarny korpus składa się zwykle z bliskich przyjaciół lub członków rodziny dyktatora. Wszystkie te osoby są zazwyczaj dobierane ręcznie. Wg badania z 2019 r. dyktatury personalistyczne są bardziej represyjne niż inne formy dyktatury;

- monarchiczne dyktatury – to reżimy, w których osoba królewskiego pochodzenia odziedziczyła pozycję głowy państwa zgodnie z przyjętą praktyką lub konstytucją. Reżimy te nie są uważane za dyktatury, jeśli rola monarchy jest w dużej mierze ceremonialna, ale monarchie absolutne, takie jak Arabia Saudyjska, można uznać za dyktatury dziedziczne. Elity w monarchiach są zazwyczaj członkami rodziny królewskiej;
- dyktatury hybrydowe – to reżimy łączące cechy dyktatur personalistycznych, jednopartyjnych i wojskowych. Kiedy reżimy posiadają cechy tych trzech form dyktatury, są one nazywane potrójnymi zagrożeniami. Najczęstsze formy hybrydowych dyktatur to hybrydy personalistyczne i jednopartyjne oraz hybrydy personalistyczne i wojskowe.

Wśród wad dyktatury zwykle wymieniane są:

- jedność i siła władzy jest często wyobrażona;
- wielu dyktatorów nie jest całkowicie pewnych siły swojej władzy i dlatego są skłonni do terroru i masowych represji politycznych w celu utrwalenia swoich wpływów;
- nadmierna centralizacja władzy sprawia, że państwo jest zakładnikiem osobistych cech dyktatora jako najwyższego władcy – śmierć dyktatora może pogrążyć państwo w kryzysie;
- istnieje ogromna możliwość przeniknięcia do władzy ludzi, dla których władza jest celem samym w sobie lub po prostu zawodowo nieodpowiednich do rządzenia;
- śmierć dyktatora może doprowadzić do przewrotu politycznego;
- nowy rząd (zwłaszcza jeśli jednocześnie zostanie obalony dyktator) może zakończyć długoterminowe projekty zainicjowane przez dyktatora ze względu na chwilowe zyski polityczne, ignorując późniejsze długoterminowe szkody polityczne, a nawet ekonomiczne, zwłaszcza jeśli nie nastąpi to natychmiast.

W porównaniu z republiką wyróżnia się także następujące wady:

- dyktatura ma większy teoretyczny potencjał do powstania monarchii;
- dyktator nie ponosi żadnej odpowiedzialności prawnej za konsekwencje swoich rządów, co może prowadzić do decyzji, które obiektywnie nie są zgodne z interesem państwa;

- pod dyktaturą pluralizm jest osłabiony lub całkowicie nieobecny;
- nie ma prawnej możliwości zmiany dyktatora, jeśli jego polityka okaże się sprzeczna z interesami państwa i społeczeństwa.

W porównaniu z monarchią istnieją zaś następujące wady:

- dyktatura zwykle nie jest uważana za „godną Boga" formę rządu, chociaż są wyjątki, np. dyktatura A. Pinocheta była wspierana przez Kościół i nie było prześladowań religijnych;
- wielu uważa dyktatora za uzurpatora, co również wywołuje pojawienie się oporu wobec jego władzy;
- w przeciwieństwie do dyktatora monarcha z reguły wychowuje i kształci się z myślą, że w przyszłości zostanie najwyższym władcą państwa, co pozwala mu od najmłodszych lat rozwijać cechy wymagane na stanowisku.

W dyktaturze podejmowane decyzje zwykle nie mają podstawy prawnej, nie występuje również ograniczenie instytucjonalne. Osoba sprawująca władzę stosuje głównie terror oraz kontroluje wszelką aktywność społeczną, w przypadku opozycji inwigiluje ją, a w państwie utrzymuje porządek i stabilizację. Dyktatura cechuje się brakiem poszanowania dla powszechnych →prawczłowieka [t. 3]. Najczęściej występującymi obecnie formami dyktatury są opierające się na ideologii komunistycznej – m.in. na Kubie, w Korei Północnej oraz w Białorusi.

Cechą dyktatury jest scentralizowana władza popierana przez zmarginalizowany parlament. Dyktatury w Ameryce Południowej charakteryzują się sprawowaniem kontroli nad władzą przez zgromadzenia zwane juntami – są to rządy wojskowe. Niekiedy w takich przypadkach do władzy dochodzi jeden charyzmatyczny oficer. Rządy junt były zazwyczaj legitymowane organizowaniem wyborów, które często fałszowano. Podobny styl działania przyjmują również dyktatorzy afrykańscy, obejmujący władzę w wyniku przewrotu wojskowego lub wyborów parlamentarnych, których rezultat jest z góry ustawiony. Zważywszy na charakterystykę kontynentu, dyktatorzy w krajach afrykańskich mają zwykle silne poparcie plemienne, co pozwala im utrzymywać się u władzy przez długi czas, nie wahają się przy tym używać zarówno aparatu administracyjnego, jak również sił mundurowych (liczne →ludobójstwa [t. 3]). W dyktaturze nie ma miejsca na dialog, wszelkie konflikty są rozstrzygane drogą siłową, co

prowadzi do zacofania i izolacji państw, w których ten system występuje. Do dyktatur zaliczamy również państwa faszystowskie oraz autorytarne. Dyktatura ma często znaczenie pejoratywne – państwo zostaje siłą i przemocą „zdobyte", a obywatele żyją w państwie policyjnym, gdzie wszystkie spory rozwiązuje się przy pomocy wojska lub policji, często dochodzi do łamania praw obywatelskich.

Jedyną rzeczywistą władzę sprawuje dyktator, który podejmuje decyzje bez konsultacji z parlamentem, senatem czy partiami politycznymi, które *de facto* nie istnieją. Z drugiej strony można zauważyć kilka zalet tego rodzaju ustroju, ponieważ wszystkie sprawy rozwiązuje się bardzo szybko, różne postanowienia w zasadzie od razu wprowadzanie są w życie. Pomimo niewielkich zalet dyktatury należy jasno stwierdzić, że nie jest ona korzystna dla obywateli.

Obecnie nadal istnieją reżimy autorytarne lub dyktatorskie, z których większość znajduje się na kontynencie afrykańskim i azjatyckim. W Europie uważane za dyktatury są reżimy na Białorusi i w Azerbejdżanie. Dyktatury to często reżimy jednopartyjne, czasem zamknięte dla reszty świata (Korea Północna lub Mjanma przed 2011 r.), czasem otwarte na handel (Chiny). Zasada nie jest bezwzględna, ponieważ historia dopuszcza pewne pluralistyczne dyktatury, dla których bardziej odpowiednią nazwą mógłby być np. „reżim autorytarny".

Zuzanna Juszczyk, Olga Wasiuta

M. Bankowicz, W. Kozub-Ciembroniewicz, *Dyktatury i tyranie. Szkice o niedemokratycznej władzy*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2007; N. Bermeo, *Democracy and the Lessons of Dictatorship*, „Comparative Politics" 1992, no. 24 (3); N.M. Ezrow, E. Frantz, *Dictators and Dictatorships: Understanding Authoritarian Regimes and their Leaders*, Continuum, New York 2011; Z. Juszczyk, *Dyktatura*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; S. Kott, M. Kula, T. Lindenberger, *Socjalizm w życiu powszednim: dyktatura a społeczeństwo w NRD i PRL*, Wydawnictwo Trio, Warszawa 2006; J. Linz, *Totalitarian and Authoritarian Regimes*, Lynne Rienner, Boulder 2009; N. McLaughlin, *Review: Totalitarianism, Social Science, and the Margins*, „The Canadian Journal of Sociology" 2010, no. 35 (3); H. Pająk, *Dyktatura nietykalnych*, Wydawnictwo Retro, Lublin 2006; K. Prokop, *Modele stanu nadzwyczajnego*,Temida 2, Poznań 2012; M. Ridenti, *The Debate over Military*

(or Civilian-Military?) Dictatorship in Brazil in Historiographical Context, „Bulletin of Latin American Research" 2018, no. 37.1; S. Zawadzki, *Dyktatura proletariatu i jej specyficzna forma w naszym kraju: na podstawie stenogramu wykładu wygłoszonego na centralnym kursie Wydziału Propagandy i Agitacji KC PZPR*, Książka i Wiedza, Warszawa 1958; A. Zoll, M. Bartosik, *Od dyktatury do demokracji i z powrotem*, Otwarte, Warszawa 2018.

DYKTATURA WOJSKOWA (ang. *military dictatorship*, *military junta*, *khakistocracy*) – określenie typu dyktatury stosowane m.in. w politologii, →naukach o bezpieczeństwie [t. 3], socjologii i historii.

Duży stopień zaangażowania sił zbrojnych w politykę od wieków stanowił jedno z →zagrożeń [t. 4] dla porządku politycznego. Z kolei →dyktatura oznaczała początkowo przejściowe i wyjątkowe skoncentrowanie władzy w ręku jednostki przy częściowym zawieszeniu porządku prawnego. Celem była obrona przed zagrożeniem zewnętrznym lub wewnętrznym (dotkliwa →wojna [t. 4], anarchia, →wojna domowa [t. 4]).

Powszechnie przyjmuje się, że dyktatura wojskowa to system sprawowania władzy państwowej przez armię. Nieprzypadkowo używa się niekiedy zamiennie pojęcia dyktatury militarnej. Jak wskazuje część badaczy, różni się ona od innych typów dyktatur m.in. motywacją przejęcia władzy, instytucjami, przez które siły zbrojne organizują swoje rządy, oraz sposobami, w jakie wojskowi rezygnują z władzy.

Dyktatury wojskowe można podzielić na te, w których wojsko bezpośrednio sprawuje władzę, oraz te, gdzie wojsko faktycznie kontroluje sytuację w państwie przy oficjalnym wycofaniu się sił zbrojnych z rządzenia krajem. B. Balcerowicz do dyktatur wojskowych zalicza także wszystkie działające dzięki poparciu armii spersonalizowane dyktatury. Nie dziwi więc, że zdaniem J. Żarnowskiego dyktatury wojskowe stanowią większość współcześnie istniejących dyktatur.

Balcerowicz dzieli dyktatury wojskowe na postępowe, reakcyjne i pośrednie. Do postępowych zalicza te, dla których najważniejszym motywem działania było zwalczenie →kryzysu władz państwa. Starają się one o pozyskanie, kontrolowanego odgórnie, szerokiego poparcia społecznego. Niekiedy występuje w nich pluralizm polityczny. Mogą doprowadzić do stopniowego wprowadzenia demokracji i uzyskania przez państwo pełnej

suwerenności. Reakcyjne (konserwatywne) przeciwnie – obalają ustroje demokratyczne i zmierzają do ograniczenia aktywności politycznej obywateli. Ten typ dyktatury wojskowej doprowadza zdaniem Balcerowicza do stabilizacji politycznej władzy albo do anarchii. Powyższa typologia nie jest jednak powszechnie przyjęta w literaturze przedmiotu.

Należy pamiętać, że zmiany w elitach rządzących nie zawsze dotyczą tylko sfery ustrojowej lub społecznej. Niekiedy dochodzi bowiem do zamachów stanu wewnątrz wojskowej elity władzy.

Większość badaczy wszystkie dyktatury wojskowe zalicza do dyktatur autorytarnych. Nieprzypadkowo M. Lisiecka używa jako synonimu dyktatury wojskowej pojęcia → a u t o r y t a r y z m u [t. 1] wojskowego. Niektóre → r e ż i m y [t. 3] funkcjonujące w XX w. w Ameryce Łacińskiej miały jednak pewne cechy państw totalitarnych. R. Borkowski traktuje dyktatury wojskowe jako osobną kategorię, obok dyktatur autorytarnych i totalitarnych.

Wprowadzeniu dyktatury wojskowej sprzyjają:

- zła sytuacja gospodarcza, zacofanie gospodarcze lub pogorszenie sytuacji gospodarczej;
- spuścizna kolonialna i związane z tym słabe zakorzenienie instytucji politycznych;
- utrata legitymizacji przez liderów cywilnych;
- konflikt polityczny między cywilnym rządem a elitami wojskowymi;
- inspiracja ze strony innych państw;
- polityczne ambicje najważniejszych przywódców wojskowych;
- znaczne nierówności społeczne;
- zagrożenie wewnętrzne lub zewnętrzne państwa;
- planowane reformy godzące w dotychczasowe polityczne i ekonomiczne przywileje elity wojskowej w państwie;
- rola sił zbrojnych w systemie autorytarnym dyscyplinujących obywateli i cementujących społeczny ład.

Niekiedy wprowadzeniu dyktatury wojskowej sprzyja tradycyjna akceptacja obywateli dla aktywności politycznej wojskowych (np. w Portugalii) i wcześniejsza szczególna misja wojska. Może ona dotyczyć modernizacji państwa, wspierania dążenia narodu do dobrobytu (Ameryka Łacińska) albo tworzenia danego państwa przez wojsko – jako organizacja

uzbrojonych polityków walczyło zbrojnie o niepodległość z państwami kolonialnymi np. wiele państw afrykańskich. D. Acemoglu, D. Ticchi i A. Vindigni uważają, że wprowadzeniu dyktatury sprzyja także wzrost ceny eksportowanych surowców naturalnych. Tak duża ilość przyczyn powstawania dyktatur nie może dziwić. Nie zdarza się bowiem, by przyczyną wprowadzenia dyktatury wojskowej był tylko jeden z wymienionych czynników, zwykle występuje ich minimum kilka. Z reguły dyktatury wojskowe powstają w efekcie przewrotu wojskowego.

Zamachu mogą dokonywać spiskowcy dowodzeni przez oficerów średniego szczebla, liczący na poparcie części jednostek wojskowych lub część dowództwa, a nawet (np. w Chile w 1976 r.) dowodzący wszystkich rodzajów sił zbrojnych. Niekiedy armia dokonuje przewrotu i wprowadza dyktaturę wojskową, mając poparcie znacznej części obywateli i części sceny politycznej. Znany jest nawet przypadek oficjalnej prośby większości parlamentarnej wzywającej wojsko do „przywrócenia porządku" (Chile w 1973 r.). Zamach stanu nie jest jednak koniecznym warunkiem wprowadzenia dyktatury wojskowej (np. Filipiny po wprowadzeniu stanu wojennego w 1972 r.).

Najważniejszą formą bezpośrednich rządów armii jest zbiorowy rząd wojskowy skupiony wokół grupy oficerów. Taki ustrój zaliczany jest niekiedy do dyktatur oligarchicznych. W tym przypadku rządzi zdominowana przez oficerów rada o różnym poziomie sformalizowania. Są one różnie nazywane, np. „Komitet Restauracji Narodowej" lub „Komitet Wyzwolenia Narodowego" czy „Rada Ocalenia Narodowego". Inną formą dyktatury wojskowej są rządy dyktatora będącego wysokiej rangi wojskowym.

Jak wskazuje J.G. Otto, w wypadku nieprzejęcia rządów cywilnych wojsko pełni funkcję strażnika państwa. Ten typ ustroju ma 2 warianty: dość szczegółową kontrolę cywilnego rządu wspieranego politycznie przez armię albo kontrolę węższego zestawu zagadnień arbitralnie uznanych przez wojskowych za kluczowe. Armia dysponuje bowiem prawem weta wobec działań rządu i parlamentu. Arbitralnie orzeka, co jest dla danego państwa dobre i w jakim kierunku mają zmierzać dokonywane w nim zmiany polityczne czy gospodarcze. W sprawach, które uznaje za strategiczne, wpływa na inne organy państwa zgodnie z odpowiednio sformułowanymi zapisami konstytucji albo wywiera nacisk za pomocą

środków pozaprawnych na działalność rządu. Wojsko jako strażnik państwa nie tylko jest inspiratorem zmian rządu, ale również zwierzchnikiem wydającym rozkazy. Rządy cywilne w krajach o takim ustroju zmuszone są więc często manewrować między oczekiwaniami elektoratu a sympatią najwyższych dowódców sił zbrojnych danego państwa. Armia, jeśli uzna to za celowe, wywołuje rekonstrukcję cywilnego rządu wbrew prawu albo otwarcie przejmuje władzę, likwidując oparte na konstytucji rządy cywilne. Często trudno określić koniec tego typu niejawnej dyktatury wojskowej, wynikającej z wyjątkowej pozycji wojska w ustroju państwa.

W państwie, w którym rządzą wojskowi, decyzje są podejmowane poza konstytucyjnymi organami władzy. Niekiedy zachowywano pozory. Rządzący wojskowi wykorzystują do tego celu i zawłaszczają istniejące instytucje państwa lub kreują nowe. Tworzą (a niekiedy także dopuszczają do działania) struktury pseudodemokratyczne, takie jak np. „tymczasowy" parlament. Często wkrótce po przejęciu władzy przez armię inscenizowane są wybory parlamentarne, nadzorowane przez wojsko. Niekiedy wojsko dysponuje własnymi partiami politycznymi. Ich znaczenie w państwie jest jednak głównie propagandowe.

W dyktaturze wojskowej siły zbrojne i jego agendy, np. sądownictwo, zostają przekształcone w struktury władzy politycznej. Nawet w przypadku braku zbrojnych walk wewnętrznych często w miarę upływu czasu rośnie rola trybunałów wojskowych. Pod pozorami rządów praw sądownictwo wojskowe bywa na dużą skalę wykorzystywane jako ważny instrument politycznej kontroli społeczeństwa.

Armia, a ściślej korpus oficerski, jest podstawowym (choć nie jedynym) zapleczem władz. Po przejęciu władzy wojskowi starają się więc wzmocnić i ustabilizować swoją realną władzę. Wzmacniają (lub uzyskują) dla wojska uprzywilejowaną pozycję ekonomiczną w przemyśle cywilnym, budownictwie, telekomunikacji, rolnictwie, a nawet (w przypadku Egiptu) w branży turystycznej. Siły zbrojne nie tylko zarządzają przedsiębiorstwami państwowymi, na szeroką skalę wojsko inwestuje w różnych sektorach gospodarki i kontroluje niektóre jej gałęzie (nie tylko przemysł zbrojeniowy). Rosną powiązania elit wojskowych z elitami gospodarczymi. Wojsko uzyskuje własny, hojnie (na tle innych grup społecznych) dotowany przez państwo system opieki medycznej. Rosną dochody oficerów. Tworzone są dla nich

specjalne sklepy. Uczelnie wojskowe mają wysoki prestiż. Służba wojskowa jest bowiem przygotowaniem do uczestnictwa w życiu politycznym i w pracy administracyjnej. Władze państwa dbają też o utrzymanie lub zwiększenie prestiżu sił zbrojnych (inną kwestią jest to, na ile skutecznie).

Ważnym elementem umacniania władzy jest dokonanie głębokich zmian personalnych w administracji, w tym nasycenie jej wieloma oficerami. Budowany jest w ten sposób zmilitaryzowany aparat państwowy. Zawodowi wojskowi są równocześnie dowódcami oraz premierami, ministrami, gubernatorami itp. Nieprzypadkowo wg klasyfikacji autorytaryzmów J.J. Linza najczęściej występującym na świecie jest autorytaryzm biurokratyczno-wojskowy.

Do ważnych celów rządzących należy centralizacja władzy. Skala praktycznego nadzoru wojska nad funkcjonowaniem administracji na niższych szczeblach organizacyjnych zależy m.in. od sytuacji w państwie. Słabość prowincjonalnej administracji sprzyja próbom wprowadzenia całkowitej dominacji wojska na wszystkich szczeblach zarządzenia państwem. W praktyce jednak, jak wskazuje J.I. Levitt, ze względu na stan kraju dyktatury wojskowe np. w państwach afrykańskich często muszą liczyć się z lokalnymi dowódcami niewchodzącymi w skład armii, ale dysponującymi uzbrojonymi oddziałami.

W późniejszym okresie dyktatorskich rządów, by ocieplić swój wizerunek, wojskowa elita rządząca czasem zdejmuje mundury i przedstawia się obywatelom jako władza cywilna.

Stopień akceptowalnego przez wojsko pluralizmu idei i postaw wśród obywateli zależy od rodzaju dyktatury wojskowej oraz sfery życia publicznego. Czasem wojsko na dużą skalę ingeruje w struktury społeczne i kulturę. Wynika to nie tylko ze słabości lokalnej administracji i struktur politycznych.

Dyktatura stara się przekonać obywateli do swej wizji państwa i usprawiedliwić wprowadzenie tej formy rządów. Program, który głoszą wojskowi, przejmując władzę, jest zdeterminowany przez sytuację w danym państwie. Można jednak wskazać pewne elementy wspólne dla większej liczby państw. Rządzący wojskowi deklarują, że dążą do dobra wspólnego wszystkich lub większości obywateli. Oficjalnie nie ma dyktatury wojskowej – armia chce uratować naród przed skorumpowanymi lub krótkowzrocznymi cywilnymi politykami. Głosi się dążenie do obrony narodu, ustrojowego

i gospodarczego uzdrowienia państwa, wzmocnienia władzy centralnej, likwidacji podziałów społecznych czy → k o r u p c j i. Wojskowi przedstawiają się jako jedyna siła, która może zapewnić skuteczne przywództwo w trudnym pod względem politycznym i gospodarczym dla państwa czasie. Podkreślają konieczność i przejściowość swych rządów, uzasadniają je jako sposób zapewnienia politycznej stabilności lub uratowania narodu przed zagrożeniem niebezpiecznymi ideologiami. W tym wypadku w zależności od kraju i okresu za główne zagrożenie uznawano → k o m u n i z m, socjalizm albo → i s l a m i z m. Niekiedy wprowadzenie dyktatury wojskowej uzasadniano udziałem państwa konflikcie pomiędzy wyznającym chrześcijańskie wartości Zachodem a amoralnym komunizmem. Rządzący oficerowie uważają się za jedyną grupę mogącą wydobyć państwo z politycznej i gospodarczej zapaści. Występują jako siła modernizująca (np. Nigeria, Pakistan, Indonezja), obrońca świeckości państwa (np. Turcja) lub przeciwnie, jako obrońca religii i tradycji (szczególnie na terenie Ameryki Łacińskiej). Równocześnie często podkreśla się konieczność jedności narodowej.

Kładziony jest nacisk na siłę i autorytet władzy oraz na porządek, któremu przeciwstawia się otwarcie krytykowana demokracja liberalna. Podkreśla się odrębność kulturową od Europy. Idealizuje się armię i jej znaczenie dla danego państwa. Można zauważyć też dążenie do zorganizowania państwa na wzór wojska.

Dyktatury wojskowe odwoływały się także do wybranych cech sił zbrojnych szczególnie jako elementu sprzyjającego spoistości państwa, gwaranta jego → s u w e r e n n o ś c i [t. 4] i integralności terytorialnej albo do cech narodowych armii. Można tu wymienić etos siły narodowowyzwoleńczej, dominację etniczną danego narodu, służbę w wojsku jako drogę awansu społecznego. W XX w. były nieliczne przypadki, gdy wojsko obalało dyktatora, zmierzając do przywrócenia demokracji (np. Boliwia, 1982 r.; Gwatemala, 1944 r.). Częściej idea ta jest wykorzystywana przez wojskowych jedynie jako propagandowe hasło. Należy tu też podkreślić znaczne zaangażowanie oddziałów wojskowych w działalność propagandową władz.

Do szerokiego wykorzystywania struktur wojskowych w praktyce rządzenia, w tym terroryzowania rzeczywistych i potencjalnych przeciwników, dyktatury wojskowe wykorzystują wprowadzenie stanu wojennego lub

stanu wyjątkowego. Wbrew deklaracjom i prawu często obowiązują one wiele lat, mimo że w zasadzie nie ma już warunków, które usprawiedliwiałyby ich dalsze podtrzymywanie. Niekiedy zawieszana jest konstytucja i wiele ustaw, nadzwyczajny stan prawny jest przez dyktaturę pozornie likwidowany drogą przeniesienia przydatnych dla niej przepisów do prawa zwyczajnego. Zdarza się, że wprowadzane są akty ważniejsze od konstytucji (np. Documentos básicos w Argentynie).

Do ważnej cechy dyktatury wojskowej zalicza się stosowanie wojskowych metod działania. Z reguły wkrótce po objęciu władzy nasila się proces militaryzacji życia społecznego. Podejmuje się próby ukształtowania u młodzieży „ducha wojskowego", związanego z posłuszeństwem, zdyscyplinowaniem i gotowością do wykonywania poleceń wojska. Powyższe często jest powiązane z uznaniem wojska za najlepszy instrument do rozwiązywania problemów i sprostania wyzwaniom stojącym przed państwem. Traktowaniu armii jako jedynej siły zdolnej do przeprowadzenia reform oraz efektywnego rządzenia sprzyja z jednej strony słabość lub brak partii politycznych, a z drugiej poziom zdyscyplinowania, zorganizowania i techniki w wojsku. W wielu państwach Trzeciego Świata zwolennicy takiego poglądu działań są często także przekonani, że zbrojenia i rozbudowa armii są drogą do wszechstronnego postępu. Nieprzypadkowo jednym ze znaczeń pojęcia militaryzmu jest ustrój, w którym siły zbrojne mają decydujący wpływ na kierowanie państwem.

Często dyktatury wojskowe ograniczają kontakty międzynarodowe obywateli. Ułatwia to budowanie strachu przed obcym, rzekomo niebezpiecznym i niemoralnym wrogiem. Dehumanizacja rzeczywistego lub rzekomego przeciwnika ułatwia utrzymanie obywateli w posłuszeństwie wobec kierujących państwem i usprawiedliwia utrzymywanie → s t a n u n a d z w y c z a j n e g o [t. 4].

Niekiedy wobec niemożności zapewnienia trwałej poprawy sytuacji gospodarczej szerokich rzesz obywateli rządzący próbują mobilizować społeczeństwo pod hasłami militarystycznymi (np. Erytrea). W licznych przypadkach wystarczyła rządzącym wytworzona dzięki temu atmosfera strachu i nienawiści.

Utrzymaniu dyktatury wojskowej sprzyja częste występowanie w szeroko pojętych elitach władz ludzi posiadających osobowość autorytarną.

Wyraźnie przeceniają oni znaczenie władzy i jej możliwości. Są przekonani o swej wielkości, niechętnie słuchają głosów krytycznych i narzucają otoczeniu swoją wolę. Równocześnie bardzo gorliwie wykonują polecenia zwierzchników. Pogardzają niżej stojącymi w hierarchii. Są wobec nich bezwzględni, surowi i gotowi okazywać agresję.

Pomimo niekiedy rozbudowanej ideologii brak legitymizacji politycznej oraz zapewnienie na stałe przywilejów i władzy nielicznej grupie powoduje, że wielu oficerom u władzy stale towarzyszy lęk przed jej utratą. W praktyce władzę mogą utrzymać przez okres wielu lat, jedynie stosując represje. Wojsko przejmuje część funkcji policyjnych. Skala stosowania →przemocy [t. 3] przez dyktatury wojskowe wobec społeczeństw jest jednak zróżnicowana. Zależy m.in. od sprzeciwu społecznego, czasu trwania dyktatury; cech charakteru osób rządzących państwem, kultury politycznej dominującej w danym kraju. Należy tu odnotować często dużą odporność elit władzy na naciski międzynarodowe.

W praktyce różny jest poziom zinstytucjonalizowania przemocy wobec politycznych wrogów dyktatury wojskowej. Czasem, by umocnić swoją pozycję, władze stosują także takie środki i metody, których nie przewiduje prawo w ramach stanu nadzwyczajnego, utrzymywane w tajemnicy przed społeczeństwem. Niekiedy tworzono w tym celu zdominowane przez wojskowych niejawne struktury. Przykładem mogą być tu nielegalne porwania osób i mordowanie podejrzewanych o wrogie działania w Argentynie. Takim działaniom wojskowych sprzyja brak zewnętrznej kontroli nad armią, stosowanie dehumanizacji przeciwników politycznych, wyłączna kontrola wojska nad państwem i przekonanie, że wrogowie wewnętrzni stanowią „element obcy", zagrażający spójności narodu. Nie zawsze jednak kryteria określające wroga były ścisłe, czasem zaliczano do tej grupy także tych, którzy nieświadomie ułatwiali działanie wrogom narodu. Nieprzypadkowo Borkowski, odnosząc się do dyktatury wojskowej, pisze o wojskowo-policyjnej formie rządów.

Czasem wojskowa elita decyduje się na konfrontację militarną. Ma to uwiarygodnić jej władzę w oczach obywateli i odwrócić uwagę społeczeństwa od gospodarczych i społecznych problemów, których rządzący nie potrafią rozwiązać. →Mobilizacja [t. 3] do →wojny [t. 4] ma zastąpić powszechne poparcie i legitymizację władzy. Odnośnie do schyłku

XX i XXI w. jako przykład można podać konflikty Erytrei z sąsiadami. Bardziej znanymi przykładami są wcześniejsze, sprowokowanie przez wojskowe dyktatury, wojny o Falklandy-Malwiny (Argentyna, 1982 r.) i o Cypr (Grecja, 1974 r.). Według badań B. Geddes dyktatury wojskowe w obrębie reżimów autorytarnych funkcjonują krócej od pozostałych (personalistycznych i jednopartyjnych). W analizowanym przez nią okresie było to średnio 8,5 roku. Przyczyn nietrwałości dyktatur wojskowych jest bardzo wiele. Przede wszystkim często dyktatura wojskowa nie jest w stanie sprostać problemom, którym miała zaradzić. Niekiedy jest odwrotnie. Przykładowo konflikty etniczne, regionalne i religijne w nasilonym stopniu negatywnie wpływają na funkcjonowanie samej armii (np. Nigeria).

Niekiedy problemem bywa rozbieżność programowa w obrębie nowej elity władzy odnośnie do przemian, jakie należy urzeczywistnić. Przykładowo w Portugalii wojskowi różnili się co do planowanego miejsca cywilów na scenie politycznej. Rozstrzygnięcia tej sprawy nie ułatwia częste zróżnicowanie sił cywilnych, które poparły dany zamach wojskowy.

Do pozostałych wyzwań stojących przed dyktaturami wojskowymi w końcu XX i w XXI w. można zaliczyć: przejęcie przez siły zbrojne funkcji, do których wojsko nie jest przygotowane (np. do zarządzania finansami państwa); represje w dłuższej perspektywie czasowej godzące w jedność i dyscyplinę w siłach zbrojnych; zły stan państwa; skala korupcji wśród oddelegowanych do administracji i przemysłu oficerów; obniżenie poziomu moralnego w jednostkach sił zbrojnych; upolitycznienie wojska powodujące pogorszenie jego możliwości bojowych.

Rządom armii tylko pod pewnymi względami sprzyja specyfika służby wojskowej. Zdaniem Ł. Fydereka najważniejszą przyczyną upadku dyktatur wojskowych są podziały wewnątrz korpusu oficerskiego. Sprzyja im fakt, że często korpus oficerski przejmuje niektóre funkcje pełnione w demokracji przez system partii politycznych. W obliczu związanej z tym groźby rozpadu sił zbrojnych na kilka części i wojny domowej często wojsko „dobrowolnie" wraca do koszar po zapewnieniu sobie nierozliczania okresu swych rządów.

Nie dziwi więc, że dyktatury wojskowe niekiedy stopniowo przywracają znaczenie władzom cywilnym przy zachowaniu kluczowej pozycji dla najważniejszego dowódcy wojskowego. Najczęściej pełni on funkcję

prezydenta (np. Pakistan). Zdarzały się jednak przypadki, gdy rządzący generał ustępował wskutek niekorzystnego dla niego wyniku plebiscytu (Chile, 1988 r.) albo skompromitowane władze wojskowe oddawały władzę dobrowolnie, w porozumieniu z opozycją rozpisując wybory.

Podatność ustrojów państw na objęcie władzy przez wojskowych była i jest różna. Dyktaturom wojskowym sprzyja ustrój autorytarny, ponieważ uniemożliwia zmianę partii rządzącej drogą demokratyczną. W szczegółach nie ma tu jednak zgody wśród badaczy. Przykładowo Fyderek wskazuje, że w państwach arabskich bardziej na wprowadzenie dyktatury wojskowej były narażone reżimy organizacyjne niż tożsamościowe.

W większości przypadków (także w odniesieniu do państw Afryki i Azji) dyktatury wojskowe są utożsamiane z juntami. Zgodnie z etymologią tego pojęcia jest to uprawnione jednak tylko w 2 sytuacjach: albo gdy faktycznie państwem rządzi więcej niż jedna osoba, a rada jest zdominowana przez wojskowych (lub składa się wyłącznie z nich), albo gdy dyktator musi faktycznie liczyć się ze zdaniem innych członków wojskowej wąskiej elity władzy (np. Pinochet w Chile).

Tomasz Skrzyński

D. Acemoglu, D. Ticchi, A. Vindigni, *A Theory of Military Dictatorships*, „National Bureau of Economic Research Working" 2008, paper no. 13915; B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Wydawnictwo Naukowe „Scholar", Warszawa 2010; M. Bankowicz, *Autorytaryzm i totalitaryzm – analiza porównawcza*, [w:] *Totalitaryzmy XX wieku. Idee – instytucje – interpretacje*, B. Szlachta, W. Kozub-Ciembroniewicz, H. Kowalewska-Stus i in. (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2010; M. Bankowicz, W. Kozub-Ciembroniewicz, *Dyktatury i tyranie. Szkice o niedemokratycznej władzy*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2007; R. Borkowski, *Upadek dyktatur i procesy demokratyzacji we współczesnym świecie*, [w:] *Konflikty współczesnego świata*, R. Borkowski (red.), Wydawnictwa Naukowo-Dydaktyczne Akademii Górniczo-Hutniczej, Kraków 2002; Ł. Fyderek, *Autorytarne systemy polityczne świata arabskiego, Adaptacja i inercja w przededniu arabskiej wiosny*, Księgarnia Akademicka, Kraków 2016; J.I. Levitt, *Illegal Peace in Africa: An Inquiry Into the Legality of Power Sharing with Warlords, Rebels, and Junta*, Cambridge University Press, New York 2012; M. Lisińska, *Zjawisko dehumanizacji w czasach argentyńskiej dyktatury wojskowej 1976–1983. Przykład działania Szkoły Mechaników Marynarki Wojennej ESMA*

w Buenos Aires, „Ameryka Łacińska" 2017, nr 3 (97); J.G. Otto, *Wojsko w reżimie politycznym – zarys analizy politologicznej*, [w:] *Demokratyczne i niedemokratyczne reżimy polityczne*, J.G. Otto (red.), Dom Wydawniczy Elipsa, Warszawa 2015; *Państwo i polityka w Ameryce Łacińskiej. Zarys systemów politycznych państw latynoamerykańskich*, P. Łaciński (red.), Wydawnictwo Difin, Warszawa 2013; W. Paruch, *Autorytaryzm w Europie XX wieku. Zarys analizy politologicznej cech systemu politycznego*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio K" 2009, vol. XVI; Z. Trejnis, *Siły zbrojne w państwie demokratycznym i autorytarnym*, Adam Marszałek, Warszawa 1997; J. Żarnowski, *Współczesne systemy polityczne. Zarys problematyki*, Uczelnia Łazarskiego, Warszawa 2012.

DYPLOMACJA OBRONNA – to różnorodna międzynarodowa pokojowa aktywność oparta na dialogu i współdziałaniu, realizowana w ramach współpracy dwustronnej, wielostronnej oraz w ramach międzynarodowych organizacji →bezpieczeństwa [t. 1] przez resort →obrony narodowej [t. 3] i podległe mu instytucje oraz siły zbrojne wraz z sojusznikami, partnerami i innymi zaprzyjaźnionymi państwami w celu wspierania polityki zagranicznej i bezpieczeństwa.

Pojęcie dyplomacji obronnej funkcjonuje w nauce i praktyce politycznej jako nowy termin dotyczący wyspecjalizowanego obszaru działań zagranicznych państwa. Wiąże się z tą sferą dyplomacji, która obejmuje specyficzne zadania stawiane przed resortami obrony i →attaché obrony [t. 1], a także siłami zbrojnymi i podmiotami cywilnymi. Dyplomacja obronna historycznie powstała w wyniku poszukiwania harmonii między sprzecznymi żywiołami polityki: dyplomacją, opartą na zasadach i sztuce unikania użycia siły, oraz wojskiem, którego działanie tradycyjnie wiąże się z akcjami opartymi na →przemocy [t. 3] lub demonstracji siły i zdolności do jej zastosowania w celach agresji, obrony i →odstraszania [t. 3]. Głównym celem dyplomacji obronnej jest pokojowe kształtowanie i prowadzenie polityki bezpieczeństwa państwa, a zadaniem kreowanie stabilnych, długotrwałych relacji i współpracy sprzyjających przejrzystości w dziedzinie obronności i wzmacnianiu zaufania.

Dyplomacja obronna jako instrument polityki państwa oznacza zatrudnienie – w czasie pokoju – sił zbrojnych i innych zasobów obronnych w celu osiągnięcia metodami pokojowymi określonych celów politycznych. Jej istotą jest więc szeroko rozumiana współpraca wojskowa umożliwiająca

zapobieganie konfliktom i minimalizacja wrogości oraz budowanie międzynarodowego zaufania. Najważniejszym elementem owej współpracy jest wymiana attaché obrony między państwami, co jest dowodem na istnienie stosunków wojskowych między nimi. Skuteczna i sprawna dyplomacja obronna niewątpliwie wzmacnia pozycję międzynarodową państwa, jest instrumentem jego polityki zagranicznej i bezpieczeństwa oraz elementem systemu antykryzysowego. Stabilizuje także stosunki międzynarodowe, zwiększa ich przejrzystość, a tym samym obniża ryzyko wybuchu konfliktu zbrojnego.

Koncepcja dyplomacji obronnej zrodziła się na początku lat 90. XX w. po upadku muru berlińskiego (1989 r.) i rozpadzie Układu Warszawskiego (1991 r.) wraz ze zmianą roli siły militarnej w osiąganiu celów politycznych państw. Nastąpił wówczas wzrost współzależności między państwami, a także wzrost liczby nowych aktorów na scenie światowej. Wojsko angażowane daleko poza obszarem jego tradycyjnych kompetencji militarnych zaczęto wykorzystywać w relacjach międzynarodowych do osiągania różnorodnych celów dyplomatycznych. W aspekcie militarnym oznaczało to redukcję sił zbrojnych i ograniczenie wydatków obronnych na rzecz komercyjnych projektów rozbudowy sektora usług i produkcji oraz przeorientowanie → d y p l o m a c j i w o j s k o w e j w dyplomację obronną. Rola wojska zaczęła się sprowadzać do głównego narzędzia → d y p l o m a c j i p r e w e n c y j n e j, zapobiegającej → k r y z y s o m i konfliktom zbrojnym w zróżnicowanym środowisku międzynarodowym, oraz zasadniczego instrumentu rozwoju pokojowych → m i ę d z y n a r o d o w y c h s t o s u n k ó w w o j s k o w y c h [t. 3].

Pierwowzorem dyplomacji obronnej, wykształconym na gruncie europejskim, była koncepcja obrony nazywana *Smart Defence* (Inteligentna Obrona). Jej istotą było rozwijanie współpracy sił zbrojnych z różnych krajów europejskich, w tym określanie priorytetów dla zdolności operacyjnych i lepszej koordynacji działań. Z biegiem czasu przerodziła się ona w powszechną koncepcję działań i instrument pokojowej polityki zagranicznej pod nazwą dyplomacji obronnej. Opierała się na założeniu, że siły zbrojne i związana z nimi infrastruktura obronna mogą wpływać na zachowanie → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o [t. 1] nie tylko przez odstraszanie i prowadzenie wojen, ale także poprzez wspieranie

i promowanie idei współpracy i stabilizacji środowiska międzynarodowego. Pokojowe wykorzystanie personelu wojskowego miało na celu zapobieganie konfliktom i kreowanie stabilnych i długotrwałych relacji współpracy oraz sprzyjanie przejrzystości w obszarze obronności.

W potocznym odbiorze pojęcie dyplomacji obronnej utożsamia się często z dyplomacją wojskową. W rzeczywistości termin „dyplomacja obronna" jest pojęciem szerszym, które precyzyjniej oddaje poszerzający się kontekst zadań i uwarunkowań funkcjonowania dyplomacji wojskowej, będąc jej – w pewnym sensie – kontynuacją w warunkach pokojowych. Przejmując tradycyjne zadania dyplomacji wojskowej (reprezentacyjne, łącznikowe, informacyjne), poszerza je o działania prewencyjne, stabilizacyjne, obronne, dialog polityczny, odpowiedzialność za kwestie współpracy wielostronnej, dyplomację osobistą przedstawicieli państwa i sił zbrojnych oraz misji międzynarodowych związanych z pokojowym wykorzystaniem wojska i personelu wojskowego. Dyplomacja obronna nie realizuje operacji wojskowych, ale prowadzi pokojowe działania obronne, jest więc ukierunkowana bardziej na budowanie zaufania między podmiotami i silnie zorientowana na dialog, zapobieganie konfliktom oraz pokojowe realizowanie interesów własnego państwa. Wciela bowiem w życie tylko te cele i zadania dyplomacji wojskowej, które są związane z rozwiązywaniem konfliktów, dialogiem obronnym, rozwijaniem współpracy dwu- i wielostronnej, a także użyciem sił zbrojnych w misjach i operacjach międzynarodowych. Dyplomacja obronna dopuszcza do grona podmiotów realizujących jej zadania, obok instytucji politycznych i wojskowych, także podmioty cywilne, takie jak organizacje międzynarodowe, akademie wojskowe, ośrodki edukacyjne, ośrodki badawcze i badawczo-rozwojowe oraz związane z resortem obrony think tanki itp. Najistotniejszym wyznacznikiem dyplomacji obronnej jest wykluczenie bezpośredniej interwencji zbrojnej o agresywnym charakterze. W literaturze naukowej określenia „dyplomacja wojskowa" i „dyplomacja obronna" współistnieją na podobnych prawach. Nie są to jednak zamienniki pojęciowe.

Pierwsze próby integrowania sił zbrojnych z dyplomacją nastąpiły w USA, a pierwszej konceptualizacji i udoskonalenia idei dyplomacji obronnej podjęli się Brytyjczycy. W 1996 r. amerykański dokument pod nazwą *Narodowa strategia bezpieczeństwa: zaangażowanie i rozszerzanie*

(*A National Security Strategy of Engagement and Enlargement*) prezydenta B. Clintona zapowiadał potrzebę porzucenia izolacji → k o m u n i z m u jako wiodącej zasady polityki zagranicznej USA i zastąpienia jej → s t r a t e g i ą [t. 4] umacniania bezpieczeństwa, wspierania narodowego dobrobytu oraz promocji demokracji na świecie. Rolę globalnego przywódcy miały odegrać USA, bowiem tylko one, jako największe gospodarczo i militarnie mocarstwo świata, mogły doprowadzić do stworzenia stabilnych stosunków politycznych i wolnego handlu. Miało to na celu zaangażowanie międzynarodowych partnerów w sprawy wojskowe i uwiarygodnienie ich obecności za granicą, a tym samym wzmocnienie współpracy między sferą wojskową i dyplomatyczną. W październiku 1998 r. powstała amerykańska *Narodowa strategia bezpieczeństwa na nowy wiek* (*A National Security Strategy For A New Century*), będąca rozwinięciem i uzupełnieniem poprzedniej.

Kontynuatorami propokojowej idei kształtowania stosunków międzynarodowych stali się Brytyjczycy, którzy ją udoskonalili, rozszerzyli i doprowadzili do jej upowszechnienia. W ocenach brytyjskich siła militarna gwarantująca jedynie osiąganie doraźnych celów wojskowych była za słaba jako narzędzie polityki. Nową propozycją długotrwałego utrzymania międzynarodowej stabilności, zapobiegania konfliktom oraz realizacji polityki bezpieczeństwa międzynarodowego miała być dyplomacja obronna. Po raz pierwszy pojęcie to pojawiło się w powszechnym użyciu w 1998 r. za sprawą brytyjskiego *Strategicznego przeglądu obronnego* (*Strategic Defence Review*). W dokumencie tym dyplomację obronną definiowano jako „pokojowe wykorzystanie środków obronnych w celu osiągnięcia pozytywnych rezultatów w rozwoju stosunków dwustronnych i wielostronnych". Oznaczało to całkowite odrzucenie klasycznych operacji wojskowych na rzecz takich form współpracy, jak wymiana personelu, okrętów i statków powietrznych, kontakty polityczne i wojskowe wysokiego szczebla, dwustronne i wielostronne spotkania eksperckie, edukacja, szkolenia i ćwiczenia, regionalne i sojusznicze fora obronne, zagraniczna pomoc wojskowa, środki budowy zaufania, kontrola zbrojeń i nieproliferacja broni masowego rażenia. Za główny cel dyplomacji obronnej uznano wówczas budowę i utrzymanie zaufania oraz pomoc w rozwoju demokratycznych sił zbrojnych, a także zapobieganie konfliktom i ich rozwiązywanie. Towarzyszący dokumentowi raport ministerstwa obrony uznawał dyplomację obronną za jedną

z kluczowych misji brytyjskich sił zbrojnych realizowaną w celu usunięcia wrogości, zbudowania i utrzymania zaufania oraz wsparcia budowy sił zbrojnych poddanych demokratycznej kontroli. Brytyjskie dokumenty rządowe ukonstytuowały ostatecznie dyplomację obronną jako ważny instrument polityki zagranicznej i bezpieczeństwa oraz wygenerowały liczne próby konceptualizacji tego pojęcia podejmowane przez badaczy z całego świata, m.in. na gruncie południowoafrykańskim (M. Edmonds, G. Mills), irlandzkim (A. Cottey, A. Forster), hiszpańskim (*Plan dyplomacji obronnej*) czy singapurskim (S. Seng Tan, B. Singh). Badacze z Singapuru zwrócili uwagę na 2 funkcje dyplomacji obronnej – pragmatyczną i transformacyjną. Funkcja pragmatyczna posiadająca charakter stabilizacyjny skoncentrowana jest na utrzymaniu istniejącego stanu współpracy bezpieczeństwa pomiędzy dwoma lub więcej państwami w wybranym regionie. Funkcja transformacyjna natomiast ukierunkowana jest na rozwiązywanie kryzysów i pokonfliktową odbudowę. W ujęciu singapurskim dyplomacja obronna powinna być prowadzona na 3 zasadniczych poziomach. Pierwszy dotyczy zaangażowania i działania liderów politycznych, ministrów, szefów obrony, szefów sztabów generalnych oraz dowództw i sztabów szczebla strategicznego. Drugi obejmuje działania akademii wojskowych, ośrodków edukacyjnych, ośrodków badawczych i badawczo-rozwojowych oraz związanych z resortem obrony think tanków. Poziom trzeci to działania przedstawicieli cywilnych organizacji pozarządowych. Badacze singapurscy zmienili dotychczasowe postrzeganie dyplomacji obronnej, utożsamianej zwykle z działalnością attaché obrony i ministerstw obrony, rozszerzając je na działania dodatkowych podmiotów cywilnych. Ich zdaniem pośrednictwo w konfliktach i działania profilaktyczne takie jak edukacja czy praktyczne szkolenia poprawiły skuteczność rozwiązywania konfliktów, prowadzenia negocjacji oraz utrzymania rozwoju pokonfliktowego. Uzasadnia to także rosnące znaczenie podmiotów pozapaństwowych na arenie międzynarodowej jako skutecznych ogniw działających na rzecz bezpieczeństwa i pokoju, a tym samym jako istotnych elementów dyplomacji obronnej.

W Polsce problematyka dyplomacji obronnej jest tematem stosunkowo nowym. Podejmowana jest coraz częściej w refleksjach naukowych takich uczonych jak m.in.: R. Kupiecki, L. Drab czy A. Sochan.

Zasadniczymi płaszczyznami działania dyplomacji obronnej obok współpracy ustanowionej i utrzymywanej przez przedstawicieli cywilnych i wojskowych są także edukacja i szkolenia wojskowe, ćwiczenia oraz misje i operacje wojskowe. Należy tu również zaliczyć współpracę wywiadowczą i wymianę → i n f o r m a c j i wojskowo-politycznych państw oraz współpracę w ramach międzynarodowych organizacji bezpieczeństwa i sojuszy. Obszarem aktywności dyplomacji obronnej jest także działalność związana z kontrolą zbrojeń, rozbrojeniem i środkami budowy zaufania oraz ze sferą współpracy prawnej i legislacyjnej, współpracą w zakresie przemysłów obronnych, pomocy wojskowej i wsparcia sił zbrojnych innych państw, a także wojskowej współpracy historycznej i edukacji patriotycznej. Wsparcie sił zbrojnych innych państw poprzez doradztwo, szkolenie oraz przekazywanie sprzętu wojskowego i uzbrojenia, współpraca techniczna i przemysłów obronnych, prowadzenie tzw. dialogów obronnych i strategicznych, współpraca w ramach szkolnictwa wojskowego, ćwiczenia angażujące środki wojskowe czy też misje i operacje pokojowe i humanitarne również realizowane są w ramach działań dyplomacji obronnej.

Do instrumentów dyplomacji obronnej zalicza się:

- siły zbrojne, których zadania w ramach dyplomacji obronnej wykraczają poza zadania bojowe i odstraszające związane z użyciem siły, a koncentrują się na realizacji kontaktów dwu- i wielostronnych między najwyższymi i wojskowymi przedstawicielami resortów obrony,
- wyznaczanie i utrzymywanie w innych państwach attaché obrony,
- wypracowywanie i uzgadnianie dwustronnych umów międzynarodowych w dziedzinie współpracy wojskowej,
- przekazywanie ekspertyz oraz doradztwo w zakresie demokratycznej i cywilnej kontroli nad siłami zbrojnymi,
- utrzymywanie regularnych kontaktów pomiędzy personelem wojskowym i jednostkami wojskowymi oraz wizyty → o k r ę t ó w w o j e n n y c h [t. 3] w portach,
- usytuowanie personelu wojskowego i cywilnego w państwach partnerskich, zarówno w ministerstwach obrony, jak i w jednostkach wojskowych,
- rozmieszczanie zespołów szkoleniowych,

- zaopatrywanie w sprzęt, uzbrojenie i inne materiały wojskowe,
- udział w dwu- i wielostronnych ćwiczeniach wojskowych i szkoleniach.

Formami współpracy w zakresie dyplomacji obronnej obok osobistych wizyt i lokowania attaché obrony w innych państwach są również szeroko rozumiane wymiany edukacyjne. Kursy i szkolenia służą nawiązywaniu kontaktów z innymi państwami oraz podniesieniu wiedzy i umiejętności zarówno własnego korpusu oficerskiego, jak i podmiotów cywilnych. Organizowanie konferencji międzynarodowych, szczytów, spotkań tematycznych i seminariów, tych o zasięgu regionalnym, jak i globalnym, umożliwia z kolei uzyskanie porad eksperckich oraz wymianę poglądów w kwestiach strategicznych, politycznych i operacyjnych. Takie spotkania często stanowią zalążek do podpisania dwu- lub wielostronnych umów dotyczących wzajemnego zaufania, wymianę informacji i podejmowanie wspólnych projektów w takich obszarach, jak szkolenia, → d o k t r y n a w o j s k o w a, sprzęt czy rozwiązywanie wspólnych problemów państw funkcjonujących np. w tym samym regionie. Jedną z ważniejszych form współpracy w ramach dyplomacji obronnej są działania logistyczne i biznesowe, związane z zakupem broni i sprzętu wojskowego oraz rozwojem przemysłu obronnego, wymianą technologii, poszukiwaniem partnerów do wspólnych przedsięwzięć produkcyjnych i logistycznych oraz związane z systemem zaopatrzenia sił zbrojnych. Kraje o wysokim poziomie rozwoju naukowego i technologicznego mogą pełnić funkcję doradców i producentów sprzętu obronnego dla krajów, w których siły zbrojne przechodzą dopiero transformację i modernizację oraz mogą w ten sposób zapoznać się z aktualnymi trendami i informacjami dotyczącymi sektora obronnego.

Zadania dyplomacji obronnej mają charakter bardzo różnorodny. Należą do nich następujące praktyki:

- promowanie współpracy dwu- i wielostronnej w zakresie stosunków wojskowych;
- promowanie bezpieczeństwa i obrony poprzez wymianę attaché obrony, wymianę osobistą oraz intensywne kontakty robocze przedstawicieli wojskowych i cywilnych;
- przygotowywanie, negocjowanie i podpisywanie umów i porozumień w dziedzinie obronnej, jak również „obsługiwanie" spotkań

dwu- i wielostronnych na różnych szczeblach, wspieranie partnerów w reformowaniu sektora bezpieczeństwa i rozwoju ich zdolności do udziału w operacjach wojskowych, pokojowych i stabilizacyjnych;
- pomoc logistyczna w operacjach kryzysowych czy humanitarnych oraz →katastrofach technicznych i →naturalnych;
- merytoryczne doradztwo wojskowe świadczone władzom państwowym, przedstawicielom dyplomatycznym, organizacjom międzynarodowym i rządom innych państw;
- wspieranie partnerów w reformowaniu sektora bezpieczeństwa oraz działania kooperatywne na rzecz rozwoju narodowych i kolektywnych zdolności do udziału w międzynarodowych operacjach pokojowych;
- wspieranie wysiłków na rzecz budowania →infrastruktury wojskowej niezbędnej do organizacji współpracy czy wspólnej obrony;
- promowanie demokratycznej cywilnej kontroli nad siłami zbrojnymi;
- wszechstronna obsługa porozumień w sferze kontroli zbrojeń i rozbrojeń oraz środków budowy zaufania;
- współpraca szkoleniowa i edukacyjna;
- ćwiczenia wojskowe;
- misje i operacje wojskowe;
- współpraca wywiadowcza oraz wymiana informacji o sytuacji wojskowo-politycznej innych;
- współpraca w ramach sojuszy;
- działalność związana z kontrolą zbrojeń, rozbrojeniem i środkami budowy zaufania;
- współpraca prawna i legislacyjna;
- współpraca w zakresie przemysłów obronnych;
- pomoc wojskowa i wsparcie sił zbrojnych innych państw;
- wojskowa współpraca historyczna i wojskowa polityka historyczna;
- organizacja wizyt statków powietrznych, okrętów lub innego sprzętu wojskowego w zaprzyjaźnionych państwach.

Tematy podejmowane w ramach dyplomacji obronnej można podzielić na trzy zasadnicze grupy. Pierwsza obejmuje działania w kierunku

promowania i ochrony szeroko rozumianych wartości uniwersalnych, do których zalicza się m.in. krzewienie zasad demokracji, idei praworządności, poszanowanie → p r a w c z ł o w i e k a [t. 3], ochronę → b e z p i e c z e ń s t w a p o l i t y c z n e g o [t. 1] i zapewnienie → b e z p i e c z e ń s t w a e k o n o m i c z n e g o [t. 1]. Wymienić tu można ponadto kształtowanie pokojowej atmosfery zaufania między państwami, współpracę w ramach polityki zagranicznej oraz ochronę pokoju i bezpieczeństwa międzynarodowego. Druga grupa tematów realizowanych przez podmioty cywilne i wojskowe w ramach dyplomacji obronnej może dotyczyć zagadnień związanych z pokojowym przeciwdziałaniem potencjalnym → z a g r o ż e n i o m [t. 4], w tym z minimalizowaniem skutków kryzysów i konfliktów. Do tego obszaru można zaliczyć wszelkie pokojowe działania w kierunku rozbrojenia i nieproliferacji broni masowego rażenia, walkę z → t e r r o r y z m e m [t. 4], przeciwdziałanie → z a g r o ż e n i o m h y b r y d o w y m [t. 4], przeciwdziałanie nielegalnej imigracji, ochronę uchodźców politycznych, promowanie demokratycznej cywilnej kontroli nad siłami zbrojnymi. To także podejmowanie szerokiej współpracy wojskowej między państwami w zakresie wymiany informacji wojskowych, rozwoju kontaktów wojskowych, prawo do obserwacji, utworzenie systemu bezpośredniej łączności między stolicami państw sygnatariuszy, w tym związanej z rozwojem przemysłu i badań naukowych w zakresie bezpieczeństwa i obronności w celu poprawy i rozwoju potencjału obronnego innych państw.

Trzecia grupa obejmuje obszar związany ze środkami i sposobami działania, za pomocą których powyższe cele można osiągnąć. W tym zakresie można więc wskazać następujące tematy: promowanie edukacji patriotycznej i pokojowej współpracy, krzewienie idei pokojowego rozstrzygania sporów i kryzysów w celu zapobieżenia rozwojowi konfliktów, wykorzystywanie dyplomacji w kształtowaniu stosunków międzynarodowych, w tym także negocjacji i mediacji. Do tej grupy tematów można zaliczyć wszelkie zagadnienia związane z promocją i kreowaniem pozytywnego wizerunku państwa na arenie międzynarodowej, np. dyplomację publiczną oraz promowanie operacji humanitarnych i ratowniczych, a także organizowanie misji pokojowych (→ m i s j a p o k o j o w a [t. 3]). Dyplomacja obronna jest bowiem mocno zakorzeniona w rzeczywistości i nie wyklucza tego, że w pewnym momencie zaistnieje konieczność

użycia siły w celu osiągnięcia celów politycznych, jednocześnie szukając porozumienia i współpracy z innymi państwami.

Sabina Olszyk

J.E. Cheyre, *Defence Diplomacy*, [w:] *The Oxford Handbook of Modern Diplomacy*, J. Heine, A.F. Cooper, R.C. Thakur (eds.), Oxford University Press, Oxford 2013; A. Cottey, A. Forster, *Reshaping Defence Diplomacy. New Role for Military Cooperation Assistance*, „Adelphi Paper" 2004, no. 365; T. Dodd, M. Oakes, *The Strategic Defence Review White Paper*, Research Paper 98/91, House of Commons Library, London 1998; L. Drab, *Dyplomacja obronna – nowy instrument polityki zagranicznej i bezpieczeństwa*, „Sprawy Międzynarodowe" 2017, r. 70, nr 1; tenże, *Dyplomacja obronna w procesie kształtowania bezpieczeństwa RP*, Difin, Warszawa 2018; S.G. Fetic, *Fields Classic Diplomacy with Defence Diplomacy Interacts Horizontally. Preventive Diplomacy, Coercive Diplomacy*, „Revista Academiei Fortelor Terestre" 2014, vol. 73, no. 1; R. Kupiecki, *Dyplomacja obronna – próba konceptualizacji*. „Dyplomacja i Bezpieczeństwo" 2016, nr 1; S. Seng Tan, *NGOs in Conflict Management in Southeast Asia*, „International Peacekeeping" 2005, vol. 12, no. 1; S. Seng, S. Seng Tan, *„From Boots" to Brouges. The Rise of Defence Diplomacy in Southeast Asia, School of International Studies*, S. Rajaratnam School of International Studies, Singapore 2011; A. Vagts, W.T.R. Fox, *Defence and Diplomacy. The Soldier and the Conduct of Foreign Relations*, King's Crown Press, New York 1958.

DYPLOMACJA PREWENCYJNA (ang. *preventive diplomacy*) – to wszelkie decyzje i działania zapobiegające powstawaniu sporów między stronami, przeciwdziałające przeradzaniu się już istniejących sporów w konflikty zbrojne oraz ograniczające zasięg tych konfliktów w przypadku ich wystąpienia, wszelkie zabiegi zmierzające do zapobiegania występowaniu elementów zagrażających pokojowi, → b e z p i e c z e ń s t w u m i ę d z y n a r o d o w e m u [t. 1] oraz stabilności na świecie, wszelkie czynności obliczone na łagodzenie sporów i zapobieganie eskalacji → k o n f l i k t ó w m i ę d z y n a r o d o w y c h. Realizuje się je poprzez programy pomocy rozwojowej dla państw dotkniętych skutkami konfliktów oraz typowe działania wyrównujące poziom życia i rozwoju gospodarczego w ramach procesów integracji regionalnej. Podejmowana jest na arenie międzynarodowej zarówno przez podmioty indywidualne, państwa, grupy państw, jak również przez aktorów subpaństwowych (regiony, miasta) oraz organizacje

międzynarodowe takie jak Organizacja Narodów Zjednoczonych (ONZ) czy Unia Europejska (UE).

Współcześnie dyplomacja prewencyjna jest najczęściej stosowanym środkiem w kontekście działań podejmowanych w ramach systemu bezpieczeństwa ONZ, UE i innych organizacji międzynarodowych. Działania prewencyjne podejmowane możliwie wcześnie są bowiem względnie skuteczną, najmniej skomplikowaną, najmniej kosztowną i najbardziej humanitarną metodą rozwiązywania sporów, jaką może zastosować społeczność międzynarodowa.

Formalne źródło dyplomacji prewencyjnej stanowi art. 2 Karty Narodów Zjednoczonych z 1945 r., a w szczególności jego pkt 3 i 4. Punkt 3 dokumentu zobowiązuje wszystkich członków do załatwiania sporów międzynarodowych pokojowymi środkami. W punkcie 4 czytamy o zakazie stosowania groźby użycia siły lub bezpośredniego jej użycia przeciwko integralności terytorialnej lub → s u w e r e n n o ś c i [t. 4] któregokolwiek z państw. Społeczność międzynarodowa, świadoma destrukcyjnego wpływu konfliktów na szeroko rozumiany rozwój i → b e z p i e c z e ń s t w o [t. 1], wskazała jednoznacznie w tych zapisach, że rozwiązanie sporu może wystąpić wyłącznie na drodze konsensusu. Potwierdzono jednocześnie, iż rozstrzyganie antagonizmów w sposób pokojowy zadziała wzmacniająco i utrwali poczucie stabilności całej wspólnoty ponadnarodowej.

Dyplomację prewencyjną do praktyki międzynarodowej wprowadził sekretarz generalny ONZ D. Hammarskjöld, który w 1960 r., w czasie rywalizacji Wschodu i Zachodu, zwrócił uwagę na konieczność utrzymywania na małych obszarach minimalnych sporów międzynarodowych po to, aby zapobiec ich przeobrażeniu w większe konflikty. W ówczesnych realiach odnosiło się to do zmniejszenia ryzyka przerodzenia się konfliktów o małej intensywności w konflikty zbrojne, w które obydwa mocarstwa (USA i ZSRR) mogłyby się zaangażować. Efektywność dyplomacji prewencyjnej w okresie → z i m n e j w o j n y [t. 4] była nieco ograniczona z uwagi na jej sprzeczność ze → s t r a t e g i a m i [t. 4] obydwu supermocarstw, przejawiającymi się w potrzebie „rozprzestrzeniania rewolucji" przez ZSRR i powstrzymywania „imperium zła" przez USA. To spowodowało tymczasowe jej zamrożenie aż do początków lat 90. XX w., kiedy to w związku z transformacją ustrojową państw byłego bloku wschodniego

na nowo zaczęto podejmować różne inicjatywy w tym kierunku. Zmiana →środowiska bezpieczeństwa [t. 4] oraz pojawienie się nowych →zagrożeń [t. 4] spowodowały, że zaczęto poszukiwać nowych metod ich rozwiązywania. Odradzanie się dyplomacji prewencyjnej uaktywniło cały wachlarz działań, z jakich mogą korzystać państwa i podmioty pozapaństwowe w zakresie zapobiegania oraz zmniejszania napięć w środowisku międzynarodowym. Uczyniło to dyplomację prewencyjną naturalnym i jednym z najbardziej skutecznych narzędzi zapewnienia bezpieczeństwa na arenie międzynarodowej.

Istotnym dokumentem kształtującym tożsamość dyplomacji prewencyjnej okazał się raport sekretarza generalnego ONZ B. Butrusa Ghalego *An Agenda for Peace* (*Program dla pokoju*) przedstawiony na forum ONZ w 1992 r. oraz obserwacje i rozważania prowadzone przez ministra spraw zagranicznych Australii G. Evansa, w 1994 r. zebrane w książce *Cooperating for Peace: The Global Agenda for the 1990s and Beyond* (*Współpraca dla pokoju: agenda globalna na lata 90. i następne*). Koncepcje wyłożone w tych publikacjach, choć znacząco uzupełnione i rozszerzone, w mniejszym lub większym stopniu opierały się na znanych już działaniach pokojowych realizowanych przez ONZ. Obydwa ujęcia dyplomacji prewencyjnej, względem siebie komplementarne, z czasem stały się swoistą wykładnią metod i środków działań prewencyjnych wykorzystywanych do stworzenia międzynarodowego systemu zapobiegania i rozwiązywania konfliktów.

W przekonaniu Butrusa Ghalego dyplomacja prewencyjna jest pierwszym krokiem w kierunku zapewnienia pokoju na świecie. Pogląd ten podzielał Evans, nadając priorytet prewencji jako najbardziej skutecznemu sposobowi ograniczania konfliktów, który, jeśli podjęty wystarczająco wcześnie, może doprowadzić do załagodzenia sporu, a nawet zablokować jego przerodzenie się w konflikt. Całościowy program budowy bezpieczeństwa i pokoju w przekonaniu obu obserwatorów składa się z konkretnych strategii działań. Ich umiejętne połączenie i współdziałanie może zapewnić międzynarodowy ład i bezpieczeństwo. Wśród owych strategii znalazły się następujące działania: pojednanie (ang. *peacemaking*), zachowanie/utrzymanie pokoju (ang. *peacekeeping*, *peace maintenance*), budowanie pokoju (ang. *peace building*), przywrócenie pokoju (ang. *peace restoration*) oraz wymuszenie pokoju (ang. *peace enforcement*). Strategie te znajdują

odzwierciedlenie w działaniach ONZ i przekładają się na typy prowadzonych przez nią operacji pokojowych.

Strategia pojednania obejmuje działania podejmowane w celu zapobiegania potencjalnym →kryzysom we wczesnym stadium rozwoju sporu oraz rozwiązywania konfliktów, które już zaistniały. Działania w ramach niej polegają zazwyczaj na aktywności dyplomatycznej dążącej do wynegocjowania i zawarcia porozumienia przez strony konfliktu. Dyplomacja i mediacja odgrywają kluczową rolę w tych staraniach. Ich celem jest monitorowanie oraz rozpoznanie w sposób precyzyjny →sytuacji kryzysowej [t. 4]. W pracach na rzecz pojednania w najwyższym stopniu uczestniczy ONZ we współpracy z innymi podmiotami. Uczestnikami →misji pokojowych [t. 3] mogą być także specjalni wysłannicy, rządy, grupy państw czy organizacje regionalne. Wysiłki w tym zakresie mogą być także podejmowane przez grupy nieoficjalne i podmioty pozarządowe, a także przez wybitne osobistości. Do zakończenia operacji pojednania dochodzi wówczas, gdy zostaną wstrzymane działania zbrojne oraz powiedzie się próba zawarcia porozumienia o przerwaniu ognia.

Strategia zachowania pokoju oznacza zmobilizowanie oraz rozmieszczenie kontyngentów sił wojskowych, policyjnych oraz cywilnych państw członkowskich ONZ w rejonie kryzysu. Ustanowiona jest z inicjatywy grupy państw członkowskich ONZ bądź bezpośrednio przez sekretarza generalnego. Ważne jest, że takie operacje są podejmowane jedynie za zgodą głównych stron konfliktu. W przypadku braku przyzwolenia którejkolwiek ze stron podmiot międzynarodowy ryzykuje utratą bezstronności w sporze i nie może efektywnie realizować celu, którym jest utrzymanie pokoju. Bezstronność jest konieczna dla zachowania zgody między stronami konfliktu oraz prowadzenia współpracy. Użycie siły przez podmioty realizujące tę strategię zawsze jest uważane za środek ostateczny. Uczestnicy misji mogą stosować siłę jedynie w przypadku samoobrony, obrony mandatu misji oraz ochrony →ludności cywilnej [t. 3], zwłaszcza w sytuacji, gdy państwo, na którego terytorium odbywa się misja, nie jest w stanie zapewnić bezpieczeństwa. Głównym działaniem w ramach tej strategii jest nadzorowanie przestrzegania zawieszenia broni oraz udzielanie pomocy we wdrażaniu porozumień pokojowych zawieranych przez strony konfliktu. Ich zadaniem jest również wspieranie procesu

przywracania rządów prawa (m.in. udzielanie pomocy przy organizacji wyborów), ochrona i promowanie → praw człowieka [t. 3], a także wspomaganie rozbrojenia, → demobilizacja oraz reintegracja byłych kombatantów ze społeczeństwem. Sukces operacji utrzymania pokoju nigdy nie jest pewny, ponieważ decyduje o nim wiele czynników takich jak sytuacja geopolityczna, postawa zwaśnionych stron czy zakres mandatu udzielonego misji.

Strategia budowania pokoju obejmuje kompleks działań podejmowanych po konflikcie na rzecz tworzenia niezbędnych warunków dla osiągnięcia trwałego pokoju, zmniejszenia ryzyka wystąpienia bądź ponownego zaangażowania w konflikt zbrojny państw i społeczności lokalnych. Przejawia się w rozdzielaniu walczących stron, udzielaniu pomocy humanitarnej zagrożonej ludności, wzmacnianiu zdolności państw do efektywnego sprawowania swoich funkcji w oparciu o prawo, zapewnieniu pomocy przy odbudowie zrujnowanej konfliktem gospodarki. Misje budowania pokoju podejmują w szczególności działania z zakresu:

- monitorowania zawieszenia broni,
- demobilizacji walczących stron,
- wspierania powrotu uchodźców i osób wysiedlonych,
- wspierania procesu wprowadzania pokoju,
- wspierania procesu wyborczego,
- wspierania reform sektorów sprawiedliwości i bezpieczeństwa,
- zapewnienia i wzmacniania ochrony praw człowieka.

Skuteczność misji budowania pokoju zależy w ogromnym stopniu od wsparcia społeczności międzynarodowej dla krajów dotkniętych konfliktem.

Zgodnie z wizją Evansa proces budowania pokoju realizowany jest w 2 wymiarach dyplomacji prewencyjnej – tzw. wczesnej (przedkonfliktowej) oraz opóźnionej (doraźnej). Wczesna dyplomacja prewencyjna zapewnia fachową pomoc stronom sporu, prowadząc działania zapobiegające eskalacji konfliktu. W wymiarze przedkonfliktowym najczęściej wykorzystuje się środki pozamilitarne w postaci rokowań, pośrednictwa, pojednania, narzędzi ekonomicznych (sankcje), społecznych i politycznych. W ramach dyplomacji opóźnionej podejmuje się próby wpłynięcia na zwaśnione strony wtedy, gdy spór już zaistniał, tak

aby nie przekształcił się w konflikt. Uwidacznia się tutaj różnica między poglądami Butrusa Ghalego i Evansa. Pierwszy z nich kładł większy nacisk na budowanie pokoju, gdy konflikt jest już obecny, drugi natomiast koncentrował się na kwestii zapobiegania jego wystąpieniu. Warto dodać, że w ramach dyplomacji prewencyjnej Butrus Ghali dopuszczał także możliwość ustanowienia sił rozjemczych, a nawet tworzenie stref zdemilitaryzowanych.

Przywrócenie pokoju to kolejna strategia dyplomacji prewencyjnej stosowana w sytuacji, gdy konflikt nabrał już zbrojnego charakteru, obejmuje działania zmierzające w kierunku pojednania zwaśnionych stron. Ich celem jest rozdzielenie walczących, →ochrona ludności [t. 3] lokalnej, przywrócenie rządów prawa i porządku, zakończenie konfliktu, ustanowienie stref bezpieczeństwa, a możliwe jest także przeprowadzanie →interwencji humanitarnych.

Strategia wymuszania pokoju występuje w sytuacji, gdy kryzysy oraz konflikty już zaistniały i brakuje porozumienia między wszystkimi zainteresowanymi stronami. Metodami wymuszania pokoju w tym przypadku mogą być działania pozamilitarne, takie jak np. sankcje, oraz środki militarne w postaci groźby użycia siły lub jej użycie. W przypadku ONZ decyzja o wymuszaniu pokoju podejmowana jest osobiście przez sekretarza generalnego ONZ, →Radę Bezpieczeństwa ONZ [t. 3] bądź Zgromadzenie Ogólne, lub w innych przypadkach przez regionalne organizacje we współpracy z ONZ. Wówczas podejmowana jest interwencja militarna, której celem jest rozdzielenie walczących stron. Przyjmuje się, że operacja taka może być przeprowadzana za zgodą przynajmniej jednej ze stron pogrążonych w konflikcie i polega na podjęciu działań w sytuacji, gdy przestały działać instytucje państwowe, bądź też z zamiarem przywrócenia bezpieczeństwa zagrożonej ludności.

Warto jednak pamiętać, że granice między strategiami zapobiegającymi konfliktom ulegają zatarciu. Często współistnieją i uzupełniają się, operacje pokojowe rzadko realizują tylko jeden typ zadań.

Skuteczność dyplomacji prewencyjnej jest uzależniona od zaistnienia kilku różnych czynników: środków budowy zaufania, rozwiniętego systemu wczesnego ostrzegania oraz wysyłania misji wyjaśniających i obserwacyjnych w rejony konfliktów. Najistotniejszym elementem działań

prewencyjnych są środki budowy zaufania, czyli podejmowanie działań mających na celu redukcję napięcia międzynarodowego, stabilizację pokojowej współpracy, a także obniżenie poziomu rywalizacji wojsk i zwiększenie przejrzystości zbrojeń, które mogłyby doprowadzić do przypadkowego wybuchu konfliktu. Budowa zaufania, kompromisowość i dobra wola stron do zażegnania sporu są elementem koniecznym dla zminimalizowania ryzyka wystąpienia konfliktu między stronami. Bardzo istotnym czynnikiem działań prewencyjnych jest posiadanie aktualnej wiedzy na temat sytuacji i relacji między podmiotami. Mogą temu służyć misje wyjaśniające i obserwacyjne oraz kontakty z rządami poszczególnych państw. Kolejnym ważnym czynnikiem jest posiadanie efektywnego systemu ostrzegania, rozwiniętego zwłaszcza w odniesieniu do takich zagrożeń jak ryzyko katastrofy nuklearnej, zagrożenia środowiskowe, masowe migracje ludności, groźby głodu i klęsk żywiołowych. Ważnym elementem dyplomacji prewencyjnej jest pokojowe, zapobiegawcze rozmieszczenie sił w sytuacji, gdy obydwie strony są zgodne co do tego, że obecność jednostek cywilnych czy wojskowych powstrzyma skutecznie działania wojenne na skonfliktowanym terenie. Zgoda stron konfliktu jest tu bezwzględnie wymagana i oznacza respektowanie suwerenności i terytorialnej integralności państw.

Do metod prowadzenia dyplomacji prewencyjnej powszechnie zalicza się klasyczne metody rozwiązywania sporów zawarte w Karcie Narodów Zjednoczonych:

- arbitraż – proces przygotowywania rozwiązania sporu przez stronę trzecią, niezaangażowaną w spór;
- koncyliacja – działanie strony trzeciej ułatwiające stronom sporu dojście do porozumienia poprzez m.in. proponowanie możliwych rozwiązań czy poprawę komunikacji;
- misje w celu stwierdzenia stanu faktycznego, dążące do ustalenia obiektywnych faktów w sprawie i zmierzające do podjęcia właściwych działań w ramach → d y p l o m a c j i o b r o n n e j;
- dobre usługi – sytuacje, w której strona trzecia wspiera nawiązanie niezbędnych kanałów komunikacji dla rozwiązania sporu;
- inspekcje – ich celem jest budowanie zaufania i wzajemnej pewności o dobrych intencjach stron sporu oraz wyjaśnianie

ewentualnych nieporozumień czy złej interpretacji dokonanych wcześniej uzgodnień;
- porozumienia zawarte na drodze prawnej – podporządkowanie się stron sporu decyzji wydanej przez sąd lub powołane do tego celu gremium;
- mediacja – wsparcie wypracowania porozumienia poprzez ułatwianie procesu negocjacji i uczestnictwo w nim;
- monitorowanie – prowadzenie aktualnego rozpoznania potencjalnych źródeł sporów i konfliktów w celu niedopuszczenia do ich rozwinięcia;
- ostrzeżenia – wskazywanie stronie/stronom sporu ewentualnych konsekwencji dalszej eskalacji konfliktu.

Współczesna dyplomacja prewencyjna, obok działań ONZ, znajduje szerokie zastosowanie również w polityce UE. Podstawy prawne działalności prewencyjnej UE zawarte są w kilku dokumentach: traktacie z Maastricht i zawartym w nim rozdziale o wspólnej polityce zagranicznej i bezpieczeństwa, traktacie amsterdamskim i w traktacie nicejskim. Unia Europejska, hołdując idei bezpieczeństwa i pokoju na świecie, w raporcie Rady Europejskiej zaprezentowanym w 1999 r. w Helsinkach, potwierdziła pryncypialną rolę postanowień Karty Narodów Zjednoczonych w zakresie działań prewencyjnych. Zaakcentowała również konieczność kooperacji w zakresie promowania bezpieczeństwa, wczesnego ostrzegania, zapobiegania konfliktom, rozwoju mechanizmów → z a r z ą d z a n i a k r y z y s o w e g o [t. 4] oraz restytucji sytuacji sprzed konfliktu.

W ramach unijnych operacji pokojowych prowadzone są działania w zakresie operacji stabilizacyjnych, zastępujących, wzmacniających, reformujących, obserwacyjnych oraz zapewniających wsparcie misjom innych organizacji. Operacje stabilizacyjne charakteryzują się tym, że siły pokojowe rozlokowane zostają w celu rozdzielenia walczących stron lub zapewnienia utrzymania pokoju w rejonie konfliktu. W operacjach zastępujących unijne kontyngenty przejmują odpowiedzialność i zarządzają sektorem bezpieczeństwa (np. → p o l i c j ą [t. 3], wojskiem), wymiarem sprawiedliwości lub administracją cywilną, które w normalnych warunkach znajdowałyby się pod kontrolą władz lokalnych i państwowych. W operacjach wzmacniających lub reformujących unijne siły monitorują,

nadzorują i zalecają reformy i kierunki odbudowy obszarów działalności państwowej; dotyczy to obrony, policji, wymiaru sprawiedliwości czy administracji cywilnej. Operacje obserwacyjne polegają na nadzorowaniu procesu wprowadzania założeń porozumienia pokojowego bądź na uczestniczeniu w działaniach zmierzających do rozstrzygnięcia konfliktu na życzenie stron. Podejmowane są także działania wspierające misje zarządzania kryzysowego innych organizacji międzynarodowych. Dotyczy to m.in. działań prowadzonych przez ONZ czy Organizację Bezpieczeństwa i Współpracy w Europie (OBWE).

Unia Europejska ma ponadto możliwość nakładania sankcji dyplomatycznych, tj. odwołania własnych dyplomatów czy też uniemożliwienia wjazdu na swoje terytorium urzędników lub przedstawicieli państw trzecich. Wpływ sankcji dyplomatycznych na inne państwa jest jednak stosunkowo niewielki i stanowi możliwość zasygnalizowania niezadowolenia, gdy unijne państwa nie są w stanie osiągnąć porozumienia. Wśród pozawojskowych instrumentów podejmowanych w ramach działań prewencyjnych wykorzystuje się także instrumenty zewnętrznej polityki ekonomicznej, takie jak polityka stowarzyszeniowa, umowy handlowe, programy pomocowe oraz pomoc humanitarna. Aktywność UE jako stabilizatora pokoju i bezpieczeństwa międzynarodowego realizuje się przede wszystkim w formie instrumentów traktatowych (wspólne stanowiska i wspólne działania) oraz zwykłych oświadczeń i deklaracji w sprawach powstających zagrożeń, toczących się konfliktów oraz problemów wymagających współpracy i pomocy międzynarodowej po wygaszonych konfliktach.

Sabina Olszyk

B. Boutros-Ghali, *An Agenda for Peace. Preventive diplomacy, peacemaking and peace-keeping*, Report of the Secretary General pursuant to the statement adopted by the Summit Meeting of the Security Council on 31 January 1992, A/47/277-S/24111, 17 June 1992; G. Evans, *Współpraca dla pokoju. Agenda na lata 90. i następne*, Polski Instytut Spraw Międzynarodowych, Warszawa 1994; M.A. Macioszek, *Dyplomacja prewencyjna Unii Europejskiej w pozimnowojennej Europie*, Wydawnictwo Adam Marszałek, Toruń 2002; B. Muratii, *The Role of Preventive Diplomacy*, „European Journal of Research in Social Sciences" 2018,

vol. 6, no. 2; M. Musioł, *Operacje pokojowe i dyplomacja prewencyjna oraz ich podstawy w polityce zewnętrznej UE w XXI wieku*, „Rocznik Bezpieczeństwa Międzynarodowego" 2013, vol. 7; *Mały słownik stosunków międzynarodowych*, G. Michałowska (red.), Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1997; *Nowe oblicza dyplomacji*, B. Surmacz (red.), Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2013; W. Stankiewicz, *Dyplomacja prewencyjna jako środek utrzymania ładu na kontynencie europejskim*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio K" 2009, vol. 16, nr 1.

DYPLOMACJA WOJSKOWA – to działalność resortu → o b r o n y n a r o d o w e j [t. 3] w sferze → b e z p i e c z e ń s t w a [t. 1] i obronności państwa na arenie międzynarodowej oraz zestaw zadań stawianych reprezentantom sił zbrojnych, attaché wojskowym i innym przedstawicielom wojska w toku misji i operacji pokojowych oraz międzynarodowej działalności wojskowej. Stanowi rozszerzenie tradycyjnych ról dyplomacji oraz sił zbrojnych o nowe obszary działań opartych na pokojowym i kooperacyjnym prowadzeniu stosunków wojskowych. Głównym motywem działań dyplomacji wojskowej jest wzmocnienie obronności własnego państwa, a jej kluczowym podmiotem jest instytucja attaché wojskowego stojącego na czele ataszatu, wyodrębnionego w ramach ambasady.

Początki dyplomacji wojskowej są ściśle związane właśnie z działalnością attaché wojskowych. Ich rozmieszczenie w państwach przyjmujących oznaczało nawiązanie stosunków wojskowych z danym państwem. Także rozwój uzbrojenia i pojawienie się nowych sposobów prowadzenia walk spowodowały, że ich ocena i rozpoznanie mogły być dokonywane tylko przez osoby posiadające odpowiednie kwalifikacje wojskowe. Dlatego też głównym zadaniem attaché było rozpoznawanie potencjału wojskowego państwa przyjmującego. Pierwsze wzmianki o wojskowych przedstawicielach towarzyszących dyplomatom można znaleźć w źródłach już z czasów starożytnych i średniowiecza. W czasach nowożytnych, odkąd w XVI i XVII w. rozpowszechniły się misje dyplomatyczne, stojący na ich czele dyplomaci przesyłali do swoich krajów raporty dotyczące sytuacji politycznej, gospodarczej i militarnej w państwie swojej służby. Istotnym elementem raportów były → i n f o r m a c j e dotyczące sił zbrojnych państwa przyjmującego. Rzeczywisty rozkwit instytucji oficjalnego przedstawicielstwa pod postacią „obserwatora wojskowego" w składzie poselstwa

wiązał się z okresem wojen koalicyjnych w Europie na przełomie XVII i XVIII w. Oficer łącznikowy – emisariusz wojskowy – przydzielany był wówczas do armii sprzymierzonej w celu uzgadniania ruchów armii. Czynił to w sposób bardziej kompetentny, niż mogli to czynić ambasadorowie.

Rozwój myśli wojskowej i rywalizacja militarna państw w XIX w., szczególnie w okresie wojen napoleońskich, wywarły duży wpływ na określenie roli i zadań eksperta wojskowego. Wojny napoleońskie, które zaangażowały całą Europę i nasiliły współzawodnictwo wojskowe między państwami, wskazały potrzebę posiadania dokładnych i fachowych informacji o siłach zbrojnych innych państw. Podstawowym zadaniem dyplomatów wojskowych w owym czasie było więc pozyskiwanie informacji wywiadowczych w celu zabezpieczenia planowanych, podejmowanych i realizowanych działań wojskowych poza granicami własnego państwa. Doszło wówczas do stałego włączenia wojskowych w skład misji dyplomatycznych i wykształcenia się w ramach służby dyplomatycznej specjalności, jaką była dyplomacja wojskowa. W pewnym momencie uwypukliła się jednak postępująca rozdzielność misji dyplomatycznych od wojskowych, co wynikało nie tylko z coraz silniejszego wpływu prawa międzynarodowego, ale także z pragmatyki działania, kształtującej zasady i formy relacji międzypaństwowych. Reprezentacja i realizacja wojskowych interesów państwa i sił zbrojnych za granicą należała bezpośrednio do wojska, ale w ramach nadzoru państwowego. Bezpieczeństwo polityczno-militarne stanowiło bowiem motyw pierwotny obecności wojska w stosunkach międzynarodowych, a misje dowódców często obejmowały funkcje wpisane w kanon polityki i dyplomacji, obejmując takie działania jak negocjacje, reprezentację zagraniczną, akty → w o j n y [t. 4] i pokoju. Ta odrębna tożsamość dyplomacji wojskowej włączyła do procesów koordynacji polityki zagranicznej i bezpieczeństwa elementy wielopoziomowej rywalizacji w ramach systemu państwowego.

W kolejnych latach XIX w. i z początkiem XX w. instytucja attaché wojskowego była już rozpowszechniona w praktyce europejskiej oraz światowej i objęła takie kraje jak Rosja, Austria, Wielka Brytania, Kanada czy USA. Attaché jako eksperci wojskowi uzyskali wysoką pozycję w środowisku dyplomatów, odnoszono się do nich jednak z nieufnością, traktując często jako szpiegów. Nie było to zupełnie bezzasadne, bowiem

podczas I wojny światowej attaché wojskowi państw w niej uczestniczących wspierali w sposób legalny i nielegalny wysiłki wojenne swoich krajów. Niektórzy z nich angażowani byli przez swoje państwa do działań na rzecz ustanowienia pokoju lub zawieszenia broni. W latach międzywojennych ekspertów wojskowych wykorzystywano do negocjacji, kontroli i nadzoru nad porozumieniami rozbrojeniowymi oraz do prowadzenia dochodzeń w przypadku sytuacji konfliktowych i incydentów wojskowych. Z początkiem XX w. krąg dyplomatów wojskowych powiększył się wraz z pojawieniem się nowych rodzajów sił zbrojnych. Tradycyjne wojska lądowe zostały uzupełnione o siły morskie i powietrzne. Stąd obok attaché wojskowego pojawili się attaché morscy i lotniczy jako przedstawiciele tych rodzajów sił zbrojnych.

W czasie II wojny światowej rola ekspertów wojskowych sprowadzała się głównie do działalności wywiadowczej. Większość z nich wywodziła się ze służb technicznych, a najliczniejszą grupę stanowili oficerowie → a r t y l e r i i [t. 1]. Po wojnie współzawodnictwo militarne Wschodu i Zachodu oraz → z i m n a w o j n a [t. 4] ściśle powiązały ponownie działalność ataszatów z → w y w i a d e m [t. 4] wojskowym. Dyplomacja wojskowa stanowiła wówczas instrument rywalizacji między blokami wojskowo-politycznymi → N A T O [t. 3] i Układu Warszawskiego oraz środek realizacji doktryny i polityki → o d s t r a s z a n i a [t. 3]. W 1965 r. w USA dokonano sformalizowania roli attaché wojskowych, w wyniku czego dowódca wojskowy stał się głównym doradcą szefa misji dyplomatycznej i głównym punktem kontaktowym dla wywiadu. Do końca zimnej wojny ewolucja dyplomacji wojskowej nie przyniosła większych zmian, nadal skupiała się na stosunkach wojskowych. Zakres odpowiedzialności dyplomacji wojskowej uległ jednak z biegiem lat systematycznemu poszerzaniu.

Po 1989 r. dokonano rozdzielenia zadań dyplomacji wojskowej i służb wywiadowczych. W latach 90. XX w., wraz ze zmianą roli siły militarnej w osiąganiu celów politycznych państw oraz zmianą systemu komunikowania się i łączności pod wpływem rewolucji informatycznej i globalizacji, dyplomacja wojskowa stała się głównie narzędziem prowadzenia → d y p l o m a c j i p r e w e n c y j n e j. Jej miejsce zajęła wówczas → d y p l o m a c j a o b r o n n a, w ramach której wyróżniono przedstawiciela cywilnego ministra obrony, ustanawiając stanowisko i stopień dyplomatyczny

→attaché obrony [t. 1]. Był on szefem jednostki organizacyjnej funkcjonującej w ramach przedstawicielstwa dyplomatycznego – ataszatu obrony. W okresie pozimnowojennym, a zwłaszcza po 11 września 2001 r., znacznym zmianom uległy funkcje dyplomacji. Zadania poszczególnych podmiotów uzależnione były od tego, czy działają w ramach stosunków dwustronnych czy wielostronnych. W stosunkach bilateralnych ataszaty obrony realizowały szereg funkcji związanych z reprezentowaniem ogólnych celów polityki zagranicznej państwa, koordynacją współpracy wojskowej i promowaniem rodzimego przemysłu obronnego, informowaniem o polityce wojskowej i militarnych aspektach polityki zagranicznej własnego kraju oraz monitorowaniem →sytuacji kryzysowych [t. 4], konfliktów zbrojnych w innych regionach świata czy z kultywowaniem tradycji wojskowo-historycznych. Funkcje dyplomacji obronnej w ramach stosunków wielostronnych określa charakter danej organizacji międzynarodowej i funkcja, jaką pełni w niej dyplomata wojskowy. Inne były bowiem role w ramach ONZ, UE czy Unii Afrykańskiej (UA), a inne w sojuszach wojskowych takich jak NATO. Dzisiaj można nakreślić uniwersalne płaszczyzny, na których działają dyplomaci obrony. Jest to m.in. pełnienie funkcji stałych lub doraźnych ekspertów w narodowych przedstawicielstwach przy ONZ oraz na konferencjach międzynarodowych czy pełnienie funkcji obserwatorów lub funkcjonariuszy w tych organizacjach (oficerowie w Doraźnych Siłach Zbrojnych ONZ). Współcześnie, wraz z rozwojem stosunków multilateralnych i wykształceniem się dyplomacji obronnej, ogromne znaczenie mają wojskowe przedstawicielstwa przy sojuszach militarnych (NATO, Organizacja Układu o Zbiorowym Bezpieczeństwie), wojskowi przedstawiciele w instytucjach organizacji międzynarodowych (ONZ, UE, UA), oddziały wojskowe, misje pokojowe (→misja pokojowa [t. 3]) ONZ, operacje pokojowe innych organizacji międzynarodowych (UE, UA) oraz operacje wojenne NATO.

Pomimo stałego wzrostu czynników pozamilitarnych w kształtowaniu →bezpieczeństwa międzynarodowego [t. 1] dyplomacja wojskowa w swym tradycyjnym rozumieniu jest nadal obecna w stosunkach międzynarodowych. W drugiej dekadzie XXI w. nie tylko zachowuje ona, ale i wzmacnia swoją rolę w ramach dyplomacji państwa w realizacji celów polityki zagranicznej. W dalszym ciągu bowiem państwa sięgają po

środki militarne dla osiągania celów polityki zagranicznej, a skuteczna dyplomacja wojskowa zwiększa efektywność ich wykorzystania. Wynika to z sytuacji, w której znaczenie siły militarnej sukcesywnie wzrasta – zarówno jako czynnika zmian w → środowisku bezpieczeństwa [t. 4] międzynarodowego, jak i efektywnego instrumentu polityki państw. Potrzeba szybkiej reakcji na → zagrożenia bezpieczeństwa [t. 4] oraz trudności w rozwiązywaniu sytuacji konfliktowych za pomocą środków dyplomatycznych i politycznych sprawiły, że coraz większego znaczenia nabierają misje pokojowe, postrzegane w kontekście militarnym. Jednak podjęcie decyzji o użyciu sił zbrojnych jest zazwyczaj trudne, długotrwałe i obarczone wieloma uwarunkowaniami. Działania wojsk podlegają bowiem kontroli politycznej i szczególnemu nadzorowi → opinii publicznej [t. 3].

Współcześnie użycie siły militarnej w polityce międzynarodowej jest dopuszczalne w sytuacji konieczności ochrony własnego terytorium i jego obrony podczas agresji zbrojnej, ochrony i obrony terytorium sojuszników w przypadku agresji zbrojnej, ochrony porządku międzynarodowego, stabilności i bezpieczeństwa poprzez wykorzystanie siły zbrojnej do ograniczenia skutków konfliktów regionalnych. Użycie siły militarnej jest także dopuszczalne w sytuacji konieczności ochrony wartości ogólnoludzkich, tj. życia i zdrowia, a także ochrony własnych interesów, którym realnie lub potencjalnie zagraża niebezpieczeństwo. Użycie siły zbrojnej w polityce międzynarodowej w XXI w. wiąże się przede wszystkim z → kryzysami natury politycznej, ekonomicznej społecznej i militarnej. Sprowadza się do klasycznych konfliktów zbrojnych o charakterze wojny oraz do działań na rzecz ich stabilizowania i rozwiązywania. W tym drugim przypadku użycie siły militarnej wiąże się z różnego typu operacjami, których celem jest stabilizowanie środowiska bezpieczeństwa w regionie, subregionie lub lokalnie.

Użycie siły militarnej wymaga przy tym szerszej koncepcji działania, która nie sprowadza się jedynie do działań militarnych – sukces militarny nie stanowi bowiem obecnie gwarancji sukcesu politycznego, ekonomicznego czy społecznego. Dopuszczalne zaangażowanie sił zbrojnych w polityce międzynarodowej może mieć charakter operacji pokojowych czy misji stabilizacyjnych. Siła militarna jako czynnik polityki państwa ma więc nadal

szczególne znaczenie. Może stanowić narzędzie odstraszania, → a g r e s j i [t. 1] czy wreszcie odwetu. Do tych wymienionych tradycyjnych funkcji siły zbrojnej w XXI w. doszły nowe, związane z zapobieganiem i pokonywaniem sytuacji kryzysowych, kontrolą i nadzorem przestrzegania ustaleń wynikających z rezolucji ONZ oraz trwałym utrzymaniem pokoju i udzielaniem pomocy humanitarnej. Różnica w podejściu do wykorzystania siły zbrojnej przez państwa i ich organizacje przejawiała się w poszerzeniu zakresu jej działania w operacjach określanych mianem pokojowych.

Sabina Olszyk

J.E. Cheyre, *Defence Diplomacy*, [w:] *The Oxford Handbook of Modern Diplomacy*, J. Heine, A.F. Cooper, R.C. Thakur (eds.), Oxford University Press, Oxford 2013; L. Drab, *Dyplomacja obronna w procesie kształtowania bezpieczeństwa RP*, Difin, Warszawa 2018; M. Flemming, *Międzynarodowe prawo humanitarne konfliktów zbrojnych. Zbiór dokumentów*, M. Gąska, E. Mikos-Skuza (red.), AON, Warszawa 2003; J. Gryz, *Współczesne znaczenie siły militarnej w polityce międzynarodowej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2010, t. 4; tenże, *Współczesny kształt dyplomacji wojskowej*, [w:] *Nowe oblicza dyplomacji*, B. Surmacz (red.), Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2013; R. Kupiecki, *Dyplomacja obronna – próba konceptualizacji*, „Dyplomacja i Bezpieczeństwo" 2016, nr 1; S. Miłosz, *Dyplomacja wojskowa*, Comandor, Warszawa 2004; T.C. Shea, *Transforming military diplomacy*, „Joint Force Quarterly" 2005, vol. 38, no. 50; J. Sutor, *Leksykon dyplomatyczny*, Lexis Nexis, Warszawa 2005; Ustawa z dnia 27 lipca 2001 r. o służbie zagranicznej, Dz. U. 2001, nr 128, poz. 1403; A. Vagts, W.T.R. Fox, *Defence and Diplomacy. The Soldier and the Conduct of Foreign Relations*, King's Crown Press, New York 1958.

DYSCYPLINA WOJSKOWA – stanowi obok życia w stanie skoszarowania, hierarchii i konieczności wykonywania rozkazów element kultury organizacji wojskowych. Dyscyplina odnosi się do elementów kulturowych związanych z biurokracją i wykonywaniem znormalizowanych ćwiczeń, nabywaniem umiejętności, podejmowaniem działań głównie wykonywanych grupowo lub zespołowo, precyzyjnego przestrzegania formalnych zasad, przepisów i procedur, szczególnie gdy dotyczą ochrony, → b e z p i e c z e ń s t w a [t. 1] i → z a g r o ż e ń [t. 4], ale także np. w odniesieniu do konserwacji i obsługi maszyn, okrętów czy samolotów oraz działania

zgodnego z instrukcjami dowódcy lub przynajmniej w jego duchu i zgodnie z jego sposobem myślenia.

Nowoczesne instytucje wojskowe są zorganizowane i wspierane przez państwa w celu prowadzenia → w o j n y [t. 4] i egzekwowania porządku wewnętrznego. Dokładna równowaga między tymi dwoma zadaniami różniła się w zależności od stanu i okoliczności historycznych. W danym momencie armie są zwykle zaangażowane tylko w jedno z tych zadań. Tak więc armie europejskie, które walczyły w wojnach napoleońskich na początku XIX w., spędzały większość czasu w ciągu następnych 30 lat, tłumiąc wewnętrzne bunty. Czasami jednak armie wykonują oba zadania jednocześnie. Np. armia brytyjska od lat 70. XX w. do końca → z i m n e j w o j n y [t. 4] utrzymywała porządek w Irlandii Północnej i została rozmieszczona w Niemczech, aby powstrzymać wojnę ze Związkiem Radzieckim. Tylko w rzadkich przypadkach państwa – takie jak Kostaryka i, w mniejszym stopniu i z zupełnie innych powodów, Japonia – utrzymywały siły zbrojne tylko do celów wewnętrznych i ograniczonych celów obronnych. Jednak przed epoką państw narodowych nie można było tak wyraźnie rozróżnić tych zadań. Przygotowywanie się do wojny i walka były centralną misją wojska. Pomimo wzrostu znaczenia zadań humanitarnych i pokojowych, które siły zbrojne podejmowały od czasów zimnej wojny, walka nadal określa główne przekonania, wartości i złożone formacje symboliczne określające kulturę wojskową.

Sama kultura wojskowa nie jest bardziej jednorodna niż kultura ludzka lub sama wojna. Tak jak we wszystkich kulturach, mamy tu do czynienia z 4 odrębnymi i powszechnie wykorzystywanymi narzędziami: dyscypliną, etosem zawodowym, ceremoniami i etykietą. Generalnie jednak w każdym elemencie znajduje się próba radzenia sobie i przezwyciężenia niepewności związanej z wojną, narzucania pewnych wzorców, kontrolowania wyników wojny i nadawania jej znaczenia, co określić można jako właśnie kreowanie dyscypliny wojskowej. Kultura militarna jest skomplikowaną konstrukcją społeczną, ćwiczeniem kreatywnej inteligencji, dzięki której można wyobrazić sobie wojnę w określony sposób i przyjmować pewne racjonalizacje dotyczące sposobu prowadzenia wojny i jej celów. Choć jest to reakcja na wojnę, jednym z efektów kultury wojskowej jest wpływ na prawdopodobieństwo wystąpienia i formę samej wojny.

Dyscyplina wojskowa odnosi się do uporządkowanego postępowania personelu wojskowego – indywidualnie lub w formacji, w → b i t w i e [t. 1] lub w garnizonie – najczęściej zgodnie z zaleceniami dowódcy. Wysoki poziom dyscypliny zaczyna się od instrukcji i jest doskonalony poprzez powtarzalne ćwiczenia, które sprawiają, że pożądane działanie staje się nawykiem, co może tłumaczyć, dlaczego wielu uważa, że wojsko jest instytucją, która wymaga bezkrytycznego i natychmiastowego posłuszeństwa rozkazom. Oczywistym celem rytuałów dyscypliny jest zminimalizowanie zamieszania i dezintegrujących konsekwencji bitwy poprzez nadanie jej porządku. Dyscyplina zapewnia personelowi wojskowemu repertuar jasnych działań, które może on wykonywać z własnej inicjatywy lub w koordynacji z innymi osobami w celu szybkiego dostosowania się i zwycięstwa w bitwie. Innym celem, być może mniej oczywistym, jest zrytualizowanie → p r z e m o c y [t. 3] wojennej, oddzielenie jej od zwykłego życia. Postępowanie w zgodzie z zasadami dyscypliny uspokaja → ż o ł n i e r z y [t. 4], mówi, kiedy są „upoważnieni" do naruszania zwykłego tabu zabijania i niszczenia. W nowoczesnych siłach zbrojnych jest to sformalizowana i celowa praktyka. Jak twierdzi D. Grossman, głównym celem współczesnego szkolenia wojskowego jest przezwyciężenie naturalnej odporności żołnierza na zabijanie innych ludzi.

Istnieją różne próby odpowiedzi na pytanie o to, jakiej dyscypliny wymaga wojsko i jak ją osiągnąć. Można wskazać co najmniej 2 historyczne wzory. Jeden jest starożytny i ma związek ze względnym znaczeniem jednostek w porównaniu do jednostek wojskowych w prowadzeniu walki. Drugi jest nowoczesny i dotyczy zmieniających się metod egzekwowania dyscypliny.

Historycznie rzecz biorąc, organizacje wojskowe często były tylko charyzmatyczną grupą indywidualnych wojowników, z których każdy walczył o swoją reputację i honor. Czasami, ale głównie współcześnie, organizacja wojskowa wymaga wysokiego poziomu koordynacji z walkami prowadzonymi przez dobrze wyszkolone jednostki w formacji. Wojna jako walka indywidualnych bohaterów i wojowników nie jest pozbawiona dyscypliny i rytualności, o czym dobrze wiedzą czytelnicy *Iliady* Homera. Tego rodzaju walkami często rządzą skomplikowane konwencje i rytuały, potrzeba nadzwyczajnej dyscypliny osobistej, by

przezwyciężyć strach przed bliską walką, znieść fizyczny wysiłek bitwy i udowodnić swoje możliwości poprzez umiejętność posługiwania się bronią. Tak rozumiana dyscyplina wojskowa nie ograniczała się do piechoty. Była charakterystyczna dla wojny zdominowanej przez kawalerię, od starożytnych jeźdźców, po zrytualizowaną feudalną wojnę europejskich rycerzy czy wyprawy Kozaków. →Walka powietrzna [t. 4] wśród pilotów myśliwców kontynuuje tę tradycję w odniesieniu do współczesnej wojny. W takich przypadkach dyscyplina wojskowa jest osobistym osiągnięciem uzyskanym poprzez indywidualne kompetencje i wysiłek.

Silny kontrast w tym zakresie stanowi wojna oparta na dyscyplinie grupowej dobrze wyszkolonej piechoty. Niezależnie od tego, czy wziąć pod uwagę hoplitów starożytnej Grecji, szwajcarskich pikinierów walczących z rycerzami feudalnymi, armie Maurycego Orańskiego i Gustawa II Adolfa wykorzystującego moc prochu, czy też prowadzenie wspólnych operacji zgodnie z doktryną współczesnej bitwy powietrzno-lądowej, walki te przewidują skoordynowany i jednoczesny ruch żołnierzy jako grupy w odpowiedzi na polecenia ich przywódców. Jest to możliwe tylko po niezliczonych godzinach instruktażu i wielu praktykach w sztuce dyscypliny. W takich armiach indywidualna wola jest podporządkowana grupie. Rezultaty dyscypliny grupowej często były zadziwiające, umożliwiając dobrze zdyscyplinowanym żołnierzom wywołanie ogromnego wstrząsu podczas ataku i pozostanie nietkniętym, jednocześnie niszcząc siły wroga. Wyniki takie uzyskiwano jednak określonym kosztem. Ponieważ dyscyplina grupowa wymaga ciągłych ćwiczeń przygotowujących do wojny, ilekroć była szczególnie ważna, konieczne stawało się tworzenie albo klasy wojskowej, jak w starożytnej Sparcie i Japonii w okresie samurajów, albo profesjonalnej armii stałej, jak w Europie od XVII w. Wyjątkiem mogą być tu masowe armie powstałe pod koniec XIX w. w krajach uprzemysłowionych, używane do prowadzenia wojen światowych w XX w. Masowe armie zależały od dyscypliny grupowej, ale obsadzone były w drodze poboru. Wywoływało to problemy z integracją – niektóre wciąż nierozwiązane nawet w armiach zawodowych – dotyczące znaczenia różnic opartych na rasie lub pochodzeniu etnicznym, religii, płci lub orientacji seksualnej. Jak dowodzą liczni badacze, tradycyjne rytuały przejścia – takie jak strzyżenie, przybieranie

jednolitych strojów, pieśni śpiewane podczas marszu piechoty i ceremonie wojskowe – zostały wytworzone w celu tłumienia indywidualności i wykształcenia wspólnej tożsamości.

Ani luźniejsza dyscyplina poszczególnych żołnierzy, ani surowsza dyscyplina dobrze wyszkolonej piechoty nie gwarantowały zwycięstwa albo przetrwania w bitwie. Historycznie dominacja jednego rodzaju dyscypliny zależała w dużej mierze od tego, jakiego rodzaju broni używano. Współczesne kultury wojskowe zakładają wysoki (być może nawet rosnący) poziom dyscypliny grupowej w ramach swojej → s t r a t e g i i [t. 4] operacyjnej i robią to, z pewnymi wyjątkami, od XVII w.

Dyscyplina funkcjonalna jest i była istotnym elementem zorganizowanej armii, będąc też częścią kultury walki. Jej istnienie prowadzi wg niektórych do makdonaldyzacji wojska, czyniąc działania zbrojne wysoce znormalizowanymi i przewidywalnymi. Dyscyplina w kontekście instrukcji kulturowych jest uważana niekiedy za ważniejszą niż kompetencje, a jej nieprzestrzeganie czyni wojskowego kulturowo niedopasowanym – w takiej sytuacji może on zostać przeniesiony na stanowisko, na którym jego niedopasowanie będzie mniej szkodliwe. Przestrzeganie zasad wynikających z dyscypliny jest istotne, aby organizacja była skuteczna, bezpieczna i przewidywalna, aby uniknąć etycznych nadużyć zarówno wobec osób z zewnątrz, jak i osób z wewnątrz, a także by chronić tych, którzy podlegają działaniom wojska.

Oprócz dyscypliny funkcjonalnej organizacje wojskowe przywiązują dużą wagę do dyscypliny ceremonialnej. Bardziej niż w innych organizacjach wygląd i etyka grupowa są uważane za ważne w wojsku. Oznacza to odpowiedni strój, fryzurę, salutowanie i maszerowanie w szeregu. Ma to historyczne korzenie: poprzez użycie sztandarów, rytm bębnów i trąb oraz kolorowe mundury można było odróżnić przyjaciół od wrogów. Podobnie jak taniec na festynach we wspólnocie, maszerowanie i wspólne ćwiczenia poprawiają samopoczucie i ułatwiają wszelkiego rodzaju wspólne wysiłki – fizyczne i psychiczne. Dzisiaj ceremonia i etyka są ważne, aby podkreślić specyfikę grupy, wizualizują wspólną tożsamość jednostek wojskowych, która ma szczególne znaczenie w chwilach zagubienia i smutku. Oczywiście organizacje wojskowe przeżywają te chwile znacznie częściej niż organizacje konwencjonalne.

Być może poza wojną ceremonie i etykieta, które przenikają życie wojskowe, są najbardziej widocznymi elementami współczesnej kultury wojskowej. Jednobarwne mundury i rozwinięte flagi stanowiły pomoc dla dowódców i żołnierzy we wczesnej nowoczesnej wojnie, choćby dlatego, że pomagały odróżnić siły przyjazne od sił wroga. Podobnie bębny i hejnały, które przerywały dzień w garnizonie, pomagały utrzymać system komunikacji w celu kierowania siłami. Parady piesze i współczesne pokazy lotnicze lotników wojskowych ukazują doskonałość w ruchu i manewrach, prezentując cel, którego istota polega na wskazaniu, że dobrze wyszkolona armia osiąga powodzenia w bitwie. Połączenie ceremonii wojskowych i etykiety z wojną jest luźniejsze i bardziej subtelne, niż sądzi się powszechnie. Dzisiejsze pola bitew wymagają kamuflażu strojów, komunikacji elektronicznej i rozproszonego ruchu pojazdów silnikowych, ale mundury wojskowe na specjalne okazje są w jaskrawych kolorach, a odgłosy bębnów wciąż towarzyszą paradom wojskowym. Ceremonie wojskowe i etykieta składają się na skomplikowany rytuał i odgrywają taką rolę, jaką rytuał zwykle odgrywa w społeczeństwie. Są elementem dyscypliny wojskowej, mają kontrolować lub maskować lęki i ignorancję, aby potwierdzić solidarność ze sobą i jedność, zwykle odnosząc się do wyższych celów, takich jak państwo, honor czy ojczyzna.

Jakub Idzik

J. Burk, *Military Culture*, [w:] *Encyclopedia of Violence, Peace & Conflict*, L. Kurtz (ed.), Elsevier, Oxford 2008; K. Dunivin, *Military Culture: Change and Continuity*, „Armed Forces & Society" 1994, vol. 20; A. King, *The combat soldier. Infantry Tactics and Cohesion in the Twentieth and Twenty-First Centuries*, Oxford University Press, Oxford 2013; W.H. McNeill, *Keeping Together in Time. Dance and Drill in Human History*, Harvard University Press, Cambridge 1995; J. Soeters, *Organizational Cultures in the Military*, [w:] *Handbook of the Sociology of the Military*, G. Caforio, M. Nuciari (eds.), Springer International Publishing, Cham 2018; R. Sennett, *Together. The Rituals, Pleasures & Politics of Cooperation*, Penguin Books, London 2013; J. Soeters, *Culture in Uniformed Organizations*, [w:] *Handbook of Organizational Culture and Climate*, N.M. Ashkanasy, C.P.M. Wilderom, M.F. Peterson (eds.), Sage, Thousand Oaks 2000; P.H. Wilson, *Defining Military Culture*, „The Journal of Military History" 2008, vol. 72 (1).

DYSFUNKCYJNE PAŃSTWO (państwo upadłe, ang. *failed state*) – państwo, które czasowo utraciło monopol (całkowicie lub częściowo) sprawowania władzy nad terytorium i/lub ludnością, nadal jednak mające uznanie międzynarodowe. Termin państwo upadłe wprowadzili na początku lat 90. XX w. G. Helman oraz S. Ratner, po raz pierwszy użyto tego sformułowania w artykule *Anarchy Rules: Saving Failed States*, który opublikowano w 1993 r. na łamach magazynu „Foreign Policy", natomiast 2 lata później wydano książkę pod tytułem *Collapsed States: The Disintegration and Restoration of Legitimate Authority* W. Zartmana. Przez lata pojęcie to funkcjonowało w szczególności w środowisku akademickim.

Państwo dysfunkcyjne, nawet jeśli pozornie posiada atrybuty państwowości (terytorium, ludność, władzę, uznanie międzynarodowe), nie może lub nie chce wykonywać podstawowych obowiązków wynikających z istoty → s u w e r e n n o ś c i [t. 4], tj. sprawowania wyłącznej i całkowitej kontroli nad określonym terytorium, zapewnienia ludności minimum praw ochrony życia i zdrowia, powstrzymania siebie lub swoich obywateli od naruszania imperatywnych norm prawa międzynarodowego, nie posiada monopolu na → p r z e m o c [t. 3]. Pewnymi cechami takiego państwa są też: nieprawidłowe zarządzanie państwem, nadużywanie władzy, → k o r u p c j a, słabość instytucji państwowych, występowanie konfliktów wewnętrznych oraz brak odpowiedzialności państwa. O państwie dysfunkcjonalnym możemy mówić wtedy, gdy faktycznie przez jakiś czas sprawowało władzę nad mieszkańcami i formalnie określonymi terytoriami, lecz na znacznym obszarze rząd utracił władzę terytorialną na rzecz innych ośrodków dysponujących środkami przymusu.

Według R.I. Rotberga państwa dysfunkcyjne osiągają różny stopień dysfunkcyjności: państwo słabe (ang. *week state*), państwo upadające (ang. *falling state*), państwo upadłe (ang. *failed state*) oraz państwo w stanie rozkładu (ang. *collapsed state*) W literaturze spotyka się też pojęcia wprowadzone prze ONZ: państwo przeżywające napięcia (ang. *state under stress*), kraje wychodzące z konfliktów (ang. *countries emerging from conflict*). Państwa takie są przeważnie pełnoprawnymi członkami ONZ, dlatego używanie wobec nich określenia „upadłe" bądź „upadające" budziłoby wątpliwości dotyczące ich międzynarodowego statusu prawnego. Administracja amerykańska B. Clintona wprowadziła też pojęcie państwa

zbójeckiego (ang. *rogue state*), ale termin ten odnosił się do państw wrogich interesom USA.

Do przyczyn dysfunkcyjności państwa można zaliczyć dziedzictwo systemu kolonialnego, a zwłaszcza niszczenie tradycyjnych struktur społecznych, wyznaczanie granic państw pokolonialnych, nie bacząc na tradycyjne podziały etniczne. Wśród innych przyczyn należałoby wymienić koniec → z i m n e j w o j n y [t. 4], a także związane z nią walki ideologiczne supermocarstw finansujących nieudolne i skorumpowanych rządy, często dla pozyskania wpływów. Ponadto czynnikiem wpływającym na kryzys państw mogą być globalne procesy modernizacyjne i pozostawanie poza główną falą modernizacji (tzw. państwa peryferie w teorii systemów-światów I. Wallersteina). Wreszcie upadek państwa może być powodowany czynnikami endogennymi, zwłaszcza: ustrojowymi, demograficznymi, etnicznymi, ekonomicznymi czy ekologicznymi.

Istotny wpływ na upadłość państw miała również demokratyzacja państw Trzeciego Świata na podstawie modelu zachodniego. Proces globalizacji przyczynił się do utraty autorytetu państwa, erozji systemu legitymizacji, braku monopolu reprezentującego państwo w środowisku międzynarodowym oraz niezdolności do kierowania służbami publicznymi.

Istotą upadłego państwa jest: upadek porządku państwowego, wewnętrzne konflikty zbrojne, masowe naruszenia praw człowieka i kryzysy humanitarne, fragmentaryzacja społeczeństwa. Do najczęstszych skutków można zaliczyć: rozkład struktur państwa, wzrost → p r z e s t ę p c z o ś c i [t. 3] i przemocy kryminalnej, groźbę eskalacji zagrożenia na kraje sąsiednie, utratę kontroli nad granicami i częścią terytorium, kryzys ekonomiczny, masową migrację.

Organizacja pozarządowa The Fund for Peace we współpracy z „Foreign Policy" co roku publikuje Failed States Index (Fragile States Index), swoisty ranking państw szeregujący je pod względem stabilności. Od lat za państwa najgorzej funkcjonujące są uznawane: Somalia, Sudan Południowy (od momentu powstania), ale także Demokratyczna Republika Konga, Jemen, Sudan, Czad czy Irak. Po drugiej stronie rankingu na ogół znajdują się państwa skandynawskie, Australia, Nowa Zelandia i Kanada. W 1994 r. utworzono State Failure Task Force (obecnie Political Instability Task Force – PITF), projekt badawczy wspierany przez rząd USA (głównie CIA),

mający na celu zbudowanie bazy danych na temat głównych przyczyn politycznych dysfunkcyjności państw. W badaniu przeanalizowano czynniki określające skuteczność instytucji państwowych, dobrobytu populacji i rozwoju handlu międzynarodowego. Ciekawym spostrzeżeniem jest korelacja pomiędzy śmiertelnością niemowląt a → k r y z y s e m państwa.

Przemysław Mazur

Bezpieczeństwo międzynarodowe. Przegląd aktualnego stanu, K. Żukrowska (red.),Wydawnictwo IUSatTAX, Warszawa 2011; Center for Systemic Peace, *PITF State Failure Dataset*, http://www.systemicpeace.org/inscrdata.html (dostęp 15.12.2019); J. Czaputowicz, *Bezpieczeństwo międzynarodowe. Współczesne koncepcje*, PWN, Warszawa 2012; S.S. Eriksen, *„State Failure" in Theory and Practice: The Idea of the State and the Contradictions of State Formation,* „Review of International Studies" 2011, no. 1; R. Kłosowicz, *Państwa upadłe i ich destabilizujący wpływ na stosunki międzynarodowe*, [w:] *Czynniki stabilizacji i destabilizacji w stosunkach międzynarodowych na początku XXI wieku*, I. Stawowy-Kawka (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009; R. Kłosowicz, A. Mania, *Problem upadku państw w stosunkach międzynarodowych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012; P. Mazur, *Państwo dysfunkcyjne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

DYWERSJA (od łac. *diversio*, odwrócenie uwagi, różnica) – skryte, starannie przygotowane działania wywrotowe (podpalenie, zniszczenie itd.), a także zastosowanie innych metod niszczenia niezwiązanych z przebiegiem → b i t w y [t. 1], prowadzone przez specjalnie przeszkolonych agentów lub grup w czas pokoju i → w o j n y [t. 4] na terytorium jakiegokolwiek państwa lub terytorium zajmowanym przez wroga w celu osłabienia jego siły gospodarczej i militarnej, a także niszczenia → m o r a l e [t. 3] i patriotyzmu społeczeństwa. Dywersja to również działania sabotażowe lub propagandowe prowadzone na terytorium wroga w celu dezorganizacji podejmowanych przez niego przedsięwzięć. Dywersja prowadzi do zakłócenia życia politycznego i gospodarczego państwa, co z kolei przysparza korzyści agresorowi. Pojęcie to odnosi się przede wszystkim do aspektów militarnych, związanych z podjęciem działań skierowanych przeciwko obronności państwa.

Należy jednak zauważyć, iż dywersja prowadzona jest zarówno w czasie stanu → z a g r o ż e n i a [t. 4] i wojny, jak również w stanie pokoju, kiedy przedmiotem zainteresowania sabotującego stają się przedsięwzięcia polityczne i gospodarcze. Dywersja to także długofalowe oddziaływanie na wrogie społeczeństwo w celu jego demoralizacji oraz dezintegracji struktur państwowych, wprowadzenie w błąd → o p i n i i p u b l i c z n e j [t. 3] i personelu; poczynienie znaczącej szkody potencjałowi gospodarczemu wroga (np. dywersja elektrowni atomowej); zrozumienie przez potencjalnego wroga, że operacje wojskowe mogą zmienić się w katastrofę ekologiczną, społeczną i polityczną.

Początkowo dywersją były nazywane operacje militarne przeprowadzane przez nieznaczne siły w celu dezorientacji wroga, odwrócenia jego uwagi i sił od głównego kierunku ataku. Na początku XX w. dywersja była traktowana jako rodzaj bitwy.

Dywersja została zdefiniowana także w dokumencie Sztabu Generalnego Wojska Polskiego w 1922 r. pt. *Dywersja nieprzyjacielska na terenie państwa polskiego*, gdzie zaznacza się, iż dywersja rozumiana jest jako

> akcja nieprzyjacielskich biur wywiadowczych lub specjalnych, której zadaniem jest planowanie, zniszczenie, paraliżowanie i osłabianie życia państwowo-społecznego danego państwa, bez względu na użyte środki. Dywersję prowadzą specjalnie przeszkoleni agenci, działacze opozycyjnych partii politycznych oraz osoby, które sympatyzują z obcymi państwami.

Podczas II wojny światowej antyniemiecki ruch oporu i ruchy partyzanckie w Europie praktykowały skuteczne dywersje przeciwko fabrykom, obiektom wojskowym, kolejom, mostom itp. Po wojnie dywersja stała się podstawową bronią licznych grup powstańczych związanych z ruchami antykolonialnymi, separatystycznymi i popieranymi przez komunistów.

Obecnie wśród dywersji można wyróżnić:

- sabotaż dywersyjny – działania bojowe na tyłach wojsk przeciwnika, mające na celu utrudnienie mu działalności na froncie; dywersja to jeden z podstawowych elementów → s t r a t e g i i [t. 4] wojny partyzanckiej;

- dywersję gospodarczą – ma na celu długofalowe i systematyczne niszczenie struktur gospodarczych przeciwnika; może polegać na niszczeniu obiektów gospodarczych i ich unieruchamianiu, jak też na przechwytywaniu dokumentacji technicznej;
- →dywersję polityczną (dywersja ideologiczna) – zespół wypracowanych naukowo form i metod w sferze ideologicznego oddziaływania (działania i →operacje psychologiczne [t. 3], →wojna psychologiczna [t. 4]) i →propagandy [t. 3] dla spowodowania określonej atmosfery w społeczeństwie poprzez manipulację i →dezinformację.

Przedsięwzięcia dywersyjne są działaniami o charakterze ideologicznym, propagandowym oraz psychologicznym, prowadzonym z wykorzystaniem form nieregularnych (w tym poprzez narzędzia →wojny informacyjnej [t. 4]). Bez względu na wykorzystane instrumentarium celem prowadzonych działań jest wewnętrzna destabilizacja kraju, prowadząca do zakłócenia porządku publicznego, narastania strachu, podważenia obowiązującego systemu politycznego oraz administracji państwa.

Za pomocą narzędzi wojny informacyjnej prowadzone są działania zmierzające do uzyskania wpływu na percepcję społeczeństwa, jego sferę mentalną oraz system dystrybucji →informacji. Wojna informacyjna definiowana jako zorganizowane oddziaływanie na sferę psychiczną społeczeństwa, w celu uzyskania kierunkowych zamierzeń politycznych, militarnych i gospodarczych, stanowi doskonałą platformę dla stosowania dywersji.

Głównym bezpośrednim obiektem dywersji jest →bezpieczeństwo [t. 1] państwa w sferze gospodarczej, środowiskowej, wojskowej lub innej, zgodnie z ukierunkowaniem określonego aktu dywersji.

Przedmiotem dywersji mogą być:

- budynki, budowle i inne przedmioty o dużym znaczeniu gospodarczym lub obronnym, od działalności których zależy istnienie niektórych regionów lub innych dużych terytoriów, właściwe funkcjonowanie niektórych sektorów gospodarki, struktur administracji publicznej (elektrownie, rurociągi wodne, gazowe, naftowe; mosty, tamy; systemy komunikacji informacyjnych; stacje kolejowe, lotniska, porty morskie lub porty rzeczne, metro lub

inne ważne przedsiębiorstwa, bez względu na formy własności, jednostki wojskowe itd.), w tym przedsiębiorstwa, których zniszczenie lub uszkodzenie jest samo w sobie zagrożeniem (chemiczne, biologiczne przedsiębiorstwa, przedsiębiorstwa produkcji materiałów wybuchowych i łatwopalnych produktów, a także ich magazynowania);

- stada zwierząt, ryb w stawach i innych zbiornikach wodnych, pasieki itp.;
- uprawy rolne lub inne uprawy, lasy itp.

Obiektywna strona dywersji objawia się w 7 formach, z których każda polega na popełnianiu niebezpiecznych społecznie działań mających na celu:

- masowe niszczenie ludzi, obrażenia lub inne szkody dla ich zdrowia;
- zniszczenie lub uszkodzenie przedmiotów o dużym znaczeniu gospodarczym lub obronnym;
- zanieczyszczenie radioaktywne;
- masowe zatrucie;
- rozprzestrzenianie epidemii – rozprzestrzenienie się zakaźnych chorób ludzi (dżumy, cholery itp.), które zachodzi w stosunkowo krótkim czasie, gdy zachorowalność zakaźna populacji w danej miejscowości i w pewnym momencie przekracza zwykły poziom charakterystyczny dla tej choroby zakaźnej i charakteryzuje się odpowiednią dynamiką;
- rozprzestrzenianie epizootii (pomór, zaraza) – występowanie zachorowań na jedną z chorób zakaźnych wśród zwierząt domowych lub dzikich na danym terenie; to proces masowego rozprzestrzeniania się chorób zakaźnych (zakaźnych i pasożytniczych, np. wścieklizna, dżuma, pryszczyca itp.) zwierząt rolniczych, domowych, trzymanych w zoo, laboratoryjnych, dzikich, cyrkowych, futerkowych, domowych i dzikich ptaków, pszczół, ryb, żab, innych przedstawicieli fauny, dotyczy także zarodków, jaj wylęgowych, jaj zapłodnionych itd.;
- rozprzestrzenianie się epifitozy – masowe występowanie zachorowań na jedną chorobę w danym czasie i miejscu wśród roślin, znaczące rozprzestrzenienie się grzybowych, wirusowych lub bakteryjnych

chorób upraw, plantacji leśnych, roślin wodnych i innych. Takie choroby mogą być wywoływane przez szkodniki (owady, kleszcze, mikroorganizmy) lub fitopatogeny (wirusy, bakterie, grzyby).

Dywersja, organizowana w dowolnej formie, zostaje zakończona, gdy nastąpi eksplozja, podpalenie, powódź, zapaść lub inna działalność, bez względu na to, czy faktycznie wystąpiły jakieś skutki. Charakterystyczną oznaką dywersji jest to, że popełnienie wymienionych działań nie jest celem samym w sobie, lecz jest wykorzystywane przez wroga jako środek do osiągnięcia jego głównego celu – osłabienia państwa.

Jacek Bil, Olga Wasiuta

T. Chinciński, *Niemiecka dywersja w Polsce w 1939 r. w świetle dokumentów policyjnych i wojskowych II Rzeczypospolitej oraz służb specjalnych III Rzeszy. Cz. 1 (marzec – sierpień 1939 r.)*, „Pamięć i Sprawiedliwość" 2005, nr 4/2 (8); D. Gibas-Krzak, *Działalność terrorystyczna i dywersyjno-sabotażowa nacjonalistów ukraińskich w latach 1921–1939*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3; M. Romański, *O sabotażu i dywersji w świetle polskiego ustawodawstwa po 1944 roku*, „Czasopismo Prawno-Historyczne" 2013, t. 65, z. 1; L. Sykulski, *Rosyjska polityka a wojna informacyjna*, PWN, Warszawa 2019; K. Śledziński, *Cichociemni. Elita polskiej dywersji*, Wydawnictwo Znak, Warszawa 2012; *Typology of Diversion. A Statistical Analysis of Weapon Diversion Documented by Conflict Armament Research*, „Diversion Digest" 2018, vol. 1; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017.

DYWERSJA POLITYCZNA – polega na nieoficjalnym działaniu aktorów politycznych, których celem jest osiągnięcie określonego skutku czy efektu, który jednak zwykle nie jest wcześniej znany →opinii publicznej [t. 3]. Współcześnie dywersja polityczna rozgrywa się głównie na płaszczyźnie psychologicznej i sprowadza się do działań manipulacyjnych lub propagandowych, które mają wywołać określone odczucia społeczne, przekonać do konkretnych racji czy poglądów, niejednokrotnie wynikających z określonego sposobu operowania opiniami, nie zaś faktami. Efektem dywersji politycznej jest ukierunkowanie działań na osiągnięcie celu, ale także niejednokrotnie odwrócenie uwagi społecznej od innego kręgu problemów.

Samo pojęcie → d y w e r s j i [t. 1] pochodzi z terminologii wojskowej, w której oznacza osłabienie nieprzyjaciela dokonane jednak nie w walce prowadzonej typowymi metodami, ale dokonane z ukrycia czy zaskoczenia. Jako typowe działania dywersyjne podaje się w tym kontekście wysadzanie mostów i dróg czy przerywanie łączności wroga.

Charakterystycznym tematem współczesnych badań sytuujących się na pograniczu nauk o polityce i o → b e z p i e c z e ń s t w i e [t. 1] jest weryfikacja teorii dywersji, która odnosi się do odpowiedzi na pytanie o przyczyny, dla których liderzy polityczni są skłonni do użycia siły. Liczni badacze zarówno na płaszczyźnie rozważań teoretycznych, jak i w oparciu o wyniki złożonych analiz empirycznych dowodzą, że np. prezydenci USA decydują się na użycie siły, ponieważ łatwo im uzyskać w tym zakresie poparcie międzynarodowej i krajowej społeczności. Decydując się na takie działania, prezydenci USA mogą uzasadnić użycie siły, ukrywając swoją motywację, a wskazując na konieczność ochrony → p r a w c z ł o w i e k a [t. 3], udzielenia odpowiedzi na wezwanie do interwencji, podkreślając porażkę międzynarodowych podmiotów i instytucji w rozwiązywaniu problemów, która uzasadnia działanie zbrojne. Badacze stawiają jednak hipotezę, że prezydenci decydują o interwencji zbrojnej, kiedy napotykają problemy w polityce wewnętrznej.

Podstawowym argumentem teorii dywersji jest wskazanie, że przywódcy prowadzą agresywną, wojowniczą lub eskalującą politykę zagraniczną w obliczu wewnętrznych problemów społecznych, ekonomicznych lub politycznych, które zagrażają ich politycznemu przetrwaniu. Przywódcy dążą do konfliktu za granicą, aby zwiększyć poparcie społeczne w swojej ojczyźnie, odwracają uwagę od problemów wewnętrznych poprzez gromadzenie się wokół idei patriotycznych lub poprzez wykazanie się kompetencjami pozwalającymi odbierać ich jako mężów stanu. Jedynym lub podstawowym celem takiego dywersyjnego działania jest wzmocnienie szans przetrwania politycznego we własnym państwie, przeciwdziałanie wewnętrznym → z a g r o ż e n i o m [t. 4] dla sprawowanej przez siebie władzy politycznej, a nie zapobieganie zagrożeniom zewnętrznym, takim jak przetrwanie własnego państwa, jego bezpieczeństwo lub dbanie o inne → i n t e r e s y n a r o d o w e.

W przypadku USA zarówno badacze, jak i media poddają analizie szereg przykładów dywersji politycznych stosowanych przez prezydentów tego państwa. Podczas wojny w Zatoce Perskiej w 1991 r. podkreślano, że prezydent G.H.W. Bush próbował odwrócić za sprawą toczącego się konfliktu zbrojnego uwagę opinii publicznej od rosnącego deficytu budżetowego i innych wewnątrzkrajowych problemów. Podobnie zezwolenie prezydenta B. Clintona z 1998 r. na wystrzelenie pocisków samosterujących, uderzających w cele terrorystyczne w Afganistanie i Sudanie, zostało wydane zaledwie 3 dni po przyznaniu się przez prezydenta do romansu z M. Lewinsky, co było przyczyną istotnego skandalu obyczajowo-politycznego w USA. Również decyzję prezydenta Busha o → i n w a z j i na Irak można wiązać z wyborami prezydenckimi z 2002 r. i wyraźną perspektywą słabnącej pozycji Busha w sondażach przedwyborczych.

Rafał Klepka

L.M. Andrade, *Presidential Diversionary Attempts: A Peaceful Perspective*, „Congress & the Presidency: A Journal of Capital Studies" 2003, vol. 30, iss. 1; K. DeRouen, J. Peake, *The Dynamics of Diversion: The Domestic Implications of Presidential Use of Force*, „International Interactions" 2002, vol. 28, iss. 2; M.T. Fravel, *The Limits of Diversion: Rethinking Internal and External Conflict*, „Security Studies" 2010, vol. 19, iss. 2; R. Klepka, *Dywersja polityczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; J. Tir, *Territorial Diversion: Diversionary Theory of War and Territorial Conflict*, „The Journal of Politics" 2010, vol. 72, iss. 2; E. Tokdemir, B.S. Mark, *When Killers Become Victims: Diversionary War, Human Rights, and Strategic Target Selection*, „International Interactions" 2017, vol. 44, iss. 2.

DZIECKO ŻOŁNIERZ lub „żołnierz dziecięcy" – w potocznym rozumieniu oznacza osobę niepełnoletnią, która dysponuje bronią i walczy w szeregach armii regularnej, armii nieregularnej, grupach zbrojnych, bojówkach lub oddziałach milicji. W 1997 r. na sympozjum w Kapsztadzie nt. zapobiegania rekrutacji dzieci w szeregi sił zbrojnych, → d e m o b i l i z a c j i [t. 1] i społecznej reintegracji dzieci → ż o ł n i e r z y [t. 4] w Afryce przyjęto definicję nieodnoszącą się wyłącznie do dziecka, które nosiło lub nosi broń. Pojęciem dziecka żołnierza określa się każdą osobę poniżej 18. roku życia, która w dowolnej roli należy do jakiejkolwiek regularnej lub nieregularnej

siły zbrojnej lub grupy zbrojnej, włącznie, ale nie tylko, z kucharzami, tragarzami, posłańcami, oraz każdą osobę towarzyszącą takim grupom, inną niż członek rodziny. Termin ten obejmuje również dziewczęta rekrutowane do celów seksualnych i przymusowych małżeństw. Definicja kapsztadzka służy celom programowym i nie jest definicją prawną. Jednak tę samą wykładnię pojęcia dziecka żołnierza zawiera *Przewodnik do Protokołu fakultatywnego w sprawie angażowania dzieci w konflikty zbrojne*.

Biuro Specjalnego Przedstawiciela Sekretarza Generalnego Organizacji Narodów Zjednoczonych ds. Dzieci i Konfliktów Zbrojnych powołuje się na zasady i wytyczne paryskie opublikowane w 2007 r. W dokumencie tym nie użyto terminu „dziecko żołnierz", ale „dziecko związane z siłami zbrojnym lub grupami zbrojonymi", nazwy odnoszącej się do każdej osoby poniżej 18. roku życia, która jest lub była rekrutowana albo wykorzystywana przez siły zbrojne lub grupę zbrojną w jakimkolwiek charakterze, w tym, ale nie wyłącznie, dzieci, chłopcy i dziewczęta, używani jako bojownicy, kucharze tragarze, szpiedzy lub do celów seksualnych. Określenie obejmuje zatem nie tylko dziecko, które bierze lub brało bezpośredni udział w działaniach wojennych. Wykorzystywanie seksualne nie ogranicza się wyłącznie do dziewcząt, jak w przypadku definicji kapsztadzkiej. Tym samym termin „dziecko żołnierz" ma zastosowanie do chłopców rekrutowanych w celach seksualnych, łącznie z praktyką baczczebazi (ang. *bacha bazi*) – „tańczących chłopców" w Afganistanie. „Siły zbrojne", które prowadzą nabór, to instytucje wojskowe państwa mające podstawę prawną oraz wsparcie infrastruktury instytucjonalnej w postaci m.in. wynagrodzeń, świadczeń, podstawowych usług itd. „Grupy zbrojne" oznaczają grupy odrębne od sił zbrojnych zgodnie z definicją zawartą w art. 4 Protokołu fakultatywnego do Konwencji o prawach dziecka w sprawie angażowania dzieci w konflikty zbrojne.

„Rekrutacja" dziecka żołnierza oznacza rekrutację obowiązkową, przymusową i dobrowolną do każdego rodzaju regularnych lub nieregularnych sił lub grup zbrojnych. Protokół fakultatywny w sprawie angażowania dzieci w konflikty zbrojne, oprócz wskazania przypadku dobrowolnej rekrutacji, implikuje także rekrutację do sił zbrojnych i grup zbrojnych pod przymusem (art. 3 i 4). Pobór do sił zbrojnych oznacza rekrutację prowadzoną przez rząd przy użyciu wszystkich środków, za pomocą których dziecko

staje się członkiem narodowych sił zbrojnych. W tym przypadku mamy do czynienia z „poborem obowiązkowym" i „ochotniczym wstępowaniem".

„Pobór obowiązkowy" odbywa się obligatoryjnie po ukończeniu określonego wieku. „Ochotnicze wstępowanie" oznacza, że rekrutacja nie jest prowadzona siłą ani pod przymusem oraz że istnieją zabezpieczenia zapewniające, że wszelka dobrowolna rekrutacja jest rzeczywiście dobrowolna, odbywa się za świadomą zgodą rodziców lub opiekunów prawnych osoby wstępującej, rekruci są w pełni poinformowani o obowiązkach związanych ze służbą wojskową i przed ich przyjęciem do narodowych sił zbrojnych przedstawili wiarygodną metrykę urodzenia. Rekrutacja do grup zbrojnych oznacza rekrutowanie dzieci siłą lub dobrowolnie oraz wykorzystywanie ich w działaniach wojennych. W tym przypadku termin poboru obowiązkowego nie ma zastosowania.

Jedną z kluczowych kwestii związanych z terminem „dziecko żołnierz" jest wiek rekruta.

Protokoły dodatkowe do konwencji genewskich nie zawierają bezwzględnego zakazu udziału w działaniach zbrojnych dzieci poniżej ani powyżej 15 lat. Art. 77 ust. 2 i 3 I protokołu dodatkowego dotyczącego ochrony ofiar międzynarodowych konfliktów zbrojnych dopuszcza powoływanie do sił zbrojnych osób między 15. a 18. rokiem życia, przyznając pierwszeństwo tym starszym. Jednocześnie zobowiązuje strony konfliktu, by poczyniły wszelkie możliwe kroki, aby dzieci poniżej 15. roku życia nie uczestniczyły bezpośrednio w działaniach zbrojnych i aby powstrzymały się od powoływania dzieci do swych sił zbrojnych. W przypadku dzieci, które nie ukończyły 15. roku życia, a które uczestniczą bezpośrednio w działaniach i mogą znaleźć się we władzy strony przeciwnej, stwierdza się, że mają one prawo nadal korzystać ze szczególnej ochrony przyznanej przez niniejszy artykuł, niezależnie od tego, czy będą jeńcami wojennymi, czy nimi nie będą. Zgodnie z art. 77 termin „dziecko" oznacza osobę poniżej 15. roku życia. W odniesieniu do przedziału wiekowego między 15. a 18. i poniżej 18. roku życia stosuje się pojęcie „osoba". Zatem przyznanie „dzieciom" w art. 77 ust. 1 prawa do korzystania ze szczególnego poszanowania i bycia chronionym może wskazywać na odniesienie do dzieci poniżej 15. roku życia, zwłaszcza że wiek ów był wielokrotnie wskazywany w konwencji genewskiej o ochronie osób cywilnych podczas → w o j n y [t. 4], jako

granica poziomu rozwoju, która nie wymaga stosowania środków specjalnych. Dzieci poniżej 15. roku życia nie powinny również być wcielane do sił lub grup zbrojnych, a także nie powinny otrzymywać zezwolenia na udział w działaniach zbrojnych prowadzonych w ramach → k o n f l i k t ó w n i e m i ę d z y n a r o d o w y c h, zgodnie z II protokołem do konwencji genewskich. Nie stosuje się tu zasady pierwszeństwa poboru dzieci starszych, jeśli są między 15. a 18. rokiem życia. Protokół ma jednak zastosowanie tylko w sytuacji istnienia rzeczywistej konfrontacji między rządowymi siłami zbrojnymi a rozłamowymi siłami zbrojnymi lub innymi zorganizowanymi uzbrojonymi grupami, istnienia odpowiedzialnego dowództwa opozycyjnych sił zbrojnych, sprawowania przez nich kontroli nad częścią terytorium, przeprowadzania ciągłych i spójnych operacji wojskowych oraz zdolności jego wdrożenia. W odniesieniu do bezpośredniego udziału w działaniach zbrojnych konwencja o prawach dziecka przyjmuje granicę wieku poniżej 15. roku życia, uznając zasadę pierwszeństwa w rekrutacji dzieci starszych w przypadku powoływania osób, które osiągnęły wiek 15 lat, lecz nie osiągnęły jeszcze 18 lat. Tym samym granica wieku chronionego wyznaczonego przez konwencję jest zgodna z granicą ustanowioną w prawie humanitarnym. Jednocześnie mamy do czynienia z brakiem konsekwencji w ochronie dziecka stanowionej innymi zapisami konwencji. W świetle art. 1 „dzieckiem" jest osoba poniżej 18. roku życia, chyba że zgodnie z prawem uzyskała ona wcześniej pełnoletniość. To oznacza, że ochrony przed rekrutacją nie mają dzieci w wieku od 15 do 18 lat. Standardy wieku rekrutacji określone w prawie międzynarodowym z granicy 15 lat podnosi Protokół fakultatywny do konwencji, chociaż nie ustanawia zakazu „równych 18 lat" zarówno w przypadku dobrowolnej, jak i obowiązkowej rekrutacji przez państwo. Protokół obliguje państwa-strony „by osoby, które nie osiągnęły 18. roku życia, nie były objęte obowiązkowym poborem do ich sił zbrojnych" (art. 2). Podnosi również minimalny wiek dobrowolnej rekrutacji w siłach zbrojnych powyżej 15. roku życia, „uznając, że w świetle Konwencji osoby poniżej 18. roku życia uprawnione są do szczególnej ochrony" (art. 3). Zgodnie z art. 4 ust. 1 „grupy zbrojne inne niż siły zbrojne danego państwa nie powinny w żadnych okolicznościach prowadzić naboru lub wykorzystywać w działaniach zbrojnych osób poniżej 18. roku życia". M. Happold twierdzi, że zakaz rekrutacji

jest bezwzględny. Jednak w takim przypadku właściwsze byłoby sformułowanie „nie wolno", „nie mogą" niż „nie powinni" rekrutować, gdyż to ostatnie świadczy bardziej o moralnym zobowiązaniu stron. *Przewodnik do Protokołu fakultatywnego w sprawie angażowania dzieci w konflikty zbrojne* wyjaśnia, że tekst art. 4 ust. 1 odzwierciedla tradycyjny pogląd, że tylko państwa mają obowiązki wynikające z międzynarodowego prawa dotyczącego →praw człowieka [t. 3] i mogą stać się stronami traktatów, podczas gdy zachowanie podmiotów niepaństwowych musi być regulowane przez prawo krajowe. Protokół fakultatywny używa zwrotu „nie powinien" zamiast „nie może" lub „nie wolno" w celu nakreślenia zakazów rekrutacji lub wykorzystywania osób poniżej 18. roku życia przez grupy zbrojne, odzwierciedlając silne poglądy społeczności międzynarodowej bez nadawania statusu prawnego takim grupom zbrojnym (w art. 4 ust. 3 zadbano o to, aby stosowanie art. 4 nie nadawało statusu prawnego grupie zbrojnej).

Mianem „dziecko żołnierz" określa się dziecko, które bierze lub brało bezpośredni udział w działaniach wojennych, ale nie tylko. Choć Konwencja o prawach dziecka i Protokół fakultatywny wyraźnie precyzują, że chodzi o udział „bezpośredni", i nie wspominają nic o udziale „pośrednim", to jednak w opinii Funduszu Narodów Zjednoczonych na rzecz Dzieci (UNICEF) i w wyjaśnieniu zawartym w *Przewodniku do Protokołu fakultatywnego* udział bezpośredni może obejmować nie tylko aktywne uczestnictwo w walce i działaniach wojskowych. Zalicza się tu również inne formy wsparcia bezpośredniego: szpiegostwo, zwiad, sabotaż, działania „wabików", kurierów, tragarzy, kucharzy czy służby pomocniczej w wojskowych punktach kontrolnych. Bezpośrednim wsparciem jest także wykorzystywanie dziewcząt do celów seksualnych i przymusowych małżeństw czy wspomniana praktyka baczczebazi. Ponieważ interpretacja UNICEF-u jest bardzo szeroka, wytyczne Komitetu Praw Dziecka dotyczące wstępnych sprawozdań państw-stron do Protokołu fakultatywnego wskazują konieczność wyjaśnienia przez państwa znaczenia terminu „udział bezpośredni", funkcjonującego w ich ustawodawstwie i praktyce.

→Rada Bezpieczeństwa ONZ [t. 3] identyfikuje rekrutację i wykorzystywanie dzieci jako jedno z sześciu poważnych naruszeń wobec dzieci podczas konfliktu zbrojnego. Apeluje do stron konfliktu

wymienionych w rocznym sprawozdaniu Sekretarza Generalnego na temat dzieci i konfliktów zbrojnych, aby te przyjęły → plan ONZ mający na celu zakończenie rekrutacji i wykorzystywania dzieci dla potrzeb konfliktu zbrojnego [t. 3].

Rekrutacja i angażowanie dzieci w działania zbrojne łamią postanowienia:

- Konwencji o prawach dziecka – art. 38.3,
- Protokołu fakultatywnego do Konwencji o prawach dziecka w sprawie angażowania dzieci w konflikty zbrojne – art. 2–4,
- I protokołu dodatkowego do konwencji genewskich – art. 77.2,
- II protokołu dodatkowego do konwencji genewskich – art. 4.3.c,
- Rzymskiego statutu → Międzynarodowego Trybunału Karnego [t. 3] – art. 8.2.b (XXVI), 8.2.e (VII),
- Konwencji Międzynarodowej Organizacji Pracy nr 182 – art. 3.a.

Naruszają również Zasady paryskie dotyczące dzieci związanych z siłami lub grupami zbrojnymi – artykuł 2.1.

Potwierdzone przez Sekretarza Generalnego ONZ przypadki rekrutacji i wykorzystywania dzieci żołnierzy mają miejsce w Afganistanie, Mjanmie, Indiach, Iraku, Izraelu i Palestynie, Jemenie, Kolumbii, Kongo, Libanie, Libii, Mali, Nigerii, Południowym Sudanie, Republice Środkowoafrykańskiej, Somalii, Sudanie, Syrii oraz na Filipinach.

Klaudia Cenda-Miedzińska

K. Cenda-Miedzińska, *Wpływ konfliktu zbrojnego na bezpieczeństwo dzieci w Islamskiej Republice Afganistanu w latach 2004–2014*, Wydawnictwo Uniwersytetu Pedagogicznego, Kraków 2019; Children and armed conflict: report of the Secretary-General, 20 June 2019, A/73/907–S/2019/509; M. Happold, *The Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict*, [w:] *Yearbook of International Humanitarian Law 2000*, vol. 3, T.M.C. Asser Press, Hague 2002; Konwencja o prawach dziecka, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r., 20 listopada 1989 r., Dz. U. 1991, nr 120, poz. 526; Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r., Dz. U. 1992, nr 41, poz. 175; Protokół Fakultatywny do Konwencji o prawach

dziecka w sprawie angażowania dzieci w konflikty zbrojne, przyjęty w Nowym Jorku dnia 25 maja 2000 r., Dz. U. 2007, nr 91, poz. 608; UNICEF, *Cape Town Principles and Best Practices*, 1997; UNICEF, *Guide to the Optional protocol on the involvement of children in armed conflict*, UNICEF, New York, 2003; ciż, *Paris Principles. Principles and Guidelines on Children Associated with Armed Forces or Armed Groups*, UNICEF, 2007.

DŻIHAD (arab. جهاد, ğihād, ang. *jihad* – walka, zmaganie, trud) – nakaz religijny w islamie, dotyczący podjęcia trudu w celu ochrony wiary własnej lub grupy. Na ogół postrzegany jako „święta wojna", czyli użycie siły wobec przeciwników islamu.

Termin pochodzi od arabskiego rzeczownika odczasownikowego (masdaru) od *gahada* i pierwotnie oznaczał „dokładanie starań", „podejmowanie wysiłków" dla osiągnięcia danego celu. Tym wysiłkiem mógł być też czyn zbrojny (*kital*), ale i walka ze swoimi słabościami. Tak powstał główny podział na dżihad daleki/wielki (*al-akbar*) i bliski/mały (*al-asghar*). Ten pierwszy oznacza *de facto* dżihad wewnętrzny (*al-nafs*), czyli drogę do wyzwolenia się ze swoich słabości, drugi to walka zbrojna (*kital*).

Część badaczy islamu proponuje jeszcze następujący podział:

- dżihad serca (*jihad bil qalb/nafs*) – walka z diabłem, ucieczka przed grzechem (czyli *al-jihad al-akbar*);
- dżihad języka (*jihad bil lisan)* – mówienie prawdy, w tym walka z oszczerstwami wobec islamu;
- dżihad ręki (*jihad bil yad*) – czyn, walka z niesprawiedliwością, ale również wędrówka do miejsc świętych czy dla obrony islamu (*hidżra*);
- dżihad pióra (*jihad bil qalam*) – wiedza, → i n f o r m a c j a, poznanie praw wiary;
- dżihad miecza (*jihad bil saif*) – to nic innego jak walka zbrojna (*kital*);

Jalala al-Din al-Suyuti i inni za nim wymieniają 8 przyczyn, dla których można wezwać do dżihadu, ale tylko 1 z nich to dżihad walki.

Zasadniczo dżihad zbrojny miał się ograniczać do walki obronnej, w surze II (*Al-Bakara*) Koran nakazuje walczyć z tymi, którzy są agresorami, sami wyznawcy nie mają być najeźdźcami (II:190). W okresie

mekkańskim Prorok zakazywał czynnego oporu, spowodowało to choćby przymusową emigrację części wyznawców do chrześcijańskiej Abisynii. Wreszcie sam Muhammad musiał ratować się ucieczką (*hidżra*) do Medyny (wówczas zwanej Jatrib). Wtedy też doszło do zmiany w doktrynie, walka jest dozwolona dla pokrzywdzonych (XXII:39): „Wolno walczyć tym, którzy doznali krzywdy – zaprawdę, Bóg jest wszechwładny, by im udzielić pomocy!". Niemniej w tym okresie, wg tradycji muzułmańskiej, Prorok podejmował walkę z Kurajszyitami (wrogim plemieniem), ale tylko w odpowiedzi na ich ataki. Na jego polecenie stoczono przynajmniej 29 → b i t e w [t. 1], on sam dowodził w 27, a w 9 brał czynny udział, z mieczem w ręku. Koran nakazuje stosować narzędzia adekwatne do tych stosowanych przez agresora (XVI:126): „Jeśli karzecie, to karzcie tak, jakbyście sami byli karani. Lecz jeśli jesteście cierpliwi, bądźcie nimi, bo to jest lepsze!". Koran nie przewiduje → w o j e n [t. 4] agresywnych, podbojów (VIII:61): „A jeśli oni skłonią się do pokoju, / to i ty się ku niemu skłoń". Łącznie pojęcie „dżihad" pojawia się 36 razy w 19 surach, lecz nie tylko w znaczeniu walki.

Jednak już w Sunnie (tradycji) dżihad jest postrzegany jako wojna agresywna, przeciwko tym, którzy żyją poza islamem (*dar al-islam*) na ziemi wojny (*dar al-harb*). Szczególnie istotny jest *hadis*: „Wysłannik Boga rzekł: Została mi polecona przez Boga walka przeciw ludziom, dopóki oni nie wyznają / Że nikt nie ma prawa być czczony jak tylko Bóg jedyny oraz / Że Mahomet jest posłańcem Boga". Tak doszło do podziału na wojujący dżihad bliski (czyli obronny – *al-daf'*) i wojujący dżihad daleki (ofensywny – *al talab*). Co jednak ważne, dżihad jest obowiązkiem każdego muzułmanina. Oczywiście nie każdy jest predysponowany do walki zbrojnej, wtedy musi udzielać pomocy wojującym, tak jak tylko może (*tajheez al-ghazi*). Takim sposobem jest np. wspieranie finansowe (*al-jihad bil mal*).

Na podstawie Koranu i *hadisów* powstała islamska koncepcja wojny. Klasyczne podręczniki islamskiego orzecznictwa (*idżtihad*) często zawierały sekcję zwaną *Księgą dżihadu*, regulującą zasady „świętej wojny". Za jednego z pierwszych teoretyków dżihadu uznaje się Muhammada ibn al-Hasana al-Shaybaniego (749/50–805). Reguły dotyczyły np. leczenia rannych, postępowania z cywilami, kobietami, dziećmi i podziału łupów. Ważnym elementem był właśnie podział łupów na *ghanimah* (zdobyte

podczas rzeczywistej walki) i *fai* (uzyskane bez walki). We wczesnym islamie → ż o ł n i e r z e [t. 4] otrzymywali żołd, ale przede wszystkim udział w zdobyczy, np. nadania ziemskie. 20% łupów było przekazywane dla władcy (kalifa lub sułtana), ta część nazywa się *chums*. Wśród łupów mogli być też niewolnicy, w tym kobiety (XXXII:50): „O Proroku! / My uznaliśmy za dozwolone dla ciebie / żony, którym dałeś wiana, / i niewolnice, które ci darował Bóg jako zdobycz…". Jednak przede wszystkim czekała nagroda po śmierci, męczennik (*szahid*) miał dostąpić bytu w rajskim ogrodzie (*dżanah*) wraz ze swoimi żonami bez skazy (*hurysy*). (IV:74–76): „Niech walczą na drodze Boga / ci, którzy za życie tego świata / kupują życie ostateczne! / A kto walczy na drodze Boga / i zostanie zabity albo zwycięży, / otrzyma od Nas nagrodę ogromną […]. Ci, którzy wierzą / walczą na drodze Boga, / a ci, którzy nie wierzą, / walczą na drodze Saguta [diabła – przyp. aut.]. / Walczcie więc z poplecznikami szatana! / Zaprawdę, podstęp szatana jest słaby!".

Jedną z cech Koranu i Sunny jest jednak wzajemne wykluczanie się pewnych norm (*naskh*) – nawet w samym Koranie znajdziemy zapisy, które mogą dopuszczać walkę zbrojną i to bez większych ograniczeń co do formy. Najlepszym przykładem jest tzw. werset miecza: „A gdy miną święte miesiące, / wtedy zabijecie bałwochwalców, / tam, gdzie ich znajdziecie; / chwytajcie ich, oblegajcie / i przygotowujcie dla nich wszelkie zasadzki!" (IX:6).

Z drugiej strony jest *hadis* określający dokładne zasady prowadzenia wojny, jakie miał wyznaczyć Prorok i przez Abu Bakra (późniejszego kalifa) przekazać młodemu dowódcy Usamahowi. Były to:

- Nie angażować się w zdradę.
- Nie brać udziału w aktach niewiary.
- Nie wolno angażować się w oszustwo.
- Nie wolno okaleczać.
- Nie wolno zabijać małych dzieci ani starców, czy to mężczyzn, czy kobiet.
- Nie wolno ścinać palm ni palić ich.
- Nie powinno się ścinać drzew owocowych.
- Nie wolno zabijać ani owcy, ani krowy, ani wielbłąda, chyba że dla pożywienia.

- Omijać pustelników, którzy przebywają w swoich celach, należy zostawić ich samym sobie.
- Jedząc z obcymi, wzywać imienia Boga.

Koncepcja dżihadu zaczęła się zmieniać, radykalne podejście prezentowali już charydżyci, dopuszczający nawet morderstwo muzułmanina, w tym samego kalifa, jeśli ten odstąpił od prawdziwej wiary. Na bazie tej ideologii powstał choćby ruch nizarytów, szyickiego odłamu ismailitów, którzy dokonywali zamachów nawet na przywódców islamskich (tzw. asasyni). Również w ramach sunnizmu doszło do znaczącej radykalizacji, nową interpretację zaproponował Ahmad ibn Tajmijja, tworzył on w czasach wielkiej trwogi dla muzułmanów, czyli upadku Kalifatu Bagdadzkiego (1258 r.), co miało zapewne wpływ na jego radykalną postawę. Uznał on dżihad za obowiązek każdego muzułmanina, sam brał udział w wyprawach wojennych, m.in. przeciwko alawitom i druzom. W swojej doktrynie uznał zarówno chrześcijan, jak i żydów za niewiernych (*kuffar*), ale poszedł nawet dalej: za takich uznał także alawitów i szyitów.

Do koncepcji dżihadu nawiązywano wielokrotnie, zwłaszcza podczas różnych zrywów politycznych, często posługiwano się przy okazji odwołaniem do koncepcji Mahdiego, czyli powracającego na świat ostatniego kalifa, którego przyjście miało zwiastować zwycięstwo islamu. Dla współczesnego pojęcia dżihadu istotna jest fatwa z 14 listopada 1914 r., wydana przez sułtana (który był jednocześnie przywódcą duchowym, czyli kalifem) osmańskiego Mehmeda V. Wzywał on wszystkich muzułmanów, nie tylko swoich poddanych, do obrony przed atakiem Rosji, Francji, Anglii i ich sprzymierzeńców, którzy „usiłują zgasić i unicestwić święte światło islamu". Ta fatwa, a zwłaszcza jej odwołania do czasów wojen krzyżowych, została później wykorzystana przez inne ruchy islamistyczne, w tym przez Bractwo Muzułmańskie i ruch *salafijja*. Głównymi myślicielami tego nurtu byli Egipcjanie Hasan al-Banna (1906–1949) i Sajjid Kutb (1906–1966) oraz Pakistańczyk Abul A'la Maududi (1903–1979). Według nich świat (również islamski) jest pogrążony w zgniliźnie i niewiedzy (*dżahilijja*), jedyną drogą do szczęścia jest rewolucja islamska, ustanowienie suwerenności boskiej (*hakimijja*), a drogą do tego jest dżihad. Muhammad Abd as-Salam Faradż (1954–1982) uznał *dżihad* za usprawiedliwione narzędzie, poszedł nawet krok dalej, uznając to za obowiązek każdego muzułmanina, za szósty filar wiary

(*szahada* – wyznanie wiary, *salat* – modlitwa, *zakat* – jałmużna, *saum* – post w Ramadanie, *hadżdż* – pielgrzymka do Mekki). Sama działalność uświadamiająca jest niewystarczająca, potrzebny jest czyn, w tym czyn zbrojny.

Koncepcję dżihadu rozwinął, a następnie wezwał do niego przeciwko radzieckim okupantom Afganistanu szejk Abd Allah Azzam (1941–1989). W 1979 r. wydał fatwę *Obrona ziem muzułmańskich, pierwszy obowiązek po wierze*. Nawiązując do ibn Tajmijji, uznał, że pierwszym obowiązkiem po wierze jest odparcie agresora, który atakuje religię i porządek światowy. Podzielił dżihad na ofensywny i obronny. Ten pierwszy (gdzie wróg jest atakowany na własnym terytorium) jest uzasadniony, gdy:

- niewierni (*kuffar*) zbierają się, by walczyć z muzułmanami,
- dla ochrony granic, w tym raz do roku można wysyłać armię, aby terroryzować wrogów Allaha,
- imam ma obowiązek gromadzenia i wysyłania wojsk do *dar al-harb* 1 lub 2 razy w roku, a ludność muzułmańska ma mu pomagać,
- służy utrzymaniu zapłaty *dżizji* (podatku płaconego przez niewiernych).

Według niego: „Dżihad jest *Dawah* (wezwaniem do stania się muzułmaninem) z siłą i jest obowiązkowy, należy wykorzystywać wszystkie dostępne możliwości, dopóki nie pozostaną tylko muzułmanie lub ludzie, którzy poddadzą się islamowi".

Dżihad obronny ma na celu wypędzenie niewiernych z ziemi islamu i jest to *Fard al-Ayn* (indywidualny obowiązek) wszystkich. Jest to najważniejszy ze wszystkich obowiązków i powstaje w następujących warunkach:

- jeśli niewierni wkroczą do *dar al-islam*,
- jeśli szeregi wojowników spotkają się w bitwie i zaczną się do siebie zbliżać,
- jeśli imam wzywa osobę lub lud do marszu naprzód z nim, należy z nim podążyć,
- jeśli *kuffar* złapią i uwięzą grupę muzułmanów.

Do tak rozumianego dżihadu odwoływały się liczne organizacje terrorystyczne i narodowowyzwoleńcze. Część z nich nawet umieszczając ten termin w swojej nazwie (np. tzw. Egipski Dżihad – *Tanzim al-Jihad*). Do dżihadu wzywali przywódcy organizacji islamistycznych. Usama ibn Ladin (Osama bin Laden) wydał m.in. 2 fatwy w tej sprawie: w 1996 r. pod nazwą

Wojna przeciwko Amerykanom okupującym Ziemię Dwóch Świętych Miejsc i w 1998 r. *Dżihad przeciwko Żydom i krzyżowcom.* Również przywódca →Państwa Islamskiego [t. 3] (ISIS, ISIL, Daesh, IS) Ibrahim Abu Bakr al-Baghdadi wzywał do dżihadu: „[Bóg – przyp. aut.] Kazał nam zwalczać wrogów i podejmować dżihad. […] A Bóg przeznaczył dla naszych braci – żołnierzy dżihadu – zwycięstwo i obdarzył ich kalifatem po wielu długich latach dżihadu, wytrwałości i walki z wrogami Boga. […] Gdybyście wiedzieli, jakie jest wynagrodzenie za dżihad, jaka jest godność, wysoka pozycja i chwała w tym i tamtym życiu, nikt z was nie odrzuciłby go!".

Dżihad nie jest zjawiskiem charakterystycznym tylko dla sunnitów. Jest jednym z dziesięciu elementów wiary w szyizmie. Podstawową różnicą jest to, że do uprawomocnionego dżihadu może wezwać tylko imam (al-Mahdi, ostatni z 12 imamów, wg imamitów do dziś żyjący w ukryciu). Zanim ten powróci z ukrycia w celu ustanowienia wiecznego pokoju i rządów islamu, dozwolona jest tylko walka w obronie islamu. Powrót ostatniego imama będzie zwiastowało nadejście Mahdiego. Do tej koncepcji nawiązał ajatollah Ruhollah Chomejni, w Iranie powstały oddziały Związku Mobilizacji Uciemiężonych, potocznie *Basidż*, które zasłynęły choćby samobójczym przechodzeniem przez pola minowe podczas wojny iracko-irańskiej. Ataki samobójcze motywowane religią i koncepcją dżihadu były też prowadzone przez członków Hezbollahu.

Obecnie koncepcja dżihadu jest rozwijana, dostosowywana do potrzeb współczesnego pola walki. Tak powstało choćby pojęcie →e-dżihadu czy cyberdżihadu, czyli walki w →cyberprzestrzeni [t. 1], począwszy od →propagandy [t. 3], na działalności hakerskiej skończywszy.

Przemysław Mazur

M. Khadduri, *War and Peace in the Law of Islam*, The Lawbook Exchange, Clark 2010; K. Kościelniak, *Dżihad święta wojna w islamie*, Wydawnictwo „M", Kraków 2002; tenże, *Rozumienie wojny w źródłowych tekstach islamu*, [w:] *Kościół i dar pokoju,* M. Chojnacki, J. Morawa, A.A. Napiórkowski (red.), Wydawnictwo Salwator, Kraków 2016; P. Mazur, *Czy dżihad to ideologia?: o niekonsekwencjach terminologicznych wokół „walki na ścieżce Boga"*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 2; tenże, *Dżihad*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo

Libron, Kraków 2018; P. Mazur, O. Wasiuta, S. Wasiuta, *Państwo Islamskie ISIS: nowa twarz ekstremizmu*, Difin, Warszawa 2018; *The History of al-Tabari. The Conquest of Arabia*: *The Riddah Wars A.D. 632–633/A.H. 11*, trans. F.M. Donner, SUNY Press, New York 1993.

DŻIHAD MEDIALNY (*media jihad*), medialny → d ż i h a d – wykorzystanie mediów do prowadzenia dżihadu, czyli obrony islamu przed niekorzystnymi wpływami czy zniszczeniem; jest to również → w o j n a i n f o r m a c y j n a [t. 4] prowadzona przez ugrupowania islamistyczne.

Termin został wprowadzony przez → P a ń s t w o I s l a m s k i e [t. 3] (ISIS, ISIL, Daesh, Daisz) w wydanym w 2016 r. dokumencie *Media Operative, You Are a Mujahid, Too*, będącym swoistą doktryną → w a l k i i n f o r m a c y j n e j [t. 4] kalifatu. Dżihad jest obowiązkiem każdego muzułmanina. W rozbudowanej koncepcji dżihadu znalazło się również uzasadnienie dla walki na polu medialnym. Teoretycy dżihadu wymieniają choćby takie obowiązki, jak dżihad języka (*jihad bil lisan*) i dżihad pióra (*jihad bil qalam*). Pierwszy rodzaj to obowiązek mówienia prawdy i demaskowania fałszu polegającego zarówno na złej interpretacji wiary, jak i szkalowania islamu przez niewiernych (*kuffar*). Dżihad pióra polega na gromadzeniu i propagowaniu wiedzy – ma charakter apostolski (zdobywanie nowych wyznawców, zwolenników), czyli rekrutacyjny, lub kaznodziejski (służący umacnianiu swoich przekonań i pogłębianiu wiary). Może mieć też stanowić wsparcie dla dżihadu wojującego (*kital*). Wówczas mówimy o formie gromadzenia informacji potrzebnych do walki (*tajheez al-ghazi*), swoistego *know how*, oraz sianiu dezinformacji (zob. → d e z i n f o r m a c j a) czy psychologicznym oddziaływaniu na wroga (zob. → o p e r a c j e p s y c h o l o g i c z n e [t. 3]).

Wykorzystanie mediów, czyli informacji, jako broni, zdaniem niektórych ideologów islamistycznych było usankcjonowane już przez samego Mahometa (Muhammada). Abu Hamza al-Muhajir, przywódca ISIS w Iraku, tak argumentował wykorzystanie mediów do walki:

> Posłannik Allaha (pokój z Nim) zwykł wykorzystywać najbardziej wpływowy rodzaj mediów w jego czasach, który miał największy wpływ na ducha [walki] Jego wrogów, którym jest poezja. On (pokój z Nim) zatrudnił także kaznodzieję do obrony islamu

> i muzułmanów, Thabit bin Qays bin Shammas (któremu zostało obiecane niebo).
>
> [Ten sam pisał również]: Prorok (niech spoczywa w pokoju) był zatroskany tym rodzajem dżihadu [media] – dowodził muzułmańskimi poetami, takimi jak Hassan Abdullah bin Rawaha i Kaab bin Malik (niech Allach będzie z nim) ośmieszającymi swoich niewierzących przeciwników.

Początków medialnego dżihadu możemy szukać w czasach wojny w Afganistanie (1979–1989), gdy zaczęto wydawać gazety kierowane do mudżahedinów (islamskich bojowników walczących z wojskami radzieckimi i ich sojusznikami), ale również do innych muzułmanów w celu uzyskania ich pomocy (wsparcia finansowego czy udziału w walkach). Działania z zakresu swoistego public relations prowadzono również za pomocą zachodnich mediów, w których przedstawiano konflikt jako obronę przed ZSRR. Ukazywały się reportaże oraz wywiady, w tym z Usamą ibn Ladinem (Osamą bin Ladenem). Na początku lat 90. XX w. główną formą przekazu były filmy pokazujące okrucieństwo wobec muzułmanów i odwagę bojowników, głównie z Bośni, ale i choćby z Czeczenii.

O bardziej spójnej koncepcji medialnego dżihadu możemy mówić od czasów powstania Al-Kaidy. Główną metodą była publikacja krótkich filmów, na ogół były to przemówienia Usamy ibn Ladina. Zazwyczaj występował on w tradycyjnym stroju, czasami z elementami umundurowania (np. kurtka wojskowa), często na tle flagi Al-Kaidy i z karabinkiem opartym o ścianę lub trzymanym na kolanach. Filmy były emitowane przede wszystkim przez katarską telewizję Al-Jazeera (→ A l - D ż a z i r a [t. 1]). Po rozpoczęciu tzw. wojny z → t e r r o r y z m e m [t. 4] ta metoda okazała się utrudniona, ponadto wymuszono na telewizji zaprzestanie emisji. Dlatego zaczęto wykorzystywać internet i wszystkie jego możliwości – powstał → e - d ż i h a d.

Polityka medialna okazała się ważnym elementem i zarówno przywódcy Al-Kaidy, jak i ISIS przykładali wagę do tej formy walki. Organizacje utworzyły nawet własne agencje informacyjne. Do ważniejszych

inicjatyw możemy zaliczyć m.in.: GIMF, Amaq, as-Sahab, al-Fajr Media oraz liczne czasopisma.

As-Sahab (względnie, choć niepoprawnie w polskiej transkrypcji: Al-Sahab, as-Sahāb, z arabskiego „chmura") to oficjalny organ medialny kierownictwa Al-Kaidy z siedzibą w Pakistanie i Afganistanie, który powstał w 2001 r. Produkcje As-Sahab zawierają m.in. wystąpienia przywódców Al-Kaidy, np. Usamy ibn Ladina i Aymana al-Zawahiriego. Za założyciela uważany jest obywatel USA Adam Gadahn vel Azzam al-Amriki, który zadbał o jakość nagrań, spójność przekazu i wypromowanie marki (filmy produkowane przez jego studio były zawsze opatrzone logo). Materiały początkowo dostarczano przy pomocy kurierów. Programy nagrywano przede wszystkim w Afganistanie i Pakistanie. Po serii ataków armii USA i sił sprzymierzonych zmieniono taktykę i zaczęto korzystać z internetu. Ocenia się, że do tego momentu nawet 3 na 4 nowe filmy wideo lub materiały audio dowódców Al-Kaidy były publikowane online przez As-Sahab. W 2014 r. zamknięto konto (@ _s7ab_m) na Twitterze.

Islamski Globalny Front Medialny (GIMF), to organizacja propagandowa ruchu islamistycznego, związana głównie z Al-Kaidą, powstała w 2004 r., pod tą nazwą działająca od 2007 r. Początkowo publikowano wyłącznie w języku arabskim, wkrótce jednak pojawiły się artykuły anglojęzyczne. Od 2005 r. działała jego niemiecka sekcja o nazwie Globale Islamische Medienfront, która okazała się liderem dżihadystycznych mediów w Europie.

Organizacja powstała jako kontynuator 2 innych platform propagandowych: Global Islamic Media Group (GIMG) i Global Islamic Media Centre (GIMC). Pierwsza z nich była listą mailingową utworzoną 29 czerwca 2001 r. na platformie Yahoo. Dostęp do materiałów wymagał hasła. Sześć miesięcy po utworzeniu GIMG miał ponad 600 subskrybentów, liczba ta stale rosła, aż osiągnęła 7400, zanim grupa zniknęła wiosną 2004 r. Za pomocą GIMG kolportowano podręczniki, teksty ideologiczne i propagandowe. W maju 2004 r. po opublikowaniu wideo przedstawiającego ścięcie w Iraku amerykańskiego dziennikarza Nicka Berga przez Abu Musaba al-Zarqawiego (przywódcę Al-Kaidy w Iraku) platforma została zlikwidowana wskutek ataku hakerskiego. Druga platforma, GIMC, miała zostać stworzona przez Ahmada al-Wathiqa Billaha, anonimowego

autora licznych tekstów internetowych na temat globalnej → s t r a t e g i i [t. 4] dżihadu. W 2007 r. utworzono swoisty kanał telewizyjny o nazwie *Voice of the Caliphate*. Format był identyczny z zachodnimi programami informacyjnymi, ale występował tam zamaskowany prezenter, który wychwalał terroryzm. Członkowie GIMF uruchomili także *Al Qaeda University of Jihad Studies* (Uniwersytet Studiów Dżihadystycznych Al-Kaidy).

W listopadzie 2006 r. „Islamskie Państwo Iraku" (później znane już jako ISIS) powołało Fundację Al-Furqan, która specjalizowała się w produkowaniu i kolportowaniu materiałów propagandowych w postaci filmów, plakatów, broszur oraz publikowaniu w internecie oficjalnych oświadczeń przywódców. Wraz z sukcesami militarnymi ISIS w 2013 r. Al-Furqan zaczęła odgrywać ważniejszą rolę. Ponadto działały Al-I'tisam Media Foundation oraz Ajnad Foundation for Media Production, tworzące treści audio.

Amaq – Agencja Informacyjna Amaq (Wikālat Aʿmāq li-l-Anbāʾ) – to nieoficjalny organ prasowy Państwa Islamskiego, podający się za profesjonalną → a g e n c j ę p r a s o w ą [t. 1]. Prawdopodobnie jej założycielem był Rayan Machaal, znany również jako Bara Kadek, syryjski dziennikarz z Aleppo. Początków tej agencji należy szukać pod koniec 2013 r., ale pierwsze potwierdzone informacje pochodzą dopiero z 2014 r., gdy relacjonowała przebieg bitwy o Kobani (kurdyjskie miasto na granicy Syrii z Turcją). Wyspecjalizowała się w potwierdzaniu autorstwa zamachów przez zwolenników ISIS. Ponadto jej reporterzy byli przy najważniejszych wydarzeniach podczas walk w Iraku i Syrii, często ich materiały były jedynymi dostępnymi dla innych mediów. Instytucja prezentowała się jako byt niezależny od władz ISIS, w przeciwieństwie do radia Al Bayan czy czasopisma „Dabiq", które były organami prasowymi ISIS.

Al-Hayat Media Center jest medialnym skrzydłem ISIS. Zostało założone w połowie 2014 r. w celu pozyskiwania zwolenników na Zachodzie i w Rosji. Większość materiałów publikowano w językach angielskim, niemieckim, rosyjskim i francuskim. Były to głownie filmy i czasopisma, z których najsłynniejszy był „Dabiq".

„Dabiq" to oficjalne czasopismo ISIS, wydawane w języku angielskim. Od 2014 r. ukazało się jego 14 numerów. Było kolportowane w wersji elektronicznej (format PDF, bardzo starannie przygotowane pod względem graficznym). Publikowano w nim odezwy ISIS, interpretacje prawa,

relacje z frontu wojennego, artykuły publicystyczne (również autorstwa konwertytów z Zachodu). Na ogół każdy numer miał motyw przewodni, zdradzany już przez okładkę; bardzo często wzywano do walki ze zdrajcami islamu, chrześcijanami i światem Zachodu (nazywanymi „krzyżowcami") oraz Żydami. Na przykład w numerze czwartym usankcjonowano niewolnictwo seksualne Jazydek. ISIS wydawało jeszcze wiele innych czasopism, w tym: „Islamic State NEWS", „Islamic State Report", „Rumiyah" (po angielsku), „Dar al-Islam" (po francusku), „Konstantiniyye" (po turecku), „Istok" i „Furat Press" (po rosyjsku), a w języku arabskim m.in. „Al-Naba" i „Al-Masra".

Nadal działa wiele innych organizacji medialnych pracujących dla Al-Kaidy, są to m.in.: Jundullah Media, Ummat Studios, Islamic Emirate of Afghanistan Media, Labayk Media Productions, Islam Awazi Information Center, Manba al-Jihad Media, Badr at-Tawheed Media, Ummat Studios. W związku z przejęciem prymu przez ISIS część działaczy wraz z organizacjami przeszła pod zarząd kalifatu.

ISIS wykorzystywało koncepcję medialnego dżihadu u szczytu swych możliwości, w celu utrzymania kontroli społecznej, przekonania potencjalnych zwolenników, osłabienia → m o r a l e [t. 3] wojskowych przeciwników i umiędzynarodowienia swojego projektu. ISIS synchronizowało informacje i operacje wojskowe, aby reagować szybko i skutecznie na wydarzenia na świecie i pojawiające się możliwości. Medialny dżihad był doktryną świetnie przemyślaną, zaplanowaną i zarządzaną.

Za politykę medialną odpowiadało specjalne „ministerstwo" (*diwan*) podległe kalifowi – Diwan al-I'lam al-Markazi (inaczej: The Central Media Office), ustanowione jeszcze w 2014 r. Zarządzało głównymi mediami ISIS, w tym agencjami: Al-Hayat, Al-Furqan, Al-Ajnad i Al-Itissam (zaprzestało działalności w 2015 r.), a także regionalnymi biurami medialnymi (na poziomie *wilayat*, czyli prowincji) i prawdopodobnie też Amaq. The Central Media Office kontrolowało także inne domy medialne, również te „odziedziczone" po Al-Kaidzie. Jednym z nich było Al-Ajnad, publikujące *anashid* – utwory muzyczne gloryfikujące islam i jego obrońców, połączone z recytacjami Koranu. Nadzorowało również działalność innych mediów ISIS, w tym radia Al-Bayan (korzystało też z nadajników naziemnych fal krótkich FM), gazet „Maktaba al-Himma" i „Zeal Press" oraz tygodnika

relacjonującego przebieg walk „Al-Naba". Jeśli dziennikarze innych agencji chcieli pracować na terenach zajętych przez ISIS, musieli starać się o akredytację tej organizacji. Urzędnicy Biura mieli prawo do cenzurowania przekazów, współpracowali bezpośrednio z dowódcami sił zbrojnych, przekaz medialny był zatem traktowany jako rodzaj oddziaływania militarnego.

Do najważniejszych cech medialnego dżihadu należy zaliczyć następujące aspekty:

- spójną narrację, która jest jednocześnie pozytywna, alternatywna i kompleksowa, oparta na odrzuceniu oficjalnej narracji mediów światowych (*counterspeech*);
- narracja jest okazjonalnie uruchamiana, starannie obliczona na efekt precyzyjnej „bomby" medialnej;
- w przypadku Państwa Islamskiego media uważa się za skuteczną broń, która przy prawidłowym użyciu ma „dalekosiężną" moc, przewyższającą moc najpotężniejszych bomb;
- Państwo Islamskie w sposób zrównoważony pobudza aktywizm, czynią to pracownicy offline lub wolontariusze online, tworzenie →propagandy [t. 3] i jej rozpowszechnianie jest czasami uważane za ważniejsze niż dżihad zbrojny;
- działacze medialni Państwa Islamskiego są pozyskiwani dzięki symbolicznemu systemowi handlu wymiennego. Propagują ideologię dostarczającą kombinacji emocji z teologicznymi i ideologicznymi apelami, co wystarcza, aby wolontariusze przez nieokreślony czas byli aktywni i zainteresowani współudziałem w swoistym misterium;
- kluczem do sukcesu ISIS jest jego elastyczna definicja zwolenników, nazywanych „medialnymi agentami". Granica między aktywizmem oficjalnym a nieoficjalnym celowo jest niewyraźna – tym samym łatwiej się utożsamiać z przekazem.

Państwo Islamskie miało olbrzymi wpływ na rozwój doktryny medialnego dżihadu, znakomicie wykorzystywało rozwój technologii informacyjnych, po raz pierwszy też skodyfikowało swoje zasady i cele, ustanowiło kontrolę i zarządzanie biurokratyczne. Należy się spodziewać, że wypracowane metody będą wykorzystywane przez inne organizacje tego typu.

Przemysław Mazur

H. Gambhir, *The Virtual Caliphate: ISIS's Information Warfare*, Institue for the Study of War, Washington 2016; P. Mazur, *Amaq*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; P. Mazur, *As-Sahab*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; P. Mazur, *Islamski Globalny Front Medialny*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; P. Mazur, O. Wasiuta, S. Wasiuta, *Państwo Islamskie ISIS: nowa twarz ekstremizmu*, Difin, Warszawa 2018; A. Wejkszner, *Państwo Islamskie. Narodziny nowego kalifatu?*, Difin, Warszawa 2016; C. Winter, *Media Jihad: The Islamic State's Doctrine for Information Warfare*, ICSR King's College London, London 2017.

E

E-BEZPIECZEŃSTWO (ang. *e-safety*, *cyber safety*) – bezpieczeństwo sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług cyfrowych – →bezpieczeństwo [t. 1] szeroko pojętych użytkowników →cyberprzestrzeni [t. 1] (w tym cyberprzestrzeni RP); można je utożsamiać z takimi określeniami jak bezpieczeństwo w internecie, →bezpieczeństwo w sieci [t. 1], bezpieczeństwo online, bezpieczeństwo cyfrowe, czy też →cyberbezpieczeństwo [t. 1].

Rozpatrując e-bezpieczeństwo w kontekście cyberbezpieczeństwa, należy zauważyć, że jest ono jednym z celów strategicznych w obszarze bezpieczeństwa RP i zapewnia ochronę kluczowym sektorom gospodarki, obywatelom oraz przedsiębiorcom. Obszar ten – wymagający stałego rozwoju i rozbudowy:

> odnosi się do technologii, procesów i praktyk zaprojektowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem.

Jak można przeczytać w *Strategii Bezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*:

> informacja jest narażona na utratę dostępności, integralności i poufności w wyniku oddziaływań pochodzących z różnych źródeł, w tym działań zamierzonych, polegających na dystrybucji szkodliwego oprogramowania, włamań do systemów teleinformatycznych, blokowaniu możliwości świadczenia usług. Atakującymi mogą być zarówno grupy przestępcze, działające z chęci zysku, pobudek terrorystycznych, jak i grupy, za którymi mogą stać obce państwa, a działania takie służą pozyskaniu informacji, destabilizacji politycznej lub gospodarczej albo wywołaniu niezadowolenia społecznego.

Dlatego też – w ramach podejmowanych przez administrację rządową działań mających na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP i rozbudowę krajowego systemu cyberbezpieczeństwa – przyjęto następujące cele (cele Polski w cyberprzestrzeni rozwija opublikowana przez Ministerstwo Cyfryzacji nowa *Strategia Cyberbezpieczeństwa RP na lata 2019–2024*):

- osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa,
- wzmocnienie zdolności do przeciwdziałania →cyberzagrożeniom [t. 1],
- zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni,
- zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Należy zauważyć, że zapewnienie bezpieczeństwa →informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się →bezpieczeństwem teleinformatycznym [t. 1] w sferze operacyjnej. Dlatego tak istotne pod względem e-bezpieczeństwa jest uzyskanie wysokiego poziomu odporności

krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów →infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni, jak również zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni.

E-bezpieczeństwo, patrząc na nie z praktycznego punktu widzenia, może być rozpatrywane jako zjawisko wtórne w stosunku do zjawiska cyberzagrożenia. To z tego właśnie powodu warto uświadomić sobie, na co człowiek przebywający w →infosferze może być narażony, czego powinien się obawiać, korzystając z internetu. Można wyróżnić kilka modułów →zagrożeń [t. 4] w cyberprzestrzeni, czyli zależnym od czasu zbiorze połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami:

- zagrożenia zdrowia psychicznego i fizycznego (m.in. dolegliwości wzroku, wady słuchu, dolegliwości układu kostno-mięśniowego, dolegliwości cieśni nadgarstka, dolegliwości kciuka, autodestrukcja, samookaleczenie, samobójstwa w cyberprzestrzeni);
- zagrożenia społeczno-wychowawcze (m.in. →przemoc [t. 3] i →agresja [t. 1] w sieci, hazard w sieci, zaburzenie kontaktów interpersonalnych, funkcjonowanie człowieka w świecie robotów humanoidalnych, miejsce człowieka w społeczeństwie nadzorowanym);
- zagrożenia moralne (m.in. cyberpornografia, prostytucja w sieci, cyberpedofilia, cyberseks, →seksting [t. 4], galerianki w sieci), zagrożenia związane z uzależnieniami (m.in. infoholizm, uzależnienie od gier komputerowych);
- zagrożenia poznawczo-intelektualne (m.in. uniformizacja i/lub redukcja doświadczenia, ograniczenia w zakresie postrzegania problemów, dominacja materiału obrazowego nad materiałem słownym);
- zagrożenia informacyjne (m.in. brak poczucia odpowiedzialności za nadawany komunikat, niedostateczna troska o prawdziwość komunikatu, stres informacyjny, →przeciążenie informacyjne [t. 3]);

- zagrożenia substancjami chemicznymi z inspiracji sieci (m.in. bigoreksja, narkotyki, napoje energetyzujące, dopalacze);
- zagrożenia →sztucznej inteligencji [t. 4] i robotów humanoidalnych;
- zagrożenia →społeczeństwa nadzorowanego [t. 4] czy kontrolowanego;
- cyberprzestępczość i nadużycia (m.in. zagrożenia dla komputera i innego sprzętu, zagrożenia dla urządzeń mobilnych, zagrożenia dla pieniędzy, zagrożenia dla prywatności, treści szkodliwe i nielegalne).

E-bezpieczeństwo dla użytkownika cyberprzestrzeni to nie tylko podnoszenie świadomości w kwestiach bezpieczeństwa online, doskonalenie kompetencji cyfrowych, czyli umiejętności związanych m.in. z mądrym i bezpiecznym korzystaniem z nowych →technologii informacyjno-komunikacyjnych [t. 4], ale także uzależniony od →kultury bezpieczeństwa sposób odczuwania bezpieczeństwa i myślenia o nim. To aspekt systemu wartości, o który należy zabiegać i pielęgnować go – potrzeba odpowiedzialnego obywatela cyfrowego (e-obywatela), rozumiejącego, że brak zachowania należytej ostrożności w sieci może być równie niebezpieczny jak brak ostrożności w prawdziwym życiu.

Należy zauważyć, że wśród obszarów kompetencji cyfrowych dla obywateli Unii Europejskiej (tzw. Rama Kompetencji Cyfrowych, znana również jako DigComp) znajdują się:

- umiejętność korzystania z informacji i z danych: przeglądanie, wyszukiwanie i filtrowanie danych, informacji i treści cyfrowych; ocena danych, informacji i treści cyfrowych; zarządzanie danymi, informacjami i treściami cyfrowymi;
- komunikacja i współpraca: komunikacja z wykorzystaniem technologii cyfrowych; dzielenie się informacjami i zasobami z wykorzystaniem technologii cyfrowych; aktywność obywatelska z wykorzystaniem technologii cyfrowych; współpraca z wykorzystaniem technologii cyfrowych; netykieta; zarządzanie tożsamością cyfrową;
- tworzenie treści cyfrowych: tworzenie treści cyfrowych; integracja i przetwarzanie treści; przestrzeganie prawa autorskiego i licencji; programowanie;

- bezpieczeństwo: narzędzia służące ochronie; ochrona danych osobowych i prywatności; → o c h r o n a z d r o w i a [t. 3] fizycznego, psychicznego i dobrostanu przed zagrożeniami wynikającymi z korzystania z technologii informacyjno-komunikacyjnych; ochrona środowiska;
- rozwiązywanie problemów: rozwiązywanie problemów technicznych; rozpoznawanie potrzeb i narzędzi niezbędnych do rozwiązywania problemów; twórcze wykorzystywanie technologii cyfrowych; rozpoznawanie braków w zakresie kompetencji cyfrowych.

Działania na rzecz e-bezpieczeństwa składają się z wielu elementów, poczynając od zupełnie prostych, poprzez coraz to bardziej złożone, aż po rozwinięte, charakteryzujące się dużym stopniem złożoności systemów zapewniania bezpieczeństwa w sieci. Mając zatem na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni, warto pamiętać o 3 hasłach, które propaguje polska wersja międzynarodowej kampanii STOP. THINK. CONNECT, czyli STÓJ. POMYŚL. POŁĄCZ, której hasła kolejno oznaczają:

- STÓJ: zanim skorzystasz z internetu, dowiedz się, jak być bezpiecznym w sieci oraz jak unikać potencjalnych zagrożeń.
- POMYŚL: poświęć chwilę, aby upewnić się, że droga do wirtualnego świata jest bezpieczna. Sprawdź, czy nie wyświetlają się komunikaty ostrzegawcze. Korzystaj z sieci z rozwagą, pamiętając nie tylko o sobie, ale i o twoim otoczeniu.
- POŁĄCZ: ciesz się możliwościami, jakie daje bezpieczne korzystanie z internetu.

Ponadto dobre praktyki promujące e-bezpieczeństwo to m.in. wykorzystanie proponowanych przez serwis Edukacja Medialna metod:

- Bądź anonimowy. Jeśli nie musisz podawać swoich danych prywatnych – nie rób tego. Im mniej informacji o tobie jest w sieci, tym jesteś bezpieczniejszy.
- Ustaw „silne" hasła. Ważne, aby twoje hasła były jak najdłuższe. Miej wiele haseł i czasem je zmieniaj.
- Sprawdzaj, czy łączysz się bezpiecznie (przez połączenie https://). Bezpieczne połączenia oznacza się za pomocą zielonego zaznaczenia lub kłódeczki koło paska adresu. Czasem występuje problem

z bezpieczeństwem połączenia i pojawiają się ostrzeżenia o błędach certyfikatu. Nie ignoruj ich, zwłaszcza jeśli witryna nie jest godna zaufania lub wcześniej nie pojawiał się na niej błąd.
- Zainstaluj programy: Adblock, NoScript, Flashblock, Cookie Monster. Blokują one niepożądane elementy stron. Np. Adblock nie tylko usunie reklamy, lecz także ograniczy przepływ informacji o historii przeglądania.
- Stosuj tryb prywatny w przeglądarkach. Jest przydatny, jeśli korzystasz z komputera dostępnego dla innych osób. Po zakończeniu sesji kasowana jest cała jej historia oraz ciasteczka.
- Wyloguj się po pracy. Nie można o tym zapomnieć!

Reasumując, warto zaznaczyć, że na e-bezpieczeństwo składają się takie elementy jak podnoszenie poziomu świadomości społecznej w obszarze cyberbezpieczeństwa poprzez informowanie o zagrożeniach i sposobach radzenia sobie z nimi, promowanie zachowań służących poprawie bezpieczeństwa internautów, ich rodzin i otoczenia, kształtowanie odpowiedzialnych postaw wszystkich użytkowników sieci, zaangażowanie sektora publicznego i prywatnego w działania promujące cyberbezpieczeństwo oraz budowanie środowiska sprzyjającego wymianie dobrych praktyk i edukacji z zakresu cyberbezpieczeństwa. Nie bez znaczenia są też dostępne w sieci informacje pozwalające na zrozumienie zagrożeń w cyberprzestrzeni oraz tego, jak stosować skuteczne sposoby zabezpieczenia się przed nimi (np. https://www.gov.pl/web/cyfryzacja/edukacja/; https://www.cert.pl/; https://cyberpolicy.nask.pl/; https://it-szkola.edu.pl/).

Emilia Musiał

Bezpieczeństwo. Teoria – badania – praktyka, A. Czupryński, B. Wiśniewski, J. Zboina (red.), Wydawnictwo CNBOP-PIB, Józefów 2015; *DIGCOMP. Ramy odniesienia dla rozwoju i rozumienia kompetencji cyfrowych w Europie*, Biuro Publikacji Komisji Europejskiej, Luksemburg 2013; Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022; S. Kozak, *Patologia cyfrowego dzieciństwa i młodości. Przyczyny, skutki, zapobieganie w rodzinach i szkołach*, Difin, Warszawa 2014; E. Musiał, *e-Bezpieczeństwo*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo,Wydawnictwo Libron, Kraków 2019; J. Piwowarski, *Fenomen bezpieczeństwa. Pomiędzy*

zagrożeniem a kulturą bezpieczeństwa, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2015; Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, M.P. 2019, poz. 1037; StojPomysl-Polacz.pl (dostęp 1.02.2020); *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, J. Lizut (red.), Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014; *Zagrożenia cyberprzestrzeni i świata wirtualnego*, J. Bednarek, A. Andrzejewska (red.), Difin, Warszawa 2014.

EDUKACJA DLA BEZPIECZEŃSTWA – przynależy do dziedziny nauk społecznych, w tym dyscypliny →nauk o bezpieczeństwie [t. 3]. Rozumienie jej istoty wymaga jednak merytorycznego i metodycznego wsparcia ze strony pedagogiki, nauk o polityce, prawa, nauk przyrodniczych, technicznych, nauk medycznych, a nawet nauk o zdrowiu. Właśnie z tego powodu edukację dla bezpieczeństwa przedstawiać należy w ujęciu interdyscyplinarnym. Tę interdyscyplinarność dostrzegł także A. Pieczywok, podkreślając związek edukacji dla bezpieczeństwa z pedagogiką, filozofią, psychologią, prakseologią, socjologią, antropologią oraz polityką społeczną.

Edukacja dla bezpieczeństwa jest filarem kształtowania środowiska i →kultury bezpieczeństwa, co wynika z dokumentów strategicznych. Fakt ten podkreślają także badacze przedmiotu – m.in. E. Szweda, który stwierdza, że „projektowanie i urzeczywistnianie bezpieczeństwa człowieka jest możliwe z wyraźną obecnością edukacji, wychowania, czyli pedagogiki".

Edukacja dla bezpieczeństwa weszła do powszechnego użytku po reformie programowej kształcenia, która miała miejsce w 2008 r. Jednak po raz pierwszy zdefiniowano ją podczas badań systemu bezpieczeństwa Rzeczypospolitej Polskiej, które na Akademii Obrony Narodowej (AON) w latach 1993–1995 realizował T. Jemioło. Edukacja dla bezpieczeństwa zastąpiła edukację obronną, natomiast ciężar jej problematyki przeniesiono z przeciwdziałania →zagrożeniom [t. 4] zewnętrznym na kształtowanie bezpieczeństwa państwa oraz narodu. Jak podkreśla Szweda, w tym okresie termin edukacja dla bezpieczeństwa obejmował:

> system dydaktyczno-wychowawczej działalności rodziny, szkoły, wojska, środków masowego przekazu, organizacji społecznych

> i stowarzyszeń służącej upowszechnianiu idei, wartości, wiedzy i umiejętności bezpośrednio istotnych dla zachowania zewnętrznego i wewnętrznego bezpieczeństwa państwa.

Pozaformalny wymiar edukacji dla bezpieczeństwa dostrzegł także J. Kunikowski, definiując ją przez pryzmat

> procesów społeczno-edukacyjnych i wychowawczych realizowanych w szkole, rodzinie, społecznych organizacjach proobronnych, a także stowarzyszeniach społecznych, które zakładają kształtowanie świadomości dotyczącej bezpieczeństwa człowieka, społeczeństwa i narodu.

Źródłem celów edukacji dla bezpieczeństwa są potrzeby i oczekiwania społeczeństwa w stosunku do niej. Takie założenia są podstawą jakości podejmowanych działań. Efektywne kształtowanie poczucia bezpieczeństwa człowieka powinno ponadto obejmować potrzeby wszystkich grup odbiorców oddziaływań edukacyjnych. W. Kitler wyróżnia: jednostkę (realizującą ważne dla siebie wartości), formalne (np. rodzina, środowisko pracy) i nieformalne grupy społeczne, organizacje społeczne, jak również struktury sformalizowane, wyodrębnione na danym obszarze (np. gmina, powiat, województwo, państwo czy grupa państw). Potrzeby w zakresie bezpieczeństwa, adekwatnie do powyższej typologii, podzielić można na jednostkowe, grupowe, ogólnonarodowe oraz międzynarodowe.

W projektowaniu i realizacji założeń edukacji dla bezpieczeństwa powinno się uwzględniać wszystkie z powyższych grup odbiorców. Niestety, w praktyce prowadzenie diagnozy poczucia bezpieczeństwa odbiorców oddziaływań edukacyjnych przed rozpoczęciem zajęć odbywa się sporadycznie. Równie rzadko definiowane są potrzeby danej grupy w zakresie bezpieczeństwa. Nośnikiem celów i wartości edukacji dla bezpieczeństwa zazwyczaj pozostają potrzeby ogólnonarodowe i międzynarodowe, które wyartykułowane są w obowiązujących aktach normatywnych. Zjawisko to dotyczy zwłaszcza edukacji dla bezpieczeństwa w ujęciu formalnym.

Edukacja dla bezpieczeństwa, jak podkreśla Pieczywok, umożliwia realizację funkcji:

- wdrożeniowej – przygotowanie człowieka do życia oraz pełnienia obowiązków zawodowych;
- korekcyjnej – w zakresie niewłaściwych postaw i zachowań w zgodnie z obowiązującymi normami społecznymi;
- socjalizacyjnej – wdrażanie do obowiązujących w danej grupie norm i wartości;
- stymulacyjnej – motywacja do efektywnego działania w zakresie eliminacji zagrożeń;
- osobotwórczej – ustawiczne doskonalenie posiadanych kompetencji.

W ramach tak rozumianej edukacji dla bezpieczeństwa człowiek może się przygotować do odgrywania ról zawodowych oraz życiowych. Właściwie rozumiana i realizowana edukacja dla bezpieczeństwa rozwija także kompetencje, które pozwalają na przeciwdziałanie zagrożeniom, a przede wszystkim umożliwiają rozwój jednostki i społeczeństwa.

Edukacja dla bezpieczeństwa powinna rozwijać wszystkie składniki kompetencji człowieka, tj. wiedzę, umiejętności oraz postawy. Współczesny paradygmat dydaktyki kładzie także nacisk na rezygnację z metod podających na rzecz metod konstruktywistycznych, dostrzegających w uczniu podmiot sprawczy, zdolny do samodzielnego budowania własnej wiedzy. Z powyższego wynika potrzeba nie tyle „przekazania" wiedzy, ile zainspirowania uczniów, słuchaczy bądź odbiorców do samodzielnego poszukiwania potrzebnych → i n f o r m a c j i czy dążenia do rozwijania postaw, które – za E. Włodarczyk – „pozwolą w kontakcie z nieznanymi dotychczas wyzwaniami i zagrożeniami zachować poczucie bezpieczeństwa".

W ramach edukacji dla bezpieczeństwa za R. Rosą można wyodrębnić 4 obszary działań, zwane także warstwami tematycznymi:

- warstwa poznawcza – system pojęć i wiedzy;
- warstwa metodologiczna – aktywność badawcza w dziedzinie nauk o bezpieczeństwie;
- warstwa aksjologiczna – edukowanie w zakresie różnych wartości, w tym bezpieczeństwa;
- warstwa prakseologiczna – sposoby efektywnej realizacji edukacji dla bezpieczeństwa.

Rozumienie i skuteczna realizacja edukacji dla bezpieczeństwa wymagają odniesienia jej definicji do pojęć edukacji i bezpieczeństwa.

Tylko wówczas możliwe jest projektowanie działań adekwatnych do przyjmowanych celów.

Należy przyjąć za B. Śliwerskim, że edukacja jest zespołem oddziaływań, które sprzyjają formowaniu się zdolności życiowych człowieka. Procesy kształcenia oraz wychowania są integralnymi składnikami tak rozumianej edukacji. Pierwszy z nich koncentruje się głównie na budowaniu wiedzy i umiejętności, drugi natomiast zmierza do rozwijania postaw niezbędnych dla człowieka na każdym etapie jego życia.

Pojęcie bezpieczeństwa ewoluowało w wyniku rozszerzania się skali zagrożeń. Zmodyfikowano w związku z tym metody, za pomocą których można im przeciwdziałać. Jak podkreśla Pieczywok, dążenie do zapewnienia „właściwego poziomu bezpieczeństwa ma charakter ciągły", toteż bezpieczeństwo znacznie częściej określa się mianem procesu. W literaturze przedmiotu bywa ono jednak opisywane również pojęciem stanu, który w określonych sytuacjach życiowych może mieć charakter zmienny, a zatem ulegać poprawie lub pogorszeniu. W 1984 r. J. Stefanowicz zaproponował podejście łączące te sposoby definiowania bezpieczeństwa. Wskazał on, że bezpieczeństwo to zarówno stan, jak i – zmienny w czasie – proces. W takim rozumieniu nie należy oczekiwać, że raz osiągnięte poczucie bezpieczeństwa będzie spełniało kryterium stałości i gwarancji. Proces ten wymaga działań ustawicznych, opartych o ciągłe modyfikowanie procedur oraz uwzględnianie zewnętrznych i wewnętrznych uwarunkowań.

Procesualne ujęcie bezpieczeństwa jest filarem rozumienia edukacji dla bezpieczeństwa, której cele – w sytuacji wszechobecnej zmiany – koncentrują się nie tylko na przeciwdziałaniu znanym już zagrożeniom, ale także na umiejętności dostrzegania i reagowania na nowe, nieznane dotychczas zagrożenia oraz radzenia sobie z wyzwaniami teraźniejszości i przyszłości. Realizacja tak sformułowanych celów wymaga podejmowania ustawicznych działań edukacyjnych. Z tego powodu w procesie kreowania środowiska i kultury bezpieczeństwa kluczowe znacznie ma samoedukacja. Jej jakość zależy od ukształtowanej w rodzinie i szkole motywacji do całożyciowego uczenia się.

Kompleksowe podejście do rozumienia istoty edukacji dla bezpieczeństwa wymaga także uwzględnienia 2 aspektów bezpieczeństwa. Bezpieczeństwo wewnętrzne – w typologii R. Zięby – odnosi się do stabilności

podmiotu, którego działalność nie powoduje generowania sytuacji zagrażających. Bezpieczeństwo zewnętrzne obejmuje natomiast przeciwdziałanie zagrożeniom, które powstają poza podmiotem. Przyjęcie tych 2 aspektów bezpieczeństwa związane jest jednak z dylematem opisanym przez B. Buzana, gdyż często trudno wskazać granicę pomiędzy wolnością działania jednostki a zagrożeniami, jakie mogą być konsekwencją tej wolności w przekonaniu innych osób. Jak podkreśla Włodarczyk:

> Edukacja dla bezpieczeństwa realizowana w tych dwóch aspektach wymaga z jednej strony troski o zmniejszenie skali zagrożeń zewnętrznych, a z drugiej rozwijania postaw społeczeństwa opartych na przekonaniu, że bezpieczeństwo to przede wszystkim niegenerowanie zagrożeń dla zdrowia i życia własnego oraz innych osób.

Holistyczne rozumienie pojęcia bezpieczeństwa wymaga także wyodrębnienia bezpieczeństwa negatywnego oraz pozytywnego, co zostało zaakcentowane w pracach J.S. Nye'a. Pierwszy składnik bezpieczeństwa (ujęcie wąskie, negatywne) koncentruje się na gwarancji przetrwania i eliminacji zagrożeń. Drugi natomiast (ujęcie szersze, pozytywne) odnosi się do swobody rozwoju człowieka oraz jego aktywności w momencie pojawiania się wyzwań. Podobne przekonanie zaprezentował B. Balcerowicz, który mówiąc o bezpieczeństwie, wskazał na jego 2 istotne elementy: gwarancję przetrwania oraz gwarancję rozwoju człowieka. W taki sposób należałoby rozumieć edukację dla bezpieczeństwa, której celem nie powinno być wyłącznie przeciwdziałanie zagrożeniom, lecz – definiowane szerzej – przygotowanie człowieka do skutecznego działania w nieznanych i często trudnych sytuacjach zagrażających jego zdrowiu lub życiu, a także efektywne reagowanie na wyzwania. Realizacja tego celu będzie możliwa jedynie wówczas, gdy absolwenci szkół będą osobami odpowiedzialnymi, asertywnymi i przekonanymi o własnej wartości, gdy będą to ludzie rozumiejący problemy współczesnego świata, ale także przygotowani do twórczego działania w odpowiedzi na wszechobecne zmiany.

Definicję edukacji dla bezpieczeństwa odnaleźć można także w dokumentach strategicznych. W Strategii Bezpieczeństwa Narodowego

Rzeczypospolitej Polskiej jest ona postrzegana jako ważny element umożliwiający budowanie kapitału społecznego. W charakterystyce → s y s t e m u b e z p i e c z e ń s t w a n a r o d o w e g o [t. 4] jest ona wyodrębniona – obok podsystemu kierowania i podsystemu wykonawczego – jako istotny składnik podsystemu wsparcia. Zagwarantowanie bezpieczeństwa obywatelom jest bowiem jedną z podstawowych funkcji każdego państwa.

Edukacja dla bezpieczeństwa w Strategii Bezpieczeństwa Narodowego jest definiowana przez pryzmat efektów uczenia się, gdyż ma ona na celu umożliwianie obywatelom nabywania kompetencji związanych z bezpieczeństwem. W ujęciu strategicznym edukacja dla bezpieczeństwa realizowana jest w ramach szkolnictwa powszechnego oraz wyższego, za pośrednictwem instytucji państwowych oraz instytucji i stowarzyszeń pozarządowych. Dostrzeżono przy tym potrzebę poprawy jakości kształcenia w tym zakresie poprzez ustawiczne doskonalenie kwalifikacji kadry.

Z powyższego wynika, że edukacji dla bezpieczeństwa nie należy postrzegać wyłącznie przez pryzmat oddziaływań formalnych. Edukacja dla bezpieczeństwa jest ważnym składnikiem edukacji narodowej, gdzie konieczne jest uwzględnienie zarówno edukacji szkolnej, jak i pozaszkolnej, zorganizowanej oraz niezorganizowanej, jak podkreślają E. Jagiełło i G. Wierzbicki. Adresatami edukacji dla bezpieczeństwa, w ujęciu P. Tyrały i A. Olaka, powinni być przedstawiciele kadry kierowniczej, reprezentanci organów władzy i administracji państwa, podmioty prowadzące działalność gospodarczą, → f o r m a c j e o b r o n y c y w i l n e j, dzieci i młodzież, jak również wszystkie pozostałe grupy społeczne bez względu na wiek i wykonywany zawód. Jedynie takie kompleksowe rozumienie istoty edukacji dla bezpieczeństwa może stać się gwarantem jej skuteczności. W zmieniającym się świecie zagrożenia ewoluują bowiem tak gwałtownie, że żaden system edukacji formalnej nie jest zdolny do tego, by przygotować ludzi do radzenia sobie z każdym niebezpieczeństwem. Niestety w praktyce edukacja dla bezpieczeństwa w systemie kształcenia formalnego jest często marginalizowana, w systemie kształcenia pozaformalnego jej realizacja odbywa się często poza kontrolą państwa, „a w systemie kształcenia nieformalnego istnieje o tyle, o ile na pewnym etapie życia rozwinięto motywację człowieka do uczenia się przez całe życie", jak argumentuje w jednej z publikacji Włodarczyk.

Edukacja jest procesem trwającym całe życie, a ograniczanie jej wyłącznie do ujęcia formalnego spłyca jej istotę.

Edukację dla bezpieczeństwa w potocznym rozumieniu utożsamia się z funkcjonującym do 2009 r. na gruncie praktyki oświatowej przysposobieniem obronnym. W 2009 r. przedmiot ten zastąpiony został w podstawie programowej edukacją dla bezpieczeństwa, choć treści kształcenia nie uległy wówczas znaczącym zmianom. Zdaniem W. Chudego i L. Wełyczki pojęciem węższym znaczeniowo w stosunku do edukacji dla bezpieczeństwa jest także edukacja obronna. O ile edukacja obronna koncentruje się na zagrożeniach, o tyle edukacja dla bezpieczeństwa powinna odpowiadać na wyzwania, które dopiero stać się mogą zagrożeniami. Należy przyjąć za A. Araucz-Boruc, że edukacja dla bezpieczeństwa obejmuje zatem przysposobienie obronne i wojskowe, wychowanie patriotyczno-obronne oraz edukację obronną.

Wyodrębnione w literaturze przedmiotu definicje edukacji dla bezpieczeństwa odnoszą się do jej ujęcia formalnego, pozaformalnego i nieformalnego. Niewiele z prezentowanych podejść kładzie jednak nacisk na uwzględnienie w definicji zarówno przygotowania do przeciwdziałania zagrożeniom, jak i do kreatywnej aktywności podmiotu w obliczu wyzwań. W kontekście powyższych rozważań, odwołując się do autorskiej definicji, przyjmuję, że edukacja dla bezpieczeństwa

> jest ogółem procesów odbywających się w toku samodzielnego działania oraz współdziałania całego społeczeństwa w ramach oddziaływań formalnych i pozaformalnych skierowanych do ludzi (dzieci, młodzieży, dorosłych i starszych), mającym na celu rozwijanie kompetencji w zakresie: dostrzegania zagrożeń współczesnego świata, zapobiegania oraz przeciwdziałania zagrożeniom wewnętrznym i zewnętrznym, jak również adekwatnego reagowania na wyzwania współczesnego świata.

Edukacja dla bezpieczeństwa jest obecnie obowiązkowym przedmiotem nauczania w szkole podstawowej i ponadpodstawowej w wymiarze 30 godzin na każdym z wymienionych etapów edukacyjnych. Przed reformą programową z 2017 r. realizowana była w wymiarze po 30 godzin

na III i IV etapie edukacyjnym (gimnazjum i szkoła ponadgimnazjalna), a przed 2009 r. w wymiarze 30 godzin w I i II klasie szkoły ponadpodstawowej. Obowiązek realizacji edukacji dla bezpieczeństwa w szkole podstawowej i ponadpodstawowej (z wyjątkiem szkół dla dorosłych) określa także art. 166 Ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej.

Wśród podstawowych celów edukacji dla bezpieczeństwa w szkole podstawowej ustawodawca wyodrębnił:

- rozumienie istoty bezpieczeństwa państwa,
- przygotowanie uczniów do działań w sytuacjach nadzwyczajnych zagrożeń (katastrof i wypadków masowych),
- kształtowanie umiejętności z zakresu podstaw →pierwszej pomocy [t. 3],
- edukację zdrowotną.

Podobne (choć rozszerzone) cele ogólne są obszarem dociekań w ramach edukacji dla bezpieczeństwa realizowanej w szkole ponadpodstawowej.

Treści z zakresu edukacji dla bezpieczeństwa są także realizowane w przedszkolu, w klasach I–III szkoły podstawowej, na innych przedmiotach w szkole podstawowej i ponadpodstawowej (np. wychowanie fizyczne, wiedza o społeczeństwie, etyka), a także w ramach niektórych programów studiów na uczelniach wyższych.

Pozaformalną edukacją dla bezpieczeństwa – jak podkreślają autorzy →*Białej Księgi Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* [t. 1] – zajmują się:

- instytucje i formacje podległe: Ministerstwu Edukacji Narodowej (przedszkola i szkoły), Ministerstwu Nauki i Szkolnictwa Wyższego (uczelnie), Ministerstwu Obrony Narodowej (np. Wojskowe Centrum Edukacji Obywatelskiej), Ministerstwu Spraw Wewnętrznych (np. →Policja [t. 3], →Państwowa Straż Pożarna [t. 3] oraz Straż Graniczna),
- organy władzy samorządowej,
- stowarzyszenia i organizacje pozarządowe (np. Związek Harcerstwa Polskiego, Związek Strzelecki „Strzelec", Policyjne Towarzystwo Sportowe, stowarzyszenia kombatanckie, Liga Obrony

Kraju, Polski Czerwony Krzyż, →ratownictwo wodne [t. 3] i górskie).

Dodatkowo w zestawieniu tym należy wyodrębnić podmioty prowadzące działalność gospodarczą ukierunkowaną na edukację dla bezpieczeństwa, np. instruktorów nauki jazdy, przedsiębiorców zajmujących się bezpieczeństwem i higieną pracy, podmioty realizujące odpłatne szkolenia z pierwszej pomocy. Powyższa klasyfikacja pozwala podzielić wszystkie podmioty, instytucje i organizacje, które zajmują się edukacją dla bezpieczeństwa, na 3 grupy:

> świadczące edukację dla bezpieczeństwa odpłatnie, realizujące ustawowe obowiązki w zakresie edukacji dla bezpieczeństwa oraz prowadzące edukację dla bezpieczeństwa świadomie i bezinteresownie dzięki zainteresowaniu zagadnieniami wchodzącymi w jej zakres. Oczywiście jest to sztywny podział, nieuwzględniający możliwości współwystępowania wszystkich trzech sposobów realizacji edukacji dla bezpieczeństwa, które w praktyce także się zdarza.

Taka klasyfikacja zamieszczona została w jednej z publikacji Włodarczyk.

W ujęciu nieformalnym edukacja dla bezpieczeństwa realizowana jest za pośrednictwem rodziny, grupy rówieśniczej, znajomych, zakładu pracy, grup wyznaniowych, a także mass mediów. Mamy w tym miejscu najczęściej do czynienia z samoedukacją w zakresie bezpieczeństwa, która może być realizowana w oparciu o niezwykle szeroką ofertę edukacyjną (w tym także aplikacje urządzeń mobilnych). Podstawową trudnością w procesie samoedukacji jest jednak podtrzymanie motywacji do nauki, umiejętność weryfikacji materiałów oraz brak możliwości jednoznacznego ustalenia i respektowania standardów jakości tego typu edukacji.

Reasumując, w szerokim rozumieniu, edukacja dla bezpieczeństwa:

- nie może przygotowywać jedynie do przeciwdziałania zagrożeniom, gdyż w otaczającej człowieka rzeczywistości wciąż pojawiają się nowe wyzwania (ekonomiczne, demograficzne czy technologiczne),

- nie może koncentrować się wyłącznie na zagrożeniach globalnych, gdyż to zagrożenia jednostkowe oraz lokalne są częściej przedmiotem zainteresowań i potrzeb odbiorców oddziaływań edukacyjnych,
- powinna opierać się na diagnozie potrzeb i oczekiwań osób, do których kierowane są oddziaływania edukacyjne,
- powinna podobnym zainteresowaniem obejmować badanie, analizę i ocenę zagrożeń militarnych, politycznych, ekonomicznych, społecznych, kulturowych, ekologicznych czy zdrowotnych i projektować w tych obszarach niezbędne działania naprawcze.

Wzrost zagrożeń współczesnego świata stawia przed edukacją dla bezpieczeństwa zupełnie nowe wyzwania. Wzmacnianie systemu bezpieczeństwa państwa nie może odbywać się w oderwaniu od wysokiej jakości edukacji, sprzyjającej budowaniu kultury i → ś r o d o w i s k a b e z p i e c z e ń s t w a [t. 4] człowieka.

Ewelina Włodarczyk

A. Araucz-Boruc, *Bezpieczeństwo i obronność w edukacji młodzieży*, Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2015; *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013, B. Buzan, *People, States and Fear: an Agenda for International Security Studies in the Post-Cold War Era*, ECPR Press, Colchester 1991; W. Chudy, L. Wełyczko, *Wybrane zagadnienia edukacji dla bezpieczeństwa*, WSOWL, Wrocław 2010; E. Jagiełło, G. Wierzbicki, *Edukacja na rzecz bezpieczeństwa dzieci*, Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2017; T. Jemioło, *Edukacja obronna w świetle strategii bezpieczeństwa*, [w:] *Patriotyzm, obronność, bezpieczeństwo*, E.A. Wesołowska, A. Szerauc (red.), Szkoła Wyższa im. Pawła Włodkowica w Płocku, AON, Płock–Warszawa 2002; J. Kunikowski, *Słownik terminów wiedzy i edukacji dla bezpieczeństwa*, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce 2015; A. Pieczywok, *Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności*, AON, Warszawa 2012; tenże, *Wybrane problemy z zakresu edukacji dla bezpieczeństwa. Konteksty, zagrożenia, wyzwania*, AON, Warszawa 2011; R. Rosa, *Edukacja do bezpieczeństwa i pokoju w obliczu nowych wyzwań cywilizacyjnych i kulturowych*, [w:] *Edukacja dla bezpieczeństwa*, R. Stępień (red.), AON, Warszawa 1994; Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym

lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej, Dz. U. 2017, poz. 356; Rozporządzenie Ministra Edukacji Narodowej z dnia 23 grudnia 2008 r. w sprawie podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego w poszczególnych typach szkół, Dz. U. 2009, nr 4, poz. 17; Rozporządzenie Ministra Edukacji Narodowej z dnia 3 kwietnia 2019 r. w sprawie ramowych planów nauczania dla publicznych szkół, Dz. U. 2019, poz. 639; Rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia, Dz. U. 2018, poz. 467; R. Stępień, *Wprowadzenie*, [w:] *Współczesne zagadnienia edukacji dla bezpieczeństwa*, R. Stępień (red.), AON, Warszawa 1999; *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2014; J. Świniarski, *Filozoficzne podstawy edukacji dla bezpieczeństwa*, Departament Społeczno-Wychowawczy Ministerstwa Obrony Narodowej, Warszawa 1999; P. Tyrała, A. Olak, *Prakseologia w edukacji dla bezpieczeństwa*, Wydawnictwo Amelia, Rzeszów 2012; Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz. U. 2019, poz. 1541; E. Włodarczyk, E. Sadowska-Wieciech, J. Rokitowska, *Edukacja dla bezpieczeństwa. Istota i uwarunkowania*, Wydawnictwo Libron, Kraków 2018; E. Włodarczyk, *Edukacja dla bezpieczeństwa*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Kwalifikacje nauczycieli edukacji dla bezpieczeństwa*, [w:] *Bezpieczeństwo współczesnego państwa. Część 2. Wymiar narodowy*, J. Falecki, P. Łubiński (red.), Wydawnictwo Drukarnia Styl Anna Dura, Kraków 2019.

EDUKACJA DLA BEZPIECZEŃSTWA INFORMACYJNEGO – jest edukacją wspierającą kształtowanie →kultury bezpieczeństwa informacyjnego w społeczeństwie, stanowiącej integralną część narodowej kultury bezpieczeństwa.

→Kultura bezpieczeństwa coraz częściej postrzegana jest w kontekście 3 wymiarów: mentalno-duchowego, społecznego i materialnego, jest łączona z dbałością o zachowanie tożsamości narodowej, z pielęgnowaniem tradycji, ochroną dziedzictwa narodowego, w czym dostrzegany jest potencjał samoobronności podmiotów należących do danego narodu. Aby rozwijać kulturę bezpieczeństwa w tych sferach, konieczne jest wykształcenie „uważności" społeczeństwa na działania

wymierzone przeciwko kulturze danego narodu, uodpornienie go na obce wpływy i mobilizowanie jego gotowości do udzielania wsparcia organom odpowiedzialnym za zapewnienie bezpieczeństwa w wymiarze narodowym. Wymaga to od narodu świadomości i dojrzałości, szczególnie w obszarze → kultury informacyjnej i medialnej, bez której trudno zapewnić → bezpieczeństwo informacyjne [t. 1] i → bezpieczeństwo medialne [t. 1] podmiotom bezpieczeństwa.

Kształtowanie świadomości i dojrzałości informacyjnej wymaga edukacji narodu przyczyniającej się do wzbogacenia go w kompetencje informacyjne, medialne i technologiczne (cyfrowe). Wsparciem kształcenia w tym obszarze może być Model Edukacji Medialnej Informacyjnej i Cyfrowej (MEMIC) opracowany przez zespół reprezentujący m.in. Centrum Edukacji Obywatelskiej, Fundację Nowoczesna Polska, Polskie Towarzystwo Edukacji Medialnej. Brak tych kompetencji przejawia się wśród obywateli brakiem krytycznego rozumienia otoczenia medialnego, brakiem rozumienia zasad rządzących światem nowych mediów, brakiem poszanowania dla różnorodności kulturowej, niedostrzeganiem wspólnotowego i partycypacyjnego charakteru mediów cyfrowych. W analizowanym modelu zawarte są treści odnoszące się do problemów → edukacji obywatelskiej i kultury bezpieczeństwa, w tym kultury bezpieczeństwa informacyjnego. Zwrócono w nim uwagę, że bezpieczeństwo człowieka zależy nie tylko od siły zbrojnej i nowoczesnej → infrastruktury wojskowej, ale i od świadomości obywatela, umiejętności dokonywania przez niego wyborów, podejmowania decyzji, sposobu wykorzystywania → informacji, wiedzy i najnowszych → technologii informacyjno-komunikacyjnych [t. 4] (TIK), od jego zaangażowania w sprawy swoje i otoczenia, od aktywności społecznej, stosunku do potrzeby ochrony bezpieczeństwa publicznego.

Ponieważ potencjalnym → zagrożeniem [t. 4] wynikającym z postępu technologicznego jest alienacja jednostek i wykluczenie społeczne całych grup i narodów, problemem współczesności stał się proces tworzenia więzi między członkami społeczeństwa. Więzi te muszą być wg J. Piwowarskiego budowane na wspólnie wypracowanych normach zachowania wynikających z akceptowanych przez naród przenikających się systemów społecznych, religijnych i filozoficznych, moralności, obyczaju

i tradycji narodowej. Wzmacniane są także dzięki kulturze informacyjnej społeczeństwa oraz jego kompetencjom informacyjnym – jak konkluduje M. Cieślarczyk, kształtowanie kultury bezpieczeństwa bez dbałości o kulturę informacyjną może nie przynieść oczekiwanych efektów. Jest tak zwłaszcza wtedy, gdy bezpieczeństwo informacyjne postrzega się w szerszej perspektywie jako czynnik stanowiący podstawę rozwoju intelektualnego, którego brak powoduje czasową lub względnie trwałą utratę przez jednostkę zdolności do szeroko rozumianego rozwoju w środowisku TIK. W tym ujęciu bezpieczeństwo informacyjne dotyczy także zachowań i postaw różnych podmiotów w →infosferze, ochrony →środowiska informacyjnego [t. 4] przed destrukcyjnymi działaniami człowieka i ochrony człowieka przed patologiami w nim występującymi. Nie ogranicza się zatem tylko do ochrony informacji przed nieuprawnionymi działaniami ludzi, przed awariami sprzętu i wadami oprogramowania, przed skutkami katastrof i działań terrorystycznych oraz przed błędami ludzkimi i organizacyjnymi. Dotyczy np. szeroko rozumianych problemów ekologii informacji.

Przygotowanie społeczeństwa do bezpiecznego funkcjonowania we współczesnej infosferze wymaga edukacji dla bezpieczeństwa informacyjnego i medialnego. Dlatego kompetencje informacyjne, medialne i cyfrowe powinny stać się przedmiotem zainteresowania dydaktyków zajmujących się →edukacją dla bezpieczeństwa, określaną „fundamentem kształtowania się kultury bezpieczeństwa w społeczeństwie". Ich znaczenie dla samorealizacji, rozwoju indywidualnego, aktywności obywatelskiej i integracji społecznej przekłada się na wychowanie świadomego obywatela. Kompetencje te są ważnymi komponentami kultury bezpieczeństwa informacyjnego, bez których trudno wychować dojrzałego informacyjnie obywatela. Dlatego do kursu z zakresu edukacji dla bezpieczeństwa powinny być włączone problemy kultury bezpieczeństwa informacyjnego, przez którą należy rozumieć:

> sferę aktywności człowieka kształtowaną przez świadomość informacyjną i sposób myślenia o bezpieczeństwie w infosferze; wartości, normy i reguły wspierające potrzebę podwyższania poziomu kultury bezpieczeństwa, pozwalającej dostrzegać wyzwania,

> szanse i zagrożenia w lokalnej i globalnej przestrzeni informacyjnej; postawy wpływające na uwrażliwienie społeczeństwa na znaczenie bezpieczeństwa informacyjnego i kształtowanie zachowań charakterystycznych dla dojrzałych informacyjnie użytkowników infosfery współodpowiedzialnych za to bezpieczeństwo. Zachowania te wynikają z oddziaływania na siebie wymienionych powyżej komponentów kultury. Odnoszą się one do przedmiotów i innych wytworów związanych z bezpieczeństwem informacyjnym i uczestnictwem podmiotów w procesie informacyjnym.

Według A. Filipek kultura bezpieczeństwa informacyjnego wymaga umiejętności

> skupiania się i poszukiwania odpowiedzi na pytania dotyczące tego, czy wykorzystywanie i posługiwanie się daną informacją, opieranie się na niej, będzie służyło bezpieczeństwu tego podmiotu i innych podmiotów: czy będzie pozytywnie oddziaływało na ich otoczenie, czy też będzie mogło powodować jego degradację

– szczególnie w odniesieniu do obszaru wartości, norm i zasad. Obszarem zainteresowania kultury bezpieczeństwa informacyjnego są zatem problemy:

- budowania świadomości bezpieczeństwa informacyjnego wśród społeczeństwa;
- pozyskiwania wiedzy o zagrożeniach generowanych przez cywilizację cyfrową;
- odpowiedzialności za utrzymywanie stanu bezpieczeństwa w infosferze;
- pielęgnowania wartości, na których można budować bezpieczeństwo jednostki i narodu;
- kształtowania postaw ludności wobec problemów bezpieczeństwa informacyjnego, ich emocji związanych z dążeniem do przeciwdziałania zagrożeniom i wzmacniania więzi;
- kształtowania zachowań, które sprzyjają budowaniu poczucia bezpieczeństwa informacyjnego i niwelowaniu stanów zagrożenia.

W →Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej zwraca się uwagę na konieczność włączenia sektora publicznego, prywatnego i obywatelskiego do działań na rzecz tworzenia →środowiska bezpieczeństwa [t. 4] informacyjnego kraju. Zwraca się także uwagę na konieczność zaangażowania przedstawicieli tych sektorów w proces ciągłego kształcenia i podnoszenia świadomości o zagrożeniach informacyjnych. Zaleca się tworzenie programów kształcenia kadr na potrzeby systemu →cyberbezpieczeństwa [t. 1]. Edukacja w zakresie bezpieczeństwa informacyjnego traktowana jest jako ważne ogniwo wsparcia tego systemu, a umiejętności i świadomość indywidualnych użytkowników za jeden z filarów cyberbezpieczeństwa. Włączenie społeczeństwa do budowania środowiska bezpieczeństwa informacyjnego powinno dokonywać się poprzez:

- zapobieganie zjawisku wykluczenia informacyjnego,
- zaangażowanie społeczeństwa w proces weryfikowania odbieranych przekazów informacyjnych,
- współpracę z organizacjami służącymi zapewnieniu tożsamości narodowej i dziedzictwa kulturowego,
- podejmowanie inicjatyw kulturalnych wchodzących w skład przedsięwzięć wspierających →politykę informacyjną [t. 3] państwa,
- podwyższanie własnej odporności na ataki informacyjne i świadomości na temat współczesnej →wojny informacyjnej [t. 4].

Nie bez przyczyny do zadań preparacyjnych systemu bezpieczeństwa informacyjnego włącza się działania tzw. ogniw wsparcia, czyli naukę, edukację i społeczeństwo.

Oznacza to, że edukacja dla bezpieczeństwa informacyjnego, oprócz kształtowania kultury bezpieczeństwa, jest ściśle związana z podstawowymi problemami bezpieczeństwa informacyjnego i zarządzania tym bezpieczeństwem. Obejmują one m.in. zagadnienia:

- rozumienia polityki bezpieczeństwa informacyjnego (PBI) i znaczenia dokumentów PBI dla prawidłowego funkcjonowania i rozwoju organizacji, grupy, narodu;
- metod i technik socjotechnicznych stosowanych przez osoby nieuprawnione do pozyskania informacji;

- znajomości technologii informatycznych pozwalających na zabezpieczenie zbiorów informacji niebędących do wglądu publicznego;
- dbanie o bezpieczeństwo infrastruktury teleinformatycznej; znajomości zagrożeń generowanych przez cywilizację cyfrową.

Przykładowo, edukacja ta mogłaby obejmować następujące bloki tematyczne:

- analiza informacji i służby analityczne;
- edukacja dla bezpieczeństwa informacyjnego i medialnego;
- ewaluacja otwartych źródeł informacji;
- komunikacja firmy z mediami;
- kultura organizacyjna firmy a kultura bezpieczeństwa;
- narzędzia wyszukiwania informacji w internecie;
- polityka bezpieczeństwa informacyjnego;
- prawne aspekty ochrony informacji i systemów informacyjnych;
- ochrona → informacji niejawnych i danych osobowych;
- przestępstwa przeciwko bezpieczeństwu informacyjnemu;
- techniki → manipulacji informacją [t. 3];
- udostępnianie informacji publicznej;
- → wywiad [t. 4] i → kontrwywiad gospodarczy;
- zarządzanie bezpieczeństwem informacyjnym.

W edukacji dla bezpieczeństwa informacyjnego nie można pominąć jednak tak ważnych dla podmiotu bezpieczeństwa zagadnień, jak:

- kształcenie kultury bezpieczeństwa w warunkach zagrożenia globalną wojną informacyjną,
- kształcenie kompetencji obywatelskich i współżycia społecznego przygotowujących jednostkę do przeciwstawiania się sterowanym działaniom popierającym i pielęgnującym niewiedzę tłumu,
- kształcenie kompetencji informacyjno-medialnych pozwalających na samodzielny dobór źródeł informacji i własną refleksję nad treścią komunikatów,
- rozwijanie kompetencji międzykulturowych i wielokulturowych, dających możliwość rozumienia innych i nieulegania wpływom szowinistycznym, nacjonalistycznym, a poprzez to budujących odporność na manipulację,

- rozwijanie kompetencji komunikacyjnych, umiejętności negocjacji, prowadzenia dialogu, rozwiązywania konfliktów, wzajemnego poznawania swoich racji wymagających umiejętności analizy i syntezy danych, uogólniania i interdyscyplinarnego podejścia do pozyskanych informacji,
- kształcenie kompetencji obchodzenia się z lękiem i niepewnością oraz funkcjonowania w →społeczeństwie ryzyka [t. 4], pozwalających na racjonalne wykorzystanie wiedzy o zagrożeniach generowanych przez cywilizację technologiczną, w tym o zagrożeniach związanych z atakami →cyberterrorystycznymi [t. 1],
- rozumienie procesów globalizacyjnych i konsekwencji wynikających z konstytuowania się światowego →społeczeństwa informacyjnego [t. 4].

W miarę eskalacji działań związanych z walką informacyjną w coraz większym stopniu edukacja dla bezpieczeństwa informacyjnego będzie musiała koncentrować się na problemach cyberbezpieczeństwa i obrony przed atakami informacyjnymi, rozpoznawania incydentów informacyjnych i postępowania w sytuacji zagrożeń, umiejętności oszacowania ryzyka planowanych operacji informacyjnych, podejmowania decyzji w warunkach permanentnej walki informacyjnej, a także odniesienia problemów bezpieczeństwa informacyjnego do prowadzonej w wymiarze globalnym wojny informacyjnej. Zmieni więc charakter z edukacji mającej uświadamiać różnorodność zagrożeń informacyjnych, generowanych w świecie rozwiniętych technologii informacyjno-medialnych, na edukację przygotowującą do takiego postępowania w cywilizacji cyfrowej, które nie pozwoli stać się podmiotowi celem ataków informacyjnych i narzędziem w walce informacyjnej prowadzonej przez nierozpoznanych agresorów. Jej celem będzie kształtowanie kultury bezpieczeństwa informacyjnego obywateli, którzy kulturę tę powinni pielęgnować w swoim środowisku prywatnym i zawodowym oraz egzekwować od swoich podwładnych.

Kształtowanie kultury bezpieczeństwa informacyjnego dotyczy całego społeczeństwa i wymaga od każdego obywatela podwyższonej wrażliwości i uważności na dostrzeganie negatywnych zjawisk mających związek z procesem informacyjnym. Dotyczy wyposażenia podmiotów bezpieczeństwa w umiejętności oceny wpływu tych zjawisk na prawidłowe

funkcjonowanie infosfery, której bezpieczeństwo oddziałuje bezpośrednio na bezpieczeństwo narodowe. Wymaga także aktywnej odporności pozwalającej na przeciwstawienie się, złagodzenie i przezwyciężenie skutków ataków informacyjnych i innych działań wymierzonych w bezpieczeństwo informacyjne w skali personalnej, organizacyjnej czy narodowej. Dzięki kulturze bezpieczeństwa informacyjnego łatwiejsze staje się pozyskanie „uważności" w postrzeganiu wyzwań, szans i zagrożeń w zmediatyzowanym społeczeństwie informacyjnym.

Hanna Batorowska

H. Batorowska, *Information and Media Literacy (IML) w edukacji dla bezpieczeństwa*, [w:] *Człowiek – Media –Edukacja*, J. Morbitzer, D. Morańska, E. Musiał (red.), Wydawnictwo Naukowe Wyższej Szkoły Biznesu, Dąbrowa Górnicza 2017; taż, *Kultura bezpieczeństwa informacyjnego*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; taż, *Kultura bezpieczeństwa w kontekście Modelu Edukacji Medialnej, Informacyjnej i Cyfrowej (MEMIC)*, [w:] *Człowiek – Media – Edukacja*, J. Morbitzer (red.), Akademia WSB, Dąbrowa Górnicza 2020; taż, *Kształcenie w obszarze bezpieczeństwa informacyjnego*, [w:] *Edukacja XXI wieku. Procesy edukacyjne w dobie globalizacji, społeczeństwa informacyjnego i zmian na rynku pracy*, M. Kozielska, A. Zduniak (red.), Wyższa Szkoła Bezpieczeństwa, Poznań 2018; taż, *Potrzeba edukacji w zakresie kultury bezpieczeństwa informacyjnego*, „Bibliotheca Nostra" 2018, nr 2 (52); H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019; M. Cieślarczyk, *Kultura informacyjna jako element kultury bezpieczeństwa*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*, t. 1, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2015; *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, BBN, Warszawa 2015; A. Filipek, *Rola edukacji w kształtowaniu kultury bezpieczeństwa informacyjnego*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; R. Klepka, E. Musiał, *Bezpieczeństwo medialne*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *Model Edukacji Medialnej, Informacyjnej i Cyfrowej (MEMIC)*, A. Pacewicz, G. Ptaszek (red.), Centrum Edukacji Obywatelskiej i in., Kraków–Warszawa 2019; J. Piwowarski, *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*, Wydawnictwo Akademii Pomorskiej, Słupsk 2016.

EDUKACJA DLA BEZPIECZEŃSTWA W SIECI – ogół procesów i oddziaływań oświatowo-wychowawczych, których celem jest przekazywanie wiedzy, kształtowanie określonych cech i umiejętności oraz postaw związanych z bezpiecznym użytkowaniem internetu.

Edukacja to termin złożony, obejmujący 2 ważne w życiu każdego człowieka procesy, a mianowicie wychowanie i kształcenie. Ma związek ze zdobywaniem wiedzy, rozwojem zdolności, nauką i doskonaleniem umiejętności, kształtowaniem pożądanych postaw i realizowaniem wartości. Jedną z nich – a opierając się na piramidzie A.H. Maslowa, można stwierdzić, że wręcz kluczową – stanowi →bezpieczeństwo [t. 1], należące równocześnie do podstawowych praw ludzkich. Bezpieczeństwo to – w dużym uproszczeniu – stan bez →zagrożenia [t. 4]. W odniesieniu do sieci będzie dotyczył umiejętności unikania lub radzenia sobie z potencjalnym niebezpieczeństwem.

W →edukacji dla bezpieczeństwa w latach 90. XX w. wyróżniono 5 obszarów, a mianowicie edukację dla bezpieczeństwa politycznego, militarnego, gospodarczego, publicznego, psychospołecznego oraz ekologicznego. Wszystkie te rodzaje wzajemnie się przenikają i uzupełniają, jednak w odniesieniu do korzystania z sieci najważniejsze wydają się oddziaływania oświatowo-wychowawcze, podejmowane w ramach edukacji dla bezpieczeństwa publicznego oraz psychospołecznego. Pierwsze z nich mają na celu kształtowanie świadomości prawnej społeczeństwa oraz właściwych postaw i zachowań w sytuacjach zagrażających obywatelom i porządkowi publicznemu, zaś drugie kształtowanie moralności społeczeństwa oraz postaw wobec zagrożeń psychospołecznych. Współcześnie podział ów należałoby poszerzyć, uwzględniając ważne aspekty bezpieczeństwa, które 30 lat temu trudno było przewidzieć, spowodowane rozwojem nowoczesnych technologii, zarówno w wymiarze indywidualnym, jak i społecznym. W ostatnich 2 dekadach postęp zmienił wyjątkowo dużo w kwestiach związanych m.in. z wychowaniem młodych pokoleń. Internet stał się powszechnym medium, wywracając do góry nogami stary porządek wraz z jego dobrze znanymi ograniczeniami i niebezpieczeństwami. Pojawiły się innowacyjne sposoby poznawania świata i uczenia się, zdobywania i gromadzenia →informacji, komunikowania się, spędzania czasu wolnego. Towarzyszyły im kolejne wyzwania, a nawet zagrożenia,

których nieustannie przybywa i na które odbiorcy nowych mediów nie do końca byli przygotowani. Równocześnie od dawna postuluje się kształtowanie kompetencji medialnych (ang. *media literacy*) i informacyjnych (ang. *information literacy*), a chociaż są one bardzo ważne i potrzebne, to węższe pojęcie – edukacja dla bezpieczeństwa w sieci – wydaje się wręcz koniecznością, ponieważ konsekwencje jej braku mogą się okazać dramatyczne.

Edukacja dla bezpieczeństwa w sieci jest niezbędna, ponieważ wkraczaniu do wirtualnego świata powinna towarzyszyć świadomość dużej skali i różnorodności prawdopodobnych sytuacji ryzykownych. Najbardziej zagrożone są tu dzieci i młodzież, gdyż nawet ich niejednokrotnie większa niż w przypadku osób dorosłych biegłość obcowania z nowymi technologiami nie chroni ich całkowicie, zwłaszcza w przypadku najmłodszych dzieci, mających praktycznie zerowe doświadczenie życiowe. Fundacja Dajemy Dzieciom Siłę donosi, że z urządzeń mobilnych korzysta aż 64% dzieci, w wieku od 6 mies. do 6,5 lat, z czego co czwarte z nich codziennie. Z kolei z badań przeprowadzonych w Polsce, Francji, Niemczech, Włoszech, Wielkiej Brytanii i Hiszpanii przez Disneya, The Future Laboratory i Taylor Nelson Sofres na 3020 respondentach w wieku 8–14 lat można się dowiedzieć, że 60% polskich dzieci w wieku 8–14 lat nie wyobraża sobie życia bez komputera i internetu. Najwięcej z nich – 77% – gra w internecie w gry, 75% szuka pomocy w odrabianiu prac domowych, a 71% kontaktuje się w sieci ze szkolnymi przyjaciółmi. W sieci dzieci i młodzież zaspokajają swoje potrzeby związane z rozrywką, edukacją i komunikacją/afiliacją.

Powszechność korzystania z internetu przez dzieci i młodzież wiąże się z coraz większą popularnością portali społecznościowych, wśród których niepodzielnie króluje Facebook. Według badań K. Borzuckiej-Sitkiewicz i K. Leksy 91% gimnazjalistów ma tam założone konto, na którym w ramach autopromocji 76% publikuje zdjęcia, 17% filmiki ze swoim udziałem, 11% dane osobowe, 31% informacje o aktualnej aktywności. Równocześnie rodzicielska kontrola aktywności młodzieży pozostawia wiele do życzenia, ponieważ 45% posiada pełną swobodę; blisko 5% ma sprawdzaną historię aktywności w sieci, w przypadku 1% założono programy służące kontroli, w 26% przypadków rodzice czasami sprawdzają, co znajduje

się na ekranie monitora, 22% respondentów nie potrafiło się odnieść do tej kwestii, a 2% udzieliło innych odpowiedzi. Niewiele lepiej wygląda kontrola czasu spędzanego w internecie: u 21% nie ma takich działań, 6% korzysta z sieci w dni wolne od nauki bez ograniczeń, a 9% również może to robić w dni wolne od nauki, jednak ma ograniczenia czasowe, u 19% rodzice nie kontrolują czasu spędzonego online w ciągu dnia, tylko wieczorem, u 40% tylko czasami ogranicza się czas spędzany w sieci, 6% odpowiedziało inaczej. Wydaje się, że rodzice częściej kontrolują czas spędzony online aniżeli treści, z jakimi stykają się ich dzieci, przy czym nie wykazano tu zależności od wykształcenia rodziców.

Aby określić zadania edukacji dla bezpieczeństwa w sieci, można posłużyć się choćby modelem kompetencji związanych z posługiwaniem się internetem przez dzieci w wieku od 9. do 13. roku życia, skonstruowanym w ramach projektu badawczego „Dzieci sieci" (realizacja – 2012 r.), którego koordynatorem był P. Siuda wraz z zespołem badawczym wspieranym konsultacjami ekspertów. Model ten obejmuje zachowania informacyjne – w tym sprawne i skuteczne docieranie do informacji oraz krytyczną ocenę informacji; zachowania produkcyjne – na które składa się tworzenie, przetwarzanie i prezentowanie treści oraz prawne aspekty produkowania i dystrybucji treści; życie w internecie obejmujące takie aspekty, jak empatia i wizerunek, a także bezpieczeństwo i prywatność oraz partycypację w społecznościach internetowych. Standard najbardziej tu interesujący, czyli bezpieczeństwo i prywatność, został wyrażony osiągnięciami, zgodnie z którymi dziecko zna zagrożenia związane z poruszaniem się w internecie, radzi sobie z internetowymi niebezpieczeństwami, uzyskuje kontrolę nad informacjami udzielanymi innym, jest świadome powiązań oraz różnic między komunikacją zapośredniczoną przez internet i niezapośredniczoną (np. w przyjaźniach realnych i wirtualnych), stosuje zasady higieny związanej z korzystaniem z komputera (prawidłowa pozycja, przerwy, ochrona wzroku etc).

Kto powinien realizować edukację dla bezpieczeństwa w sieci? Przypisanie tego zadania tylko jednej instytucji może okazać się niewystarczające. Z pewnością kluczową rolę mają tu pierwsi i najważniejsi wychowawcy dziecka, czyli rodzice. M. Jędrzejko i D. Morańska, analizując rolę rodziny w przygotowaniu młodego pokolenia do obsługi i rozumienia mediów

oraz życia w → społeczeństwie informacyjnym [t. 4], podkreślają potrzebę istnienia świadomości medialnej u opiekunów, która umożliwiałaby wsparcie edukacyjne i moralne młodego internauty, aby potrafił bezpiecznie poruszać się w cyfrowym świecie, nie stając się ofiarą licznych niebezpieczeństw.

Z drugiej strony potrzebne są kompetencje profesjonalistów, dlatego powinno się budować wieloletnie programy profilaktyki, które rozpoczynałyby się w I klasie szkoły podstawowej i byłyby realizowane corocznie. Proponuje się, by odbywały się cykliczne zajęcia dla uczniów i rodziców, a w przypadku nastoletnich uczniów także z udziałem nauczycieli. Niestety w większości szkół nie prowadzi się systematycznych programów w zakresie edukacji do mediów, w tym pedagogizacji multimedialnej rodziców. Także badania EU Kids Online Polska 2018 potwierdzają, że w polskiej szkole zdecydowanie zbyt rzadko podejmuje się tematykę korzystania uczniów z sieci, zarówno w sferze dydaktycznej, jak i wychowawczej, nawet w stosunku do samych uczniów. W odniesieniu do rodziców stwierdza się, że niechętnie uczestniczą w zajęciach poświęconych → zagrożeniom internetowym [t. 4]. Z drugiej strony okazuje się, że spora część rodziców stara się podejmować działania mające na celu bezpieczne korzystanie z internetu przez ich dzieci, przy czym chętniej prowadzą z nimi rozmowy na ten temat, niż stosują nakazy i zakazy. Najniższe wyniki dotyczyły wykorzystywania rozwiązań technologicznych – programów stworzonych dla ochrony. Kiedy jakaś sytuacja w sieci jest niepokojąca, młodzi internauci najczęściej wycofują się, licząc na samoistne rozwiązanie problemu. Jeśli podejmują rozmowę na ten temat, to głównie z rówieśnikami, z którymi też najczęściej wymieniają się informacjami technicznymi, a najrzadziej poruszają kwestie etyczne związane z użytkowaniem internetu. Jednak blisko połowa dzieci (częściej młodsze i płci żeńskiej) opowiada rodzicom o tym, co je niepokoi i denerwuje w sieci. Większość ocenia wsparcie rodziców w tym względzie jako (trochę lub bardzo) pomocne – tu ponownie częściej dzieci młodsze i dziewczęta. Istotną informacją jest to, że aż 2/3 badanych dzieci i młodzieży twierdzi, że nie lekceważy rad i zaleceń rodziców dotyczących korzystania z internetu, a niektórzy wręcz sami o nie proszą, co wydaje się mocnym argumentem za potrzebą dokształcania się rodziców w tym względzie.

Edukacja dla bezpieczeństwa w sieci może być prowadzona w ramach niezwykle potrzebnej współcześnie edukacji medialnej i informacyjnej. Niestety w polskiej szkole wciąż istnieją braki w tym zakresie. Istniała co prawda międzyprzedmiotowa ścieżka edukacji czytelniczej i medialnej, jednak została zlikwidowana i przerzucona w rozproszonej formie do nowej podstawy programowej kształcenia ogólnego. Zatem kompetencji medialnych i informacyjnych, w tym związanych z bezpiecznym poruszaniem się po wirtualnym świecie, uczniowie nie zdobędą w ramach jednych, systematycznie prowadzonych zajęć. Podstawa programowa przedmiotu edukacja dla bezpieczeństwa nie obejmuje tych zagadnień; porusza się je zwykle w ramach informatyki bądź godzin wychowawczych, niekiedy w szkołach organizuje się dodatkowo zebrania lub warsztaty poświęcone tej problematyce, jednak są to działania dorywcze. Nie poświęca się również wystarczającej uwagi odpowiedniemu przygotowaniu nauczycieli w zakresie edukacji informacyjnej i medialnej, a także komunikacji społecznej (w tym interpersonalnej).

Poprawie sytuacji w tym polu powinien sprzyjać rozwój pedagogiki medialnej, której zadania są następujące:

- wypracowanie celów, metod, środków odpowiednich dla praktyki wychowawczej, mającej na celu przygotowanie wychowanków do właściwego odbioru mediów;
- badanie oddziaływania mass mediów na człowieka, uwzględniając ich wpływ, zasięg i skuteczność;
- wskazanie nauczycielom i wychowawcom celów mediów i zagrożeń wynikających z ich użytkowania w kontekście wychowawczym;
- pedagogizacja nauczycieli, rodziców, dziennikarzy w obszarze relacji wychowanek – media;
- określanie wymiaru pedagogicznego poszczególnych środków masowego przekazu.

Zadania te winno się realizować, korzystając z teorii i doświadczeń innych nauk i dyscyplin, takich jak pedagogika społeczna, psychologia społeczna, socjologia, andragogika, dydaktyka, medioznawstwo. Pedagogika medialna powinna spełniać funkcję opisową i diagnostyczną (naświetlającą to, jak jest, w kontekście sytuacji edukacyjnych oraz pozytywnego i negatywnego oddziaływania mediów); wyjaśniającą, czyli eksplikacyjną

(objaśniającą, odwołując się do różnych dyscyplin naukowych, dlaczego tak jest); prognostyczną (przewidującą konsekwencje różnych zjawisk) oraz techniczną, czyli praktyczną (zawierającą wskazówki, jak działać, aby osiągnąć pożądane cele lub uniknąć niepożądanych następstw). W jej ramach należy prowadzić edukację medialną będącą elementem kształcenia ogólnego, której cele dotyczą przygotowania do właściwego, krytycznego odbioru mediów oraz do wykorzystywania mediów jako narzędzi rozwoju intelektualnego i zawodowego, obejmującego również zagadnienia związane z technologią informacyjną.

Poza systematycznymi działaniami ze strony rodziny czy szkoły udział w edukacji dla bezpieczeństwa w sieci powinny mieć poszczególne rządy, promując →kulturę bezpieczeństwa cybernetycznego, wspierając badania i kształcenie w tym zakresie oraz dbając o odpowiednie ustawodawstwo dotyczące →cyberprzestępczości [t. 1], zwłaszcza wobec dzieci. Pomocne mogą być działania organizacji pozarządowych takie jak organizacja warsztatów czy konferencji, jak również wszelkie kampanie społeczne mające możliwość dotarcia do ogromnej rzeszy osób w każdym wieku. Należy zauważyć, że niezależnie od tego, kto zajmuje się kształceniem w omawianej dziedzinie, biorąc pod uwagę nieustanny rozwój technologii, wiedza powinna być systematycznie aktualizowana i weryfikowana.

Zarówno w kształceniu kompetencji medialnych i informacyjnych, jak i w samej edukacji dla bezpieczeństwa w sieci należy uwzględnić nie tylko warstwę instrumentalną, ale i sferę aksjologiczną. Jak podkreśla J. Morbitzer, zwracając uwagę zarówno na udogodnienia, jak i liczne zagrożenia związane z internetem i nowymi mediami, „humanistyczna orientacja staje się koniecznością, ponieważ inaczej niż w przypadku wiedzy technicznej, ta o człowieku i wartościach nie jest kumulowana, zatem każde pokolenie odkrywa ją na nowo".

Małgorzata Bereźnicka

M. Bereźnicka, *Edukacja dla bezpieczeństwa w sieci*, [w:] *Współczesne problemy bezpieczeństwa państwa*, O. Wasiuta, P. Mazur (red.), Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie, Stalowa Wola 2017; taż, *Edukacja dla bezpieczeństwa w sieci*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*,

O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; K. Borzucka-Sitkiewicz, K. Leksy, *Ekshibicjonizm społeczny w Internecie. Motywy i potencjalne zagrożenia dla zdrowia i bezpieczeństwa młodzieży*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2017; Fundacja Dajemy Dzieciom Siłę, FDDS.pl (dostęp 12.12.2019); S. Juszczyk, *Człowiek w świecie mediów – szanse i zagrożenia*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2000; J. Morbitzer, *Edukacja wspierana komputerowo a humanistyczne wartości pedagogiki*, Wydawnictwo Naukowe Akademii Pedagogicznej, Kraków 2007; A. Pieczywok, *Wybrane problemy z zakresu edukacji dla bezpieczeństwa. Konteksty, zagrożenia, wyzwania*, AON, Warszawa 2011; J. Pyżalski, *Rodzina i szkoła a przeciwdziałanie zaangażowaniu młodych ludzi w ryzykowne zachowania online*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2013, vol. 12, nr 1; J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, K. Abramczuk, *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*, Wydawnictwo Naukowe UAM, Poznań 2019; R. von Solms, S. von Solms, *Cyber Safety Education in Developing Countries, Systemics*, „Cybernetics and Informatics" 2015, vol. 13, no. 2; Ł. Wojtasik, *Kontakt dzieci z niebezpiecznymi treściami w Internecie, Raport z badań Gemius/FDN*, FDDS.pl (dostęp 15.10.2019).

EDUKACJA I KULTURA JAKO ŚRODKI WOJNY INFORMACYJNEJ FR – edukacja jest dziś nie mniej niż jakakolwiek inna sfera przedmiotem →wojny informacyjnej [t. 4] ze strony putinowskiej Rosji. Ale edukacja nie jest tylko biernym przedmiotem, ofiarą tej →agresji [t. 1], ma ona potencjał, aby być aktywnym podmiotem →przestrzeni informacyjnej [t. 3], dlatego w kontekście wojny informacyjnej edukację należy rozpatrywać nie tylko jako cel ataku, ale także jako strategiczne źródło zwycięstwa. Wojna informacyjna w edukacji jest przede wszystkim walką nie o teksty w podręcznikach i nie retorykę nauczycieli w klasach szkolnych, lecz walką o młodzież, jej umysł, sposób myślenia. Podręczniki, programy i technologie edukacyjne są środkiem do osiągnięcia tego celu. Głównym celem w tej →wojnie [t. 4] jest narzucenie młodemu człowiekowi gotowych wniosków, „prawomyślnego" sposobu rozumowania i właściwej ideologii poprzez zniekształcanie i selekcję →informacji; ucieka się od nauczania krytycznego myślenia i samodzielnego wyciągania wniosków.

To, co Rosja robi w przestrzeni edukacyjnej, wpisuje się w ogólną politykę informacyjnej agresji skierowanej przeciwko sąsiadom. Głównym środkiem oddziaływania na starsze pokolenia w przestrzeni informacyjnej

jest telewizja, w przypadku młodzieży są to internet, klasy szkolne i studenckie audytoria.

W swoim czasie R. Kjellén podkreślał, że kulturowa rosyjska dominacja nad narodami Europy Wschodniej „była w rzeczywistości nadużyciem niższej kultury nad wyższą". Ta dominacja była podtrzymywana przez

> politykę systematycznego ucisku wyższych narodów na europejskiej granicy oraz sztucznym i wymuszonym mieszaniem (w przeciwieństwie do naturalnego w Ameryce), które miały zniszczyć strefę buforową w Europie i pozwolić Rosji całą swoją masą nacisnąć na Zachód. Właśnie to jest rosyjska idea.

Obecny konflikt rosyjsko-ukraiński tylko to potwierdza. Na początku lat 90. ubiegłego wieku L. Gumilow, znany rosyjski historyk i etnolog, przedstawił rozczarowujące dla Rosjan wnioski, stwierdzając:

> Mechaniczne przeniesienie w warunkach Rosji zachodnioeuropejskich tradycji zachowania dało mało dobrego i nie jest to zaskakujące. Ponieważ rosyjski superetos pojawił się o 500 lat później. Zarówno my, jak i zachodni Europejczycy zawsze odczuwaliśmy tę różnicę, mieliśmy świadomość i za „swoich" jeden drugiego nie uważaliśmy. Ponieważ jesteśmy o 500 lat młodsi, to jak byśmy nie badali doświadczenia europejskiego, nie jesteśmy w stanie osiągnąć dobrobytu i zwyczajów charakterystycznych dla Europy. Nasz wiek, nasz poziom… przewiduje w ogóle inne imperatywy zachowania.

Rosja stara się oddziaływać na byłe republiki ZSRR nie tylko na płaszczyźnie gospodarczej, finansowej i energetycznej, lecz również poprzez humanistyczną ekspansję → *russkiego mira* [t. 3] („świata rosyjskiego"), religii, języka, historii i kultury. Objawia się to przede wszystkim w stosunku do Ukrainy i Białorusi. Wykorzystuje się przy tym komunistyczne pozostałości w postaci mitów wspólnej historii, „jednego narodu", prawosławia, „wielkiej wojny ojczyźnianej", a także blokowanie rozwoju struktur demokratycznych, gospodarczych, patriotycznych elit narodowych.

Granicami *russkiego mira* są granice przestrzeni informacyjnej, które kontroluje Moskwa. Rosja ma swoje ogromne terytoria, ale znacznie większa jest jej przestrzeń informacyjna. Granica językowa jest najważniejszą granicą państwa w wojnie informacyjnej, a front kulturowy jest nie mniej ważny niż rzeczywiste walki zbrojne.

P. Polańskyj, wiceminister oświaty i nauki Ukrainy, podczas przemówienia na międzynarodowej konferencji „Wojna informacyjna w XXI wieku – doświadczenia ukraińskiego konfliktu 2014–2015 lat dla Polski i Europy", która odbyła się w marcu 2015 r. w Warszawie, podkreślił, że rosyjscy agresorzy pokazują na Krymie całe spektrum wojny informacyjnej. Rodzice tamtejszych uczniów i nauczyciele podają, że wszystkie przedmioty związane z Ukrainą są eliminowane. Ogólna polityka jest taka, aby dzieci „zapomniały" o Ukrainie. W podręcznikach do historii informacja o Ukrainie jest ograniczona tylko do krótkiej wzmianki o „antypaństwowym, antykonstytucyjnym przewrocie". Funkcjonują biblioteki, ale dostęp do całości zbiorów nie jest możliwy. Blokuje się także dostęp do literatury „ekstremistycznej", do której zalicza się np. wiersze Ł. Ukrainki.

Jeszcze w 2010 r. Rosja rozprzestrzeniła w edukacji podejście typowe dla modelu FR: brak multidyscyplinarnego ujęcia problemów i różnorodności opinii, występuje tylko jeden „poprawny" punkt widzenia, wykorzystuje się jeden podręcznik do jednego przedmiotu. Wszystko to ma globalny cel – szerzyć w różnych państwach model rosyjskiej edukacji. Moskwa dobrze wie, że przepisywanie wzorów reakcji chemicznych lub wyrażeń algebraicznych nie daje zysków politycznych. Natomiast zniekształcanie humanistycznych przedmiotów pozwala osiągnąć planowany efekt ideologiczny. Tak samo była przyjęta w Ukrainie koncepcja kształcenia literackiego, przygotowana na podstawie wzorca *russkiego mira*. Wprost zapisano w niej, że wiodącą literaturą światową jest literatura rosyjska. Według tej koncepcji musiały zostać zmienione wszystkie szkolne programy nauczania i podręczniki. Jest to wewnętrzny front walki informacyjnej.

Zewnętrzny front wojny informacyjnej w edukacji ze strony Kremla jest ideologiczną indoktrynacją młodzieży poprzez edukację na tymczasowo okupowanym przez FR Krymie i próbą zniszczenia ukraińskiej edukacji w okupowanych regionach Doniecka i Ługańska. Na anektowanym Krymie edukacja, polityka i → p r o p a g a n d a [t. 3] są jedną całością.

Innym działaniem Kremla w wojnie informacyjnej w edukacji jest tworzenie próżni informacyjnej dla uczniów, rodziców i nauczycieli, tak aby nie mieli dostępu do innych źródeł informacji, ponieważ ułatwia to manipulację. Kontynuacja rosyjskiej agresji przeciwko ukraińskiej edukacji wyraźnie przejawia się w okupowanych przez rosyjskie wojska regionach Doniecka i Ługańska. Od września 2014 r. Rosja próbuje narzucić tam wyłącznie rosyjski język nauczania, rosyjskie standardy kształcenia, programy, podręczniki oraz całą historię Ukrainy. Wojska rosyjskie w okupowanych miastach Krymu i Donbasu zmuszają dzieci, rodziców i nauczycieli do przejścia na rosyjski program edukacji i rosyjskie podręczniki. Nikt nie pyta o opinię uczniów, rodziców czy nauczycieli. Ukraińska literatura edukacyjna i piękna są usuwane ze szkół i bibliotek oraz zabraniane. Kreml chce jak najszybciej i jak najintensywniej oddziaływać na młodych ludzi poprzez swoją ideologię, propagandę i *russkij mir*.

Ostatnie wydarzenia w Ukrainie mówią o pogłębieniu nie tylko walki politycznej wewnątrz partii politycznych, lecz również powiązanych z nimi procesów w życiu kulturalnym. Reformy w Ukrainie trwają, a walka na płaszczyźnie kulturowej nie zatrzymuje się ani na chwilę. „Historia stosunków kulturalnych między Ukrainą a Rosją – to historia wielkiej i jeszcze nie skończonej wojny", pisał jeszcze w 1954 r. J. Szewelow, kiedy w ZSRR hucznie obchodzono 300. rocznicę ugody perejasławskiej jako „świętego połączenia" Ukrainy z Rosją, i podkreślał, że „Perejasław z perspektywy trzech wieków wydaje się nam początkiem wielkiej tragedii".

Wojna w dziedzinie kultury toczy się także w trakcie zbrojnej ofensywy Rosji na Ukrainę. Dowodem na to jest uroczyste odsłonięcie pomnika w centrum Moskwy kijowskiemu księciu Włodzimierzowi I Wielkiemu, który w 988 r. ochrzcił Ruś Kijowską. Prezydent Ukrainy P. Poroszenko nazwał ten krok Kremla próbą hybrydowego przywłaszczania historii. Uroczysty charakter zdarzenia określał dzień wybrany na odsłonięcie pomnika, 4 listopada 2016 r., w Rosji obchodzony jako Dzień Jedności Narodowej, oraz udział osób zajmujących najwyższe stanowiska w państwie. Ten nowy artefakt rosyjskiej propagandy pokazuje, że imperialna interpretacja Rusi Kijowskiej jako „kolebki trzech bratnich narodów – rosyjskiego, ukraińskiego i białoruskiego" pozostaje w FR kanonicznym schematem

historycznym, zapominając przy tym, że Księstwo Moskiewskie powstało kilka wieków po śmierci księcia Włodzimierza.

W światowej naukowej myśli politycznej już dawno został sformułowany pogląd, opracowywany przez wielkich filozofów, pedagogów, pisarzy i lingwistów, wg którego każda kultura zaczyna się od znajomości języka ojczystego, że pogarda dla języka ojczystego jest formą depersonalizacji i samousunięcia, że po stosunku do języka ojczystego można ocenić moralny i intelektualny poziom danej osoby, że język jest żywym symbolem narodu, a upadek języka narodowego jest bezpośrednim dowodem upadku narodu i wielką stratą dla duchowego skarbca ludzkości. Dla tożsamości człowieka każda → p r z e m o c [t. 3] wobec jego języka oznacza ingerencję w jego własne „ja" i jego naród.

Niestety ukraińska kultura pod względem swojego statusu społecznego nie stała się w latach niepodległości kulturą suwerennego narodu – tzn. kulturą, która funkcjonuje na całym narodowym terytorium, w jakimś stopniu obejmuje całą ludność i opiera się na zrozumiałych dla większości kodach kulturowych oraz organicznie używanym w życiu codziennym języku. Kultura popularna pod wieloma względami jeszcze dziś funkcjonuje jako regionalna, prowincjonalna część kultury „ogólnoimperialnej", ogólnorosyjskiej – przy czym tak właśnie jest ona postrzegana nie tylko w metropolii, lecz również, w dużym stopniu, w samej Ukrainie. Jeśli zaś chodzi o ukraińską kulturę wysoką, to – pozbawiona całego bogactwa różnorodnych, przenikających się związków z kulturą masową – zamyka się ona w etnicznym getcie i funkcjonuje w istocie jako kultura mniejszości we własnym, suwerennym kraju, fatalnie zmarginalizowana przez obcy dyskurs i dominujące instytucje imperialno-kreolskie.

Wpływ ideologii rosyjskiej pogłębia polaryzację społeczeństwa ukraińskiego, wykorzystując językowe, kulturowe i ideologiczne preferencje miejscowej ludności. Ideologia rosyjska zapobiega powstawaniu ukraińskiej tożsamości, wykorzystując propagandę sztucznie stworzonych przez rosyjskich technologów politycznych wartości wschodnio-prawosławnej cywilizacji, a także uobecniając w społeczeństwie ukraińskim ideę „nierozerwalnej braterskiej jedności dwóch narodów" itd.

Osoby, którzy nienawidzą wszystkiego, co jest związane z Ukrainą i Ukraińcami, i których jest wiele we wszystkich dziedzinach życia

społecznego, szczególnie w mediach, zrozumiały, że kultury ukraińskiej nie uda się pośpiesznie zniszczyć czy szybko i całkowicie zastąpić surogatem, czymś, co ma niewiele wspólnego z tradycyjną kulturą. W związku z tym zaczęły się jawne ataki na niektórych znanych artystów, ludzi kultury, na całe twórcze zespoły, oskarżające swoich oponentów o „sowkowost'".

Sowkowost' to pejoratywna potoczna nazwa Związku Radzieckiego, człowieka radzieckiego, a także sowieckiej rzeczywistości w ogóle. Sowkowost' to zestaw negatywnych cech charakterystycznych dla narodu radzieckiego; to również fanatyzm, bliski religijności. Jest to choroba, w dodatku zaraźliwa. To rodzaj zbiorowego obrazu moralnie ułomnego, ale dumnego sowieckiego człowieka; to podejrzliwość, to chęć poniżenia kogoś i upokorzenie własne, niegrzeczność itp. Przejawia się tym, że człowiek dzieli ludzi na tych, którzy zajmują jakieś stanowisko, i tych, o których nie można tego powiedzieć; jednych wywyższa, a na innych patrzy z góry. Termin „sowok" ma to samo znaczenie, co termin *homo sovieticus* używany w literaturze naukowej, „sowok" częściej występuje w życiu codziennym oraz w języku potocznym, określenie pojawiło się w latach 70. XX w. W większości przypadków „sowok" to osoba, która ocenia innych ludzi, zjawiska i otaczający ją świat, posługując się niezmiennym systemem mitów zaczerpniętych z radzieckiej propagandy, nietolerancyjna, agresywna wobec odmiennych opinii, przekonana do własnych racji. Sowok jest kimś zacofanym, niekonstruktywnym, skostniałym ze swoimi uprzedzeniami i lękami. Najgorszą rzeczą, jaką przyniósł „sowok", jest kategoryczność, ujmowanie wszystkiego jako białe lub czarne. Sowokami początkowo nazywano sowieckich turystów za granicą, którzy kupowali rozmaite towary na pchlim targu, aby zwróciły im się pieniądze wydane na podróż, nie odwiedzając żadnych zabytków czy muzeów. Stopniowo termin „sowok" zaczął oznaczać wszystkie negatywne tendencje z czasów ZSRR (łącznie z samym krajem), inaczej to także „prawdziwy człowiek radziecki".

Taktyka ataków na artystów i ludzi kultury nie jest tak prosta, jak się wydaje. Jedną z jej technik jest konfrontacja fanów jednego stylu muzycznego przeciwko fanom innego, jednego pokolenia przeciwko innemu, tak aby w tej walce kultura ukraińska poniosła stałe i znaczące straty, a w tym samym czasie pustka została wypełniona nowymi projektami komercyjnymi.

Wszystkie te działania to przejawy tej samej →wojny hybrydowej [t. 4] – wojny o dusze i umysły. Kultura to cały kompleks, niekiedy doskonały, niekiedy kontrowersyjny, ale żywy organizm, który zmienia się wraz ze społeczeństwem. Wojna kultur odzwierciedla wojnę, która trwa na Wschodzie.

Kulturę oporu może stworzyć tylko →społeczeństwo obywatelskie [t. 4], któremu będą w tym pomagać profesjonalni artyści. Ci, którzy poparli Rewolucję Godności słowem i czynem, teraz są →żołnierzami [t. 4] i ochotnikami – i na froncie kulturalnym, i wojskowym. Wojna odsłania swoje prawdziwe oblicze. Klipy, wiersze, artykuły, wystawy fotograficzne, raporty, graffiti, performanse – nie są one finansowane przez państwo, nie finansują ich oligarchowie, ale pojawiają się każdego dnia i za każdym razem nowe. Artyści, którzy tworzą w imię zwycięstwa, potrzebni są wszędzie, a najpierw w społeczeństwie, które walczy przeciwko pladze putinizmu. Ta wojna wymaga, aby cała kultura ukraińska skoncentrowała się na zwycięstwie tak, aby zachować nie tylko dziedzictwo kulturowe, ale także własny honor i przyszłość.

Dziś w Ukrainie często przypominane są słowa brytyjskiego premiera W. Churchilla, który w czasie II wojny światowej nie pozwolił na zmniejszenie wydatków budżetu państwa na kulturę i edukację, zadając retoryczne pytanie: „Jeżeli nie ma kultury, to o co my do cholery walczymy?". Prędzej czy później Ukraina poruszy kwestię zachowania dziedzictwa kulturowego na poziomie priorytetowych sfer związanych z →bezpieczeństwem [t. 1], ponieważ kto nie dba o własną kulturę, ten zmuszony jest finansować obcą.

Dziś Rosja prowadzi przeciwko Ukrainie prawdziwą wojnę. Jej ostatecznym celem nie jest →aneksja [t. 1] części terytorium ukraińskiego ani pozbawienie Ukrainy cywilizacyjnego wyboru, a całkowite zniszczenie Ukraińców jako narodu. Nawet jeśli Kreml wycofa się z agresji zbrojnej, to będzie kontynuować agresję humanitarną, której celem jest zniszczenie państwa ukraińskiego „pokojowymi" środkami. Dlatego równolegle z obroną terytorialną państwa Ukraina musi przeciwdziałać →zagrożeniom [t. 4] →bezpieczeństwa narodowego [t. 1] w sferze humanitarnej. Są zagrożeniem strategicznym dla ukraińskiej państwowości. Nowoczesne ukraińskie państwo zrobiło zdecydowane kroki do

zapewnienia wyłącznego stosowania w obiegu urzędowym i oświacie jednego języka, nie ograniczając użycia w życiu społecznym zarówno dialektów, jak i języków mniejszości narodowych.

Podstawowym narzędziem tworzenia kultury narodowej wg Jana Pawła II jest język: za jego pomocą człowiek wypowiada prawdę o świecie i o sobie samym, pozwala innym mieć udział w owocach swoich poszukiwań w różnych dziedzinach. Komunikuje się z innymi, a to służy wymianie myśli, głębszemu poznaniu prawdy, jak również pogłębianiu i gruntowaniu własnej tożsamości. Dla Jana Pawła II naród jest ściśle związany z kulturą, naród jest wspólnotą kultury. Ci, którzy uważają, że można gardzić kulturą całego narodu, poniżają sami siebie. Kultura jest tym, co zostało przekazane z mlekiem matki, tym, co znane z jej kołysanek, bajek, opowieści i legend o swojej ziemi. W przemówieniu w → UNESCO [t. 4] 2 czerwca 1980 r. papież mówił: „Naród to wspólnota ludzi, których łączą różne spoiwa, ale nade wszystko właśnie kultura. Naród istnieje «z kultury» i «dla kultury»". Każdy naród żyje dziełami swojej kultury.

Z punktu widzenia Kremla utrzymywanie dominującej pozycji rosyjskiego języka i kultury w Ukrainie jest motywowane pragmatyką zapewnienia sobie najpotężniejszej siły oddziaływania do utrzymania Ukrainy w orbicie wpływów Rosji. Właśnie poprzez językowo-kulturowe manipulacje w stosunku do ukraińskich grup ludności Kreml jest w stanie kontrolować zachowania aktorów politycznych, którzy dążą do uzyskania poparcia tych wyborców. Uświadomienie tego imperatywu określa politykę kulturalną Kremla wobec Ukrainy – literatura, muzyka popularna, film, prasa i wreszcie religia są wykorzystywane do osiągnięcia celów taktycznych i strategicznych oraz do kontroli elit ukraińskich. Marginalizacja ukraińskiej literatury, muzyki, prasy, cerkwi jest pierwszym warunkiem zachowania hegemonii kulturowej – a tym samym i politycznej – Rosji nad Ukrainą. Tam, gdzie naród nie ma własnej kulturowej i informacyjnej przestrzeni, tworzą się warunki dogodne dla najeźdźców. Jednak głównym czynnikiem jest, oczywiście, język ojczysty. W Ukrainie ten czynnik jest jakoś pomijany przez propagandę „rosyjskojęzycznego patriotyzmu" i nikt nie podkreśla tego, że okupant nie zajął północnej części obwodu ługańskiego, ponieważ są tam ukraińskojęzyczne wioski. Najpotężniejszą bronią Ukraińców jest ich język, który jest tarczą, najwyższym murem

granicznym, którego we współczesnym świecie nie może pokonać żaden agresor.

Dziś zarówno władze, jak i społeczeństwo obywatelskie Ukrainy zgadzają się z tym, że kultura jest drugim frontem walki, na którym operuje Rosja. Należy być silnym na tym froncie, czasami jest to nawet ważniejsze niż zwycięstwa dyplomatyczne lub cyniczna rywalizacja polityczna. Nie tylko w kręgu artystów, ale także na poziomie decyzji politycznych panuje zgoda co do tego, że kultura jest głównym składnikiem prezentacji państwa na arenie międzynarodowej.

Ukraińcy ze swoją Rewolucją Godności obrazili specyficzną kolonialną mentalność Rosjan – pragnienie miłości i wdzięczności ze strony podbitych narodów. Rosjanie na ziemiach etnicznie „obcych" nie zawsze mogli zachowywać się jako kolonizatorzy i asymilatorzy, a próbowali przekonać dane narody, że tylko Rosja może przynieść postęp, cywilizację i kulturę. Najwięcej przez taką „kulturę" kolonizatorów ucierpiał naród ukraiński, ponieważ Rosja postrzega wysoki poziom ukraińskiej świadomości narodowej jako szowinistyczną rusofobię. Dla Rosji normą jest niemal całkowity brak świadomości narodowej, oczywiście, u innych narodów. Rosjanie mają tendencję do przypisywania innym narodom wrogości i niechęci do siebie, którą oni sami odczuwają do świadomych swojej etnicznej odrębności narodów – w ten sposób słowa „my ich nienawidzimy" przemieniają się w wygodniejsze i korzystne psychologicznie „oni nas nienawidzą".

Polityczna i humanitarna agresja *russkiego mira*, która doprowadziła do konfliktu zbrojnego, to problem nie tylko Ukrainy, ma ona ogólnoeuropejski charakter. Rosja celowo niszczy polityczne i prawne zasady europejskiej przestrzeni bezpieczeństwa. Obecnie Ukraina przeżywa tragiczne konsekwencje → i n w a z j i *russkiego mira*. Jutro, jeśli nie zostanie zatrzymany, w podobnej sytuacji znajdą się inne państwa Europy Wschodniej i Środkowej. Dlatego humanitarna i militarna ekspansja *russkiego mira* jest problemem ogólnoeuropejskim, który powinien zostać rozwiązany poprzez wspólne wysiłki.

Wydarzenia ostatnich 5 lat udowodniły, że silny opór patriotycznie nastawionego ukraińskiego społeczeństwa obywatelskiego podczas agresji okazał się prawdziwym zaskoczeniem dla Moskwy i odegrał ważną rolę

w kluczowych aspektach konfliktu. Podczas tych dramatycznych wydarzeń można było przekonać się, że walka o wartości kulturowe, tożsamość, interpretację historii, zachowanie tradycji, otwartość na inne kultury, o swobodny i równoprawny dialog czasem kosztują ludzkie życie.

Olga Wasiuta

H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019; Jan Paweł II, *Pamięć i tożsamość. Rozmowy na przełomie tysiącleci*, Wydawnictwo Znak, Kraków 2005; T.A. Olszański, *Problem językowy na Ukrainie. Próba nowego spojrzenia*, „Prace OSW" 2012, nr 40; M. Riabczuk, *Ukraińska kultura po komunizmie: między postkolonialnym wyzwoleniem a neokolonialnym zniewoleniem*, [w:] *Raport o stanie kultury i NGO w Ukrainie*, Wydawnictwo Episteme, Lublin 2012; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017; *Гібридна війна: in verbo et in praxi*, Р.О. Додонов (ред.), Донецький національний університет імені Василя Стуса, ТОВ «НіланЛТД», Вінниця 2017; Ю. Шевельов, *З історії незакінченої війни*, Видавничий дім «Києво-Могилянська Академія», Київ 2009; І.М. Дзюба, *Інтернаціоналізм чи русифікація*, Києво-Могилянська Академія, Київ 2005; Л.Н. Гумилев, *От Руси до России. Поиски вымышленного царства*, Издательство „Вече", Москва 2009; П. Полянський, *Інформаційна війна в освіті – це боротьба за молодь, її свідомість, мислення*, 17.03.2015, PedPresa.ua (dostęp 19.10.2018); П. Полянський, *Освіта як об'єкт інформаційної війни Росії проти України і як ресурс протидії такій війні*, 23.03.2015, Maidan.org.ua (dostęp 19.10.2018); П. Полянський, *Інформаційна війна в освіті – це боротьба за молодь, її свідомість, мислення*, old.mon.gov.ua (dostęp 19.10.2018); Г. Пагутяк, *Війна проти культури, культура проти війни. Культуру спротиву може породити лише громадянське суспільство і допомагатимуть йому в цьому професійні митці*, Zaxid.net (dostęp 30.11.2018).

EDUKACJA OBYWATELSKA – jako zjawisko społeczne jest czymś nowym w polskiej rzeczywistości. U podstaw tego procesu stoi niezawisłość i → suwerenność państwa [t. 4], a co za tym idzie wolność jednostki w społeczeństwie. Procesy modernizacji społecznej i transformacji ustrojowej, które dokonały się w Polsce w ciągu ostatnich 20 lat, zmieniły społeczeństwo, gospodarkę i państwo jako takie. Fakt, że przez prawie 60 lat Polska była krajem podporządkowanym interesom władzy totalitarnej,

spowodował, że pojedynczy obywatel nie miał możliwości wywierania wpływu na rzeczywistość, w której żył. Nieliczne przykłady stowarzyszeń, kółek czy lokalnych samorządów potwierdzały tę regułę, bowiem każda taka forma była ściśle kontrolowana przez władzę lokalną lub centralną. Ponad pół wieku braku suwerenności w polskiej rzeczywistości stwarza obecnie trudne warunki do budowania nowych struktur. W 1989 r. społeczeństwo polskie nie było gotowe do przejęcia nowych obowiązków, ponieważ zbyt długo było uzależnione od centralnie wydawanych decyzji. Przez ostatnie 20 lat starało się ono nauczyć, jak być →społeczeństwem obywatelskim [t. 4]. W tym procesie miały udział zarówno unowocześnione struktury administracji państwowej, jak i inne instytucje, choćby fundacje. Dużą rolę odegrały także wielostronne kontakty samorządowe na różnych szczeblach w ramach Unii Europejskiej. Chcąc szerzej rozważyć temat edukacji obywatelskiej w Polsce po 1989 r., należy zwrócić uwagę na kilka zasadniczych faktów, które miały wpływ na obecny stan społeczeństwa obywatelskiego, jeśli można o takim mówić w Polsce.

Obywatelskość może oznaczać bycie dobrym obywatelem. Pojęcie to bywa definiowane w różnorodny sposób, w zależności od tradycji i myśli filozoficznej autorów. Immanentnym elementem struktury państwowej jest uświadomiony obywatel, który zna swoje prawa, obowiązki, a także posiada wiedzę o tym, że państwo winno stwarzać warunki dla jego lepszej egzystencji, nie tylko w sferze zagwarantowania podstawowych motywacji do współudziału w społeczeństwie, ale także troski o jego potrzeby. Pojęcie obywatelstwa skupia się na sposobach, poprzez które państwo oddziałuje na jednostki, i nie dotyczy kwestii, w jaki sposób samo państwo kształtuje własny projekt polityczny. Obywatel ma świadomość, że jest uczestnikiem wszystkich procesów w państwie, ma prawo o nich decydować. Definicje obywatelskości podkreślają postawę jednostki wobec społeczności oraz konieczność uściślenia jej praw. Obywatelskość można określić jako przywiązanie do całości społeczeństwa, objawiające się decyzjami i działaniami zmierzającymi do ochrony i pomnażania dobra całego społeczeństwa o zbiorowej samoświadomości, która ogranicza i kształtuje działania jednostek. Można mówić o pewnym poziomie doskonałości cech osobowościowych jednostki, odzwierciedlonych w jej postawie moralno-politycznej, wyrażającej się w zamiarze odgrywania roli

aktywnego, odpowiedzialnego, w pełni kooperującego przy tworzeniu dóbr publicznych podmiotu. Przy dookreślaniu obywatelskiej postawy mówi się o empatii, altruizmie, a także zakreśla ramy prospołecznego zachowania jednostki. W postawie obywatelskiej dostrzega się także zdolności do ponoszenia trudów w imię wspólnoty, troskę o wspólne sprawy. Rozważając obywatelskość, będącą ważnym zjawiskiem w społecznościach, można ją traktować jako wiarę w istotność pewnych wartości, takich jak choćby braterstwo, solidarność, akceptacja równości praw, zaufanie, respektowanie dobra wspólnego, współpraca, przestrzeganie wspólnie ustalonych reguł, podmiotowe traktowanie współobywateli. Uściślając zakres pojęcia obywatelskości, warto przytoczyć jeszcze inne stanowiska definiujące szeroki, wieloaspektowy obszar tego pojęcia.

Społeczeństwo obywatelskie to przestrzeń pomiędzy rodziną, państwem a rynkiem, w której działają oddolne organizacje społeczne. W tej przestrzeni obywatele prowadzą debatę, w efekcie której wypracowywane są rozwiązania społeczne dla dobra wspólnego. Tocząc dalej rozważania w tej materii, zauważa się, że społeczeństwo obywatelskie jest autonomicznym bytem zdolnym równoważyć władzę państwową, pozwalając jednocześnie społeczeństwu przejawiać swoje interesy i potrzeby, jednoczyć je wobec spraw wspólnej troski oraz wpływać na decyzje publiczne. Aby społeczeństwo obywatelskie mogło odgrywać tę rolę, musi posiadać wewnętrzne siły żywotne, własną strukturę, utkaną w sieć wzajemnych i niekontrolowanych przez państwo i jego aparat powiązań między ludźmi i grupami społecznymi. Precyzując, społeczeństwo obywatelskie to ogół niepaństwowych instytucji, organizacji i stowarzyszeń cywilnych działających w sferze publicznej. Są to struktury względnie autonomiczne wobec państwa, powstające oddolnie i charakteryzujące się na ogół dobrowolnym uczestnictwem ich członków.

Społeczeństwo obywatelskie to idea instytucjonalnego i ideologicznego pluralizmu, który zapobiega ustanowieniu monopolu władzy i prawdy i stanowi przeciwwagę dla tych instytucji centralnych, które, chociaż są konieczne, mogą w innym przypadku zdobyć monopol. Patrząc na dzieje rozwoju państwowości w różnych krajach, można zasugerować tezę, że tworzenie społeczeństwa obywatelskiego jest możliwe jedynie w warunkach państw demokratycznych. Pojęcie wolności w demokracji polega na

uczestnictwie w kierowaniu państwem. Nowożytna demokracja opiera się na liberalnym rozumieniu wolności, wyznaczającym zakres swobód indywidualnych określających działania jednostek w sferze nieobjętej działaniem państwa, czyli w tzw. społeczeństwie obywatelskim, oraz łączących się z tym systemem gwarancjach państwa, umożliwiających respektowanie tych swobód. Musi temu jednak towarzyszyć również społeczna refleksja o demokracji i państwie, dostrzegająca fakt, że demokratyczny ustrój jest zawsze zagrożony przez różnorodne siły, choćby przez odradzające się siły nacjonalistyczne, totalitarne, skrajnie prawicowe. Demokracja bowiem nie jest raz na zawsze danym dobrem, a wymaga ciągle nowej witalności w postaci ludzkiej woli uczestniczenia w jej rozwoju i doskonaleniu. Demokracja nie jest nigdy dziełem jednego aktu i raz na zawsze dokonanym.

Budowanie demokracji jest procesem długotrwałym, jest wynikiem wysiłków w równej mierze społecznych, co jednostkowych. Demokracja jest zatem wynikiem wspólnie podejmowanych działań, ale jednak w ciągłym procesie tworzenia, który nigdy nie zostanie do końca zrealizowany. Społeczeństwo, chcąc być świadomym i obywatelskim, musi dokonywać ciągłej budowy demokracji, równocześnie dbając o jej unowocześnianie. Przez to pojęcie należy rozumieć nieprzerwany proces wytwarzania w obywatelu poczucia odpowiedzialności za trud utrzymania *status quo* demokratycznego państwa. Takie procesy, można założyć, nie dotyczyłyby państw, w których demokracja trwa od dziesięcioleci. Dotyczy to nowych demokracji, państw, które po okresie transformacji i rozpadzie sowieckiego imperium uczą się nowych zasad współżycia w demokratycznych strukturach. Społeczeństwo obywatelskie jest szczególnym rodzajem społeczeństwa. W dużym stopniu cechuje je podzielna, zbiorowa samoświadomość. Pełni ona ważną funkcję, wchodzi w publiczną sferę, jest dziełem prywatnych i rządowych instytucji. Zbiorową samoświadomość całego społeczeństwa charakteryzuje zainteresowanie wspólnym dobrem. Uczestnictwo jednostek w zbiorowej samoświadomości pociąga za sobą światopogląd nazywany obywatelskością. Jest to postawa jednostki, która w sposób intencjonalny pozwala na własne uczestnictwo w osobowości zbiorowej, modeluje jej decyzje i działanie, afirmuje zobowiązania do pracy na rzecz wspólnego dobra, nawet gdy jest to sprzeczne z jej interesami. Za obywatelskie można uznać społeczeństwo, w którym taka postawa staje się powszechnym wzorem.

Najważniejszym warunkiem istnienia społeczeństwa obywatelskiego jest to, aby wszyscy jego członkowie zdawali sobie sprawę z przynależności do tego społeczeństwa jako całości. Społeczeństwo obywatelskie to społeczeństwo pluralistyczne, w którym autonomia konstruujących ją jednostek, zbiorowości i warstw ograniczana jest za sprawą uznania przez poszczególnych obywateli ich zobowiązań wobec społeczeństwa jako całości, wobec właściwych mu centralnych organów i praw. Proces tworzenia się państwowych struktur, w których obywatel miałby status w pełni odpowiedzialnego i w pełni współpracującego w społeczeństwie, tworzył się przez lata w społeczeństwach europejskich i nie tylko. Przemiana społeczeństw napotykała bariery Starej Europy, a w USA proces ten przebiegał łatwiej, demokracja USA już w XIX w. odwoływała się do tradycji Jeffersona, do idei równości praw i do nieufności wobec wszelkich przywilejów, monopoli, hierarchii społecznych. W przypadku krajów, które przeszły transformację w latach 90. XX w., po długotrwałym okresie rządów totalitarnych, świadomość obywatelska członków społeczeństw jeszcze się kształtuje.

Kształtowanie się społeczeństw obywatelskich, które budują się na podwalinach formujących się praw obywatelskich, przebiega w 3 etapach: kształtowania się wolności obywatela i przysługujących mu praw osobistych, poprzez uczestniczenie w wolności i nabywaniu praw politycznych, aż do rozbudowania systemu praw socjalnych i ekonomicznych. Mówiąc o edukacji obywatelskiej i społeczeństwie świadomie obywatelskim, należy prześledzić samą figurę obywatela jako takiego w ciągu wieków i w świetle obowiązujących filozofii, doktryn i systemów politycznych. Demokratyczne państwo, ustrój, który zakłada wolność jednostki, daje jej prawo głosu i pozwala na samostanowienie o swym losie, zatem jest strukturą państwową pozwalającą na złożony proces budowania się postawy obywatelskiej. Społeczeństwo obywatelskie będzie się rozwijać dobrze wtedy, gdy na znaczeniu będzie zyskiwać jednostka. To właśnie wtedy w społeczeństwach zachodnich idea społeczeństwa obywatelskiego została rozwinięta i w pewnym stopniu zrealizowana.

Uczenie się obywatelskości to proces rozwoju jednostki w kierunku częściowego odrzucenia indywidualistycznych zasad w imię dobrze pojętej wspólnoty. Społeczeństwo obywatelskie jest przecież syntezą interesu

indywidualnego i interesu publicznego, zatem jest to społeczeństwo, w którym jednostka współtworzy dobrobyt powszechny nie tylko poprzez płacenie podatków, ale także oddając część swojego czasu, energii i sił wyobraźni. Ważna jest zatem rola procesu edukacji w kształceniu postaw obywateli. Najogólniej rzecz biorąc, o społeczeństwie obywatelskim można mówić wtedy, gdy jest to obszar działalności publicznej nieobjętej kontrolą państwa. Społeczeństwo obywatelskie jest jednym z kluczowych pojęć politologii oraz nauk socjologicznych.

Łukasz Czekaj

Ł. Czekaj, *Edukacja obywatelska*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka. R. Kopeć. (red.), Wydawnictwo Libron, Kraków 2018; K. Dziubka, *Teoria demokratycznej obywatelskości – zarys problemu*, [w:] *Społeczeństwo obywatelskie*, W. Bojkała, K. Dziubka (red.), Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2001; H. Hovenberg, T. Maliszewski, W. Wojtowicz, J. Żerko, *Demokratyzacja oświaty. Materiał na konferencję w ramach Projektu „S/z/koldem" (2 grudnia 1994 r.)*, Linköping 1994; J. Jedlicki, *Jakiej cywilizacji Polacy potrzebują. Studia z dziejów idei i wyobraźni XIX wieku*, WAB, CiS, Warszawa 2002; A. Koźminski, P. Sztompka, *Rozmowa o wielkiej przemianie*, Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego w Warszawie, Warszawa 2004; W. Osiatyński, *Rzeczpospolita obywateli*, Rosner i Wspólnicy, Warszawa 2004; E. Shils, *Co to jest społeczeństwo obywatelskie*, [w:] *Europa i społeczeństwo obywatelskie: rozmowy w Castel Gandolfo*, K. Michalski (red.), Wydawnictwo Znak, Kraków–Warszawa 1994; G. Ulicka, *Demokracje zachodnie: zasady, wartości, wizje*, PWN, Warszawa 1992; H. Wit, *Społeczeństwo obywatelskie*, Wydawnictwo IFiS PAN, Warszawa 2008.

E-DŻIHAD (cyberdżihad) – prowadzenie → d ż i h a d u z wykorzystaniem narzędzi informatycznych. Jest to forma walki informacyjnej (ang. *information warfare*), obejmuje zatem przestępstwa finansowe, działania wywiadowcze, → s t r a t e g i e [t. 4] manipulacyjne mass mediów czy nawet ataki na infrastrukturę informatyczną przeciwnika. Obserwatorium Językowe Uniwersytetu Warszawskiego zarejestrowało słowo „cyberdżihad" w 2016 r. W nauce spotykamy też takie określenie jak *inter-fada*.

Historię korzystania z internetu przez dżihadystów możemy podzielić na 3 zasadnicze okresy:

- Do ataku na World Trade Center (11 września 2001 r.). Pojawiały się pewne próby wykorzystania tego narzędzia, przełomem było założenie strony Azzam.com – nazwa pochodziła od nazwiska głównego ideologa dżihadu lat 80. XX w. Abdullaha Azzama. Strona została założona w Wielkiej Brytanii, poświęcona była głównie walkom w Czeczenii. W 1998 r. powstała strona Alneda.com, pisana była po arabsku, a jej założycielem był członek Al-Kaidy Yusuf al-Uyairi (Yusuf bin Salih bin Fahd al-Ayeri).
- Od 2001 r. do powstania → Państwa Islamskiego [t. 3] (ISIS). Charakterystyczne dla tego okresu było pojawianie się zapisów wideo czy przejście od stron internetowych do przestrzeni → mediów społecznościowych [t. 3]. To znacznie utrudniło kontrolę i zwalczanie treści dżihadystów za pomocą tradycyjnych środków. W tym czasie powstała organizacja Islamski Globalny Front Medialny (Global Islamic Media Front, GIMF). To ona zaczęła w sposób systematyczny pracować nad → propagandą [t. 3] w internecie. Jeszcze istotniejszy był portal As-Sahab (arab.: Chmura). Powstał najprawdopodobniej już w 2001 r. Jego twórcy byli odpowiedzialni za kolportaż filmów, w tym tych z Usamą ibn Ladinem (Osamą bin Ladenem).
- Od powstania ISIS. Dzięki własnym dochodom, własnemu terytorium, umiejętnemu wykorzystaniu diaspory z jej znajomością języków, kultury i zdobyczy technologicznych udało się uzyskać niespotykany stopień rozwoju. Ponadto rozwój technologii i znaczny spadek kosztów, internet mobilny, nowoczesne smartfony i kamery nagrywające w wysokiej rozdzielczości – wszystko to znacznie ułatwiało działalność.

Do najbardziej znanych ataków cyberdżihadystów możemy zaliczyć przejęcie kontroli nad kontem CENTCOM (jednego z dowództw USA) na Twitterze przez grupę CyberKalifat, która swoje działania sama nazwała CyberDżihadem. Ta grupa podejrzana jest też o atak na stronę francuskiej stacji telewizyjnej TV 5 Monde. Inną znaną grupą są The Desert Falcons, przeprowadzała ona ataki głównie z terenu Jordanii, Palestyny, Izraela i Egiptu. Używała oprogramowania typu malware, infekowano komputery z systemem Windows oraz urządzenia wykorzystujące system

Android. Wykorzystywano również fałszywe strony internetowe, konta w mediach społecznościowych itp. (→ p h i s h i n g [t. 3]). Od 2014 r. notowane były ataki grupy Rocket Kitten, w jej skład wchodzili głównie Irańczycy. Odpowiedzialni byli za serię ataków na infrastrukturę informatyczną w Niemczech czy Izraelu.

Cyberdżihadyści tworzą też oprogramowania służące walce. Przykładem może być: „Elektroniczny Dżihad – wersja 2.0" wykorzystywany do przeprowadzania ataków typu blokada usługi (ang. *Denial of Service*, DoS). GIMF przygotował oprogramowanie szyfrujące korespondencję o nazwie Sekrety Mudżahedinów (Mujahedeen Secrets, Asrar al-Mujahedeen). Wydawane są też poradniki i materiały szkoleniowe, z dostępnych tytułów wymienić można czasopismo „Technical Mujahid" ukazujące się co 2 miesiące, a wydawane przez Abu al-Mothannę al-Nadżdiego.

Dobrym przykładem wykorzystywania internetu do szkolenia są materiały w ten sposób publikowane. Taką rolę odgrywał GIMF. Na jego stronach można było znaleźć podręczniki z zakresu taktyki wojskowej czy nawet instrukcje przygotowywania materiałów wybuchowych. Ciekawym przykładem są też materiały rekrutacyjne dostępne online. Państwo Islamskie korzysta z przygotowanego wcześniej przez Al-Kaidę specjalnego programu pozyskiwania zwolenników. Autorem kursu jest Abu Amru Al Qa'idi. Jest to rozpisany na poszczególne elementy proces, w którym zastosowano nawet formularze ewaluacyjne dla oceny stopnia zaawansowania zmanipulowania aspiranta. Jednym z popularniejszych źródeł jest seria „Jihad Recollections". Cztery pierwsze internetowe magazyny wyprodukował Amerykanin Samir Khan (od kwietnia do września 2009 r.) dla Al-Kaidy Półwyspu Arabskiego (Al-Qaeda in the Arabian Peninsula, AQAP), pozostałe wydał Gaidi M'Taani z Asz-Szabab (Ruch Młodzieży Mudżahedińskiej), wszystkie ukazały się nakładem „Inspire". Dwa pierwsze numery były wydane w języku angielskim.

Najbardziej znaną serią podręczników jest *Open Source Jihad*, seria artykułów wydanych w „Inspire". Kompilacja zawiera instrukcje operacyjne dotyczące różnorodnych metod ataku, w tym zamachów samochodowych, zabójstw politycznych i ataków samochodowych. Przedstawia się także podstawowe protokoły → c y b e r b e z p i e c z e ń s t w a [t. 1], w tym

wykorzystanie zaszyfrowanych za pomocą Sekretów Mudżahedinów platform komunikacyjnych.

O *Open Source Jihad* zrobiło się również głośno po artykule *Zrób bombę w kuchni swojej mamy* (oryg. ang. *Make a Bomb in the Kitchen of Your Mom*), który zawierał instrukcję budowy niskobudżetowego improwizowanego ładunku wybuchowego (ang. *Improvised Explosive Device*, IED). Niemal dekadę od pierwszej publikacji w 2010 r. podręczniki nadal utrzymują znaczenie wśród zachodnich dżihadystów. Zamachy bombowe podczas maratonu w Bostonie w 2013 r. należą do najbardziej znanych, w których wykorzystano wiedzę z serii.

Publikacje cyberdżihadystów są dostępne głównie dzięki wykorzystaniu tzw. → d a r k n e t u, czyli sieci o ograniczonym dostępie. Innym narzędziem wykorzystywanym jest komunikator Telegram. Duża część anglojęzycznych podręczników instruktażowych rozpowszechnianych przez zwolenników Państwa Islamskiego w Telegramie to kopie instrukcji opracowanych przez Al-Kaidę i inne grupy dżihadystyczne. Zdecydowana większość jest jednak arabskojęzyczna.

Oczywiście taka działalność spotyka się z odpowiedzią. W 2007 r. internauci w wyniku swych działań zablokowali szereg stron internetowych mudżahedinów. 10 września 2007 r. udało się zablokować malezyjskie serwery, które miały posłużyć Al-Kaidzie do ataków cybernetycznych w rocznicę zamachów w USA. Służby wywiadowcze coraz dokładniej sprawdzają publikowane w sieci treści, prowadzą też działania ofensywne, jak choćby pułapki typu honeypot, specjalnie preparowane strony czy posty, dzięki którym udaje się „zwabić" radykałów. Dokonywano też blokad serwerów czy kont w mediach społecznościowych, np. Twitter w 2016 r. zlikwidował blisko 125 tys. kont. Pojawiły się projekty monitorujące e-dżihad i propagujące dobre praktyki, takie jak Clean IT Project.

Przemysław Mazur

O. Adaki, *AQAP Publishes Biography of American Jihadist Samir Khan*, 25.11.2014, LongWarJournal.org (dostęp 1.12.2019); I. Awan, *Cyber-Extremism: Isis and the Power of Social Media*, „Society" 2017, vol. 54; J.M. Berger, J. Morgan, *The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter*, „The Brookings Project on U.S. Relations with the Islamic World Analysis Paper"

2015, no. 20; J. Brachman: *Global Jihadism: Theory and Practice*, Routledge, New York–London 2009; *Jihadismus und Internet: Eine deutsche Perspektive*, G. Steinberg (hrsg.), SWP, Berlin 2012; A.F. Lemieux, J.M. Brachman, J. Levitt, J. Wood, *Inspire Magazine: A Critical Analysis of Its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model*, „Terrorism and Political Violence" 2014, no. 26 (2); P. Mazur, *E-dżihad,* [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *E-dżihad, soft power radykalizmu islamskiego*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN, Kraków 2017; P. Mazur, O. Wasiuta, S. Wasiuta, *Państwo Islamskie ISIS: nowa twarz ekstremizmu*, Difin, Warszawa 2018; H. Sarat-St. Peter, *„Make a Bomb in the Kitchen of Your Mom". Jihadist Tactical Technical Communication and the Everyday Practice of Cooking*, „Technical Communication Quarterly" 2017, no. 26 (1); J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad: Cyberspace is the New Great Equalizer*, Institute for Critical Infrastructure Technology, 2016; A. Wejkszner, *Państwo Islamskie. Narodziny nowego Kalifatu?*, Difin, Warszawa 2016; C. Winter, *Media Jihad: The Islamic State's Doctrine for Information Warfare*, ICSR King's College London, London 2017.

EFEKTY ODDZIAŁYWANIA MEDIÓW – grupa zjawisk istotnych z perspektywy → b e z p i e c z e ń s t w a [t. 1] jednostek i społeczeństw z uwagi na stale wzrastającą rolę mediów. Środki masowego przekazu mogą mieć szerokie spektrum oddziaływania – na wiedzę, postawy, emocje, zachowania społeczne, reputację osób prezentowanych w mediach. Mogą to być konsekwencje korzystania z mediów, ale także wynik interakcji z ludźmi, którzy z nich korzystali. Wyjaśnienia problemu są zwykle oparte na 2 teoriach. Podejścia oparte na teorii uczenia się dotyczą prawidłowego odtwarzania → i n f o r m a c j i, dlatego rozbieżności między przekonaniami a informacjami dostarczanymi przez media uważa się za deficyty uczenia się, które można również interpretować jako brak efektów medialnych. Podejścia teorii poznawczej dotyczą przetwarzania informacji z doniesień medialnych. Przekonania i opinie nie są traktowane jako kopie ich medialnych prezentacji, ale wskazują na sposób przetwarzania informacji.

Relacje bieżące w mediach mają wpływ na publiczną ocenę znaczenia problemów społecznych i pilność ich rozwiązania. Porównanie wszystkich zagadnień znajdujących się w agendzie mediów z agendą zainteresowań ich odbiorców w krótkim okresie, a także porównanie rozwoju relacji

medialnych w pojedynczych kwestiach z rozwojem przekonań populacji w dłuższym okresie mogą wskazywać na efekt oddziaływania mediów. Koncepcja *agenda setting* po raz pierwszy została przetestowana empirycznie w wyborach prezydenckich w USA w 1968 r. przez profesorów dziennikarstwa z Karoliny Północnej, M. McCombsa i D. Shawa. Podejście to początkowo koncentrowało się na zdolności środków masowego przekazu do informowania → o p i n i i p u b l i c z n e j [t. 3], „o czym" mamy myśleć, a nie o tym, „co" mamy myśleć. Było to zerwanie z poprzednimi badaniami efektów medialnych, które koncentrowało się na tym, co ludzie myślą, ich opiniach i postawach oraz na zachowaniach takich jak głosowanie. Rangę i znaczenie tematów prezentowanych w mediach wyznacza częstotliwość ich występowania. Wielokrotne mówienie w mediach o → z a g r o ż e n i a c h [t. 4] będzie potęgowało poczucie, że jest to problem palący i ważny. Podobnie rzecz ma się z odczuciami związanymi z zagrożeniem wybuchem → w o j n y [t. 4] czy prawdopodobieństwem wystąpienia zamachu terrorystycznego. Niezależnie od rzeczywistych zamiarów terrorystów i działań służb antyterrorystycznych częstotliwość podawania informacji w mediach o zamachach terrorystycznych przekłada się na poczucie bezpieczeństwa. Podkreślić należy, że dużą rolę poza częstotliwością odgrywa także kolejność podawania informacji, która tworzy odpowiedni porządek w umysłach odbiorców, hierarchizując tematy od najważniejszych przez mniej istotne aż po błahe. Wiadomości rozpoczynające główne wydania serwisów informacyjnych, tematy z okładek dzienników czy problemy najbardziej rozbudowanych artykułów w tygodnikach będą uważane za ważniejsze od tych informacji, które podano na końcu serwisu lub o których napisano jedną kolumnę w gazecie czy czasopiśmie. Zgodnie z koncepcją *agenda setting* media tworzą w naszych umysłach swoistą mapę rzeczy ważnych i mniej ważnych, co dodatkowo utrwalane jest w świadomości osób stale korzystających z mediów.

Media mogą także wpływać na przekonania odbiorców i ich zmiany, co tłumaczy m.in. koncepcja spirali milczenia, zaproponowana przez E. Noelle-Neumann, niemiecką badaczkę opinii publicznej i profesor badań nad komunikacją. Termin „spirala milczenia" pojawił się w jej pracach, gdy próbowała wyjaśnić sondaże opinii publicznej, dowodząc, że nie można przewidzieć wyników wyborów w Niemczech Zachodnich.

Model spirali milczenia pierwotnie służył jako wyjaśnienie interakcji między opinią publiczną a zachowaniem wyborców. U podstaw teorii leżało założenie, że potencjalna presja grupowa przekazywana za pośrednictwem środków masowego przekazu (zwykle w postaci danych opinii publicznej, ilustrujących opinię większości) zmusza zwolenników niepopularnych poglądów (o kandydatach politycznych, wierzeniach lub ideach) do milczenia, a nawet zmiany ich opinii. Po uruchomieniu efekt się wzmacnia. W tym spiralnym procesie rośnie poparcie dla powszechnego przekonania, a pogląd mniejszości jest na każdym kroku coraz bardziej wyciszany. Środki masowego przekazu jako źródło informacji o popularnych przekonaniach odgrywają kluczową rolę w tym procesie. Pojawienie się internetu i → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3], przy jednoczesnym zapewnieniu nowych kanałów i środków komunikacji masowej, może potencjalnie zmienić naturę mechanizmów spirali milczenia.

Początki zainteresowania zmianami przekonań pojawiły się w związku z zainteresowaniem wynikami wyborów federalnych w Niemczech Zachodnich w 1965 i 1972 r. Trudności z trafnością prognozowania wyników wyborów zaintrygowały Noelle-Neumann i innych uczonych i analityków. Zarówno w 1965 r., jak i w 1972 r. 2 główne partie walczyły, aby zdobyć większość w Bundestagu. Zamiary głosowania w niemieckich okręgach wyborczych pozostawały w dużej mierze niezmienione do ostatniej chwili, gdy pojawiły się informacje o „oczekiwanym zwycięzcy" i wówczas popularność partii wskazywanej jako mająca większe szanse na wygraną zaczęła radykalnie rosnąć. Jak pisała Noelle-Neumann, pod naciskiem opinii publicznej wielu wyborców zmieniło zdanie.

Założenia koncepcji spirali milczenia można przedstawić w formie 5 głównych hipotez:

- Zagrożenie izolacją – wynika z faktu, że w społecznej zbiorowości spójność musi być stale zapewniona przez wystarczający poziom porozumienia co do wartości i celów. Aby zagwarantować to porozumienie, społeczeństwo grozi izolacją osób, które naruszają konsensus.
- Strach przed izolacją – kształtowanie się indywidualnej opinii i działania charakteryzuje strach jednostek przed „izolatami społecznymi". Założenie to pochodzi z eksperymentalnych badań zgodności.

Zgodność społeczna może być albo informacyjnym wpływem społecznym, odzwierciedlonym w jednostkach akceptujących informacje od innych jako dowody na rzeczywistość, albo normatywnym wpływem społecznym, w którym jednostki dostosowują się do oczekiwań innych. Noelle-Neumann używa tych ostatnich do wyjaśnienia i dostarczenia dowodów na przypuszczalny wpływ lęku przed izolacją na chęć wypowiadania się. Odnosi się do eksperymentów, w których badani zgadzali się z większością w wykonywaniu stosunkowo prostych zadań, takich jak wybranie linii pasującej do innej długością i wybranie dłuższego z 2 tonów akustycznych.

- Sens quasi-statystyczny – w wyniku lęku przed izolacją jednostki stale monitorują swoje otoczenie, aby sprawdzić dystrybucję opinii, a także przyszły trend opinii. Takie monitorowanie może obejmować odbiór treści medialnych pozostających w związku z danym problemem, bezpośrednią obserwację własnego otoczenia lub interpersonalną dyskusję. Sens quasi-statystyczny jest prawdopodobnie najszerzej interpretowanym pojęciem w spirali milczenia. Krytycy kwestionują pogląd, że quasi-statystyczne postrzeganie klimatu opinii jest zazwyczaj dokładne.
- Gotowość do wypowiadania się i skłonność do milczenia – jednostki mają tendencję do publicznego wyrażania swoich opinii i postaw, kiedy postrzegają swój pogląd jako dominujący lub rosnący. W przeciwieństwie do tego, gdy ludzie wyczuwają, że ich pogląd znajduje się w mniejszości, stają się ostrożni i milczący.
- Spirala milczenia – interakcja tych 4 czynników prowadzi do procesu formowania, zmiany i wzmacniania opinii publicznej. Tendencja jednej osoby do mówienia, a drugiej do milczenia stają się spiralnym procesem, który coraz bardziej ustanawia jedną opinię jako dominującą. Z biegiem czasu zmieniające się postrzeganie klimatu opinii wpływa na gotowość ludzi do wyrażania opinii mniejszości i ustanowienia jednej opinii jako dominującej. Opinia publiczna jest przekształcana z pytania obciążonego moralnie w „solidną" normę lub dogmat.

Aby w pełni wyjaśnić proces spirali milczenia, należy wziąć pod uwagę także moralny wymiar opinii publicznej, rolę czasu i mediów. Proces spirali

milczenia działa tylko w przypadku kwestii moralnych lub zagadnień obciążonych wartością, przez które poszczególne osoby izolują się lub mogą izolować się publicznie. Tylko z tego moralnego lub normatywnego powodu opinia publiczna wyczuwa zagrożenie izolacją. Postrzegany klimat opinii i jej przyszły rozwój są kluczowymi czynnikami w spirali milczenia, a więc najważniejsza pozostaje odpowiedź na pytanie, który punkt widzenia jest dominujący lub może stać się dominujący, a który jest wyrażany przez mniejszość i prawdopodobnie przegra. Procesy tu opisane mogą mieć miejsce tylko wtedy, gdy media zajmą rozpoznawalną pozycję w konflikcie.

Jeśli opinia publiczna jest formą kontroli społecznej i wiąże się z postrzeganiem innych, to można ją zdefiniować jako postawy lub zachowania, które należy wyrazić publicznie, jeśli jednostka nie ma zamiaru się izolować; w obszarach kontrowersji lub zmian opinie publiczne są postawami, które można wyrazić bez narażania się na izolację. Ludzkie zachowanie, a zwłaszcza gotowość do wypowiadania się, są silnie kierowane przez strach przed izolacją.

W badaniach Noelle-Neumann przypadki, w których ludzie mylili się co do popularnej opinii, były bardzo prawdopodobne, co było konsekwencją medialnych relacji zapewniających mieszankę punktów widzenia nieproporcjonalnych do ich siły w społeczeństwie. W swojej książce Noelle-Neumann sugeruje, że ankieterzy zadają złe pytania. Zamiast pytać: „Na kogo zamierzasz głosować?", należy zapytać: „Kto według ciebie wygra wybory?". Odpowiedzi na to drugie pytanie, po przeanalizowaniu w książce o danych opinii publicznej, wykazują większą spójność z ostatecznym wynikiem wyborów i ilustrują znacznie wyraźniejsze trendy. Jeśli obecna większość zostanie w danej chwili uznana za mniejszość, w przyszłości jej poparcie będzie spadać. Dopóki grupa jest postrzegana jako mniejszość, ludzie nie będą chcieli wyrazić poparcia dla niej. Odwrotnie, jeśli mniejszość jest postrzegana jako przyszła większość, może ostatecznie zdobywać coraz większe poparcie.

Środki masowego przekazu, główne źródło informacji o opinii większości, odgrywają bardzo istotną rolę w wyjaśnianiu efektu spirali milczenia. Zgodnie z teorią dowiadujemy się za pośrednictwem środków masowego przekazu, kim jest większość i jakie są jej poglądy. Różne systemy

medialne (otwarte i zamknięte, ściśle kontrolowane i liberalne) w różnych systemach politycznych (demokratycznych, autorytarnych i totalitarnych) oferują różne narzędzia, które pretendujący do władzy mogą wykorzystać w walce o uznanie jako większość, która może ostatecznie wygenerować i powiększyć ich rzeczywiste poparcie.

Internet, a w szczególności media społecznościowe, chociaż mniej podatne na zewnętrzną kontrolę i obejmujące większą liczbę bardziej zróżnicowanych wiadomości, komunikatorów i odbiorców, ulegają procesowi spirali milczenia. Media społecznościowe zapewniają łatwy dostęp do masowej widowni, za niską cenę, co potencjalnie powinno promować różnorodność opinii. Media społecznościowe, które reprezentują większą różnorodność opinii, mogą zmniejszyć lęk przed izolacją: można łatwiej znaleźć grupę, do której chce się przynależeć, opowiadającą się za niepopularną opinią.

Badania pokazują, że efekty spirali milczenia są nadal obecne w środowisku mediów społecznościowych. Jednak wielkość tego efektu jest zmniejszona przez wiele czynników. Wiele z nich zależy od natury mediów społecznościowych, a inne są zdeterminowane przez odmienne cechy ich odbiorców. Podczas gdy → m e d i a t r a d y c y j n e [t. 3] nadal zajmują pozycję głównego źródła informacji na temat kontrowersyjnych kwestii politycznych, coraz popularniejsze stają się nowe kanały komunikacji. W → r e ż i m a c h [t. 3] autorytarnych i totalitarnych, gdzie dostęp do alternatywnych informacji jest limitowany (jeśli nie jest ograniczony), rola mediów społecznościowych w komunikacji politycznej staje się bardziej znacząca. Znaczenie mediów społecznościowych jest wyższe w przypadku tradycyjnie niepopularnych grup, takich jak społeczności lesbijek, gejów, osób biseksualnych i transpłciowych (LGBT), które mogą uzyskać głos, podczas gdy w dużej mierze przez długi czas ignorowane były przez media głównego nurtu.

Koncepcją tłumaczącą specyficzny sposób, w jaki media prezentują odbiorcom informacje, jest *framing*, oznaczający dosłownie ramowanie. Medialne ramy tematyczne odnoszą się do polityki, relacjonowania wyborów i kampanii wyborczych, debat politycznych, ale także zjawisk takich jak kataklizmy czy konflikty społeczne. Ramowanie nie ma incydentalnego charakteru i jest przez badaczy analizujących medialne

przekazy często identyfikowane, co pozwala mówić o pewnej typowości i powtarzalności w sposobie prezentacji wielu problemów w mediach. D. Tewksbury i D.A. Scheufele, tłumacząc istotę *framingu*, w metaforyczny sposób wskazują, że dziennikarze postępują w podobny sposób do artystów, którzy wiedzą, że rama wokół obrazu może wpłynąć na to, jak widzowie interpretują i reagują na samo dzieło. Właśnie dlatego niektórzy artyści troszczą się o to, w jaki sposób prezentują swoją pracę, wybierając ramy, które wg nich sprawią, że odbiorcy zobaczą obraz w odpowiedni sposób. Dziennikarze, często podświadomie, angażują się zasadniczo w ten sam proces, decydując, jak opisać świat polityczny. Wybierają obrazy i słowa, które mają wpływ na to, jak odbiorcy interpretują i oceniają relacjonowane wydarzenia i problemy.

Poza samą diagnozą medialnych komunikatów pojawiają się także pytania o to, jak sposób prezentacji danego tematu przekłada się na jego postrzeganie przez odbiorców. Rozważania te pojawiły się wraz z pierwszymi naukowymi badaniami dotyczącymi ramowania, mającymi swe korzenie w psychologii i socjologii. W pracach eksperymentalnych D. Kahnemana i A. Tversky'ego w latach 70. ubiegłego wieku badano, w jaki sposób różne odsłony identycznych scenariuszy decyzyjnych wpływają na wybory dokonywane przez ludzi i na ich ocenę różnych przedstawionych im do wyboru opcji. W podobnym okresie socjologiczne podstawy konstrukcji ramowania zostały nakreślone przez E. Goffmana, który dowodził, że jednostki nie mogą w pełni zrozumieć świata i nieustannie poszukują możliwości interpretacji swoich doświadczeń życiowych i nadawania sensu otaczającemu ich światu. Aby skutecznie przetwarzać nowe informacje, jak wskazywał Goffman, poszczególne osoby stosują schematy interpretacyjne, czyli ramy ułatwiające klasyfikacje informacji i ich rozumienie.

R.M. Entman, amerykański badacz, który znaczną część swoich prac teoretycznych oraz empirycznych poświęcił badaniu procesów ramowania, wskazuje, że *framing* polega głównie na selekcji i eksponowaniu. Ramowanie pozwala na wybranie pewnych aspektów przedstawianej rzeczywistości i uczynieniu ich bardziej wyrazistymi w komunikowanym materiale tak, aby promować daną definicję określonego problemu, interpretację przyczynową, ocenę moralną czy zalecenie dotyczące dalszego działania. Na podstawie licznych analiz przekazów medialnych w prasie

i telewizyjnych programach informacyjnych dotyczących polityki H.A. Semetko i P.M. Valkenburg wskazują na istnienie 5 najpopularniejszych ram tematycznych zidentyfikowanych we wcześniejszych badaniach dotyczących *framingu*:

- odpowiedzialności,
- konfliktu,
- ludzkich interesów,
- skutków ekonomicznych,
- moralności.

Większość informacji podawanych przez media odpowiada określonym schematom zgodnym z jednej strony z praktyką dziennikarską, z drugiej z oczekiwaniami i przyzwyczajeniami widzów i czytelników. Dla przykładu informacje o wojnach, atakach terrorystycznych, wypadkach czy katastrofach zawsze podaje się z liczbą zabitych i rannych. Z kolei w przypadku informowania o wyborach czy referendum naturalną formułą jest posługiwanie się stylistyką sportową lub wojenną, używanie takich określeń jak „w peletonie", „na pierwszym miejscu", „zwycięzca tej batalii", „przegrany w tej grze". Zmiany w budżecie zwykle są prezentowane przez pryzmat podkreślania, na co i dokładnie ile zabrakło. Polityka najczęściej przedstawiana jest, zwłaszcza w telewizyjnych programach informacyjnych, jako → s t r a t e g i a [t. 4], gra lub wyścig o władzę, wpływy i prestiż.

Istnieje mnogość przypadków, gdy wielostronność i złożoność problemu wkładana jest w karby określonej „ramy tematycznej" i w taki właśnie, uproszczony sposób jest odbierana przez użytkowników mediów. Nie ulega wątpliwości, że dla większości odbiorców problem przedstawiony w określonej ramie istnieje tylko w niej – sami dalej posługują się jego uproszczonym i schematycznym sposobem postrzegania.

Efektem oddziaływania mediów na odbiorców pozostaje także pogłębianie się w czasie różnicy w zakresie wiedzy i rozumienia świata społecznego, w tym zjawisk politycznych, co wyjaśnia z kolei koncepcja luki wiedzy. Wiedza zakłada istnienie informacji, jednak nie oznacza to z definicji, że osoba posiadająca informacje ma też wiedzę. Jako minimum założyć należy, że ten, kto posiada wiedzę, jest w stanie zrozumieć informacje i ich właściwy kontekst. Wiedza stanowi zatem istotną podstawę do

tego, w jaki sposób przyjęta zostanie informacja, z drugiej zaś strony ta sama informacja w odpowiedni sposób poszerzy wiedzę, którą jednostka już posiada. Proces ten nastąpi także wówczas, gdy wiedza jednostki jest niedostateczna do tego, by we właściwy sposób zrozumieć informację.

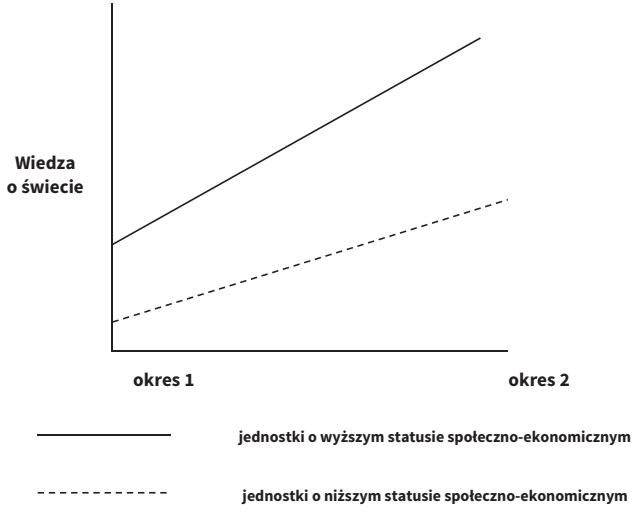
Problem zależności pomiędzy informacjami o świecie płynącymi z mediów a wiedzą jest złożony, zaś badania empiryczne nie przynoszą dowodów, które jednoznacznie weryfikowałyby formułowane hipotezy. Niezwykle trudno potwierdzić choćby relację przyczynowości, a więc stwierdzić bez większych wątpliwości, czy to wiedza w większym stopniu warunkuje odbiór informacji, czy przeciwnie, w większym stopniu to informacje czerpane z mediów odpowiadają za wiedzę. Nie udało się także jednoznacznie ocenić, czy dominacja mediów komercyjnych nad publicznymi, jak często się zakłada, sprzyja tabloidyzacji i spadkowi poziomu wiedzy w stosunku do tych systemów medialnych, w których media publiczne mają szczególnie silną pozycję. Często powtarzana, obiegowa opinia, wg której większą wiedzą o świecie mogą pochwalić się osoby, które pozyskują informacje z gazet, a nie z telewizji, posługującej się uproszczoną kulturą obrazu, również nie znajduje wyraźnego potwierdzenia w badaniach empirycznych.

Jednocześnie należy wskazać, że na kształtowanie się wiedzy mają wpływ informacje medialne, jednak nie są one jedynym czynnikiem, a odbiór treści przekazu medialnego nie następuje u wszystkich jednostek w taki sam sposób. Innymi słowy, ten sam przekaz medialny może zostać inaczej odebrany przez różnych odbiorców. Istnieją rozliczne badania próbujące wyodrębnić i scharakteryzować czynniki wyjaśniające sposób, w jaki obywatele przyjmują wiedzę na temat polityki. R.M. Perloff podkreśla, że poza użytkowaniem mediów na proces przyswajania wiedzy o polityce wpływają także czynniki demograficzne oraz psychologiczne procesy poznawcze.

Badania empiryczne prowadzone w różnych państwach prowadzą do wniosku, że na kształtowanie wiedzy o świecie i sposób odbioru informacji medialnych największy wpływ ma poziom formalnej edukacji danej osoby oraz miejsce w strukturze społecznej, w mniejszym zaś zakresie wiek oraz płeć. Wyniki te tłumaczy i rozwija koncepcja luki wiedzy. Łączy ona perspektywę socjologiczną i wyniki badań w obszarze komunikacji masowej.

Jako jedno z trwałych ustaleń w badaniach nad komunikacją polityczną można wskazać istnienie luk w wiedzy, które są jedynie powiększane przez informacje medialne. Zjawisko to wywołane jest przez 2 czynniki socjologiczne: dochód i wykształcenie, a więc status społeczno-ekonomiczny. Zgodnie z koncepcją luki wiedzy osoby o wyższym statusie społeczno-ekonomicznym mają na początku więcej wiedzy na temat świata niż osoby o niższym statusie społeczno-ekonomicznym. Najlepiej byłoby, gdyby informacje płynące z przekazu medialnego dostarczały osobom o niższym statusie więcej informacji, wyrównując różnicę. Jednak hipoteza dotycząca luki w wiedzy dowodzi, że dzieje się odwrotnie: osoby o wyższym statusie społeczno-ekonomicznym, dobrze poinformowani obywatele, zdobywają więcej informacji i robią to szybciej niż osoby o niższym statusie, zdecydowanie słabiej poinformowane. W efekcie opisane zróżnicowanie zwiększa się, a nie zmniejsza, w konsekwencji czego lepiej zorientowani wiedzą jeszcze więcej, a posiadający mniejszą wiedzę na początku mają ją po czasie jeszcze mniejszą. Koncepcję tę ilustruje poniższy schemat:

Schemat 1. Luka wiedzy



Polityczne i komercyjne oddziaływanie mediów wiąże się ze stałym przekonywaniem odbiorców do określonych działań. Tę specyfikę medialnych oddziaływań wyjaśnia częściowo model ELM (ang. *elaboration likelihood model*), który dowodzi, że ważne różnice w charakterze medialnej perswazji są funkcją prawdopodobieństwa tego, że odbiorcy zaangażują się w ewaluację informacji istotnych dla kwestii perswazyjnej. W zależności od stopnia ewaluacji można zastosować 2 różne rodzaje procesu perswazji. Te 2 procesy perswazji nazywane są „drogą centralną" i „drogą peryferyjną".

Droga centralna odnosi się do procesów perswazji związanych z relatywnie wysokim poziomem ewaluacji. Tam, gdzie perswazję osiąga się drogą centralną, zwykle dzieje się to poprzez szeroko zakrojone myślenie istotne dla danego problemu: staranne badanie informacji zawartych w wiadomości, ścisłą analizę argumentów i ich ocenę. Droga peryferyjna reprezentuje procesy perswazji związane z relatywnie niskim poziomem ewaluacji. Tam, gdzie perswazję osiąga się drogą peryferyjną, zwykle dzieje się tak, ponieważ odbiorca stosuje pewną prostą regułę decyzyjną (pewną zasadę heurystyczną) do oceny zalecanej pozycji. Np. odbiorcy mogą kierować się tym, czy uważają komunikator za wiarygodny.

Stopień ewaluacji w danej sytuacji (a tym samym wybór drogi, która zostanie aktywowana) wynika z wielu czynników, które można ogólnie zaklasyfikować jako wpływające na motywację lub zdolność oceny. Na motywację do wyboru drogi centralnej może wpływać trafność tematu (większe znaczenie osobiste prowadzi do większej motywacji do oceny) i poziom „potrzeby poznania" odbiorcy, cecha osobowości odzwierciedlająca tendencję do czerpania przyjemności z myślenia. Ponieważ perswazja drogi centralnej i drogi peryferyjnej mają różne podstawowe procesy, czynniki determinujące sukces perswazyjny odpowiednio się różnią. W perswazji drogi centralnej efekty perswazyjne zależą od dominującej wartościowości (pozytywnej lub negatywnej) myśli istotnych dla odbiorcy. W zakresie, w jakim odbiorca ma w przeważającej mierze przychylne myśli na temat zalecanej pozycji, wiadomość prawdopodobnie będzie względnie skuteczna. Na dominującą wartościowość ewaluacji ma wpływ to, czy zalecana pozycja wiadomości jest nastawiona pozytywnie wobec postawy odbiorcy, czy przeciwnie do odbiorcy (wiadomości *pro* prawdopodobnie wywołują

głównie pozytywne myśli, wiadomości *contra* głównie myśli niekorzystne), oraz siła argumentów wiadomości (argumenty lepszej jakości prowadzą do bardziej pozytywnych przemyśleń).

Natomiast w perswazji przy wyborze drogi peryferyjnej odbiorcy stosują zasady heurystyczne, proste procedury decyzyjne uruchamiane przez sygnały peryferyjne. Np. w heurystyce wiarygodności zamiast uważnego rozważania argumentów wiadomości odbiorcy po prostu polegają na pozornej wiedzy nadawcy jako przewodnika po tym, w co warto wierzyć. Inne heurystyki opierają się na upodobaniu odbiorcy do nadawcy i reakcjach innych na wiadomość. Wraz ze wzrostem liczby ewaluacji wpływ takiej heurystyki maleje, ale tam, gdzie odbiorcy nie są w stanie lub nie są zmotywowani do analizy wiadomości, na tych skrótach można polegać. Wiedza na temat sposobów oceny sytuacji przez odbiorców pozwala na aktywizację tych elementów, które przekonają go do wyboru, zakupu czy oceny zgodnej z intencjami nadawcy.

Głównym powodem, dla którego niezwykle trudne, a zdaniem niektórych badaczy wręcz niemożliwe jest precyzyjne badanie empiryczne efektów mediów, pozostaje brak możliwości wyizolowania wpływu mediów w rozwiniętych społeczeństwach. Znalezienie kogoś, kto nie byłby narażony na środki masowego przekazu, jest prawie niemożliwe. Nawet osoby, które nie oglądają telewizji, nie czytają gazet ani nie surfują po internecie, regularnie wchodzą w interakcje z innymi, którzy to robią. Brak możliwości porównania osób pozostających pod wpływem mediów z osobami, które pod takim wpływem nie są, czyni rozważania nad oddziaływaniem mediów w dużej mierze nieweryfikowalnymi empirycznie.

Jakub Idzik, Rafał Klepka

R.M. Entman, *Framing: Toward Clarification of a Fractured Paradigm*, „Journal of Communication" 1993, t. 43, no. 4; E. Goffman, *Frame Analysis: An Essay on the Organization of Experience*, Northeastern University Press, Boston 1986; J. Idzik, *Man in the World of Old and New Media – Selected Concepts of Media Influence and their Contemporary Interpretations*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 9 (3); H.M. Kepplinger, *Media Effects*, [w:] *The Concise Encyclopedia of Communication*, W. Donsbach (ed.), Blackwell Publishing, Malden, Oxford, Carlton 2015; R. Klepka, *Obrazy polityki w mediach: podstawowe*

uwarunkowania, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018; E. Noelle-Neumann, *The Spiral of Silence: Public Opinion – Our Social Skin*, University of Chicago Press, Chicago 1993; T. Petersen, *Spiral of Silence*, [w:] *The Concise Encyclopedia of Communication*, W. Donsbach (ed.), Blackwell Publishing, Malden–Oxford–Carlton 2015; D.A. Scheufle, P. Moy, *Twenty-Five Years of the Spiral of Silence: A Conceptual Review and Empirical Outlook*, „International Journal of Public Opinion Research" 2000, vol. 12, iss. 1; D.A. Scheufele, D. Tewksbury, *Framing, Agenda Setting, and Priming: The Evolution of Three Media Effects Models*, „Journal of Communication" 2007, t. 57, no. 1; ciż, *News Framing Theory and Research*, [w:] *Media Effects: Advances in Theory and Research*, J. Bryant, M.B. Oliver (eds.), Routledge, New York–London 2009; D. Yuran, *Spiral of Silence*, [w:] *Encyclopedia of Social Media and Politics*, K. Harvey (ed.), SAGE, Los Angeles–London–New Delhi–Singapore–Washington 2011.

EKOCYD (ang. *ecocide*) – ekobójstwo, termin będący zbitką wyrazową stgr. οἶκος (*oikos*, dom) i łac. *caedere* (złamać, ściąć, rąbać, zabić), dosłownie oznacza „zabicie naszego domu". Ekocyd oznacza poważne naruszenie, zdegenerowanie lub całkowite zniszczenie ekosystemów, które zagraża życiu lub zdrowiu populacji ludzkiej; masowe zniszczenie flory lub fauny, zatrucie atmosfery lub zasobów wodnych, a także inne działania, które mogą spowodować katastrofę ekologiczną; to również ostatnia faza całkowitego zniszczenia środowiska naturalnego (zniszczenie wszelkiego życia) na danym obszarze w wyniku działalności człowieka, w szerszym ujęciu także w wyniku przyczyny naturalnej, np. zalania danego terenu lawą wulkaniczną. Ekocyd oznacza przestępstwo przeciwko ekosystemom, przewiduje utratę, uszkodzenie lub zniszczenie ekosystemu danego terytorium (terytoriów) na taka skalę, że pokojowe korzystanie z nich przez mieszkańców zostało lub zostanie poważnie ograniczone.

Ekocyd to również przestępcza działalność człowieka, która narusza zasady sprawiedliwości środowiskowej, takie jak powodowanie rozległych szkód lub niszczenie ekosystemów, szkodzenie zdrowiu i dobrostanowi gatunku (w tym ludzi). Pojęcie ekocydu odnosi się zarówno do naturalnie zachodzących procesów degradacji środowiska lub ekosystemu, jak i niszczenia środowiska spowodowanego działalnością człowieka. Na przykład migracja gatunków inwazyjnych na dany obszar, która prowadzi

do zmniejszenia lub wyginięcia gatunków endemicznych na tym obszarze, jest również formą ekocydu.

Termin ekocyd jest używany w różnych kontekstach i oznacza:

- eksterminację narodu poprzez zniszczenie jego zasobów naturalnych, jak np. wyniszczenie brazylijskich lasów deszczowych;
- przymusowe odebranie niezależności kulturowej narodowi poprzez zniszczenie jego ekologicznego krajobrazu kulturowego;
- czasami śmiertelne długoterminowe konsekwencje użycia środków bojowych, które mogą prowadzić do uszkodzenia środowiska naturalnego i dziedzictwa ekologicznego, jak miało to miejsce np. w Wietnamie (Agent Orange);
- ogólną degradację środowiska spowodowaną przez cywilizację przemysłową i zaburzenie równowagi ekologicznej z powodu ogromnego zanieczyszczenia.

Ekocyd może być nieodwracalny, gdy ekosystem odniesie szkody przekraczające jego zdolność do regeneracji. Termin został po raz pierwszy zaproponowany w 1970 r. przez amerykańskiego botanika i bioetyka A.W. Galstona na Konferencji kongresowej w sprawie wojny i odpowiedzialności narodowej w Waszyngtonie (Congressional Conference on War and National Responsibility). Termin został wpisany do dokumentu końcowego z konferencji, a Galston zaproponował nową umowę międzynarodową ws. zakazu ekocydu. W obliczu zmian klimatycznych działacze w różnych krajach występują o prawne uznanie zniszczenia środowiska za przestępstwo międzynarodowe. W efekcie końcowym ściganie i pociągnięcie do odpowiedzialności winnych za wyrządzone szkody ekologiczne radykalnie zmieni podejście do →bezpieczeństwa ekologicznego [t. 1] świata.

Myślą przewodnią walki z licznymi przejawami ekobójstwa we współczesnym świecie jest uznanie na poziomie prawa międzynarodowego tego zjawiska za międzynarodowe przestępstwa ze szczególnym okrucieństwem. W związku z powyższym ważne jest określenie sfery odpowiedzialności za charakter oddziaływania społeczeństwa na środowisko. Od tego w dużej mierze zależą podstawy prawa międzynarodowego oraz narodowe realia walki o rozwój i przetrwanie.

W latach 70. XX w. w myśl rozszerzenia konwencji w sprawie →ludobójstwa [t. 3] z 1948 r. powstało wiele szeroko zakrojonych badań

dotyczących tego, czy ekocyd powinien zostać uznany przez ONZ za przestępstwo międzynarodowe. W 1972 r. podczas pierwszej konferencji ONZ ws. środowiska ludzkiego (konferencji sztokholmskiej ONZ), na której została przyjęta Deklaracja Sztokholmska, w przemówieniu otwierającym obrady premier Szwecji O. Palme jako pierwszy na forum międzynarodowym politycznie zaproponował użycie terminu ekocyd w znaczeniu ekobójstwa, przyjmując go do opisania katastrofalnych szkód wyrządzonych środowisku naturalnemu podczas → w o j n y [t. 4] w Wietnamie. Mówiąc o wojnie we Wietnamie jako o ekocydzie, podkreślił potrzebę globalnego podejścia do ochrony środowiska i odpowiedzialności za jego stan. Inni światowi liderzy, w tym I. Gandhi z Indii i przywódca chińskiej delegacji Tang Ke, również potępili wojnę w kategoriach środowiskowych. Apelowali także, aby ekocyd był traktowany jako przestępstwo międzynarodowe. Podczas konferencji utworzono grupę roboczą ds. przestępstw przeciwko środowisku, a projekt konwencji o ekocydzie został przedłożony ONZ w 1973 r. Na Forum Ludowym, wydarzeniu równoległym do konferencji ONZ, tysiące ludzi wyszło na ulice, domagając się uznania ekobójstwa za przestępstwo.

W 1972 r. Dai Dong z oddziału Międzynarodowego Towarzystwa Pojednania sponsorował konferencję, która także odbyła się w Sztokholmie i także dotyczyła ekobójstwa. Spotkanie zgromadziło wiele wybitnych osobistości, w tym R.A. Falka, eksperta w zakresie międzynarodowego prawa dotyczącego → z b r o d n i w o j e n n y c h [t. 4], oraz R.J. Liftona, amerykańskiego psychiatrę i pisarza, znanego przede wszystkim ze swoich badań psychologicznych przyczyn i skutków wojen i → p r z e m o c y [t. 3] politycznej, psychologii ludobójstwa oraz psychohistorii. Zgromadzenie zaapelowało o przyjęcie konwencji ONZ o wojnie ekobójczej, która m.in. miałaby na celu zdefiniowanie i potępienie ekocydu jako międzynarodowej zbrodni wojennej. W 1973 r. Falk opracował konwencję o ekocydzie, w preambule której wyraźnie stwierdzano, że człowiek świadomie i nieświadomie wyrządził nieodwracalną szkodę środowisku w czasach wojny i pokoju. Od samego początku uznano, że element intencji nie zawsze ma prawne zastosowanie, ponieważ ustanowienie zamiaru może być nie tylko niemożliwe, ale i w zasadzie już nieistotne.

Podkomisja ds. Zapobiegania Dyskryminacji i Ochrony Mniejszości upubliczniła badanie omawiające skuteczność konwencji o ludobójstwie,

proponujące przyjęcie ekocydu (ekobójstwa) oraz ludobójstwa kulturowego na listę przestępstw. W następnych latach fakty dokonania ekocydu były badane przez różne grupy robocze i wymieniane w kilku innych raportach.

Statut Rzymski → Międzynarodowego Trybunału Karnego [t. 3] jest najważniejszym dokumentem prawnie regulującym istniejące przestępstwa międzynarodowe. W procesie uzgadniania prawnych podstaw tego dokumentu termin ekocyd został użyty i sprecyzowany. Pojęcie ekocydu było uwzględnione w większości pierwotnych projektów dokumentów, przygotowanych do uzgodnienia między państwami. W szczególności w 1978 r. na forum ONZ pojawiły się projekty artykułów prawnych na temat ekologicznej odpowiedzialności państw w kontekście definiowania przestępstw międzynarodowych. W szczególności stwierdzano, iż przestępstwo międzynarodowe może wynikać m.in. z poważnego naruszenia międzynarodowego zobowiązania o zasadniczym znaczeniu dla ochrony i zachowania środowiska ludzkiego, takiego jak te, które zabraniają masowego zanieczyszczenia atmosfery lub mórz. Krajami, które opowiadały się za wprowadzeniem kar za zbrodnię ekocydu, były Rumunia, Stolica Apostolska, Austria, Polska, Rwanda, Kongo i Oman. Wspomniane definicje prawne zbrodni ekocydu zostały poddane dyskusji 4 lipca 1978 r. w ramach Podkomisji ONZ ds. Zapobiegania Dyskryminacji i Ochrony Mniejszości w sprawie zapobiegania i karania zbrodni ludobójstwa.

W połowie lat 80. XX w. został upubliczniony raport specjalnego sprawozdawcy ONZ B. Whitakera, zlecony przez Podkomisję ds. Promocji i Ochrony Praw Człowieka, w sprawie zapobiegania i karania zbrodni ludobójstwa. W trakcie jego prezentacji i dyskusji Whitaker podkreślał, że niektórzy członkowie podkomisji zaproponowali rozszerzenie definicji ludobójstwa na ludobójstwo kulturowe (ang. *ethnocide*), a także na ekocyd jako niekorzystne, często nieodwracalne, zmiany dla środowiska – np. w wyniku zastosowania → broni nuklearnej [t. 1] lub → broni chemicznej [t. 1], inne poważne zanieczyszczenie, kwaśne deszcze, zniszczenie lasów tropikalnych itd. – które zagrażają istnieniu całej populacji, celowo lub z zaniedbania. Projekt rezolucji przygotowany dla Komisji Praw Człowieka, przedłożony przez J. Deschênesa i C. Mubangę-Chipoya w ramach przeglądu, zawierał zalecenie, aby specjalny sprawozdawca ONZ Whitaker rozszerzył i pogłębił studium pojęć etnocydu i ekocydu.

Natomiast w dokumentach i rezolucjach 38, 39 i 40 sesji ONZ zabrakło →informacji dotyczących ostatecznych wywodów podkomisji na ten temat.

W 1987 r. dyskusje o ekologicznych przestępstwach międzynarodowych w Komisji Prawa Międzynarodowego były kontynuowane, zaproponowano, aby lista przestępstw międzynarodowych zawierała ekocyd jako odzwierciedlenie potrzeby ochrony i zachowania środowiska, a także jako skutek użycia broni jądrowej, kolonializmu, apartheidu, agresji ekonomicznej itd.

W 1991 r. projekt kodeksu zbrodni przeciwko pokojowi i bezpieczeństwu ludzkości zawierał 12 rodzajów przestępstw. Termin ekocyd został zastąpiony przez definicje „umyślnej i poważnej szkody dla środowiska" (art. 26) bez głosowania. Projekty artykułów przekazano rządom w celu uzyskania ich uwag i opinii. Na dzień 29 marca 1993 r. sekretarz generalny ONZ otrzymał 23 odpowiedzi od państw członkowskich i jedną odpowiedź od państwa trzeciego. Były to: Australia, Austria, Białoruś, Belgia, Brazylia, Bułgaria, Kostaryka, Ekwador, Grecja, Holandia, Dania, Finlandia, Islandia, Norwegia, Szwecja, Paragwaj, Polska, Senegal, Sudan, Turcja, Wielka Brytania, USA, Urugwaj i Szwajcaria. Tylko 3 kraje – Holandia, Wielka Brytania i USA – sprzeciwiły się włączeniu przestępstwa przeciwko środowisku. Holandia poparła tylko 4 przestępstwa, nie popierając ekocydu. USA i Wielka Brytania w ogóle sprzeciwiły się projektowi kodeksu *per se*. USA termin „ekocyd – przestępstwo przeciwko środowisku" oznaczyły jako „niejasne", a Wielka Brytania jako nieznaną międzynarodową →przestępczość [t. 3], natomiast Austria skomentowała to w ten sposób, że „ponieważ sprawcy tego przestępstwa zwykle działają w celu zarobkowym, zamiar nie powinien być warunkiem odpowiedzialności karnej". Takie kraje jak Australia, Belgia i Urugwaj również zajęły stanowisko, wg którego żaden element intencji nie jest konieczny dla art. 26 – określenia ekologicznego przestępstwa „umyślnego".

W 1995 r. Komisja Prawa Międzynarodowego ONZ zredukowała 12 proponowanych rodzajów przestępstw do 6. Projekt dyskusji nad kodeksem został przeniesiony do Szóstego Komitetu Zgromadzenia Ogólnego. Na dwunastym spotkaniu komitetu, które odbyło się 12 października 1995 r. „specjalny sprawozdawca na ten temat przedstawił swój 13. raport

zalecający zachowanie tylko 6 z 12 przestępstw określonych w pierwszym czytaniu w celu włączenia do kodeksu, a mianowicie – „umyślne i poważne szkody w środowisku" (art. 26). Dokumenty wskazują, że były zgłoszone obawy, a powodem ich utrzymania był fakt, że likwidacja szkód dla środowiska jest obowiązkiem konkretnego państwa.

Podczas szóstego posiedzenia 50. sesji Zgromadzenia Ogólnego ONZ, które odbyło się w dniu 17 października 1995 r., usunięto wyrażenie „umyślne i poważne szkody dla środowiska". Niektóre kraje, np. Chile, nie zgodziły się. Odnotowano, że przestępstwa przeciwko środowisku w czasie pokoju zostały usunięte z projektu kodeksu z 1996 r., ponieważ specjalny sprawozdawca chciał podczas drugiego czytania ograniczyć listę przestępstw przeciwko bezpieczeństwu ludzkości do tych, które trudno w ogóle odrzucić.

W 1996 r. definiowanie pojęcia „umyślne i poważne szkody dla środowiska" (art. 26) powierzono grupie roboczej Komisji Prawa Międzynarodowego ONZ. Z kolei komisja postanowiła, że konsultacje będą kontynuowane i że będzie utworzona grupa robocza w celu zbadania możliwości uwzględnienia w projekcie kodeksu „umyślnej i poważnej szkody dla środowiska".

W 1996 r. znany prawnik M. Gray zaproponował swoją definicję zbrodni ekocydu, opartą na ustalonym międzynarodowym prawie ochrony środowiska i → p r a w c z ł o w i e k a [t. 3]. Zdefiniował, że państwa, osoby i organizacje, powodujące lub pozwalające wyrządzić szkodę środowisku naturalnemu na masową skalę, naruszają obowiązek ochrony środowiska przynależącego ogólnie do ludzkości. Zaproponował, aby takie naruszenia, gdy są umyślne, lekkomyślne lub niedbałe, zostały zidentyfikowane jako ekocyd, jeżeli pociągają za sobą poważne, rozległe lub trwałe szkody ekologiczne, konsekwencje międzynarodowe i marnotrawstwo.

W Komisji Prawa Międzynarodowego ONZ 19 krajów opowiedziało się za utrzymaniem środowiskowych szkód na liście przestępstw ujętych w projekcie kodeksu. Na 50. sesji Zgromadzenia Ogólnego ONZ (1995–1996) większość państw członkowskich opowiedziała się za wprowadzeniem określenia ekocyd jako przestępstwa, ale 3 państwa – Francja, Brazylia i Czechy – były temu przeciwne. Jednak w ciągu kilku tygodni Komisja Prawa Międzynarodowego zredukowała listę składającą się z 6 przestępstw do 4 bez głosowania. 5 lipca 1996 r. Komisja Prawa

Międzynarodowego ONZ przyjęła ostateczny projekt kodeksu zbrodni przeciwko pokojowi i bezpieczeństwu ludzkości. W nim definicja ekocydu jako przestępstwa została usunięta za zamkniętymi drzwiami spotkania, a „umyślne i poważne szkody dla środowiska" zostały usunięte, podobnie jak i odpowiedzialność państw.

Reasumując, pojęcie ekocydu było uwzględnione w większości pierwotnych projektów dokumentów przygotowanych do uzgodnienia między państwami, dopóki nie zostały usunięte w 1996 r. z ostatecznego projektu na żądanie 4 krajów – Wielkiej Brytanii, USA, Holandii i Francji.

Ostateczny projekt kodeksu został w 1998 r. przemianowany na Statut Rzymski, w którym przewiduje się odpowiedzialność za 4 międzynarodowe zbrodnie – ludobójstwa, → z b r o d n i p r z e c i w k o l u d z k o ś c i [t. 4], zbrodni wojennych oraz zbrodni agresji. Pojęcie ekocydu zostało wykluczone, a wszelkie wzmianki o szkodach dla środowiska ograniczały się wyłącznie do zbrodni wojennych, a nie do zbrodni w czasach pokojowych.

Zgodnie z Konwencją o zakazie używania technicznych środków oddziaływania na środowisko z 1977 r. (*Environmental Modification Convention*, ENMOD) pojęcie ekocydu jako zniszczenia środowiska w czasie wojny sklasyfikowano jako proces „szeroko rozpowszechniony, długoterminowy i poważny", podczas gdy art. 8 ust. 2 lit. b) Statutu Rzymskiego z 1998 r. zmodyfikował wyżej przytoczony tekst ENMOD ze zmianą jednego słowa na „powszechny, długofalowy i poważny". Zgodnie z tym zapisem szkoda dla środowiska jest przestępstwem tylko w ograniczonych okolicznościach, gdy

> celowo przeprowadza się atak, wiedząc, że taki atak będzie powodować przypadkową utratę życia lub obrażenia ciała wśród ludności cywilnej lub szkody w obiektach cywilnych lub powszechne, długotrwałe i poważne szkody w środowisku naturalnym, które byłyby wyraźnie nadmierne w stosunku do konkretnej i bezpośredniej ogólnej przewidywanej przewagi wojskowej.

W ten sposób zlekceważono fakt powszechnego zniszczenia środowiska naturalnego w czasach pokoju, natomiast wzięto pod uwagę tylko wyjątkowe okoliczności.

W marcu 2010 r. założycielka ruchu Stop Ecocide, znana prawniczka P. Higgins, ponownie zaczęła kampanię o prawne uznanie ekocydu za przestępstwo międzynarodowe. Higgins przedłożyła Komisji Prawnej ONZ poprawkę do Statutu Rzymskiego, proponując definicję ekocydu rozumianego jako „utrata, uszkodzenie lub zniszczenie ekosystemu na danym terytorium (terytoriach) […] tak, że pokojowe korzystanie przez mieszkańców zostało lub zostanie poważnie ograniczone". Definicja ta określała projekt kierunku zmian w Statucie Rzymskim, nad którym zaczęli pracować międzynarodowi eksperci prawa karnego. W 2010 r. Statut został nowelizowany, dodano do niego termin „zbrodnie agresji", ale pojęcie ekocydu nadal nie otrzymało statusu prawnego jako przestępstwo międzynarodowe.

Higgins prowadziła trwającą dekadę kampanię na rzecz uznania ekocydu za zbrodnię przeciwko ludzkości. Organizacja Eradicating Ecocide, założona również przez Higgins, swego czasu wykonała przełomowe prace na rzecz stworzenia międzynarodowego prawa ekocydu. Na stronie internetowej StopEcocide.earth Polly Higgins podkreślała, że zniszczenie Ziemi jest przestępstwem i powinno być ścigane.

Chociaż do dziś ekocyd nie został uznany prawnie, to jego znaczenie z dnia na dzień wzrasta w związku z → k r y z y s e m klimatycznym i ilością niepodważalnych dowodów, że duże firmy lobbują przeciwko polityce, która mogłaby chronić ludzi przed zanieczyszczeniami i innymi szkodami dla klimatu i środowiska.

W celu kształtowania jednolitego systemu prawa międzynarodowego zapobiegającego ekologicznym przestępstwom, które można określić pojęciem ekocydu, społeczna organizacja Extinction Rebellion apeluje do społeczeństwa i rządzących, domagając się ogłoszenia alarmu klimatycznego, postulując, żeby rząd wraz z mediami i szkołami miał obowiązek informowania i edukowania o → z a g r o ż e n i a c h [t. 4] wynikających z ocieplenia klimatu i niszczenia środowiska naturalnego, oraz wymagając pełnego i wyczerpującego informowania społeczeństwa o działaniach, które w związku z tym muszą zostać podjęte przez państwo, obywateli, samorządy i przedsiębiorstwa. Działacze podkreślają, że polityka klimatyczna musi być oparta o aktualny stan wiedzy naukowej. Domagają się również, by władze wszystkich państw natychmiast rozpoczęły skuteczne

działania prawne i polityczne prowadzące do redukcji emisji gazów cieplarnianych i osiągnięcia neutralności węglowej w 2025 r., a także aby reformy gospodarki poszły w takim kierunku, by zasoby odnawialne były eksploatowane w tempie pozwalającym na ich całkowite odtwarzanie się.

Przedstawiciele Extinction Rebellion domagają się powołania Panelu Obywatelskiego, którego zadaniem będzie wypracowanie wiążących dla rządu rozwiązań. Rządy nie są wystarczająco zdeterminowane do podejmowania zdecydowanych, szybkich i długoterminowych działań. Przeciwdziałanie oraz zwalczanie skutków kryzysu klimatycznego wymaga wysiłku całego społeczeństwa o dotychczas niespotykanej skali i intensywności, dlatego niezbędne jest włączenie społeczeństwa do podejmowania kluczowych decyzji niezbędnych dla ratowania życia na Ziemi.

Społeczeństwa potrzebują zaangażowania systemowego, większego uwzględnienia spornych kwestii w procesach legislacyjnych, co z kolei otworzy drzwi ku uznaniu ekocydu w kategoriach prawnych. Ustanowienie tej kategorii jako zbrodni okrucieństwa na mocy prawa międzynarodowego spowodowałoby, że osoby na różnych poziomach odpowiedzialności podlegałyby ściganiu karnemu jako osoby fizyczne. W ten sposób dyrektorzy generalni i ministrowie mogliby być ukarani więzieniem za spowodowanie lub przyczynienie się do masowej lub systematycznej szkody i zniszczenia ekosystemów, tak jak zrobiliby to, gdyby nakazali masakrę lub zezwolili na nią.

Obecny system prawny, w którym postrzega się ludzi jako mających większą wartość moralną niż zwierzęta i świat przyrody, wynika z takiego typu kultury, w której priorytetem jest niekontrolowany wzrost i zysk. Istnieje jednak wiele społeczeństw, populacji i społeczności, których cała kultura i źródła utrzymania są zakorzenione w zupełnie innej kosmologii, najczęściej są to te, które działają w bliskim sąsiedztwie i wzajemności ze światem przyrody. We współczesnym świecie często pomija się fakt, że ekocyd zagraża nie tylko różnorodności biologicznej i siedliskom przyrodniczym, ale także ludziom, ich praktykom gospodarczym i kulturowym.

Kryminalizacja ekocydu na poziomie międzynarodowym wymaga, aby państwa będące stronami Statutu Rzymskiego zaproponowały na forum międzynarodowym włączenie ekocydu do listy istniejących najpoważniejszych przestępstw. Mechanizm zmian prawa międzynarodowego

dotyczącego ekocydu jest procesem odpowiedzialnym. Zmiany w Statucie muszą zostać zaproponowane, przyjęte i ratyfikowane zgodnie jego z art. 121 i 122. Procedura implementacji zmian przewiduje, że jedno państwo sygnatariusz statutu może zaproponować włączenie ekocydu jako przestępstwa. Każde państwo członkowskie może zaproponować poprawkę, a po 3 miesiącach ewentualnej dyskusji potrzeba zwykłej większości członków obecnych do przegłosowania. Przy liczbie 122 państw, które ratyfikowały Statut Rzymski, potrzeba pozytywnego głosu 82 państw, aby poprawka została przyjęta.

Jeszcze w 1992 r. amerykańscy naukowcy M. Feshbach i A. Friendly Jr. w monografii *Ecocide in ZSRR: Health and Nature Under Siege* wprost napisali:

> Kiedy historycy dokonają wreszcie rozcięcia trupa zmarłego Związku Radzieckiego i radzieckiego komunizmu […], to możliwe, że przyczyną śmierci nazwą oni zabójstwo natury. Dla nowej ery to będzie bezprecedensowy […], ale wiarygodny wniosek. Żadna inna cywilizacja przemysłowa nie zatruwała tak długo i na tyle planowo swojej ziemi, powietrza, wody i narodu. Nikt, na tyle głośno deklarując swoje wysiłki w doskonaleniu systemu ochrony zdrowia i ochrony natury, nie doprowadził do takiego nędznego stanu i jednych, i drugich. [ZSRR – przyp. aut.] doprowadził siebie do nędzy, poddając zagrożeniu zdrowie swoich obywateli, przede wszystkim dzieci i pracowników, żyzność swoich gleb i czystość swojego powietrza i wód. To zagrożenie z kolei podważa przyszłość odnowienia gospodarki, nawet jeśli radykalne reformy ekonomiczne powiodą się. Koszty oczyszczania zdolne wyeliminować astronomiczne resursy, potrzebne do budowy mieszkań, szpitali, dróg, elektrowni i systemów dostarczania wody, modernizacji przemysłu i rolnictwa, nie mówiąc już o czasie, który potrzebny jest, by zlikwidować skutki dziesięcioleci barbarzyńskiego obchodzenia się ze środowiskiem naturalnym […]. W najlepszym przypadku, żeby skompensować szkodę, której doznały tylko dwa najważniejsze rodzaje resursów – przyroda i zdrowie ludzkie, nowe państwa będą zmuszone w okresie pomiędzy rokiem 1990

> a 2015 zainwestować zasoby, które wielokrotnie przekraczają wielkość PKB ZSRR za 1990 r. […].W sytuacji nieprzeprowadzenia takiej akcji uzdrowienia zaniechany już i tak stan środowiska nadal będzie powodować dodatkowe komplikacje w osłabionym systemie ochrony zdrowia.

Analiza nielicznych prac dotyczących niezwykłej aktualności badań problemów ekologicznych nawet w ostatnich czasach nie przybrała na sile w krajowych podejściach naukowych. Bardzo mało jest takich prób w dziedzinie nauk społecznych i w państwach Europy Środkowo-Wschodniej. Po raz pierwszy decydującą rolę bodźców politycznych w genezie oraz stanie współczesnego kryzysu ekologicznego, skalę antropotechnicznej presji, jej źródła, współczesne przejawy jej procesów i tendencji w różnych regionach Ukrainy, niejednorodność oraz wzajemne uzależnienie wskaźników socjalno-ekologicznego kryzysu systemowo pokazano w monografii S. Wasiuty *Radziecki ekocyd w Ukrainie: historyczne źródła, trudności likwidacji* oraz dwutomowej monografii S. Wasiuty, O. Wasiuty i G. Filipczuka *Ekologia i polityka*. Ukoronowaniem wieloletnich doświadczeń i wysiłku badawczego w dziedzinie ekologii w Ukrainie stała się 4-tomowa monografia *Ekologiczna polityka: narodowe i globalne realia*, publikowana w latach 2003–2004. S. Wasiuta, O. Wasiuta oraz G. Filipczuk po raz pierwszy poddali systemowej analizie rolę politycznych bodźców genezy i współczesnego stanu kryzysu ekologicznego w kontekście narodowych i globalnych realiów, tendencji i perspektyw polityczno-ekologicznych. Przytoczone przykłady udowadniają potrzebę upowszechniania wiedzy ekologicznej, głębokiej analizy problemów ekologicznych za pomocą metod nauk społecznych i argumentacji jej wyników, warunkują konieczność rozwoju i integracji ekologii społecznej oraz ekologii historycznej do bardzo szerokiego kręgu dyscyplin naukowych, wykorzystywania wyników ich badań do analizy systemowej genezy, stanu i perspektyw wpływu antropotechnicznego i stosunków społeczeństwa ludzkiego i środowiska przyrodniczego.

Przybierają na znaczeniu różne sposoby pokojowego wywierania społecznej presji w celu uznania ekocydu za przestępstwo międzynarodowe. Ekocyd za przestępstwo został uznany w kodeksach karnych 10 krajów,

są to: Wietnam (1990, art. 278 kk); Federacja Rosyjska (1996, art. 358 kk); Kazachstan (1997, art. 161 kk); Kirgistan (1997, art. 374 kk); Tadżykistan (1998, art. 400 kk); Gruzja (1999, art. 409 kk); Białoruś (1999, art. 131 kk); Ukraina (2001, art. 441 kk); Mołdawia (2002, art. 136 kk); Armenia (2003, art. 394 kk). Np. w art. 441 Kodeksu karnego Ukrainy z dn. 5 kwietnia 2001 r. ze zmianami z dn. 7 kwietnia 2013 r. „ekocyd" uważany jest za przestępstwo i został zdefiniowany jako:

> masowe zniszczenie świata zwierzęcego lub roślinnego, trucie atmosfery lub zasobów wodnych, a także popełnienie innych czynów, które mogą spowodować katastrofę ekologiczną, podlega karze pozbawienia wolności od lat 8 do 15 lub dożywotniego pozbawienia wolności.

Warto zauważyć, że w większości kodeksów karnych wymienionych krajów zbrodnia ekocydu jest zdefiniowana jako masowe niszczenie fauny i flory, zanieczyszczenie atmosfery lub zasobów wodnych, a także inne działania mogące doprowadzić do katastrofy ekologicznej, stanowią one zbrodnię przeciwko pokojowi i bezpieczeństwu ludzkości, obok 4 międzynarodowych zbrodni przeciwko pokojowi.

Aktywiści w celu tworzenia międzynarodowego prawa ekocydu proponują połączyć siły w misji zapobiegania ekobójstwu, zachęcają do zaangażowania poprzez przyjęcie funkcji protektora Ziemi. Np. w Australii, aby wesprzeć realne działania potępiające fakty ekocydu i promujące prawa przyrody, proponuje się zostać członkiem Australian Earth Laws Alliance (AELA), wspierać Australijski Trybunał Ludowy ds. Społeczności i Praw Natury oraz Australijskie Centrum Praw Natury, a także wspomagać tworzenie przepisów dotyczących ekocydu.

W historii znanych jest wiele przypadków ekocydu militarnego:

- W IV w. p.n.e. jeden z „siedmiu mędrców" starożytnej Grecji, Solon, podczas oblężenia Kirry zatruł rzekę, co doprowadziło do masowej śmierci obrońców miasta. Fakty zatrucia wody znane są również w starożytnym Rzymie (podczas walki z rzymskimi legionami niemieccy wojownicy specjalnie zatruwali wodę w studniach, aby zmniejszyć liczbę rzymskich → ż o ł n i e r z y [t. 4]).

- Podczas I wojny światowej wojska niemieckie jako pierwsze wykorzystały w 1915 r. w pobliżu miasta Ypres (Belgia) →broń chemiczną [t. 1] masowego rażenia przeciwko swoim wrogom, Francuzom i Anglikom. Oprócz zabójczego działania na żołnierzy, chemikalia miały również fatalny wpływ na środowisko.
- Podczas II wojny światowej niemieccy najeźdźcy masowo wywozili pociągi żyznej czarnej ziemi z północnej i wschodniej Ukrainy. W rezultacie nieodwracalnie została uszkodzona fauna glebowa na dużych obszarach, zmniejszyła się żyzność gleby.
- Podczas wojny w Wietnamie amerykańskie myśliwce rozpyliły ponad 100 tys. ton defoliantów na Kambodżę i Wietnam. Skład tych chemikaliów zawierał arborycydy (środki chemiczne stosowane do niszczenia krzewów i drzew) oraz dioksyny. Związki te miały druzgocący wpływ na indochińskie dżungle. Z powodu użycia ich prawie połowa gruntów ornych w Wietnamie została wyprowadzona z użycia; zniszczono 2 mln ha lasów, wyginęło 2/3 gatunków ptaków i zwierząt.
- Podczas wojny w Zatoce Perskiej siły rządowe Iraku celowo podpaliły 1200 pól naftowych, szereg składów ropy i tankowców. Produkty spalania uderzyły w atmosferę, glebę i ocean światowy, powodując niespotykane zanieczyszczenie środowiska.
- W 2004 r. wojska amerykańskie wykorzystały amunicję fosforową do bombardowania irackiego miasta Al-Falludża, które spowodowało nie tylko masową śmiertelność ludzi, ale także katastrofalne zanieczyszczenie otaczającej gleby związkami fosforu.

Zgodnie z prawem międzynarodowym akty te mieszczą się w definicji „wojennego ekocydu".

Jednym z klasycznych przykładów ekocydu był wyciek ropy w Zatoce Meksykańskiej w kwietniu 2010 r. na platformie wiertniczej Deepwater Horizon, która eksplodowała, tragicznie zabijając 11 pracowników i skutkując wyciekiem do morza tysięcy baryłek ropy dziennie przez kilka miesięcy. Wyciek ropy zabił także setki gatunków ptaków, ryb i ssaków oraz wpłynął na źródła utrzymania tych, którzy mieszkali na lądzie i łowili ryby w okolicy. Klęska spowodowała trwałe szkody w lokalnym ekosystemie. Śmiertelność delfinów znacznie wzrosła. Straty ptaków morskich

mogły być liczone w setkach tysięcy, również bezkręgowce zostały mocno dotknięte problemem. Pojawiły się również doniesienia o zdeformowanej faunie po wycieku. Ponad 1 tys. mi² wybrzeża Zatoki Meksykańskiej zostało uszkodzonych.

Skutki długoterminowe nie są jeszcze znane, koszty środowiskowe wycieku są zaś nadal oceniane. Firma naftowa odpowiedzialna za te szkody – BP – już wydała ponad 13,7 mld GBP na grzywny. Najnowsze dane potwierdzają, że wyciekło ok. 3,19 mln baryłek ropy, a wyciek już kosztował firmę 42 mld GBP. Obecnie nasilają się protesty społeczności międzynarodowej, aby przerwać wiercenia naftowe w Arktyce, gdzie warunki morskie są bardziej surowe i niebezpieczne. Arktyka już cierpi z powodu zmian klimatu i globalnego ocieplenia. Kopalnie niklu w arktycznym regionie Szwecji zatruwają dawne pastwiska społeczności Saamów i zagrażają ich egzystencji.

22 stycznia 2013 r. w Parlamencie Europejskim oficjalnie uruchomiono europejską inicjatywę obywatelską End Ecocide in Europe (Zakończmy Ekocyd w Europie), której celem jest obrona prawa obecnych oraz przyszłych pokoleń do życia w zdrowym środowisku. Inspiracją do powstania inicjatywy było wystąpienie międzynarodowej prawniczki P. Higgins, która zaproponowała uznanie ekocydu (ekobójstwa) za piątą zbrodnię przeciwko pokojowi. Po wprowadzeniu takiej zmiany ekobójstwo byłoby nielegalne na całym świecie i jeśli ktokolwiek próbowałby ten porządek naruszyć, byłby rozliczany wg prawa karnego. Przestępstwa przeciwko środowisku, takie jak zanieczyszczenie zbiorników wodnych czy niszczenie ekosystemów, mogą być postrzegane jako zbrodnie przeciwko ludzkości.

Obecny → r e ż i m [t. 3] prawny pozwala państwom i korporacjom bezkarnie ograbiać środowisko. Ta niesprawiedliwość zainspirowała nowy ruch ekspertów prawnych i obywateli wzywających do kodyfikacji ekobójstwa jako piątej zbrodni przeciwko pokojowi. Ich praca ma na celu przekształcenie rozumienia natury jako własności w postrzeganie jej jako równorzędnego partnera w budowaniu trwałych społeczeństw. Przeszkody polityczne i przeszkody w egzekwowaniu prawa są ogromne, ale zaangażowani obywatele, wzmocnieni porozumieniem klimatycznym z Paryża, mogą okazać się wystarczająco silni, aby podnieść kwestię

zapobiegania przestępstwom przeciwko naturze do uznanej na całym świecie normy.

Reasumując, pomimo istnienia wielu umów międzynarodowych – kodeksów i regulacji postępowania, rezolucji ONZ, traktatów, konwencji, protokołów itd. – szkody w środowisku są coraz większe i coraz bardziej dotkliwe. Żadna z istniejących umów międzynarodowych definitywnie nie zabrania ekocydu, który ma coraz większy wpływ na wszystkie formy życia, włącznie z ludzkim. Potrzebne jest zatem radykalne rozszerzenie zbiorowego społecznego obowiązku i monitoringu, aby chronić środowisko naturalne i jego bioróżnorodność. Międzynarodowy system prawa ekologicznego musi być prawem chroniącym wszystkie formy życia na Ziemi. Tylko w ten sposób można zmienić świat w skali lokalnej i globalnej, wyegzekwować prawo obrony życia.

Sergiusz Wasiuta

F. Broswimmer, *Ecocide: A Short History of Mass Extinction of Species*, Pluto Press, London 2002; A.D.C. Cherson, *Ecocide: Humanity's Environmental Demons*, Greencore, New York 2009; *Citizen Campaign to End Ecocide in Europe*, 22.01.2013, EnviroSecurity.org (dostęp 30.03.2020); J. Diamond, *Collapse: How Societies Choose to Fail or Succeed*, Penguin Books, London 2005; M. Feshbach, A. Friendly, *Ecocide in USRR: Health And Nature Under Siege*, Basic Books, New York 1992; A. Gauger, M. Pouye Rabatel-Fernel, L. Kulbicki i in., *The Ecocide Project: Ecocide is the missing 5th Crime Against Peace*, Human Rights Consortium, 2013; P. Higgins, *Eradicating Ecocide: Laws and Governance to Prevent the Destruction of our Planet*, Shepheard-Walwyn, London 2010; *Making Ecocide a Crime*, StopEcocide.earth (dostęp 30.03.2020); O. Wasiuta, S. Wasiuta, G. Filipczuk, *Ekolohija i polityka*, t. 1–2, Wydawnictwo Zielona Bukowina, Czerniowce 1998; ciż, *Ekologiczna polityka: narodowe i globalne realia*, t. 1–4, Wydawnictwo Zielona Bukowina, Czerniowce 2003–2004; S. Wasiuta, *Development of History-Ecological Education in a Context of Global Imperatives and Educational Transformations*, [w:] *International Transfer of Higher Education*, t. 1, R. Brazis (ed.), Vilnius 2006; tenże, *Międzydyscyplinarne historyczno-ekologiczne badania przestrzeni Ukrainy: historiograficzna analiza genezy i rozwoju*. „Społeczeństwo i Polityka" 2012, nr 4 (33); tenże, *Radziecki ekocyd w Ukrainie: historyczne źródła, trudności likwidacji*, Wydawnictwo Aston, Tarnopol 2000; tenże, *Ukraine before and after Chernobyl: Social and Medical Aftermath of the Disaster in Chernobyl as a Result of Soviet Ecological Policy*, [w:] *Globalne i regionalne problemy ochrony*

środowiska, W. Pawlak, T. Noch (red.), Gdańska Wyższa Szkoła Administracji, Gdańsk 2006; J. Watts, *Make environmental damage a war crime, say scientists*, 24.07.2019, TheGuardian.com (dostęp 30.03.2020); F. Wijdekop, *Against Ecocide: Legal Protection for Earth*, Great Transition Initiative, 2016.

EKOLOGIA INFORMACJI (ang. *information ecology*) – dyscyplina wiedzy zajmująca się wzajemnym oddziaływaniem → i n f o r m a c j i na ludzi i odwrotnie; oznacza związek między ideami ekologicznymi z dynamiką i właściwościami coraz bardziej gęstego, złożonego i ważnego cyfrowego → ś r o d o w i s k a i n f o r m a c y j n e g o [t. 4], zyskuje akceptację w coraz większej liczbie dyscyplin. Pojęcie jest często używane jako metafora, ujmująca → p r z e s t r z e ń i n f o r m a c y j n ą [t. 3] jako ekosystem. Ekologia informacji to również nauka, która bada prawa rządzące wpływem informacji na tworzenie i funkcjonowanie biosystemów, w tym ludzi, społeczności ludzkich i ogólnie ludzkości oraz na zdrowie i psychiczne, fizyczne i społeczne samopoczucie człowieka i która zajmuje się opracowaniem metodologii poprawy środowiska informacyjnego.

Ekologia informacji jest dyscypliną multidyscyplinarną umiejscowioną przez W. Babika w ramach informacji naukowej i podobnie jak → k u l t u r a i n f o r m a c y j n a czy koncepcja *information literacy* reprezentuje nowoczesne pola badawcze informatologii. Związek ekologii informacji z kulturą informacyjną jest szczególnie ścisły, np. w obszarze profilaktyki → c h o r ó b i n f o r m a c y j n y c h [t. 1] i przeciwdziałania → z a g r o ż e n i o m [t. 4] cywilizacyjnym wynikającym z funkcjonowania człowieka w → s p o ł e c z e ń s t w i e i n f o r m a c y j n y m [t. 4]. E. Głowacka stwierdza nawet, że „potrzeba rozwoju kultury informacyjnej w środowisku informacyjnym zapoczątkowała powstanie i rozwój […] ekologii informacji".

Według rosyjskiego teoretyka A.L. Eryomina z Centrum Kultur Narodowych w Krasnodarze w Rosji zadaniem ekologii informacji jest odkrywanie praw rządzących przepływem informacji w biosystemach, włącznie z człowiekiem, społeczeństwem, ich wpływem na zdrowie psychiczne, fizyczne i społeczne ludzi oraz rozwijanie odpowiednich metodologii mających na celu kształtowanie środowiska informacyjnego. Ekologię informacji odnosi do identyfikacji ilościowych i jakościowych kryteriów oceny informacji, sposobów zarządzania nią w miejscu pracy,

w organizacjach, w społecznościach bogatych i ubogich w informacje oraz w społeczności światowej, a także do produktów powstających w wyniku procesu informacyjnego, do wartości informacji oraz potrzeb i usług informacyjnych. Przedmiotem tej dyscypliny są relacje pomiędzy informacją a człowiekiem jako jej użytkownikiem, przejawiające się w postaci różnego rodzaju interakcji informacyjnych i komunikacyjnych, a jej celem jest wypracowanie środków pozwalających na regulację przepływu informacji w sposób korzystny dla zdrowia jednostek i grup, np. opanowanie emocjonalnego → przeciążenia informacyjnego [t. 3] (trafność, domniemana objętość, stronniczość), kształtowanie → świadomości informacyjnej [t. 4] i odpowiedzialności społecznej za informacje wprowadzane do obiegu. W relacji tej akcent położony jest na informację, którą należy chronić tak, jak chroni się środowisko przyrodnicze. Oznacza to, że ekologia informacji daje nie tylko możliwość ukazania społecznych i ekonomicznych zagrożeń wynikających z rozwoju techniki, ale też wskazuje sposoby przeciwdziałania tym zagrożeniom i potrzebę podjęcia walki przez człowieka o jego byt w → infosferze. Eryomin zaproponował podział ekologii informacji na:

- ekologię informacyjną odnoszącą się do polityki;
- ekologię informacji międzynarodowej;
- ekologię informacji w kontekście ekonomii;
- ekologię lingwistyki informacyjnej;
- ekologię informacji publicznej;
- ekologię mediów;
- ekologię informacji w aspekcie fizjologii, medycyny i higieny;
- ekologię informacji ludzkiej.

Polski badacz tych problemów Babik definiuje ekologię informacji jako:

> domenę badawczą dotyczącą wzajemnych oddziaływań człowieka na informację i odwrotnie, a także relacji informacyjnych między ludźmi w publicznej i prywatnej przestrzeni informacyjnej oraz wpływu na nie środowiska informacyjnego. Jej przedmiotem jest struktura i funkcjonowanie środowiska informacyjnego człowieka.

Do podstawowych czynników ekologicznych mających wpływ na rozwój człowieka uczestniczącego w procesie informacyjnym zalicza: drugiego człowieka, władzę, technologie informacyjne, masowe środki przekazu, informację naukowo-techniczną, internet itd. Aby uczestniczyć w działaniach na rzecz ekologii informacji, każdy człowiek powinien mieć rozwiniętą świadomość informacyjną i dysponować kompetencjami umożliwiającymi racjonalne zarządzanie informacją, zapanowanie nad nadmiarowością informacji, uniezależnienie się od niepożądanych wpływów informacji i wykorzystywania jej jako narzędzia manipulacji ludzkimi postawami i zachowaniami, bycie odpowiedzialnym za jej tworzenie, przetwarzanie i rozpowszechnianie, podejmowanie działań w zakresie →zrównoważonego rozwoju [t. 4] człowieka w świecie techniki i informacji, który nie jest aksjologicznie obojętny, wykorzystanie informacji do budowania wiedzy dla wspólnego dobra ludzkości.

Podsumowując, do zadań ekologii informacji należy „zapewnienie wartościowego, bezpiecznego i dobrze zorganizowanego dostępu do informacji i wiedzy", etyczne wykorzystanie informacji i →technologii informacyjno-komunikacyjnych [t. 4], racjonalne uczestniczenie w procesie informacyjnym, niedopuszczenie do powstawania informacji niespełniającej norm jakościowych, ochrona społeczeństwa przed zagrożeniami wynikającymi z nadprodukcji informacji generowanej przez cywilizację techniczną, poprawa i usprawnianie funkcjonowania człowieka w środowisku informacyjnym itp. Ekologia informacji nawiązuje także do eutyfroniki, filozofii trudu, zasady prostomyślności. Można wskazać zarówno jej kontekst psychologiczny związany z przeciwstawianiem się zagrożeniom związanym z funkcjonowaniem jednostki w cywilizacji technologicznej, np. ze stresem informacyjnym, alienacją lub przymusem bycia w sieci, jak też kontekst techniczny nawiązujący do walki z →cyberprzestępczością [t. 1], utratą danych, kontekst prawny dotyczący →ochrony własności intelektualnej w sieci [t. 3], czy kontekst medyczny obejmujący działania profilaktyczne w zakresie przeciwdziałania szkodliwemu oddziaływaniu komputera na zdrowie człowieka. Dbałość o informację i jej użytkowników należy wg K. Materskiej do podstawowych zadań ekologii informacji.

W literaturze do najbardziej znanych sposobów ochrony antropoinfosfery należą koncepcje zaproponowane przez takich badaczy jak R. Cappuro, L. Floridi, B.A. Nardi, V.L. O'Day, T. Davenport, L. Prusak czy A.L. Eryomin.

W pragmatycznej koncepcji Cappura ekologia informacji postrzegana jest jako równowaga między ludzkim myśleniem a działaniem, uwzględniającym różne technologie komunikacyjne do przekazywania informacji w otoczeniu człowieka. Jej główne zadania koncentrują się wokół wytwarzania zgodnych relacji pomiędzy ludźmi i technologią, ochrony informacji, kształcenia postaw zgodnych z wyznawanymi wartościami i charakteryzujących zachowania dojrzałych informacyjnie użytkowników, rozpatrywania informacji w szerokim kontekście społecznym. Ekologia informacji w tym modelu traktowana jest jako rodzaj higieny informacyjnej, której zadaniem jest ochrona społeczeństwa przed zagrożeniami występującymi w jego środowisku informacyjnym, do których zalicza w pierwszej kolejności podział ludzkości na grupy mające i niemające dostępu do informacji. Zatem głównym celem ekologii informacji w tej koncepcji jest walka z wykluczeniem technologicznym i informacyjnym w skali globalnej.

Natomiast aksjologiczna koncepcja ekologii informacji, wypracowana przez Floridiego, skoncentrowana jest wokół zasad etycznych dotyczących pozyskiwania, wymiany i dostępu do informacji. Można ją uznać za deklaratywną, bowiem, jak konkluduje Babik, etyczne korzystanie z narzędzi TIK ma gwarantować użytkownikom tych technologii (ale też korzystającym z informacji analogowej) przekształcenie infosfery w „otwarte na użytkowników miejsce wymiany bezpiecznych i sprawdzonych informacji, w którym zachęca się do komunikacji i współpracy, a wolność słowa gwarantuje dostęp do informacji dla każdego bez wyjątku".

Wartościująca koncepcja ekologii informacji Nardi i O'Day krytykowana jest za jej utopijność z powodu odrzucania możliwości występowania wśród uczestników ekologii informacji także postaw nieetycznych i zachowań szkodliwych dla całego ekosystemu. W tej koncepcji zasadnicze znaczenie odgrywa kontekst aksjologiczny. Stosunki międzyludzkie normowane są poprzez wyznawane wartości.

Organizacyjna koncepcja ekologii informacji Davenporta i Prusaka uwypukla jej związek z zarządzaniem informacją. Cytując za Babikiem,

ekologia ta rozumiana jest jako „sposób zarządzania przez ludzi informacją w firmie i jest skoncentrowana na człowieku, a nie na technologii". W odniesieniu do badania otoczenia informacyjnego organizacji wg tej koncepcji uwzględnione powinny być następujące elementy: misja organizacji; cele, którym ma służyć zarządzanie informacją; plany zarządzania informacją; kultura informacyjna organizacji; → polityka informacyjna [t. 3]; fizyczna lokalizacja zasobów, pracowników informacji oraz kierowania informacją. Materska akcentuje fakt, że koncepcja ta wyróżnia się kładzeniem nacisku na efektywne wykorzystanie stosunkowo niedużej ilości informacji, co sprzyja odpowiedzialności pracowników za jej wykorzystanie. Stawianie pracowników w sytuacji nadmiarowości informacji i żądanie podejmowania trafnych wyborów nie przynosi spodziewanych efektów. Zatem kultura informacyjna winna być postrzegana nie tylko jako zabezpieczenie sprawnego przepływu informacji w firmie w celu zapewnienia jej rozwoju, a nawet ekspansji, ale jako kultura informacyjna pracowników, których świadomość informacyjna pozwala odróżnić działania firmy przyjazne lub szkodliwe dla środowiska informacyjnego człowieka. Dlatego Davenport i Prusak, proponując model ekologicznego zarządzania informacją, opowiadają się za koniecznością ochrony infosfery przed wszystkimi chorobami informacyjnymi, które generuje współczesna cywilizacja.

Każda z wymienionych koncepcji ekologii informacji może być wykorzystywana w tworzeniu polityki przeciwdziałania zagrożeniom środowiska informacyjnego. Współcześnie świadomość istnienia chorób informacyjnych jest w społeczeństwie duża, ale łączy się z bagatelizowaniem skutków, jakie mogą one wywoływać, i możliwością przekształcenia się w swoiste epidemie w przypadku niepodjęcia z nimi walki. Choroby informacyjne definiowane są jako fizyczne i psychiczne niedomagania człowieka, które są wywoływane przez informacje docierające do człowieka z zewnątrz i łączą się ze źle zorganizowanym przepływem informacji. Do ich powstania mogą się przyczynić zarówno nadawcy, jak i odbiorcy informacji. Babik do najbardziej uciążliwych chorób informacyjnych zalicza: stres informacyjny, pośpiech informacyjny, frustrację informacyjną, natłok informacji, przeciążenie informacyjne, samotność informacyjną, manipulowanie informacją, sterowanie

informacją, urojenia informacyjne, bulimię informacyjną (chroniczny głód informacji), anoreksję informacyjną (brak łaknienia informacji) oraz cały zestaw niewłaściwych reakcji człowieka w trakcie korzystania z informacji związanych z brakiem odpowiedzialności za tworzone i rozpowszechniane informacje, z bezkrytycznym i tendencyjnym odbiorem informacji, z niewłaściwym rozumieniem komunikatów, z fragmentarycznym przekazywaniem wiadomości itp.

Z chorobami należy walczyć, ale lepiej im zapobiegać, zanim zaatakują infosferę. Ekonomika informacji koncentruje się na eliminacji informacji niespełniającej norm jakości, psychologia walczy ze stresem informacyjnym, ekologia zabiega o zrównoważony rozwój środowiska informacyjnego człowieka, wychowanie informacyjne koncentruje się na przygotowaniu do godnego życia w świecie ryzyka i katastrof, nauka o informacji rozwija świadomość informacyjną jednostek funkcjonujących w społeczeństwie informacyjnym, kultura informacyjna staje się narzędziem profilaktyki zagrożeń generowanych przez cywilizację techniki poprzez kształcenie dojrzałości informacyjnej, edukacja informacyjna wyposaża jednostkę w kluczowe kompetencje nieodzowne do przetrwania w społeczeństwie informacyjnym (*information literacy*), eutyfronika pozwala bronić psychikę człowieka przed zniewoleniem ze strony techniki i światopoglądu technokratycznego, technologia informacyjna ułatwia sprawne zarządzanie informacją w sytuacji jej natłoku i chaosu informacyjnego. Edukacja dla ekologii informacyjnej jest więc edukacją opartą na kulturze informacyjnej jednostki. Dlatego na kulturę informacyjną należy patrzyć z punktu widzenia potrzeb ekologii informacji. Oznacza to poszukiwanie w szeroko rozumianej kulturze elementów i związków pomiędzy nimi, które z jednej strony pozwalają zabezpieczyć się przed chorobami informacyjnymi, a z drugiej pozwalają chronić informację przed szkodliwym działaniem człowieka. Podejście to dotyczy zatem relacji między człowiekiem a środowiskiem informacyjnym, wskazując, jak kulturalnie i roztropnie zarządzać informacją. Do ważnych elementów kultury informacyjnej w kontekście ekologii informacji Babik zalicza: umiejętność obserwacji zmian w otaczającym środowisku informacyjnym, gromadzenie o nim informacji, dążenie do rozumienia tych zmian. Wiedza i zrozumienie mają wykształcić w człowieku poczucie odpowiedzialności za to środowisko. Dlatego rozpatrując

kulturę informacyjną z ekologicznego punktu widzenia, należy założyć, że „środowisko informacyjne jest decydującym czynnikiem w analizach zjawisk społecznych i wpływa na kulturę informacyjną człowieka".

Kształtowanie tego środowiska wymaga edukacji informacyjnej obywateli i kształtowania umiejętności brania odpowiedzialności, ponoszenia odpowiedzialności i bycia odpowiedzialnym za działania podejmowane w środowisku informacyjnym. Połączenie edukacji informacyjnej z wychowaniem do informacji może wspomagać rozwój zarówno jednostki, jak i społeczeństwa. Stąd konieczność opracowania kanonu wykształcenia informacyjnego, w którym „potrzeby człowieka i prymat człowieka, a nie prymat techniki czy cywilizacji informacyjnej" będzie podstawowym celem przygotowania jednostki do życia w cywilizacji technologicznej w taki sposób, aby chciała ona i dążyła do dobra drugiego człowieka. Tylko wówczas środowisko informacyjne nie będzie zagrożone, a człowiek osiągnie w nim zrównoważony rozwój. Wychowanie informacyjne należy zatem rozumieć także w kontekście wychowania do ekologii informacji.

Wychowanie do informacji jest więc nieodzowne w przygotowaniu człowieka do roztropnego funkcjonowania w środowisku społecznym, w którym zapotrzebowanie na informację wynika wg L. Korporowicza i S. Jaskuły z trzech wzajemnie warunkujących i dopełniających się procesów, tj. z procesu globalizacji, procesów gospodarczych uzależnionych od globalizacji i procesu dynamicznego rozwoju technologii, szczególnie informacyjno-komunikacyjnych. Procesy te wymienieni badacze antropologii informacji nazywają makrokontekstem, który „generuje genezę, charakter i życie informacji jako czynnika ogarniającego wszystkie czynności współczesnego człowieka w jego życiu prywatnym i publicznym, indywidualnym i zbiorowym" . Celem wychowania informacyjnego musi być przygotowanie jednostki do odpowiedzialnego funkcjonowania w tych trzech makrokontekstach współczesnego świata. W obszarze procesu globalizacji następuje wzmożona współzależność organizacji, grup i osób mająca konsekwencje w zapotrzebowaniu na coraz bardziej rozbudowane zasoby informacji. Z kolei nasilenie zjawisk interakcji społecznych powoduje wzrost znaczenia informacji, np. w zakresie polityki socjalnej, edukacyjnej, samorządowej, a wzrost intensywności i znaczenia procesów komunikacji społecznej „wytwarza kolejny

obszar cywilizacyjnego głodu informacji. W obszarze wyzwań wynikających z procesów gospodarczych człowiek musi wykształcić umiejętność równoważenia aktywnych stron współczesnej cywilizacji i postępować zgodnie z zasadą równoważenia procesów, zasobów i potencjałów oraz bilansowania zagrożeń i szans rozwoju.

Ekologiczne podejście do środowiska H. Dauber uważa za jeden z ważnych obszarów „uczenia się w przyszłości". Wychowanie ekologiczne ma zatem prowadzić do wykształcenia takich zachowań, które będą uwzględniały problemy środowiska, a ekologiczne myślenie ma ograniczać te struktury, które zagrażają życiu i przeżyciu. Zasada zrównoważonego rozwoju jest trudna do pogodzenia z regułą współczesnej gospodarki, w której liczy się tylko jakość, skuteczność, efektywność, optymalizacja, kreatywność, innowacyjność i rozwój. Nieustający wyścig do osiągnięcia totalnego mistrzostwa w każdym sektorze działań człowieka powoduje eskalację zapotrzebowania na informację i traktowania jej jako strategicznego kapitału. Kolejny obszar dotyczy informacyjnych wyzwań nowej techniki i technologii. Charakteryzuje go zjawisko przyspieszenia technologicznego, którego konsekwencją jest nadmiarowość produkowanej informacji i przeciążenie informacyjne potencjalnych odbiorców. Nadprodukcja informacji i tempo ich przekazu prowadzą bezpośrednio do chronicznego stresu informacyjnego, powodowanego niemożnością ich selekcji, porządkowania i łączenia z dotychczasowym zasobem wiedzy. Warunkiem dalszego przyspieszenia staje się „nie tyle techniczna, ale mentalna ich dostępność, oswojenie z ich mnogością, różnorodnością i wszechobecnością, co czyni wychowanie do informacji niemal koniecznym komponentem procesu socjalizacji". Omówione procesy generują dylematy natury społecznej, kulturowej i etycznej, przed którymi staje współczesny człowiek. Ich rozstrzygnięcie w świecie płynnej nowoczesności nie jest łatwe, gdyż nie tylko zmienia się hierarchia dotychczasowych wartości, ale tracą swoje znaczenie także wartości uniwersalne.

Hanna Batorowska

W. Babik, *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014; tenże, *Ekologia informacji a bezpieczeństwo człowieka i informacji we współczesnym świecie*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; tenże, *Ekologia informacji katalizatorem równoważenia rozwoju społeczeństwa informacji i wiedzy*, „Zagadnienia Informacji Naukowej" 2012, nr 2; tenże, *Infologiczno-ekologiczne aspekty zrównoważonego rozwoju a dostęp społeczeństwa do informacji i wiedzy*, „Praktyka i Teoria Informacji Naukowej i Technicznej" 2009, nr 1–2; tenże, *Kultura informacyjna – spojrzenie z punktu widzenia ekologii informacji*, „Bibliotheca Nostra" 2012, nr 2; H. Batorowska, *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej*, Wydawnictwo SBP, Warszawa 2013; taż, *Kultura informacyjna*, [w:] *Nauka o informacji*, W. Babik (red.), Wydawnictwo SBP, Warszawa 2016; taż, *Refleksja nad kulturą informacyjną w ujęciu interdyscyplinarnym*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym*, t. 2, H. Batorowska, Z. Kwiasowski (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2016; R. Capurro, *Towards an information ecology*, [w:] *Information Quality Definitions and Dimensions. Proceedings of a NORDINFO Seminar, Royal School of Librarianship, Copenhagen, 1989*, I. Wormel (ed.), Taylor Graham, London 1990; M. Cieślarczyk, *Ekologia informacji, kultura informacyjna i kultura bezpieczeństwa informacyjnego w teorii i w praktyce*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; H. Dauber, *Obszary uczenia się w przyszłości. Perspektywa pedagogiki humanistycznej*, Oficyna Wydawnicza Impuls, Kraków 1997; A.L. Eryomin, *For Question of Development New Direction – Information Ecology. Ecology and Society's Development. 1-st International Conference. Abstracts*, Center of IAESVS, Sankt-Petersburg 1995; tenże, *Information Ecology – A Viewpoint*, „International Journal of Environmental Studies" 1998, no. 3–4, L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Cortina Raffaello, Milano 2017; H. Forest, *Information Ecology*, „Journal of Systems Management" 1978, vol. 29, no. 9; E. Głowacka, *Ekologia informacji – sposób na choroby informacyjne?*, „Forum Bibliotek Medycznych" 2009, vol. 2, nr 2 (4); S. Jaskuła, L. Korporowicz, *Wychowanie do informacji: wyzwania i nadzieje*, „Pedagogika Społeczna" 2008, nr 1 (27); K. Materska, *Ekologiczne zarządzanie informacją*, „Przegląd Informacyjno-Dokumentacyjny" 2005, nr 2 (289).

EKOTERRORYZM (czasem jako „zielony terroryzm") – forma → t e r r o r y z m u [t. 4] prowadzonego pod hasłami ochrony środowiska naturalnego, ochrony praw zwierząt lub fauny i flory w ogóle; określa również

szereg praktyk uważanych za nielegalne w ramach danego systemu legislacyjnego. Jest często definiowany jako użycie → p r z e m o c y [t. 3] w celu dalszej zmiany polityki ochrony środowiska. Termin jest dość kontrowersyjny. Ekoterroryści są gotowi wyrządzić ofiarom stres emocjonalny i fizyczny, jeśli wierzą, że przyczyni się to do realizacji ich celów. Ta radykalna wersja działań na rzecz ochrony środowiska jest niezgodna z prawem, można ją porównywać z ich umiarkowanym prekursorem, czyli ekoaktywizmem, który nie jest nielegalny i zostałby sklasyfikowany jako forma obywatelskiego nieposłuszeństwa wykorzystująca protesty i udział w innych aktywnościach w celu zmiany środowiska. Ekoterroryzm może również obejmować sabotaż w imię środowiska, co jest nielegalne, ponieważ obejmuje przestępstwa przeciwko mieniu, które mogą prowadzić do szkód dla ludzi. W USA definicja terroryzmu wg FBI obejmuje akty przemocy wobec własności, co powoduje, że większość aktów sabotażu można sklasyfikować w ramach terroryzmu wewnętrznego.

Ekoterroryzm to niezgodne z prawem, radykalne metody wywierania presji przez obrońców przyrody na rządy i przemysłowców w celu uzyskania konkretnych celów politycznych. Ekoterroryzm jest formą aktywności, której podłoże stanowi środowisko naturalne, a działania skierowane są na realizację aktów przestępczych o zróżnicowanym charakterze. Działania te najczęściej są wymierzone w gospodarkę, przedsiębiorców oraz konkretne podmioty i jednostki. Zjawisko to może przybierać rozmaite formy, a często inspiracją aktywności ekoterrorystów jest nie ochrona środowiska naturalnego, lecz motywacje natury politycznej, biznesowej, a nawet agenturalnej. Istotnym czynnikiem, pomijanym z powodu trudności dotyczących analizy aktów normatywnych oraz konkretnych przypadków naruszeń porządku prawnego, jest motywacja finansowa, która staje się coraz częstszym faktycznym powodem podejmowania działań o charakterze pseudoekologicznym. Korzyści uzyskiwane w ramach opisywanego procederu określane są mianem ekoharaczu.

Ekoterroryzm to stosowanie siły lub przemocy wobec ludzi, pośrednio również za pomocą niszczenia mienia do nich należącego. Akcje bezpośrednie prowadzone przez aktywistów można podzielić na akcje typu bez przemocy (ang. *non-violence*) oraz z użyciem przemocy (ang. *violence*). W typowych akcjach pierwszego typu używa się zastraszania, ale groźby

dotyczą z reguły nie użycia siły, a jedynie osłabienia czyjegoś wizerunku za pomocą ujawniania niewygodnych faktów. Ewentualne szkody w takich akcjach, jak np. niszczenie ogrodzeń, same w sobie nie są celem i służą wyłącznie dotarciu aktywistów do niedostępnych publicznie miejsc. Ekoterroryzm zaś jest ściśle związany z akcjami typu bezpośredniego użycia przemocy (ang. *violence direct action*), których celem jest fizyczne lub materialne zniszczenie. Takie akcje są stosowane przez skrajnie radykalne środowiska ekologiczne, które jako takie działają w ukryciu, nie tworzą formalnych grup i przypominają środowiska antysystemowe.

Różne źródła definiują ten termin nieco inaczej. Z punktu widzenia FBI z 2002 r. ekoterroryzm jest definiowany jako:

> bezprawne użycie gróźb lub grożenie przemocą o charakterze przestępczym wobec niewinnych ofiar lub ich mienia przez grupę lub osobę zajmujące się ochroną przyrody z powodów środowiskowo-politycznych lub skierowaną do odbiorców spoza grupy docelowej, często włączając działania symboliczne.

Według danych FBI w latach 2003–2008 ekoterroryzm powodował roczne straty w wysokości ok. 200 mln USD w samych USA, a od początku XXI w. takie działania i taktyki stały się społecznie niebezpieczne. Większość stanów USA wprowadziła przepisy mające na celu karanie ekologicznego terroryzmu.

Do opisu działań zwolenników ekoterroryzmu czasami jest używany termin ekosabotaż, który jest dość nowym pojęciem, spopularyzowanym przez amerykańskiego pisarza i eseistę, E.P. Abbeya (1927–1989), znanego z popierania kwestii ochrony środowiska, uzasadniał on zasadność ekosabotażu w powieści *The Monkey Wrench Gang* z 1975 r. Oznacza ukryte zniszczenie/uszkodzenie własności prywatnej np. poprzez wywołanie pożaru, w tym sprzętu przemysłowego i maszyn, aby czynić ekologicznie szkodliwe działania ekonomicznie nieopłacalnymi. Wiele ataków uważanych za ekoterrorystyczne wiąże się z użyciem graffiti i ekosabotażu. W książce grupa 4 osób walczy ze zniszczeniem natury Arizony przez rząd i prywatne firmy. Ich metody obejmują np. wlewanie piasku do zbiorników paliwa koparek, niszczenie billboardów lub uszkadzanie linii

kolejowych przeznaczonych do transportu węgla do elektrowni. Powieść stała się „biblią" niektórych członków radykalnego ruchu ekologicznego, którzy przyjęli opisane w niej metody.

Głównym problemem jest zdefiniowanie aktu sabotażu jako aktu terrorystycznego. Za tym pomysłem opowiadał się R. Arnold, krytyk ruchu ekologicznego. Jednak inni, jak Abbey, który był pokojowym anarchistą i inspiracją dla organizacji Earth First!, wskazują, że istnieje wyraźna różnica między sabotażem (przemocą wobec własności) a terroryzmem (przemocą wobec ludzi).

Ekoterroryści wykorzystują również ekoszantaż – ogół czynności opartych na wywieraniu presji na inwestora przez organizację pseudoekologiczną lub jej poszczególnych członków w celu uzyskania korzyści majątkowej pod groźbą wyrządzenia szkód finansowych i wizerunkowych wynikających z blokowania procesu inwestycyjnego.

W aktywnościach ekoterrorystów własność lub osoby są atakowane z powodów środowiskowych, działania te mają więcej wspólnego z sabotażem niż z terroryzmem zorganizowanym. Najczęściej jest to symboliczny gest niezadowolenia z systemu niszczącego przyrodę. Duże firmy, które prowadzą wycinanie lasów, budowę dróg, eksperymenty na zwierzętach lub inne działania szkodliwe dla środowiska, są często ich celem.

Działania ekoterrorystyczne zostały po raz pierwszy zauważone w Wielkiej Brytanii w latach 70. XX w., a do USA dotarły w latach 80. XX w. Od tego czasu zaobserwowano, że tego rodzaju aktywności (niezależnie lub w powiązaniu z różnymi grupami ekoterrorystów) rozprzestrzeniły się na inne kraje.

Podstawy światopoglądowe dla współczesnego ekoterroryzmu przyniosły lata 60. XX w., zwłaszcza książki *Silent Spring* R. Carson, *The Quiet Crisis* S. Udalla, *The Population Bomb* P. Ehrlicha oraz *The Closing Circle* B. Commonera. To one stały się podłożem, na którym wyrosły pierwsze grupy ekoterrorystów. Pionierami byli Eco-Raiders, studenci z Uniwersytetu Arizony. Dewastując place budowy na pustynnym terenie, otworzyli ekologiczną puszkę Pandory. Aktywiści Greenpeace próbowali zapobiegać wybuchom jądrowym; sabotowali połowy wielorybów, lawirując pontonami między zwierzętami a wielorybnikami; uniemożliwiali zrzuty

odpadów radioaktywnych i chemicznych w głębiny czy zasłaniali swymi ciałami foki przed myśliwymi. W 1977 r. P. Watson, usunięty z zarządu Greenpeace, utworzył Sea Shepherd Conservation Society. Specjalnością tej organizacji stały się akcje przeciw poławiaczom wielorybów polegające na taranowaniu statków wielorybniczych specjalnymi jednostkami.

Organizacja Earth First!, obok nieposłuszeństwa obywatelskiego i sabotażu, stosowała okupowanie drzew i szpikowanie ich długimi gwoździami, w 1980 r. zniszczono helikopter rozpylający środek chwastobójczy koło Takilmy (Oregon, USA), obalono słupy wysokiego napięcia i zaatakowano linię energetyczną w górach w okolicy Tucson.

Pod koniec lat 80. XX w. pojawiła się inna radykalna organizacja, Evan Mecham Eco-terrorist International Conspiracy (EMETIC), która zasłynęła m.in. z planowania ataku na elektrownie jądrowe w 3 stanach USA. Podobny cel postawiła przed sobą grupa o nazwie People for Ethical Treatment of Animals (PETA). Organizacja liczyła 600 tys. członków i była niezwykle aktywna. W samej tylko północnej Kalifornii przeprowadzono 9 zamachów (m.in. podpalenia domów towarowych w Bay Area, uszkodzenie linii energetycznej w Watsonville).

Osiągnięcia przypisywane stowarzyszeniom, wobec których działalności stosuje się prawną definicję ekoterroryzmu, są bardzo zróżnicowane. Organizacje takie jak Animal Liberation Front (ALF), Earth Liberation Front (ELF), Greenpeace, Earth First! i inne, mniej liczne organizacje, na różnych etapach działalności były oskarżane o ekoterroryzm. Najczęściej stosowaną formą zastraszenia były podpalenia, które dotyczyły np. miejsc strategicznych lub mienia należącego do przedsiębiorców prowadzących działalność szkodliwą dla środowiska. Aktywiści Earth First!, sprzeciwiający się nadmiernej wycince lasów, dopuszczali się niszczenia sprzętu należącego do osób pracujących przy wyrębie. Stosowali oni również technikę *tree spiking*, polegającą na wbijaniu metalowych przedmiotów w podstawę drzewa. Mogło to doprowadzić do uszkodzenia pił mechanicznych oraz wyrządzić krzywdę ich operatorom. Aktywiści ALF niszczyli wyposażenie rzeźni, sal wiwisekcyjnych, w których były przeprowadzane zabiegi operacyjne dokonywane na żywych zwierzętach w celach naukowych lub doświadczalnych, oraz uwalniali zwierzęta. Organizacje udostępniały również → i n f o r m a c j e w internecie lub we

własnych wydawnictwach prasowych, dotyczące sposobu przygotowania materiałów pirotechnicznych.

Ekolodzy z kolei, oskarżani o ekoterroryzm, używali tego terminu do opisywania zniszczenia środowiska spowodowanego przez firmy takie jak ExxonMobil, General Electric, McDonald's, a także przez wielorybników.

Największe organizacje ekologiczne na świecie są najczęściej krytykowane za działania, które w sposób niezaplanowany lub nieprzemyślany doprowadziły do nieodwracalnych zniszczeń. Przykładem jest akcja w Peru, zorganizowana przez aktywistów Greenpeace, w wyniku której zniszczeniu uległy mające ponad 2000 lat geoglify kultury Nazca. Z krytyką spotkała się PETA, powodem było finansowe wsparcie organizacji takich jak ELF i ALF, oficjalnie uznawanych w USA za terrorystyczne.

Radykalne organizacje ochrony przyrody angażują się w ekoterroryzm, aby wpłynąć na → o p i n i ę p u b l i c z n ą [t. 3]. Poszczególni zwolennicy praw zwierząt i zwolennicy biocentryzmu jednoczą się w grupach odpowiadających za prowokacyjne i nielegalne działania przeciwko temu, co uważają za znęcanie się nad zwierzętami. Pierwsze takie niezgodne z prawem działania wg amerykańskiego FBI zostały popełnione w 1977 r., kiedy działacze Greenpeace i organizacji ochrony fauny morskiej przecinali sieci wykorzystywane w przemyśle rybnym.

Prawdopodobnie największym wydarzeniem była ekoterrorystyczna operacja organizacji ELF, przeprowadzona w październiku 1998 r. w Vail w stanie Kolorado, podpalono 4 wyciągi narciarskie i 5 budynków należących do ośrodka narciarskiego Vail Resorts. ELF oskarżyła firmę o zniszczenie nietkniętej natury Gór Skalistych. Oprócz tego zostało podpalone biuro zarządzania zasobami ziemi w Oregonie i biuro Służby Leśnej USA (US Federal Forest Service) w Oak Ridge (strata 9 mln USD), podpalono rzeźnie w Redmond w Kalifornii (1,3 mln USD, 1997), doprowadzono do eksplozji i całkowitego zniszczenia biura Boise Cascade Company, które planowało rozpocząć budowę kompleksu maszyn do obróbki drewna w Chile (1999), podpalono kompleks mieszkalny w San Diego w Kalifornii (2003). Straty w wysokości ponad 1 mln USD zostały spowodowane przez kilka innych ataków.

Taką samą działalność prowadził ALF, podpalając biuro korporacji Weyerhauser, która sponsorowała badania genetyczne prowadzone na Uniwersytecie Stanowym Oregonu; podpalono Centrum Naukowe White Sands; zniszczono również laboratorium firmy Sierra Biomedical, która prowadziła badania z wykorzystaniem zwierząt; podłożono ładunki wybuchowe w budynku korporacji Huntingdon Life Sciences.

Według FBI w okresie od 1996 do 2002 r. organizacje ELF i ALF były odpowiedzialne za ponad 600 aktów ekoterroryzmu.

W lipcu 2000 r. w centrum Minneapolis nieznani ekologiczni ekstremiści rozmieścili 3 słoje z cyjankiem potasu, w ramach protestu przeciwko odbywającej się tam konferencji na temat inżynierii genetycznej.

Celem działaczy organizacji ekoterrorystycznych jest przywrócenie pierwotnych ekosystemów, które zostały „zniszczone przez nieświadome i samolubne działania ludzi". Według liderów ELF „najwyższy cel usprawiedliwia środki i żadna ofiara (tzw. efekt uboczny) nie powinna nas powstrzymywać". Jak twierdzi B. Taylor:

> Nie możemy zrozumieć tych facetów, jeśli nie zrozumiemy ich etycznej i duchowej motywacji w ogóle. Raczej pobieżna znajomość „zielonych" terrorystów z naukami o środowisku i nowoczesnym mechanizmem polityki państwa prowadzi do moralnego zakłócenia i cynizmu bojowników o odrodzenie dziewiczej przyrody.

Pod koniec XX w. działacze ELF zjednoczyli się z organizacją ALF. W 2001 r. FBI umieściło ją na liście organizacji terrorystycznych.

W Wielkiej Brytanii działają: Front Wyzwolenia Zwierząt, Milicja Wyzwolenia Zwierząt, Departament Sprawiedliwości, Front Wyzwolenia Ziemi, Brytyjskie Stowarzyszenie Sabotażystów Polowań. W październiku 2008 r. w Wielkiej Brytanii rozpoczęły się przesłuchania obrońców praw zwierząt. Byli oskarżani o to, że przez 6 lat rozpowszechniali informacje oczerniające pracowników brytyjskiego biomedycznego centrum Huntingdon Life Sciences i wysyłali im pogróżki. Spośród 8 oskarżonych 5 było członkami Stop Huntingdon Animal Cruelty. Działacze na rzecz praw zwierząt byli oskarżani o wysyłanie listów ostrzegawczych i fałszywych bomb do pracowników centrum, niszczyli ich samochody, na ścianach

ich domów pisali, że „tutaj mieszkają pedofile", „tutaj mieszkają zabójcy szczeniąt". Oskarżeni obiecali dać naukowcom spokój tylko wtedy, gdy odmówią współpracy z Huntingdon Life Sciences. W styczniu 2009 r. 7 z nich zostało skazanych na od 4 do 11 lat więzienia za szantażowanie firm naukowych i farmaceutycznych. Uznano ich za winnych organizowaniu kampanii przeciwko firmom wykonującym testy na zwierzętach. Według sądu działania grupy miały na celu zakończenie eksperymentów laboratoryjnych z wykorzystaniem zwierząt, a przestępcy próbowali wytworzyć „atmosferę strachu" w instytucjach naukowych i firmach farmaceutycznych. Zdaniem → p o l i c j i [t. 3] takie wyroki „osłabiły ruch ekstremistów obrońców praw zwierząt w Wielkiej Brytanii".

W 2004 r. grupa nieznanych sprawców dokonała serii ataków (ostatni 8 maja) na Wydział Biologii Uniwersytetu Moskiewskiego im. Łomonosowa, skradła wiele zwierząt doświadczalnych z Wydziału Zoologii Kręgowców. Z laboratoriów zniknęły wrony, duża liczba szczurów i 5 królików (prawdopodobnie zostały wypuszczone). Na ścianach namalowano logotypy i napisy wskazujące na organizację ALF, ale podejrzewano także studentów i pracowników Wydziału Biologii (ponieważ porywacze swobodnie weszli na wydział i otworzyli drzwi kluczem). Nieco wcześniej, 21 kwietnia 2004 r., w podobnych okolicznościach z wiwarium Instytutu Badawczego Fizjologii Normalnej było wypuszczono 119 żab.

W lutym 2012 r. w USA 27-letnia M. Lowell z Ohio próbowała za pośrednictwem Facebooka wynająć zabójcę, aby zabił mężczyznę noszącego futro naturalne. Dziewczyna potrzebowała wymówki, by rozdawać pocztówki na temat okrucieństwa wobec zwierząt. Została zatrzymana przez funkcjonariuszy FBI, którzy uważają działania wojowniczych ekologów i obrońców zwierząt za „największe zagrożenie terrorystyczne w USA" oraz → z a g r o ż e n i e [t. 4] dla państwa. FBI oskarża ekologów o podpalanie budynków mieszkalnych, laboratoriów naukowych i salonów samochodowych oraz organizowanie wybuchów w różnych miejscach. Według ekspertów straty spowodowane działaniami ekoterrorystów przekroczyły 100 mln USD i jest tylko kwestią czasu, zanim taka przestępcza działalność zacznie prowadzić do śmierci ludzi.

Jednymi z najbardziej widowiskowych przedsięwzięć ekoterrorystów są wtargnięcia na platformy wiertnicze. W marcu 2018 r. działacze

organizacji Greenpeace weszli w Norwegii na platformę należącą do koncernu Statoil. Chcieli uniemożliwić wysłanie jednostki do wykonywania odwiertów w Arktyce.

W raporcie do Senatu dyrektor FBI L. Free przyrównał do działalności terrorystycznej radykalnych działaczy na rzecz praw zwierząt, ekologów, bojowników przeciwko →broni nuklearnej [t. 1] i energetycznej.

Niszczycielskie działania radykalnych organizacji ekologicznych były wielokrotnie krytykowane przez bardziej umiarkowanych ekologów. Na przykład R. Skears napisał o ELF, że działania organizacji mogły wyrządzić więcej szkody niż pożytku. W końcu większość rzeczy, które zniszczyli aktywiści, została odbudowana, powodując dwukrotne zniszczenia przyrody – użyto 2 razy więcej drewna do budowy tego samego budynku. Skears uważa, że najbardziej nieprzyjemną konsekwencją działań tej organizacji jest to, że ruch ekologów kojarzy się z terroryzmem, a najbardziej lojalni działacze trafili do więzienia.

Przejawy ekoterroryzmu dotarły też do Polski. W lipcu 2018 r. organizacja Brygada Wschód wysadziła w powietrze blok budowany w Bielsku-Białej. Miał to być protest przeciwko praktykom dewelopera, który – zdaniem ekoterrorystów – budował nielegalnie. W lutym 2019 r. policjanci z Centralnego Biura Śledczego ujęli sprawcę, któremu postawiono zarzuty sprowadzenia niebezpieczeństwa zagrażającego mieniu w wielkich rozmiarach.

W kategoriach ekoterroryzmu można też postrzegać akcję Greenpeace w Elektrowni Bełchatów, która polegała na wtargnięciu podstępem na tereny jednostki. Według informacji podanych przez Ministerstwo Energii aktywistom udało się przedostać przez bramę wjazdową, gdyż podszyli się pod pracowników spółki należącej do GK PGE. Następnie ekolodzy weszli na chłodnię kominową, stwarzając w ten sposób niebezpieczeństwo dla siebie i zakładu pracy.

Nie są powszechnie znane sytuacje w Polsce, w których stosowano terroryzm z powodów ekologicznych czy prozwierzęcych. Jeżeli w Polsce pojawia się dyskusja na temat ekoterroryzmu, praktycznie zawsze dotyczy potocznego znaczenia tego słowa. Czasami uprzedzenia są tak silne, że nie pozwalają na prowadzenie rzetelnej, merytorycznej dyskusji. Większość aktywistów ekologicznych jest zgodna, że przemoc nie powinna być środkiem do osiągnięcia celu.

Akcje ekoterrorystyczne powodują więcej szkód niż pożytku dla ochrony środowiska naturalnego. Powodem tego jest fakt, że media, które mogą służyć do nagłaśniania problemu ekologicznego, zgodnie z oczekiwaniami społecznymi skupiają się na popełnionych przestępstwach. Działania takie są szkodliwe również dla organizacji stosujących akcje bezpośrednie *non-violence*, ponieważ wpływa to negatywnie na wizerunek całego ruchu ekologicznego, a określenie ekoterroryzm przedostaje się do powszechnego, błędnego użycia w stosunku do wszystkich akcji ekologicznych.

Według amerykańskich analityków jednym z czołowych niebezpieczeństw związanych z sektorem energetycznym w Stanach Zjednoczonych w najbliższych latach będzie działalność grup pseudoekologicznych określanych też mianem Zielonej Antify. Ugrupowania ekoterrorystyczne w USA mają na koncie wiele akcji wymierzonych w transport ropy naftowej i gazu, które spowodowały wielomilionowe straty dla sektora energetycznego w USA, a ich aktywność w ciągu ostatnich 2 lat gwałtownie wzrosła. Grupy pseudoekologicznie zapowiedziały intensyfikację działań wymierzonych w „brudną energię", za którą uważają wykorzystywanie takich surowców jak np. ropa, gaz i węgiel. W październiku 2016 r. na fali protestów przeciwko przepływowi ropy naftowej przez Dakotę Północną grupa pseudoekologicznych aktywistów włamała się do stacji przesyłowej rurociągu Dakota Access i tymczasowo zatrzymała transfer surowca. Sąd w Dakocie Północnej dotychczas postawił zarzuty 2 zatrzymanym osobom, 2 kolejne wciąż oczekują na akt oskarżenia, a piąta została skazana za włamanie drugiego stopnia.

W tym samym roku działacze Zielonej Antify wzniecili pożar w pobliżu tego samego rurociągu, sprowadzając realne zagrożenie ekologiczne oraz powodując straty w wysokości 2 mln USD. Z kolei w hrabstwie Mahaska w stanie Iowa 2 kobiety uszkodziły rurociąg za pomocą palników. Ich niebezpieczna akcja zatrzymała transfer surowca i wywołała straty, które ponownie wyniosły blisko 2 mln USD.

Pewną przeszkodą w skutecznym ściganiu przestępstw popełnianych przez pseudoekologów jest prawo, które często klasyfikuje ich czyny jako zwykły wandalizm lub np. włamania, jak w przypadku incydentu w stacji przesyłowej Dakota Access. Władze stanu Oklahoma w odpowiedzi na

akty przemocy ze strony działaczy Zielonej Antify wprowadziły legislację, która pozwoli penalizować nieuprawnione wtargnięcie na teren krytycznej infrastruktury. Zaliczono do niej rurociągi, rafinerie, elektrownie, linie kolejowe, przedsiębiorstwa chemiczne i terminale LNG. Z kolei 84 członków Kongresu wysłało petycję do Prokuratora Generalnego USA, w której domagają się uznania ataków wymierzonych w infrastrukturę energetyczną za akty terroryzmu.

Olga Wasiuta, Sergiusz Wasiuta

R.E. Dunlap, *Deep Ecology and Radical Environmentalism*, [w:] *American Environmentalism: The U.S. Environmental Movement, 1970–1990*, R.E. Dunlap, A.G. Mertig (eds.), Taylor & Francis, Philadelphia 1992; S.P. Eagan, *From Spikes to Bombs: The Rise of Eco-terrorism*, „Studies in Conflict & Terrorism" 1996, no. 19, EarthFirstJournal.org (dostęp 25.01.2020); *Ecodefense: A Field Guide to Monkeywrenching*, D. Foreman, B. Haywood (eds.), Abbzug Press, Chico, California 1993; *Ekoterroryzm wśród największych zagrożeń 2018 roku*, Ekoterroryzm.pl (dostęp 25.01.2020); K. Głowacki, *Ekoterroryzm w Polsce. Ekoterroryzm a ochrona środowiska*, Ekologia.pl (dostęp 25.01.2020); K.H. Govern, *Agroterrorism and Ecoterrorism: A Survey of Indo-American Approaches Under Law and Policy to Prevent and Defend Against These Potential Threats Ahead*, „Florida Coastal Law Review" 2009, vol. 10 (223); *Greenpeace zbecześciło „kolibra" z Nazca*, 13.12.2014, TVN24.pl (dostęp 25.01.2020); S.H. Leader, P. Probst, *The Earth Liberation Front and Environmental Terrorism*, „Terrorism and Political Violence" 2003, no. 15 (4); D. Liddick, *Eco-Terrorism: Radical Environmental and Animal Liberation Movements*, Praeger Publishers, Westport, Connecticut 2006; National Consortium for the Study of Terrorism and Responses to Terrorism, *Background Report: Discovery Communications Building Hostage-Taking*, 1.09.2010, Start.UMD.edu (dostęp 25.01.2020); A. Plows, D. Wall, B. Doherty, *Covert Repertoires: Ecotage in the UK*, „Social Movement Studies" 2004, no. 3 (2); J. Wiech, *Ekoterroryzm w Polsce? Tajemniczy „Zielony Front" podpalił harwestery na Dolnym Śląsku*, 10.04.2019, Energetyka24.com (dostęp 30.01.2019).

EKSPANSJONIZM GEOPOLITYCZNY – rozszerzenie wpływów politycznych lub gospodarczych przez wykorzystanie innych państw, zwykle poprzez → a g r e s j ę [t. 1] wojskową. Ekspansjonizm jest polityką, która zakłada, że interesy mogą być w znaczący sposób reprezentowane jedynie poprzez rozszerzenie własnego terytorium lub strefy wpływów.

Ekspansjonizm nie bierze pod uwagę, lub uwzględnia je tylko w drugiej kolejności, interesów tych, którzy są ostatecznie dotknięci dążeniem do ekspansji, jeśli jest to szkodliwe lub użyteczne dla jego własnych celów. →Irredentyzm, rewanżyzm lub zjednoczenie są czasem wykorzystywane do uzasadnienia i legitymizacji ekspansjonizmu, ale tylko wtedy, gdy ich celem jest odzyskanie utraconych terytoriów lub przejęcie obcych ziem. Zwykły spór terytorialny, taki jak spór graniczny, nie jest uważany za ekspansjonizm.

Ekspansjonizm geopolityczny jest przekonaniem, że można rozsądnie reprezentować własne interesy jedynie poprzez poszerzanie własnej strefy wpływów. Istnieją różne rodzaje ekspansjonizmu: wojskowy, gospodarczy, ideologiczny. Ekspansja zbrojna dotyczy zajęcia obcych terytoriów przy użyciu środków zbrojnych.

Badania nad ekspansjonizmem geopolitycznym koncentrują się głównie na badaniu czynników geograficznych dla celów politycznych. F. Ratzel, uznawany za ojca teorii ekspansjonizmu, uważał, że dążenie państwa do powiększenia swoich granic jest naturalne, stworzył 7 praw rozwoju państwa, inaczej nazwanych prawami ekspansjonizmu. Mówi o zajmowaniu przez ludność o podobnej kulturze coraz szerszego obszaru, przy wchłanianiu niekiedy mniejszych grup. Kierunek ekspansji przesuwa się od państw bardziej rozwiniętych cywilizacyjnie do państw słabiej rozwiniętych.

Ekspansjonizmowi sprzyjają poglądy, że wzrost gospodarczy i dobrobyt są warunkiem poszerzenia granic państwa. Dochodzi wtedy do ekspansji militarnej, tak jak podczas II wojny światowej, kiedy Niemcy i Japonia dążyły do konfliktu zbrojnego, w wyniku którego zdobyły nowe terytoria, a z nimi dostęp do surowców oraz taniej siły roboczej Warto również zauważyć, że ekspansjonizm wywoływany jest w społeczeństwie przez silną ideologię nacjonalistyczną. Często występuje przy okazji utracenia przez społeczeństwo swobód obywatelskich, co rekompensują sukcesy militarne na arenie międzynarodowej. Spojrzenie w polityce powinno być multisekularne zwłaszcza w dzisiejszych czasach, gdy mamy do czynienia z procesem hegemonicznym.

Po zakończeniu →zimnej wojny [t. 4] pozostało tylko jedno mocarstwo, USA. Dzisiaj jednak nie można już tak powiedzieć, ponieważ

następuje policentryzacja świata polegająca na tworzeniu się mocarstw regionalnych, dzielących się wpływami. Dzisiejsze zmiany geopolityczne prowadzą do pułapki Tukidydesa, tj. mechanizmu rywalizacyjnego pomiędzy dominującym mocarstwem, hegemonem, a państwem pretendentem, mowa tutaj o USA i Chinach. Porównać ją można do walki Sparty i Aten, rywalizacji krajów morza i lądu – USA są w tym przypadku niewątpliwie krajem morza, a Chiny krajem lądu. Pułapka Tukidydesa polega na tym, że mocarstwo będące hegemonem nie może wytrzymać presji państwa pretendenta i w ostateczności podejmuje działania wojenne. Oczywiście nie chodzi tutaj o działania zbrojne, lecz o →wojnę [t. 4] handlową, której początki możemy obserwować.

Z drugiej strony istnieje inna przeszkoda w postaci pułapki Kindlebergera, która może być głównym problemem współczesnej Polski, ponieważ gwarantem jej →bezpieczeństwa [t. 1] jest członkostwo w →NATO [t. 3], wsparcie USA, które w omawianym tu przypadku jest mocarstwem hegemonem, gospodarcze powiązanie z Unią Europejską, a ideologicznie bezpieczeństwo jest zapewniane dzięki demokracji. Pułapka Kindlebergera mówi o sytuacji, gdzie hegemon przestaje być gwarantem bezpieczeństwa zapewniającym pokój w kluczowych częściach świata. W ostatnich latach można zauważyć, że USA przestają powoli pełnić funkcję hegemona, a to dla Polski oznacza brak wystarczającej uwagi poświęcanej jej położeniu. Pułapkę Kindlebergera można obserwować na Bliskim Wschodzie, gdzie wielki konflikt może być jej konsekwencją. Amerykański plan zmiany układu sił za pomocą arabskiej wiosny nie powiódł się, a co za tym idzie wszystkie działania dokonywane na tych obszarach mogą oddziaływać na bezpieczeństwo Polski w ciągu najbliższych lat. Naciski Izraela na USA w sprawie ostrzejszej polityki w stosunku do Iranu są z tym powiązane, podobnie interwencja Arabii Saudyjskiej wraz z sojusznikami w Jemenie. Arabia Saudyjska i Izrael są świadomi zmiany hegemonicznej, a w rezultacie obniżenia poczucia bezpieczeństwa i gwarancji zapewnienia go przez USA.

W historii świata doszło do 2 wybuchów europejskiego ekspansjonizmu geopolitycznego. Pierwszy miał miejsce we wczesnym okresie nowożytnym, począwszy od eksploracji morskiej pod koniec XV w. Drugi przypadał na koniec XIX w. i zbiegł się z uprzemysłowieniem. Chociaż ta

ostatnia ekspansja pod pewnymi względami opierała się na imperialnych i quasi-imperialnych więziach ustanowionych jeszcze przed wiekami, podstawa ekonomiczna, stosunki społeczne i formy kulturowe w przypadku obu wybuchów były odmienne.

W XXI w. niektóre państwa nadal wykorzystują ekspansjonizm do osiągnięcia swoich celów:

- Chińska Republika Ludowa jest oskarżana o ekspansjonizm poprzez swoje operacje i roszczenia na Morzu Południowochińskim;
- Federacja Rosyjska wykazuje agresywną postawę od 2008 r., a zwłaszcza od 2014 r.: wojna rosyjsko-gruzińska w 2008 r. oraz okupacja Osetii Południowej i Abchazji; rosyjska agresja militarna na Ukrainę w 2014 r., → a n e k s j a [t. 1] Krymu i wojna w Donbasie; interwencja wojskowa w Syrii.

Zuzanna Juszczyk

P. Bartosiewicz, *Geografia polityczna i geopolityka*, Wydawnictwo Wyższej Szkoły Stosunków Międzynarodowych i Komunikacji Społecznej w Chełmie, Chełm 2008; Z. Juszczyk, *Geopolityczny ekspansjonizm*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; K. Mingst, *Podstawy stosunków międzynarodowych*, Wydawnictwo Naukowe PWN, Warszawa 2006; L. Moczulski, *Geopolityka – potęga w czasie i przestrzeni*, Bellona, Warszawa 2010; Z. Lach, J. Wendt, *Geopolityka: elementy teorii, wybrane metody i badania*, Instytut Geopolityki, Warszawa 2010; I.P. Piotrzkowicz, *Geopolityka: Polska w grze mocarstw: historia vitae magistra. Historia jest nauczycielką życia*, ZonaZero, Warszawa 2019; R.S. Ross, *Nationalism, Geopolitics, and Naval Expansionism from the Nineteenth Century to the Rise of China*, „Naval War College Review" 2018, vol. 71, no. 4, art. 4; R.A. Sauers, *Expansionism (Key Concepts in American History)*, Chelsea House Publications, New York 2010; L. Sykulski, *Geopolityka a bezpieczeństwo Polski*, Wydawnictwo Fronda, Warszawa 2018.

EKSTREMIZM – wielowymiarowe i wieloaspektowe zjawisko, którego istotą jest skrajny sposób działania, niezależnie od jego formy czy treści pozostający daleko poza głównym nurtem możliwej aktywności. W XX w. ekstremizm polityczny był zazwyczaj utożsamiany z postawą skrajnie prawicową lub skrajnie lewicową. Ekstremizm we współczesnym znaczeniu tego słowa jest ucieleśnieniem negatywnych zjawisk, które mają na celu

wzbudzenie wśród członków społeczności, często międzynarodowej, strachu, a w szerszej perspektywie wątpliwości co do możliwości utrzymania stabilności na świecie na zasadach demokracji, poszanowania → p r a w c z ł o w i e k a [t. 3] i wolności.

Specyfika ekstremizmu wiąże się nie tylko z kierunkiem politycznego działania, lecz również z tym, że może on dotyczyć → n a c j o n a l i z m u [t. 3], religii, → b e z p i e c z e ń s t w a [t. 1] lub jakiegokolwiek innego politycznie ważnego wymiaru. Ponadto ekstremizm odnosi się również do skrajnych metod działania, takich jak → p r z e m o c [t. 3] lub → t e r r o r y z m [t. 4], które przybliżają ekstremistów do osiągnięcia ich celów. Ekstremiści są zazwyczaj przeciwni wszelkim kompromisom i całkowicie pewni swojej pozycji, a także nie tolerują sprzeciwu w swojej grupie. Osoby lub ruchy można nazwać ekstremistami, kiedy ich poglądy są dalekie od głównego nurtu w określonych kwestiach, lub dlatego, że używają przemocy, aby osiągnąć swoje cele, lub też dlatego, że są bezkompromisowe i nietolerancyjne z innych powodów. Ekstremizm występuje już wtedy, gdy w działaniu politycznym można dostrzec tylko jedną z tych cech. Niektóre ruchy, takie jak Al-Kaida, są przykładami wykazującymi wszystkie wskazane cechy.

Działania ruchów ekstremistycznych często są odbierane są jako zaskakujące, przerażające i irracjonalne. Wskazuje się, że ekstremiści tacy jak Osama bin Laden różnią się od przeciętnych osób determinacją, skłonnością do dewiacji i fanatyzmem. Jednym z powodów jest skala zniszczeń, do których są zdolni, co symbolizują wydarzenia z 11 września 2001 r. Innym powodem jest pozornie jednoznaczna pasja ich przywódców, którzy często wydają się dogmatyczni, jednak zwykle obserwowana jest także fanatyczna lojalność ich wyznawców.

Ekstremizm nie jest zjawiskiem nowym. Choć środki przemocy używane przez współczesnych terrorystów nigdy wcześniej nie były używane, pod wieloma względami zjawiska te są znane z historii. Można mówić o długiej historii ekstremizmu w Europie. Być może pierwszym współczesnym przykładem ekstremizmu władzy był terror związany z dominacją jakobińską w czasie Wielkiej Rewolucji Francuskiej. To wówczas słowo terror zostało użyte po raz pierwszy. W XX w. ruchy ekstremistyczne przejmowały władzę w Europie wraz z powstaniem faszyzmu we Włoszech,

nazizmu w Niemczech i → k o m u n i z m u w byłym Związku Radzieckim i Europie Wschodniej. W kolejnych dziesięcioleciach grupy ekstremistyczne w Europie pozostawały znacznie mniejsze i nigdy nie sięgnęły po władzę, ale były ważne i destrukcyjne. Przykładami takich ruchów były lewicowe Czerwone Brygady i prawicowa Propaganda Due (P-2) we Włoszech w latach 70., grupa Baader-Meinhof działająca w latach 70. w Niemczech oraz antyimigracyjny Front Narodowy Le Pen we Francji, funkcjonujący do dziś (od 2018 r. jako Zjednoczenie Narodowe; od 1972 r. kierowany przez J.-M. Le Pena, od 2011 r. przez M. Le Pen). W Ameryce Północnej należy wskazać Ku Klux Klan, John Birch Society, Weathermen i prawicowe milicje w Stanach Zjednoczonych oraz Front Wyzwolenia Quebecu w Kanadzie.

Ekstremizm jako forma działania zmieniał także swoje znaczenie i sposób, w jaki był odbierany. Ruchy gejowskie i lesbijskie w USA były uważane za ekstremalne, podczas gdy dziś należą do ruchów społecznych głównego nurtu. Za ruch ekstremistyczny uznawano także gandyzm, który propagował ideę walki bez stosowania przemocy, co w ówczesnych okolicznościach historycznych miało skrajny wymiar.

Rafał Klepka

S. Jackson, *Non-normative Political Extremism: Reclaiming a Concept's Analytical Utility*, „Terrorism and Political Violence" 2019, vol. 31, iss. 2; M.A. Jensen, A.A. Seate, P.A. James, *Radicalization to Violence: A Pathway Approach to Studying Extremism*, „Terrorism and Political Violence" 2020, vol. 32, iss. 5; R. Klepka, *Ekstremizm*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; M.I. Midlarsky, *Origins of Political Extremism: Mass Violence in the Twentieth Century and Beyond*, Cambridge University Press, Cambridge 2011; C. Mudde, *On Extremism and Democracy in Europe*, Routledge, London–New York 2016; R. Wintrobe, *Rational Extremism: The Political Economy of Radicalism*, Cambridge University Press, Cambridge 2006.

ELFY PRZECIWKO ROSYJSKIM TROLLOM INTERNETOWYM – grupa internetowych wolontariuszy, ruch powstały w krajach bałtyckich w 2014 r., aby przeciwdziałać trollom rosyjskim, wyłapywać ich w sieci i walczyć z nimi. Aktywistów są już tysiące, próbują oni ujawniać manipulacje informacyjne w sieci – rosnący ruch oporu na Litwie to grupa ponad 5 tys. wolontariuszy. Określenie „elfy" ma źródło w mitologii nordyckiej,

w której te istoty są przeciwnikami innych mitycznych stworzeń – trolli – z którymi walczą tak, jak elfy z państw bałtyckich walczą z internetowymi trollami, szerzącymi → d e z i n f o r m a c j ę i prorosyjską → p r o p a g a n d ę [t. 3]. Rosja do dziś postrzega Estonię, Łotwę i Litwę jako strefę swoich wpływów. Dlatego w krajach nadbałtyckich został stworzony ruch elfów, by stawić opór → r o s y j s k i e j f a b r y c e t r o l l i w P e t e r s b u r g u [t. 3]. Na Litwie elfy nie występują już tylko w książkach fantastycznych – każdego dnia toczą prawdziwą walkę z trollami w sieci, co jest konsekwencją → w o j n y i n f o r m a c y j n e j [t. 4]. Wiedzą, że dzielenie społeczeństwa i wspieranie skrajności są intencjonalnym działaniem, za którym stoją interesy innych państw będących wrogami demokratycznych wartości, mających różne motywacje.

Litewskie elfy nie są istotami mitologicznymi lub fantastycznymi, lecz prawdziwymi, obywatelskimi i patriotycznymi ludźmi, których nie ograniczają granice państwowe. Łączy ich wspólny cel: dobrowolne przyczynianie się do walki z dezinformacją antylitewską za pomocą różnych środków. Elfy są myśliwymi, wojownikami i obrońcami przed dezinformacją i propagandą. To niewidoczna, niezastąpiona, pierwsza i ostatnia linia obrony w przestrzeni wirtualnej. Elfy są opiekunami świadomości obywatelskiej, kultury, historii i innych wartości, które wzmacniają odporność społeczeństwa litewskiego na → z a g r o ż e n i a [t. 4] informacyjne, dając dobry przykład sojusznikom.

Elfy indywidualnie lub w sposób zorganizowany podążają za źródłami dezinformacji w mediach internetowych, kanałach telewizyjnych, sieciach społecznościowych i analizują zawartość tych źródeł o każdej porze dnia. Elfy mogą ostrzegać o dezinformacji innych działaczy, społeczność medialną lub władze państwowe. Zaawansowana technicznie platforma Demaskuok.Lt reaguje na każdą dezinformację, oceniając i komentując artykuły, przedstawiając swoje argumenty, które pomagają odkryć fałszywe wiadomości.

Pierwsza grupa elfów została założona przez zaprzyjaźnionych, wykształconych i aktywnych Litwinów, którzy nie mogli pozostać obojętni wobec dezinformacji. Po raz pierwszy nazwa grupy wybrzmiała głośno na konferencji zorganizowanej przez Centrum Komunikacji Strategicznej NATO w 2015 r.

Elfem może stać się osoba patriotyczna, bez względu na płeć, wiek, narodowość, rasę, wyznanie, wykonywany zawód, orientację polityczną lub seksualną. Działacze nie mają formalnych kontraktów, obowiązków, oficjalnego statusu ani centrali – działają praktycznie. Najważniejsze kryteria podjęcia współpracy to wiarygodność osoby cenionej przez samą społeczność elfów, chęć wykorzystania swoich umiejętności, wiedzy, doświadczenia lub po prostu zdrowy umysł. Elfy są niewidzialnymi wojownikami państwa, a ich działania opierają się na zasadach dobrowolnej i osobistej poufności. Jest to doskonała okazja dla osób, które chciałyby przyczynić się do powstrzymania dezinformacji, ale nie mają narzędzi, żeby to robić. Nawet przy minimalnym wkładzie elfy mogą znacząco zwiększyć odporność społeczeństwa litewskiego na ataki informacyjne, rozwijać osobiste i publiczne umiejętności rozpoznawania dezinformacji. Działania elfów mogą być zabawą, grą, która wzmacnia jedność i społeczność cywilizowanych ludzi. Elfy mogą osiągnąć pożądany rezultat szybko, w pracy zespołowej lub indywidualnie, efekty ich aktywności są widoczne nie tylko na poziomie krajowym, ale także międzynarodowym. Działania elfów są dobrowolne i nieodpłatne.

Główną metodą walki z rosyjską dezinformacją w mediach jest aktywna i odpowiedzialna postawa →społeczeństwa obywatelskiego [t. 4]. Samorzutnie tworzące się grupy ochotników złożonych z publicystów, dziennikarzy i zwykłych obywateli są dużo bardziej efektywne niż sformalizowane struktury powoływane przez instytucje państwowe. Najsłynniejszą grupą internetowych aktywistów z państw bałtyckich jest litewska grupa elfów. Jest to grupa wolontariuszy prowadzących działania w sieci w czasie wolnym. Jej działalność jest bezpośrednią odpowiedzią na działania grup rosyjskich zawodowych propagandystów najniższego szczebla, zwanych powszechnie trollami. Medialną twarzą organizacji litewskich elfów jest R. Savukynas, bloger i doradca biznesowy.

Elfy bałtyckie codziennie pracują nad ujawnianiem rosyjskiej propagandy. Prowadzą dochodzenia, starają się dokładnie zbadać i ujawnić trolli, fałszywe konta i całe kampanie dezinformacyjne. Prowadzą też własne kampanie, wykorzystując pozytywne emocje i humor, dzięki którym starają się rozpowszechniać pozytywne informacje. Organizacje

rządowe bardzo je wspierają. Wolontariusze współpracują z dziennikarzami, dokładnie sprawdzając fakty.

Elfy walczą w pierwszym rzędzie z „hybrydowymi trollami" – trollami, które w odróżnieniu od klasycznych trolli (działających wyłącznie w swoim własnym interesie w celu zasiania niezgody i podżegania do konfliktu w środowisku online) rozprzestrzeniają pewne wiadomości na zlecenie konkretnego państwa i są narzędziem wojny informacyjnej. To odróżnia je od indywidualnych, prywatnych spamerów, trolli i hejterów, których celem jest po prostu szokowanie, zastraszanie i tworzenie konfliktów.

Eksperci badający →trolling [t. 4] w →mediach społecznościowych [t. 3] na zlecenie prowadzonego przez →NATO [t. 3] ośrodka StratCom w Rydze zwracają uwagę na coraz częstsze pojawianie się trolli hybrydowych, produkujących i wysyłających wypowiedzi na fora dyskusyjne. W rozmowie z Deutsche Welle Savukynas wyjaśniał mechanizm rosyjskiej propagandy: najpierw wybiera się jakąś grupę osób, by następnie ją spolaryzować, wysyłając na koniec zawsze to samo przesłanie: Związek Radziecki był najlepszy, a nasz rząd pozbawia nas podstawowych praw.

Celami trolli hybrydowych są intensywnie repostowane wiadomości, powtarzanie treści wysłanych z różnych adresów IP i pod różnymi pseudonimami oraz publikowanie fałszywych lub dezinformujących →informacji i linków. Zazwyczaj trolle hybrydowe silnie wspierają konkretne stanowisko polityczne i są bardziej skłonne do komentowania tematów związanych z określonymi obszarami polityki. Charakterystyczną cechą prorosyjskich trolli hybrydowych są ich często niewielkie umiejętności językowe w przypadku języków innych niż rosyjski.

Litewscy wolontariusze analizują portale społecznościowe, koordynują swoje działania za pośrednictwem Facebooka lub Skype'a. Codziennie elfy usuwają 10–20 stron rosyjskich trolli. Zdaniem naukowca z Instytutu Stosunków Międzynarodowych Uniwersytetu Wileńskiego N. Maliukevičiusa, który bada rolę technologii informacyjnej w czasach konfliktów, wprawdzie elfy zwalczają i ujawniają manipulacje w sieciach społecznościowych i na stronach internetowych, ale Litwa potrzebuje kompleksowej →strategii [t. 4] sprzeciwu wobec propagandy Kremla.

Walka litewskich elfów z rosyjskimi trollami w sieciach społecznościowych to tylko jedno pole konfrontacji. Serwisy informacyjne i kanały

telewizyjne również dołączają do tej walki. Propagandowa ofensywa jest mniej zauważalna niż czołgi czy samoloty, ale ona też uderza w bardzo szeroki zakres celów. Trolle wypełniają → p r z e s t r z e ń i n f o r m a c y j n ą [t. 3] tak wieloma → t e o r i a m i s p i s k o w y m i [t. 4], że nawet inteligentni ludzie ulegają dezinformacji.

Wiele organizacji pozarządowych, fundacji i ośrodków analitycznych angażuje się we wzmacnianie litewskiego i regionalnego społeczeństwa obywatelskiego poprzez promowanie wartości zachodnich i opracowywanie nowych strategii obronnych. Litwa jest zaniepokojona wpływem rosyjskiej propagandy państwowej na jej mniejszość rosyjską. Choć ochrona przed atakami cybernetycznymi miarowo się poprawia, zwalczanie dezinformacyjnych kampanii w internecie pozostaje wyzwaniem dla krajów bałtyckich. Jeśli chodzi o telewizję, to przynajmniej na Litwie dotrzymuje się pewnej zasady: od 2014 r. litewska komisja ds. radia i telewizji wielokrotnie zakazywała nadawania rosyjskich kanałów telewizyjnych za wykorzystanie fejków do zniekształconego przedstawiania wydarzeń historycznych lub za podżeganie do nienawiści i → w o j n y [t. 4].

W odwecie za opublikowanie przez trolli Kremla pod koniec 2017 r. listy ok. 1 tys. litewskich działaczy litewscy aktywiści uruchomili własną internetową bazę danych „rosyjskich trolli". Baza Vatnikas.lt została uruchomiona w celu zwalczania rozprzestrzeniania się rosyjskiej propagandy. Strona ujawnia nazwy propagatorów wrogiej propagandy i dezinformacji Kremla, którzy manipulują i starają się wpływać na ludzi. *Vatnik* to rosyjskie słowo, mem internetowy, który oznacza tanią radziecką bawełnianą pikowaną kurtkę. W maju 2012 r. w internecie w języku ukraińskim, rosyjskim, łotewskim (*vatņiks*) i litewskim (*vatnikas*) *vatnik* stało się obraźliwym określeniem przedstawiciela pewnego stereotypu Rosjanina, który niewolniczo popiera → r e ż i m [t. 3] totalitarny. Pod koniec listopada 2014 r., kiedy w Ukrainie zaczęła się rewolucja godności, słowo *vatnik* było coraz częściej wykorzystywane w sieciach społecznościowych w Ukrainie i Litwie. Termin ten jest zwykle rozumiany jako oznaczenie zwolenników ideologii „rosyjskiego świata" poprzez ośmieszanie i upokarzanie. Potencjał tego memu opiera się na tym, że w kulturze wielu krajów postsowieckich, od momentu powstania Związku Radzieckiego, słowo *vatnik* było popularne i pozostawało w obiegu za pośrednictwem różnych kanałów

medialnych: wspomnień byłych więźniów gułagów, internetu i radzieckich filmów telewizyjnych. *Vatnik* to osoba, która jest głupia i ślepo kocha swoją ojczyznę – Rosję, brak jej krytycznego myślenia, potrzebuje cara, prawa i porządku. *Vatniki* nienawidzą USA, z oddaniem chwalą Stalina i Putina. Według nich Rosja wygrała wszystkie wojny w historii świata. *Vatniki* nadużywają alkoholu, polityczny obraz jest dla nich całkiem jasny: Rosja znów będzie rządzić światem. „Celem naszej strony na Facebooku i witryny jest regularne […] demaskowanie vatników i zmaganie się z ich propagandą w ramach prawa", twierdzą twórcy projektu Vatnikas.lt.

Elfy zajmują się przede wszystkim identyfikowaniem oraz zgłaszaniem administratorom forów i →mediów społecznościowych [t. 3] fałszywych kont. Te ostatnie udaje się odkrywać drogą monitorowania komentarzy na portalach informacyjnych. Działalność litewskich elfów zyskała na popularności jesienią 2016 r., po nagłośnieniu przez media (głównie zachodnie).

Kolejne oddziały elfów zaczęto organizować w innych krajach. Inicjatywę podjęli również Łotysze. W marcu 2017 r. na Łotwie rozpoczęto rekrutację do lokalnej grupy elfów, na czele których stał były pracownik łotewskiego MSZ I. Bisenicex. Wolontariusze walczą z fałszywymi informacjami i propagandą rozpowszechnianymi przez trolli Kremla w łotewskich mediach elektronicznych. Działania grupy zainicjowały ruch społeczny w celu odróżniania informacji prawdziwej od fałszywej. Łotewskie elfy opierają się na doświadczeniach litewskich działaczy.

Po wydarzeniach w Ukrainie zauważono, że ataki na portalach są skoordynowane i zorganizowane. Głównym celem, jaki postawili przed sobą wolontariusze z Łotwy, jest podnoszenie świadomości ludzi, głównie młodych, którzy codziennie korzystają z internetu. Nie ma bowiem sensu zwalczanie pojedynczych komentarzy trolli, jest to fizycznie niemożliwe i niepotrzebne, istotne jest zaś uświadamianie samego istnienia zjawiska skoordynowanego trollingu.

W drugiej połowie 2018 r. elfy zaczęły aktywnie rozwijać się również w Czechach. Czechy po państwach bałtyckich stały się następnym regionem, w którym ludzie zaczęli bez wsparcia ze strony państwa w sposób zorganizowany walczyć z rosyjskimi trollami na portalach społecznościowych – „przeciwko tym, którzy świadomie przyczyniają się do zakłócenia

funkcjonowania naszego państwa", jak mówią czeskie elfy. Czeskie elfy pozostają anonimowe, a inspiracją ich działań były elfy z państw bałtyckich.

Według strony internetowej Denikn.cz w Republice Czeskiej działacze koordynują swoje wysiłki w celu ochrony przestrzeni informacyjnej przed trollami Federacji Rosyjskiej. W państwach bałtyckich elfy były w stanie ograniczyć rosyjskie operacje informacyjne, a czeskie elfy chcą ich naśladować. Zachowują anonimowość, żeby nie zaczęła się przeciwko nim aktywna kampania, mająca na celu ich dyskredytację. Ofiarą takiego prześladowania była np. fińska dziennikarka J. Aro, zdobywczyni nagrody Great Journalist Award, przyznanej jej za pracę, w której eksponowała wspierane przez Rosję trolle w mediach społecznościowych. W serii artykułów o trollach w mediach społecznościowych oraz w komentarzach prasowych autorka wyjaśniała, w jaki sposób działa „fabryka trolli" w Sankt Petersburgu. Po napisaniu kilku materiałów ujawniających manipulacje informacyjne Kremla propagandyści FR oskarżyli ją o to, że jest obcym agentem, że brała narkotyki, rozpowszechniały memy z jej zdjęciami itd. Po opublikowaniu artykułów nasiliła się kampania zastraszania i nękania Aro za pomocą SMS-ów, połączeń telefonicznych, poczty e-mail i mediów społecznościowych. W jednym przypadku otrzymała wiadomość tekstową rzekomo od ojca, który zmarł 20 lat wcześniej.

Czeskie elfy podkreślają, że nie działają przeciwko ludziom, którzy po prostu krytykują coś, ale przeciwko tym, którzy celowo zajmują się niszczeniem ich kraju. W Republice Czeskiej jest ich kilkudziesięciu, ale ze względów → b e z p i e c z e ń s t w a [t. 1] ukrywają swoje dane identyfikacyjne, aby nie narazić na szwank kariery, uniknąć gróźb i ataków na bliskich. Należą do nich lekarze, studenci, nauczyciele, strażacy, biznesmeni, specjaliści od → c y b e r z a g r o ż e ń [t. 1], artyści, rzemieślnicy, naukowcy, policjanci, a także w szczególności personel wojskowy. W gronie elfów znalazło się kilka znanych publicznie osób, które zamierzają w późniejszym czasie ujawnić swoją tożsamość. Wśród elfów są ludzie, którzy w razie wojny przyłączą się do ruchu oporu, obywatele, którzy czują się odpowiedzialni za swój kraj. Względy bezpieczeństwa i poufność danych osobowych nie pozwalają elfom akceptować każdego, kto ma chęć przystąpić do ich działań. Członkiem może być tylko ten, do kogo oni sami się zwrócą.

Pod fikcyjnymi tożsamościami elfy wchodzą do społeczności na Facebooku, poprzez które dezinformacja aktywnie rozprzestrzenia się, i angażują się w poszukiwanie jej inicjatorów. Monitorują, jakie kłamstwa są dystrybuowane w łańcuszkach e-mailowych i kto za nimi stoi. A wszystko to dobrowolnie, bezpłatnie, w czasie wolnym od pracy. Najbardziej pracowici wolontariusze przeznaczają na zwalczanie dezinformacji i trolli 6 godzin w tygodniu. Pracują zarówno w tradycyjnej przestrzeni publicznej, jak i w → c y b e r p r z e s t r z e n i [t. 1], śledzą aktywność trolli w sieci i docierają do informacji o konkretnych ludziach niszczących wartości, na których opiera się Republika Czeska. Zdarza się, że informacje są przekazywane do służb wywiadowczych. Czeskie elfy wyjaśniają, że trolle kierują swoje wysiłki przeciw ludziom nieszczęśliwym, rozczarowanym. Takie osoby wspierają → e k s t r e m i z m i starają się podzielić społeczeństwo na 2 obozy, które nie będą miały zdolności i chęci do współpracy. Elfy nie kwestionują wartości pracy czeskich → s ł u ż b s p e c j a l n y c h [t. 4] i organizacji non profit, zaangażowanych w obalanie kłamstw i dezinformacji, a tylko uzupełniają ich wysiłki. Grupa czeskich elfów specjalizuje się w łańcuszkach e-mailowych, działacze tworzą bazę danych służącą obnażaniu dezinformacji.

Olga Wasiuta

2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations. Kremlin Watch Report, 13.06.2018, KremlinWatch.eu (dostęp 16.03.2019); J. Aro, *The Cyberspace War: Propaganda and Trolling as Warfare Tools*, „European View" 2016, vol. 15, iss. 1; *Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia*, NATO Strategic Communication Centre of Excellence, Riga 2015; A. Król, *Obrona przestrzeni informacyjnej na przykładzie Litwy, Łotwy i Estonii*, „The Warsaw Institute Review" 2017, edycja specjalna: dezinformacja; *Lithuania Suspends Russian TV After Anti-U.S. Comments*, 17.11.2016, RFERL.org (dostęp 16.03.2019); J.-B.J. Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Information Manipulation: A Challenge for Our Democracies*, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris 2018; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017; J. Wirnitzer, *Češi budují informační odboj. Pronikli jsme do sítí prokremelských trollů, hlásí skrytí elfové*, 30.10.2018, Denikn.cz (dostęp 16.03.2019); Y. Zoria, *Baltic „Elves"*

Launch Online Database of Pro-Russian Trolls to Tackle Propaganda, 20.01.2018, EuromaidanPress.com (dostęp 16.03.2019); *Як Литва бореться з російською дезінформацією*, 8.10.2018, UkraNews.com (dostęp 16.03.2019).

ETYKA WALKI – to zbiór zasad, które powinny obowiązywać podczas działań zbrojnych. Wiążą się one bezpośrednio z użyciem siły, którą dysponują poszczególne strony konfliktu. Starcie, w którym strony przestrzegają tych zasad, można porównać do pojedynku rycerskiego, w którym walka uznawana jest za sprawiedliwą, odbywającą się wg wcześniej ustalonych reguł, co do których każda ze stron wyraża świadomą zgodę. Ewidentny jednakże pozostaje fakt, że wraz z rozwojem cywilizacji, postępem technologicznym i modernizacją uzbrojenia etyka także musiała ulec ewolucji. Z jednej strony etyka wskazuje, jak należy postępować, a czego należy się wystrzegać, z drugiej zaś przestrzeganie zasad etyki zależne jest tylko od jednostki oraz jej wizji osoby, którą chce się stać.

Obecne wyzwania etyczne związane z → w o j n ą [t. 4] z pozoru przynależą szczególnie do współczesności, ale w rzeczywistości wynikają z sięgającej wielu wieków tradycji myślenia o etyce wojny. Nazywano ją tradycją → w o j n y s p r a w i e d l i w e j [t. 4]. Jak zauważa R. Norman, była to dominująca intelektualna tradycja myślenia o moralności wojny, która stanowiła od zawsze wyrafinowany opis okoliczności, w których moralnie słuszne jest wywołanie wojny. Obejmowała zasady, takie jak słuszna przyczyna, prawowity autorytet i ostateczność, a także określała to, czego należy się wystrzegać w trakcie wojny – najbardziej znaną regułą jest tu zasada immunitetu osób nieuczestniczących w konflikcie, oznacza to, że w czasie wojny → ż o ł n i e r z e [t. 4] nie mogą atakować jednostek niebiorących bezpośredniego udziału w działaniach bojowych.

Jednym z często stawianych obecnie pytań jest to, czy współczesne wydarzenia wojenne sprawiły, że tradycyjnie przyjęte zasady przestały być aktualne. Należy zastanowić się, czy → b r o ń n u k l e a r n a [t. 1] sprawia, że rozróżnienie na walczących i niewalczących staje się nieistotne? Czy reakcje na terrorystów, którzy ewidentnie atakują kogokolwiek, muszą być powstrzymywane przez ostrożność, aby nie atakować tych, którzy nie są zaangażowani? Czy → t o t a l i t a r y z m [t. 4] wojenny, zarówno pod względem rozwoju broni, jak i demokratycznego zaangażowania

wszystkich – przynajmniej wszystkich dorosłych i uprawnionych do głosowania – sprawia, że tradycyjne ograniczenia w wojnie nie mają znaczenia? Czy nowe wojny, jak to miało miejsce np. przy rozpadzie Jugosławii, sprawiają, że całe tradycyjne ramy etyczne stają się bezcelowe? To tylko wybrane, często nierozstrzygalne dylematy etyczne odnoszące się do problematyki etyki walki i wojny.

Badacze etyki podkreślają, że jej przedmiot obejmuje nie tylko reguły lub zasady, ale także cnoty, zalety dążenia do perfekcji lub doskonałości. Przeciwwagą dla tych pojęć jest zwykła karykatura działań wojennych, która zakładałaby, że wojna jest sferą konieczności i grozy, w której wszystko jest dopuszczalne: „wojna to piekło", a w piekle nie ma żadnego dobra. Niektórzy nazywają ten pogląd wojennym realizmem.

B. Rhodes podkreśla, że u podstaw etyki leży dokonywanie wyborów. Tłumaczy tę zależność, wskazując, że ludzie nie myślą o pogodzie jako o „etycznej" lub „nieetycznej", ponieważ nie myślą o ziemi jako o czynniku etyki. Oznacza to, że nie korzysta ona z żadnej wolności wyboru, a więc nie jest uważana za odpowiedzialną za to, co się dzieje. Pogoda, podobnie jak inne zjawiska w świecie fizycznym, jest zdeterminowana przez siły naturalne, a więc nie istnieje dlatego, że ktoś zdecydował o jej zaistnieniu. Odzwierciedla się to w języku: nie byłoby rozsądne powiedzieć, że w przyrodzie „powinno" być inaczej, ale powszechnie uważa się, że ludzie „powinni" zachowywać się inaczej niż w rzeczywistości. Podobnie drzewa czy skały nie zasługują na ocenę etyczną, ale tego rodzaju oceny są często używane w odniesieniu do ludzi. Innymi słowy, etyka zakłada wybór, a wybór zakłada przynajmniej pewną dozę wolności.

Jako dyscyplina zorganizowana etyka kładzie nacisk na systematyczne znajdowanie najlepszych powodów do dokonywania konkretnych wyborów lub tworzenia poszczególnych polityk. Może być postrzegana jako przewodnik w korzystaniu ze swojej swobody wyboru. Studiowanie etyki pomaga odróżnić lepsze i gorsze powody stojące za poszczególnymi działaniami oraz wybrać najrozsądniejszą drogę w świetle wartości – takich jak wolność polityczna – i fakty – takie jak nierówny podział władzy wojskowej. Etyka wojskowa odnosi się do wyspecjalizowanej sfery i z biegiem czasu opracowała odpowiednie dla niej zasady, które pomagają kierować przyszłymi działaniami. Chociaż istnieją określone sztywne reguły, to mają

one sens praktyczny głównie dla doświadczonych wojskowych, profesjonalistów i mężów stanu, a także sens teoretyczny dla akademickich filozofów.

Niedoskonałość świata nie uzasadnia ignorowania etyki. Szczególnie w dyskusjach o wojnie można znaleźć ludzi skłonnych odrzucać etykę jako nieistotną. „To jest wojna" i cytując gen. W.T. Shermana, „wojna to piekło", jednak fakt, że ludzie źle się traktują na wojnie, nie określa tego, czy powinni tak działać. Fakt, że nieetyczne zachowania występują i prawdopodobnie będą występować nadal, nie ma większego znaczenia dla etyki, podobnie jak fakt istnienia śmiertelnej choroby nie oznacza, że badania medyczne są bezcelowe, wręcz przeciwnie – fakty cierpienia i zła sprawiają, że studiowanie etyki, a w szczególności etyki wojskowej, jest tym bardziej wartościowe.

Liczne pisma pochodzące z Chin i Indii z VI i V w. p.n.e., które przetrwały do dziś, prezentują moralne wskazówki dotyczące wojny i działań wojennych, które chińscy myśliciele, tacy jak Laozi (Lao Tzu) i Sun Zi (Sun Tzu), oferowali generałom. Hinduistyczna *Księga Manu* również zawierała zasady zalecające ograniczenie → p r z e m o c y [t. 3], podobne do tych, które popierają dziś zwolennicy humanitarnego podejścia do wojen.

Pisma Żydów, Greków i Rzymian ustanowiły podstawowe idee tego, co znane jest jako „tradycja sprawiedliwej wojny". Na przykład w biblijnej Księdze Powtórzonego Prawa wymieniono różne zasady, począwszy od wymogu zaoferowania miastu pokoju przed walką z jego mieszkańcami. Platon argumentował, że wojna jest konieczna, ale walczy się o pokój. W *Etyce nikomachejskiej* oraz *Polityce* Arystoteles przychylił się do poglądu Platona i po raz pierwszy użył terminu „wojna sprawiedliwa". Rzym miał wyraźne prawa rządzące jego dowódcami angażującymi się w wojnę. W *De re publica* Cycerona znalazło się pełne omówienie zasadniczych kwestii odnoszących się do etyki walki.

Tradycja wojny sprawiedliwej była przedmiotem rozważań wielu chrześcijańskich myślicieli, w tym Augustyna z Hippony i Tomasza z Akwinu. Augustyn (354–430) nie napisał żadnego traktatu o wojnie czy działaniach wojennych, ale wyraził w wielu miejscach zarówno uwagi dotyczące wojny w ogóle, jak i konkretne zalecenia dla przywódców państwa dotyczące ich obowiązków w czasie wojny. Nauki Augustyna służyły za podstawę zachodniego chrześcijaństwa aż do syntezy dokonanej

przez Tomasza z Akwinu (1225–1274) w *Sumie teologicznej*. W dziele ustanowił on podstawowe zasady sprawiedliwej wojny. Wskazywał, że musi być słuszna przyczyna, odpowiednia władza i odpowiednia intencja. Wieki później Hiszpan F. de Vitoria rozwinął koncepcję wojny sprawiedliwej w *De Indis* i *De Jure belli*, w których krytykował traktowanie przez hiszpańskich konkwistadorów rdzennych mieszkańców Ameryki Południowej i Środkowej. Twierdził, że usprawiedliwienie monarchy dla wojny musi spełniać obiektywne standardy wyznaczane przez mędrców i prawych ludzi. Ponadto nigdy nie jest zgodne z prawem umyślne zabijanie niewinnych, czyli tych, którzy nie są bezpośrednio zaangażowani w walkę.

Tradycja wojny sprawiedliwej proponuje 2 zestawy zasad, które określają etykę prowadzenia wojny. *Ius ad bellum*, czyli prawo do prowadzenia wojny, określa, kiedy odwołanie się do wojny jest moralnie legalne. *Ius in bello*, czyli prawo wojenne (prawo w czasie wojny), z kolei reguluje, jakie środki są moralnie dozwolone w trakcie działań wojennych. W ramach tej tradycji istnieje problem zakresu rozumienia i stosowania wskazanych zasad, zwłaszcza w odniesieniu do *ius ad bellum*. W konkretnym przypadku może nie być zgody co do oceny przesłanek moralnych wojny, pomimo zgody co do przedmiotowych zasad.

W zasadzie wszyscy zgadzają się, że musi być słuszny powód prowadzenia wojny. Państwa mają prawo do obrony przed agresją zbrojną. Wojny obronne są zatem określane jako dozwolone. Podobnie, jeśli popełniono wielką niesprawiedliwość wobec danego państwa, to może być konieczne rozpoczęcie wojny w celu jej naprawienia. Dyskutuje się również o tym, czy państwo może z wyprzedzeniem rozpocząć wojnę, jeśli ma przekonujące dowody, że jego wrogowie mogą wkrótce zaatakować.

Istnieje powszechna zgoda co do właściwego autorytetu wymaganego do wypowiedzenia wojny – może to być tylko najwyższa władza polityczna. Nie może zatem dojść do sytuacji, w której Kalifornia wypowiada wojnę Nevadzie, ponieważ uzurpuje sobie właściwą władzę rządu USA. Istnieją jednak poważne trudności w określeniu właściwej władzy, kiedy państwo się rozpada. Doskonałym przykładem są wydarzenia, które miały miejsce w Jugosławii, gdy Słowenia, Chorwacja, a następnie Bośnia i Hercegowina stały się niepodległymi państwami, uznanymi przez inne państwa

europejskie, a nawet ONZ w latach 1991 i 1992. Istniała wówczas trudność w odpowiedzi na pytanie, która władza jest odpowiednia.

W przeciwieństwie do słusznej sprawy i właściwego autorytetu zagadnienie intencji było przedmiotem wielu kontrowersji i debat w licznych kręgach politycznych i naukowych. Gdy w czasach cesarzy i królów istniała właściwa władza, problem intencji koncentrował się na osobie przywódcy i jego zamiarach. Zwolennicy tej zasady zdają sobie sprawę, że człowiek może czynić coś, co jest obiektywnie dobre, co w całym oglądzie zagadnienia wydaje się odpowiednie, a jednak nawet ta osoba może mieć ukryty motyw, który zamienia dobro w zło. W późniejszym czasie ludzie mogliby zrozumieć, że to, co wydawało się dobre, mogło być w rzeczywistości częścią nikczemnego spisku, a intencje monarchy czy władcy wiązały się przede wszystkim z zaspokojeniem jego potrzeb, pragnień czy ambicji. Tytułem egzemplifikacji takiego dylematu w XXI w. wskazać można motywy → i n w a z j i USA na Irak w 2003 r., mimo braku jednoznacznych dowodów na posiadanie broni masowego rażenia przez → r e ż i m [t. 3] Saddama Husajna.

Etyka wojny w tym kontekście dotyczy przywódcy, który wypowiedział lub prowadzi wojnę, nie odnosi się zaś do tych, którzy w dobrej wierze podejmowali konkretne działania wojenne, a do których byli zobowiązani. Żołnierze w wojnie nie ponoszą ciężaru moralnej winy w takich sprawach. Celem tej zasady jest przypisanie winy tym, którzy byli odpowiedzialni za podjęcie decyzji i działań, nie zaś za ich faktyczne wykonanie.

Teoretycy i badacze, którzy krytykują zasadę słusznej intencji, twierdzą, że w czasach dominacji państw narodowych nie jest jasne, czy państwa jako podmioty mogą mieć intencję. Ponadto trudno ocenić, czy państwo lub przywódca mieli intencję wywołania wojny, a to z uwagi na fakt, że niezwykle trudno w sposób obiektywny ocenić intencje kogoś innego. To właśnie sprawia, że niektórzy odmawiają słuszności stosowania tej zasady, podnosząc, że istotnym pytaniem jest to, czy istniała słuszna przyczyna. Mając na uwadze powyższe, często proponuje się inną zasadę, czyli deklaracje celów wojny. Wynika ona z tego, że zazwyczaj istnieje potrzeba wydania formalnego wypowiedzenia wojny, a w przypadku USA, które nie wypowiedziały wojny od czasu II wojny światowej, potrzeba ogłoszenia swoim obywatelom celów, do których dążą, angażując swoje siły

zbrojne w walkę. Wojna w Wietnamie wymagała stałego przekonywania amerykańskiej → o p i n i i p u b l i c z n e j [t. 3], że żołnierze giną w słusznej sprawie, a ofiary każdej z walczących stron były warte prób realizacji idei zahamowania ekspansji → k o m u n i z m u.

Wreszcie istnieje kilka innych zasad, które niektórzy stosują w ocenie tego, czy wojna jest sprawiedliwa. Obejmują one ostateczność, porównywalną sprawiedliwość, rozważenie kosztów i prawdopodobieństwo sukcesu. Wszystkie te rozważania wymagają oceny, czy istnieją dodatkowe powody pozwalające sądzić, że wojna jest sprawiedliwa w tym przypadku lub niesprawiedliwa w innym przypadku, gdy istniałaby możliwość zastosowania innego rozwiązania mogącego doprowadzić do rozwiązania zaistniałego problemu. Podobnie koszty wojny, zarówno pod względem materialnym, jak i strat w ludziach, mogą przeważyć nad dobrem, które można osiągnąć dzięki wojnie. Ponadto może istnieć dobry powód, aby zrezygnować z wojny z powodu słusznej przyczyny, ponieważ istnieje małe prawdopodobieństwo, że ostatecznie wojsku uda się obalić niesprawiedliwość.

W odniesieniu do *ius in bello* wyróżnia się 2 zasady: dyskryminacji i proporcjonalności. Pierwsza z nich podnosi, że niewłaściwe jest celowe ukierunkowanie wojny na cywilów, a nie żołnierzy. Zasada proporcjonalności nadaje moralne znaczenie poszczególnym aktom wojny. Ma pozwolić odpowiedzieć na pytanie, czy akt wojny spowoduje więcej zła niż dobra. Adekwatny pozostaje tu przykład pytania, czy zniszczenie wioski dla jej ratowania ma sens moralny. Wielu analityków i filozofów podejmujących rozważania dotyczące moralności wojny uważa zasadę dyskryminacji za podstawową i poprzedzającą zastosowanie zasady proporcjonalności, chociaż inni sądzą, że lepiej byłoby, gdyby założenia proporcjonalności były częściej stosowane w razie konieczności podejmowania decyzji o wojnie.

Problemy etyczne stały się nieodłączną częścią szkoleń, w których uczestniczą wojskowi w wielu krajach cywilizacji zachodniej i nie tylko. Prowadzenie działań na froncie jest misją, dlatego należy otaczać wielką troską rozwój etyki zawodowej walczących.

Istnieją trzy tradycyjne punkty widzenia dotyczące etyki wojennej. Pierwszym z nich jest realizm, który w odniesieniu do wojny często idzie w parze z realizmem w zakresie stosunków międzynarodowych. Zakładając,

że nie istnieją etyczne relacje między państwami, a także, w konsekwencji tego, podważając etyczne relacje między ludźmi, realizmem wojennym będzie pogląd, wg którego państwa mogą wypowiedzieć wojnę, gdy jest ona odpowiednia dla ich interesów, bez względu na to, czy mają słuszną przyczynę (choć twierdzenie, czy istnieje słuszna przyczyna, może być częścią → s t r a t e g i i [t. 4]). Według takich założeń wojna może być prowadzona w każdy sposób, który przynosi korzyść państwu walczącemu (choć w pewnych okolicznościach zachowuje się pewną powściągliwość ze względów ostrożnościowych). Te poglądy są konsekwencją poglądów na temat realizmu w stosunkach międzynarodowych.

Z realistycznego punktu widzenia, rozpatrując okazję do rozpoczęcia wojny, możliwa jest sytuacja, w której państwo wszczyna wojnę, aby zabezpieczyć swoją przewagę, ale pozostaje to nierealistyczne w odniesieniu do stosunków międzynarodowych w ogóle. Oznacza to, że państwa są rzeczywiście związane rozmaitymi konwencjami, ustanawianymi z biegiem czasu, na ogół w celu przestrzegania granic terytorialnych i honorowania umów i ustanowionego prawa międzynarodowego – zasadniczo programu internacjonalnego – ale ponieważ ten zbiór norm jest ustanowiony przez zwyczaj i porozumienie, a nie opiera się na prawdach moralnych ustanowionych przez rozum, przywódca polityczny może mieć powody, by łamać konwencje. Nie jest to zatem pełnowymiarowy realizm stosunków międzynarodowych, a słabo wspierana moralność międzynarodowa połączona z realizmem w odniesieniu do okazji do wojny.

W przeciwieństwie do realizmu hipotetyczne stanowisko ogólne może być nierealistyczne zarówno w odniesieniu do ogólnego postępowania w stosunkach międzynarodowych, w tym decyzji o udziale w wojnie, jak i w odniesieniu do szczególnych stosunków między podmiotami, które pozostają ze sobą w kontakcie, np. poprzez transakcje gospodarcze na całym świecie lub podróże zagraniczne. Niemniej jednak, gdy dochodzi do wojny, zwykłe zasady moralne zostają albo uchylone, albo zawieszone. Są one nadrzędne (lub przeważające), ponieważ po rozpoczęciu wojny zwycięstwo jest najważniejsze, a rozróżnienie między żołnierzami a cywilami jest nieistotne, gdyż każdy z nich jest traktowany jako przedstawiciel strony przeciwnej. Jest to zatem przekonanie, wg którego normy moralne zależą od konwencji, a w trakcie działań wojennych konwencje tracą

moc. Należy zauważyć, że nadrzędne lub zawieszone normy moralne nie muszą być postrzegane jako „wszystko albo nic". Okrucieństwa mogą być nadal odbierane jako zakazane i złe, a czynione mimo to. Zdarza się to szczególnie w przypadku wojen opartych na realistycznych przesłankach.

Zazwyczaj identyfikuje się szereg elementów *ius ad bellum* takich jak konieczność wypowiedzenia wojny przez uprawniony organ, istnienie słusznego powodu takiego jak samoobrona czy wojna jako ostateczność oraz istnienie rozsądnej perspektywy sukcesu i proporcjonalności. *Ius in bello* odnosi się do sposobu prowadzenia wojny. Zasady rozsądnej perspektywy sukcesu i proporcjonalności funkcjonują tu również w odniesieniu do poszczególnych operacji. Być może najbardziej istotnym elementem jest ograniczenie potencjalnego obiektu bezpośredniego ataku. Istnieje powszechne przekonanie, że celem ataków są wyłącznie walczący, a dążenie do zabijania cywilów, a nawet żołnierzy po ich poddaniu się, rozbrojeniu czy uwięzieniu jest błędem i przestępstwem.

Należy jednak zaznaczyć, że istnieje wiele różnych uzasadnień powodów wojny. Bywają one związane z utylitaryzmem, prawem naturalnym, konwencjonalizmem, tradycją, zbiorową roztropnością, → p r a w a m i c z ł o w i e k a [t. 3] itd. Wiele z tych argumentów wywodzi się z internacjonalistycznej tradycji, a wiele z nich pochodzi z rozważań kosmopolitycznych. Cechują one w szczególności daleko idący relatywizm w odniesieniu do oceny słuszności wojny.

Trzecim podejściem jest pacyfizm. Istnieją znaczące rozbieżności w definiowaniu pacyfizmu, jednak rdzeń pozostaje niezmienny – wojna jest niewłaściwa. Istotę stanowi zatem antywojenność. Pacyfizm jest przedstawiany zazwyczaj jako ogólne zalecenie dotyczące tego, jak powinny postępować jednostki, jednakże czasami ujmowany jest jako czysto osobiste zobowiązanie. Występuje w 2 głównych formach: pacyfizmu pryncypialnego lub deontologicznego oraz pacyfizmu warunkowego. Wersja pryncypialna twierdzi, że walka w wojnach jest błędna, bez względu na konsekwencje, stąd etykieta „deontologiczny". Może wynikać ze szczególnego charakteru walki na wojnach, przeciwnego obronie własnej, lub z ogólnego odrzucenia wszelkiego zabijania – przynajmniej istot ludzkich. Wersja warunkowa twierdzi, że konsekwencje braku walki na wojnach są generalnie lepsze niż konsekwencje walki na wojnach.

Motywacja pacyfizmu może być religijna lub świecka. Większość jednostek pacyfistycznych ma przekonania kosmopolityczne, przynajmniej można tak domniemywać. Dzieje się tak, ponieważ pacyfizm wyraża stanowisko niepodejmowania walki, nie jest jednak zobowiązaniem do promowania pokoju. Podmioty pacyfistyczne są zainteresowane nie tylko zajmowaniem stanowiska w sprawie walki, ale także zwalczaniem niesprawiedliwości i tworzeniem warunków, w których jednostki wcale nie muszą walczyć, co świadczyłoby o kosmopolityzmie tych podmiotów.

Etyka, w tym także etyka walki, pozostaje w dalszym ciągu zagadnieniem, które rodzi dylematy, nie zaś problemy czy zadania. Te ostatnie zwykle zakładają możliwość istnienia prawidłowych rozwiązań czy właściwych działań. Dylematy etyczne zdaniem wielu filozofów są nierozwiązywalne. Niezależnie od kierunku rozwoju wojen i konfliktów zbrojnych w przyszłości uwagę zwraca fakt, że relatywizuje się granicę między dobrem i złem, a odróżnienie rozwiązań optymalnych i słusznych od krwawych i nieludzkich wciąż zwykle jest względne.

Jakub Idzik

P. Christopher, *The Ethics of War and Peace*, Prentice Hall, New York 1999; A.J. Coates, *The Ethics of War*, Manchester University Press, Manchester–New York 1997; N. Dower, *The Ethics of War and Peace*, Polity, Cambridge–Malden 2009; J.T. Johnson, *Morality and Contemporary Warfare*, Yale University Press, New Haven 1999; R. Norman, *Ethics, Killing and War*, Cambridge University Press, New York 1995; J.R. Popiden, *Ethics of Warfare*, [w:] *Ground Warfare: An International Encyclopedia*, S. Sandler (ed.), ABC-CLIO, Santa Barbara–Denver–Oxford 2002; B. Rhodes, *An Introduction to Military Ethics: A Reference Handbook*, ABC-CLIO, Santa Barbara–Denver–Oxford 2009; *Routledge Handbook of Ethics and War: Just War Theory in the Twenty-first Century*, F. Allhoff, N.G. Evans, A. Henschke (eds.), Routledge, New York–London 2013; *Routledge Handbook of Military Ethics*, G.R. Lucas (ed.), Routledge, New York–London 2015; *The Ethics of War: Shared Problems in Different Traditions*, R. Sorabji, D. Rodin (eds.), Ashgate, Burlington 2006; M. Walzer, *Just and Unjust Wars*, Basic Books, New York 1992; O. Wasiuta, *Wojna czwartej generacji*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

ETYKA ZAWODOWA FUNKCJONARIUSZA POLICJI – to doktryna moralna systematyzująca oceny i normy moralne związane z wykonywaniem

zawodu policjanta, formułująca normy moralne postulowane do przyjęcia przez przedstawicieli tego zawodu. Inne definicje wyraźnie podkreślają precyzującą funkcję etyki zawodowej, definiując ją jako implementację ogólnych norm moralnych występujących w danym społeczeństwie do konkretnych sytuacji zawodowych, tj. jako konkretyzację moralności ogólnospołecznej. Etyka zawodowa kryje w sobie podejście nie opisowe, co ma miejsce w przypadku etosu, ale wartościujące i normatywne, co w praktyce oznacza, że zajmuje się ona tym, „jak być powinno" i „dlaczego być powinno". Można zatem powiedzieć, że przez etykę zawodową rozumie się próbę opracowania najważniejszych etycznych norm i dyrektyw dla określonego zawodu, a także ich faktycznych motywacji. Najprościej można powiedzieć, że etyka zawodowa to normy i zasady rządzące zachowaniem członków grupy zawodowej. Deontologia (zbiór norm moralnych obowiązujących przedstawicieli danego zawodu) zawodowa funkcjonariuszy służb mundurowych odpowiedzialnych za ochronę →bezpieczeństwa wewnętrznego [t. 1] musi być osadzona z jednej strony w przepisach prawa, z drugiej zaś w szeroko pojmowanej płaszczyźnie aksjologicznej opartej na systemie podstawowych praw i wolności jednostki.

Te wysokie wartości moralne, którymi każdy policjant powinien się kierować w służbie, w tym zasady etyki zawodowej, są już zaakcentowane w rocie ślubowania policyjnego, które policjant składa przed podjęciem służby:

> Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków policjanta, ślubuję: służyć wiernie Narodowi, chronić ustanowiony Konstytucją Rzeczypospolitej Polskiej porządek prawny, strzec bezpieczeństwa Państwa i jego obywateli, nawet z narażeniem życia. Wykonując powierzone mi zadania, ślubuję pilnie przestrzegać prawa, dochować wierności konstytucyjnym organom Rzeczypospolitej Polskiej, przestrzegać dyscypliny służbowej oraz wykonywać rozkazy i polecenia przełożonych. Ślubuję strzec tajemnic związanych ze służbą, honoru, godności i dobrego imienia służby oraz przestrzegać zasad etyki zawodowej.

Przestrzeganie zasad etyki zawodowej, poprzez umieszczenie ich m.in. w treści roty ślubowania, stanowi fundamentalny obowiązek każdego funkcjonariusza → P o l i c j i [t. 3].

Służba policjanta jest niewątpliwie zawodem wymagającym szczególnych predyspozycji i umiejętności. Ze względu na specyficzny zakres wykonywania czynności służbowych wobec obywateli powinien się on cechować również wysokimi wartościami etycznymi i moralnymi objawiającymi się w przestrzeganiu zasad etyki zawodowej funkcjonariusza Policji.

Przez wiele lat od powstania Policji funkcjonowanie zasad etyki zawodowej nie było sformalizowane w aktach prawa wewnętrznego. Pierwsze formalne decyzje kierownictwa Policji w tym zakresie zostały podjęte poprzez wydanie w dniu 14 lipca 1999 r. decyzji nr 121/999 w sprawie zasad etyki zawodowej. Określała ona w 11 punktach ogólne zasady etyczne zachowania policjanta. W decyzji tej stwierdzono, że policjant, służąc ludziom, powinien kierować się następującymi normami:

- poszanowania godności i praw każdego człowieka;
- lojalności wobec Rzeczypospolitej Polskiej i jej konstytucyjnych organów;
- szacunku dla społeczeństwa – jego symboli, języka, zwyczajów i tradycji;
- sumiennego i rzetelnego wypełniania obowiązków nałożonych przez prawo, a szczególnie bezwzględnego zwalczania → p r z e s t ę p c z o ś c i [t. 3];
- bezstronności, a zwłaszcza postępowania bez jakichkolwiek uprzedzeń rasowych i narodowościowych, politycznych bądź światopoglądowych;
- stosowania siły oraz innych → ś r o d k ó w p r z y m u s u b e z p o ś r e d n i e g o [t. 4] ściśle w granicach wyznaczonych prawem i zgodnie z zasadami humanitaryzmu;
- uczciwości, szczególnie bezwzględnego wystrzegania się → k o r u p c j i;
- wykonywania wydanych przez przełożonych rozkazów i poleceń służbowych z wyjątkiem tych, które są sprzeczne z prawem;
- utrzymywania relacji służbowych w duchu wzajemnego poszanowania;

- zachowania w dyskrecji → i n f o r m a c j i mogących zaszkodzić dobru służby lub dobremu imieniu innych osób;
- udzielania życzliwej pomocy wszystkim tym, którzy jej potrzebują z racji przyrodzonej godności lub przysługujących im praw.

Zasady te obowiązywały w polskiej Policji do 2003 r.

Wprowadzając w życie obecnie obowiązujące Zasady etyki zawodowej policjanta, szczególnie dbano, by stale mieć na uwadze znaczenie problematyki moralnej w wykonywaniu zawodu policjanta i jego służebną rolę wobec społeczeństwa, a także konieczność wzmocnienia oraz uzupełnienia obowiązków i praw policjanta wynikających z przepisów obowiązującego prawa. Wzięto także pod uwagę rozwiązania stosowane m.in. w rezolucji nr 690 Zgromadzenia Parlamentarnego Rady Europy, znanej pod nazwą Deklaracji o Policji, zaleceniu Rec (2001) 10 Komitetu Ministrów dla państw członkowskich ws. Europejskiego Kodeksu Etyki Policyjnej, rezolucję 34/169 Zgromadzenia Ogólnego Narodów Zjednoczonych – Kodeks postępowania funkcjonariuszy porządku prawnego. Na podstawie dotychczasowych rozwiązań oraz wymienionych wytycznych Komendant Główny Policji wydał Zarządzenie nr 805 z dnia 31 grudnia 2003 r. ws. „Zasad etyki zawodowej policjanta". Zarządzenie weszło w życie w dniu 1 stycznia 2004 r. i obowiązuje do dziś. Załącznikiem do zarządzenia są „Zasady etyki zawodowej policjanta". Określają jednoznacznie, że zasady etyki zawodowej policjanta wynikają z ogólnych wartości i norm moralnych uwzględniających specyfikę zawodu policjanta i że obowiązkiem każdego policjanta jest przestrzeganie zasad etyki zawodowej (§ 1). Zasady etyki zawodowej policjantów są szczegółowo opisane i określają, że:

- W sytuacjach nieuregulowanych przepisami prawa lub nieujętych w niniejszych zasadach etyki zawodowej policjant powinien kierować się zasadami współżycia społecznego i postępować tak, aby jego działania mogły być przykładem praworządności i prowadziły do pogłębiania społecznego zaufania do Policji (§ 2).
- Policjant powinien wykonywać czynności służbowe według najlepszej woli i wiedzy, z należytą uczciwością, rzetelnością, wykazując się odpowiedzialnością, odwagą i ofiarnością (§ 3).
- Policjant we wszystkich swoich działaniach ma obowiązek poszanowania godności ludzkiej oraz przestrzegania i ochrony → p r a w

człowieka [t. 3], w szczególności wyrażający się w respektowania prawa każdego człowieka do życia oraz zakazie inicjowania, stosowania i tolerowania tortur bądź nieludzkiego lub poniżającego traktowania albo karania (§ 4).

- Policjant, podejmując decyzję o użyciu broni palnej lub zastosowaniu środków przymusu bezpośredniego, powinien zachować szczególną rozwagę i stale mieć na uwadze charakter tych środków.
- Postępowanie policjanta w kontaktach z ludźmi powinna cechować życzliwość oraz bezstronność wykluczająca uprzedzenia rasowe, narodowościowe, wyznaniowe, polityczne, światopoglądowe lub wynikające z innych przyczyn (§ 6).
- Policjant powinien przestrzegać zasad poprawnego zachowania, kultury osobistej i dbać o schludny wygląd (§ 7).
- Wykonując zadania służbowe, policjant powinien dostosowywać swoje zachowanie do sytuacji i cech osób uczestniczących w zdarzeniu, w szczególności wieku, płci, narodowości i wyznania, a także uwzględniać uzasadnione potrzeby tych osób (§ 8).
- W trakcie wykonywania czynności służbowych policjant powinien zachować szczególną wrażliwość i takt w stosunku do ofiar przestępstwa lub innego zdarzenia, udzielać im możliwie wszechstronnej pomocy, a także dbać o zachowanie dyskrecji (§ 9).
- Zawiadamiając osobę o zamachu na jej dobra lub przekazując najbliższej rodzinie wiadomość dotyczącą osoby bliskiej, która stała się ofiarą przestępstwa lub innego zdarzenia, policjant powinien zachować takt (§ 10).
- Policjant jako → funkcjonariusz publiczny powinien wystrzegać się korupcji w każdej postaci oraz zwalczać wszelkie jej przejawy (§ 11).
- Policjant nie może wykorzystywać swojego zawodu do celów prywatnych, a w szczególności nie może wykorzystywać informacji uzyskanych w związku z wykonywaniem obowiązków służbowych ani uzyskiwać informacji do tych celów przy użyciu służbowych metod (§ 12).
- Policjant powinien zachować dyskrecję w odniesieniu do informacji mogących zaszkodzić społecznie pojętemu dobru służby

lub dobremu imieniu osób uczestniczących w czynnościach podejmowanych przez policjanta (§ 13).

- Stosunek policjanta do innych policjantów powinien być oparty na przestrzeganiu zasad poprawnego zachowania, poszanowania godności, a także tolerancji w zakresie nienaruszającym porządku prawnego (§ 14).
- Policjant powinien w miarę możliwości udzielać pomocy innym policjantom w realizacji zadań służbowych oraz wspierać w rozwiązywaniu ich problemów osobistych (§ 15).
- Przełożony powinien dawać podwładnym przykład nienagannego zachowania, w szczególności nie powinien nadużywać stanowiska, funkcji, stopnia policyjnego w celu poniżenia podległego policjanta (§ 16).
- Przełożony powinien zapewnić podległym policjantom właściwe warunki wykonywania zadań i rozwoju zawodowego oraz dbać o atmosferę pracy i dobre stosunki międzyludzkie (§ 17).
- Kierując działaniami podległych policjantów, przełożony powinien wydawać jasne i zrozumiałe polecenia oraz inspirować i motywować ich do działania (§ 18).
- Przełożony, oceniając podległych policjantów, jest zobowiązany kierować się jasno określonymi i znanymi im kryteriami oraz sprawiedliwością i obiektywizmem (§ 19).
- Przełożony powinien wysłuchać podwładnego w sprawach zawodowych i osobistych oraz udzielić mu wsparcia bądź pomocy, z zachowaniem dyskrecji (§ 20).
- Policjant powinien rzetelnie wykonywać polecenia przełożonego oraz odnosić się do niego z szacunkiem (§ 21).
- Policjant powinien stale doskonalić i uzupełniać swoją wiedzę oraz umiejętności zawodowe, a także dbać o sprawność fizyczną (§ 22).
- Policjant powinien dbać o społeczny wizerunek Policji jako formacji, w której służy, i podejmować działania służące budowaniu zaufania do niej (§ 23).
- Policjant nie powinien akceptować, tolerować ani lekceważyć zachowań policjantów naruszających prawo lub zasady etyki zawodowej (§ 24).

Należy podkreślić, że stosowanie się do zasad etyki zawodowej przez policjanta to wymóg prawny. Jego naruszenie rodzi określone konsekwencje dla funkcjonariusza. Zgodnie z art. 132. ust 1 ustawy o Policji policjant odpowiada dyscyplinarnie za popełnienie przewinienia dyscyplinarnego polegającego na naruszeniu dyscypliny służbowej lub nieprzestrzeganiu zasad etyki zawodowej. Na podstawie ustawy każdy policjant odpowiada nie tylko za naruszenie dyscypliny służbowej, ale również za naruszenie zasad etyki zawodowej. Zasady, normy etyki zawodowej są zatem obwarowane sankcjami nie tylko typowymi dla moralności, czyli napiętnowaniem społecznym i wyrzutami sumienia, ale również sankcjami dyscyplinarnymi. Rozszerza to w olbrzymi sposób katalog zachowań, działań i powinności, jakim powinien się podporządkować funkcjonariusz.

Krzysztof Dymura

Decyzja Komendanta Głównego Policji z dnia 14 lipca 1999 r. nr 121/99; Deklaracja o Policji (rezolucja nr 690 Zgromadzenia Parlamentarnego Rady Europy z dnia 8 maja 1979 r.); B. Jaworski, M. Ura, *Współdziałanie służb mundurowych i etyka zawodowa funkcjonariuszy*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2016; M. Michalik, *Społeczne przesłanki, swoistość i funkcje etyki zawodowej*, [w:] *Etyka zawodowa*, A. Sarapata (red.), Wydawnictwo Książka i Wiedza, Warszawa 1971; R. Rauhut, *Etyka zawodowa*, Wydawnictwo Szkoły Policji w Pile, Piła 2008; Rezolucja Zgromadzenia Ogólnego ONZ 34/169 z 1979 r. Kodeks Postępowania Funkcjonariuszy Porządku Prawnego; R. Sarkowicz, *Amerykańska etyka prawnicza*, Wydawnictwo Zakamycze, Kraków 2004; H. Skorowski, *Moralność społeczna. Wybrane zagadnienia z etyki społecznej, gospodarczej i politycznej*, Wydawnictwo Salezjańskie, Warszawa 1996; Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. 1990, nr 30, poz. 179; Zalecenie Rec (2001) 10 Komitetu Ministrów Rady Europy dla państw członkowskich dotyczące Europejskiego Kodeksu Etyki Zawodowej Policji przyjęte przez Komitet Ministrów 19 września 2001 r. na 765. sesji Zastępców Ministrów; Zarządzenie nr 805 Komendanta Głównego Policji z dnia 31 grudnia 2003 r. w sprawie Zasad etyki zawodowej policjanta, Dz. Urz. KGP.2004.1.3; Z. Ziembiński, *Podstawy nauki o moralności*, Wydawnictwo UAM, Poznań 1981.

ETYKA ZAWODOWA FUNKCJONARIUSZY PUBLICZNYCH – zespół norm i zachowań → funkcjonariuszy publicznych i ich postępowania w związku z wykonywaniem czynności służbowych. Postępowanie

etyczne rozumiane jest jako zbiór zachowań zgodnych z powszechnie przyjętymi normami ogólnymi. Za zachowania nieetyczne uważa się natomiast te, które wychodzą poza obszar ustanowionych norm etycznych. Etyka jest zatem źródłem normatywnym, szeregującym określone zachowania w katalogu tych, które są zgodne lub niezgodne z ogólnie przyjętymi wartościami. Etyka normatywna dąży do wskazania wartości i budowy norm, które wpływają na godne życie człowieka. Przyjęte normy etyczne – rozumiane jako prawo moralne – nie są tak rygorystyczne jak przepisy prawa stanowionego, ponieważ z uwagi na aksjologiczny charakter wyznaczają ogólną drogę postępowania.

Etyka zawodowa funkcjonariuszy publicznych obejmuje obszary ukierunkowane przede wszystkim na:

- normy wyznaczające właściwą postawę funkcjonariusza publicznego,
- normy stojące na straży rzetelności i uczciwości funkcjonariusza publicznego,
- normy stojące na straży godności i zawodowego prestiżu funkcjonariusza publicznego,
- normy regulujące stosunki funkcjonariuszy publicznych w miejscu pracy/pełnienia służby.

Z uwagi na służebną rolę funkcjonariuszy publicznych wobec społeczeństwa określa się normy etyczne, które pozostając w zgodzie z demokratycznie stanowionym prawem, tworzą kodeksy etyczne dedykowane poszczególnym grupom zawodowym. Do kodeksów tych można zaliczyć m.in.: Kodeks etyki funkcjonariuszy CBA, Zasady etyki zawodowej policjanta, Zasady etyki zawodowej funkcjonariuszy straży granicznej, Kodeks etyki funkcjonariusza służby celnej, Kodeks honorowy żołnierza zawodowego Wojska Polskiego, Zasady etyki radcy prawnego, Zbiór zasad etyki adwokackiej i godności zawodu, Zbiór zasad etyki zawodowej sędziów, Kodeks etyki zawodowej komornika, Kodeks zawodowej etyki w rachunkowości, Zasady etyki doradcy podatkowego, Kodeks etyki lekarskiej, Kodeks etyczno-zawodowy psychologa, Kodeks etyki nauczycielskiej, Kodeks etyczny Fundacji na rzecz Nauki Polskiej, Kodeks etyki pracownika naukowego.

Zasady etyki zawodowej funkcjonariusza publicznego wynikają z wartości i norm zawodowych przypisanych określonej grupie zawodowej, a obowiązkiem każdego funkcjonariusza publicznego jest ich

przestrzeganie. W sytuacjach nieuregulowanych przepisami prawa lub w przepisach etyki zawodowej funkcjonariusz publiczny powinien kierować się zasadami współżycia społecznego i postępować tak, by jego działania były przykładem praworządności i prowadziły do pogłębiania zaufania społecznego do państwa i do podmiotów, które je reprezentują. Funkcjonariusz publiczny, wykonując przypisane mu obowiązki, zobowiązany jest do poszanowania godności ludzkiej oraz przestrzegania i ochrony →p r a w c z ł o w i e k a [t. 3] (a zwłaszcza: przestrzegania prawa każdego człowieka do życia, zakazu inicjowania, stosowania i tolerowania tortur bądź nieludzkiego lub poniżającego traktowania albo karania). Funkcjonariusz publiczny nie może być podatny na →k o r u p c j ę oraz zobowiązany jest do jej zapobiegania, a także nie może wykorzystywać zajmowanego stanowiska i uzyskiwanych w ramach obowiązków służbowych →i n f o r m a c j i do celów prywatnych. Funkcjonariusz publiczny zobowiązany jest do sumiennego wykonywania obowiązków służbowych oraz nie powinien tolerować i akceptować zachowań innych funkcjonariuszy naruszających prawo lub zasady etyki zawodowej.

Jacek Bil

G. Jankowski, *Etyka zawodowa policjanta w aspekcie wybranych przymiotów osobowych*, Centrum Szkolenia Policji, Legionowo 2013; Kodeks etyki funkcjonariuszy służby celnej; J. Kudrelek, *Podstęp w postępowaniu karnym a zasady etyki zawodowej*, [w:] *Zasady etyki zawodowej w służbach mundurowych*, P. Jóźwiak, K. Opaliński (red.), Szkoła Policji w Pile, Piła 2013; M. Kulesza, M. Niziołek, *Korupcja*, [w:] *Etyka służby publicznej*, Wolters Kluwer Polska, Warszawa 2010; M. Mironowicz, *Przekroczenie uprawnień przez funkcjonariuszy publicznych*, „Obronność. Zeszyty Naukowe" 2015, nr 3 (15); A. Piontek, *Kodeks etyczny jako narzędzie kreowania zachowań organizacyjnych na przykładzie Policji*, „ZN WSH Zarządzanie" 2016, nr 1; J. Piwowarski, *Etyka funkcjonariusza Policji. Źródła, motywacje, realizacja*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2012; M. Stefański, *Etyka zawodowa policjanta*, Wydawnictwo Szkoły Policji w Słupsku, Słupsk 1996; Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. 1990, nr 30, poz. 179; Ustawa z dnia 12 października 1990 r. o Straży Granicznej, Dz. U. 1990, nr 78, poz. 462 z pózn. zm.; Zarządzenie nr 805 Komendanta Głównego Policji z 31 grudnia 2003 r. w sprawie Zasad etyki zawodowej policjanta, Dz. Urz. KGP z 7 stycznia 2004 r., nr 1, poz. 3; P. Żuraw, *Etyczny wymiar służb*

mundurowych, [w:] *Etyka w zarządzaniu Policją*, A Letkiewicz (red.), Wydawnictwo Wyższej Szkoły Policji, Szczytno 2011.

EUROPEJSKIE CENTRUM DOSKONALENIA DS. PRZECIWDZIAŁANIA ZAGROŻENIOM HYBRYDOWYM (The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) – to międzyrządowy think tank z siedzibą w Helsinkach (Finlandia) dla praktyków i ekspertów, który koncentruje się na przeciwdziałaniu →zagrożeniom hybrydowym [t. 4] pod auspicjami Unii Europejskiej i →NATO [t. 3], takim jak →cyberataki [t. 1], →propaganda [t. 3] i →dezinformacja. Większość pracy centrum jest poświęcona prowadzeniu szkoleń, organizacji warsztatów dla decydentów i praktyków, testowaniu nowych pomysłów, poprawie sposobów wymiany →informacji, a także opracowaniu białych ksiąg na temat zagrożeń hybrydowych, takich jak słabości sieci elektrycznej lub możliwe wykorzystanie niejasnych przepisów. Centrum promuje zarówno świadomość sytuacyjną i odporność, jak i zdolność do reagowania na zagrożenia hybrydowe.

Centrum zostało formalnie utworzone 11 kwietnia 2017 r. na mocy fińskiego prawa z protokołem ustaleń między 8 państwami europejskimi (Wielka Brytania, Francja, Niemcy, Szwecja, Polska, Finlandia, Łotwa, Litwa) i USA oraz zgodnie z decyzjami UE i NATO. Obecni byli także przedstawiciele Służby Działań Zewnętrznych UE i NATO. W uroczystości udział wzięli m.in. sekretarz generalny NATO i prezydent Finlandii.

Przemawiając na tym wydarzeniu, sekretarz generalny NATO J. Stoltenberg zwrócił uwagę, że zagrożenia hybrydowe dotyczą szerokiej gamy możliwych ataków, „od tweetów po czołgi i od propagandy po prowadzenie wojny", że działania Moskwy skutkowały zacieśnieniem współpracy w regionie, a centrum stanowi dowód, że „Europa szybko reaguje na Rosję". Stoltenberg podkreślił również szczególną rolę Finlandii w stosunkach z Rosją, z którą ma ona „dłuższą granicę niż wszystkie kraje NATO razem wzięte". Prezydent Finlandii dodał, że najlepszym sposobem przeciwstawienia się zagrożeniom hybrydowym jest „jedność społeczeństw i chęć obywateli do obrony własnego państwa".

Podobnie F. Mogherini, szefowa polityki zagranicznej UE, powiedziała, że centrum jest znakiem tego, że obie organizacje – UE i NATO – współpracują

na „bezprecedensowym poziomie", o czym świadczy utworzenie Centrum w Finlandii, kraju UE niebędącym członkiem Sojuszu Północnoatlantyckiego. „Silna Unia Europejska pod względem bezpieczeństwa i obrony czyni także NATO silniejszym" – stwierdziła Mogherini. → Z a g r o ż e n i a [t. 4] wprowadzające w błąd nie są nowością, są bowiem znane od czasów konia trojańskiego, nowością jest natomiast zakres niebezpieczeństw i ich szybkość; stworzenie centrum jest odpowiedzią Europy na zagrożenia hybrydowe ze strony Rosji.

Centrum zostało zainaugurowane 3 października 2017 r., na jego działanie przeznaczono roczny budżet w wysokości 1,5 mln EUR (2,8 mln EUR w 2020 r.). Potrzebę utworzenia takiej jednostki skomentował podczas konferencji prasowej fiński minister spraw zagranicznych T. Soyni: „Centrum stanowi prawdziwy bodziec dla współpracy UE – NATO. Działalność hybrydowa stała się stałym wyzwaniem dla bezpieczeństwa europejskiego". Prezydent Finlandii S. Niinistö oświadczył podczas uroczystości otwarcia centrum, że jego kraj ma nadzieję wnieść wkład w rozwijanie metod pozwalających przeciwdziałać zagrożeniom hybrydowym. Podkreślił znaczenie zachowania spokoju, ponieważ „wiele takich zagrożeń na pierwszy rzut oka wygląda gorzej, niż jest w istocie". Wystarczy jednak zachować zimną krew, żeby skutecznie sobie z nimi poradzić, a w tym Finlandia ma bogate doświadczenie, którym chętnie podzieli się z innymi. „Musimy zrozumieć na poziomie strategicznym cele i środki naszych przeciwników" – mówił. Od tego czasu centrum nadal cieszy się najwyższą uwagą: Niinistö reklamuje je jako kluczowy wkład w → b e z p i e c z e ń s t w o e u r o p e j s k i e [t. 1], a sekretarz obrony USA J. Mattis wyraził pochwałę działania instytucji podczas wizyty w Helsinkach w listopadzie 2019 r., nazywając ją „tak potrzebną w naszych czasach".

Zaraz po otwarciu centrum w Helsinkach stało się ono celem ataku w postaci rozpowszechniania o nim nieprawdziwych informacji za pośrednictwem internetu i → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3], za którymi stała Rosja.

Jednym z głównych zadań centrum jest określenie, w jaki sposób różne słabości, takie jak słabo chroniona sieć elektryczna lub niejasne prawo, mogą zostać wykorzystane przez nieprzyjaciela w nieprzewidziany sposób. Instytucja stara się również odnaleźć najlepsze sposoby obrony

przed takimi atakami. W tym duchu centrum jest bardziej wewnętrznym ośrodkiem analitycznym niż grupą zadaniową zajmującą się obalaniem propagandy lub śledzeniem → h a k e r ó w w → c y b e r p r z e s t r z e n i [t. 1].

Celami Hybrid CoE są:

- zapewnienie demokratycznego procesu decyzyjnego i rozpowszechnianie dobrych praktyk;
- wzmocnienie ogólnego podejścia do → b e z p i e c z e ń s t w a [t. 1] na poziomie krajowym, UE i współpracy międzynarodowej;
- zacieśnienie współpracy między UE i NATO, polegające na walce z zagrożeniami hybrydowymi;
- wspieranie aktywności na rzecz wzmacniania zdolności cywilnych i militarnych do przeciwdziałania zagrożeniom hybrydowym;
- podniesienie świadomości i zrozumienia na temat zagrożeń hybrydowych i podatności na zagrożenia w społeczeństwach, które można wykorzystać w operacjach hybrydowych i obrona przed nimi.

Główne funkcje Hybrid CoE to:

- być platformą dla narodów, by wspólnie dzielić się najlepszymi praktykami, budować zdolności, testować nowe pomysły i ćwiczyć obronę przed zagrożeniami hybrydowymi;
- być neutralnym pośrednikiem między UE i NATO poprzez strategiczne dyskusje i ćwiczenia;
- prowadzić rozmowę na temat przeciwdziałania hybrydom poprzez badania i wymianę najlepszych praktyk.

Powstanie Hybrid CoE poprzedzały różne spotkania państw UE. W maju 2015 r. Rada do Spraw Zagranicznych UE upoważniła Wysokiego Przedstawiciela UE do spraw zagranicznych i polityki bezpieczeństwa do przygotowania wniosków w odpowiedzi na zagrożenia hybrydowe. Rada Europejska w czerwcu 2015 r. wezwała również do podjęcia działań w celu rozwiązania zagrożeń hybrydowych. 27 stycznia 2016 r. Komitet Ministrów UE poinformował, że Finlandia zbada możliwość ustanowienia ewentualnego centrum. W następstwie sprawozdań Rada do Spraw Zagranicznych przedstawiła swoje konkluzje 19 kwietnia 2016 r., zachęcając państwa członkowskie do rozważenia ustanowienia centrum wiedzy specjalistycznej.

Inicjatywa powstania takiego centrum pochodzi ze wspólnego komunikatu Komisji Europejskiej i wysokiej przedstawiciel, przedstawionego

w Brukseli 6 kwietnia 2016 r. Parlamentowi Europejskiemu i Radzie pod nazwą Wspólne ramy przeciwdziałania zagrożeniom hybrydowym – reakcja Unii Europejskiej. 8 lipca 2016 r. Rada Europejska, przewodniczący Rady Europejskiej, przewodniczący Komisji i sekretarz generalny NATO zadeklarowali w Warszawie potrzebę zwalczania zagrożeń hybrydowych, a następnie we wspólnej deklaracji UE i NATO wezwano członków do stworzenia centrum przeciwdziałania zagrożeniom hybrydowym. Inicjatywę poparto we wspólnym zbiorze wniosków dotyczących wdrożenia wspólnej deklaracji UE i NATO, zatwierdzonym przez Radę UE i Radę Północnoatlantycką w dniu 6 grudnia 2016 r. 24 maja 2017 r. rząd fiński przedłożył Parlamentowi projekt ustawy o Europejskim Centrum ds. Zwalczania Zagrożeń Hybrydowych. Ustawa weszła w życie z dniem 1 lipca 2017 r.

Od kwietnia 2017 r. liczba uczestniczących państw wzrosła z 9 do 27 w styczniu 2020 r., a kilka kolejnych państw wyraża coraz większe zainteresowanie przystąpieniem do centrum. Uczestnikami centrum są: Austria, Kanada, Cypr, Republika Czeska, Dania, Estonia, Finlandia, Francja, Niemcy, Grecja, Węgry, Włochy, Łotwa, Litwa, Luksemburg, Czarnogóra, Holandia, Norwegia, Polska, Portugalia, Rumunia, Słowenia, Hiszpania, Szwecja, Turcja, Wielka Brytania i Stany Zjednoczone. Centrum ściśle współpracuje z UE i NATO. Członkostwo jest otwarte dla wszystkich państw członkowskich UE i sojuszników NATO.

Podobne centra istnieją już w Estonii, na Łotwie i Litwie, jednak Hybrid CoE jako pierwsze połączyło sojusz wojskowy z auspicjami UE. Co więcej, nowe centrum ma funkcjonować jako uzupełnienie innych centrów i podkreślać zwiększoną współpracę między UE a NATO od czasu → a n e k s j i [t. 1] Krymu przez Rosję i → w o j n y [t. 4] w Ukrainie w 2014 r.

Hybrid CoE powstało w celu zbadania „wojny hybrydowej" – strategicznego wykorzystania dyplomacji, polityki, mediów, cyberprzestrzeni i wojska w celu destabilizacji i osłabienia rządu przeciwnika. W tym czasie stosunki między Rosją a Zachodem osiągnęły pozostawały napięte. W centrum tego rosnącego sporu jest wykorzystanie przez FR połączenia wojskowej postawy, dezinformacji i technologii XXI w.: rosyjskie odrzutowce sondowały fińską i szwedzką przestrzeń powietrzną; rosyjska propaganda atakowała kraje bałtyckie – Estonię, Łotwę i Litwę; USA

oskarżyły Kreml o ingerowanie w wybory w 2016 r. Moskwa zaprzeczyła wtrącaniu się w wewnętrzne sprawy innych krajów i twierdziła, że jej postawa wojskowa jest uzasadnioną reakcją na wkraczanie NATO w jej granice. W tym kontekście nowe centrum dąży do znalezienia skutecznych sposobów przeciwstawienia się zagrożeniom hybrydowym ze strony Rosji.

Praca nowego centrum nie ogranicza się wyłącznie do śledzenia połączenia jawnej i tajnej taktyki Kremla, koncentruje się również na tym, w jaki sposób grupy takie jak ISIS (→ P a ń s t w o I s l a m s k i e [t. 3]) wykorzystują media społecznościowe i propagandę do dalszego przekazywania swoich wiadomości. Ponadto, oprócz zewnętrznych zagrożeń, centrum bada również, w jaki sposób problemy wewnętrzne, takie jak napięcia na tle rasowym i nierówności ekonomiczne, mogą być wykorzystywane w celu osłabienia demokratycznych rządów.

Centrum zostało podzielone na 4 główne obszary, a za każdy obszar odpowiada jedno z państw członkowskich. Wielka Brytania prowadzi badania ds. hybrydowych metod wywierania wpływu, Szwecja – badania dla podmiotów niepaństwowych, Finlandia ds. słabości i odporności państw członkowskich centrum, dzięki czemu uczestnicy inicjatywy dzielą się najlepszymi praktykami w kwestiach takich jak odporność systemów prawnych, bezpieczeństwo obszarów morskich i portów, sieci elektroenergetyczne, → d r o n y i zakłócanie wyborów. Czwarty obszar – do spraw → s t r a t e g i i [t. 4] i obrony w odniesieniu do → w o j n y h y b r y d o w e j [t. 4]– jest kierowany przez Niemcy.

W kwietniu 2019 r. Centrum Hybrid COE zorganizowało regionalne seminarium w celu wymiany najlepszych praktyk w dziedzinie zwalczania zagrożeń hybrydowych w gronie państw nordyckich i bałtyckich, we współpracy z Dowództwem Sił Operacji Specjalnych NATO. Jednym z wniosków była konieczność wypracowania ogólnorządowych i ogólnospołecznych metod reagowania na zagrożenia hybrydowe. Przedsięwzięciu temu służy współpraca regionalna – Centrum i NATO będą współpracować nad organizacją podobnych seminariów w innych regionach.

W maju 2019 r. Hybrid CoE wspólnie z UE i NATO zorganizowały warsztaty symulacyjne dotyczące ochrony portów w warunkach zagrożeń hybrydowych, w trakcie których to spotkań analizowano sposoby

zmniejszania zagrożeń hybrydowych skierowanych przeciwko europejskim portom oraz metody zwiększania ich odporności.

Wszystkie państwa uczestniczące w centrum wnoszą duży wkład w jego wysiłki. 4 państwa podjęły się wiodących ról w ramach centrum, a 6 z nich wspiera także centrum poprzez delegowanie pracowników do sekretariatu w Helsinkach. Konkretnym przykładem wkładu pojedynczego państwa jest wszechstronne szkolenie w zakresie bezpieczeństwa organizowane przez centrum we współpracy z fińskimi siłami zbrojnymi, które jest kierowane do państw członkowskich NATO oraz wybranych państw partnerskich, aby wspierać je w wypracowaniu szerokiego podejścia lub syntezy doktryn w celu zwalczania zagrożeń hybrydowych. Podstawą jest wielokierunkowy fiński model bezpieczeństwa, ale jest on omawiany w kontekście doświadczeń innych państw i instytucji w zakresie wszechstronnego bezpieczeństwa.

W sierpniu 2019 r. na stanowisko dyrektora centrum na 5-letnią kadencję została powołana doktor nauk politycznych T. Tiilikainen, która wcześniej była dyrektorem Fińskiego Instytutu Spraw Międzynarodowych. Przed mianowaniem na to stanowisko w 2010 r. była dyrektorem sieci studiów europejskich na Uniwersytecie Helsińskim (2003–2009), pracowała również w Ministerstwie Spraw Zagranicznych Finlandii w latach 2007–2008. Jak podkreśliła:

> Zagrożenia hybrydowe stały się nieodłączną częścią środowiska bezpieczeństwa zarówno w Finlandii, jak i innych demokratycznych społeczeństwach, dlatego ważne jest, aby wyzwania, które stawiają przed społecznością, były rozwiązywane we współpracy.

Hybrid CoE ma służyć jako centrum wiedzy specjalistycznej wspierające indywidualne i zbiorowe wysiłki krajów uczestniczących w celu zwiększenia ich zdolności cywilno-wojskowych, odporności i gotowości do przeciwdziałania zagrożeniom hybrydowym ze szczególnym uwzględnieniem w sprawie bezpieczeństwa europejskiego. Centrum ma zamiar oferować to wspólne doświadczenie i wiedzę fachową z korzyścią dla wszystkich uczestniczących krajów, a także UE i NATO. Centrum będzie

stosować kompleksowe, międzynarodowe, multidyscyplinarne i akademickie podejście.

Raporty zlecone przez Hybrid CoE to dokładne, pogłębione badania lub produkty wspólnych projektów instytucji. Raporty te mają na celu kompleksowe zrozumienie zagadnień związanych z zagrożeniami hybrydowymi. Przedstawiają one zalecenia polityczne lub inne praktyczne wnioski.

Raporty są wynikiem spotkań grup ekspertów na dany temat, kształtują dyskurs akademicki z nim związany, podkreślają główne trendy, wskazują różne perspektywy i służą jako materiał pomocniczy dla decydentów. Mają na celu rozróżnienie między tym, co naprawdę stanowi zagrożenie, a tym, co wydaje się zagrożeniem, i tym, co może się stać. Badania i analizy Hybrid CoE angażują zespoły ekspertów w 11 następujących tematach: →terroryzm [t. 4], bezpieczeństwo, informacja, gospodarka, prawo, energia, →cyberbezpieczeństwo [t. 1], Rosja, Chiny, Bałkany i Bliski Wschód. Każdy raport jest przygotowany przez najwyżej ocenianych ekspertów akademickich w danej dziedzinie z każdego z państw członkowskich.

Natowska strategia zapobiegania zagrożeniom hybrydowym opiera się na wzmacnianiu koordynacji działań z UE, większym wykorzystaniu sojuszniczych struktur wywiadowczych, zwiększeniu częstotliwości ćwiczeń oraz →przeciwdziałaniu dezinformacji [t. 3]. Nowa instytucja już wpisała się w działania pozostałych centrów eksperckich, które obecnie zaangażowane są w zwalczanie zagrożeń hybrydowych, takich jak Centrum Strategicznej Komunikacji w Rydze i Centrum Obrony Cybernetycznej w Tallinie. Wszystkie te instytucje mają charakter ekspercki, stanowiąc wsparcie merytoryczne, jednak nie posiadają statusu oficjalnych departamentów NATO.

Chociaż osiągnięto już dużo, wciąż wiele pozostaje do zrobienia, w pierwszym rzędzie jest to przejście od opisywania zagrożeń do przeciwdziałania im. W dziedzinie szkolenia i ćwiczeń należy wskazać zapotrzebowanie na ćwiczenia sztabowe oraz dyskusje prowadzone na podstawie scenariusza, które mogą być rozgrywane wspólnie albo jako indywidualne ćwiczenia krajowe. Państwa uczestniczące w tych działaniach powinny sobie ufać i wspierać się w identyfikowaniu narodowych słabości oraz

powinny wspólnie budować odporność. Wspólne zrozumienie zagrożeń hybrydowych jest z konieczności ciągłym procesem, który wymaga nieprzerwanej uwagi, badań i upowszechniania danych. Tak długo, jak nie wszystkie spośród państw członkowskich NATO i UE przystąpią do centrum, tak długo będą istnieć możliwości jego rozbudowy.

Przeciwdziałanie zagrożeniom hybrydowym w szybkim czasie stało się głównym mechanizmem wzmocnionej współpracy pomiędzy NATO a UE, przede wszystkim w oparciu o wzajemne interesy. Ponieważ centrum nie jest organem ani UE, ani NATO, ale samodzielnym podmiotem prawnym, może ono odgrywać unikalną rolę w dziedzinie ułatwiania i wzmacniania tej współpracy. Centrum jest częścią większego wysiłku NATO i UE, aby połączyć wiedzę ekspercką swoich członków i pomóc im szybko dostosować się do zmieniającego się oblicza konfliktów. Wśród rosnących doniesień o wtrącaniu się Kremla w sprawy państw zachodnich, od → zielonych ludzików [t. 4] wykorzystywanych podczas aneksji Krymu przez Moskwę w 2014 r. po ingerencję w wybory prezydenckie w USA w 2016 r. i inne wybory w państwach UE, NATO zwiększyło swoją obecność na wschodniej flance, a wielu członków sojuszu zwiększa wydatki na obronę.

Olga Wasiuta

EU And NATO Welcome Hybrid CoE. 4.10.2017, StratComCoE.org (dostęp 15.02.2020); A. Hagelstam, *Cooperating to Counter Hybrid Threats*, „Nato Review" 23.11.2018, NATO.int/docu/review (dostęp 15.02.2020); *Hybrid CoE. The European Centre of Excellence for Countering Hybrid Threats*, HybridCoE.fi (dostęp 15.02.2020); R. Standish, *Inside a European Center to Combat Russia's Hybrid Warfare*, 18.01.2018, ForeignPolicy.com (dostęp 15.02.2020); tenże, *Finland Opens a New Center to Fight „Hybrid Threats" from Russia and Beyond*, 3.10.2017, Pri.org (dostęp 15.02.2020).

EUROPOL (Europejski Urząd Policji) – to instytucja, której państwa Unii Europejskiej powierzyły zarządzanie zwalczaniem → przestępczości zorganizowanej [t. 3]. Na mocy postanowień przyjętych w Traktacie o Unii Europejskiej ma tworzyć sprawny system zapobiegania i zwalczania przestępczości zorganizowanej, handlowi

ludźmi i →terroryzmowi [t. 4]. Europol zainaugurował działalność 1 lipca 1999 r., co było konsekwencją uchwalenia w dniu 26 lipca 1995 r. konwencji o Europolu. Polska stała się członkiem tej instytucji 1 listopada 2004 r. Państwa członkowskie od dawna uznawały terroryzm międzynarodowy za priorytet w zapewnianiu →bezpieczeństwa [t. 1]. Wypracowywanie efektywnych rozwiązań w tym obszarze zainicjowano już w latach 70. XX w. w odpowiedzi na spektakularne ataki terrorystyczne. Z tych samych względów działania te zostały zdynamizowane w pierwszej dekadzie XXI w., po zamachach w Nowym Jorku, Madrycie i Londynie. Europol stał się ważnym narzędziem przeciwdziałania →zagrożeniom [t. 4] terrorystycznym. Na początku zamachy terrorystyczne nie należały jednak do zakresu przedmiotowego działania Europolu. Do mandatu organizacji zostały włączone decyzją Rady Unii Europejskiej z dnia 3 grudnia 1998 r., nakazującą Europolowi objęcie działalnością przestępstw przeciwko: życiu, zdrowiu, wolności osobistej lub mieniu, popełnionych lub takich, których popełnienie jest prawdopodobne podczas działań terrorystycznych (1999/C 26/06) 3.

Europol nie realizuje własnych przedsięwzięć operacyjno-śledczych. Jego główna aktywność polega na prowadzeniu wymiany →informacji w konkretnych postępowaniach oraz w obszarze szerokiej problematyki dotyczącej poszczególnych rodzajów przestępczości zorganizowanej. Dla podjęcia przez Europol działań w konkretnej sprawie karnej konieczne jest złożenie przez państwo członkowskie uzasadnionego wniosku potwierdzającego zorganizowany charakter przestępstwa, którego mają dotyczyć czynności Europolu. Skutki takiego przestępstwa muszą wystąpić przynajmniej dla 2 państw członkowskich.

Działania Europolu koncentrują się głównie na prowadzeniu →wywiadu [t. 4] kryminalnego. Sprowadza się to do: gromadzenia, przetwarzania, analizy, oceny, interpretacji oraz wymiany uzyskanych informacji. Delegacja Europolu do prowadzenia czynności służących zwalczaniu terroryzmu została określona w art. 88 Traktatu o funkcjonowaniu Unii Europejskiej. Zawarte jest tam też uprawnienie do koordynowania, organizowania i prowadzenia dochodzeń i działań realizowanych wspólnie z właściwymi organami państw członkowskich lub w ramach wspólnych zespołów dochodzeniowych, w stosownych przypadkach, w powiązaniu z Eurojustem.

Głównym kierunkiem działań Europolu jest realizowanie zadań związanych z przeciwdziałaniem przestępczości zorganizowanej i innym formom poważnej przestępczości oraz przestępstwom z nimi powiązanym, które dotyczą, jak wskazano wcześniej, co najmniej 2 państw członkowskich (zagrożenia transgraniczne). Celem wspomagania dochodzeń Europol przekazuje krajowym służbom państw członkowskich wszelkie istotne informacje, niezbędne do efektywnego prowadzenia działań operacyjnych. Samo wykorzystanie tych informacji i danych wywiadowczych podlega krajowym przepisom o ochronie danych obowiązujących w państwie członkowskim otrzymującym informacje. Uzyskane informacje i dane wywiadowcze podlegają takim samym przepisom o ochronie danych, jak gdyby zostały zgromadzone w otrzymującym je państwie członkowskim.

Realizacja zadań wywiadowczych przez Europol podlega wielu obwarowaniom prawnym regulującym m.in. ochronę danych osobowych i →informacji niejawnych. Zapewniają one także sprawowanie nad agencją właściwego nadzoru i kontroli, poprzez Radę UE, Parlament Europejski, Komisję Europejską, a w zakresie kontroli sądowniczej przez →Trybunał Sprawiedliwości UE [t. 4]. Funkcję kontrolną sprawują także: zarząd Europolu, parlamenty krajowe państw członkowskich, urząd ombudsmana oraz Wspólny Organ Nadzorczy.

Obecne działania społeczności międzynarodowej zmierzają do zwiększenia potencjału Europolu w obszarze zwalczania zagrożeń występujących na terenie Europy, o czym świadczy duża liczba regulacji dotyczących agencji, uchwalonych przez Radę UE od momentu jej powołania. Dzięki nim następujące po sobie prezydencje w Radzie UE rozbudowywały kompetencje Europolu o kolejne zadania i uprawnienia ukierunkowane na zwalczanie zagrożeń transgranicznych.

Obecnie w Polsce we współpracę w ramach Europolu są zaangażowane następujące służby: →Policja [t. 3], →Straż Graniczna [t. 4], →Centralne Biuro Antykorupcyjne [t. 1], →Agencja Bezpieczeństwa Wewnętrznego [t. 1] (ABW), Generalny Inspektor Informacji Finansowej oraz Krajowa Administracja Skarbowa. Polska, podobnie jak i inne państwa członkowskie, nie jest w stanie bez wsparcia Europolu skutecznie dokonywać analiz strategicznych na potrzeby predykcji zagrożenia przestępczością zorganizowaną oraz terroryzmem.

Duże znaczenie ma tu jednak liczba i jakość (aktualność oraz ważność) informacji przekazywanych do Europolu. Sama spójność systemu zarządzania informacjami ma tu wtórne znaczenie. Głównymi nadawcami informacji kryminalnych, a także odbiorcami danych wywiadowczych uzyskanych w wyniku analiz przeprowadzonych przez Europol są państwa członkowskie.

Uzależnienie informacyjne Europolu od państw członkowskich jest obecnie całkowite. Stąd wyniki działań operacyjnych tej instytucji zależą od pełnej współpracy z państwami członkowskimi, która ma decydujące znaczenie dla zapewnienia kompleksowych działań wywiadowczych Europolu. Bez wkładu informacyjnego państw członkowskich agencja ta nie jest w stanie spełniać swojej misji oraz realizować oczekiwań artykułowanych przez Radę Unii Europejskiej, Komisję Europejską czy państwa członkowskie Unii. Europol usytuowany jest w międzynarodowym systemie zwalczania przestępczości na styku 3 poziomów: narodowego, unijnego i globalnego. Dokonujący się przepływ informacji jest zwornikiem łączącym te poziomy.

Zasadniczą rolą Europolu jest pośredniczenie i inspirowanie państw członkowskich do zbierania i wymiany informacji kryminalnych oraz danych wywiadowczych o wspólnych zagrożeniach. Na skutek działań związanych z realizacją wywiadu kryminalnego w ramach tej organizacji zwiększyły się możliwości współpracy transgranicznej państw członkowskich w obszarze wspólnych przedsięwzięć zapobiegawczych i wykrywczych. Krytycy oceniający funkcjonowanie Europolu podnoszą, że występuje w nim wielość instytucji i mechanizmów o kompetencjach, które się na siebie nakładają, co może utrudniać jego skuteczne działanie.

Centrala Europolu mieści się w Hadze i zatrudnia funkcjonariuszy różnych służb, takich jak policja, urzędy celne, imigracyjne i finansowe. Organem kierowniczym Europolu jest Zarząd, który odbywa posiedzenia 2 razy do roku. W jego skład wchodzą przedstawiciele wszystkich państw członkowskich, których bieżącymi pracami kieruje dyrektor. Raz w roku ukazują się raporty Europolu zawierające analizę występujących aktualnie zagrożeń ze strony przestępczości zorganizowanej wraz z zaleceniami dla poszczególnych państw członkowskich.

W 2002 r. Europol uzyskał możliwość powoływania wspólnych zespołów dochodzeniowo-śledczych, których celem jest gromadzenie informacji

i koordynowanie zadań w konkretnych postępowaniach, obejmujących obszar kilku państw. Ze względu na różnice w uregulowaniach prawnych obowiązujących w państwach członkowskich czynności operacyjno-dochodzeniowe na ich terenie dokonywane są przez policje krajowe. Każde państwo członkowskie tworzy lub wyznacza jednostkę krajową odpowiadającą za całokształt współpracy prowadzonej z Europolem. Komenda Główna Policji (KGP) jest jednostką krajową Europolu, której szefem jest komendant główny Policji. Regulamin KGP określa zadania w zakresie organizowania i koordynowania przedsięwzięć wynikających z członkostwa w Europolu, wskazując, że są one realizowane przez Biuro Międzynarodowej Współpracy Policji KGP. Poprzez to ogniwo KGP jako jednostka krajowa Europolu koordynuje działalność wszystkich organów ochrony porządku prawnego na terenie Polski. Każda jednostka krajowa kieruje do pracy w Europolu co najmniej jednego oficera łącznikowego. Wykonuje on zadania krajowego punktu kontaktowego.

Obecnie w skład polskiego biura łącznikowego przy Europolu wchodzi 3 policjantów oraz po jednym przedstawicielu Straży Granicznej i ABW. Polskie organy ścigania mogą korzystać z wielu usług operacyjnych Europolu, przede wszystkim z możliwości analizy operacyjnej, w tym z tzw. analitycznych plików roboczych, które obejmują najważniejsze obszary międzynarodowej przestępczości zorganizowanej w UE. Duże znaczenie ma dostęp do systemów informatycznych Europolu. Agencja ta jest gospodarzem i organizatorem spotkań operacyjnych, podczas których funkcjonariusze wymieniają się wiedzą, doświadczeniami i dobrymi praktykami. Spotkania te finansowane są z budżetu Europolu. Polska była gospodarzem takich spotkań, a jedno z nich odbyło się we Wrocławiu. Polska wzięła także udział w wielu operacjach koordynowanych przez Europol. Oto niektóre z nich:

- IKEA – była skierowana przeciwko grupie sprawców podkładających ładunki wybuchowe w sklepach sieci IKEA na terenie całej Europy w celu wymuszenia haraczy. W śledztwo zaangażowane były policje większości krajów europejskich, co powodowało konieczność koordynacji i wymiany informacji, za pośrednictwem Europolu. Polska policja, korzystając z tych danych, zatrzymała 2 sprawców odpowiedzialnych za podkładanie bomb.

- NIGHT CLONE CARD – skierowana przeciwko zorganizowanej grupie przestępczej zajmującej się skimmingiem. Ujawniona została we Włoszech, a operację koordynował Europol (FP Terminal). Strona polska uzyskała dzięki temu informacje dotyczące osób, które działały na terenie naszego kraju. W Chorzowie zatrzymano 2 osoby pochodzenia bułgarskiego, z których jedna była członkiem rozpracowywanej zorganizowanej grupy przestępczej.
- ICARUS – operacja międzynarodowa ukierunkowana na zwalczanie pornografii dziecięcej, którą koordynował AWF FP Twins. Dzięki materiałom przekazanym przez Europol w Polsce dokonano 16 przeszukań, które skutkowały zatrzymaniem 17 osób oraz zabezpieczeniem materiału dowodowego, który stanowiło: 21 komputerów, 41 dysków, 2607 płyt CD i DVD, 101 kaset VHS i 4 mobilne nośniki pamięci.
- BLUE BALSAM – operacja dotycząca zwalczania nieuczciwej konkurencji w branży produkcji i dystrybucji kosmetyków. Europol uzyskał informację od firmy produkującej kosmetyki, że na rynku europejskim, m.in. w Rumunii i Wielkiej Brytanii, pojawiają się podrobione produkty oznakowane jej marką. W czerwcu 2012 r. informacja ta została przekazana do Polski, co umożliwiło realizację operacji, podczas której zabezpieczono: 10 ton podrobionego proszku do prania, 12 tys. butelek oraz 60 tys. etykiet szamponu, 8,2 tys. butelek z perfumami.
- OPTIQUE 40 – operacja zrealizowana przez Polskę oraz Francję, przy wsparciu informacyjnym Europolu. Była skierowana przeciwko polskiej grupie przestępczej dokonującej włamań do obiektów i kradzieży sprzętu optycznego. Europol zapewnił analizę danych przekazanych przez Polskę i Francję oraz zorganizował i sfinansował spotkania operacyjne, z których jedno odbyło się na terenie Polski, w Słupsku. Akcja zakończyła się zatrzymaniami członków grupy, którzy przebywali we Francji i w Polsce.

Andrzej Czop

10 lat polskiej Policji w Europolu, 3.06.2014, Policja.pl (dostęp 10.12.2019); A. Czop, *Europol*, *Interpol*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć

(red.), Wydawnictwo Libron, Kraków 2018; T. Safjański, *Europejskie Biuro Policji Europol: geneza, główne aspekty działania, perspektywy rozwoju*, Wolters Kluwer Polska, Warszawa 2009; tenże, *Efektywność działań operacyjnych Europolu w zwalczaniu terroryzmu międzynarodowego – próba oceny*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8; tenże, *Pozycja EuroPolu w architekturze bezpieczeństwa*, „Zeszyty Naukowe AON" 2014, nr 1 (94).

F

FAKEAPP – popularny program komputerowy, który pojawił się w styczniu 2018 r. i który za pomocą mocy obliczeniowej karty graficznej jest w stanie stworzyć algorytm, który do dowolnego wideo wstawi obraz twarzy na podstawie przeanalizowanego wcześniej materiału graficznego. Ta aplikacja umożliwia użytkownikom łatwe zmanipulowanie wideoklipów, pozwala na tworzenie i udostępnianie filmów wideo, w których zamieniono obrazy twarzy, jest to rodzaj automatycznego Photoshopa dla filmów. Program wykorzystuje sztuczną sieć neuronową i moc obliczeniową nowoczesnego procesora graficznego oraz od 3 do 4 GB przestrzeni dyskowej do generowania fałszywego wideo.

Dla uzyskania przekonujących efektów wymaga dużej ilości materiału wizualnego, na podstawie którego program, wykorzystując głębokie uczenie (ang. *deep learning*), będzie potrafił podmienić w sekwencjach wideo obrazy twarzy na inne. Potrzebne jest minimum 500 dobrej jakości zdjęć portretowych osoby (bardzo dobre efekty można uzyskać, mając 2–3 tys. ujęć), na podstawie których aplikacja „uczy się" danej twarzy, a następnie samodzielnie ją podmienia. „Nowa" twarz zachowuje się tak jak oryginał. Generowane tą metodą montaże przez internetową społeczność zostały nazwane → d e e p f a k e ' a m i, na początku dotyczyły głównie wstawiania twarzy aktorek, piosenkarek i celebrytek do scen z filmów dla dorosłych.

Zostało to wykorzystane do stworzenia fałszywych, ale czasami bardzo przekonujących pornograficznych klipów z rzekomym udziałem aktorek takich jak Gal Gadot i innych. Nie brakowało także czysto humorystycznych filmików, np. takich, w których twarze innych aktorów zostały zastąpione twarzą N. Cage'a, prezentowano także fałszywe nagrania z B. Obamą. Nic dziwnego, że tego typu filmiki błyskawicznie rozpowszechniły się przede wszystkim w portalach społecznościowych. Program korzysta z zasobów ogólnie dostępnych serwisów Google'a, generując rezultaty o niespotykanej dotychczas jakości. Na stronach internetowych znajdują się całe kolekcje klipów wyprodukowanych w FakeApp. Niektóre platformy, takie jak Reddit albo Twitter, zbanowały wiele takich treści.

Technologia, która stoi za tymi filmami, istnieje już od jakiegoś czasu, ale ogromną różnicą jest to, że dziś oprogramowanie jest dostępne wszędzie i jest łatwe w użyciu. Wystarczy pobrać program FakeApp i postępować zgodnie z instrukcją. Inny, podobny program – FaceApp – automatycznie generuje bardzo realistyczne transformacje twarzy na zdjęciach. Pozwala na zmianę stylu fryzury, płci, wieku i innych cech za pomocą smartfona.

Fala pornograficznych scen z rzekomym udziałem gwiazd kina, muzyki i celebrytek, powstałych dzięki zastosowaniu zaawansowanej sztucznej inteligencji, nie tylko pokazuje możliwości technologii, ale dowodzi, że każdy może z niej korzystać. W sieci coraz popularniejsza staje się aplikacja oparta na skrypcie, który powoli zbliża nas do rzeczywistości, w której wszystko jest możliwe. Sfabrykowanych materiałów z politykami nie rozpozna nikt, a wideo jako dowód sądowy przestanie mieć jakikolwiek sens.

Niedawne postępy w sztucznej inteligencji skutkowały wytworzeniem nowych sposobów tworzenia fałszywych i zmanipulowanych filmów. Korzystając ze specjalnego oprogramowania, takiego jak Face2Face i Project Voco, naukowcy mogli zamienić zdjęcie śnieżnego krajobrazu na wiosnę, symulować mimikę twarzy i ruch warg, a nawet stworzyć oryginalną treść mówioną na podstawie głosów polityków. Można tu wspomnieć np. o fałszywym nagraniu Obamy mówiącego o przepłacaniu pracowników, który wygląda i brzmi jak prawdziwa osoba.

Zdarzały się przypadki, w których młode dziewczyny były zmuszane do samobójstwa z powodu sfałszowanych obrazów i szantażowane przez

istnienie fałszywych profili zawierających treści pornograficzne. Wiele osób ma bardzo rozbudowaną obecność w →mediach społecznościowych [t. 3] lub tworzy i przesyła wideo na YouTube'a, co może ułatwić gromadzenie danych i stanowić →zagrożenie [t. 4] dla tych osób oraz uczynić je celem nękania, kampanii nienawiści i szantażu.

Wyprodukowana za pomocą technologii pornografia dziecięca, oparta na częściowo lub całkowicie wytwarzanych komputerowo obrazach, rodzi ważne pytania etyczne, a nowe przepisy będą konieczne, aby chronić ofiary i usunąć tę szarą strefę.

Obecnie generowanie obrazów za pomocą FakeApp można co najwyżej uznać za naruszenie prywatności i danych, naruszenie praw autorskich, nękanie lub zniesławienie. Ponieważ większość szkód dokonuje się poprzez krążenie materiałów w sieci, powstrzymywanie i zapobieganie temu jest prawie niemożliwe przy dzisiejszej technologii. Dokładne motywacje twórców i widzów są niejasne i należy się zastanowić, czy konsumenci mediów uczestniczą w tworzeniu popytu.

Pokrzywdzeni są zdegradowani i odhumanizowani, cierpią z powodu obrażeń psychicznych, uszkodzenia ich reputacji, stają się ofiarami fałszywej narracji, której nie mogą się sprzeciwić. Te nowe zastosowania technologii wywołają dyskusje i wszyscy – prawodawcy, badacze, widzowie – będą musieli współpracować, aby zapobiec złemu wykorzystaniu zaawansowania technologicznego.

W rzeczywistości →fake newsów obawy budzi także możliwość tworzenia takich sfałszowanych materiałów z udziałem ważnych osób świata polityki, biznesu czy sportu.

Połączeniu twarzy D. Trumpa wklejonej do przemówienia A. Merkel trudno odmówić walorów humorystycznych, lecz nietrudno domyślić się, co ktoś pozbawiony poczucia humoru i zdeterminowany do osiągnięcia politycznego celu mógłby potencjalnie zrobić. Jeden podstawiony gest, grymas, wypowiedziane zdanie mogą w jednej chwili zmienić nastawienie →opinii publicznej [t. 3], a przy dzisiejszym tempie rozprzestrzeniania się fałszywych →informacji w sieci, także wpłynąć na relacje międzynarodowe.

Na ten moment aplikacja FakeApp dostępna jest w wersji dla Windows. Po jej pobraniu i zainstalowaniu potrzebne są także dostępne za darmo

narzędzia deweloperskie, takie jak CUDA firmy NVIDIA i Visual C++ Microsoftu oraz FFmpeg (FFmpeg jest kompletnym pakietem elementów umożliwiających nagrywanie, konwertowanie i streaming audio i wideo. Warto dodać, że ten zbiór narzędzi umożliwia konwersję pomiędzy różnymi formatami wideo i jest całkowicie wolny i rozpowszechniany na licencji GPL). Potem następuje proces głębokiego uczenia oprogramowania twarzy, która ma zostać zastąpiona, oraz tej należącej do przyszłej ofiary. Wymagane jest przygotowanie odpowiedniej liczby ujęć, przeprowadzenie ich dopasowania i „treningu" sztucznej inteligencji – to właśnie w tym momencie oprogramowanie uczy się detali wyglądu i mimiki charakterystycznych dla obu twarzy. Kolejny element to wyodrębnienie z filmu poszczególnych klatek i poddanie ich w aplikacji konwersji, po której film trzeba złożyć na nowo.

Sztuczna inteligencja potrafi m.in.: tworzyć trójwymiarowe modele twarzy ze zwykłych zdjęć; tworzyć oryginalne obrazy w odpowiedzi na żądanie (narysuj wulkan, ptaka, uliczkę); ocenić wartość estetyczną obrazu i zmodyfikować go tak, aby ją podnieść (oceny SI porównywano z tymi wystawionymi przez ludzi); samodzielnie zmieniać źródło oświetlenia i cienie na zdjęciu; tworzyć podkład dźwiękowy na podstawie obrazu niemego filmu; zmieniać detale wyglądu osoby (np. pozbawienie Trumpa włosów) podczas transmisji na żywo; zmieniać mimikę twarzy, np. dodawać osobom przekonujący uśmiech na zdjęciach portretowych.

Nietrudno sobie wyobrazić sytuację, gdy z tej technologii korzysta ktoś, kto chce osiągnąć jakiś polityczny czy ekonomiczny cel, kogo zamiarem jest sprowokowanie →agresji [t. 1] wymierzonej przeciwko konkretnej osobie lub grupie społecznej, kogo motywacją jest wykorzystanie sfałszowanych obrazów do wywoływania napięć politycznych. Problem jest uwzględniany przez jednostki rządowe. Główną metodą obrony przed wprowadzeniem w błąd jest zwiększanie świadomości odbiorców.

Olga Wasiuta, Sergiusz Wasiuta

Cyberspace Safety and Security: 9th International Symposium, CSS 2017, Xi'an China, 23–25.10.2017. Proceedings, Sheng Wen, Wei Wu, A. Castiglione (eds.), Springer, Cham 2017; D.R. Des Autels, *Social Networking Safety: It All Starts with the User*, BookCountry, 2013; A. Dodge, L. House, E. Johnstone, *Using Fake Video*

Technology To Perpetrate Intimate Partner Abuse, 25.04.2018, WithoutMyConsent.org (dostęp 15.03.2019); Y. Du Aafer, W. Yin, H. Droid, *APIMiner: Mining API-Level features for robust malware detection in Android*, [w:] *Security and Privacy in Communication Networks*, T. Zia, A. Zomaya, V. Varadharajan, M. Mao (eds.), Springer, Heidelberg 2013; A. Echamea, *Mastering Backbone.js*, Packt Publishing, Birmingham 2016; R. Heartfield, G. Loukas, *Protection Against Semantic Social Engineering Attacks*, [w:] *Versatile Cybersecurity. Advances in Information Security*, M. Conti, G. Somani, R. Poovendran (eds.), Springer, Cham 2018; Ł. Kruczkowski, *FakeApp – czy powinniśmy obawiać się aplikacji, która z każdego może zrobić gwiazdę filmów dla dorosłych?*, 30.01.2018, KomputerSwiat.pl (dostęp 18.04.2019); tenże, *FakeApp ponownie prezentuje swoje przerażające możliwości. Tym razem „ofiarą" jest Obama*, 18.04.18, KomputerSwiat.pl (dostęp 18.04.2019); P. Lehr, *Counter-Terrorism Technologies: A Critical Assessment Advanced Sciences and Technologies for Security Applications*, Springer, Cham 2018; D. Rivera, A. García, M.L. Martín-Ruiz i in., *Secure Communications and Protected Data for a Internet of Things Smart Toy Platform*, „IEEE Internet of Things Journal" 2019, vol. 6, no. 2; O. Wasiuta, S. Wasiuta, *FakeApp jako nowe zagrożenie bezpieczeństwa politycznego i informacyjnego*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 3; S. Wasiuta, *FakeApp*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

FAKE NEWS – popularna nazwa wszelkich materiałów i przekazów medialnych, zawierających →informacje, które są weryfikowalnym kłamstwem, rozumianym jako przeciwieństwo prawdy, a zatem wprowadzającym w błąd. Pojęciem tym określa się zarówno historię fantastyczną, będącą wytworem czyjejś wyobraźni, kłamstwem czy żartem, jak i celowe zmylenie odbiorcy, coraz częściej jednak fake newsem nazywa się twierdzenie, któremu zarzuca się, że jest nieprawdziwe. Coraz częściej oskarżenie o mijanie się z prawdą lub nawet posiadanie innej opinii na dany temat, zwłaszcza w polityce i medialnych komentarzach, bywa zamykane formułą, że tezy adwersarza są po prostu kolejnym fake newsem.

Tworzenie i rozpowszechnianie fałszywych wiadomości ma długą tradycję, która sięga odległych czasów. Jednym z najbardziej znanych przykładów jest wielkie księżycowe oszustwo z 1835 r., kiedy to „New York Sun" opublikował serię artykułów o odkryciu życia na Księżycu. Na początku XX w. zostały wydane *Protokoły mędrców Syjonu*, publikacja

opisująca rzekome żydowskie plany dominacji nad światem, która pozostaje jednym z najbardziej znanych zastosowań fałszywego tekstu do celów propagandowych. Najbardziej spektakularnym wśród najnowszych przykładów fake newsa jest „Flamandzka secesja" z 2006 r. Wówczas to belgijska telewizja publiczna podała wiadomość, że parlament flamandzki ogłosił niepodległość i secesję od Belgii, co wielu widzów błędnie odebrało jako prawdziwą wiadomość, a nie prowokacyjny żart.

Według wąskiej definicji fake newsa kluczowym kryterium są intencje nadawcy. Tego typu komunikat zgodnie z taką koncepcją jest materiałem stworzonym dla celów propagandowych, aby wywołać emocjonalną reakcję odbiorców i w ten sposób stworzyć lub wzmocnić istniejące uprzedzenia wobec określonej grupy lub osoby i uzyskać korzyści polityczne. Przykładem tak rozumianych fake newsów mogą być liczne wiadomości emitowane przez Pierwyj kanał (ros. Первый канал), główny kanał publicznej telewizji nadającej w Federacji Rosyjskiej, która w czasie → w o j n y h y b r y d o w e j [t. 4] z Ukrainą przedstawiała newsy prezentujące fikcyjne wydarzenia, by w ten sposób kształtować rosyjską i częściowo ukraińską → o p i n i ę p u b l i c z n ą [t. 3] co do natury i specyfiki trwającego konfliktu.

W szerszej definicji fake newsa za główne kryterium jego odróżnienia od innych informacji przyjmuje się niezgodność treści wiadomości ze stanem faktycznym. W takim ujęciu w grupie fake newsów znajdą się niezamierzone błędy w relacjach medialnych, takie jak np. nieprawidłowe doniesienie, że D. Trump usunął popiersie M.L. Kinga z Gabinetu Owalnego w Białym Domu, plotki pochodzące z mediów, → t e o r i e s p i s k o w e [t. 4], które są z definicji trudne do zweryfikowania jako prawdziwe lub fałszywe i zwykle pochodzą od ludzi, którzy uważają je za prawdziwe, materiały satyryczne, co do których uznać można za mało prawdopodobne, aby zostały błędnie zinterpretowane jako prawdziwe, oraz materiały medialne skrajnie stronnicze i wypaczające fakty, które wprowadzają w błąd, ale nie są całkowicie fałszywe.

Ogromnym polem działania dla twórców fake newsów jest internet. Przykładowo Wikipedia daje możliwość publikowania informacji encyklopedycznych wszystkim swoim użytkownikom. Głównym problemem jest jednak to, że publikowane informacje niekoniecznie muszą być prawdziwe i że wiele osób czytających te błędy, żarty lub kłamstwa akceptuje je,

traktując jako prawdę. J. Seigenthaler, amerykański pisarz i dziennikarz, doświadczył tego, gdy jego biografia na stronie została zmodyfikowana tak, iż pojawiła się w niej wzmianka, że był podejrzany o zabójstwo J.F. Kennedy'ego i R. Kennedy'ego. Fałszywe informacje pojawiły się na Wikipedii i były tam obecne przez dłuższy czas. Minęło ponad 100 dni, zanim zidentyfikowano i usunięto błędne informacje. Mając na uwadze szkody, które fake newsy mogą wyrządzić reputacji, ważne jest, aby pamiętać, że nie ma znaczenia, czy polegają na prawdzie, lecz istotne jest to, czy ludzie uwierzą, że to informacja jest prawdziwa.

Pomimo długiej historii fałszywych wiadomości istnieje kilka powodów, aby sądzić, że fake newsy mają coraz większe znaczenie. Po pierwsze, bariery wejścia na rynek w branży medialnej gwałtownie spadły, zarówno ze względu na łatwość zakładania stron internetowych, jak i łatwość zarabiania na treściach internetowych za pośrednictwem platform reklamowych. Ponieważ obawy przed utratą reputacji zniechęcają media do świadomego zgłaszania fałszywych newsów, zwykle nawet odkrycie pomyłki czy zwykłego błędu nie prowadzi do ogłoszenia tego i wycofania się z podanego fake newsa. Po drugie, → m e d i a s p o ł e c z n o ś c i o w e [t. 3] są dobrze przystosowane do fałszywego rozpowszechniania wiadomości, a ich wykorzystanie gwałtownie wzrosło: w 2016 r. liczba aktywnych użytkowników Facebooka miesięcznie osiągnęła 1,8 mld, a Twittera ponad 400 mln. Po trzecie, wyraźny jest ciągły spadek zaufania do środków masowego przekazu jako źródła w pełni dokładnych i rzetelnych wiadomości. Utrata zaufania do mediów głównego nurtu może być zarówno przyczyną, jak i konsekwencją coraz większej liczby fake newsów.

Chociaż fałszywe wiadomości odgrywały ważną rolę już w okresie I i II wojny światowej, termin fake news zyskał na znaczeniu podczas amerykańskiej prezydenckiej kampanii wyborczej w 2016 r. Monitorowanie tego terminu w Google pokazało znaczny wzrost liczby jego wyszukiwań w okresie wyborów w listopadzie 2016 r. w Stanach Zjednoczonych, a Trumpowi przypisuje się wykorzystanie tego terminu w dyskursie publicznym podczas jego pierwszej konferencji prasowej w styczniu 2017 r. Trump i inni politycy amerykańscy uzurpowali sobie ten termin i wykorzystali go do określenia nim treści pochodzących z tradycyjnych źródeł medialnych, takich jak „The New York Times" czy telewizja CNN,

z którymi się nie zgadzali. W ten sposób termin ten uzyskał status pejoratywnej etykiety dla liberalnych mediów i utracił powszechnie akceptowane znaczenie.

Podjęte zostały także poważne starania, aby sklasyfikować fałszywe wiadomości i zidentyfikować źródła → d e z i n f o r m a c j i. Jeden z takich wysiłków zaowocował stworzeniem wkrótce po wyborach w listopadzie 2016 r. bazy danych witryn posortowanych wg 13 kategorii, które były – zdaniem twórców zestawienia – odpowiedzialne za tworzenie i rozpowszechnianie fake newsów. Wysiłek ten był przedmiotem dużej krytyki z uwagi na uwzględnienie źródeł wiadomości uważanych częściej za krytyczne niż fałszywe, a także z powodu niedoskonałej typologii opartej na pokrywających się kategoriach. Obawy przed fake newsami często obracają się wokół pytania, co jest lub nie jest uważane za prawdziwe, stanowiąc podstawę do publicznej dyskusji, szczególnie w okresach wyborów.

Fałszywe artykuły prasowe odegrały dużą rolę w ważnych wydarzeniach politycznych, takich jak wybory prezydenckie w USA, głosowanie nad opuszczeniem struktur Unii Europejskiej przez Wielką Brytanię czy w trakcie wojny hybrydowej Rosji w Ukrainie. Badacze ustalili, że fake newsy pochodzą z kilku rodzajów stron internetowych. Np. niektóre witryny są tworzone wyłącznie w celu generowania umyślnie sfabrykowanych i wprowadzających w błąd artykułów, jak np. DenverGuardian.com. Nazwy takich stron są często wybierane tak, aby przypominały wiarygodne serwisy informacyjne. Inne witryny (satyryczne) zawierają artykuły, które mogą być interpretowane jako prawdziwe, gdy są oderwane od kontekstu, jak np. witryna WTOE5News.com. Jeszcze inne witryny, takie jak sprzyjająca Trumpowi EndingTheFed.com, publikują mieszankę artykułów prawdziwych, często stronniczych, wraz z kilkoma fałszywymi materiałami. Witryny dostarczające fałszywych wiadomości mają tendencję do krótkiej egzystencji, a wiele z nich – ważnych w okresie poprzedzającym wybory w 2016 r. w USA – wkrótce przestało istnieć. Oddzielne dochodzenia przeprowadzone przez BuzzFeed i „The Guardian" ujawniły, że ponad 100 stron publikujących fałszywe wiadomości było prowadzonych przez nastolatków w Wełesie (maced. Велес), małym miasteczku w Macedonii. EndingTheFed.com, strona, która była odpowiedzialna za 4 z 10 najpopularniejszych fałszywych wiadomości na Facebooku, była

prowadzona przez 24-letniego mężczyznę z Rumunii. Amerykańska firma o nazwie Disinfomedia posiada wiele fałszywych witryn z wiadomościami, w tym NationalReport.net, USAToday.com.co i WashingtonPost.com.co, a jej właściciel twierdził, że zatrudnia od 20 do 25 autorów. Inny właściciel strony z fake newsami z USA, P. Horner, prowadził fałszywy serwis informacyjny o nazwie National Report na wiele lat przed wyborami prezydenckimi w 2016 r. Wśród jego najbardziej rozpowszechnionych fake newsów był materiał z 2013 r., w którym opisano, że prezydent B. Obama wykorzystał swoje własne pieniądze, aby utrzymać muzeum muzułmańskie. Podczas wyborów Horner wyprodukował wiele fake newsów, głównie sprzyjających kandydaturze Trumpa.

Wskazuje się, że istnieją 2 główne motywacje do dostarczania fake newsów. Pierwsza z nich ma charakter finansowy: artykuły z wiadomościami, które stają się popularne w mediach społecznościowych, mogą przyciągnąć znaczne przychody z reklam. Wydaje się, że był to główny powód dla większości autorów, których tożsamość została ujawniona. Na przykład nastolatkowie w Wełesie tworzyli historie faworyzujące zarówno Trumpa, jak i H. Clinton, zarabiając dzięki nim dziesiątki tysięcy dolarów. Horner tworzył protrumpowskie doniesienia dla zysku, wbrew stwierdzeniom, że jest osobiście przeciwny Trumpowi. Drugi rodzaj motywacji ma charakter ideologiczny. Niektórzy dostawcy fake newsów starają się dzięki nim wyrazić poparcie dla kandydatów, których popierają. Twórca fake newsów z Rumunii, który prowadził portal EndingTheFed.com, twierdził, że stworzył witrynę głównie w celu pomocy w kampanii Trumpa.

Od początku swojej kampanii prezydenckiej i politycznie oryginalnej prezydentury Trump prowadził wojnę z mediami. Walka mediów i codzienne ataki Trumpa na media poprzez jego kampanie na Twitterze i spostrzeżenia wygłaszane w sprzyjających mu mediach były znaczącą cechą zarówno kampanii prezydenckiej Trumpa, jak i początków jego prezydentury. Kiedy media krytykowały jego wypowiedzi lub działania, Trump kontynuował atak. Kiedy składał wątpliwe lub ewidentnie fałszywe oświadczenia i przedstawiano mu dowody obnażające ich nieprawdziwość, Trump i jego stronnicy odrzucali wszelką krytykę jako fake newsy i „alternatywne fakty". Odwołując się do Mao i Stalina, Trump nazywał media głównego nurtu „wrogami ludu" i kontynuował wypowiadanie

się przeciwko mediom poprzez Twittera. Skala i zakres stosowania fake newsów oraz oskarżeń o wykorzystywanie sfałszowanych wiadomości kierowanych pod adresem wszystkich oponentów przez kandydata na prezydenta, a później głowę państwa doprowadziły do trudnej dla przeciętnych obywateli sytuacji zaniku orientacji w tym, co jest i co może być prawdą, a co fałszem.

Uwagę badaczy fake newsów zwracają mechanizmy, za pomocą których można wpływać na uwagę odbiorców. Istnieją aplikacje umożliwiające szybkie wzmocnienie emocjonalnie nacechowanych wiadomości na platformach takich jak Twitter. To strategiczne narzędzia sterujące uwagą, które mogą przyspieszyć rozprzestrzenianie się dezinformacji i tworzenie alternatywnych faktów. Gdy użytkownik Facebooka pisze określone słowa, aplikacja wpływa na słowa wybrane później przez ich przyjaciół. Podobnie działają narzędzia do dzielenia się oparte na sentymentach, jak np. emocje „reakcji" na Facebooku, które dodatkowo komplikują problem zniekształceń społecznych, ponieważ kodyfikują i agregują uczucia związane z wiadomościami. Oznacza to, że nawet jeśli kontrowersyjny fake news może być odpowiednio zweryfikowany pod kątem faktów, już wcześniej może wzbudzić oburzenie lub zamieszanie docelowych odbiorców. Zasadniczym problemem dotyczącym fake newsów i portali społecznościowych jest funkcjonowanie całej branży tradycyjnie skoncentrowanej na tworzeniu widowni. Poprzez gromadzenie szczegółowej wiedzy na temat ludzkich, często najintymniejszych, pragnień i upodobań, platformy opracowują narzędzia zarządzania konkretnymi potrzebami, kierowania nimi i wytwarzania ich. Podstawowa działalność firm technologicznych obejmuje projektowanie systemów gromadzenia i profilowania danych opartych na tożsamości. Oznacza to zarówno potencjalną możliwość adresowania fake newsów do określonej grupy odbiorców, dla której dana treść jest emocjonalnie czy z innych przyczyn istotna, jak i możliwość kreowania oczekiwań użytkowników portali społecznościowych do odbioru nieprawdziwych treści.

W wielu środowiskach pojawia się pytanie o możliwości walki z fake newsami. Jedna z metod wykorzystywana jest na Ukrainie. →Kryzys w tym państwie dowiódł silnej pozycji rosyjskiej telewizji jako najsilniejszego atutu rządu w jego →wojnie informacyjnej [t. 4].

Internet pozwolił jednak innym użytkownikom kwestionować narrację Kremla, tworząc odpowiedzi na fake newsy i obalając zniekształcone informacje i fałszywe obrazy. Założenia te realizuje witryna StopFake.org. Została ona uruchomiona w marcu 2014 r. w Kijowie jako projekt walki z dezinformacją pochodzącą głównie z rosyjskich mediów i internetu. Inicjatorami działań na początku byli studenci dziennikarstwa, ale dołączyli do nich wkrótce inni profesjonaliści i doświadczeni komputerowo użytkownicy internetu z Ukrainy i innych krajów. Społeczność mobilizuje zwykłych użytkowników internetu do angażowania się w wykrywanie i ujawnianie fake newsów, sfabrykowanych historii i obrazów na temat kryzysu na Ukrainie za pomocą przycisku „zgłoś fake news".

Problemem związanym z fake newsami pozostaje w szczególności rosnący zakres i zasięg ich wykorzystania, który należy wiązać także z powszechnym dostępem do takich aplikacji jak → F a k e A p p czy techniki → d e e p f a k e, które umożliwiają nie tylko specjalistom i ekspertom, ale w zasadzie każdemu użytkownikowi internetu, nawet posiadającemu przeciętne umiejętności, wygenerowanie w dowolnym celu określonego fake newsa zaopatrzonego w film, obraz czy nagranie dźwiękowe wytworzone przy użyciu specjalnego oprogramowania. W konsekwencji powszechnego wykorzystania takich narzędzi nie tylko polityka czy biznes, ale także codzienne relacje międzyludzkie mogą stać się elementem → p o s t - p r a w d y [t. 3], zbudowanej z trudnych do oddzielenia od siebie faktów i elementów wygenerowanych przez zainteresowanych lub osoby trzecie.

Jakub Idzik, Rafał Klepka

J. Albright, *Welcome to the Era of Fake News*, „Media and Communication" 2017, vol. 5, iss. 2; M. Dentith, *The Problem of Fake News*, „Public Reason" 2017, vol. 8, iss. 1–2; H. Allcott. M. Gentzkow, *Social Media and Fake News in the 2016 Election*, „Journal of Economic Perspectives" 2017, vol. 31, no. 2; M. Cross, *Social Media Security: Leveraging Social Networking While Mitigating Risk*, Elsevier, Amsterdam 2014; *Fake News: A Roadmap*, J. Althuis, L. Haiden (eds.), NATO Strategic Communications Centre of Excellence, Riga 2018; J. Idzik, R. Klepka, *Fake news*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; N. Jankowski, *Researching Fake News: A Selective Examination of Empirical Studies*, „Javnost – The Public" 2018, vol. 25, iss. 1–2; D. Kellner, *Trump's War Against the Media, Fake News, and*

(A)Social Media, [w:] *Trump's Media War*, C. Happer, A. Hoskins, W. Merrin (eds.), Palgrave Macmillan, Cham 2019; I. Khaldarova, M. Pantti, *Fake News*, „Journalism Practice" 2016, vol. 10, iss. 7; R. Klepka, *Fake news (Fałszywa wiadomość)*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Obrazy polityki w mediach: podstawowe uwarunkowania*, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018; E. Tandoc Jr., Z. Wei Lim, R. Ling, *Defining Fake News*, „Digital Journalism" 2017, vol. 6, iss. 2; O. Wasiuta, S. Wasiuta, *Medialna manipulacja informacją w wojnie hybrydowej Rosji przeciwko Ukrainie*, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018; D. Welch, *Fakes*, [w:] *Propaganda and Mass Persuasion. Historical Encyclopedia 1500 to the Present*, N. Cull, D. Culbert, D. Welch (eds.), ABC-CLIO, Santa Barbara–Denver–Oxford 2003.

FARMAKOLOGIZACJA WOJNY – celowe zastosowanie wśród stron biorących udział w konflikcie zbrojnym środków odurzających, takich jak alkohol i narkotyki, mających na celu: wydłużenie okresu koncentracji →ż o ł n i e r z y [t. 4], redukcję potrzeby snu, redukcję stresu, redukcję strachu, zwiększenie odwagi itp. Pojęcie „farmakologizacja wojny" zostało użyte w wydanej w 2012 r. książce Ł. Kamieńskiego *Farmakologizacja wojny. Historia narkotyków na polu bitwy*, przetłumaczonej 4 lata później i wydanej przez Oxford University Press po tytułem *Shooting Up: A Short History of Drugs and War*. Zdaniem autora przykłady stosowania środków odurzających do celów militarnych znaleźć można już w → w o j n a c h [t. 4] okresu starożytnego i średniowiecza. Asasyni w XI w. używali haszyszu, który miał pomagać przełamać strach przed dokonywaniem morderstw. Plemiona stepów Azji Północnej zamieszkujące Syberię spożywały wysuszone grzyby muchomora czerwonego, który zwiększał siłę fizyczną, uśmierzał ból oraz utrzymywał umysł w stanie wyjątkowego pobudzenia. Sukcesy militarne państw zachodnich w Chinach w XIX w. wynikały m.in. z faktu, iż ponad 90% żołnierzy armii cesarskiej było uzależnionych od opium, co pozwala nazwać chińską armię tamtego okresu największą „makową armią" świata. Środki odurzające były stosowane również w czasie wojny secesyjnej, gdzie masowe używanie morfiny i opium doprowadziło do powstania tzw. żołnierskiej choroby. W czasie II wojny światowej armia niemiecka zaopatrywała swoich żołnierzy w środek o nazwie pervitin,

będący pochodną metamfetaminy. 2 tabletki eliminowały potrzebę snu na 3–8 godzin. W czasie → z i m n e j w o j n y [t. 4] CIA prowadziło szereg badań nad wykorzystaniem środków odurzających, mających na celu wypracowanie skutecznych technik przesłuchiwania jeńców, wymazywania pamięci czy uzyskania kontroli nad umysłem. Przykładem był projekt MKUltra z lat 50. XX w., opisany przez prasę w latach 70. XX w.

Problem wykorzystania środków odurzających do celów militarnych poruszył także L. Rózsa w pracy *A Psychochemical Weapon Considered by the Warsaw Pact: A Research Note*, w której opisał, jak państwa Układu Warszawskiego, podobnie jak CIA w latach 50. XX w., pracowały nad metodami zastosowania środków odurzających mających na celu obezwładnianie sił zbrojnych przeciwnika.

Obecnie środki odurzające stosowane są zarówno przez regularne siły zbrojne, jak również ugrupowania terrorystyczne. Podczas I wojny w Zatoce Perskiej amerykańskim pilotom podawana była amfetamina celem utrzymania koncentracji w czasie wykonywania lotów bojowych. Siły zbrojne USA, Wielkiej Brytanii, Kanady i Francji interesują się również środkiem o nazwie modafinil – substancją o działaniu pobudzającym, wykorzystywaną medycznie do leczenia narkolepsji. W przeciwieństwie do innych stymulantów modafinil nie wywołuje skutków ubocznych poza zmniejszeniem odporności organizmu. Do tej pory poza siłami powietrznymi wykorzystywany był również w wojskach powietrzno-desantowych i → m a r y n a r c e w o j e n n e j [t. 4]. Od 1999 r. badania nad wojskowym wykorzystaniem środków farmakologicznych prowadzi również chińska armia. Jednym z jej efektów jest środek o nazwie „Nocny orzeł" (Night Eagle), którego działanie umożliwia utrzymanie czujności do 72 godzin. Może być podawany ratownikom podczas trzęsień ziemi i powodzi lub żołnierzom prowadzącym operacje wojskowe w trudnych warunkach środowiskowych, np. w górach, gdzie dostępność tlenu jest ograniczona. Na Bliskim Wschodzie w szeregach bojowników → P a ń s t w a I s l a m s k i e g o [t. 3] bardzo często stosowany był captagon (fenetylina) – związek chemiczny zawierający amfetaminę, wprowadzony do lecznictwa w 1961 r. Pierwotnie captagon był wykorzystywany do leczenia pacjentów z deficytem uwagi w zespole nadpobudliwości ruchowej (ADHD), stanów narkolepsji oraz jako lek przeciwdepresyjny. Wykorzystywany przez

ugrupowania terrorystyczne spełnia 2 funkcje. Po pierwsze, jego produkcja i sprzedaż stanowi jeden z głównych dochodów takich ugrupowań, jak Ludowy Front Wyzwolenia Palestyny, Hamas, Hezbollah czy Islamski Dżihad. Po drugie, działanie captagonu powoduje wzrost agresji i zmniejszenie poczucia empatii. Zażywający go terroryści gotowi są do nadludzkiego wysiłku, koncentracji utrzymującej się 2–3 dni oraz okrucieństw w stosunku do →ludności cywilnej [t. 3] i pojmanych jeńców.

Tomasz Wójtowicz

K. Dongsoo, *Practical Use and Risk of Modafinil, a Novel Walking Drug*, „Environmental Health and Toxicology" 2012, vol. 27; Ł. Kamieński, *Farmakologizacja wojny. Historia narkotyków na polu bitwy*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012; tenże, *Shooting Up: A Short History of Drugs and War*, Oxford University Press 2016; M. Motyka, J.T. Marcinkowski, *Captagon – narkotyk używany przez terrorystów*, „Problemy Higieny i Epidemiologii" 2016, vol. 2; L. Rózsa, *A Psychochemical Weapon Considered by the Warsaw Pact: A Research Note*, „Substance Use & Misuse" 2009, no. 44 (2); T. Wójtowicz, *Wykorzystywanie środków farmakologicznych przez Chińską Armię Ludowo-Wyzwoleńczą*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2018, nr 8.

FASZYZM (wł. *fascismo*, od łac. *fasces* – wiązki, rózgi liktorskie, pęk rózg z zatkniętym w nich toporem, symbol władzy funkcjonariuszy w starożytnym Rzymie towarzyszących najwyższym urzędnikom – oraz od wł. *fascio* – wiązki, związek, w zn. liga, partia) – można rozumieć na kilka sposobów. Po pierwsze, faszyzm jest ruchem społeczno-politycznym, którego początek istnienia wiązać należy z inicjatywą włoskiego nauczyciela i dziennikarza B. Mussoliniego (późniejszego twórcy Narodowej Partii Faszystowskiej, twórcy „Czarnych Koszul", premiera, dyktatora), który 23 marca 1919 r. w mediolańskiej hali na Piazza San Sepolcro powołał do istnienia organizację Fasci italiani di combattimento (Związki Kombatanckie), przekształconą w 1921 r. w partię faszystowską. W drugim znaczeniu faszyzm jest →reżimem [t. 3] politycznym utożsamianym z totalitarystycznym stylem rządzenia, który w klasycznej, czystej postaci funkcjonował w międzywojennych Włoszech. Natomiast trzecie znaczenie faszyzmu to ideologia społeczno-polityczna, której podstawowymi wyznacznikami są: idea autokratyzmu pod postacią charyzmatycznego

wodza, „wspólnota ziemi i krwi" oraz antydemokratyczne, antyliberalne i skrajnie nacjonalistyczne hasła spotęgowane przez demagogię i wszechobecną → p r o p a g a n d ę [t. 3], a także w skrajnych przypadkach szowinizm i rasizm. Do wyznaczników tych O. Grott dodaje monopartyjne rządy, totalną indoktrynację oraz skrajny populizm, stworzenie „nowej kultury" i wychowanie „nowego człowieka", militaryzm będący konsekwencją imperializmu, gospodarkę planową, antyindywidualizm i antypersonalizm oraz światopogląd nieoparty na nauce Kościoła. Choć nietrudno doszukiwać się związków ówczesnych faszystów z włoskimi duchownymi, to należy tłumaczyć ten fakt utylitarystyczną koncepcją wykorzystania władz kościelnych do realizacji partykularnych interesów, tym bardziej że faszyzm, jak twierdził Mussolini, osiągnął poziom religii – sam więc na pewien sposób stał się religią dla swoich „wyznawców".

Część naukowców (historyków, politologów) uważa, że faszyzm był pewnego rodzaju fenomenem społeczno-politycznym i kulturowym, na którego początki złożyły się okoliczności, które w kontekście wydarzeń okresu dwudziestolecia międzywojennego wymienia A. Heywood: wstrząs po I wojnie światowej, militaryzm, frustracja charakterystyczna dla postawy nacjonalistycznej, „młodość" kultury demokratycznej, potęga wielkiego biznesu stanowiąca → z a g r o ż e n i e [t. 4] dla klasy średniej, strach wśród elit spowodowany rewolucją październikową oraz załamanie gospodarcze lat 20. i 30. XX w. Faszyzm miał być dla ówczesnych Włochów (i w znacznym stopniu tak było) ucieleśnieniem najwyższych uczuć narodowych i odzwierciedleniem narodowej dumy Włoch po latach socjalistycznej i bolszewickiej propagandy. W. Jabłonowski, jako znawca i wręcz propagator idei faszystowskiej, uważał, że poprzez faszyzm przemawiało sedno włoskiej idei zwycięstwa wartości narodowych, co wyrażało się w patriotycznym ruchu odrodzenia myśli nacjonalistycznej.

Faszyzm, nawiązując do rewolucyjnie nastawionych robotniczych organizacji końca XIX w., sytuował się pomiędzy pojęciami ideologii (w sferze teoretycznej) i rewolucji (w sferze praktycznej). O totalizmie faszyzmu świadczyło przekonanie o wyższości koncepcji („konstruktu") umysłu ludzkiego nad obiektywną rzeczywistością oraz przeświadczenie o posiadaniu władzy nad wszelkimi środkami → p r z e m o c y [t. 3]. Faszyzm jest pojęciem niezwykle szerokim w swej warstwie treściowej

i biorąc to pod uwagę, w szerokim znaczeniu jest kierunkiem i ruchem politycznym o totalitarnej podstawie programowej, odwołującym się do zasad ideologii faszystowskiej i będącym fundamentem faszystowskiego reżimu politycznego. Pierwszy program faszystów z Fasci italiani di combattimento pod względem ideologicznym był niezwykle niespójny. Zawierał bowiem następujące postulaty: obalenie monarchii, zawłaszczenie majątku kościelnego, nacjonalizację przemysłu zbrojeniowego, opodatkowanie „wojennych spekulantów", program płacy minimalnej i wprowadzenie ośmiogodzinnego dnia pracy, udział robotników w procesie zarządzania przemysłem, zniesienie senatu oraz wprowadzenie czynnego prawa wyborczego dla kobiet.

W faszyzmie rozumianym jako ideologia polityczna w centrum stawiano koncepcję zwartej wewnętrznie wspólnoty narodowej budującej swą siłę dzięki jedności jej części składowych. Jednakże tożsamość poszczególnych jednostek wchodzących w skład wspólnoty przestawała mieć jakiekolwiek znaczenie dla niej samej. Faszyzm odwracał właściwie znaczenie kluczowych dla zachodniej cywilizacji wartości. Podkreślano, że dla faszystów wolność miała oznaczać całkowite podporządkowanie, a demokracja zrównała się z → d y k t a t u r ą. Postęp dla faszystów wiązał się nierozerwalnie z koniecznością podejmowania ciągłej walki i → w o j n y [t. 4], natomiast tworzenie było na stałe związane z destrukcją. Tego typu postawa i stawianie partii faszystowskiej przez Mussoliniego na pozycji „trzeciej drogi" miało na celu nie tyle radykalne zerwanie z przeszłością, co utworzenie i utrzymywanie ruchu politycznego mającego w założeniu dopełnić Risorgimento (odradzanie, jednoczenie się Włoch).

Specyfika faszyzmu polegała więc na braku sprecyzowania jego swoistej ideologii. Nie można zatem mówić o stworzeniu pewnej podstawy, fundamentu pod wytworzenie w masowej świadomości Włochów określonych postaw zgodnych z monolitycznym zestawem idei. To pozornie dobre relacje z Kościołem na linii polityki bieżącej i kwestii doktrynalnych (szczególnie po zawarciu konkordatu 11 lutego 1929 r.) spełniały rolę faszystowskiego umocowania w społeczeństwie i dawały Mussoliniemu legitymację do sprawowania realnej władzy w europejskiej stolicy chrześcijaństwa. Faszyzm w oczach 2 głównych myślicieli nacjonalistycznych – E. Corradiniego (głównego teoretyka włoskiej doktryny narodowej

i założyciela Zrzeszenia Nacjonalistów Włoskich) oraz L. Federzoniego (dziennikarza, polityka, członka Wielkiej Rady Faszystowskiej), miał być ideologiczną odpowiedzią na problemy polityki wewnętrznej i zewnętrznej państwa. Miał być zatem utożsamieniem programu narodowego Włoch przełomu XIX i XX stulecia oraz pierwszych dekad wieku XX. Program ten był obliczony na pragmatyzm działalności faszystów w dążeniu do głównego celu – zdobycia masowego poparcia. Jak podaje B. Grott, faszystom chodziło zwłaszcza o pozyskanie włoskiego społeczeństwa i duchowieństwa, ponieważ religia we Włoszech była czynnikiem kluczowym dla „wymuszenia" posłuchu. Jednak pomimo pewnego uregulowania stosunków między partią faszystowską a Kościołem katolickim wciąż utrzymywał się konflikt, który mógłby ulec pogłębieniu wraz z postępującą radykalizacją środowisk faszystowskich. Stosunki, względnie poprawne, jakie kształtowały się pomiędzy faszystami a Kościołem, były więc konsekwencją bieżących potrzeb politycznych oraz podatnej na wpływy faszystów płaszczyzny kulturowej.

W *Doktrynie faszyzmu* (1932 r.) Benito Mussolini wyłożył podstawowe założenia, na których winna się opierać idea faszystowska. Były to m.in.: bezwzględne podporządkowanie się władzy duce (tytuł, jaki przyjął Mussolini, z wł. „wódz"), powszechne zdyscyplinowanie oraz radykalna zmiana obecnych stosunków społecznych i politycznych. Wszystko to wyrażać miała tzw. doktryna czynu. Faszyzm zakładał zastąpienie systemu kapitalistycznego systemem korporacyjnym, w którym najważniejszą zasadą był solidaryzm społeczny. Korporacjonizm miał być oparty na zbiorowych (obowiązkowych) umowach o pracę. Tworzone były syndykaty branżowe, które zrzeszały pracodawców i pracowników, były poddane regularnemu nadzorowi państwa i partii faszystowskiej. Korporacjonizmem włoskim zainteresowane były także środowiska polskiego → n a c j o n a l i z m u [t. 3]. K. Kawalec pisze, że ciekawa wydawała się perspektywa usprawnienia państwa poprzez podporządkowanie poważnej siły związków zawodowych oraz zapewnienie reprezentacji organizacjom społeczno-zawodowym. Budziło to zainteresowanie nie tylko w środowisku nacjonalistów, choć opinia obozu narodowego w tej materii nie była jednolita. Poparcie dla korporacjonizmu było domeną raczej „młodych" działaczy nacjonalistycznych, upatrujących w faszyzmie elementów pobudzających do działania

gospodarczego i politycznego. Pomimo walki faszyzmu z ustrojem kapitalistycznym nie brakowało opinii, jakoby korporacjonizm stanowił czynnik wykorzystujący kapitał, a nie go zwalczający. W warstwie deklaratywnej chodziło bowiem nie o „walkę" z kapitalistami, ale o wyzwolenie z ludu pracującego i posiadaczy kapitału siły jednoczącej naród, realizującej jego aspiracje.

Co do politycznej sfery założeń faszystowskich należy stwierdzić, iż wszelkie odmiany faszyzmu nawiązywały do decyzjonizmu C. Schmitta, który uznawał wyższość działania i decyzji politycznych wodza ponad demokratycznymi procedurami podejmowania decyzji. K. Dziubka podaje, iż negatywny stosunek Mussoliniego do liberalno-demokratycznych zasad funkcjonowania państwa wynikał z tego, iż wg duce stanowiły one tzw. przedsionek anarchii. Co ciekawe, dla Mussoliniego i jego popleczników głównym celem rozwiązywania konfliktów między państwami była wojna, natomiast ekspansja narodów miała stanowić o ich „żywotności". Pod koniec lat 30. XX w., za sprawą samego Mussoliniego, faszyzm zaczął dryfować w stronę antysemityzmu, a duce, będąc pod coraz większym wpływem A. Hitlera, w antysemityzmie zaczął upatrywać czynnika regenerującego faszystowski → r a d y k a l i z m [t. 3] (choć nie był on tak zajadły i konsekwentny jak w nazistowskich Niemczech). Ideologia faszystowska znalazła propagatorów w wielu krajach. Tzw. rodzima gleba kulturowa polskiej przestrzeni społecznej zadecydowała o tym, że faszyzm i towarzyszący mu totalizm nie zapanowały jednak nad tradycjonalistyczno-katolicką wersją nacjonalizmu polskiego. Podobnie było w przypadku Hiszpanii, Portugalii czy Francji (Action Française).

Traktując faszyzm, szczególnie w jego początkowej formie, bardzo powierzchownie, tzn. nie dostrzegając jego rzeczywistego, destrukcyjnego wpływu na szacunek do pewnych wartości i ich zachowanie, można było w nim dostrzec przeciwwagę dla z jednej strony → k o m u n i z m u, a z drugiej liberalnej demokracji (stąd „trzecia droga"). Jako rozwiązanie wielu problemów natury społecznej i politycznej ówczesnych Włoch, faszyzm miał służyć zabezpieczeniu socjalnemu i pokojowi społecznemu. Połączenie w faszyzmie elementów socjalizmu i nacjonalizmu wydawało się tak korzystnym i ciekawym rozwiązaniem, że włoski odpowiednik nacjonalizmu stał się w pierwszej fazie jego rozwoju atrakcyjny również

dla polskich nacjonalistów. Dopiero lata 30. XX w. przesądziły o zakwalifikowaniu faszyzmu do ideologii szkodliwych dla istoty polskiej kultury i wartości wyznawanych przez Kościół katolicki. Choć wyraźne zbliżenie doktryny polskich nacjonalistów do idei katolickiej nastąpiło dopiero pod koniec lat 20. XX w. (po wydaniu w 1927 r. słynnej broszury R. Dmowskiego pt. *Kościół, naród i państwo*), to faszyzm, pomimo wywodzenia się z kręgów kultury chrześcijańskiej, ostatecznie w pewnym sensie sprzeniewierzył się idei katolickiego państwa narodowego i lata 30. zadecydowały o zupełnie odmiennym charakterze włoskiego i polskiego nacjonalizmu. Pomimo wielu sporów naukowych i współczesnych debat na temat podobieństw i różnic polskiego nacjonalizmu oraz faszyzmu należy za Kawalcem dosyć jednoznacznie stwierdzić, iż zdecydowanych różnic było więcej niż pozornych podobieństw. Autor zauważa, że chociażby główny trzon Narodowej Demokracji, a więc Związek Ludowo-Narodowy, na wzór partii typu zachodnioeuropejskiego zarówno organizacyjnie, jak i programowo zasadniczo różnił się od formacji politycznej Mussoliniego, a do 1926 r., poza działaniami ekstremistycznymi, jedyne, co łączyło oba ruchy, to odwoływanie się do ideologii nacjonalistycznej – w swoistej dla każdej ze struktur formie.

Paweł Łubiński

K. Dziubka, *Faszyzm*, [w:] *Leksykon politologii wraz z aneksem reforma samorządowa w Polsce, partie, parlament, wybory (1989–1997)*, A. Antoszewski, R. Herbut (red.), Wydawnictwo Atla2, Wrocław 1999; R. Eatwell, *Faszyzm. Historia*, tłum. T. Oljasz, Dom Wydawniczy REBIS, Poznań 1999; E. Gentile, *Fascism as Political Religion*, „Journal of Contemporary History" 1990, vol. 25, no. 2/3; tenże, *Fascism, Totalitarianism and Political Religion: Definitions and Critical Reflections on Criticism of an Interpretation*, „Totalitarian Movements and Political Religions" 2004, vol. 4, no. 3; B. Grott, *Dylematy polskiego nacjonalizmu. Powrót do tradycji czy przebudowa narodowego ducha*, Wydawnictwo von Borowiecky, Warszawa 2014; O. Grott, *Ugrupowania faszystowskie i narodowosocjalistyczne w okresie międzywojennym na ziemiach polskich*, [w:] *Główne obozy polityczne II Rzeczypospolitej na tle wydarzeń epoki*, M. Ryba (red.), Wydawnictwo Katolickiego Uniwersytetu Lubelskiego, Lublin 2012; A. Heywood, *Klucz do politologii. Najważniejsze ideologie, systemy, postaci*, Wydawnictwo Naukowe PWN, Warszawa 2008; K. Kawalec, *Narodowa Demokracja wobec faszyzmu 1922–1939. Ze studiów nad dziejami myśli*

politycznej obozu narodowego, Państwowy Instytut Wydawniczy, Warszawa 1989; M. Kiwior-Filo, *Droga włoskiego nacjonalizmu do nacjonalfaszyzmu*, [w:] *Ideologie, doktryny i ruchy narodowe. Wybrane problemy*, S. Stępień (red.), Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2006; J.G. Kellas, *The Politics of Nationalism and Ethnicity*, Macmillan Press LTD, London 1998; A. Lew, *Fascynacja czy akceptacja? Włoski faszyzm w poglądach Władysława Jabłonowskiego (1922–1939)*, [w:] *Narodowa Demokracja XIX–XXI wiek. Dzieje ruchu politycznego. Księga pamiątkowa poświęcona pamięci profesora Romana Wapińskiego (1931–2008)*, t. 1, T. Sikorski, A. Wątor (red.), Wydawnictwo Adam Marszałek, Toruń 2012; P. Łubiński, *Faszyzm*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; M. Podstawski, *Faszyzm jako uosobienie mitu rewolucji czyli o modernistycznych strategiach społecznej suwerenności*, Wydawnictwo Adam Marszałek, Toruń 2012.

FORMACJE OBRONY CYWILNEJ – podstawowe jednostki organizacyjne realizujące zadania →obrony cywilnej [t. 3] (OC). Formacje są powoływane w drodze rozporządzenia przez ministrów oraz na mocy zarządzenia przez szefów obrony cywilnej województwa, powiatów i gmin, z jednoczesnym uwzględnieniem skali występujących →zagrożeń [t. 4], rodzaju formacji, ich przeznaczenia, stanu osobowego, a także organizacji wewnętrznej. Formacje mogą być tworzone również przez pracodawców.

Szefowie OC, powołując formacje OC, powinni wykorzystać instytucje i firmy, których profil działalności jest tożsamy z zadaniami poszczególnych formacji. Do realizacji zadań OC są zatem włączane jednostki ochotniczej straży pożarnej, inspekcje, straże oraz pozostałe jednostki organizacyjne, dysponujące specjalistycznym sprzętem oraz kadrami przygotowanymi do podejmowania działań w trakcie usuwania skutków zdarzeń nadzwyczajnych. W sytuacjach nadzwyczajnych, np. w stanie klęski żywiołowej, formacje muszą osiągnąć gotowość do działania w czasie kilkunastu godzin. Oprócz spełnienia wymogu profesjonalnego wyszkolenia i wyposażenia formacje OC mają służyć jako wsparcie w działaniach służb ratowniczych.

Ważne, aby zasoby sprzętowe dla potrzeb formacji OC z uwzględnieniem normatywu nie były przewidziane jedynie w przypadku ewentualnego zewnętrznego →zagrożenia bezpieczeństwa [t. 4] państwa i groźby wybuchu konfliktu militarnego. Zgodnie z obowiązującymi aktami urzędowymi Szefa Obrony Cywilnej Kraju zasoby powinny

być wykorzystywane w normalnych warunkach funkcjonowania państwa, w trakcie codziennych działań ratowniczych, a także w razie zagrożeń wymagających uruchomienia procedury udzielenia konkretnej pomocy humanitarnej. Zasoby OC w czasie → w o j n y [t. 4] nie powinny różnić się od unormowań funkcjonujących na co dzień. Niemniej jednak warto zauważyć, iż zadania OC w czasie pokoju i wojny znacznie się od siebie różnią, dlatego też zasoby sprzętowe również powinny ulec zróżnicowaniu, adekwatnie do realizacji poszczególnych zadań w określonym stanie zagrożenia. Najlepiej zorganizowanymi, najbardziej efektywnymi w swoich działaniach i w zasadzie jedynymi czynnie działającymi formacjami OC są ochotnicze straże pożarne, co potwierdziły wyniki raportu Najwyższej Izby Kontroli, sporządzonego w 2011 i 2018 r.

Wśród formacji wyróżnia się oddziały przeznaczone do wykonywania zadań ogólnych lub specjalnych oraz inne jednostki tych formacji. Formacje do zadań ogólnych są podstawowymi formacjami terenowymi oraz podstawowymi formacjami zakładowymi w zakładach niestwarzających zagrożenia skażeniem substancjami niebezpiecznymi. Są również podstawowymi formacjami, które wspomagają formacje specjalistyczne w zakładach cechujących się wysokim ryzykiem zagrożenia skażeniem. Formacje do zadań ogólnych realizują czynności pomocnicze, wspierające wykonywanie zadań przez służby i formacje przeznaczone do zadań specjalistycznych oraz inne służby i instytucje. Do czynności tych zalicza się: obsługę środków zaciemnienia; doraźne grzebanie zmarłych; → p i e r w s z ą p o m o c [t. 3] medyczną; przygotowanie i organizowanie schronów; dostarczanie doraźnych pomieszczeń i zaopatrzenia; doraźną pomoc w przywróceniu i utrzymaniu porządku w strefach dotkniętych klęskami; pomoc w ratowaniu dóbr koniecznych do przetrwania; odbudowę awaryjnych ujęć wody; ochronę płodów rolnych, produktów żywnościowych, zwierząt gospodarskich i pasz; dodatkowe rodzaje działalności, niezbędne dla wypełnienia któregoś z zadań protokołów dodatkowych do konwencji genewskiej, w tym planowanie i prace organizacyjne.

Formacje do zadań specjalnych bazują na działalności ochotniczych straży pożarnych, włączonych do Krajowego Systemu Ratowniczo-Gaśniczego (KSR-G), i innych lokalnych organizacjach pozarządowych, a także na specjalistycznych podmiotach komunalnych. Formacje przeznaczone

do realizacji zadań specjalistycznych to formacje profesjonalne, w pełni wyposażone, pozostające w natychmiastowej gotowości do działania, zarówno w gotowości obronnej państwa czasu → k r y z y s u, czasu wojny, jak i w miarę możliwości w stałej gotowości obronnej państwa.

Najbardziej charakterystycznymi rodzajami formacji specjalistycznych OC są formacje następujących rodzajów ratownictwa: chemicznego i ekologicznego, medycznego, technicznego, wodnego, wysokościowego oraz komunalnego.

Działania formacji ratownictwa chemicznego i ekologicznego polegają w głównej mierze na: rozpoznaniu i zabezpieczeniu miejsca zdarzenia oraz wyznaczeniu strefy zagrożenia; próbie identyfikacji zagrożenia; ewakuacji poszkodowanych i zagrożonych ludzi oraz zwierząt poza strefę zagrożenia; ostrzeganiu i alarmowaniu o zagrożeniu, a także informowaniu o zasadach właściwego postępowania; przeprowadzaniu pomiarów za pomocą dostępnych przyrządów; redukcji skutków wycieku substancji ropopochodnych; rozmieszczaniu kurtyn wodnych; dekontaminacji wstępnej ludzi na granicy strefy zagrożenia przy użyciu dostępnego sprzętu; udzielaniu kwalifikowanej pierwszej pomocy poza strefą zagrożenia; współdziałaniu z innymi podmiotami ratowniczymi, zwłaszcza ze specjalistycznymi grupami ratownictwa chemiczno-ekologicznego → P a ń s t w o w e j S t r a ż y P o ż a r n e j [t. 3] i wojskowymi zespołami ratownictwa chemicznego. Formacja składa się z komendanta oraz pozostałych członków legitymujących się uprawnieniami ratownika: chemicznego (18 osób), chemicznego z dodatkowym przeszkoleniem w zakresie zagrożeń czynnikami masowego rażenia – CBRN (6 osób), materiałów wybuchowych (6 osób), ochrony radiologicznej (6 osób), w zakresie transportu i magazynowania towarów niebezpiecznych oraz konstrukcji opakowań (6 osób), z zakresu kwalifikowanej pierwszej pomocy (18 osób), a także z uprawnieniami do obsługi pojazdów i sprzętu specjalistycznego, stanowiących wyposażenie formacji (6 osób).

Formacje ratownictwa medycznego realizują działania ratownicze w razie nieobecności zespołu ratownictwa medycznego, jeśli nie jest możliwe wykorzystanie personelu jednostek → o c h r o n y z d r o w i a [t. 3] (np. jeśli niemożliwe jest dotarcie do poszkodowanych znajdujących się w strefie zagrożenia) oraz w trakcie zdarzenia masowego. Do zakresu

obowiązków formacji ratownictwa medycznego należą głównie: udzielanie kwalifikowanej pierwszej pomocy poprzez rozpoznanie u osób poszkodowanych stanu nagłego zagrożenia zdrowotnego oraz dokonywanie segregacji pierwotnej lub udział w segregacji wtórnej; wykorzystanie technik i sprzętu niezbędnego do ratowania życia i zdrowia, z uwzględnieniem rodzaju, skali, miejsca zdarzenia oraz liczby poszkodowanych; zapewnienie ciągłości procedury ratowania osób znajdujących się w stanie nagłego zagrożenia zdrowotnego w miejscu zdarzenia. W ramach kwalifikowanej pierwszej pomocy ratownicy formacji zajmują się: tamowaniem krwotoków zewnętrznych i opatrywaniem ran; unieruchomieniem złamań i podejrzeń złamań kości oraz zwichnięć; ochroną przed wychłodzeniem lub przegrzaniem poszkodowanych; resuscytacją oddechowo-krążeniową; prowadzeniem wstępnego postępowania przeciwwstrząsowego; stosowaniem tlenoterapii biernej; ewakuacją z miejsca zdarzenia osób w stanie nagłego zagrożenia zdrowotnego; prowadzeniem segregacji pierwotnej, a także wsparciem psychicznym osób w stanie nagłego zagrożenia zdrowotnego. W skład formacji wchodzą: komendant; członkowie grupy z uprawnieniami ratownika (6 osób) oraz ratownicy uprawnieni do obsługi pojazdów i sprzętu specjalistycznego, jakimi dysponuje grupa (3 osoby).

Do obowiązków formacji ratownictwa technicznego w zakresie specjalistycznym należą przede wszystkim: wykonywanie zadań określonych dla ratownictwa technicznego w zakresie podstawowym; rozpoznanie i identyfikacja zagrożenia; zabezpieczenie strefy działań ratowniczych poprzez wyznaczenie i oznakowanie strefy zagrożenia; włączanie lub wyłączanie instalacji, urządzeń i mediów zapewniających → b e z p i e c z e ń s t w o [t. 1] osób poszkodowanych i ratowników; priorytetowe wykonanie czynności umożliwiających dotarcie i dostęp do zagrożonych lub poszkodowanych osób wraz z udzieleniem im kwalifikowanej pierwszej pomocy oraz ewakuacją poza strefę zagrożenia; organizowanie przejść, dojść i dojazdów do osób zagrożonych lub poszkodowanych wraz z usuwaniem przeszkód ograniczających dostęp do nich i utrudniających wykonanie medycznych działań ratowniczych; ewakuacja zagrożonych i poszkodowanych zwierząt poza strefę zagrożenia; ocena rozmiarów powstałego zagrożenia i prognozowanie jego rozwoju; oświetlenie miejsca zdarzenia

i jego zabezpieczenie przed osobami postronnymi oraz wykonywanie innych czynności na rzecz zabezpieczenia logistycznego; włączanie lub wyłączanie instalacji i urządzeń mających wpływ na rozmiar strefy zagrożenia; stabilizowanie lub przenoszenie konstrukcji, instalacji i urządzeń, a także części obiektów oraz przeszkód naturalnych i sztucznych w celu zlikwidowania lub ograniczenia zagrożenia dla osób, zwierząt, środowiska, infrastruktury i innego mienia. Formacje tego typu składają się z dowódcy formacji, 54 ratowników (30 z uprawnieniami hakowego oraz 18 z uprawnieniami do obsługi pojazdów i sprzętu będących na wyposażeniu grupy.

Formacje ratownictwa wodnego, realizując zadania z zakresu ratownictwa wodnego, zajmują się: rozpoznaniem i oceną zagrożenia dla życia i zdrowia; niesieniem pomocy tonącym (także na akwenach zalodzonych), poprzez dotarcie do poszkodowanych lub zagrożonych ludzi oraz udzielenie im kwalifikowanej pierwszej pomocy, a także przekazanie poszkodowanych poza strefę zagrożenia zespołom → Państwowego Ratownictwa Medycznego [t. 3]; ratowaniem życia ludzi na wodach powodziowych poprzez dotarcie do poszkodowanych lub zagrożonych osób oraz udzielenie im kwalifikowanej pierwszej pomocy i ewakuację poza strefę zagrożenia; zabezpieczeniem działań ratowniczych na lodzie oraz innym obszarze wodnym, zapewniając asekurację ratowników; ewakuacją ludzi i zwierząt z terenów zalanych, kry lodowej, obszaru wodnego, łodzi, pojazdów lub obiektów i urządzeń hydrotechnicznych; zabezpieczeniem działań technicznych, chemicznych i ekologicznych polegających na usuwaniu lub minimalizacji zagrożeń na obszarach wodnych, obszarach objętych powodzią i innych zbiornikach wodnych; współdziałaniem z podmiotami uprawnionymi do wykonywania zadań charakterystycznych dla ratownictwa wodnego. Obsadę etatową tejże formacji tworzą: komendant, członkowie z uprawnieniami ratownika (10 osób); ratownictwa lodowego (3 osoby); ratownictwa na rzekach górskich i wodach szybkopłynących (3 osoby); ratownictwa w czasie powodzi (10 osób); sterowania łodziami z napędem silnikowym adekwatnie do wymagań związanych z parametrami łodzi dostosowanej do rodzaju akwenu (dotyczy szkolenia dla podmiotów KSRG i formacji OC posiadających jednostki pływające z napędem silnikowym – 3 osoby).

Zadania formacji OC ratownictwa wysokościowego polegają głównie na: zabezpieczeniu poszkodowanego przed upadkiem z wykorzystaniem liny, pętli do asekuracji i uprzęży ewakuacyjnej oraz sprawnej ewakuacji osób, zwierząt i mienia z terenów i miejsc zagrożonych. Ratownictwo wysokościowe jest realizowane przez wszystkie jednostki ratowniczo-gaśnicze Państwowej Straży Pożarnej, jednostki ochrony przeciwpożarowej (jednostki OSP włączone do KSR-G, które zadeklarowały gotowość operacyjną do realizacji wspomnianych zadań oraz spełniają standardy gotowości, wyszkolenia i wyposażenia), a także przez inne podmioty ratownicze, które zadeklarowały gotowość operacyjną. Obsada etatowa formacji składa się z komendanta i 10 ratowników.

Formacja ratownictwa komunalnego składa się z zespołu energetycznego (zajmującego się prowadzeniem akcji ratunkowych w obiektach i rejonach, w których znajdują się uszkodzone lub zniszczone urządzenia energetyczne), zespołu pogotowia wodno-kanalizacyjnego (prowadzącego akcję ratunkową w obiektach i rejonach, w których znajdują się uszkodzone lub zniszczone sieci kanalizacyjne i wodociągowe) oraz z zespołu pogotowia gazowego (odpowiedzialnego za likwidację skutków i zabezpieczenie uszkodzonych sieci, stacji lub urządzeń gazowych). W skład formacji wchodzą: komendant, komendant zespołu energetycznego, sekcja pogotowania energetycznego, kierowca, komendant zespołu wodno-kanalizacyjnego, sekcja pogotowia sieci kanalizacyjnej, kierowca, sekcji usuwania awarii i remontu sieci wodociągowej, kierowca, komendant zespołu gazowego, sekcja pogotowia gazowego oraz jej kierowca.

Ponadto w strukturach OC działają również drużyny wykrywania i alarmowania, a także lotnicza formacja OC, powoływana przez szefa OC województwa – wojewodę, poprzez nadanie przydziałów organizacyjno-mobilizacyjnych personelowi lotniczemu, technicznemu i naziemnemu personelowi zabezpieczającemu aerokluby na obszarze jego działania.

Do obowiązków drużyn wykrywania i alarmowania należą: rozwinięcie posterunku wykrywania oraz alarmowania; utrzymanie stałej łączności z powiatowym ośrodkiem analizy danych i alarmowania; powołanie ze swego składu patroli rozpoznania skażeń; prowadzenie rozpoznania skażeń i rozpoznania ogólnego; prowadzenie obserwacji terenu; pobieranie próbek materiałów skażonych, wstępne określenie rodzaju i stopnia

skażenia oraz przekazywanie tych danych do analiz laboratoryjnych; analiza sytuacji wg danych z rozpoznania; określanie warunków atmosferycznych w przyziemnej warstwie powietrza; alarmowanie zagrożonej ludności za pośrednictwem scentralizowanych systemów i syren alarmowych oraz punktów alarmowania sołectw i zakładów pracy; powiadamianie szefa OC gminy o zagrożeniach i wnioskowanie w sprawie ostrzegania ludności; informowanie o skażeniach, napromieniowaniu, uderzeniach bronią masowego rażenia i innych nadzwyczajnych zagrożeniach ludności szefa OC gminy.

Lotnicza formacja OC zajmuje się: rozpoznaniem dróg, mostów i przepraw, a także stanu ruchu na nich dla potrzeb sił ratowniczych i ewakuacji ludności; prowadzeniem rozpoznania skutków ataków przeciwnika na obiekty przemysłowe, administracyjne, komunikacyjne i skupiska ludności; prowadzeniem rozpoznania ognisk pożarów i kierunków ich rozprzestrzeniania się; patrolowaniem obszarów leśnych i zbiorników wodnych, rurociągów, linii energetycznych wysokiego napięcia, szlaków kolejowych w celu wykrycia ewentualnych uszkodzeń lub pożarów; prowadzeniem akcji informacyjnych (zrzucanie ulotek, podawanie komunikatów za pomocą urządzeń nagłaśniających); ewakuacją rannych i chorych z rejonów zagrożonych (transport tylko w pozycji siedzącej).

W polemikach na temat efektywności funkcjonowania formacji OC zauważa się 2 rozbieżne stanowiska. Zwolennicy radykalnych reform w OC polegających na utworzeniu nowych struktur są zdania, że funkcjonujące formacje nie realizują swoich ustawowych zadań, co więcej, są tworami biurokratycznymi, istniejącymi jedynie w teorii. W myśl takiego poglądu zasadne byłoby zatem utworzenie struktur OC w ministerstwie właściwym do spraw i ścisłe powiązanie OC ze strukturami →zarządzania kryzysowego [t. 4]. Oponenci takich rozwiązań twierdzą, iż możliwości Polski nie pozwalają na utworzenie nowej organizacji OC. Nie można realizować zadań z zakresu →ochrony ludności [t. 3] i OC, nie ponosząc żadnych kosztów, a tym bardziej powołać nowoczesnej OC, która nie bazowałaby na działaniach funkcjonujących dotychczas podmiotów państwowych, upoważnionych do wykonywania tego typu zadań. Uwzględniając aktualny stan wyszkolenia i wyposażenia, a także biorąc pod uwagę finansowanie zadań, nie wydaje się zasadne tworzenie

formacji OC na okres wojny z możliwością ich wykorzystywania jedynie podczas klęsk żywiołowych. Jest to propozycja nieracjonalna nie tylko ze względów ekonomicznych, ale również dlatego, że na rzecz ochrony ludności i OC działa szereg podmiotów, którym należy nadać obowiązek zadaniowy w czasie wojny pod znakiem OC. Niestety takie rozwiązanie ma też swoje negatywne strony, gdyż organy odpowiedzialne za OC nie realizują wówczas w sposób należyty powinności związanych z tworzeniem i utrzymaniem formacji OC. Ponadto, jak wynika z raportu Najwyższej Izby Kontroli, liczba formacji OC jest nieadekwatna do zidentyfikowanych zagrożeń i z każdym kolejnym rokiem maleje, a wyposażenie istniejących formacji jest niekompletne i w wielu wypadkach przestarzałe, gdyż część sprzętu pochodzi z lat 50. i 60. ubiegłego wieku.

Julia Anna Gawęcka

J.A. Gawęcka, *Włączanie organizacji pozarządowych w struktury Obrony Cywilnej na przykładzie Ochotniczych Straży Pożarnych*, [w:] *Organizacje pozarządowe w zapewnianiu bezpieczeństwa państwa*, B. Pacek, T. Szmidtka, K. Jakubczak-Krawczyńska (red.), Naukowe Wydawnictwo Piotrkowskie, Piotrków Trybunalski 2017; taż, *Wybrane aspekty prawno-organizacyjne Obrony Cywilnej w Polsce*, [w:] *W trosce o bezpieczne jutro. Reminiscencje i zamierzenia*, M. Michalski, A. Bolewski (red.), Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu, Poznań 2017; J.A. Grochocka, *Obrona cywilna w Polsce. Stan obecny i możliwe perspektywy rozwoju*, [w:] *Współczesne problemy bezpieczeństwa państwa*, O. Wasiuta, P. Mazur (red.), Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie, Stalowa Wola 2017; Informacja o wynikach kontroli. Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, Departament Porządku i Bezpieczeństwa Wewnętrznego, KPB.430.009.2017 nr ewid. 147/2018/P/17/039/KPB, NIK, Warszawa 2018; Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej z 21 listopada 1967 r., Dz. U. 1991, nr 113, poz. 491 z pózn. zm.; Wytyczne Szefa Obrony Cywilnej Kraju z dnia 3 marca 2014 r. w sprawie normatywów, w zakresie zaopatrywania organów i formacji obrony cywilnej w sprzęt, środki techniczne i umundurowanie niezbędne do wykonywania zadań obrony cywilnej, z uwzględnieniem ramowych struktur organizacyjnych i podstawowych zadań formacji obrony cywilnej, Warszawa 2014.

FORMACJE UZBROJONE – instytucje funkcjonujące w ramach systemu →bezpieczeństwa wewnętrznego państwa [t. 1], które są uprawnione przez prawo tego państwa do stosowania w jego imieniu

lub na jego terytorium przymusu bezpośredniego w postaci ustawowo określonych środków wobec innych osób w celu zapewnienia →bezpieczeństwa [t. 1] i porządku publicznego oraz egzekwowania obowiązującego prawa.

To właśnie ustawowe uprawnienie funkcjonariuszy, →żołnierzy [t. 4] lub pracowników poszczególnych służb i innych instytucji do stosowania przymusu państwowego w sposób bezpośredni, czyli do legalnego stosowania przymusu fizycznego wobec obywateli tego państwa oraz innych osób przebywających na jego terytorium, powinno stanowić podstawowe kryterium wyodrębnienia formacji uzbrojonych z całego systemu bezpieczeństwa wewnętrznego państwa.

Umocowanie działalności tak rozumianych formacji należy wywodzić z filozofii funkcjonowania państwa jako organizacji przymusowej, która może go stosować w celu zagwarantowania obywatelom bezpieczeństwa, sprawiedliwości i spokoju oraz ochrony praw i wolności. Podstawy filozoficzne takiego rozumowania są zawarte przede wszystkim w koncepcjach powstania państwa w drodze umowy społecznej, które podkreślają istotę przejścia ludzi ze stanu natury do społeczeństwa i państwa poprzez powołanie suwerennej władzy państwowej w drodze dobrowolnej umowy zawieranej między jednostkami. Ludzie zrzekli się w ten sposób niczym nieograniczonej wolności na rzecz władzy, która powinna zapewnić bezpieczeństwo i sprawiedliwość między nimi. Miało to na celu zamianę walki każdego z każdym ze stanu natury (w którym panowała naturalna nierówność między ludźmi i gdzie konflikty były rozwiązywane siłowo, a wygrywał je silniejszy fizycznie lub bogatszy) na taki stan funkcjonowania społeczeństwa, w którym państwo będzie rozwiązywało konflikty między jednostkami i grupami społecznymi w sposób sprawiedliwy (stworzenie możliwości ochrony jednostek słabszych przez silniejszymi). W tym celu państwo musiało zostać wyposażone w monopol na stosowanie przymusu.

W ramach demokratycznego państwa prawa taka działalność musi mieć również, a nawet przede wszystkim, jasno określone podstawy prawne, tzn. musi odbywać się na podstawie i w granicach prawa. W Polsce podstawowym aktem prawnym, jak również swoistą implementacją zarysowanych idei filozoficznych, jest Konstytucja Rzeczypospolitej Polskiej

z dnia 2 kwietnia 1997 r., w której zostały zawarte podstawowe zasady funkcjonowania państwa oraz ułożenia wzajemnych relacji między instytucją władzy a obywatelami, jak również podstawowe wolności i → p r a w a c z ł o w i e k a [t. 3] i obywatela oraz możliwości ich ograniczania, a także podstawowe zobowiązania państwa do zapewniania bezpieczeństwa. Z kolei podstawą zasadniczą, w oparciu o którą można dokonać wyodrębnienia formacji uzbrojonych z systemu bezpieczeństwa wewnętrznego państwa, jest Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, która wskazuje enumeratywnie podmioty systemu bezpieczeństwa państwa, które mogą stosować środki przymusu bezpośredniego lub broń palną oraz określa pełny katalog tych środków.

Z tego punktu widzenia jest kluczowym aktem prawnym pozwalającym ująć ten fragment systemu bezpieczeństwa państwa. Natomiast bardzo istotne w zakresie szczegółowych uprawnień w odniesieniu do stosowania środków przymusu bezpośredniego lub broni palnej są ustawy powołujące poszczególne formacje i regulujące ich działalność w zakresie właściwości podmiotowej, przedmiotowej oraz miejscowej (terytorialnej), w ramach których ich funkcjonariusze mogą korzystać z przymusu bezpośredniego w celu realizacji ustawowo określonych zadań. To w tych aktach prawnych zostały w sposób szczegółowy uregulowane podstawowe zasady, obowiązki, możliwości, zadania oraz przypadki korzystania ze środków przymusu bezpośredniego lub broni palnej przez uprawnionych do tego funkcjonariuszy, żołnierzy, strażników, inspektorów czy pracowników.

Ustawa o środkach przymusu bezpośredniego i broni palnej wskazuje, że do używania oraz wykorzystywania środków przymusu bezpośredniego i broni palnej uprawnieni są:

- funkcjonariusze → A g e n c j i B e z p i e c z e ń s t w a W e w n ę t r z n e g o [t. 1] (ABW),
- funkcjonariusze → A g e n c j i W y w i a d u [t. 1] (AW),
- funkcjonariusze → S ł u ż b y O c h r o n y P a ń s t w a [t. 4] (SOP),
- funkcjonariusze → S ł u ż b y C e l n o - S k a r b o w e j [t. 4] (SCS),
- funkcjonariusze → C e n t r a l n e g o B i u r a A n t y k o r u p c y j n e g o [t. 1] (CBA),
- strażnicy Państwowej Straży Łowieckiej (PSŁ),
- strażnicy Państwowej Straży Rybackiej (PSR),

- funkcjonariusze → Policji [t. 3],
- funkcjonariusze i żołnierze → Służby Kontrwywiadu Wojskowego [t. 4] (SKW),
- funkcjonariusze Służby Więziennej (SW),
- funkcjonariusze i żołnierze → Służby Wywiadu Wojskowego [t. 4] (SWW),
- strażnicy → straży gminnych (miejskich) [t. 4],
- funkcjonariusze Straży Granicznej (SG),
- strażnicy Straży Leśnej (SL),
- strażnicy Straży Marszałkowskiej (SM),
- funkcjonariusze Straży Ochrony Kolei (SOK),
- funkcjonariusze Straży Parku (SP),
- żołnierze Żandarmerii Wojskowej (ŻW) lub wojskowych organów porządkowych,
- pracownicy ochrony uprawnieni do użycia lub wykorzystania środków przymusu bezpośredniego lub broni palnej na podstawie przepisów ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia,
- inspektorzy → Inspekcji Transportu Drogowego (ITD).

Natomiast w zakresie używania lub wykorzystania tylko i wyłącznie środków przymusu bezpośredniego uprawnienie to przysługuje ponadto:

- członkom służby porządkowej, powoływanej na podstawie przepisów o bezpieczeństwie → imprez masowych,
- pracownikom zakładów poprawczych, schronisk dla nieletnich i młodzieżowych ośrodków wychowawczych.

Piotr Swoboda

M. Gałka, *Reformy służb specjalnych III RP*, „Poliarchia" 2013, nr 1; T. Kosobudzki, *Bezpieka w MSZ. Służby specjalne w polityce zagranicznej RP w latach 1989–1997*, Kielce–Warszawa 1998; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78, poz. 483 (z późn. zm.); D. Laskowski, *Prawne podstawy funkcjonowania służb specjalnych z perspektywy potrzeb obronnych państwa*, „Obronność. Zeszyty

Naukowe" 2014, nr 2 (10); Ł. Roman, G. Winogrodzki, *Służby specjalne w systemie bezpieczeństwa państwa*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, Józefów 2016; *Służby specjalne w systemie bezpieczeństwa państwa. Przeszłość – teraźniejszość – przyszłość. Materiały i Studia*, t. 1, A. Krzak, D. Gibas-Krzak (red.), Wojskowe Centrum Edukacji Obywatelskiej, Szczecin–Warszawa 2012; P. Swoboda, *Podstawy funkcjonowania oraz miejsce formacji uzbrojonych w systemie bezpieczeństwa wewnętrznego państwa*, [w:] *Uwarunkowania bezpieczeństwa międzynarodowego i narodowego na początku XXI wieku*, P. Swoboda, A. Warchoł (red.), Avalon, Kraków 2019; B. Szmulik, M. Żmigrodzki, *Geneza państwa*, [w:] *Wprowadzenie do nauki o państwie i polityce*, B. Szmulik, M. Żmigrodzki (red.), Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2003; Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, Dz. U. 2013, poz. 628 (z późn. zm.); E. Zieliński, *Nauka o państwie i polityce*, Dom Wydawniczy Elipsa, Warszawa 2006.

FUNDAMENTALIZM RELIGIJNY – przekonanie, często usystematyzowana doktryna, zakładająca konieczność rygorystycznego przestrzegania zasad religijnych wywodzonych wprost ze świętych pism, które nie podlegają interpretacji, lecz są wynikiem egzegezy literalnej. Zwolennicy kwestionują współczesny porządek religijny i społeczny, uważając, że należy wrócić do fundamentów religijnych, a porządek – w tym polityczny – należy oprzeć na zasadach religijnych.

Jest to zaprzeczenie osiągnięć modernizmu i powrót do wartości płynących ze świętych tekstów w ich pierwotnej formie – wg takiej koncepcji prawda jest objawiona i nie należy szukać jej indywidualnie.

Sami zwolennicy fundamentalizmu niekoniecznie są zainteresowani władzą polityczną, mogą faktycznie być przekonani, że realizują dzieło boskie. Fundamentalizmy współczesne to spotkanie religii, ideologii i polityki. Wcale nie musi to oznaczać jakiejś reformy samej religii. Jest to raczej wykorzystanie religii jako pewnego fundamentu, na którym buduje się ideologię opartą o brak zaufania dla współczesności, a zwłaszcza globalizacji i modernizacji.

Termin początkowo odnosił się do protestanckich ruchów odnowy powstałych głównie w USA. Zaczęto negować nową teologię, wprowadzaną choćby przez niemieckiego pastora F. Schleiermachera, uważając, że wiara nie może podlegać racjonalizmowi tak jak nauka (np. E.W. Hengstenberg).

Sam termin pojawił się na początku XX w. i był związany z grupami protestantów negujących modernizm, sekularyzację życia społecznego i nawet czasami postęp jako taki. Został sam przez nich wymyślony i miał na celu wskazanie, że ich zdaniem należy odrzucić nowe tendencje teologiczne, które nie mają już nic wspólnego z prawdziwym przesłaniem Boga. Należy zatem wrócić do „fundamentów" wiary, czyli Biblii, którą należy czytać i rozumieć dosłownie. Za propagatorów pojęcia uważa się braci M. i L. Stewartów, ale sam termin wymyślił C.L. Lawes, redaktor „The Watchman-Examiner".

Na początku lat 90. XX w. postawiono 2 bardzo odważne tezy. Autorem pierwszej był G. Kepel. Zauważył on powrót religii do dyskursu, w tym politycznego, i do możliwości wykorzystania tego przez grupy, zwłaszcza ludzi sfrustrowanych. O ile opisywane przez niego fundamentalizmy żydowskie i chrześcijańskie nie zmieniły w sposób znaczący świata (nie licząc może zamachu na I. Rabina w 1995 r.), o tyle odmiana islamska owszem. Tutaj jego prognoza była więcej niż trafna. Drugą koncepcją była sformułowana przez S. Huntingtona teoria zderzenia cywilizacji. Pierwszym bardzo ważnym aspektem w tej teorii jest to, że wprowadzony podział cywilizacyjny został oparty na religii. Huntington wykazał, że pomiędzy cywilizacją Zachodu (czyli chrześcijańską oraz w części prawosławną) a islamem istnieje „fundamentalny" rozdźwięk, niedający się pogodzić. Huntingtonowska teoria zakłada, że po upadku → k o m u n i z m u konflikty światowe będą się odbywały na fundamencie różnic cywilizacyjnych. Religia ma zatem zająć miejsce ideologii, przy czym być może zasadniejsze byłoby uznanie, że jedna ideologia została po prostu zastąpiona drugą. Koncepcja ta okazała się bardzo użyteczna politycznie po zamachach na World Trade Center i Waszyngton w 2001 r. Kepel uważa, że nie mamy tu do czynienia z → w o j n ą [t. 4] ideologiczną, a faktycznie religijną, że islam wypiera chrześcijaństwo, które popadło w wielki → k r y z y s, który zaczął się w okresie oświecenia. Dla niego islam jest odpowiedzią na problemy Zachodu, nie jest to zatem walka ideologii, a religii, a dla islamu walka ta stoczy się w Europie. To tutaj zdecyduje się przyszłość rewolucji islamskiej, zapoczątkowanej jego zdaniem w 1979 r. w Iranie. B. Tibi uważa, że obecny fundamentalizm religijny to upolitycznienie religii, a nie jej renesans. Jednocześnie zauważa, że jest to kultura

defensywna, nie kreacjonistyczna. Nie proponuje więc niczego nowego, a jedynie jest oparta na negacji i przeciwstawianiu się współczesności, kulturze globalizującego się świata.

J. Habermas uważa, że fundamentalizmy (nie tylko religijne) nie dadzą się pogodzić z liberalną zachodnią cywilizacją:

> Fundamentalistyczne światopoglądy są dogmatyczne […], nie dopuszczają refleksji nad swymi związkami z innymi światopoglądami, z którymi dzielą to samo uniwersum dyskursu i wobec których mogą się ugruntować jedynie na podstawie konkurencyjnych praw do legitymizowania się. Nie dopuszczają żadnego *reasonable disagreement* […]. Niefundamentalistyczne światopoglądy […] dopuszczają – w sensie Lessingowskiej tolerancji – ucywilizowany spór na temat przekonań, w którym jedna strona, nie rezygnując z własnych praw do legitymizmu, pozostałe strony uznaje za współuczestniczące w sporze o autentyczne wartości.

Najbardziej znany jest fundamentalizm islamski, zwłaszcza że na jego bazie powstała ideologia ugrupowań terrorystycznych – → i s l a m i z m. Źródeł fundamentalizmu islamskiego można szukać już u jego początków, gdy powstała grupa zwana charydżytami. Odrzucali oni wszelkie prawa, które nie są zgodne z naukami Koranu, nie widzieli nic zdrożnego nawet w zabiciu kalifa, jeśli ten nie był posłuszny nakazom religii. W głównym nurcie islamu – sunnizmie – za fundamentalistyczną uważana jest szkoła hanbalicka. Jest to najmłodsza z 4 szkół prawa koranicznego, została założona przez Ahmada ibn Hanbala (780–855). Odrzucał on stosowanie interpretacji (*fiqh*, zrozumienie) przy użyciu metod takich jak logika, sofistyka czy *idżma* (dosł.: jednomyślne postanowienie), uważał zatem, że kształtowanie nowego prawa (*idżtihad*, „wysiłek twórczy") jest błędne. Zwracał uwagę na potrzebę sięgania bezpośrednio do Koranu i Sunny. Co ważne, wprowadził restrykcyjną metodę interpretacji w przypadku norm kolizyjnych (*naskh*) i uznał, że wszystko, co nowsze, deroguje to, co dawniejsze, i tym samym dał prymat Sunnie nad Koranem. Egzegeza hanbalicka zakłada 2 ważne podejścia. W przypadku, gdy pojawia się norma zezwalająca lub zakazująca, należy wybrać zakaz. Po drugie, należy

kierować się prawem specjalistycznym (jak w prawie rzymskim *lex specialis derogat legi generali*). Ważnym kontynuatorem był Ahmad ibn Tajmijja (1263–1328), jego wkład to przede wszystkim usankcjonowanie potępienia dla innych odłamów islamu, zwłaszcza alawitów, druzów (o ile ich religię można uznać za odłam islamu), a nawet szyitów. Muzułmanów inaczej interpretujących religię uznał za *takfir*, niemuzułmanów, apostatów.

Z tego nurtu wywodzą się współczesne ruchy fundamentalistyczne Bliskiego Wschodu. W XVIII w. na Półwyspie Arabskim działalność rozpoczął Abd al-Wahhab (1703–1792), swojemu ruchowi religijnemu (zwanemu wahhabizmem) nadał wymiar polityczny, a nawet militarny dzięki współpracy z Muhammadem ibn Saudem. Jest to bardzo rygorystyczna szkoła, zabraniającą kultu świętych, pielgrzymek do miejsc historycznych islamu, a nawet krytykująca szczególną cześć dla Mahometa, są zatem wahhabici restrykcyjnymi monoteistami. Ta szkoła do dziś jest szczególnie popularna w Arabii Saudyjskiej.

Drugim istotnym ruchem jest salafizm (arab. *salafijja*, od *salaf*, przodkowie) powstały zasadniczo w XIX w., głównie na terenie Egiptu, Syrii, Iraku czy nawet Indii. Za prekursorów tego ruchu uważani są Dżamal Ad-Din al-Afgani (1838–1897), ale przede wszystkim Raszid Rida (1865–1935). Ten ostatni nawiązał do nauki ibn Hanbala, z tym że uznał *idżtihad* za uprawniony, miał on pozwolić się dostosować islamowi do nowych wyzwań, natomiast należało zrezygnować z naleciałości innych religii czy filozofii i tradycji (arab. *bay'a*, sprzedaż; przysięga wierności składana kalifowi) oraz powrócić do Koranu i Sunny

Sam ruch ewoluował, tzw. druga fala została zapoczątkowana przez Egipcjanina Hasana al-Bannę (1906–1949). Doszło wówczas do pewnego odejścia od wpływów wahhabickich. Ten nurt zwany jest Braćmi Muzułmanami lub Bractwem Muzułmańskim. Al-Banna był przeciwnikiem radykalnych kroków i uważał, że odrodzenie nastąpi w drodze pokojowego rozwoju i zwycięstwa prawdy nad fałszem i obłudą. Tzw. trzecia fala powstała na bazie konfliktów politycznych, m.in. powstania państwa Izrael, głównym jej ideologiem został Sajjid Kutb (1906–1966), który m.in. zerwał z tolerancją dla innych religii księgi (arab. *al-Kitab*), a nawet dla innych ruchów wewnątrz islamu, wszystkich traktując jako innowierców. To na bazie tego nurtu powstała ideologia Al-Kaidy i → P a ń s t w a

Islamskiego [t. 3] (ISIS), zwana islamizmem czy też politycznym islamem. Salafici uważają, że konieczne jest wprowadzenie światowego porządku opartego na prawie koranicznym (*szari'at*, „droga prowadząca do wodopoju"), drogą do tego będzie rewolucja muzułmańska, a metodą → dżihad. M. Sageman dla precyzyjnego określenia tego nurtu posługuje się terminem „globalny salaficki dżihad" czy „sunnicki salaficki dżihad". Część salafitów nie podziela jednak politycznego kursu, wskazując, że jest to odejście od religii na rzecz ideologii.

Sam termin „fundamentalizm islamski" nie występował w języku arabskim, został użyty przez naukowców zachodnich dla zrozumienia istoty szyickiej rewolucji w Iranie. Po przejęciu władzy przez ajatollaha Chomeiniego wprowadzono tam prawo szariatu, powiązano stanowiska polityczne z religijnymi. W przypadku szyitów jednak trudno mówić o fundamentalizmie *sensu stricto*, ponieważ prawo przywódców religijnych do interpretacji zasad religii jest jednym z fundamentów tego odłamu. W literaturze arabskojęzycznej pojawia się termin *usulijja*, jest to jednak kalka językowa z języków zachodnich.

Fundamentalizm chrześcijański powstał na przełomie XIX i XX w. wśród protestantów brytyjskich i amerykańskich jako reakcja na teologiczny liberalizm i modernizm kulturowy. Był to sprzeciw wobec zmian teologicznych, zakładano konieczność powrotu do literalnego czytania Biblii i odrzucenia logiki i filozofii w interpretacji. Tworzenie się ruchu fundamentalistycznego zapoczątkowała konferencja protestancka w Niagara Falls w 1898 r., na której przyjęto deklarację o niepodważalnym autorytecie Biblii i absolutnej pewności paruzji (ponownego przyjścia Chrystusa na ziemię). Liczne kościoły fundamentalistyczne zrzeszyły się w organizacji IFCA International, dawniej znanej jako Niezależne Fundamentalne Kościoły Ameryki (Independent Fundamental Churches of America). Powstała w 1930 r. w Cicero w stanie Illinois w USA jako kontynuatorka Amerykańskiej Konferencji Kościołów Bezdenominacyjnych (American Conference of Undenominational Churches). Przyjęła obecną nazwę w 1996 r. W katolicyzmie za fundamentalistyczny można uznać ruch Bractwa Kapłańskiego Świętego Piusa X, czyli tzw. lefebrystów lub lefebvrystów, negujących niektóre postanowienia Soboru Watykańskiego II.

Na bazie fundamentalizmu chrześcijańskiego dochodziło również do zamachów terrorystycznych. W latach 80. XX w. pojawił się ruch antyaborcyjny. Zapoczątkował go w 1986 r. R. Terry, zakładając wraz z J. Scheidlerem, twórcą organizacji Pro-Life Action League, ugrupowanie Operation Rescue (Operacja Ratunkowa/Ocalenia). Początkowo ruch ograniczał się do pikiet czy blokowania dostępu do klinik aborcyjnych. Na przełomie lat 80. i 90. doszło do radykalizacji metod i dochodziło do zamachów bombowych czy podpaleń. Drugi nurt to ruchy milenarystyczne, zapowiadające nadchodzący koniec świata. Do najbardziej znanej należy grupa Gałąź Dawidowa, założona jeszcze w latach 50. XX w. Przywództwo w niej przejął V.W. Howell, znany bardziej jako David Koresh. Podczas próby odbicia członków grupy doszło do masakry, na oblężonej farmie zginęło 80 osób (1993 r.).

Fundamentalizm żydowski może odnosić się do wojującego syjonizmu religijnego lub judaizmu *Charedim* (hebr. bojący się Boga). Ten ostatni składa się z grup w obrębie judaizmu ortodoksyjnego charakteryzujących się ścisłym przestrzeganiem interpretacji prawa i wartości żydowskich w przeciwieństwie do współczesnych wartości i praktyk. Jego członkowie są często określani jako ściśle ortodoksyjni lub ultraortodoksyjni.

Judaizm ultraortodoksyjny jest reakcją na zmiany społeczne, w tym emancypację, akulturację, sekularyzację, reformy religijne. Niektóre grupy uważają powstanie państwa Izrael za świętokradztwo. Do takich należy Neturei Karta (Strażnicy Miasta), odrzuca syjonizm i protestuje przeciw istnieniu państwa Izrael przed nadejściem Mesjasza. Ruch został założony w 1938 r. w Jerozolimie po odłączeniu się od mesjanistycznego ugrupowania Agudat Izrael (Związek Izraela). Obecnie szacuje się jego liczebność na 15 tys., co stanowi 2 proc. ultraortodoksyjnej społeczności w Izraelu. W 1974 r. powstał masowy ruch o nazwie Gusz Emunim (Blok Wiernych). Jego niekwestionowanym liderem i przewodnikiem duchowym był Cwi Jehuda Kuk (Kook), który wykształcił rzeszę rabinów związanych z *jeszibą* (jeszybotem, szkołą talmudyczną dla nieżonatych studentów). Tolerancja i demokracja są, ich zdaniem, całkowicie obce narodowi izraelskiemu i powinny zostać odrzucone. Nie chodzi tu o całkowite pozbycie się dorobku cywilizacyjnego Zachodu, a jedynie o odrzucenie tych wartości, które stoją w sprzeczności z Torą, Talmudem czy *halahą*

(żydowską tradycją prawniczą) lub mają zgubny wpływ na jedność narodu żydowskiego. Ideologia głoszona przez rabinów Gusz Emunim inspirowała jego członków do wielu aktów agresji i → p r z e m o c y [t. 3]. Ich celem było m.in. Wzgórze Świątynne w Jerozolimie, gdzie uzbrojeni żydowscy osadnicy kilkakrotnie próbowali się wedrzeć i dokonać zniszczenia meczetu Al-Aksa i Kopuły na Skale (*Kubbat as-Sachra*). Szczególnie istotne dla polityki na Bliskim Wschodzie było zabicie premiera Izraela Icchaka Rabina w 1995 r. przez żydowskiego fundamentalistę Jigala Amira.

Fundamentalizm religijny występuje też w religiach politeistycznych, np. w hinduizmie. Jest to o tyle specyficzne, że nie ma w tej religii świętej księgi, w tym ruchu jej funkcję pełnią Wedy. Ponadto religię powiązano z poczuciem „hinduskości" jako elementem tożsamości. Ten ruch nazywany jest hindutwą, prekursorami było Arja Samadź (Stowarzyszenie Ariów), założone w 1875 r. przez swamiego Dajanandę Saraswatiego.

Przemysław Mazur

K. Armstrong, *W imię Boga. Fundamentalizm w judaizmie, chrześcijaństwie i islamie*, tłum. J. Kolczyńska, W.A.B., Warszawa 2005; J. Habermas, *Anerkennungskämpfe im demokratischen Rechtsstaat*, [w:] Ch. Taylor, A. Gutman, J. Habermas i in., *Multikulturalismus und die Politik der Anerkennung*, Frankurt am Main 1992; S.P. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, tłum. H. Jankowska, Warszawskie Wydawnictwo Literackie Muza, Warszawa 2000; K. Izak, *Nie tylko islam. Ekstremizm i terroryzm religijny*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12 (7); G. Kepel, *Zemsta Boga: religijna rekonkwista świata*, tłum. A. Adamczak, Wydawnictwo Krytyki Politycznej, Warszawa 2010; P. Mazur, O. Wasiuta, S. Wasiuta, *Państwo Islamskie ISIS: nowa twarz ekstremizmu*, Difin, Warszawa 2018; R.E. Olson, *Historia teologii chrześcijańskiej: dwadzieścia wieków tradycji i reform*, tłum. K. Wiazowski, Chrześcijański Instytut Biblijny, Warszawa 2003; E. Pace, P. Stefani, *Współczesny fundamentalizm religijny*, tłum. K. Stopa, WAM, Kraków 2002; M. Sageman, *Sieci terroru*, tłum. M. Król, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2008; F.D.E. Schleiermacher, *Mowy o religii do wykształconych spośród tych, którzy nią gardzą*, tłum. J. Prokopiuk, Wydawnictwo Znak, Kraków 1995; B. Tibi, *Fundamentalizm religijny*, tłum. J. Danecki, Państwowy Instytut Wydawniczy, Warszawa 2001; *W poszukiwaniu prawdziwej wiary: współczesne ruchy odnowy religijnej w krajach pozaeuropejskich*, A. Mrozek-Dumanowska (red.), Semper, Warszawa 1995.

FUNKCJONARIUSZ PUBLICZNY – osoba korzystająca ze szczególnej ochrony prawnej, ale jednocześnie podlegająca szczególnej odpowiedzialności karnej z uwagi na specyficzną pozycję zawodową lub posiadane kompetencje związane ze sprawowaniem władzy publicznej. Definicja legalna omawianego pojęcia zawarta została w art. 115 § 13 kk. Zgodnie ze wskazanym przepisem funkcjonariuszem publicznym jest: Prezydent Rzeczypospolitej Polskiej; poseł, senator, radny; poseł do Parlamentu Europejskiego; sędzia, ławnik, prokurator, funkcjonariusz finansowego organu postępowania przygotowawczego lub organu nadrzędnego nad finansowym organem postępowania przygotowawczego, notariusz, komornik, kurator sądowy, syndyk, nadzorca sądowy i zarządca, osoba orzekająca w organach dyscyplinarnych działających na podstawie ustawy; osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych; osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe; osoba zajmująca kierownicze stanowisko w innej instytucji państwowej; funkcjonariusz organu powołanego do ochrony → bezpieczeństwa publicznego [t. 1] albo funkcjonariusz Służby Więziennej; osoba pełniąca czynną służbę wojskową, z wyjątkiem terytorialnej służby wojskowej pełnionej dyspozycyjnie; pracownik → Międzynarodowego Trybunału Karnego [t. 3], chyba że pełni wyłącznie czynności usługowe.

W kodeksie karnym dokonano zatem określenia kręgu podmiotów, którym przysługuje status funkcjonariusza publicznego, stosując różne metody – niektórzy zostali wymienieni wprost z nazwy, inni przez wskazanie pełnionych przez nich funkcji czy też z uwagi na zajmowane stanowiska.

Termin funkcjonariusz publiczny używany jest w kodeksie karnym w dwojakim znaczeniu. W pierwszej kolejności wskazać należy tę grupę przypadków, gdy za pomocą tego terminu określono podmiot dopuszczający się → czynu zabronionego [t. 1]. Przepisy tego rodzaju wskazać można zarówno w części ogólnej (art. 105 § 2, art. 111 § 3, art. 112, 115 § 19), jak i w części szczególnej (art. 231 § 1, art. 246, 247 § 3, art. 266 § 2,

art. 271 § 1). Druga grupa dotyczy przepisów, w których wyrażenie funkcjonariusz jest wykorzystywane do scharakteryzowania czynności sprawczej albo opisania przedmiotu czynności wykonawczej (art. 148 § 3 – zabójstwo funkcjonariusza, art. 222 § 1 – naruszenie nietykalności funkcjonariusza, art. 223 § 1 i 2 – czynna napaść na funkcjonariusza, art. 226 § 1 – znieważenie funkcjonariusza, art. 231a – bezprawny zamach, 272 – wyłudzenie poświadczenia nieprawdy od funkcjonariusza).

Pojęcie funkcjonariusza publicznego jest także istotne z perspektywy ustalania odpowiedzialności majątkowej funkcjonariuszy publicznych wobec Skarbu Państwa, jednostek samorządu terytorialnego lub innych podmiotów ponoszących odpowiedzialność za szkodę wyrządzoną przy wykonywaniu władzy publicznej, za działania lub zaniechania prowadzące do rażącego naruszenia prawa. Problematyka ta została uregulowana w ustawie z 2011 r., która definiuje funkcjonariusza jako osobę działającą w charakterze organu administracji publicznej lub z jego upoważnienia albo jako członka kolegialnego organu administracji publicznej lub osobę wykonującą w urzędzie organu administracji publicznej pracę w ramach stosunku pracy, stosunku służbowego lub umowy cywilnoprawnej, biorącą udział w prowadzeniu sprawy rozstrzyganej w drodze decyzji lub postanowienia przez taki organ. Definicja ta zakresem podmiotowym w sposób istotny odbiega od tej, którą znajdujemy w art. 115 § 13 kk, albowiem inny jest też jej cel. Wyjaśnić należy, iż ustawa reguluje odpowiedzialność funkcjonariuszy publicznych w przypadku, gdy na skutek ich wadliwego (bezprawnego i zawinionego) działania obywatel poniósł szkodę, za którą odszkodowanie musiał wypłacić Skarb Państwa. W takim przypadku powinno nastąpić rozliczenie regresowe między współodpowiedzialnymi, które doprowadzi do zrealizowania aksjologicznych racji odpowiedzialności, wymagających lokalizacji ryzyka u osoby winnej (bądź tej, która czerpała korzyści z działania będącego źródłem szkody). Celem ustawy jest ujednolicenie reguł odpowiedzialności funkcjonariuszy, co ma służyć także realizowaniu funkcji prewencyjnej – przestrzegającej przed podejmowaniem przez nich działań mogących skutkować stosowaniem wobec nich sankcji ustawowych.

Anna Pacholska, Jakub Idzik

J. Majewski, *Komentarz do art. 115 kk*, [w:] *Kodeks karny. Część ogólna. Tom I. Część II. Komentarz do art. 53–116*, W. Wróbel, A. Zoll (red.), Wolters Kluwer Polska, Warszawa 2016; A. Matan, *Rażące naruszenie prawa jako przesłanka odpowiedzialności majątkowej funkcjonariusza publicznego*, Wolters Kluwer Polska, Warszawa 2014; T. Oczkowski, *Komentarz do art. 115 kk*, [w:] *Kodeks karny. Komentarz*, V. Konarska-Wrzosek (red.), Wolters Kluwers Polska, Warszawa 2018; Ustawa z dnia 20 stycznia 2011 r. o odpowiedzialności majątkowej funkcjonariuszy publicznych za rażące naruszenie prawa, Dz. U. 2011, nr 34 poz. 173.

G

GEOPOLITYKA – pojęcie zostało ukute przez szwedzkiego politologa R. Kjellena na początku XX w., określa szczególny rodzaj analizy politycznej (przede wszystkim, chociaż nie tylko, polityki zagranicznej państw narodowych) prowadzonej w odniesieniu do uwarunkowań tworzonych przez czynniki przestrzenne – nie tylko czysto fizyczne, ale głównie z perspektywy współzależności między bytami politycznymi określanymi terytorialnie.

L. Sykulski określa geopolitykę jako refleksję o panowaniu nad przestrzenią. Pojawiają się tu więc 2 kluczowe pojęcia: przestrzeń i władza. Władza w geopolityce traktowana jest jako forma ekspansji, rozumianej jako poszerzanie, zdobywanie, pomnażanie w odniesieniu do terytorium, zasobów (naturalnych i ludzkich), stref wpływów, poparcia społecznego, przestrzeni mentalnej (świadomości ludzkiej). P.M. Gallois precyzuje, że geopolityka to studia nad relacjami pomiędzy potęgą na poziomie międzynarodowym a ramami geograficznymi, w których jest ona kształtowana. Przedmiotem geopolityki są więc relacje pomiędzy ośrodkami siły (państwami, ale nie tylko) a przestrzenią geograficzną. Geopolityka bada zależność zewnętrznej i wewnętrznej polityki państw oraz stosunków międzynarodowych od systemu powiązań politycznych, wojskowych i ekonomicznych, uwarunkowanych geograficznym położeniem państwa

i jego regionów oraz innymi czynnikami fizyczno-ekonomiczno-geograficznymi. W tym rozumieniu dziedzina ta prowadzi badania relacji między państwami czy też ośrodkami siły (rozumianymi szerzej, nie tylko jako państwa, ale także jako np. zgrupowania państw w różnego rodzaju sojuszach i organizacjach) poprzez pryzmat przestrzeni geograficznej i jej roli w kształtowaniu się ww. stosunków w kategoriach długookresowych. Tradycyjnie geopolitykę można rozpatrywać jako naukę o wpływie geoprzestrzeni na polityczne cele i interesy państwa. Prostą i użyteczną definicję prezentuje C. Gray, twierdząc, że geopolityka to studia oraz praktyka (warty podkreślenia jest ów aplikacyjny charakter geopolityki) o charakterze przestrzennym nad stosunkami międzynarodowymi.

Kluczowymi pojęciami geopolitycznymi są siła i potęga. Za M. Kleinowskim potęgę możemy zdefiniować jako:

> hipotetyczną zdolność uczestnika stosunków międzynarodowych do użycia swoich materialnych i pozamaterialnych zasobów w celu wykonania własnej woli, bez względu na sprzeciw lub współdziałanie innych uczestników.

Siła z kolei to:

> użycie przez uczestnika stosunków międzynarodowych zmobilizowanych w określonych uwarunkowaniach zasobów materialnych i pozamaterialnych w celu wykonania własnej woli w ramach danych stosunków międzynarodowych, bez względu na sprzeciw lub współdziałanie innych uczestników.

Potęga i siła opierają się więc na tych samych zasobach materialnych i niematerialnych, przy czym potęga to potencjał, a siła to jego użycie. Do wyznaczenia poziomu siły możemy zatem brać pod uwagę tylko te zasoby, spośród wszystkich tworzących potęgę, które mogą być przydatne oraz możliwe do zmobilizowania w danej sytuacji wewnętrznej i międzynarodowej. Stąd też nie ma znaku równości między potęgą a siłą. Według N. Spykemana walka o potęgę jest głównym celem polityki państw, gdyż tylko z pomocą potęgi można realizować cele polityki.

Kluczowym czynnikiem geopolityki są więc interesy ośrodka siły. Ośrodek ten postrzegany jest kolektywnie jako środowisko, w ramach którego koncentrują się wpływowe kręgi polityczne oraz grupy interesu (szczególnie w kategoriach ekonomicznych). Imperatywowi poszerzania interesów ośrodka siły podporządkowane są inne czynniki (społeczeństwa, rynki) traktowane jako narzędzia w rękach tegoż ośrodka.

Nadal nierozstrzygnięte jest pytanie o szerokość postrzegania geopolityki. J. Macała proponuje następujące ujęcia geopolityki:

- Geopolityka jako nauka. Według tego rozumienia geopolityka jest odrębną dyscypliną, umiejscowioną zazwyczaj (stosując pojęcia oficjalnej polskiej klasyfikacji) w dziedzinie nauk społecznych (w przeciwieństwie do geografii, funkcjonującej w ramach nauk o Ziemi). Towarzyszy temu założenie, że geopolityka posiada odrębny zakres podmiotowy (co najwyżej pokrywający się z peryferyjnymi obszarami badawczymi innych nauk, ale niepodlegający żadnej z nich) i odrębną metodologię. W tym ujęciu geopolityka będzie nauką interdyscyplinarną, czymś pośrednim pomiędzy geografią i naukami o polityce (większość definicji geopolityki kładzie akcent na te 2 pojęcia), wkraczającym także na pogranicza innych nauk, jak historia, ekonomia, → n a u k i o b e z p i e c z e ń s t w i e [t. 3] i obronności. Wielu autorów umiejscawia ją na trójstyku nauk o polityce, nauk geograficznych i nauk historycznych. Geopolityka jest również czymś odmiennym od geografii politycznej, która akcentuje wpływ człowieka na przestrzeń, podczas gdy w geopolityce to przestrzeń w mniejszym lub większym stopniu wpływa na działanie, przede wszystkim działanie polityczne. Geopolityka, w przeciwieństwie do geografii politycznej, wartościuje przestrzeń, przede wszystkim z punktu widzenia panowania nad nią.
- Geopolityka jako część innych nauk. W tym ujęciu nie jest samodzielną dyscypliną naukową, lecz częścią innych dyscyplin (np. subdyscypliną geografii politycznej, czyli pozostaje w kręgu nauk przyrodniczych; albo subdyscypliną nauk politycznych, zwłaszcza w ramach stosunków międzynarodowych; czy też elementem → g e o s t r a t e g i i, gdzie miałaby zajmować się przestrzennymi uwarunkowaniami polityki bezpieczeństwa – to spojrzenie

jest częste wśród badaczy anglosaskich). Warto zaznaczyć, że to ostatnie ujęcie nie jest powszechnie akceptowane, mało tego – często spotyka się ujęcie postrzegające na odwrót relacje między geopolityką i geostrategią, ujmującą tę drugą (geopolitykę wojskową) jako subdyscyplinę geopolityki.

- Geopolityka jako paradygmat badaczy. To ujęcie mieści się w ramach ujęcia poprzedniego, będącego jej uszczegółowieniem. Według niego geopolityka jest wzorcem prostego i wewnętrznie spójnego rozpatrywania procesów, zdarzeń, tendencji w stosunkach międzynarodowych w optyce kategorii geograficznych przy agregowaniu interdyscyplinarnej wiedzy. Paradygmat ten służy badaniom wpływu czynników przestrzennych na działalność polityczną.
- Geopolityka jako ideologia i doktryna polityczna. Tzw. myśl geopolityczna, będąca pochodną myśli politycznej, stanowi refleksję nad interakcjami geografii i polityki, przybierającą formę systemów o różnym stopniu uporządkowania – ideologii, idei, teorii, doktryny, koncepcji. Myśl geopolityczna stanowi więc pewien całokształt, co więcej, przez związek z ideologią, instrumentalizujący przestrzeń dla własnych celów (zwłaszcza w zakresie interpretacji wpływu czynników geograficznych na politykę państw).
- Geopolityka stosowana. Spojrzenie to kładzie nacisk na praktyczny wydźwięk geopolityki. W tym sensie może być traktowane jako odmiana poprzedniego ujęcia, gdyż każda ideologia nie tylko przynosi opis świata oraz wizję pożądanej przyszłości, ale i stanowi podstawę działania (zorganizowanego działania politycznego). Tak pojmowana geopolityka jest wiedzą stosowaną, instrumentalną, poddaną potrzebom praktycznym i ideologicznym. Ma ona określać kierunki polityki zagranicznej, a jej konkluzje mają być praktycznie użyteczne. Ma więc charakter partykularny, ma kształtować i wspierać politykę państwa. Geopolityka staje się zatem nie tyle gałęzią nauki o polityce, ile samej polityki. Tak postrzegał jej zadanie K. Haushofer, twierdząc, że powinna ona być nauką stosowaną i sumieniem ojczyzny. Podobnie postrzegali geopolitykę autorzy anglosascy – A.T. Mahan, H. Mackinder, bardziej

współcześni Z. Brzeziński i H. Kissinger – przygotowujący użyteczne politycznie analizy geopolityczne pod przykrywką naukowej wiedzy o relacjach międzynarodowych. Takie stanowisko otwarcie deklaruje A. Dugin, wpływowy geopolityk rosyjski, mówiąc, że geopolityka to „podręcznik władzy" niezbędny dla podejmowania właściwych decyzji politycznych.

Współczesne rozumienie geopolityki stara się uciec od pułapki determinizmu geograficznego, podkreślając, że aktywność państwa zależy nie tylko od czynników geograficznych, ale i kulturowych czy cywilizacyjnych. Zagadnienie determinizmu w geopolityce ma znaczenie fundamentalne – jest to pytanie o to, czy społeczeństwa i państwa mogą kształtować swój los w sposób wolny, czy też są one nierozerwalnie i absolutnie zależne od uwarunkowań środowiskowych. Być może w ujęciu posybilistycznym geopolityka traci ostrość spojrzenia i zdolność do formułowania prostych, a przy tym zarazem eleganckich i chwytliwych prawideł, ale z pewnością staje się lepszym narzędziem wyjaśniania rzeczywistości politycznej. Prekursorem ujęcia posybilistycznego był J. Fairgrieve – nie traktował on rzeczywistości geograficznej jako przeszkody czy wręcz fatum, ale jako podłoże rozwoju działalności społeczno-politycznej, która zakłada dużą rolę wolnej woli, także w pewnym stopniu w kształtowaniu rzeczywistości geograficznej. Jak piszą G. Sloan i C.S. Gray, państwa nie znajdują się w krępującym ich geograficznym kaftanie bezpieczeństwa, lecz geografia i konfiguracje geograficzne warunkują możliwości dla twórców i wykonawców polityki. To, na ile te możliwości zostaną wykorzystane, zależy już od wyboru i realizacji → s t r a t e g i i [t. 4]. Geopolityka nie powinna ograniczać się do spojrzenia na uwarunkowania geograficzne same w sobie, lecz postrzegać je poprzez pryzmat związków z przemysłem, handlem, techniką, energią, ludnością, strukturą społeczną, psychologią, strukturami militarnymi, środowiskiem. Czynnik geograficzny jest więc elementem warunkującym, ale nie determinującym działalność polityczną. Definitywne odejście od determinizmu geograficznego miało miejsce już w latach 50. XX w., wraz z renesansem geopolityki za sprawą takich autorów jak H. Morgenthau czy N. Spykeman. Wcześniejsza geopolityka, spod znaku takich autorów jak K. Haushofer, stała się przedmiotem krytyki nie tylko ze względu na jej rolę służebną wobec imperializmów (a zwłaszcza

nazizmu), ale także ze względu na determinizm geograficzny. Anglosascy autorzy od lat 50. XX w. przywrócili geopolityce reputację m.in. ze względu na położenie większego nacisku na ludzkie działanie (chociażby pod postacią rozwoju przemysłowego czy instytucji społecznych), ograniczając przy tym bezpośredni wpływ czynników geograficznych. Nie można także zapominać o wkładzie geopolityki francuskiej z takimi pojęciami jak geografia humanistyczna czy geografia historii, której czołowi przedstawiciele (P.V. de la Blache, E. Reclus) zwracali uwagę na inicjatywę i wolę człowieka, ujmując czynniki geograficzne jako jeden z wielu elementów wpływających na idee i działania polityczne.

Kosmicznym derywatem geopolityki jest astropolityka. E. Dolman definiuje ją jako „studia nad relacjami specyficznej przestrzeni geograficznej, jaką jest przestrzeń kosmiczna, z immanentnym uwzględnieniem czynnika technicznego, ze sferami polityki, polityki militarnej oraz strategii". Astropolityka jest kolejnym, logicznym krokiem względem geopolityki. Ziemska geopolityka była nowością względem dotychczasowych spojrzeń na kwestie polityczne i militarne o tyle, że po raz pierwszy widziała je w perspektywie prawdziwie globalnej. Ziemia po raz pierwszy była konceptualną całością. Poszczególne państwa postrzegane były jako elementy systemu, którego fragmenty wzajemnie na siebie oddziałują w skali globalnej. Takie całościowe podejście było swego czasu rewelacją geopolityki i odróżniało ją od innych sposobów patrzenia na relacje międzynarodowe. W przypadku astropolityki ten sposób widzenia zostaje rozciągnięty na przestrzeń pozaziemską – to kosmos staje się konceptualną całością.

Rafał Kopeć

E. Dolman, *Astropolitik. Classical Geopolitics in the Space Age*, Frank Cass, London–Portland 2005; *Geopolitics, Geography and Strategic History*, G. Sloan (ed.), Routledge, London–New York 2017; R.D. Kaplan, *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate*, Random House, New York 2013; M. Kleinowski, *Czynniki budujące siłę i potęgę państwa na arenie międzynarodowej*, „Świat Idei i Polityki" 2010, t. 10; R. Kopeć, *Geopolityka*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; J. Macała, *Czym jest geopolityka? Spory wokół definicji*, [w:] *Geopolityka. Elementy teorii, wybrane metody i działania*, Z. Lach, J. Wendt (red.),

Instytut Geopolityki, Częstochowa 2010; L. Moczulski, *Geopolityka. Potęga w czasie i przestrzeni*, Wydawnictwo Bellona, Warszawa 2000; J. Potulski, *Wprowadzenie do geopolityki*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2010; *Przestrzeń i polityka. Z dziejów niemieckiej myśli politycznej*, A. Wolff-Powęska, E. Schulz (red.), Wydawnictwo Poznańskie, Poznań 2000; L. Sykulski, *Geopolityka. Skrypt dla początkujących*, Wydawnictwo Naukowe Grategia, Częstochowa 2014.

GEOSTRATEGIA – dziedzina →geopolityki, w której →strategia [t. 4] państwa, w tym polityka zagraniczna i polityka bezpieczeństwa, jest kształtowana z uwzględnieniem kwestii geograficznych. Jest to więc strategia w wymiarze geopolitycznym, postrzegana szczególnie w perspektywie średnio- oraz długoterminowej.

Geostrategia koncentruje się na kwestiach militarnych, często jest traktowana wręcz jako militarna odnoga geopolityki. Geostrategia ujmuje przestrzeń militarną przede wszystkim w kategoriach militarnego planowania. Geostrategia zakłada uwzględnienie czynników geograficznych wielkiej skali w rozmieszczeniu i wykorzystaniu sił zbrojnych, ale tym różni się od taktyki, sztuki operacyjnej czy nawet →sztuki wojennej [t. 4], że koncentruje się na poziomie globalnym. Skupia się na kontroli i dostępie do obszarów kluczowych z punktu widzenia zasobów, rozumianych przede wszystkim jako środki zapewniające przewagę militarną.

Sam termin strategia w pierwotnym znaczeniu odnosi się tylko do prowadzenia →wojny [t. 4], strategia jest więc zawsze wojenna czy też militarna. Geostrategia zakłada uwzględnienie czynników geograficznych wielkiej skali w ramach planowania militarnego, m.in. w rozmieszczeniu wojsk. Ważnym elementem geostrategii jest pojawianie się technologii o znaczeniu militarnym, zwłaszcza jeśli prowadzą one do „kurczenia się" terytorium (przykładem takich technologii jest kolej, która uwolniła Niemców od konieczności utrzymywania osobnych armii na wschodzie i zachodzie, czy też międzykontynentalne pociski balistyczne, które po raz pierwszy w tak dużym stopniu podważyły pozycję kontynentalnej części Stanów Zjednoczonych jako „bezpiecznej wyspy").

Do kluczowych koncepcji geostrategicznych można zaliczyć:

- Koncepcję potęgi morskiej A.T. Mahana. Potęga morska – umożliwiająca dominację polityczną, ekonomiczną i militarną – wymaga

kontroli nad głównymi drogami transportu. To tzw. punkty węzłowe (ang. *chokepoints*)– wąskie wody zdominowane przez punkty geograficzne (Gibraltar, cieśnina Malakka, Przylądek Dobrej Nadziei, Malta, Kanał Sueski). Jeśli punkt nie istniał, należało go stworzyć – Mahan był więc orędownikiem budowy Kanału Panamskiego. Postulował on ustanowienie sieci baz morskich na całym świecie, których położenie miało być zdeterminowane przez czynniki geograficzne (możliwość kontroli nad punktami węzłowymi) oraz techniczne (zasięg okrętów).

- Koncepcję strategii morskiej J. Corbetta. Dla Corbetta, będącego krytykiem jednostronnego → n a w a l i z m u [t. 3] Mahana, morza i oceany nie były głównym polem działania, lecz drogą przerzutu sił i środków. Corbett był więc prekursorem koncepcji projekcji siły z morza na ląd. Potęga morska i armia ekspedycyjna zmuszą przeciwnika do rozśrodkowania swych sił lądowych wzdłuż wybrzeży, co pozwoli na uderzenie w osłabione punkty.
- Koncepcję potęgi powietrznej A. Severskiego. Rozwój lotnictwa strategicznego zredukuje znaczenie innych rodzajów wojska, a w warunkach rywalizacji między Stanami Zjednoczonymi i Związkiem Radzieckim głównym polem starcia będzie Arktyka, ze względu na względną bliskość geograficzną obu państw w tym ujęciu i możliwość wykorzystania tego obszaru przez siły powietrzne (co w przypadku → w o j s k l ą d o w y c h [t. 4] i → m a r y n a r k i w o j e n n e j [t. 3] byłoby co najmniej niezmiernie trudne). Do wyznaczenia stref wpływów obu mocarstw (obszaru dominacji powietrznej USA i ZSRR i strefy decydującej) stosował więc mapę z biegunem północnym w centralnym punkcie. Strefa decydująca (ang. *area of decision*) miała być kluczowym obszarem starcia w przyszłym konflikcie.
- Koncepcję potęgi kosmicznej E. Dolmana. Koncentruje się ona na identyfikacji kluczowych punktów na Ziemi i w kosmosie, nad którymi kontrola może zaowocować militarną i polityczną dominacją nad przestrzenią kosmiczną, a co najmniej może zapobiec osiągnięciu takiej dominacji przez stronę przeciwną. Dolman postrzega kosmos przede wszystkim jako źródło zasobów (nie tylko,

nawet nie przede wszystkim, w sensie zawłaszczenia ekonomicznego, ale głównie jako źródła dającej przewagę pozycji strategicznej, pozwalającej na rozszerzenie hegemonii na Ziemi). Identyfikuje przy tym cztery strategicznie ważne rejony kosmosu, zwracając szczególną uwagę na tzw. przestrzeń okołoziemską (ang. *Earth Space*), rozciągającą się od najniższych orbit do orbity geostacjonarnej. Kontrola nad tym obszarem, w tym rozmieszczenie broni kosmicznej, powinna umożliwić kontrolę innych regionów kosmosu oraz w pewnym stopniu kontrolę terytoriów ziemskich.

Rafał Kopeć

E. Dolman, *Geostrategy in the Space Age: An Astropplitical Analysis*, „The Journal of Strategic Studies" 1999, vol. 22 (203); *Global Geostrategy: Mackinder and the Defence of the West*, B.W. Blouet, F. Cass (eds.), Routledge, London–New York 2005; R. Kopeć, *Geostrategia*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Krzeczunowicz, *Geopolityka i geostrategia*, Wydawnictwo Akademii Polonijnej Educator, Częstochowa 2010; Z. Lach, J. Skrzyp, *Geopolityka i geostrategia*, AON, Warszawa 2007; M.P. Noonan, *American Geostrategy in a Disordered World*, „Orbis" 2015, vol. 59, iss. 4.

GLOBALIZACJA INFORMACYJNA – rozwój środków szybkiej komunikacji w skali światowej ułatwiający dostęp do → i n f o r m a c j i, informacja staje się jednocześnie towarem i medium.

Pojawienie się nowych środków komunikacji, zwłaszcza elektronicznych, w tym internetu, w znaczący sposób wpływa na szybkość przekazywania informacji, ich ilość i dostępność. Nowoczesne technologie wywierają zasadniczy wpływ na dystrybucję informacji i priorytety medialne (*targeting*). Sytuacja ta określa istotę → s p o ł e c z e ń s t w a i n f o r m a c y j n e g o [t. 4] (D. Bell), które ukształtowało się na początku lat 70. XX w. Przez społeczeństwo informacyjne rozumie się społeczne i polityczne relacje, których rozwój zależy całkowicie od produkcji, obsługi i stosowania informacji oraz działania systemu technologicznego, zapewniającego dystrybucję tych informacji. Informacja jest traktowana tak samo jak towar, społeczeństwo informacyjne zatem jest następcą społeczeństwa przemysłowego. Jedną z pierwszych osób, które opracowały koncepcję

społeczeństwa informacyjnego, był ekonomista F. Machlup. W 1933 r. rozpoczął badania nad wpływem innowacyjności i dostępu do wiedzy na gospodarkę. Wyniki opublikował w 1962 r. w książce *The Production and Distribution of Knowledge in the United States*, udowadniając, że istnieje sektor gospodarki, jakim jest wiedza (ang. *knowledge economy*). Wiedza staje się zatem towarem, jednocześnie ludzie posiadający wiedzę czy uzyskujący pewne kompetencje są postrzegani jako kapitał ludzki.

Dzięki technologii cyfrowej społeczeństwo jest w stanie przyspieszyć podejmowanie wielu codziennych decyzji, rozumiejąc ich konsekwencje. Globalna transparentność informacyjna może pomóc społeczeństwom promować lepsze wykorzystanie zasobów i bardziej indywidualną odpowiedzialność. Jednocześnie zwiększa się ilość informacji, których jednostka nie jest w stanie przyswoić.

M. Castells zaproponował paradygmat technologii informacyjnej. Jego cechą jest to, że informacja stanowi surowiec, są to technologie działające na informację, a nie odwrotnie (inaczej niż w rewolucji przemysłowej). Drugą cechą jest wszechobecność wpływu nowych technologii. Trzecia cecha to „sieciowa logika" każdego zbioru stosunków, w których operuje się tymi nowymi technologiami informacyjnymi. Ta sieciowa logika wpływa na następną cechę, jaką jest elastyczność. Następuje łączenie się poszczególnych technologii w wysoce zintegrowany system.

Ludzkość podlega obecnie cywilizacyjnym procesom intensywnego kulturowego przekształcania, a zjawiska kulturowego ujednolicania i globalizacji stają się jej realnością. Pierwszy zjawisko uniformizacji pewnych zachowań i zwyczajów kulturowych dostrzegł J. Ortega y Gasset w swojej koncepcji buntu mas. M. McLuhan, badając wpływ mediów na zachowania społeczne, użył jako pierwszy terminu „globalna wioska" na określenie uniformizacji wzorców kulturowych. Pewną kontynuacją tej koncepcji była makdonaldyzacja G. Ritzera. Jest to pewne przekonanie o sukcesie konsumpcyjnego sposobu życia, postępującej amerykanizacji i triumfie mediów, zwłaszcza telewizji. Castells sukcesu tej ostatniej upatruje, nawiązując do McLuhana, w konsekwencji „prymitywnego instynktu leniwego odbiorcy". W społeczeństwie i w wielu aspektach jego życia dochodzi do fetyszyzacji i podporządkowania się sprawności, wymierności, racjonalności (żelazna klatka racjonalizmu) i przewidywalności.

Na początku lat 90. XX wieku niemiecki badacz U. Beck sformułował nową teorię →społeczeństwa ryzyka [t. 4] (ang. *risk society*). Podkreśla on znaczenie ryzyka wynikającego z totalnego utechnicznienia niemal całego życia człowieka. Współczesne społeczeństwo ma trwałą cechę, jaką jest wszechobecne ryzyko, wpływające pośrednio nie tylko na samego człowieka, ale i na związane z nim instytucje, organizacje, władzę, działania gospodarcze czy relacje międzynarodowe. Olbrzymia ilość informacji i brak możliwości ich pełnej percepcji mogą prowadzić do wytworzenia się swoistego napięcia u jednostki, a w konsekwencji w całym społeczeństwie.

Przemysław Mazur

B.R. Barber, *Dżihad kontra McŚwiat*, tłum. H. Jankowska, Muza, Warszawa 1997; Z. Bauman, *Globalizacja. I co z tego dla ludzi wynika*, Państwowy Instytut Wydawniczy, Warszawa 2000; tenże, *Ponowoczesność jako źródło cierpień*, Wydawnictwo Sic!, Warszawa 2000; U. Beck, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Wydawnictwo Naukowe Scholar, Warszawa 2002; D. Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, Basic Books, New York 1976; M. Castells, *Społeczeństwo sieci*, PWN, Warszawa 2010; A. Giddens, *Runway Word. How Globalization Is Reshaping Our Lives*, Routledge, London 2000; U. Hannerz, *Powiązania transnarodowe: kultura, ludzie, miejsca*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006; F. Machlup, *The Production and Distribution of Knowledge in the United States*, University Press, Princeton 1962; P. Mazur, *Globalizacja informacyjna*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. McLuhan, *Galaktyka Gutenberga. Tworzenie człowieka druku*, Narodowe Centrum Kultury, Warszawa 2017; D. McQuail, *D. McQuail's Mass Communication Theory*, Sage Publications, Los Angeles–London 2007; J. Ortega y Gasset, *Bunt mas*, tłum. P. Niklewicz, Replika, Zakrzewo 2016; G. Ritzer, *Mcdonaldyzacja społeczeństwa*, tłum. S. Magala, Muza, Warszawa 1999.

GLOBALNA KOMISJA DS. STABILNOŚCI CYBERPRZESTRZENI (Global Commission on the Stability of Cyberspace, GCSC) – została powołana z inicjatywy Haskiego Centrum Studiów Strategicznych (HCSS) w celu stworzenia globalnego forum dla osiągnięcia międzynarodowego konsensusu w sprawach pokoju i →bezpieczeństwa [t. 1] w →cyberprzestrzeni [t. 1] między zainteresowanymi podmiotami. Komisję

powołano na zorganizowanej przez HCSS konferencji bezpieczeństwa w Monachium w 2017 r. Zadania GCSC polegają na opracowywaniu standardów i adekwatnych praktyk bezpieczeństwa w porozumieniu ze społecznościami internetowymi, co daje szansę na wypracowanie możliwie spójnych i ujmujących wielostronną perspektywę rozwiązań. Według początkowych założeń na lata 2017–2020 grupa miała spotykać się bezpośrednio 4 razy w roku.

Komisja ma szerokie wsparcie naukowe i organizacyjne zarówno ze strony sektora prywatnego, jak i państwowego: współpracuje na zasadzie partnerstwa z rządem Holandii, korporacją Microsoft, rządem Singapuru, Ministerstwem Spraw Zagranicznych i Rozwoju Międzynarodowego Francji oraz szeroko rozumianą społecznością internetu, jest też sponsorowana przez Ministerstwo Spraw Zagranicznych Estonii i GLOBSEC. Cieszy się też wsparciem najbardziej znaczących instytucji związanych z bezpieczeństwem cyberprzestrzeni, takich jak Packet Clearing House, Black Hat USA i Uniwersytet w Tel Awiwie.

Struktura GCSC składa się ze ściśle powiązanych ze sobą pionów, grup spełniających określone zadania. Komisji współprzewodzą M. Chertoff, były sekretarz ds. bezpieczeństwa wewnętrznego USA, oraz L. Reddy, była zastępczyni ds. bezpieczeństwa narodowego Indii. Wcześniej funkcję przewodniczącej pełniła M. Kaljurand, była minister spraw zagranicznych Estonii. Drugim pionem jest ścisły skład komisji liczący 26 członków, a trzecim grupa Doradców Specjalnych składająca się z 4 członków. Czwartym pionem jest Grupa Doradcza ds. Badań Naukowych (The Research Advisory Group), licząca 5 członków. Spełnia ona funkcję organu wykonawczego oraz zajmuje się badaniami, jest też elementem spajającym organizację ze środowiskiem naukowym poprzez prowadzenie i wspieranie badań naukowych oraz publikacje tekstów naukowych komisarzy. Do innych obowiązków członków grupy należy odpowiadanie na pytania pozostałych członków GCSC, formułowanie problemów badawczych oraz składanie przez wybranych członków grupy 2 razy do roku zeznania przed ogólnym zebraniem komisji. Całą grupą zarządza przewodniczący S. Kanuck, który podlega pod komisję i Sekretariat.

Bezpośrednia aktywność Grupy Doradczej ds. Badań Naukowych jest oparta na moderowanym kontakcie w ramach listy mailingowej,

której moderatorzy ponadto koordynują treść badań. Obecnie funkcjonują 4 tego typu podgrupy: pierwsza jest związana z przepisami prawa, zarówno na poziomie krajowym, jak i międzynarodowym, koncentruje swoje cele na opracowaniu interpretacji prawnych dotyczących cyberprzestrzeni, określenia obszarów wymagających regulacji prawnych, ustalenia różnic między prawem międzynarodowym i krajowym poszczególnych podmiotów państwowych; druga dotyczy ścisłego zarządzania internetem, podejmuje inicjatywy mające związek z →bezpieczeństwem międzynarodowym [t. 1] i pokojem, głównie poprzez realizację prac w Pierwszym Komitecie ONZ. Trzecia podgrupa zajmuje się sprawami międzynarodowego pokoju i bezpieczeństwa w kontekście stabilizacji geopolitycznej, politycznej i wojskowej państw. W aspekcie praktycznym odnosi się do systemowych →zagrożeń [t. 4], które wynikają z →konfliktów międzynarodowych w cyberprzestrzeni, takich jak →cyberszpiegostwo [t. 1], kwestie techniczne →cyberwojny [t. 1], atrybucje działań, polityczne normy zachowań czy środki budujące zaufanie w relacjach multilateralnych. Prace grupy obejmują także zagadnienie wpływu podmiotów niepaństwowych i sektora prywatnego na prawo międzynarodowe w odniesieniu do zagadnień związanych z ochroną danych, szyfrowaniem, ogólną kooperacją sektora prywatnego z publicznym. Wiele projektów tej podgrupy jest konsultowanych z Pierwszym Komitetem ONZ ds. Rozbrojenia i Bezpieczeństwa Międzynarodowego, a z racji swoich priorytetów jest wspierana przez osobę przewodniczącego Grupy Doradczej ds. Badań Naukowych. Prace czwartej podgrupy obejmują techniczne aspekty stabilności cyberprzestrzeni, są to m.in. problemy dotyczące protokołów podstawowych sieci, jej standardów, zarządzania i ochrony krytycznych infrastruktur informatycznych oraz wszelkich innych spraw dotyczących bezpieczeństwa sieci i →informacji. Ostatnim elementem wspierającym operacyjnie komisję jest Sekretariat, w skład którego wchodzi 4 członków pod kierownictwem A. Klimburga z HCSS.

Wojciech Cendrowski

Chinese Academy of Cyberspace Studies, *World Internet Development Report 2017*, Springer, Pekin 2019; CyberStability.org (dostęp 25.04.2019); S. Kanuck, *Promoting Peace and Stability in Cyberspace*, [w:] *Research Handbook on International*

Law and Peace, C.M. Bailliet (ed.), Edward Elgar Publishing, Massachusets 2019; T. Maurer, *Cyber Mercenaries. The State, Hackers, and Power*, Cambridge University Press, Cambridge 2018.

GŁĘBOKIE PAŃSTWO (ang. *deep state*, tur. *derin devlet*) – pojęcie (koncepcja) wskazujące na funkcjonowanie „państwa w państwie", tajnej organizacji działającej poza kontrolą rządu i parlamentu, mającej realny wpływ na bieg wydarzeń politycznych. Głębokie państwo mogą tworzyć zarówno instytucje państwowe, jak również prywatne (wielki biznes). Spośród instytucji publicznych może składać się ze struktur wojska, → s ł u ż b s p e c j a l n y c h [t. 4], wymiaru sprawiedliwości, służby cywilnej, dyplomacji, uczelni wyższych czy szeroko pojętego aparatu państwowego. Pojęcie głębokiego państwa do niedawna kojarzone było wyłącznie z Turcją i decydującym wpływem sił zbrojnych na przebieg wydarzeń politycznych. Aktualnie badania naukowe poświęcone zjawisku prowadzone są w wielu krajach. W 2012 r. na łamach „The New Yorker" Dexter Filkins opublikował tekst *The Deep State*. W 2014 r. ukazała się książka *The American Deep State: Wall Street Big Oil, and the Attack on U.S. Democracy* autorstwa byłego kanadyjskiego dyplomaty P. Scotta. W 2018 r. na łamach „The National Interest" ukazał się artykuł *An American Deep State?* W Polsce tą tematyką interesują się naukowcy, ale przede wszystkim dziennikarze, m.in. W. Gadowski i B. Zalewski. Pierwszy z nich opisał *deep state* w artykule *Genopolityka albo kod „Głębokiego Państwa"*, wskazał na wpływ „starych elit" postkomunistycznych na przebieg wydarzeń politycznych w Polsce, a Zalewski w tekście *Moja rekonstrukcja intencji „głębokiego państwa III RP"*. W 2019 r. w ramach opracowań Ośrodka Studiów Wschodnich ukazał się raport *Putinizm po Putinie. O „głębokich strukturach" rosyjskiego autorytaryzmu* autorstwa M. Domańskiej.

Przykłady głębokiego państwa:

- Turcja,
- Rosja,
- Stany Zjednoczone.

Bardzo trudno jest wskazać początki głębokiego państwa w Turcji. Zdaniem niektórych badaczy powstało ono po ustanowieniu Republiki Tureckiej w 1923 r. i tworzyły je siły zbrojne – autonomiczny podmiot

polityczny stojący na straży kemalizmu i modelu państwa opracowanego przez założyciela republiki, Mustafę Kemala Atatürka. Jak podkreślił jednak S. Kaya w publikacji *The Rise and Decline of the Turkish „Deep State": The Ergenekon Case*, geneza *deep state* sięga 1889 r., czyli powstania tajnej organizacji Komitetu Jedności i Postępu (ang. Committee of Union and Progress, tur. İttihad ve Terakki Cemiyeti), mającej na celu zmianę → r e ż i m u [t. 3] panującego w Turcji. Organizacja ta nigdy nie przyjęła formy partii politycznej, działając w sposób konspiracyjny. W 1913 r. jej członkowie przeprowadzili zamach stanu, w wyniku którego śmierć poniósł minister obrony, 2 urzędników, a wielki wezyr został zmuszony do ustąpienia. Ustanowiony został tym samym precedens → p u c z ó w w o j s k o w y c h [t. 3] i ultimatów politycznych. Komitet Jedności i Postępu został rozwiązany w 1918 r., jednak kultura polityczna przez niego ukształtowana przetrwała i jest aktualna do dzisiaj. Składają się na nią ultranacjonalizm, zaangażowanie wojska w politykę oraz uzasadnienie stosowania → p r z e m o c y [t. 3] w imię ojczyzny. Zamachy stanu w historii najnowszej Turcji przeprowadzane były kilkukrotnie. W 1960 i 1980 r. doszło do bezpośredniej interwencji wojskowej, a w 1971 i 1997 r. zmuszono rząd do dymisji.

Od 2002 r. głębokie państwo jest sukcesywnie osłabiane przez rządzącą Turcją Partię Sprawiedliwości i Rozwoju (AKP). W swoim programie odwoływała się do tradycji politycznej islamu i oficjalnie kontestowała laicki charakter Republiki Tureckiej, odrzucając tym samym tradycję kemalizmu, którego strzegła armia. Opierając się na idei demokratyzacji i dowartościowania mas społecznych, wygrywała kolejne wybory parlamentarne, zdobywając w 2002 r. 34,28% głosów, w 2007 r. 46,58% głosów, w 2011 r. 49,83% głosów, w 2015 r. 49,50% głosów i 2018 r. 42,56% głosów. W 2018 r. samodzielnie utworzyła rząd. Jednym z pierwszych przykładów oporu, jaki AKP postawiła głębokiemu państwu, był wybór A. Güla na prezydenta Turcji w 2007 r., pomimo sprzeciwu opozycji politycznej i wojska. Kolejnymi były afery Ergenekon i Balyoz. Balyoz („Młot") był kryptonimem spisku, w którym miało uczestniczyć kilkuset przedstawicieli wojska celem obalenia demokratycznie wybranego rządu AKP. Głównym dowodem przeciwko oskarżonym były nagrania z 2003 r. wysokich rangą wojskowych planujących zdestabilizować państwo za pomocą serii zamachów terrorystycznych

i sprowokowania Grecji do zestrzelenia tureckiego samolotu, co stworzyłoby pretekst do przeprowadzenia puczu i odsunięcia Partii Sprawiedliwości i Rozwoju od władzy. Śledztwo rozpoczęło się w 2010 r. i zakończyło w 2012 r. W stan oskarżenia postawieni zostali m.in.: były dowódca 1. Armii tureckiej gen. C. Dogan, dowódca sił powietrznych gen. H. Ibrahim i dowódca → m a r y n a r k i w o j e n n e j [t. 3] adm. O. Omek, łącznie 325 → ż o ł n i e r z y [t. 4]. Sąd skazał oskarżonych na kary od 13 do 20 lat pozbawienia wolności. Równolegle do procesu Balyoz toczył się proces w sprawie afery Ergenekon, domniemanej organizacji terrorystycznej, której celem również miała być destabilizacja polityczna kraju dokonana za pomocą zamachów terrorystycznych. W wyniku śledztwa sąd skazał 327 czynnych i byłych wojskowych na kary do 20 lat pozbawienia wolności.

Definiowanie głębokiego państwa w Turcji zaczęło zmieniać się w 2013 r., kiedy dotychczasowi sojusznicy – ówczesny premier R.T. Erdoğan stojący na czele AKP oraz muzułmański uczony i duchowny F. Gülen stojący na czele Ruchu Cemaat (Ruch Fethullaha Gülena) – rozpoczęli rywalizację o wpływy. Jednym z powodów otwartego konfliktu miała być rosnąca frustracja członków ruchu w obliczu postępującej dominacji Erdoğana oraz ograniczanie wpływów Cemaat. W 2013 r. powiązani z Gülenem prokuratorzy ujawnili aferę korupcyjną, oskarżając ministrów rządu AKP, łącznie z premierem i jego synem. Władze tureckie rozpoczęły zwalczanie ruchu i jego członków znajdujących się w wielu instytucjach państwa, takich jak sądownictwo, szkolnictwo, media i biznes. Główną bitwą, jaką AKP stoczyła z głębokim państwem, był nieudany pucz, do którego doszło w nocy z 15 na 16 lipca 2016 r. Według oficjalnej wersji przedstawionej przez stronę rządową był on próbą obalenia rządu i odsunięcia od urzędu prezydenta Erdoğana, zorganizowaną przez zbuntowaną część wojska, inspirowaną przez Ruch Fethullaha Gülena. W puczu wzięło udział ponad 8 tys. żołnierzy, tysiąc kadetów akademii wojskowej służących w 1., 2. i 3. Armii tureckiej, siłach powietrznych i marynarce wojennej, wspieranych przez ciężki sprzęt, samoloty, helikoptery i → o k r ę t y w o j e n n e [t. 3]. W czasie jego trwania śmierć poniosło ponad 300 osób, w tym 179 cywilów. Zamach stanu stał się pretekstem dla AKP do ostatecznego osłabienia, jeśli nie zniszczenia głębokiego państwa. Do 5 listopada 2016 r. aresztowanych zostało ponad 34 tys. osób, zwolniono z pracy 105 tys. funkcjonariuszy

służby cywilnej, usunięto ze stanowisk 3,6 tys. sędziów i prokuratorów kojarzonych z Ruchem Cemaat, zwolniono z pracy ponad 6 tys. pracowników naukowych, 20 tys. nauczycieli, zamknięto 2 tys. placówek oświatowych oraz 186 gazet i telewizji. Zwycięstwo nad puczystami umożliwiło AKP i prezydentowi Erdoğanowi przyśpieszoną konsolidację władzy w obszarach do tej pory niedostępnych dla nich, czyli w wojsku i wymiarze sprawiedliwości. Przyśpieszyło również proces budowania Nowej Turcji, oficjalnie odwołującej się do tradycji osmańskiej, odrzucającej laickość państwa i uprzywilejowaną pozycję elit wojskowych.

W Rosji głębokie państwo ma 2 znaczenia. Z jednej strony są to tajne służby, tworzące niezależnie od panującego ustroju podmiot polityczny będący jednym z filarów władzy (Ochrana – Czeka – GPU – OGPU – KGB – FSB/GRU/SWR). Z drugiej strony funkcjonuje pojęcie „głębokich struktur". M. Domańska z Ośrodka Studiów Wschodnich zdefiniowała głębokie struktury jako kompleks podstawowych wartości, norm, wzorców zachowań i współzależności między nimi, porządkujący obraz świata i stanowiący fundament modelu rządów i kultury politycznej Rosji. Składają się na nie patrymonialne wyobrażenie establishmentu na temat państwa jako własności przywódcy oraz podporządkowanie stosunków społeczno-politycznych logice relacji patron – klient. Innymi słowy ujmuje się ustrój polityczny w Rosji jako ustrój zbliżony do wczesnośredniowiecznej formy organizacji władzy, w której państwo wraz z ludnością poddaną stanowiło prywatną dziedziczoną własność władcy.

Głębokie struktury, w skład których wchodzi bliskie otoczenie prezydenta (władcy), struktury siłowe, wielki biznes, zorganizowane grupy przestępcze oraz administracja państwa, przez dziesięciolecia utrudniały realną demokratyzację Rosji, czerpiąc korzyści z wpływu na bieg wydarzeń politycznych. Ich funkcjonowanie generuje szereg →patologii społecznych [t. 3], takich jak →korupcja, nepotyzm, masowa defraudacja środków publicznych przez przedstawicieli władz w prywatnych celach czy powiązanie organów władzy z →przestępczością zorganizowaną [t. 3]. Zasadniczym celem przywódcy Rosji staje się w związku z powyższym wypracowanie konsensusu między kluczowymi grupami wpływu tworzącymi głębokie struktury. W przeciwieństwie do Turcji nie ma obecnie w Rosji siły politycznej podważającej dominującą

rolę głębokich struktur w polityce wewnętrznej i zagranicznej państwa. Do ograniczenia ich wpływów może dojść w 2 przypadkach: zachwiania równowagi między poszczególnymi grupami i wzajemnego zwalczania się lub „kolorowej rewolucji", czyli aktywnych protestów społecznych na dużą skalę, zmierzających do zmiany obecnych elit decyzyjnych i formy sprawowania władzy. Efektem „kolorowych rewolucji" mogłoby być zmuszenie do rezygnacji z urzędu prezydenta bądź rządu (obecnie wariant mało prawdopodobny) lub zawarcie kompromisowego taktycznego porozumienia między przedstawicielami protestujących a głębokimi strukturami państwa, co doprowadziłoby do ograniczenia roli rządzących.

W Stanach Zjednoczonych pojęcie głębokiego państwa nabrało nowego znaczenia w 2017 r. po zaprzysiężeniu Donalda Trumpa na prezydenta USA. Urzędnicy z otoczenia prezydenta stosowali je w kontekście politycznych, wojskowych i biznesowych grup wpływu, które sprzeciwiały się nowej administracji. Po raz pierwszy pojawiło się jednak kilka lat wcześniej, kiedy były pracownik amerykańskiego Kongresu M. Lofgren po przejściu na emeryturę zaczął opisywać zjawisko *deep state*. W pierwszej kolejności poruszył tę tematykę w eseju *Anatomy of the Deep State*, a następnie w książce *The Deep State. The Fall of the Constitution and the Rise of a Shadow Government*. Problematykę tę poruszył również Scott w książce *The American Deep State: Wall Street, Big Oil, and the Attack on U.S. Democracy.* Określił on *deep state* jako drugi porządek lub drugi rząd, który rozwinął się po II wojnie światowej za konstytucyjnymi organami państwa. Jest on częściowo zinstytucjonalizowany w postaci agencji wywiadowczych, takich jak CIA i NSA, prywatnych korporacji – Booz Allen Hamilton czy SAIC – Wall Street i przedsiębiorstw naftowych. W badaniu →opinii publicznej [t. 3] przeprowadzonym w marcu 2018 r. przez Monmouth University Polling Institute 37% respondentów odpowiedziało, że spotkało się z pojęciem głębokiego państwa. Na pytanie, czy wierzą w działanie niewybieralnych urzędników i wojskowych manipulujących polityką krajową, ponad 2/3 badanych odpowiedziało „tak".

Tomasz Wójtowicz

S. Ananicz, *Turcja: wyrok w sprawie Balyoz*, 26.09.2012, OSW.waw.pl (dostęp 28.12.2019); B. Burnett, *The War on Democracy: The Deep State*, 3.07.2014,

HuffPost.com (dostęp 27.12.2019); M. Chudziak, *Pucz jako mit założycielski. Filary ideologiczne nowej Turcji*, Ośrodek Studiów Wschodnich, Warszawa 2017; M. Domańska, *Putinizm po Putinie. O „głębokich strukturach" rosyjskiego autorytaryzmu*, Ośrodek Studiów Wschodnich, Warszawa 2019; D. Filkins, *The Deep State*, 5.03.2012, NewYorker.com (dostęp 27.12.2019); S. Kaya, *The Rise and Decline of the Turkish „Deep State": The Ergenecon Case*, „Insight Turkey" 2009, vol. 11, no. 4; M. Lofgren, *Essay: Anatomy of the Deep State*, 21.02.2014, BillMoyers.com (dostęp 31.12.2019); P.D. Scott, *The State, the Deep State, and the Wall Street Overworld*, „The Asia-Pacific Journal" 2014, vol. 12, iss. 10, no. 5; K. Wasilewski, *Układ po turecku*, 6.04.2011, PSZ.pl (dostęp 27.12.2019); B. Zalewski, *Moja rekonstrukcja intencji „głębokiego państwa" III RP*, RMF24.pl (dostęp 30.12.2019).

GŁOS AMERYKI (Voice of America, VOA) – amerykańska agencja multimedialna, która służy jako instytucja rządowa Stanów Zjednoczonych dla pozamilitarnego nadawania zewnętrznego z siedzibą w Waszyngtonie. Jest największym amerykańskim nadawcą międzynarodowym. VOA produkuje treści cyfrowe, telewizyjne i radiowe w 47 językach, które dystrybuuje do stacji stowarzyszonych na całym świecie. Są one odbierane przede wszystkim przez zagranicznych odbiorców, więc działalność VOA ma wpływ na zagraniczną → o p i n i ę p u b l i c z n ą [t. 3] w sprawie USA i ich obywateli. Głos Ameryki opiera się na wiadomościach, → i n f o r m a c j a c h i programach kulturalnych.

VOA został założony w 1942 r. przez War Reporting Office i miał produkować programy radiowe dla Europy i Afryki Północnej okupowanych przez Niemcy w celu zwalczania nazistowskiej → p r o p a g a n d y [t. 3] za pomocą dokładnych i bezstronnych wiadomości i informacji. Od tego czasu VOA służył światu konsekwentnym przesłaniem prawdy, nadziei i inspiracji. VOA zapewnia wiadomości, informacje i programy kulturalne za pośrednictwem internetu, mediów mobilnych i → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3], radia i telewizji. VOA jest finansowany przez rząd USA za pośrednictwem amerykańskiej agencji Global Media.

Pierwsza audycja w języku niemieckim została nadana 1 lutego 1942 r. W.H. Hale otworzył program słowami: „Dzisiaj i codziennie będziemy rozmawiać z tobą o Ameryce i wojnie. Wiadomości mogą być dla nas dobre. Wiadomości mogą być złe. Ale powiemy ci prawdę". Głos Ameryki powstał w opozycji do machiny propagandowej Goebbelsa. Zgodnie z prawem

Stanów Zjednoczonych państwowe stacje radiowe nie mogą nadawać bezpośrednio do obywateli USA. Ma to na celu ochronę obywateli USA przed propagandą i manipulacją ich własnego rządu.

Pierwsza transmisja VOA do Europy została wykonana za pomocą nadajników długiej i średniej fali BBC. Przed tą datą rząd Stanów Zjednoczonych utworzył w 1941 r. Służbę Informacji Zagranicznej (Foreign Information Service, FIS) do produkcji programów dla Europy i Azji transmitowanych przez stacje krótkofalowe prywatne znajduje się w USA.

Stany Zjednoczone były jedyną potęgą światową bez sponsorowanej przez rząd międzynarodowej usługi radiowej. Holandia była pierwszym krajem, który nadawał regularne audycje poza swoimi granicami, inaugurując program krótkofalowy na Dalekim Wschodzie w 1927 r. Postrzegając radio jako instrument polityki zagranicznej, Związek Radziecki zbudował centrum radiowe w Moskwie i nadawał w 50 językach i dialektach do końca 1930 r. Włochy i Wielka Brytania rozpoczęły swoje „usługi imperialne" w 1932 r., a następnie Francja w kolejnym roku. Nazistowskie Niemcy zbudowały ogromną sieć nadajników w 1933 r. i zaczęły rozprzestrzeniać wrogą propagandę w Austrii. W tym samym roku Berlin rozpoczął transmisje krótkofalowe do Ameryki Łacińskiej. Tymczasem Japonia wykorzystywała radio do promowania swoich narodowych ambicji na Dalekim Wschodzie. Pomimo wysiłków wielu wybitnych osobistości, w tym nowojorskiego kongresmana E. Cellera (który proponował ustawy w 1937, 1938 i 1939 r. w celu utworzenia stacji rządowej, która mogłaby zareagować na niemiecką propagandę), Stany Zjednoczone weszły w lata 40. XX wieku bez żadnych planów utworzenia rozgłośni operującej w skali globalnej. Zasoby krótkofalowe Stanów Zjednoczonych składały się z kilkunastu nadajników o niskiej mocy, będących własnością komercyjną.

Głos Ameryki rozpoczął nadawanie polskiej audycji 7 maja 1942 r. Na przestrzeni lat zmieniały się godziny i częstotliwości, do nadawania wykorzystywano nawet 10 różnych częstotliwości w zakresie fal krótkich, z nadajników zlokalizowanych w różnych częściach świata (Europa, Azja i Stany Zjednoczone), część audycji była nadawana na fali średniej 1197 kHz z nadajnika VOA w Monachium. Najdłuższy program zaczęto nadawać wkrótce po wprowadzeniu stanu wojennego (1981–1983) w PRL, wówczas nadawano 2-godzinny blok poranny w godz. 6:00–8:00 i 5-godzinny blok

wieczorny w godz. 20:00–1:00 po północy. Poza informacjami politycznymi w audycjach polskiej redakcji starano się wówczas pokazywać także różne aspekty życia na Zachodzie, nieznane w komunistycznej rzeczywistości. Po 1989 r. długość programu zredukowano, w 1991 r. nadawano godzinny program poranny w godz. 6:30–7:30 i trzygodzinny program wieczorny w godz. 22:00–1:00, ograniczono też liczbę częstotliwości. Pod koniec lat 90. XX wieku polskie programy VOA były też dostępne w internecie. Ostatnia audycja Głosu Ameryki z Waszyngtonu, prowadzona przez W. Żórniaka, została nadana 27 lutego 2004 r.

Po zakończeniu II wojny światowej rozpoczęła się epoka → z i m n e j w o j n y [t. 4]. Równało się to rozpoczęciu bezprecedensowej → w o j n y [t. 4] propagandowej pomiędzy Zachodem a Wschodem. Narody, które znalazły się w sowieckiej strefie wpływów, były stopniowo odcinane od kontaktów ze światem zewnętrznym. Niezależną informację zastąpiła brutalna indoktrynacja, wysławiająca J. Stalina i „przodujący" ustrój komunistyczny. Izolacja obywateli tych państw miała być pełna i całkowita: ograniczono możliwości wyjazdów zagranicznych, zastopowano wymianę kulturalną, bardzo poważnie ograniczono dostęp do zachodniej prasy i książek. Działania te przyniosły jednak ograniczony sukces – fale radiowe płynące z Zachodu potrafiły przebić się przez żelazną kurtynę.

Z końcem II wojny światowej wiele transmisji VOA zostało zredukowanych lub wyeliminowanych. Następnie pod koniec 1945 r. powołana przez Departament Stanu komisja złożona z prywatnych obywateli pod przewodnictwem profesora Uniwersytetu Columbia A. McMahona poinformowała, że rząd USA nie może być „obojętny na sposób, w jaki nasze społeczeństwo jest przedstawiane innym krajom". W związku z tym 31 grudnia 1945 r. usługi nadawcze VOA i CIAA (Coordinator of Inter-American Affairs) w Ameryce Łacińskiej zostały przekazane Departamentowi Stanu, a Kongres niechętnie przeznaczył środki na ich dalszą działalność w 1946 i 1947 r.

Niechęć wobec międzynarodowych transmisji zniknęła w 1948 r. W tym roku członkowie Kongresu byli pod silnym wpływem eskalacji zimnej wojny i wrogiego nadawania międzynarodowego przez Związek Radziecki i kraje kontrolowane przez ZSRR. Blokada Berlina w 1948 r. potwierdziła potrzebę istnienia amerykańskiego głosu radiowego dla świata.

Uchwalenie ustawy Smith–Mundt Act w tym roku na stałe ustanowiło międzynarodowe programy wymiany informacji i kultury w Ameryce, określając zadania, które VOA realizował już od 6 lat.

Przez następne 2 lata urzędnicy amerykańskiego rządu debatowali nad właściwą rolą amerykańskiej oficjalnej międzynarodowej służby nadawczej. Czy chodziło o doniesienie o nowościach i przedstawianie obrazu Ameryki, czy też miało to być narzędzie polityki zagranicznej USA i „broń" przeciwko Związkowi Radzieckiemu? Kongres postrzegał to jako coraz istotniejszą rolę agencji. Wraz z wybuchem wojny koreańskiej w 1950 r. VOA zaczął nadawać serwisy informacyjne w dodatkowych językach i opracował plany budowy kompleksów nadajników zarówno na wschodnim, jak i zachodnim wybrzeżu Stanów Zjednoczonych.

W 1947 r. Głos Ameryki rozpoczął nadawanie audycji dla obywateli ZSRR w języku rosyjskim pod pretekstem zwalczania „bardziej szkodliwej radzieckiej propagandy skierowanej przeciwko amerykańskim przywódcom i polityce" przez sowieckie media, zgodnie z opracowaniem J.B. Whittona.

W okresie zimnej wojny VOA (tak jak BBC i → Radio Wolna Europa [t. 3]) był uznawany przez ZSRR za „rozgłośnię dywersyjną", skierowaną przeciwko państwom bloku wschodniego. Sygnał Głosu Ameryki był zagłuszany przez wyspecjalizowane struktury armii ZSRR i MSW PRL (podobnie jak transmisje wspomnianych BBC i Radia Wolna Europa). Państwa socjalistyczne, w których nadawał Głos Ameryki, zaczęły również sponsorować proces „wyciszenia" tej transmisji. W 1956 r. Polska Republika Ludowa przestała zagłuszać VOA, ale np. Ludowa Republika Bułgarii robiła to do lat 70. XX w. Chiny tłumiły transmisje Głosu Ameryki od 1956 do 1976 r.

W latach 60. i 70. XX w. Głos Ameryki nadawał najważniejsze wiadomości epoki, takie jak przemówienia M.L. Kinga (*I Have a Dream*) czy pierwszy spacer N. Armstronga po Księżycu. W trakcie → kryzysu na Karaibach VOA nadawał wiadomości w języku hiszpańskim 24 godziny na dobę.

Na początku lat 80. XX w. Głos Ameryki wydał 1,3 mld USD na program przywracania i ulepszania nadawania z lepszymi możliwościami technicznymi. Ponadto w latach 80. VOA emitował programy telewizyjne i regionalne na Kubę, które Kuba próbowała zakłócać.

W 1985 r. Głos Ameryki Europa został utworzony jako specjalna usługa w języku rosyjskim, transmitowana z modulacją częstotliwości FM i z modulacją amplitudy AM oraz w sieciach kablowych w całej Europie. Usługa była nadawana w nowoczesnym formacie 24 godziny na dobę. Głos Ameryki Europa przestał nadawać bez uprzedniego publicznego ogłoszenia w styczniu 1997 r. z uwagi na redukcję kosztów. Transmisja została wznowiona w projekcie Głos Ameryki Express 4 lipca 1999 r., który później stał się Głosem Ameryki Music Mix, a od 1 listopada 2014 r. – Głosem Ameryki 1.

W 1989 r. Głos Ameryki rozpoczął nadawanie w języku mandaryńskim i kantońskim, aby informować miliony Chińczyków o ruchu demokratycznym w tym kraju, w tym o demonstracjach na placu Tian'anmen. Od 1990 r. Stany Zjednoczone wzmocniły międzynarodowy system nadawania, kiedy utworzyły Biuro Nadawcze.

Wprowadzenie nowych i rozszerzonych programów dla słuchaczy w Iranie, Afganistanie i Chinach otworzyło przed VOA drogę do ogromnej liczby nowych odbiorców. Jednak, jak przewidywał Giddens, potencjał VOA w dotarciu do coraz większej liczby obywateli świata był upośledzany przez niewystarczające zasoby. Wraz z końcem lat 70. rozdźwięk między założeniami programowymi VOA a poziomem finansowania doprowadził do poważnych niedociągnięć zarówno wśród personelu, jak i obiektów. Prawie każda obsługa językowa była słabo obsadzona. Słuchacze w wielu częściach świata skarżyli się, że transmisje VOA brzmiały słabo i były zniekształcone. Na początku lat 80. wiele nadajników VOA miało ponad 30, a niektóre ponad 40 lat, rosła konkurencja w branży nadawczej. W połowie lat 80. XX w. ok. 160 stacji tłoczyło się w międzynarodowej przestrzeni radiowej z ponad 25 tys. godzin transmisji tygodniowo.

Po utworzeniu Wspólnoty Niepodległych Państw (WNP) i upadku rządów komunistycznych w całej Europie Wschodniej VOA kontynuował codzienne transmisje wiadomości i informacji do regionu. Nowe rządy próbowały – z różnym powodzeniem –realizować zasady demokracji. Przywódcy Europy Wschodniej, np. V. Havel, prosili Zachód, aby pomógł im zrozumieć, jak stworzyć infrastrukturę instytucji demokratycznych. VOA odpowiedział transmisjami wyjaśniającymi, jak działa demokracja na Zachodzie i jak funkcjonują gospodarki rynkowe.

Niektórzy komentatorzy uważają Głos Ameryki za formę propagandy. W *Przewodniku najlepszych praktyk VOA* (*VOA Best Practices Guide*) stwierdza się jednak:

> Dokładność, jakość i wiarygodność VOA są jego najważniejszymi atutami, opierają się na postrzeganiu VOA jako obiektywnego i wiarygodnego źródła amerykańskich, regionalnych i światowych wiadomości i informacji.

W odpowiedzi na wniosek Departamentu Sprawiedliwości Stanów Zjednoczonych, aby → RT [t. 3] zarejestrowano jako → agenta zagranicznego [t. 1] na podstawie ustawy o rejestracji zagranicznych agentów, rosyjskie Ministerstwo Sprawiedliwości uznało wspierane przez USA rozgłośnie radiowe Głos Ameryki i → Radio Swoboda [t. 3], przeznaczone dla odbiorców w Rosji, za media „pełniące funkcję zagranicznego agenta" w grudniu 2017 r. Taki status nadano również 7 związanym z nimi projektom.

Głos Ameryki nadaje obecnie w 47 językach. Publiczność VOA ma dostęp do treści nadawanych w radiu, telewizji, internecie i mediach społecznościowych, za pośrednictwem ponad 2,2 tys. platform radiowych i telewizyjnych na całym świecie, które odbierają programy VOA drogą satelitarną. Co tydzień ponad 275 mln ludzi odbiera wiadomości i informacje Głosu Ameryki. VOA obiecuje w dalszym ciągu wykorzystywać nowe technologie i platformy cyfrowe oraz udoskonalać transmisje tak, aby uwzględniać potrzeby słuchaczy i dostarczać im wyczerpujących, aktualnych i wiarygodnych informacji.

Łukasz Czekaj, Olga Wasiuta

M.I. Ayish, *The VOA Arabic Service: A Study of News Practices and Occupational Values*, „Gazette" 1987, vol. 40, no. 2; J.F. Broderick, D.W. Miller, *Consider the Source: A Critical Guide to 100 Prominent News and Information Sites on the Web*, Information Today, Medford 2007; R. Chalmers, *New Image for Voice of America*, „New York Times Magazine", 13.04.1980; Ł. Czekaj, *Voice of America*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; W.P. Dizard, *Inventing Public*

Diplomacy: The Story of the U.S. Information Agency, Lynne Rienner Publishers, Boulder 2004; A. Heil, *Voice of America: History*, Columbia University Press, New York 2003; J. Houseman, *Front and Center*, Simon and Schuster, New York 1979; T. Leszkowicz, *Oblicza propagandy PRL*, Promohistoria Michał Świgoń, Warszawa 2016; P. Machcewicz, *„Monachijska menażeria". Walka z Radiem Wolna Europa 1950–1989*, IPN, Warszawa 2007; A. Puddington, *Rozgłośnie wolności. Tryumf Radia Wolna Europa i Radia Swoboda w zimnej wojnie*, tłum. A. Borzym, Wydawnictwo UMK, Toruń 2009; W.A. Rugh, *American Encounters with Arabs: The „Soft Power" of U.S. Public Diplomacy in the Middle East*, Praeger Publishers, Santa Barbara 2006; J. Semelin, *Wolność w eterze*, tłum. H. Abramowicz, Wydawnictwo UMCS, Lublin 1999; M. Święcicki, *Z mikrofonem przez USA: audycje „Głosu Ameryki"*, Oficyna Wydawnicza RYTM, Warszawa 1991; J.B. Whitton, *Cold War Propaganda*, „The American Journal of International Law" 1951, vol. 45, no. 1.

GOTOWOŚĆ PRZEMYSŁU OBRONNEGO (ang. *defence industry readiness*) – już ponad 100 lat temu zauważono, że przygotowania do → w o j n y [t. 4] to jedna z 2 głównych części składowych ekonomii politycznej wojny. W warunkach konfliktu zbrojnego szanse powodzenia państwa warunkuje m.in. przestawienie gospodarki na tory wojenne i przyznanie priorytetu produkcji wojennej. Nie dziwi więc troska wielu państw o to, by – pomimo przemian politycznych i gospodarczych – utrzymywać narodową bazę przemysłu obronnego. Zdają sobie sprawę, że samoistna siła militarna, bazująca na wysokim poziomie wydatków wojskowych, jest potencjalnie znacznie mniej skuteczna niż siła militarna oparta na własnym przemyśle obronnym.

Słowo „potencjalnie" nie jest tu przypadkowe – w czasie pokoju wspomniana gałąź gospodarki powinna bowiem być przygotowana ze strony wojskowej, gospodarczej i organizacyjnej do zaspokajania zwiększonych potrzeb wojska wynikających z → z a g r o ż e n i a [t. 4] konfliktem zbrojnym lub jego trwania. Chodzi nie tylko o produkcję uzbrojenia. Ważnym elementem gotowości przemysłu obronnego będzie też m.in. jego zdolność do dokonywania na bieżąco masowo poważnych napraw sprzętu bojowego i zdolność do innowacyjności.

Gotowość przemysłu obronnego jest stopniowalna. Za podstawową miarę gotowości przemysłu obronnego można uznać prawdopodobieństwo realizowania przez niego wymaganej funkcji w określonych

warunkach wojennych, w konkretnym okresie i przy założeniu, że mimo przeszkód czynionych przez wroga dostarczono wymagane środki zewnętrzne (podzespoły, półfabrykaty, surowce itp.).

Jeśli dany podmiot prawa międzynarodowego posiada odpowiednio rozbudowany przemysł obronny, można rozważyć dokonanie oceny gotowości przemysłu obronnego w odniesieniu do poszczególnych rodzajów wojsk.

Przy ocenie gotowości przemysłu obronnego sojuszu wojskowego stosowany jest podział na poszczególnych jego członków. Jak wynika z ustaleń M. Sułka, pozwala to ustalić państwa, które w pewien sposób pasożytują na wysiłku obronnym innych. Do obliczenia poziomu gotowości przemysłu częściowo przydatny jest współczynnik → m o b i l i z a c j i [t. 3] (uruchomienia) potencjału gospodarczo-obronnego.

Gotowość przemysłu obronnego uzyskuje się głownie dzięki działaniom planistycznym i rzeczowym. W ramach programowania obronnego przygotowywane są warunki pozwalające na przygotowanie określonych przedsiębiorstw do funkcjonowania w czasie zagrożenia konfliktem zbrojnym i po jego wybuchu.

W → d y k t a t u r a c h w o j s k o w y c h i państwach totalitarnych gotowość omawianej gałęzi gospodarki łatwiej osiągnąć i utrzymać niż w państwach demokratycznych o gospodarce wolnorynkowej. Przyczynami tego są m.in.: centralne planowanie, nieustępliwe nakazowe kierowanie, preferowanie przemysłu obronnego kosztem gałęzi gospodarki nastawionych na potrzeby obywateli oraz większe szanse utrzymania tajemnicy. W przypadku takich państw problemem jest jednak ograniczona innowacyjność tego przemysłu powodująca znaczne uzależnienie od zagranicznych dostaw pod względem określonych typów uzbrojenia, technologii lub podzespołów.

Skala dbałości władz państw o gotowość przemysłu obronnego zależy od kilku czynników. Najważniejsza jest ocena prawdopodobieństwa wystąpienia konfliktu zbrojnego. Poziom dbałości jest także powiązany z ewentualnymi ofensywnymi koncepcjami militarnymi władz państwa.

W przypadku niektórych dyktatur wojskowych, państw totalitarnych oraz takich podmiotów prawa międzynarodowego, które planują w najbliższym czasie atak np. na sąsiadów, bardzo duża część lub całość

możliwości produkcyjnych przemysłu obronnego jest uruchomiona i wykorzystana na potrzeby własne armii albo militarnego bloku państw, do których dane państwo należy.

Wynika to z reguły z preferencji władz i decydującej lub istotnej pozycji armii w strukturach państwa. W takich przypadkach poziom gotowości przemysłu obronnego często jest wysoki, gdyż niewykorzystane moce produkcyjne są niewielkie.

Częściej omawiana wytwórczość ma tylko pewien udział w całej produkcji przedsiębiorstw zaliczanych do przemysłu obronnego. Część spośród przedsiębiorstw produkujących na potrzeby obrony danego państwa lub sojuszu militarnego stanowią podmioty, w których udział wytwórczości jest wysoki. Przykładowo w XXI w. w USA dominują koncerny mające z reguły mniejszościowy udział komponentu cywilnego. W firmach o dużym udziale produkcji cywilnej niekiedy specjalistyczny potencjał produkcyjny przeznaczony na cele wojskowe w czasie pokoju nie jest uruchamiany.

Wyzwaniem są także rozwój technologiczny i coraz większe zróżnicowanie zadań jednostek wojskowych w konfliktach zbrojnych oraz tendencje na rynku uzbrojenia. Przykładem mogą być cykliczne → k r y z y s y zaufania do czołgów w związku z sukcesami modernizacji broni przeciwpancernej. Niekiedy niski stopień modernizacji i skala kapitałochłonności przemysłu obronnego powoduje decyzję władz o faktycznej likwidacji części przedsiębiorstw w tym sektorze gospodarki. Kładziony jest nacisk na rozwój najbardziej nowoczesnych zakładów i import pozostałych rodzajów uzbrojenia.

Poziom gotowości do zaspokajania wojennego zapotrzebowania wojska można podnieść dzięki odpowiedniej międzynarodowej współpracy przemysłów zbrojeniowych. Pozwala ona włączyć wybrane przedsiębiorstwa w ramy międzynarodowych programów badawczo-rozwojowych. Współpraca w ramach bloku wojskowego pozwala na redukcję kosztów produkcji uzbrojenia oraz rozwoju tej części gospodarki i związanego z tym obniżenia ryzyka ekonomicznego.

W momencie konfliktu zbrojnego ułatwia to także przyjęcie pomocy od sojuszników. To ostatnie wymaga bowiem zadbania o odpowiednie wsparcie produkcyjne i logistyczne sojuszniczych oddziałów oraz

kompatybilność własnej produkcji z dostarczanymi przez sojuszników wyrobami gotowymi, częściami zamiennymi, półproduktami itp.

Ograniczeniem współpracy w ramach sojuszu wojskowego jest m.in. spoistość danego bloku wojskowego oraz wiarygodność należących do niego państw, np. jako terminowych dostawców pożądanej jakości części zamiennych do sprzętu wojskowego.

Cenna bywa też współpraca dwustronna. Przykładowo, jak zauważa K. Boutin, chiński przemysł zbrojeniowy może zaspokoić zapotrzebowanie armii w zakresie → o k r ę t ó w w o j e n n y c h [t. 3], ale nie jest w stanie wyprodukować dostatecznie nowoczesnych samolotów. W tym przypadku, by podnieść swój poziom gotowości, podjęto współpracę z przemysłem zbrojeniowym rosyjskim.

W wielu krajach w praktyce często dominuje jednak polityka ochrony własnego przemysłu obronnego. Przewiduje się kooperację jedynie z sojusznikami w ramach bloku wojskowego czy UE.

Największym wyzwaniem w staraniach o gotowość do odpowiedniego zwiększenia produkcji uzbrojenia i wyposażenia wojskowego są koszty generowane przez rozbieżność między bieżącymi zamówieniami państwa a możliwościami produkcyjnymi. Przedsiębiorstwa wchodzące w skład przemysłu obronnego są często odgórnie zobowiązane przez państwo do utrzymania gotowości na wypadek kryzysu i rozpoczęcia konfliktu zbrojnego. Utrzymywanie z własnej inicjatywy przez przedsiębiorcę rezerw parku maszynowego, mocy produkcyjnych oraz surowców jest jednak sprzeczne z podstawowymi zasadami ekonomii. Wykorzystanie znacznej części potencjału wytwórczego do zaspokojenia potrzeb cywilnych jest często ograniczone przez specyfikę technologii oraz przepisy prawne.

W wielu krajach koszty produkcji na potrzeby armii często są wysokie. Jak wskazuje K. Kowalski, niekiedy stosowane są wyższe standardy niż w produkcji skierowanej na rynek komercyjny pod względem niezawodności, obsługiwalności itp. Nie może to dziwić, skoro – zdaniem badacza – wyposażenie wojskowe pozostaje w eksploatacji w warunkach pokojowych nie mniej niż 30 lat.

Na koszt ekonomiczny utrzymania gotowości przedsiębiorstw dualnych wpływa też ich lokalizacja. Priorytetem przy ich budowie były często względy wojskowe, a nie ekonomiczne.

W tej sytuacji poziom gotowości przemysłu obronnego do dostaw broni wysokiej jakości najczęściej zależy od wysokości nakładów państwa na utrzymanie i modernizację przemysłu obronnego, badania, prace wdrożeniowe, inwestycje specjalne, utrzymywanie rezerw mobilizacyjnych, mocy produkcyjnych i remontowych oraz zakup nowych technologii.

Dla utrzymania gotowości przemysłu obronnego ważne są także długie serie zamówień. Pozwalają one rozłożyć wysokie koszty badań i inwestycji na dużą liczbę wyrobów, zgromadzić odpowiednią kadrę i podnosić jej kwalifikacje. By osiągnąć odpowiedni poziom gotowości, ważna jest także dbałość o efektywność i skuteczność finansowania w perspektywie wieloletniej. Ich osiągnięcie wymaga koordynacji działań między różnymi strukturami rządowymi.

By zwiększyć jakość produktów, brytyjscy naukowcy proponowali znaczne premie wypłacane przez rząd zakładom, których produkty są w danej kategorii najwyższej jakości. Byłyby one doliczane do kosztów produkcji.

Jak słusznie zauważył Sułek, przy dużej ilości trudnych do jednoznacznej oceny zmiennych bardzo trudno ustalić odpowiednią wielkość środków przeznaczanych na gotowość przemysłu obronnego.

Ważnym sposobem utrzymania nowoczesnych linii produkcyjnych, wysoko wykwalifikowanych pracowników oraz zasobów badawczo-rozwojowych jest produkcja skierowana do odbiorców zagranicznych. W niektórych przedsiębiorstwach większość produkcji specjalnej jest przeznaczona na eksport. Często władze państw wspierają go przez rozmowy z cudzoziemskimi politykami wysokiej rangi oraz udzielają nabywcom kredytu. Decyduje o tym m.in. miejsce w budżecie kraju zysków z handlu bronią i dostaw jej części zamiennych. W latach 2014–2019 wyraźną większość wśród 10 największych eksporterów tego typu produktów na świecie stanowiły stabilne państwa demokratyczne. Trafne jest tu rozróżnienie dokonane przez G. Dunk na politykę przemysłową obronną i politykę przemysłową w opakowaniu obronnym.

Bardzo ważna dla gotowości przemysłu obronnego jest znajomość i akceptacja nie tylko wymagań armii, ale i ograniczeń wynikających z braku dostępu do odpowiednich technologii oraz źródeł dostaw podzespołów i surowców. Przy ocenie tej drogi obniżenia kosztów i zachowania

gotowości przemysłu obronnego należy bowiem pamiętać, że na rynkach międzynarodowych broni panuje znaczna rywalizacja.

Do osiągnięcia odpowiedniego poziomu gotowości przemysłu obronnego bardzo ważne są także analizy strategiczne dotyczące stanu obecnego, prognoz i trendów, analizy skutków zaniechanych działań, analizy wrażliwości na zmiany tych parametrów, które zostały wykorzystane w najważniejszych prognozach. Optymalny poziom gotowości przemysłu obronnego danego państwa może być różny w zależności także od rodzaju i skali branego pod uwagę konfliktu zbrojnego, jego państw sojuszniczych itp. Wynika to m.in. ze zróżnicowania poziomu i ilości uzbrojenia, którym dysponują poszczególni potencjalni przeciwnicy, uwarunkowań geograficznych poszczególnych potencjalnych konfliktów zbrojnych itp.

Trzeba też ocenić, w jakim stopniu poszczególne potencjalne konflikty zaszkodziłyby funkcjonowaniu przemysłu obronnego. Chodzi tu o np. dostawy półproduktów, eksport części produkcji (odbiorca, → b e z p i e c z e ń s t w o [t. 1] transportu dostaw), import surowców i materiałów, polityczne funkcje przedsiębiorstw międzynarodowych mających główne siedziby poza granicami danego państwa. Należy tu pamiętać o różnicy między wrażliwością w sferze przemysłu obronnego i wrażliwością systemu politycznego. Ten ostatni bywa często bardziej odporny.

Czasem państwo jest formalnym właścicielem wielu lub zdecydowanej większości z zakładów zbrojeniowych (np. w Chinach). Władze szeregu krajów dbają o ograniczony udział sektora prywatnego w tej gałęzi przemysłu. Z jednej strony podnosi on efektywność produkcji, z drugiej jednak zmniejsza poziom gotowości na czas konfliktu zbrojnego. Niekiedy ograniczenia te dotyczą wybranych części przemysłu obronnego. Bardziej powszechne jest dbanie przez państwo o ograniczony udział firm zagranicznych w tej części przemysłu.

Utrzymanie gotowości tej dziedziny gospodarki na wypadek zagrożenia konfliktem zbrojnym lub po jego wybuchu komplikuje jeszcze jeden czynnik. Jest nim zmienność znaczenia przedsiębiorstw o wysokim i niskim udziale produkcji przemysłowej w przemyśle obronnym danego państwa na przestrzeni czasu. Zależy to głównie od polityki wojskowej władz i możliwości budżetowych państwa. Nie zawsze jest wynikiem polityki długofalowej i związanego z nią programu rozwoju sił zbrojnych.

Jak wskazuje W. Lewandowski, czasem są to działania doraźne. W sytuacji znacznych przemian ustrojowych lub gospodarczych z polecenia lub za zgodą władz państwowych część zakładów redukuje część potencjału przeznaczonego na cele wojskowe lub odwrotnie – rośnie jego udział w całości mocy produkcyjnej przedsiębiorstw. W pierwszym przypadku redukcja czasem jednak to pozory. Jest bowiem uzyskiwana przez fuzje lub wykup firm produkujących na potrzeby cywilne.

Nie można produkować uzbrojenia bez zgromadzonych i zabezpieczonych odpowiednich materiałów oraz półproduktów. Niezbędny jest więc zakup i przechowywanie odpowiednio przygotowanych państwowych rezerw gospodarczych, rezerw strategicznych oraz państwowych rezerw mobilizacyjnych. Wiele z wliczanych w ich skład surowców, materiałów i paliw warunkuje gotowość przemysłu obronnego do sprostania wymogom konfliktu zbrojnego. Zapewniają bowiem efektywność działania i nieprzerwaną produkcję.

Dla zapewnienia dostaw surowców na czas zagrożenia konfliktem zbrojnym lub po jego wybuchu ważne jest obniżenie zużycia przez przemysł obronny tych surowców, które w kraju występują zbyt rzadko (lub w ogóle nie występują). Zważywszy na ograniczenia technologiczne, dotyczy to też części półproduktów, niemniej o tym, czy zależność przemysłu obronnego od importu osiągnęła poziom zagrażający jego gotowości obronnej, decydują rządzący politycy.

Gospodarowanie rezerwami przeznaczonymi na wypadek konfliktu zbrojnego wymaga doprecyzowania zadań oraz kompetencji w zakresie tworzenia, przechowywania i wykorzystywania rezerw; bieżącej aktualizacji planów w tym zakresie w razie zmian politycznej i gospodarczej sytuacji międzynarodowej.

Przechowywaniem rezerw zajmują się struktury państwa, ale także, w części krajów, przedsiębiorcy prywatni pod nadzorem państwa. Wadą przechowywania rezerw są wysokie koszty: przechowywania, ekspertyz (stwierdzających, czy mimo upływu ważności np. materiał wybuchowy może być jeszcze przechowywany na cele wojskowe) i odtwarzania (np. w wypadku upłynięcia daty ważności produktu).

By zwiększyć poziom gotowości przemysłu obronnego, ważna jest też dbałość o odpowiednie rozmieszczenie rezerw. Ma ułatwić szybkie

i w miarę bezpieczne dostarczenie ich do fabryki w razie konfliktu zbrojnego. Z tego punktu widzenia istotny jest także rozwój infrastruktury pozwalający wówczas na szybkie dostarczenie wyprodukowanych towarów do wytypowanych przez władze jednostek wojskowych.

Na gotowość przemysłu wojennego wpływa też stopień przygotowania pozostałych elementów składowych opisanej przez Sułka bazy produkcyjno-usługowej nakierowanej na zaspokojenie potrzeb obronnych danego państwa lub sojuszu militarnego. Poza wymienionymi najważniejsze są przedsiębiorstwa wchodzące w skład wyróżnionego przez F. Marczaka przemysłu obronnie zorientowanego – obecnie produkującego wyłącznie na potrzeby cywilne, a w razie konfliktu przestawiającego się na potrzeby konfliktu zbrojnego.

Orientacja w zakresie gotowości przemysłu obronnego przeciwnika wpływa na politykę zagraniczną wobec niego. Przy analizie gotowości przemysłu obronnego trzeba więc także brać pod uwagę działalność obcych służb wywiadowczych (zarówno państw, jak i korporacji zbrojeniowych). Bardzo istotne jest także skuteczne zabezpieczenie mocy produkcyjnych przed zniszczeniem przez przeciwnika. Stąd słusznie podkreślana przez A. Żebrowskiego konieczność dbałości w tym kontekście o ochronę →i n f o r m a c j i dotyczącej gotowości przemysłu obronnego.

Można uznać gotowość przemysłu obronnego za część gotowości militarnej, gospodarki obronnej oraz, w pewnym uproszczeniu, stosowanym przez M. Kaldor, potencjału projektowania i produkcji broni. Analizowane pojęcie w części pokrywa się z przemysłowym potencjałem obronnym i z gotowością techniczną. Ta ostatnia dotyczy jednak także zupełnie innych gałęzi gospodarki.

Tomasz Skrzyński

Defence Industries in Russia and China: Players and Strategies, R.A. Bitzinger, N. Popescu (eds.), European Union Institute for Security Studies, Paris 2017; G. Dunk, *Defence Industry Policy 2016 – Well-Intentioned but Conflicted*, „Security Challenges" 2016, vol. 12, no. 1; E. Jędrych, D. Klimek, *Przemysł wojenny w warunkach globalizacji*, „Biznes Międzynarodowy w Gospodarce Globalnej" 2016, nr 2 (35); K. Kowalski, *Nieuszkadzalność, gotowość i obsługiwalność systemów uzbrojenia*, „Postępy Nauki i Techniki" 2012, vol. 12; T. Kubaczyk, T. Nalepa, *Rezerwy*

strategiczne a zadania wynikające z PMG [Programu Mobilizacji Gospodarki], „Kwartalnik Bellona" 2013, nr 2 (673); S. Kurinia, *Współczesna brytyjska myśl obronno-ekonomiczna*, AON, Warszawa 2000; W. Lewandowski, *Polski przemysłowy potencjał obronny w dobie konsolidacji*, „Bezpieczeństwo Narodowe" 2011, vol. 1 (17); P. Modzelewski, *Finansowanie zadań obronnych w państwie – skuteczność i efektywność a ryzyko*, [w:] *Minister Obrony Narodowej i Naczelny Dowódca Sił Zbrojnych w systemie kierowania bezpieczeństwem narodowym RP. Wybrane problemy*, W. Kitler (red.), AON, Warszawa 2013; M. Sułek, *Programowanie gospodarczo-obronne*, Bellona, Warszawa 2008; A. Żebrowski, *Zagrożenia i bezpieczeństwo przemysłu zbrojeniowego u progu XXI wieku (wybrane aspekty)*, [w:] *Przemysł zbrojeniowy. Tendencje, perspektywy, uwarunkowania, innowacje*, R. Kopeć (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016.

GRABIEŻ DÓBR KULTURY – rabunek dóbr danej kultury, dziedzictwa kulturowego, dzieł sztuki, zwykle zaplanowany i zorganizowany, towarzyszący z reguły konfliktowi zbrojnemu. W kategorii grabieży mieszczą się też kradzieże dóbr kultury, dzieł sztuki, które mogą odbywać się również w czasie pokoju. Rabunkowi może towarzyszyć także – planowane lub nie – niszczenie dóbr kultury. Zagadnienia te są przedmiotem zainteresowania →bezpieczeństwa kulturowego [t. 1].

Mianem *dziedzictwa kulturowego* określa się, na podstawie Konwencji w sprawie ochrony światowego dziedzictwa kulturowego i przyrodniczego z 1972 r.:

> zabytki: dzieła architektury, dzieła monumentalnej rzeźby i malarstwa, elementy i budowle o charakterze archeologicznym, napisy, groty i zgrupowania tych elementów mające wyjątkową powszechną wartość z punktu widzenia historii sztuki lub nauki;
>
> zespoły: budowli oddzielnych lub łącznych, które ze względu na swą architekturę, jednolitość lub zespolenie z krajobrazem mają wyjątkową powszechną wartość z punktu widzenia historii sztuki lub nauki;
>
> miejsca zabytkowe: dzieła człowieka lub wspólne dzieła człowieka i przyrody, jak również strefy, a także stanowiska archeologiczne,

> mające wyjątkową powszechną wartość z punktu widzenia estetycznego, etnologicznego lub antropologicznego.

Mianem *dzieł sztuki* określa się „przedmiot objęty konwencjami międzynarodowymi". Z powodu polityki prowadzonej przez mocarstwa kolonialne:

> Zgr. Og. NZ 13 XII 1973 Rez. 3187 (XXVIII) uchwaliło 113 głosami przy 17 wstrzymujących się, że mocarstwa kolonialne, które wywiozły ze swoich kolonii dzieła sztuki stanowiące dziedzictwo kulturalne danego kraju, winny zwrócić je nieodpłatnie w jak najszybszym czasie.

Dobra kulturalne to przedmiot Konwencji UNESCO o ochronie dóbr kulturalnych, podpisanej 14 maja 1954 r. w Paryżu, która zdefiniowała je w art. 1 w następujący sposób:

> Uważa się za dobra kulturalne, bez względu na ich pochodzenie oraz na osobę ich właściciela: a) dobra ruchome lub nieruchome, które posiadają wielką wagę dla dziedzictwa kulturalnego Narodu, np. zabytki architektury, sztuki lub historii, zarówno religijne, jak świeckie; stanowiska archeologiczne; zespoły budowlane, posiadające jako takie znaczenie historyczne lub artystyczne – dzieła sztuki, rękopisy, książki i inne przedmioty o znaczeniu artystycznym, historycznym lub archeologicznym, jak również zbiory naukowe i poważne zbiory książek, archiwaliów lub reprodukcji wyżej określonych dóbr; b) gmachy, których zasadniczym i stosowanym w praktyce przeznaczeniem jest przechowywanie lub wystawianie dóbr kulturalnych ruchomych, określonych pod literą a), np. muzea, wielkie biblioteki, składnice archiwalne, jak również schrony, mające na celu przechowywanie w razie konfliktu zbrojnego dóbr kulturalnych ruchomych określonych pod literą a); c) ośrodki obejmujące znaczną ilość dóbr kulturalnych określonych pod literą a) i b), zwane ośrodkami zabytkowymi (ang. *centres containing monuments*).

Z hasłem grabieży związane jest też hasło *restytucji dóbr kultury*. Zwroty zagrabionych czy pozyskanych w niewyjaśnionych okolicznościach dóbr kultury są współcześnie zagadnieniem bardzo problematycznym, mimo licznych konwencji i porozumień międzynarodowych, które miały upraszczać tę kwestię. Mianem restytucji dzieł sztuki określa się:

> zwrot dzieł sztuki wywiezionych za granicę lub zagrabionych, przedmiot sporów międzynarodowych. Zgr. Og. NZ 19 XI 1975, Rez. 3391/XXX o restytucji dzieł sztuki krajom, ofiarom ekspropriacji uznała za obowiązek zwrot dzieł sztuki, pomników, rzeczy muzealnych, manuskryptów i dokumentów, stanowiących dziedzictwo kulturalne danego narodu. Konwencja UNESCO z 1970 zakazuje importu, eksportu i transferu przywłaszczonych bezprawnie dzieł sztuki.

Grabieże w polskiej historii kojarzone są przede wszystkim z rabunkiem dóbr polskiej kultury, przeprowadzonym w wyniku zorganizowanej i zaplanowanej działalności i polityki III Rzeszy oraz ZSRR w trakcie II wojny światowej. W toku polskich dziejów trzeba jednak wspomnieć o innych zdarzeniach. Pierwszym odnotowanym przypadkiem rabunku tego typu wydaje się wywiezienie do Czech relikwii św. Wojciecha przez księcia Brzetysława I w trakcie jego najazdu na Polskę w 1038 r. Relikwie, które złożone były w katedrze w Gnieźnie, nigdy nie powróciły do Polski i do dzisiaj umieszczone są w katedrze św. Wita w Pradze (choć szczątki św. Wojciecha znalezione zostały lata później w czasie odbudowy katedry gnieźnieńskiej).

Zjawisko rabunku dóbr kultury, a także ich niszczenie znane jest jednak od starożytności. Szczególnie doświadczone przez takie wydarzenia były tereny europejskie. W związku z → w o j n a m i [t. 4], podbojami, zdobywaniem nowych terenów, migracjami walecznych ludów dochodziło do rabunku i niszczenia miejscowych kultur. Jeśli chodzi o Europę i tereny basenu Morza Śródziemnego, którymi podbijający byli zainteresowani, trzeba wspomnieć o rabunkach w trakcie podbojów Rzymu (wojny punickie, Kartagina i Korynt, II w. p.n.e.), w czasie podbojów związanych z migracjami Wandalów i Wizygotów, zdobyciem

przez nich Rzymu (V w.) i spaleniem miasta, działalności rabunkowej Wenecjan, w trakcie XV i XVI-wiecznych wojen włoskich (plądrowanie bibliotek w Neapolu i Pawii), *Sacco di Roma* w 1527 r., podczas tragedii XVII-wiecznych konfliktów: wojny trzydziestoletniej, wojny turecko-weneckiej (zniszczenie Akropolu) oraz w czasie potopu szwedzkiego, który odcisnął niebywałe piętno także na polskich stratach dzieł sztuki, porównywalne jedynie z grabieżami wojennymi XX w. na terenie ziem polskich.

W czasie VI wojny polsko-szwedzkiej, tzw. potopu szwedzkiego, w wyniku działań armii szwedzkiej, na której czele stał król Karol X Gustaw, Polska poniosła ogromne straty – oprócz ogromnych strat ludności, ocenianych w skali procentowej na ok. 40% populacji, także materialne, oceniane na ok. 50% całego majątku, w tym straty dóbr kultury oraz terytorialne. Miastami, które najbardziej ucierpiały na szwedzkiej → i n w a z j i, były Warszawa (łupiona trzykrotnie, nie tylko przez samych Szwedów, ale i innych, biorących udział w najazdach z ramienia wojsk szwedzkich, → ż o ł n i e r z y [t. 4]) i Kraków (wzgórze wawelskie łupione było wielokrotnie, łącznie z dewastacją królewskich grobowców).

Rozbiory były kolejną tragedią z perspektywy strat kultury polskiej oraz światowej, mowa o kolekcjach polskich władców i możnych rodów. Trudno rozstrzygnąć, który z zaborców zagrabił najcenniejsze z przedmiotów tworzących zbiory królów i magnatów. Jeśli chodzi o poszczególne grabieże, niewątpliwie kilka z nich miało dla przyszłej Polski i Polaków największe znaczenie. Bezdyskusyjnie symboliczne znaczenie miało zagrabienie przez Rosjan sztandaru zdobytego przez Jana III Sobieskiego pod Wiedniem. Natomiast najtragiczniejszym wydarzeniem było z pewnością najpierw wywiezienie, a później zniszczenie przez Prusaków regaliów znajdujących się w skarbcu królewskim na Wawelu. Decyzję o przetopieniu insygniów władców polskich oraz innych przedmiotów związanych ze sprawowaniem władzy, np. relikwiarzy, podjął Fryderyk Wilhelm III Pruski. Jednym z najbardziej znanych insygniów, które utraciła wówczas Polska, była tzw. korona Bolesława Chrobrego, znana m.in. ze szkiców i rysunków różnych artystów, m.in. J.K. Wernera oraz M. Bacciarellego. Austriacy z kolei doprowadzili do upadku renesansowej świetności Zamku Królewskiego na Wawelu, przebudowując go na wojskowe koszary.

XX-wiecznymi konfliktami zbrojnymi, które wyrządziły najwięcej szkód polskiemu dziedzictwu kulturowemu, były bez wątpienia dwie wojny światowe. W I wojnie światowej Polska ucierpiała zwłaszcza w związku z rabunkiem rosyjskim, ale Niemcy również wykazali się zorganizowanym działaniem np. wobec Kalisza, w którym, jak się ocenia, zburzonych zostało 95% budynków. Historycy i historycy sztuki podkreślają jednak, że największych strat w obszarze kultury i sztuki doznała Polska w wyniku II wojny światowej. Podobnie jak przy okazji wcześniejszych konfliktów zbrojnych, które miały miejsce na terenie ziem polskich, niszczenie i rozgrabianie dóbr kultury nie wiązało się z polityką jednej z sił. Przyznać jednak trzeba, że tylko jedna ze stron, okupant niemiecki, miała zorganizowany plan grabieży. Wojska radzieckie grabiły w sposób przypadkowy to, czego nie udało się wcześniej wywieźć Niemcom. Jak podaje MKiDN, w bazie danych ministerstwa znajduje się 60 tys. rekordów dot. zaginionych obiektów, zabytków kultury. Do ponad 10 tys. ustalonych dzieł zgromadzono dodatkowo dokumentację ikonograficzną. Opracowaniem takiej dokumentacji nadal zajmują się specjaliści z różnych obszarów nauk, prowadząc badania, kwerendy archiwalne w Polsce i poza jej granicami (w Rosji, Niemczech, Austrii, Czechach, Francji i w Stanach Zjednoczonych). Opracowanie materiałów dokonywane jest na zlecenie Departamentu Dziedzictwa Kulturowego. Pozyskane w ten sposób → i n f o r m a c j e podawane są do informacji publicznej w publikacjach z serii wydawniczej „Straty Kultury Polskiej". Dzięki takim pracom istnieje możliwość przygotowania wniosków restytucyjnych, a także prowadzenia różnego rodzaju działań zmierzających do odzyskiwania utraconych obiektów.

Jeśli chodzi o najtragiczniejsze wydarzenia współczesne, które wstrząsnęły ludzkością z perspektywy ogólnoświatowych dóbr kultury, nie można nie wspomnieć o niszczeniu zabytków kultury przez talibów oraz → P a ń s t w o I s l a m s k i e [t. 3]. Wymienić tutaj trzeba zniszczenie w 2001 r. przez afgańskich talibów posągów Buddy z VI w. w prowincji Bamian na terenie dzisiejszego Afganistanu (wpisane na listę światowego dziedzictwa → U N E S C O [t. 4] w 2003 r.) oraz próby wysadzenia w 2007 r. przez pakistańskich talibów na terenie dzisiejszego Pakistanu, we wsi Dżehanabad w dolinie Swatu, płaskorzeźby z II w p.n.e. przedstawiającej Buddę. Innymi przejawami łupieżczej działalności jednej ze stron konfliktu

było także niszczenie przez tzw. Państwo Islamskie stanowisk archeologicznych i muzeów, np. Muzeum Niniwy w Mosulu, czy znajdujące się również na terenie dzisiejszego Iraku, a kiedyś mezopotamskie miasto Nimrud ze stanowiskiem archeologicznym (zniszczenie potępione przez ówczesną dyrektor generalną UNESCO I. Bokową) lub mezopotamska Hatra (na liście światowego dziedzictwa UNESCO od 1985 r.). Wszystkie trzy miejsca zniszczone zostały w 2015 r. Działania te motywowane były przez członków obu grup względami religijnymi. Powołują się oni na Koran i zakaz przedstawień ludzkich (oraz zwierzęcych), mogący prowadzić do bałwochwalstwa, które jest w islamie oczywiście zakazane. Krajobraz kulturowy i pozostałości archeologiczne doliny Bamian w 2003 r., a Hatra w 2015 r. wpisane zostały na Listę Dziedzictwa Zagrożonego UNESCO.

Najcenniejszymi dziełami sztuki, utraconymi z perspektywy Polski, o których grabieży wiemy, była tzw. Wielka Trójka z kolekcji Czartoryskich: *Portret młodzieńca* Rafaela Santiego (do dzisiaj nieodnaleziony), *Portret damy z gronostajem* (zwyczajowo *Dama z łasiczką*, rzadziej *Dama z gronostajem*) Leonarda da Vinci oraz *Krajobraz z miłosiernym Samarytaninem* Rembrandta van Rijna. Skomplikowane losy tych trzech dzieł sztuki, wycenianych na niebagatelne kwoty, były związane ze zorganizowaną polityką III Rzeszy. Dzieło Rafaela miało wzbogacić planowane przez Adolfa Hitlera muzeum sztuki w Linzu, ale w wyniku działań Hansa Franka trafiło na Wawel i prawdopodobnie zaginęło podczas ewakuacji Niemców z Generalnego Gubernatorstwa. *Portret młodzieńca* do dzisiaj jest najbardziej poszukiwanym dziełem sztuki utraconym w wyniku II wojny światowej.

Przewrotna jest natomiast historia związana z grabieżą dzieł sztuki przez Szwedów. Można powiedzieć, że dzięki Szwedom właśnie udało się ustalić miejsce pochówku Mikołaja Kopernika. Do 2004 r. uważano, że Kopernik co prawda spoczywa na terenie katedry we Fromborku, jednak nie było znane dokładne umiejscowienie jego zwłok. Wieloletnie, zainicjowane już na początku XIX w. poszukiwania, natrafiały na kolejne trudności. Momentem przełomowym było pozyskanie materiału DNA z jednej z ksiąg należących do astronoma, a znajdującej się od potopu szwedzkiego w bibliotece uniwersyteckiej w Uppsali. Badania genetyczne i ich potwierdzenie doprowadziły do uwierzytelnienia potencjalnego dotychczas miejsca pochówku Kopernika w 2008 r.

Ważnym problemem grabieży dóbr kultury są dzisiaj również kradzieże, w tym szczególnie dzieł sztuki, niezwiązane z konfliktami zbrojnymi. Najbardziej rozpoznawalnym dziełem, które kiedykolwiek zostało ukradzione, była bezcenna *Mona Lisa* Leonarda da Vinci. Kradzież tego arcydzieła była wyjątkowa dlatego, że nikt jej się nie spodziewał. Obraz został ukradziony przez pracownika Luwru w 1911 r., a 2 lata później przypadkowo odnaleziony. Innym wartym przypomnienia rabunkiem była kradzież obrazów z Muzeum im. Isabelli Stewart Gardner w Bostonie w 1990 r. Złodzieje, przebierając się za policjantów, wynieśli 13 obrazów, w tym *Koncert* Jana Vermeera, *Burzę na jeziorze galilejskim* Rembrandta van Rijna, 2 inne prace tego malarza, 4 obrazy Edgara Degasa i 1 Édouarda Maneta. Do dzisiaj odzyskano tylko 1 z obrazów Rembrandta, jego autoportret.

Uwzględniając konwencje i istniejące rekomendacje UNESCO oraz rozstrzygnięcia prawne dotyczące pewnych aspektów ochrony dóbr kultury, społeczność międzynarodowa posiada narzędzia ochrony zabytków materialnych (i niematerialnych). Polskie prawo również reguluje te potrzeby obowiązującą ustawą z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami.

Polska bierze też udział w różnych inicjatywach mających na celu przeciwdziałanie zawłaszczaniu dzieł sztuki oraz odzyskiwanie utraconych lub nielegalnie sprzedawanych dzieł sztuki. Flagową akcją międzynarodową, w którą zaangażowane były siły wielu krajów, w tym → E u r o p o l, → I n t e r p o l, UNESCO, Światowa Organizacja Celna, była Akcja Pandora, przeprowadzana już kilkukrotnie. Także Polska brała w niej udział po raz kolejny (Pandora IV). Przygotowaniem akcji, a także jej realizacją zajęło się Biuro Kryminalne Komendy Głównej Policji. Funkcjonuje w nim punkt kontaktowy nieformalnej Sieci ds. Przestępczości przeciwko Dobrom Kultury EU CULTNET. Wszystkie działania prowadzone były we współpracy z komendami wojewódzkimi oraz Komendą Stołeczną Policji, a także koordynatorem ds. zwalczania → p r z e s t ę p c z o ś c i [t. 3] przeciwko zabytkom w CBŚP.

Katarzyna Pabis-Cisowska

J. Gąssowski, *Jak odkryto grób Mikołaja Kopernika*, 3.01.2019, Rp.pl (dostęp 6.02.2020); M. Kuhnke, *Przyczynek do historii wojennych grabieży dzieł sztuki*

w Polsce, Zabytki.pl (dostęp 6.02.2020); A. Mężyński, *Straty polskich dóbr kultury w czasie II wojny światowej*, 2014, DzielaUtracone.gov.pl (dostęp 6.02.2020); MKiDN, *Obiekty utracone w wyniku wojny*, gov.pl (dostęp 6.02.2020); E.J. Osmańczyk, *Encyklopedia ONZ i stosunków międzynarodowych*, Wiedza Powszechna, Warszawa 1986; *Prawo ochrony zabytków*, K. Zajdler (red.), Wolters Kluwer Polska, Wydawnictwo Uniwersytetu Gdańskiego, Warszawa–Gdańsk 2014; Rezolucja Parlamentu Europejskiego z dnia 17 stycznia 2019 r. w sprawie transgranicznych roszczeń o zwrot dzieł sztuki i dóbr kultury zagrabionych podczas konfliktów zbrojnych i wojen (2017/2023(INI)); M. Romanowska-Zadrożna, *Grabieże szwedzkie w Polsce (1). Przyczyny, charakterystyka i skutki*, „Cenne, Bezcenne / Utracone" 2005, nr 3; E. Wiedemann, *Spór o dzieła sztuki*, „Tygodnik Forum" 2007, nr 35; K. Zalasińska, *Konwencja UNESCO z roku 1970*, „Cenne, Bezcenne / Utracone" 2015, nr 1–2; A. Zieliński, *Pierwsze stulecie Polski. Państwo – władcy – sensacje*, Bellona, Warszawa 2012.

GRUPA BILDERBERG lub klub Bilderberg, forum Bilderberg – to coroczne i nieformalne spotkanie ok. 130 najbardziej wpływowych ludzi na świecie, głównie Amerykanów i Europejczyków, najwyższej rangi polityków (premierów, ministrów, przedstawicieli monarchii), członków zarządów wielkich instytucji międzynarodowych, znaczących fundacji, banków i korporacji o globalnym zasięgu i wpływie. Podczas spotkań omawiane są najważniejsze w danym czasie dla świata sprawy dotyczące →bezpieczeństwa [t. 1], polityki i gospodarki. Grupa Bilderberg utrzymuje bliskie kontakty także z europejską arystokracją, nie wyłączając brytyjskiej rodziny królewskiej czy członków domów panujących Szwecji, Holandii i Hiszpanii.

Spotkania Bilderberg to nieformalne zebrania wpływowych osób z biznesu, polityki, wojska, mediów, uczelni i →służb specjalnych [t. 4], gdzie są wymieniane pomysły na temat aktualnych problemów politycznych, gospodarczych i społecznych. Udział w dorocznej konferencji zależy od zaproszenia przewodniczącego i 2 honorowych sekretarzy generalnych, które jest udzielane po otrzymaniu zalecenia komitetu sterującego. Po ogłoszeniu oficjalnych organizatorów uczestnicy zostają wybrani w taki sposób, aby zapewnić „dobrze poinformowaną, zrównoważoną dyskusję" na temat określonych punktów porządku obrad. Językiem biznesowym jest angielski.

W Klubie Bilderberg nie ma statusu członka ani umowy założycielskiej. Punkty porządku obrad i listy uczestników zostają udostępniane międzynarodowym agencjom prasowym dopiero po spotkaniach. Ich uczestnicy są zobowiązani do całkowitej dyskrecji. Niektórzy grupę określają jako ponadnarodową organizację próbującą tworzyć rząd światowy. Wokół klubu narosło wiele mitów.

Ta ściśle tajna organizacja została oficjalnie powołana w maju 1954 r., po nieformalnych spotkaniach członków elit europejskich w latach 40. XX w. Podczas II wojny światowej były polski dyplomata J. Retinger, jako doradca polskiego rządu na uchodźstwie, organizował w Londynie spotkania przedstawicieli rządu na uchodźstwie z ministrami spraw zagranicznych krajów europejskich. Na tych konferencjach, które odbyły się między październikiem 1942 r. a sierpniem 1944 r., narodziła się powojenna umowa celna między krajami Beneluksu.

W latach 50. XX w. Retinger i A. Nielsen, zaniepokojeni wzrostem antyamerykanizmu w Europie Zachodniej spowodowanego przez plan Marshalla, postanowili zgromadzić przywódców Europy i Ameryki Północnej w celu promowania porozumienia między nimi oraz wspierania współpracy w dziedzinie polityki, gospodarki i obrony. H. Védrine, były francuski minister spraw zagranicznych, podkreślał, że w tym czasie celem było przekonanie europejskich i amerykańskich przywódców do zacieśnienia więzi i nieobniżenia czujności wobec potężnego Związku Radzieckiego. Wśród gości byli holenderski książę Bernhard, który postanowił promować ten pomysł, D. Rockefeller, który sfinansował spotkanie, oraz premier Belgii P. van Zeeland.

Retinger zwrócił się do księcia Bernharda, który zgodził się promować tę ideę wraz z byłym premierem Belgii P. van Zeelandem i ówczesnym szefem Unileveru, P. Rijkensem. Ze swojej strony książę skontaktował się z gen. W.B. Smithem, ówczesnym dyrektorem CIA, który poprosił doradcę Eisenhowera, C.D. Jacksona, o zbadanie propozycji. Lista gości miała zostać sporządzona poprzez zaproszenie po 2 uczestników z każdego państwa, reprezentujących konserwatywne i liberalne punkty widzenia.

W rezultacie ruch europejski otrzymał znaczny wkład finansowy zarówno od rządu USA oraz CIA, jak i ze źródeł prywatnych za pośrednictwem Amerykańskiego Komitetu ds. Zjednoczonej Europy (American

Committee on United Europe, ACUE) i innych instytucji. W 1952 r. Retinger zrezygnował z funkcji sekretarza generalnego Ruchu Europejskiego i zaczął promować nieoficjalne i poufne spotkania polityków europejskich i amerykańskich oraz liderów biznesu. W szczególności rozmowy te powinny były usunąć narastające napięcia między państwami europejskimi a Stanami Zjednoczonymi. Retinger, po konsultacji z P. van Zeelandem i innymi przedstawicielami rządów europejskich, opracował plany konferencji cyklicznej. Dzięki pozycji Bernharda i powiązaniom Retingera szybko znaleziono 10 osób:

- M. Brauer (burmistrz Hamburga, Niemcy);
- H. Gaitskell (poseł do parlamentu, Wielka Brytania);
- A. de Gasperi (premier, Włochy);
- C. Gubbins (gen. dyw., Wielka Brytania);
- O. Bjørn Kraft (minister spraw zagranicznych, Dania);
- G. Mollet (poseł do parlamentu, Francja);
- R. Mueller (prezes Towarzystwa Polityki Gospodarczej (WiPoG), prawnik, Niemcy);
- A. Pinay (premier, Francja);
- P. Pipinelis (były minister spraw zagranicznych, Grecja);
- P. Quaroni (ambasador Włoch we Francji).

Zastrzeżenia państw europejskich wobec USA zostały omówione na pierwszej konferencji europejskiej grupy podstawowej 25 września 1952 r.

Niemniej jednak dopiero w 1954 r. udało się rozstrzygnąć wszystkie kwestie organizacyjne i 28 maja członkowie grupy spotkali się w pałacu Soestdijk w Holandii. Pierwsza konferencja w hotelu de Bilderberg została otwarta przez księcia Bernharda. W programie spotkania omówiono stanowiska w sprawie „komunizmu i Związku Radzieckiego", „kolonii i ich populacji", „polityki gospodarczej i ich problemów" oraz „integracji europejskiej i europejskiej wspólnoty obronnej". Nie chodziło o rozwiązywanie kwestii, ale o wymianę poglądów dotyczących tych zagadnień.

Retinger podkreślił na pierwszym spotkaniu, że uczestnicy powinni być otwarci, nie mieć oczywistych przekonań narodowych, dzielić zachodnie wartości kulturowe i etyczne, aby osiągnąć cel, jakim jest dotarcie do jak największej liczby osób z różnych środowisk. Poszukiwana jest równowaga dla odpowiedniego składu każdego spotkania, która odzwierciedla

w możliwie największym stopniu dominującą opinię danego kraju na dany temat.

50 delegatów z 11 krajów Europy Zachodniej wzięło udział w pierwszej konferencji wraz z 11 Amerykanami. Wtedy zostały określone cele i misja Klubu Bilderberg:

> Intencją przyświecającą każdemu spotkaniu grupy Bilderberg jest stworzenie „arystokracji woli" łączącej Europę i Stany Zjednoczone, a także uzgodnienie polityki, spraw gospodarczych i strategii we wspólnym rządzeniu światem.

Sukces spotkania zachęcił organizatorów do przygotowywania corocznej konferencji. Utworzono stały komitet sterujący, a Retinger został mianowany jego stałym sekretarzem. Podczas organizowania konferencji komitet prowadził również rejestr nazwisk uczestników i danych kontaktowych w celu stworzenia nieformalnej sieci osób, które można byłoby zapraszać osobno. Zadaniem grupy było „zawiązanie węzła wokół wspólnej linii politycznej między Stanami Zjednoczonymi a Europą w opozycji do Rosji i komunizmu". Holenderski ekonomista E. van der Beugel zastąpił Retingera na stanowisku w 1960 r. po jego śmierci. Książę Bernhard był przewodniczącym spotkania do swojej śmierci w 2004 r. Konferencje przez kolejne 3 lata od 1954 r. odbyły się we Francji, Niemczech i Danii. W 1957 r. odbyła się pierwsza amerykańska konferencja na wyspie St. Simons w stanie Georgia.

Grupa bierze nazwę od hotelu Bilderberg, który znajduje się w Holandii w miejscowości Oosterbeek, w którym odbyło się pierwsze spotkanie pod przewodnictwem holenderskiego księcia Bernharda. Spotkania grupy są skierowane na wzmocnienie konsensusu dot. wolnego rynku zachodniego i jego interesów na całym świecie. Uczestnikami są przywódcy polityczni, eksperci z przemysłu, finansów, środowisk akademickich i mediów. Uczestnicy są uprawnieni do korzystania z →informacji uzyskanych na spotkaniach, ale nie mogą przypisywać ich nazwanemu mówcy. Ma to na celu zachęcenie do szczerej debaty przy jednoczesnym zachowaniu prywatności, co podsyca →teorie spiskowe [t. 4] zarówno z lewej, jak i prawej strony.

Jak wynika ze „ściśle tajnych" notatek z pierwszego spotkania grupy Bilderberg, doszła ona do wniosku, że do tej pory poświęcono zbyt mało uwagi długofalowemu planowaniu i budowaniu międzynarodowego porządku, który wykraczałby poza →kryzys związany z →zimną wojną [t. 4].

W 1956 r. powołano także ośmioosobowy komitet sterujący. Członkowie komitetu mogą uczestniczyć w dowolnej konferencji lub spotkaniu. Członkowie są powoływani przez przewodniczącego konferencji, a po konsultacji z tymi członkami uczestnicy są wybierani na nadchodzącym spotkaniu. Pomiędzy dorocznymi dużymi konferencjami Bilderberg dalsze spotkania komitetu sterującego odbywają się tylko przy ważnych okazjach. Komitet zawsze ma 2 członków z Niemiec, z których jeden jest odpowiedzialny za finanse, a drugi za wybór tematów i mówców.

W artykule opublikowanym 6 maja 1975 r. w „Lombardzie", stałej rubryce pisma „Financial Times", dziennikarz C.G. Tether ostro skrytykował działania grupy, podkreślając, że zachowuje się zupełnie tak, jakby była jakimś spiskiem – nawet jeżeli nim nie jest.

Holenderski książę Bernhard, który był współzałożycielem grupy Bilderberg, wyraził nadzieję, że można uniknąć poważnych perturbacji gospodarczych, takich jak Wielki Kryzys, jeśli odpowiedzialni i wpływowi przywódcy będą mogli zarządzać światowymi wydarzeniami. W podobnym tonie wyraził się inny architekt elitarnego klubu – brytyjski poseł Partii Pracy D. Healey: „Bilderberg to najbardziej przydatna międzynarodowa grupa, w której kiedykolwiek uczestniczyłem. Poufność pozwoliła mówić nam uczciwie bez obawy o konsekwencje".

Członkowie grupy spotykają się zwykle raz w roku w luksusowych hotelach lub kurortach w różnych częściach świata, zwykle w Europie, a raz na cztery lata w Stanach Zjednoczonych lub Kanadzie, a ich poczynania okrywa całkowita tajemnica, mimo że uczestniczą w nich przedstawiciele czołowych mediów amerykańskich. Hotele konferencyjne są zazwyczaj zamknięte dla innych gości na czas konferencji Bilderberg. Chociaż grupa twierdzi, że wymienia tylko nieformalne poglądy na temat spraw światowych, są dowody na to, że jej zalecenia często stają się oficjalną polityką. Centralne biuro znajduje się w Leiden (Holandia), co roku decyduje ono, w którym kraju odbędzie się nadchodzące spotkanie. Kraj goszczący musi

następnie zarezerwować cały hotel na 4 dni, a także zorganizować wyżywienie, transport i ochronę. Aby to sfinansować, gospodarz prosi o datki od korporacji, takich jak Barclays, Fiat Automobiles, GlaxoSmithKline, Heinz, Nokia i Xerox.

Spotkania klubu odbywają się w całkowitej tajemnicy, ze specjalnymi zaproszeniami, daty ich zwołania nie są ogłaszane w prasie. Każde spotkanie grupy jest bardzo interesujące dla społeczności światowej. Niemożliwe jest ukrycie przybycia do jednego miejsca dużej liczby znanych osób, w tym prezydentów, królów, książąt, kanclerzy, premierów, ambasadorów, bankierów, dyrektorów dużych korporacji. Bezpieczeństwo spotkania zapewnia → p o l i c j a [t. 3] i służby specjalne kraju, w którym spotkanie się odbywa. Rozważane kwestie i podejmowane decyzje są utrzymywane w tajemnicy. Ze względu na nieformalny charakter spotkania nie można podejmować żadnych wiążących prawnie decyzji. Dyskusje mają na celu osiągnięcie konsensusu w rozmaitych sprawach. Spotkań grupy nie można nagrywać, zabronione jest składanie oświadczeń prasowych lub omawianie dyskusji odbywających się na tych spotkaniach.

Konferencja Bilderberg jest organizowana co roku w maju lub czerwcu przez stały komitet sterujący, w skład którego wchodzi po 2 członków z ok. 18 różnych krajów. W klubie funkcjonują stanowiska przewodniczącego komitetu sterującego i honorowego sekretarza generalnego. Oprócz komitetu istnieje osobna grupa doradcza z pokrywającym się członkostwem oraz grupa organów nadzoru. Przewodniczący komitetu sterującego jest odpowiedzialny za zarządzanie konferencjami grupy. Od 1954 do 1976 r. tę funkcję sprawował książę Bernhard. W 1976 r. zastąpił go były premier Wielkiej Brytanii A. Douglas-Home. Obecnie przewodniczącym jest H. de Castries.

Każda konferencja trwa od 2 do 3 dni, w miejscu wskazywanym zaproszonym gościom na krótko przedtem. Zaproszeni uczestnicy nie mogą opuścić hotelu w trakcie konferencji i nie może im towarzyszyć małżonek lub sekretarz. Wszyscy członkowie klubu zasiadają w kolejności alfabetycznej. Do lat 80. XX w. angielski i francuski były dwoma oficjalnymi językami spotkań grupy, później używano tylko języka angielskiego. Klub liczy 383 osób, z czego 128 to Amerykanie, reszta to Europejczycy i Azjaci (Japończycy, Koreańczycy, Singapurczycy, Tajwańczycy i Hongkończycy).

Co roku do udziału w spotkaniu zaproszonych jest ok. 130 liderów politycznych i ekspertów.

Na konferencjach grupy przede wszystkim omawiane są kwestie gospodarki światowej i stosunków międzynarodowych. Rozmowy nie prowadzą do ostatecznej deklaracji, a konkluzje nie są publikowane. Po każdej konferencji każdy uczestnik i wszyscy, którzy wcześniej uczestniczyli w konferencji, otrzymują protokół ze spotkania. Protokoły te są jedynie streszczeniami obrad, w których dane oświadczenia nigdy nie są przypisywane do konkretnego uczestnika, ale zawsze tylko do kraju jego pochodzenia. Od 1963 r. uczestnicy otrzymują również tekst wyjaśniający. Wszystkie dokumenty są poufne.

W latach 1954–2019 odbyło się ponad 60 konferencji. Do 1957 r. odbywały się 2 spotkania każdego roku, później zaś jedno rocznie. Od 1954 r. w konferencji wzięło udział ok. 2,5 tys. osób z 28 krajów i 15 organizacji międzynarodowych. Kobiety brały również udział w tych wydarzeniach od 1972 r. Wszyscy uczestnicy biorą udział w konferencjach wyłącznie jako osoby prywatne, a nie na oficjalnym stanowisku, chociaż ich pozycja w życiu publicznym może odgrywać decydującą rolę. Od samego początku wśród uczestników były brytyjskie, belgijskie i holenderskie rodziny królewskie, bankierzy oraz polityczni i wojskowi strategowie NATO. Najbardziej aktywnymi uczestnikami byli G. Agnelli (Fiat) i D. Rockefeller (Chase Manhattan Bank), którzy byli obecni na ok. 20 konferencjach Bilderberg, a także należeli do grupy doradczej. Były sekretarz stanu USA H. Kissinger również cieszy się silną pozycją na spotkaniach. Do połowy lat 60. XX w. spotkania grupy były w dużej mierze nieznane na całym świecie.

Wydatki na spotkania grupy są w całości pokrywane z prywatnych datków; członkowie komitetu sterującego, którzy pochodzą z kraju, w którym odbywa się konferencja, są odpowiedzialni za finansowanie kosztów przyjęcia poszczególnych uczestników konferencji. Na konferencji w Szwajcarii w 2011 r. organizator i rząd federalny podzieliły się kosztami szeroko zakrojonych środków bezpieczeństwa. Uczestnicy ponoszą koszty podróży na konferencję.

Częściowo z powodu metod pracy zapewniających ścisłą prywatność i poufność grupa została skrytykowana za brak przejrzystości i odpowiedzialności. Nieujawniony charakter postępowania doprowadził do

powstania kilku teorii spiskowych. Grupa jest oskarżana o spiskowanie w celu narzucenia światowego rządu, rządów kapitalistycznych i/lub planowanej gospodarki. Ta lista wpływowych na całym świecie postaci wzbudziła zainteresowanie międzynarodowej sieci spiskowców, którzy od dziesięcioleci postrzegają grupę jako program globalistyczno-korporacyjny i są przekonani, że potężna elita prowadzi planetę w kierunku nowego porządku świata (łac. *Novus Ordo Mundi*, ang. *New World Order*).

We wrześniu 2005 r., pragnąc odeprzeć oskarżenia o konspiracje, 73-letni przewodniczący grupy Bilderberg wicehrabia É. Davingon udzielił wywiadu B. Haytonowi z BBC. Przedstawił w nim cel „prywatnych" spotkań grupy: „Moim zdaniem jest to forum, na którym ludzie, którzy mają wpływy, mogą swobodnie porozmawiać z innymi wpływowymi osobami i rozważyć dzielące ich różnice bez niepotrzebnego krytycyzmu i publicznej debaty na temat ich poglądów". Davignon zaprzeczył, jakoby grupa zamierzała utworzyć światową klasę rządzącą, „nie sądzę, by taka klasa istniała" – mówił. Powiedział natomiast, że „biznes wpływa na społeczeństwo, podobnie jak polityka – tak podpowiada rozsądek. Nie jest tak, że biznes odbiera prawo do rządzenia demokratycznie wybranym przywódcom".

W 2001 r. D. Healey, założyciel grupy Bilderberg i członek komitetu sterującego przez 30 lat, powiedział, że stwierdzenie o dążeniu do stworzenia rządu światowego jest przesadzone, ale nie całkowicie niesprawiedliwe. Według byłego ambasadora USA w Berlinie, członka tego stowarzyszenia, J. McGhee, konferencje Bilderberg odegrały „ważną rolę" w opracowywaniu traktatów rzymskich dotyczących ustanowienia Europejskiej Wspólnoty Gospodarczej. J. Sheinken, prezes Amalgamated Bank i członek grupy Bilderberg, oświadczył w 1996 r.:

> W niektórych przypadkach dyskusje rzeczywiście znajdują odbicie w polityce. Projekt wspólnej waluty europejskiej był dyskutowany kilka lat wcześniej, zanim stał się celem politycznym. Dyskutowaliśmy o nawiązaniu przez USA oficjalnych stosunków z Chinami, zanim Nixon rzeczywiście je nawiązał.

Regulamin spotkania grupy pozwala uczestnikom na wykorzystanie wszelkich informacji uzyskanych podczas konferencji, ale bez ujawniania

nazwisk mówców lub innych uczestników. Według byłej przewodniczącej É. Davignon w 2011 r. główną atrakcją spotkań grupy jest to, że stwarzają one możliwość debaty oraz dowiedzenia się, co tak naprawdę sądzą najważniejsze osoby, bez ryzyka, że komentarze trafią do mediów. W komunikacie prasowym *American Friends of Bilderberg* z 2008 r. stwierdzono, że „jedyną działalnością Bilderberg jest coroczna konferencja i że na spotkaniach nie proponowano żadnych rezolucji, nie podjęto głosów ani nie wydano oświadczeń politycznych". Jednak w listopadzie 2009 r. grupa zorganizowała spotkanie obiadowe w zamku Val-Duchesse w Brukseli przed doroczną konferencją w celu promowania kandydatury H. Van Rompuya na przewodniczącego Rady Europejskiej.

Grupa Bilderberg stała się przedmiotem badań w latach 1979–1980. W tekście *The Bilderberg and the West*, opublikowanym w 1980 r., P. Thompson wyjaśnia, że doroczne forum Bilderberg to spotkanie liderów najważniejszych międzynarodowych korporacji z kluczowymi postaciami politycznymi krajów zachodnich w celu wspólnego omówienia głównych problemów międzynarodowych.

W 2003 r. w odpowiedzi na pytanie parlamentarne Szwajcarska Rada Federalna stwierdziła:

> Konferencje Bilderberg to forum wymiany głównych aktualnych tematów w najróżniejszych dziedzinach między członkami rządów, dyplomatami, politykami, osobistościami gospodarki, przedstawicielami nauki, prasy i wyspecjalizowanych instytutów. […] Celem tej prywatnej konferencji jest bezpłatna i otwarta dyskusja. Uczestnicy bronią swoich osobistych opinii i nie zabierają głosu w imieniu swojego rządu lub pracodawcy. Z tego powodu organizatorzy powstrzymują się od reklamy wokół tych dyskusji. […] Uczestnicy, którzy przyjmą osobiste zaproszenie na konferencję, deklarują gotowość rezygnacji z wszelkiej reklamy. Poza tym nie chodzi o negocjacje.

Spotkania odbywają się zgodnie z regułą Chatham House. Zasada ta zezwala na podanie do publicznej wiadomości informacji z sekretnych spotkań i niejawnych debat, jednak pod warunkiem zachowania

w tajemnicy tożsamości uczestników zebrania. Reguła ta obowiązuje z pewnymi modyfikacjami od 1927 r. w angielskiej instytucji Chatham House. Tajne są dane osobowe oraz formalne związki i afiliacje tak mówców, jak i pozostałych uczestników. Uczestnicy mogą swobodnie korzystać z otrzymanych informacji, ale ani tożsamość, ani przynależność mówcy, ani żadnego innego uczestnika nie może zostać ujawniona. Dzięki prywatnemu charakterowi spotkań uczestnicy biorą w udział jako osoby indywidualne, a nie w charakterze urzędowym, zatem nie są związani konwencjami ich urzędu ani wcześniej ustalonymi stanowiskami. W związku z tym mogą poświęcić czas na słuchanie, refleksję i gromadzenie spostrzeżeń. Nie ma szczegółowego porządku obrad, nie proponuje się żadnych rezolucji, nie podejmuje się głosowań ani nie wydaje się żadnych oświadczeń dotyczących polityki.

Ostatnie spotkanie Bilderberg odbyło się w dniach 30 maja – 2 czerwca 2019 r. w szwajcarskim hotelu Montreux Palace nad Jeziorem Genewskim, uczestniczyli w nim przedstawiciele 23 krajów. Ważnymi uczestnikami szczytu grupy Bilderberg byli: przewodniczący Światowego Forum Ekonomicznego B. Brende, premier Holandii M. Rutte, były premier Włoch M. Renzi, minister obrony Niemiec U. von der Leyen, były sekretarz stanu USA H. Kissinger, szef koncernu Axel Springer M. Dopfner, prezes Banku Anglii M. Carney, były dyrektor CIA D. Petraeus i doradca Białego Domu J. Kushner, zięć D. Trumpa. Obecny był również szef Google J. Cohen, a także prezes Ryanair M. O'Leary. Polaków reprezentowali były szef MSZ R. Sikorski, prezydent Warszawy R. Trzaskowski i dziennikarka TVN J. Pieńkowska – żona bankiera-milionera L. Czarneckiego. W poprzednich latach Polskę reprezentowali m.in. J. Rostowski, A. Olechowski, A. Kwaśniewski, H. Suchocka oraz żona Sikorskiego A. Applebaum.

Na oficjalnej stronie grupy Bilderberg wymieniono 11 kluczowych tematów, które zostały poruszone w 2019 r., wśród nich są m.in.: stabilny porządek strategiczny, przyszłość Europy, zmiany klimatyczne i → z r ó w n o w a ż o n y r o z w ó j [t. 4], Chiny, Rosja, przyszłość kapitalizmu, brexit, etyka → s z t u c z n e j i n t e l i g e n c j i [t. 4] i rola → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3] w → w o j n i e h y b r y d o w e j [t. 4]. Przedstawiciele mediów nie byli zapraszani, przebieg i efekty szczytu nie były relacjonowane.

Przez lata spotkania stały się forum dyskusji na szeroki zakres tematów – od handlu przez miejsca pracy po technologię, od polityki pieniężnej po inwestycje i od wyzwań ekologicznych po zadanie promowania → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o [t. 1]. W kontekście zglobalizowanego świata trudno jest odszukać jakąkolwiek kwestię związaną z Europą lub Ameryką Północną, którą można by rozwiązać jednostronnie.

Olga Wasiuta

V. Aubourg, *Organizing Atlanticism: The Bilderberg Group and the Atlantic Institute, 1952–1963*, „Intelligence and National Security" 2003, vol. 18, no. 2; BilderbergMeetings.org (dostęp 12.02.2020); M. Biskupski, *War and Diplomacy in East and West: A Biography of Józef Retinger*, Routledge, London–New York 2017; *Dziennikarka TVN, były szef MSZ. Kto weźmie udział w spotkaniu tajemniczej grupy Bilderberg?*, 29.05.2019, DoRzeczy.pl (dostęp 12.02.2020); R. Eringer, *The Global Manipulators*, Pentacle Books, Bristol 1980; D. Estulin, *The True Story of the Bilderberg Group*, Trine Day, Oregon 2007; T. Gijswijt, *Informal Alliance. The Bilderberg Group and Transatlantic Relations During the Cold War, 1952–1968*, Routledge, London–New York 2019; A. Hatch, *H.R.H. Prince Bernhard of the Netherlands: An Authorized Biography*, London 1962; Ch. Hodapp, A. Von Kannon, *Conspiracy Theories & Secret Societies For Dummies*, John Wiley, Hoboken 2008; L. Kantor, *Bilderberg Group and Transnational Capitalist Class: Recent Trends in Global Elite Club as Vindication of neo-Marxism*, „Critique: Journal of Socialist Theory" 2017, vol. 45, no. 1–2; S. Klimczuk, G. Warner, *Secret Places, Hidden Sanctuaries: Uncovering Mysterious Sites, Symbols and Societies*, Sterling, New York–London, 2010; I. Richardson, A. Kakabadse, N. Kakabadse, *Bilderberg People. Elite Power and Consensus in World Affairs*, Routledge, London 2011; J. Ronson, *THEM: Adventures with Extremists*, Picador, London 2001; *Spotkanie grupy Bilderberg. Z Polski pojawią się m.in. Rafał Trzaskowski i Radosław Sikorski*, 29.05.2019, TVP.info (dostęp 12.02.2020); H. Wilford, *CIA Plot, Socialist Conspiracy, or New World Order? The Origins of the Bilderberg Group, 1952–55*, „Diplomacy & Statecraft" 2003, vol. 14, no. 3; B. Zalewski, *Grupa Bilderberg w wielkiej tajemnicy radzi w Szwajcarii nad losami świata*, 29.05.2019, RMF24.pl (dostęp 12.02.2020).

GRUPA WYSZEHRADZKA (określana także jako Wyszehradzka Czwórka lub V4) – organizacja regionalna skupiająca państwa Europy Środkowej: Polskę, Czechy, Węgry i Słowację. Nazwa pochodzi od miasta Wyszehrad położonego w północnej części Węgier, w którym to w 1335 r. królowie

Czech, Węgier i Polski spotkali się, by uzgodnić współpracę między swoimi królestwami w dziedzinie polityki oraz handlu. Pamiętając o tym wydarzeniu 656 lat później, w lutym 1991 r. prezydenci Czechosłowacji, Polski i Węgier w tym samym mieście zainicjowali współpracę, którą nazwano wówczas Trójkątem Wyszehradzkim. Działania państw regionu koncentrowały się na współpracy w ramach integracji ogólnoeuropejskiej.

Sama idea polsko-czesko-słowacko-węgierskiej współpracy regionalnej wysunięta została przez prezydenta Czech V. Havla w trakcie jego wystąpienia w Sejmie RP w styczniu 1990 r. Powołanie trójkąta poprzedziły 3 szczyty przedstawicieli państw: 9 kwietnia 1990 r. w Bratysławie, potem w Budapeszcie, a następnie w dniach 12–15 lutego 1991 r. w Wyszehradzie. Na jego zakończenie podpisana została Deklaracja o współpracy Czeskiej i Słowackiej Republiki Federacyjnej, Rzeczypospolitej Polskiej i Republiki Węgierskiej w dążeniu do integracji europejskiej, w której stwierdzono, że zbieżność celów w polityce zagranicznej, podobieństwo doświadczeń historycznych oraz bliskość geograficzna predestynują tę trójkę państw do powołania nowego związku regionalnego, jak też zdefiniowano główne cele współpracy, wśród których nadrzędnym była integracja ze strukturami euroatlantyckimi. Zaakcentowano wspólne dążenie do pełnego przywrócenia niezależności państwowej, demokracji i wolności w krajach Trójkąta Wyszehradzkiego. Kolejne szczyty przedstawicieli państw odbyły się w Krakowie w czerwcu i październiku 1991 r., a ich konsekwencjami było przyjęcie Deklaracji Krakowskiej, w której ustalono, że współpraca trójkąta obejmie strefy takie jak polityka zagraniczna, gospodarka, transport, ochrona środowiska i nauka. Na czwartym szczycie przedstawicieli państw trójkąta w Pradze w dniach 5–6 maja 1992 r. zdecydowano, że 3 państwa nadal będą koordynować swoje działania integracyjne z Europą i wspólnie złożą wniosek o przyjęcie do EWG.

Od 1993 r. mówić można o nieznacznym spadku dynamiki współpracy państw Trójkąta Wyszehradzkiego z uwagi na podział Czechosłowacji, który dokonał się z dniem 1 stycznia 1993 r. oraz zapowiedź indywidualnego rozpatrywania kandydatur do pełnego członkostwa w strukturach europejskich. Czechy przyjęły też → s t r a t e g i ę [t. 4] wzmocnienia indywidualnych starań o szybsze przyjęcie do Unii Europejskiej i → N A T O [t. 3], kosztem współpracy w ramach Grupy Wyszehradzkiej. W latach 1993–1998

spotkania grupy odbywały się nieregularnie i nie wychodzono w nich poza sferę deklaracji, co było konsekwencją koncentracji wysiłków każdego z państw na integracji euroatlantyckiej.

Kolejny szczyt wyszehradzki odbył się dopiero w 1998 r. w Budapeszcie, gdzie spotkali się premierzy Czech, Polski i Węgier, jednak bez udziału premiera Słowacji, gdzie w końcu odbyły się wybory parlamentarne i został wyłoniony nowy premier. Zebrani szefowie rządów wyrazili przekonanie o potrzebie rewitalizacji Grupy Wyszehradzkiej, w duchu deklaracji założycielskiej z 1991 r. 12 marca 1999 r. Polska, Czechy i Węgry stały się stronami traktatu waszyngtońskiego: w rocznicowym szczycie NATO w dniach 23–25 kwietnia 1999 r. w Waszyngtonie brały już udział jako pełnoprawni członkowie Sojuszu, zaś 31 marca 1998 r. rozpoczęły negocjacje państw Grupy Wyszehradzkiej ws. członkostwa w UE.

W dniach 11–12 marca 2004 r. w Koszycach spotkali się prezydenci państw V4, a 1 maja 2004 r. Czechy, Polska, Słowacja i Węgry stały się członkami UE. Po przystąpieniu do UE państwa Grupy Wyszehradzkiej podpisały 12 maja 2004 r. w Kromieryżu deklarację w sprawie współpracy, w której stwierdzono, że „kluczowe cele zawarte w Deklaracji Wyszehradzkiej z 1991 r. zostały osiągnięte", oraz podkreślono „determinację do dalszego rozwoju współpracy państw Grupy Wyszehradzkiej, jako państw członkowskich Unii Europejskiej i NATO." Ponadto państwa V4 zadeklarowały, że

> postrzegają swoje przystąpienie do Unii Europejskiej i NATO jako ważny krok w kierunku ponownego zjednoczenia Europy oraz jako historyczny kamień milowy na drodze ich demokratycznych przemian, działań na rzecz integracji i wzajemnej współpracy. Integracja krajów Grupy Wyszehradzkiej w ramach europejskich i euroatlantyckich struktur otwiera nowe możliwości i stawia nowe wyzwania dla ich dalszej współpracy w kwestiach będących przedmiotem ich wspólnego zainteresowania.

W kolejnych latach kontynuowano spotkania państw grupy, podejmując także próby poszerzenia współpracy o nowe sfery, takie jak obronność i →bezpieczeństwo energetyczne [t. 1].

Współpracy wyszehradzkiej nie nadano kształtu ani charakteru organizacji międzynarodowej, lecz pozostano przy formie regularnych konsultacji i współpracy, która wg deklaracji powinna przebiegać w szczególności w obszarach:

- kultury,
- szkolnictwa,
- wymiany młodzieży,
- nauki,
- dalszego umacniania obywatelskiego wymiaru współpracy wyszehradzkiej w ramach Międzynarodowego Funduszu Wyszehradzkiego i jego struktur,
- współpracy transgranicznej,
- infrastruktury,
- środowiska,
- zwalczania →terroryzmu [t. 4], →przestępczości zorganizowanej [t. 3] i nielegalnej migracji,
- współpracy w ramach strefy Schengen,
- →zarządzania kryzysowego [t. 4],
- wymiany poglądów na temat ewentualnej współpracy w dziedzinie polityki zatrudnienia i społecznej,
- wymiany doświadczeń na temat zagranicznej polityki pomocy rozwojowej,
- przemysłu obronnego i zbrojeniowego.

Instrumenty współpracy wyszehradzkiej w wiodącym wymiarze międzyrządowym ustalone zostały w wytycznych z Kromieryża z 2004 r., gdzie wskazano:

- rotacyjne roczne przewodnictwo;
- każde państwo przewodniczące Grupie przygotowuje własny program swojego przewodnictwa, zapewniający m.in. ciągłość długoterminowej współpracy V4;
- jeden oficjalny szczyt premierów corocznie, na zakończenie każdego kolejnego okresu przewodnictwa;
- okolicznościowe, nieformalne spotkania premierów, względnie ministrów spraw zagranicznych, przed wydarzeniami międzynarodowymi;

- spotkania wiceministrów spraw zagranicznych, poprzedzające oficjalne szczyty premierów;
- spotkania innych ministrów w grupie państw V4;
- zintensyfikowana komunikacja między krajowymi koordynatorami V4 oraz ich kluczowa rola w wewnętrznej i międzypaństwowej koordynacji;
- konsultacje i współpraca Stałych Przedstawicielstw przy UE i NATO w Brukseli, jak również na wszystkich istotnych forach (OBWE, ONZ, Rady Europy, OECD, WTO itp.);
- Międzynarodowy Fundusz Wyszehradzki i jego struktury.

Badacze na ogół krytycznie oceniają dorobek Grupy Wyszehradzkiej. E. Kużelewska i A.R. Bartnicki podkreślają, że nie potrafiono i nie przejawiano woli, by opracować nową, wspólną wizję i cele działania, wychodzące poza rytualne zapewnienia o konieczności dalszego pogłębiania współpracy. Ponadto brakowało wspólnych strategii i obszarów realnego współdziałania z uwagi na odmienne interesy, różne definiowanie → z a g r o ż e ń [t. 4] oraz odmienne spojrzenia na własną rolę w UE. Grupa Wyszehradzka stanowiła raczej klub dyskusyjny, któremu brakowało moderatora. W swojej historii państwa Grupy Wyszehradzkiej przez niemal 2 dekady nie dopracowały się wspólnych projektów infrastrukturalnych, nie potrafiły przemawiać jednym głosem na forum UE i NATO, wspólnie określać obszarów zagrożeń i współpracować w celu ich eliminacji. Gospodarki państw grupy nie wytworzyły pozytywnej synergii, ale raczej rywalizowały głównie o przyciągnięcie inwestycji. Grupa Wyszehradzka była przy tym mało rozpoznawalna, nawet w obrębie społeczeństw państw członkowskich, nie wykształciła ram współpracy na wzór Beneluksu czy Grupy Nordyckiej, nie miała wspólnej tożsamości, a cele i interesy członków wydawały się coraz częściej rozbieżne.

Jakub Idzik, Rafał Klepka

W. Gizicki, *Architecture of the Visegrad Cooperation*, [w:] *Political Systems of Visegrad Group Countries*, W. Gizicki (ed.), University of Ss Cyril and Methodius in Trnava Slovakia, The John Paul II Catholic University of Lublin Poland, Trnava–Lublin 2012; T. Kubin, *Grupa Wyszehradzka – perspektywy dalszej współpracy*, „Athenaeum. Polskie Studia Politologiczne" 2014, vol. 42; E. Kużelewska,

A.R. Bartnicki, *Grupa Wyszehradzka – nowe wyzwania bezpieczeństwa i perspektywy współpracy*, „Rocznik Integracji Europejskiej" 2017, nr 11; J. Marušiak i in., *Internal Cohesion of the Visegrad Group*, Institute of Political Science, Slovak Academy of Sciences VEDA, Publishing House of the Slovak Academy of Sciences, Bratislava 2013; S. Puzyna, *Informacja na temat Grupy Wyszehradzkiej*, Kancelaria Senatu – Biuro Spraw Międzynarodowych i Unii Europejskiej, Warszawa 2012; VisegradGroup.eu (dostęp 17.01.2020).

GRUPY BOJOWE UNII EUROPEJSKIEJ (European Union Battlegroups) – europejskie związki taktyczne, formacje wojskowe sił reagowania kryzysowego Unii Europejskiej, które są niestałą wojskową organizacją bojową, tworzone na okres pół roku. To jednostki wojskowe, które dostosowują się do wspólnej polityki bezpieczeństwa i obrony (WPBiO) UE i które w zależności od swojej misji składają się z elementów różnych rodzajów wojsk. Są one przeznaczone na misje w regionach kryzysowych i stwarzają niezbędne warunki do dalszego wykorzystania (np. w ramach ONZ).

Dzięki połączeniu sił koalicji państw członkowskich każda z kilkunastu grup bojowych składa się z sił o rozmiarach batalionu (1,5 tys. → ż o ł n i e r z y [t. 4]) wzmocnionych elementami wsparcia bojowego. Grupy aktywnie się zmieniają, dzięki czemu 2 są zawsze gotowe do wdrożenia. Siły znajdują się pod bezpośrednią kontrolą Rady UE.

Pierwsze pomysły dla konkretnych grup bojowych UE pojawiły się na szczycie Rady Europejskiej w dniach 10–11 grudnia 1999 r. w Helsinkach, na którym szefowie państw i rządów starej piętnastki postanowili utworzyć siły szybkiego reagowania, które mogłyby zostać wykorzystane do poradzenia sobie z → k r y z y s e m w kraju trzecim, w bardzo krótkim terminie i w razie potrzeby daleko od granic europejskich.

Budowa grup bojowych została zdynamizowana po zamachach z 11 września 2001 r. Przyspieszenie w tworzeniu WPBiO miało miejsce bezpośrednio po wojnie w Iraku w 2003 r. Rada UE opracowała główny cel i określiła potrzebę zdolności szybkiego reagowania, którą członkowie powinni zapewnić w postaci małych sił o wysokiej gotowości.

Pomysł ten został powtórzony na szczycie francusko-brytyjskim 4 lutego 2003 r. w Le Touquet, na którym podkreślono, że w celu jednoczesnego przeprowadzenia kilku operacji i poprawy zdolności szybkiego

reagowania Unia powinna wyznaczyć nowe cele w zakresie zdolności, zarówno ilościowe, jak i jakościowe. Podkreślono również potrzebę poprawy zdolności szybkiego reagowania, „w tym początkowego rozmieszczenia sił lądowych, morskich i powietrznych w ciągu 5–10 dni". Właśnie wtedy narodził się pomysł grup bojowych UE wspierających działania ONZ. Zostało to ponownie opisane jako niezbędne w Celu głównym 2010 (Headline Goal 2010).

Operacja Artemis w Demokratycznej Republice Konga w 2003 r. – pierwsza autonomiczna operacja wojskowa prowadzona przez UE – wykazała szybką reakcję Unii i rozmieszczenie sił w krótkim czasie. UE przeszła od koncepcji → zarządzania kryzysowego [t. 4] do uruchomienia operacji w ciągu zaledwie 3 tygodni, rozmieszczenie wojsk zajęło 20 dni. Sukces tej operacji doprowadził do stworzenia grup szybkiego reagowania, umożliwiając rozważenie tego pomysłu bardziej praktycznie. Na kolejnym francusko-brytyjskim szczycie w listopadzie 2003 r. stwierdzono, że w oparciu o doświadczenia z operacji UE powinna być w stanie rozmieścić siły w ciągu 15 dni w odpowiedzi na wniosek ONZ. Należy stwierdzić, że koncepcja Grup Bojowych opiera się na wykorzystaniu „szybko wchodzącego i szybko wycofywanego" potencjału w celu przywracania porządku, zwłaszcza w Afryce, w ramach operacji prowadzonych „zwłaszcza, ale nie wyłącznie" z mandatu Rady Bezpieczeństwa ONZ.

10 lutego 2004 r. Francja, Niemcy i Wielka Brytania przedstawiły wspólną koncepcję powstania 7–9 grup bojowych. Bazując na wnioskach z operacji Artemis, w dokumencie zaproponowano kilka grup, które byłyby autonomiczne, składające się z ok. 1,5 tys. żołnierzy i które mogłyby być rozmieszczone w ciągu 15 dni. Takie grupy są odpowiedzią głównie na postulaty ONZ o wytworzeniu zdolności szybkiej reakcji i jednoczesnej możliwości dostosowania do konkretnych misji. Ich zadaniem jest koncentracja na łączeniu operacji i przygotowaniu pola dla działania większych sił. 17 czerwca 2004 r. Rada UE podjęła decyzję o utworzeniu Grup Bojowych UE w ramach realizacji Celu głównego 2010 (Headline Goal 2010). 22 października 2004 r. w Brukseli ministrowie obrony krajów członkowskich zatwierdzili utworzenie 13 grup bojowych, które miałyby podejmować interwencje w promieniu 6 tys. km od Brukseli. Od tego czasu dołączyły do nich kolejne grupy bojowe.

W 2004 r. sekretarz generalny ONZ Kofi Annan z zadowoleniem przyjął plany utworzenia takich grup i podkreślił ich wartość i znaczenie we wspieraniu ONZ w rozwiązywaniu różnorodnych problemów.

1 stycznia 2005 r. grupy osiągnęły początkową zdolność operacyjną: co najmniej jedna grupa bojowa pozostawała w gotowości przez 6 miesięcy. Zarówno Wielka Brytania, jak i Francja miały działającą grupę bojową w pierwszej połowie 2005 r., a Włochy w drugiej połowie. W pierwszej połowie 2006 r. działała Francusko-Niemiecka Grupa Bojowa (French–German Battlegroup) oraz Hiszpańsko-Włoska Grupa Ziemnowodna (Spanish–Italian Amphibious Battlegroup). W drugiej połowie tego roku działała tylko jedna grupa bojowa złożona z Francuzów, Niemców i Belgów.

Pełna zdolność operacyjna została osiągnięta 1 stycznia 2007 r., co oznacza, że Unia mogłaby jednocześnie podjąć 2 operacje z wykorzystaniem grupy bojowej lub jednocześnie rozmieścić je w tym samym regionie. Grupy zmieniają się co 6 miesięcy. Są one wykorzystywane *ad hoc* w misjach wyznaczanych przez UE i zostały przez niektórych określone jako nowa czynna armia europejska. Oddziały i sprzęt pochodzą z państw członkowskich UE przewodzących konkretnym grupom.

14 listopada 2016 r. 56 europejskich ministrów spraw zagranicznych i obrony wyraziło zgodę na globalną → s t r a t e g i ę [t. 4] UE w zakresie → b e z p i e c z e ń s t w a [t. 1] i polityki zagranicznej. Obejmowało to nowe możliwości szybkiego rozmieszczenia grup bojowych UE z lotniczym wsparciem operacji cywilnych i wojskowych w strefach konfliktów poza Europą, np. przed przybyciem → s i ł p o k o j o w y c h O N Z [t. 4]. Na osiągnięcie zgody ministrów, oprócz Brexitu i zmiany prezydenta USA, wpłynął również rosyjski ekspansjonizm wojskowy i europejski kryzys migracyjny.

W dniu 6 marca 2017 r. ministrowie spraw zagranicznych i obrony zgodzili się na utworzenie europejskiego centrum dowodzenia w Brukseli dla wojskowych misji szkoleniowych za granicą, które może w przyszłości stać się europejskim sztabem generalnym. Ta zdolność planowania i prowadzenia działań wojskowych została potwierdzona i ustanowiona przez Radę Unii Europejskiej w dniu 8 czerwca 2017 r. Stało się to dzień po uruchomieniu przez Komisję Europejską Europejskiego Funduszu Obrony z budżetem 5,5 mld EUR rocznie na „koordynację, uzupełnienie i zwiększenie krajowych inwestycji w badania w dziedzinie obronności,

w rozwój prototypów oraz w zakup sprzętu i technologii obronnych". Do tego czasu brak wspólnego funduszu wojskowego był główną przeszkodą w skutecznym rozmieszczeniu operacyjnym grup bojowych UE.

Na szczycie UE w Brukseli w dniach 22–23 czerwca 2017 r. osiągnięto porozumienie ws. stałej współpracy strukturalnej w dziedzinie obronności (PESCO). Badanie →opinii publicznej [t. 3] Eurobarometru z czerwca 2017 r. wykazało, że 75% Europejczyków popiera WPBiO, a 55% opowiada się nawet za armią europejską.

Każda grupa bojowa musi być przygotowana do rozpoczęcia operacji po upływie maksymalnie 15 dni od podjęcia decyzji politycznej. Przez pierwsze 5 dni (maks.) mogą trwać konsultacje polityczne, kolejne 10 dni to czas na przerzut i rozmieszczenie wojsk. Operacje powinny być wyposażone w mandat Narodów Zjednoczonych w oparciu o VII rozdział Karty Narodów Zjednoczonych. Operacje te mogą być zlecane przez samo ONZ. Po okresie trwania operacji (30–120 dni) rolę UE przejmują błękitne hełmy. Początkowo proponowano, aby miejscem działania grup bojowych był kontynent afrykański, stwierdzono jednak, że nie należy stosować ograniczeń geograficznych.

Grupa bojowa jest uważana za najmniejszą samowystarczalną jednostkę wojskową, którą można rozmieścić i utrzymać w teatrze działań. Nie ma ustalonej struktury, „standardowa" grupa obejmuje kompanię główną, 3 kompanie piechoty i odpowiedni personel pomocniczy. Określone jednostki mogą wykorzystywać piechotę zmechanizowaną, grupy wsparcia (np. wsparcie przeciwpożarowe lub medyczne), których połączenie umożliwia niezależne działanie grupy w trakcie wykonywania różnych zadań. Oprócz tego w skład każdej grupy powinien wchodzić 500-osobowy batalion wyposażony w kołowe transportery opancerzone i lekki sprzęt. Pododdział ten musi być zdolny do szybkiego przerzucenia w rejon konfliktu. Koszty europejskich sił szybkiego reagowania pokrywają tworzące je kraje. Za planowanie i wsparcie logistyczne odpowiedzialne jest państwo wiodące w grupie.

Grupy bojowe mają za cel realizację zadań WPBiO, a mianowicie są to zadania wojskowe o charakterze humanitarnym, utrzymywania pokoju i przywracania pokoju. Planiści twierdzą, że grupy bojowe mają wystarczający zasięg, aby poradzić sobie z tymi wszystkimi zadaniami,

chociaż ich misje powinny być ograniczone „rozmiarem i intensywnością" ze względu na niewielki rozmiar grup. Takie misje mogą obejmować zapobieganie konfliktom, ewakuację, udzielanie pomocy lub wstępną stabilizację. Zasadniczo można by je podzielić na 3 kategorie: krótkie wsparcie istniejących wojsk, szybkie rozmieszczenie przygotowujące grunt pod działanie większych sił lub niewielkie misje szybkiego reagowania.

Istnieją 2 rodzaje grup bojowych: narodowe i wielonarodowe. Większe państwa członkowskie zazwyczaj tworzą własne grupy bojowe (Francja, Wielka Brytania, Hiszpania oraz Włochy), podczas gdy od mniejszych członków oczekuje się tworzenia wspólnych grup. Niemcy tworzą grupy bojowe we współpracy z mniejszymi krajami UE i są członkami 4 z 9 wielonarodowych grup bojowych. Państwa wiodące w grupach przejmują dowodzenie operacyjne w oparciu o model ustanowiony podczas operacji Artemis w Demokratycznej Republice Konga.

W tworzeniu grup bojowych biorą udział następujące kraje UE: Austria, Belgia, Bułgaria, Cypr, Czechy, Estonia, Finlandia, Francja, Grecja, Hiszpania, Holandia, Litwa, Luksemburg, Łotwa, Niemcy, Polska, Portugalia, Rumunia, Słowacja, Słowenia, Szwecja, Węgry, Wielka Brytania, Włochy. 2 kraje →NATO [t. 3] nienależące do UE – Norwegia i Turcja – uczestniczą w tworzeniu grup bojowych, tak jak i inne 2 państwa nienależące do UE – Macedonia Północna i Ukraina. Dania ma klauzulę neutralności zawartą w traktacie z Maastricht i nie jest zobowiązana do uczestnictwa w WPBiO. Również Malta obecnie nie uczestniczy w żadnej grupie bojowej. Istnieją także plany rozszerzenia grup o siły powietrzne i morskie. Oprócz państw członkowskich UE potencjalnymi uczestnikami wojsk są kraje zaproszone przez innych członków UE lub kandydaci do członkostwa. Niektóre państwa członkowskie zaoferowały także swoje możliwości wsparcia grup bojowych UE:

- Cypr (grupa medyczna);
- Litwa (jednostka oczyszczania wody);
- Grecja (Athens Multinational Sealift Coordination Center);
- Francja (struktury wielonarodowego i mobilnego dowództwa);
- Irlandia (eksperci od usuwania bomb).

Oczekuje się, że Finlandia zaangażuje żołnierzy przeszkolonych do walki z →bronią chemiczną [t. 1] i →biologiczną [t. 1].

W ramach gier wojennych w 2008 r. grupy bojowe UE trenowały w celu ochrony pierwszych wolnych wyborów w wyimaginowanym kraju Vontinalys. W czerwcu 2014 r. 3 tys. żołnierzy z Belgii, Niemiec, Luksemburga, Macedonii Północnej, Holandii i Hiszpanii trenowało w Ardenach w trakcie ćwiczeń pod kryptonimem Quick Lion, aby zapobiec →przemocy [t. 3] na tle etnicznym między „Szarymi" oraz „Białymi" w wyimaginowanym kraju Blueland.

Grupy bojowe Unii Europejskiej dążą do tworzenia kilku szybkich jednostek wdrożeniowych dla międzynarodowych operacji i misji przyszłości, najpierw w strefie →wojny [t. 4].

Na poziomie strategicznym przywództwo polityczne, a zatem najwyższe, sprawuje Komitet Polityczny i Bezpieczeństwa UE. Dowódca operacji może decydować o szczegółowych wymaganiach dla danej misji. Ze względu na możliwą specjalizację zaangażowanych sił (np. przeznaczenie do rozmieszczenia w obszarach miejskich, górach, pustyni, dżungli) lub ich skład (np. w przypadku jednostek desantowych) grupa bojowa może mieć specjalne kwalifikacje, a zatem nadawać się do konkretnego zastosowania.

Ponieważ zdolności grup bojowych UE są bardzo ograniczone (np. nie obejmują transportu strategicznego), przydziela im się dodatkowe siły: medyczne, logistyczne i specjalne, a także części sił powietrznych lub morskich wykorzystywanych do rozszerzania lub uzupełniania zakresu zdolności na poziomie operacyjnym lub strategicznym.

Chociaż od 2005 r. w ramach WPBiO formowane są grupy bojowe, państwa członkowskie nie zdołały ani razu porozumieć się w sprawie ich użycia. Na przeszkodzie stawały zazwyczaj różnica zdań dotycząca optymalnej formy odpowiedzi UE na dany kryzys i zbyt wysokie koszty użycia grup, związane m.in. z transportem strategicznym. Ze względu na skromne zasoby i zobowiązania wobec NATO członkowie UE mają też kłopoty z utrzymywaniem 2 grup bojowych w półrocznym pogotowiu jednocześnie. Konieczność zachowania zdolności do efektywnego działania skłoniła już do zacieśnienia współpracy dwustronnej Wielką Brytanię i Francję – państwa o diametralnie różnych spojrzeniach na NATO i WPBiO. Na pogłębienie współpracy wojskowej poza strukturami UE i NATO zdecydowały się także państwa skandynawskie, które utworzyły organizację NORDEFCO (Dania, Finlandia, Islandia, Norwegia i Szwecja).

Dzięki odpowiednim zasobom militarnym UE mogłaby w przyszłości prowadzić misje, co do których nie ma zgodności wewnątrz Sojuszu, zmniejszając w ten sposób ryzyko podziałów w NATO. Grupy bojowe zwiększają także zdolność do wspólnego działania oddziałów z różnych państw i pełnią funkcję mechanizmu wymuszającego modernizację sił zbrojnych. Rezultatem takiej współpracy w ramach UE mogą być więc lepiej wyszkolone i uzbrojone siły zdolne do współpracy i prowadzenia misji także w ramach NATO.

Dzięki grupom bojowym UE chce realizować Europejską Strategię Bezpieczeństwa i poprawić swoją zdolność szybkiego reagowania na kryzysy i konflikty wojskowe po wydaniu odpowiedniej decyzji politycznej. Możliwe opcje obejmują pomoc humanitarną, zapobieganie działaniom wojennym lub napadom lub obronę przed nimi (ewentualnie nawet przez →odstraszanie [t. 3] w okresie poprzedzającym konflikt), gwałtowne oddzielenie stron konfliktu oraz wdrożenie początkowych operacji obejmujących rozmieszczenie, aby umożliwić działania dalszych sił, takich jak siły pokojowe ONZ. Możliwe miejsca działania grup to kraje zdezintegrowane lub dotknięte rozpadem państwa. Jest to reakcja na nowy rodzaj wojny, tzw. →wojny czwartej generacji [t. 4], które powstają w różnych zakątkach świata. Przede wszystkim ważne jest oddzielenie stron konfliktu w celu rozpoczęcia procesu pokojowego.

Główne wyzwania stojące przed Grupami Bojowymi UE to wyzwania praktyczne – takie jak dalsze dopracowanie standardów (w razie potrzeby) czy zapewnienie rezerw strategicznych. Innym rodzajem wyzwań są te o charakterze bardziej politycznym, ponieważ wciąż nie istnieje konsensus co do tego, które konkretne zadania są istotne dla grup bojowych i kiedy ich realizacja powinna się rozpocząć.

Sergiusz Wasiuta

A. Barcikowska, *EU Battlegroups – Ready to Go?*, „Brief Issue" 2013, vol. 40; C. Bickerton, *European Union Foreign Policy: From Effectiveness to Functionality*, Palgrave Macmillan, London 2015; Y. Boyer, *The Battle Groups: Catalyst For a European Defence Policy*, Brussels 2007; Fact Sheets on the European Union, *The EU Battlegroups and the EU civilian and military cell*, 2005, EuroParl.Europa.eu/FactSheets (dostęp 17.02.2020); *Ireland Prepares to Join EU Battle Group Next Year*, 28.06.2019,

EUObserver.com (dostęp 17.02.2020); M. de Langlois, A. Capstack, *The Role Of The Military In The Eu's External Action: Implementing The Comprehensive Approach*, „Laboratorie de L'Irsem" 2014, no. 23; G. Lindstrom, *Enter the EU Battlegroups*, Institute for Security Studies, Paris 2007; tenże, *The EU Battlegroups: Options for the Future*, „Chaillot Paper" 2011, vol. 64, no. 1; G. Quille, *The EU Battle Groups*, European Parliament, Brussels 2006; tenże, *The European Security and Defence Policy: From the Helsinki Headline Goal to the EU Battlegroups*, European Parliament, Brussels 2006; S. Raine, *Europe's Strategic Future: From Crisis to Coherence?*, Routledge, London 2019; J. Stańczyk, *Grupy Bojowe jako instrument polityki reagowania kryzysowego Unii Europejskiej* „Studia Europejskie" 2009, nr 4 (52); *The Path of the European Union Battlegroups A Historical Institutionalist Analysis of the Development of the EU Battlegroups since 1998*, J. Pekelder (ed.), Utrecht University, Utrecht 2018; V. Volpi, *Why Europe Will Not Run the 21st Century: Reflections on the Need for a New European Federation*, Cambridge Scholars Publishing, Cambridge 2011; Ł. Zalesiński, *Grupa Bojowa V4 coraz bliżej powstania*, 14.03.2014, Polska-zbrojna.pl (dostęp 17.02.2020).

H

HAKER – osoba, która zmienia lub modyfikuje programowalny kod, aby dostosować go do celu, dla którego ten program nie był pierwotnie przeznaczony. Powszechnie przyjmuje się błędne uproszczenie, że hakerzy to specyficzny rodzaj przestępców działających w →cyberprzestrzeni [t. 1], choć kwestia przestrzegania prawa jest aspektem zasadniczym, który dzieli środowisko hakerów i do dziś wzbudza w nim wiele dyskusji.

Obecnie, ze względu na specyfikę działania oraz podejście do przestrzegania etyki i prawa, wykształciły się 3 typy w środowisku hakerów. Pierwszy to *black hat* – utożsamiani z crackerami. Do tej kategorii zalicza się hakerów, którzy celowo naruszają lub łamią etykę hakerską, uzyskują nieautoryzowany dostęp do komputerów lub sieci w celu osiągnięcia korzyści materialnych lub osobistych. Najczęstsza forma ich działania to rozprzestrzenianie →złośliwego oprogramowania [t. 4], kradzież danych – finansowych, osobowych, danych logowania, ale też modyfikacja, uszkodzenie lub zniszczenie tych danych. Konsolidacja nurtu *black hat,* jak i jego globalny rozwój są datowane na 2004 r., a zaczęły się od manifestu J. Hammonda, który nawoływał innych hakerów *black hat* do przeprowadzania →cyberataków [t. 1] mających na celu ingerencje polityczne. Ta ideologia doprowadziła do powstania →cybergrupy [t. 1] Anonymous, a następnie jej odgałęzienia LulzSec.

Reprezentantami hakerów typu *black hat*, działających indywidualnie, są m.in.: N. Popescu (kontrolowanie 70-osobowej cybergrupy hakerów, sprzedaż przez internet nieistniejących samochodów i innych rzeczy na kwotę ponad 3 mln USD), E.M. Bogachev (szereg oszustw, rozprzestrzenienie →ransomware [t. 3] „gameover Zeus"). Najsłynniejszym działaniem *black hat* w Polsce jest przypadek hakera o pseudonimie Polsilver z 2015 r., który wykradł dane klientów z Plus Banku i żądał za nie okupu 200 tys. PLN.

Drugim typem hakerów są *gray hat.* Są to hakerzy, którzy w dużej mierze przestrzegają zasad etyki i prawa, incydentalnie dopuszczając się ich naruszeń.

Dla hakerów trzeciego typu – *white hat*, nazywanych też *ethical hakers* – wartością nadrzędną jest przestrzeganie zasad etyki i prawa. Hakerzy tego rodzaju przeprowadzają symulowane „cyberataki", czyli tzw. testy penetracyjne systemów operacyjnych, oprogramowania itd., w celu znalezienia luk →bezpieczeństwa [t. 1]. Wykryte w systemie błędy są zgłaszane do administratorów, następnie do przetestowanego systemu wdrażane są odpowiednie łatki (ang. *patch*), niwelujące wykryte problemy.

Działania hakerów *white hat* nie ograniczają się zwykle tylko do systemów IT, ale testują także np. czynnik ludzki (przestrzeganie przez personel danej instytucji wewnętrznej polityki bezpieczeństwa) najczęściej poprzez operacje wykorzystujące socjotechnikę czy →phishing [t. 3]. Wielu z nich działa w sektorze prywatnym jako konsultanci i specjaliści →cyberbezpieczeństwa [t. 1], uważanego za lukratywną branżę IT.

Całe środowisko hakerskie, bez względu na wymienione wyżej podziały, jest stosunkowo hermetyczne, nieformalne członkostwo wymaga posiadania dużej wiedzy oraz ciągłego doskonalenia swojego warsztatu. Z tych powodów przyszli hakerzy najczęściej korzystają z hakerskich forów, kanałów komunikacji typu IRC i uczą się bezpośrednio z dokumentacji, opisów ataków lub od hakerów mających poważanie w środowisku. Jeśli kandydat będzie wystarczająco dobry, będzie się udzielał, ma szansę zostać zaakceptowany przez grupę. Z niej zostanie „wydelegowany" mentor, który następnie uczy go konkretnych technologii, form cyberataków, wskazuje repozytoria, z których może czerpać wiedzę. Dużą wagę przywiązuje się

do praktyki (podstawową dewizą jest „ucz się przez robienie oraz przez zadawanie dużej ilości pytań"). Jest to spowodowane koniecznością przyswajania ogromnych ilości wiedzy i jej stałego uaktualniania. Przeważnie, po opanowaniu podstaw, kolejnym etapem jest łamanie zabezpieczeń oprogramowania.

Środowisko hakerskie przeszło wiele podziałów, przekształceń etycznych, pozostawił na nim ślad również dynamiczny rozwój IT, co ostatecznie uformowało dosyć specyficzny światopogląd, pewnego rodzaju ideologię – doprowadziło to do wypracowania szeregu społecznych norm, umożliwiających jej członkom funkcjonowanie w strukturze interakcji. Elementarnym założeniem jest nacisk na znaczenie sieci związków między technologią a całą społecznością hakerów, w której działają i za pośrednictwem której realizują swoje interesy. Drugim filarem jest indywidualne ustawiczne zdobywanie wiedzy i pogłębianie rozumienia procesów w dziedzinie IT. Trzecim ważnym elementem jest jednostkowa samoświadomość hakerów, że poziom zaawansowania posiadanej wiedzy, technologii i przeprowadzonych akcji ma rzeczywiste przełożenie na postrzeganie hakerów. Ostatnim „dogmatem" tej subkultury jest znajomość obowiązującego prawa, dla jasnego określenia, które aktywności w cyberprzestrzeni są nielegalne.

Istnieje 12 praktycznych zasad społecznych obowiązujących hakerów we wzajemnych relacjach w komunikacji internetowej:

- Sprawdź w wyszukiwarce, zanim zadasz pytanie na forum (ewentualna sankcja: zignorowanie pytania).
- Zakaz wysyłania obraźliwych wiadomości, trollowania, nękania, molestowania (ewentualna sankcja: wyrzucenie z forum).
- Zadawaj właściwe, precyzyjne pytania (ewentualna sankcja: zignorowanie pytania).
- Bądź pokorny, proś o pomoc tylko wtedy, gdy nie można łatwo znaleźć odpowiedzi (ewentualna kara: zignorowanie pytania i wyrzucenie z forum).
- Nie podejmuj prób włamania się do systemu hakera ani mu nie groź (ewentualna kara: wykluczenie z forum, bardzo prawdopodobne ryzyko odwetu).
- Nie popisuj się, robiąc głupie rzeczy (kara: zignorowanie, strata reputacji).

- Nie przypisuj sobie wyników pracy innych (ewentualna kara: odwet środowiska na zasadzie cyberataku, doniesienie o przestępstwie do służb państwowych).
- Dziel się wiedzą, źródłami wiedzy i materiałami (udostępnianie bezużytecznych rzeczy jest sankcjonowane wykluczeniem, także ryzykiem odwetu).
- Zachęcaj do wykorzystywania i rozwijania istniejących już narzędzi – także dla innych (jest to też sposób na legalny zarobek. Cenione w środowisku są także materiały z nowych technologii, →informacje o nowych lukach w zabezpieczeniach, nowe narzędzia hakerskie itd.).
- Nie handluj bezużytecznymi programami.
- Kwestia piractwa – dzielenie się informacjami jest uznawane w środowisku za dobrą rzecz, natomiast kradzież dokonań takich jak np. programy penetracyjne, których stworzenie wymagało dużej ilości czasu, jest stygmatyzowana.
- Nie ufaj nikomu. Jest to bardziej rada niż reguła, oczekuje się, że udostępniane programy będą poufne i ich działanie będzie zgodne z opisem, jednak nie ma na to gwarancji.

Geneza terminu haker ma swój początek w latach 60. XX w. w Massachusetts Institute of Technology (MIT). Początkowo termin ten oznaczał informatycznego wynalazcę, programistę osiągającego swoje cele w sposób niestandardowy, niezgodny z ogólnie przyjętymi metodami. Nazwa wzięła się z zawierających informatyczne innowacje technologiczne żartów studenckich, które nazwano *hacks*. Umiejętność ich wykonania wymagała rozległej wiedzy technicznej, ponadto z racji małej liczby sprzętu i jego dużej wartości pierwsi hakerzy działali tak, by nie uszkodzić uczelnianej infrastruktury i oprogramowania.

Znaczenie tak rozumianego hackingu zmieniło się pod koniec lat 60. XX w. Dostrzeżono duży potencjał w informatyzacji armii i struktur rządu federalnego, dzięki czemu ośrodki naukowe związane z informatyką zaczęły być finansowane przez podmioty publiczne. Wiązało się to z narzuceniem środowisku naukowców odpowiedniej polityki bezpieczeństwa informacji, co było niezgodne z dotychczas wypracowaną etyką kultury technomerytokratycznej.

Zaistniała sytuacja wzbudziła sprzeciw oraz doprowadziła do powstania paradygmatu, który stał się fundamentem subkultury hakerskiej, jaką znamy obecnie. Jego założenia to:

- Każdy człowiek ma prawo dostępu do komputera.
- Dostęp do informacji powinien być bezpłatny.
- Nieufanie legalnym organom władzy.
- Hakerów należy sądzić wg przeprowadzonego hackingu, a nie formalnych obostrzeń prawnych.
- Każdy może tworzyć sztukę i piękno na komputerze.
- Komputery mogą ulepszyć życie człowieka.

M. Castells w *The Age of Information* twierdzi, że w perspektywie antropologicznej relacje w środowisku hakerskim polegają na tzw. kulturze daru, wartością jest wolność przejawiająca się w 3 aspektach: tworzeniu, dostępie do wiedzy oraz formie dzielenia się wiedzą.

Wraz z informatyzacją społeczeństw od lat 80. XX w. i rosnącymi trendami → c y b e r p r z e s t ę p c z o ś c i [t. 1] ustawodawcy z opóźnieniem dostosowywali prawo dotyczące bezpieczeństwa sieci i informacji. Początkowo środowisko hakerskie utrzymywało, że ich działalność jest legalna, co miało na celu odróżnienie hakerów od subkultury cyberprzestępców, dla których hakowanie czy szeroko pojęta działalność w sieci jest sposobem osiągania korzyści finansowej cudzym kosztem np. poprzez przestępstwa takie jak oszustwo, *scamming* czy defraudacja. Było to założenie polaryzujące środowisko na „dobrych" hakerów oraz „złych" cyberprzestępców, których z czasem nazwano crackerami, podział ten do dziś jest dosyć powszechny.

Perspektywa zdobycia cennych umiejętności i aura elitarności środowiska hakerów przyciąga wiele osób w młodym wieku aspirujących do zostania hakerami, określanych jako *script kiddies*. Przez środowiska hakerskie nie są one uznawane za hakerów w pełni tego słowa znaczeniu. Nie posiadają wystarczającej eksperckiej wiedzy z zakresu sieci i programowania, więc korzystają z gotowego kodu, skryptów, narzędzi i złośliwego oprogramowania w celu naruszania bezpieczeństwa systemów informatycznych. Najczęściej przeprowadzają niepotrzebne ataki na innych niedoświadczonych hakerów bez większej → s t r a t e g i i [t. 4] czy też atakując cele, których naruszenie wzbudza ogólne oburzenie społeczne.

Ich motywacją jest najczęściej zdobycie popularności oraz uznania na forach związanych z hackingiem, naruszenia praw autorskich. Często są uczestnikami ataków DDoS, angażują się w działalność haktywistyczną. Formy ich cyberataków nie są wyrafinowane, standardem jest podejmowanie prób hakowania kont na portalach społecznościowych (przeważnie na Facebooku) lub *defacing* (zmienianie wyglądu) stron internetowych.

Pojawienie się *script kiddies* naruszyło ustaloną hierarchię wartości hakerów – szacunek u innych w tym środowisku można było wcześniej zdobyć wyłącznie poprzez posiadanie bardzo dobrej znajomości sieci i systemów operacyjnych komputerów, udowadnianie swoich umiejętności oraz dzielenie się wiedzą dotyczącą przeprowadzonych cyberataków. Duże znaczenie miał też poziom zaawansowania i finezji cyberataku. Działanie *script kiddies* często sprowadza się do umieszczania bardzo ogólnych pytań, wskazujących znaczne braki wiedzy w temacie typu „jak zhakować serwer mojej szkoły". Osoby uznające się za hakerów na forach zadają bardzo precyzyjne pytania, dopiero po przeprowadzeniu przeglądu źródeł i literatury.

W tym momencie nasuwa się pytanie o granice umiejętności, rozróżniające tego typu nowicjuszy od hakerów, bowiem używanie istniejących już narzędzi jest wbrew pozorom standardem u nawet zaawansowanych hakerów, bardziej chodzi o posiadanie wiedzy na temat możliwych ataków – jak one działają i dlaczego tak działają. W analogicznym kontekście w środowisku toczą się dyskusje, czy można zaliczyć do środowiska hakerow pentesterów – nie tworzą oni bowiem swoich narzędzi, nie rozwijają własnych programów typu *exploit* itd. Warto jednak zaznaczyć, że tworzenie własnych programów bardzo rozwija, natomiast korzystanie z istniejących narzędzi wspiera handel nimi, to zaś wzmacnia społeczność, która współpracuje w celu wymiany wiedzy, narzędzi i technik.

Przykładem *script kiddies* w polskiej cyberprzestrzeni są *anoni* (z ang. *anonymous*, anonimowy), związani z forami typu imageboard takimi jak Karachan.org, Wilchan.org, Vichan.org, Kiwichan.org, Lolifox.org, 8chan.org czy forum Cebulka w sieci Tor. Wypracowali oni własną, bardzo prymitywną kulturę wartości zbliżoną do quasi-subkultury inceli oraz ruchu Men Going Their Own Way, która opiera się przede wszystkim na dychotomicznym dzieleniu społeczeństwa na *anonów* i *normików* oraz

wychwalaniu *piwniczenia,* czyli izolowania się od społeczeństwa. Posługują się mocno zwulgaryzowanym slangiem zbliżonym do grypsery więziennej, często opierającym się na komunikacji w sposób półobrazkowy – poprzez memy, odnoszące się do uprzedmiotowienia seksualnego kobiet, dewaluacji wartości oraz podważania autorytetów. Typowym przykładem ich działalności jest podmienianie treści na stronach internetowych na charakterystyczne grafiki.

Haktywiści są najbardziej otwartym odłamem hakerów, który zrzesza się i konsoliduje swoje działania w celu zmiany podejścia władzy państwowej do kultury i postulatów środowisk hakerskich. Najczęściej działają w cyberprzestrzeni, choć założenia etyczne stojące u podstaw ideologii hakerskiej, takie jak wolny dostęp do dóbr kultury, przeciwdziałanie monopolom, ochrona prawa do prywatności, znalazły wielu zwolenników w społeczeństwach krajów rozwiniętych, w efekcie czego przeobraziły się w globalny polityczny ruch antyestablishmentowych aktywistów – obecnie w parlamentach Czech i Szwecji stanowiący trzecią siłę polityczną. W innych krajach, po początkowych sukcesach, poparcie polityczne dla tego typu ugrupowań zmalało do ok. 1%, jak było w przypadku niemieckiej Piratenpartei czy Polskiej Partii Piratów.

Wojciech Cendrowski

W. Cendrowski, *Haker*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; R. Chiesa, S. Ducci, S. Ciappi, *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, Auerbach Publications, Boca Raton 2008; M. Dawson, M. Omar, *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, Information Science Reference, Hershey 2015; R.A. Grimes, *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*, Wiley, Indianapolis 2017; F. Jacob, *White Hat*, [w:] *Encyclopedia of Cyber Warfare*, P.J. Springer (ed.), ABC-CLIO, Santa Barbara 2017; S. Levy, *Hackers: Heroes of the Computer Revolution*, O'Reilly Media, Sebastopol 2010; Ch. Menking, *Hacker*, [w:] *Encyclopedia of Cyber Warfare*, P.J. Springer (ed.), ABC-CLIO, Santa Barbara 2017; R. Wadle, *Black Hat*, [w:] *Encyclopedia of Cyber Warfare*, P.J. Springer (ed.), ABC-CLIO, Santa Barbara 2017.

HAKTYWIZM – połączenie słów „hack" i „aktywizm". Sformułowanie „hack" zyskało popularność w latach 60. XX w. w Massachusetts Institute of Technology (MIT). Były to żarty, które charakteryzowały się pomysłowością i nie przynosiły szkód. Z ang. *hack* oznacza z jednej strony pochwałę, z drugiej to obelga w języku potocznym. W kulturze hakerskiej *hack* to moment, w którym →haker uzyskuje dostęp do czegoś, co jest pozornie niedostępne i znajduje się poza zasięgiem. Jest to także „umiejętność programowania, manipulacje w kodzie źródłowym programu".

Aktywizm to czynna postawa, zaangażowanie w sprawy publiczne. Może być również definiowany jako nieodpłatna, dobrowolna działalność polityczna lub społeczna, zazwyczaj niebędąca źródłem dochodów. Są to działania z wyboru, często będące wyrazem solidarności społecznej.

D. Denning wskazuje, że aktywizm to normalne korzystanie z internetu. Nie rodzi problemów i nie powoduje zakłóceń. Aktywizm to m.in. wyszukiwanie, przekazywanie i umieszczenie →informacji w sieci, tworzenie stron internetowych, prowadzenie dyskusji oraz współdziałanie. Jest to aktywność użytkownika sieci, która nie powoduje strat dla innych.

Haktywizmem nazywane są ataki w →cyberprzestrzeni [t. 1], przeprowadzane w imię idei. Haktywiści motywowani są chęcią zmian, ideologią i wartościami. Działania haktywistów mają spowodować, że atak zostanie dostrzeżony i uzyska medialny rozgłos. Wiedza i umiejętności haktywistów używane są do realizacji celów za pomocą np. niszczenia danych, modyfikacji, ataków na serwery czy podmiany treści stron internetowych.

Działalność haktywistów skoncentrowana jest na problemach globalnych i wartościach społecznych, takich jak godność człowieka, równość, wolność, egalitaryzm, solidarność, subsydiarność, sprawiedliwość, →społeczeństwo obywatelskie [t. 4], partycypacja obywatelska, własność, wspólnotowość.

Haktywizm rozwinął się w latach 90. XX w. Za twórcę terminu uważa się członka grupy Cult of the Death Cow (cDc) o pseudonimie Omega, który użył go po raz pierwszy w 1994 r. Haktywizm zrodził się z pierwotnej formy hackingu, nieposiadającej znamion przestępstwa.

A. Chodubski definiuje haktywizm jako „ruch kulturowo-cywilizacyjny polegający na łączeniu aktywności politycznej z osiągnięciami

technologicznymi, w celu manifestowania sprzeciwu wobec działań w przestrzeni szeroko rozumianej polityki". Badacz dodatkowo wskazuje, że haktywizm jest „zjawiskiem politycznym, aktywnością polityczną i technologiczną ukierunkowaną na przeciwdziałanie rosnącej dehumanizacji, degradacji intelektualnej globalnego społeczeństwa, a tym samym ujawniającym się zagrożeniom dla ludzkości". Denning, amerykańska specjalistka w zakresie → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o [t. 1], wskazuje, że „haktywizm obejmuje działania wykorzystujące techniki hakerskie przeciwko witrynie internetowej z zamiarem zakłócenia jej normalnego funkcjonowania, a nie spowodowania poważnych szkód", natomiast T. Jordan i P. Taylor opisują haktywizm jako połączenie oddolnego protestu politycznego i hakerstwa komputerowego. Badacze uwypuklają bezpośredniość działań, które podejmowane są w sieci w celu wywołania zmian na płaszczyźnie politycznej. W 2004 r. Jordan i Taylor wyodrębnili 2 typy działań haktywistów:

- haktywizm masowych akcji – technicznie są to głownie ataki typu DDoS (ang. *Distributed Denial of Service*), np. nieposłuszeństwo obywatelskie w formie elektronicznej zapoczątkowane w 1994 r. przez Electronic Disturbance Theatre;
- haktywizm cyfrowo poprawny – skupia się na walce o wolność słowa, wolny przepływ informacji, np. projekt Hactivismo, który skupiał się na tworzeniu narzędzi do walki z → c e n z u r ą [t. 1] w sieci. Sprzeciwia się atakom DdoS, uważając je za złamanie prawa do wolności słowa.

W literaturze przedmiotu występuje także określenie „rosyjski haktywizm". Haktywizm zazwyczaj charakteryzuje się tym, że działania podejmowane są przeciw poczynaniom władz państwowych. W Federacji Rosyjskiej tego typu działania często służą interesom Kremla. Rosyjskich haktywistów można podzielić na pro- i antykremlowskich. Ich działania charakteryzują podobne metody działania, takie jak cyberpropaganda, → d e z i n f o r m a c j a, blokowanie serwerów czy też włamania do skrzynek e-mailowych.

Działania haktywistów przybierają formę protestu i zorientowane są zazwyczaj na rozwiązywanie spraw o zasięgu globalnym. Wartości, w imię których walczą haktywiści, to m.in.: godność człowieka, równość,

sprawiedliwość, wolność, solidarność, prawa zwierząt, własność, budowa i rozwój społeczeństwa obywatelskiego. Nierzadko działania haktywistów przenoszą się z sieci do świata fizycznego, np. w sieci następuje → m o b i l i z a c j a [t. 3], która następnie manifestuje się w świecie fizycznym w formie protestów ulicznych, stąd można stwierdzić, że haktywizm łączy sferę wirtualną z realną.

Wśród ekspertów toczy się spór o to, czy haktywizm jest działalnością przestępczą, czy wyłącznie przejawem internetowej mobilizacji. Większość → c y b e r a t a k ó w [t. 1] przeprowadzanych przez haktywistów nie jest ścigana z mocy prawa z uwagi na problemy związane z wykryciem sprawców, niską szkodliwością czynu oraz niskimi kosztami naprawy szkód. Jednak zarówno w Europie, jak i w Stanach Zjednoczonych wiele metod działania haktywistów jest uznawanych za nielegalne. Poniższa tabela ilustruje przestępstwa w cyberprzestrzeni skatalogowane w Konwencji Rady Europy o → c y b e r p r z e s t ę p c z o ś c i [t. 1] z 2001 r.

Tab. 1. Podział cyberprzestępstw przyjęty w Konwencji RE o cyberprzestępczości

Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów	Przestępstwa komputerowe	Przestępstwa ze względu na charakter zawartych informacji	Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych
Nielegalny dostęp	Fałszerstwo komputerowe	Przestępstwa związane z pornografią dziecięcą	Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych
Nielegalne przechwytywanie danych	Oszustwo komputerowe		
Naruszenie integralności danych			
Naruszenie integralności systemu			
Niewłaściwe użycie urządzeń			

Źródło: opracowanie własne na podstawie *Konwencji UE o cyberprzestępczości.*

Członkowie grup haktywistycznych wywodzą się z różnych środowisk i grup społecznych. Są to też indywidualiści: twórcy, aktywiści polityczni, ekonomiści, grupy, eksperci IT, politycy, nastolatkowie. Często haktywiści to tzw. nawróceni hakerzy. Ponadto haktywizm jest działaniem wykorzystywanym przez artystów, protestujących przeciwko niesprawiedliwości i monopolom. W ujęciu kulturowo-cywilizacyjnym jest on aktywnością polityczną i technologiczną ukierunkowaną na przeciwdziałanie rosnącej dehumanizacji i degradacji intelektualnej społeczeństwa w wymiarze globalnym.

Reprezentantom haktywizmu bliska jest idea nieposłuszeństwa obywatelskiego. Jest to postawa, która zakłada wyższość zasad moralnych nad obowiązującymi normami prawnymi. Haktywiści są świadomi tego, że łamią prawo, jednak idee, w imię których popełniają przestępstwa w cyberprzestrzeni, mają dla nich większe znaczenie.

Termin „haktywizm" często wywołuje pejoratywne skojarzenia. Należy jednak zwrócić uwagę, że haktywiści przyczyniają się do rozwoju i rozpowszechnienia ciekawych i ważnych dla społeczeństwa inicjatyw oraz projektów, które zazwyczaj nie mają szans powodzenia bez nagłośnienia medialnego. Z działalności haktywistycznej korzystają również organizacje pozarządowe, tzw. trzeci sektor oraz ruchy społeczne. Haktywista dąży do realizacji celów społecznych, politycznych oraz ekonomicznych, głównie wykorzystując swoją wiedzę i umiejętności technologiczne. Haktywiści nie mają zorganizowanych struktur.

Przykłady działalności haktywistycznej:

- Electronic Disturbance Theater to jedno z pierwszych ugrupowań haktywistycznych. Grupa wspierała meksykański ruch zapatystów, organizowała cyberataki na strony internetowe: prezydenta Meksyku, giełd papierów wartościowych we Franfurcie i Mexico City, Pentagonu, amerykańskiego Białego Domu, tym samym przyczyniła się do propagacji zjawiska haktywizmu.
- Internet Black Tigers – związani z Tamilskimi Tygrysami. Haktywiści, wysyłając ok. 800 e-maili dziennie, przez kilka tygodni bombardowali skrzynkę e-mailową ambasady Sri Lanki.
- milworm – w 1998 r. zaatakowali indyjskie Bhabha Atomic Research Centre w proteście przeciwko testom nuklearnym prowadzonym przez Indie.

- Anonymous to grupa haktywistów, której początki działalności przypadają na 2004 r. Pierwsi Anonymous to użytkownicy „forów obrazkowych", tzw. *imageboardów*. Anonymous to ponadnarodowa grupa aktywistów, których działania skupiają się głównie w internecie i oscylują wokół problemów związanych z zachowaniem otwartości sieci i wolnością słowa. Za pośrednictwem internetu działa ich komunikacja, planowanie i organizowanie akcji protestacyjnych, które czasem manifestują się w świecie fizycznym. Symbolem Anonymous jest biała maska G. Fawkesa, angielskiego katolika, który w 1605 r. dokonał nieudanego zamachu na budynek brytyjskiego parlamentu. Pierwsze akcje Anonimowych, które miały charakter zorganizowany, miały miejsce w latach 2006–2008. Świat poznał ruch Anonymous w związku z protestami przeciwko ACTA w 2012 r. Inne znane akcje tej grupy to m.in.: wsparcie Irańczyków protestujących przeciwko fałszerstwom wyborczym w 2009 r., operacja Titstorm – sprzeciw haktywistów wobec planu australijskiego rządu usunięcia z internetu niektórych materiałów pornograficznych w 2010 r., operacja Empire State Rebellion – haktywiści ujawniali e-maile, które pozyskali z Bank of America, a które ukazywały →k o r u p c j ę urzędników w 2011 r., Project Chanology – miał na celu walkę z Kościołem scjentologicznym w latach 2008–2009.
- J. Assange – haktywista, redaktor naczelny serwisu WikiLeaks – witryny internetowej, która umożliwiła publikację dokumentów rządowych, korporacyjnych oraz pochodzących od osób fizycznych przez anonimowych informatorów, chcących ujawnić działania niezgodne z prawem. Serwis opublikował tajne informacje dotyczące np. wojny w Iraku, więźniów Guantanamo, wojny w Afganistanie.
- LulzSec – ataki na korporacje, agendy rządowe, media. Działalność haktywistów z tej grupy charakteryzuje się niekonsekwencją, niespójnością i rozbieżnymi celami oraz motywami. Z jednej strony grupa podkreślała, że głównym motywem ich działań jest rozrywka, z drugiej nie odcinała się od pewnych idei, w imię których działała, można wspomnieć np. po połączeniu z Anonymous realizację wspólnej operacji AntiSec.

Agnieszka Warchoł

A. Chodubski, *Haktywizm jako zjawisko polityczne w cywilizacji informacyjnej*, [w:] *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, M. Marczewska-Rytko (red.), Wydawnictwo UMCS, Lublin 2014; D. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, [w:] *Networks and Netwars: The Future of Terror, Crime, and Militancy*, J. Arquilla, D. Ronfeldt (eds.), RAND Corporation, Santa Monica 2001; U. Hadar, *Psychoanalysis and Social Involvement*, Palgrave Macmillan, London 2013; A. Karatzogianni, *WikiLeaks Affects: Ideology, Conflict and the Revolutionary Virtual*, [w:] *Digital Cultures and the Politics of Emotion: Feelings, Affect and Technological Change*, A. Karatzogianni, A. Kuntsman (eds.), Palgrave Macmillan, Basingstoke 2012; Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz. U. 2015, poz. 728; A. Kura, *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku*, Wydawnictwo Sztafeta, Stalowa Wola 2016; C. Meszyński, *Wpływ kultury hakerskiej na rozwój społeczeństwa informacyjnego. Hakerzy jako awangarda technologiczna*, [w:] *Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne*, L.H. Haber, M. Niezgoda (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006; M. Piotrowska, *Haktywizm – społeczna korzyść czy zagrożenie?*, „Studia Humanistyczne AGH" 2017, t. 16 (2); A. Warchoł, *Haktywizm*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; taż, *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku* [praca doktorska], Kraków 2017.

HARD POWER (z ang. twarda siła) – element potęgi (siły) państwa. Za M. Kleinowskim potęgę możemy zdefiniować jako „hipotetyczną zdolność uczestnika stosunków międzynarodowych do użycia swoich materialnych i pozamaterialnych zasobów w celu wykonania własnej woli, bez względu na sprzeciw lub współdziałanie innych uczestników". Potęga jest więc zdolnością do osiągania własnych celów lub realizacji dążeń. Z kolei siła to „użycie przez uczestnika stosunków międzynarodowych zmobilizowanych w określonych uwarunkowaniach zasobów materialnych i pozamaterialnych w celu wykonania własnej woli w ramach danych stosunków międzynarodowych, bez względu na sprzeciw lub współdziałanie innych uczestników". Potęga i siła opierają się więc na tych samych zasobach materialnych i niematerialnych, z tym że potęga to potencjał, a siła to jego użycie. Do wyznaczenia poziomu siły można więc uwzględnić tylko te zasoby, spośród wszystkich tworzących potęgę, które mogą być przydatne

oraz możliwe do zmobilizowania w danej sytuacji wewnętrznej i międzynarodowej. Stąd też nie ma znaku równości między potęgą a siłą. Co więcej, siła – podobnie zresztą jak potęga – nie jest pojęciem bezwzględnym. Jest po pierwsze pojęciem relacyjnym – nie jest wykorzystywana w próżni, ale w odniesieniu do innego podmiotu, po drugie zaś relatywnym – siła zawsze jest kalkulowana względem innych podmiotów.

Podział potęgi i siły na *hard power* (twarda siła) i *soft power* (miękka siła) został sformułowany i wprowadzony do szerokiego dyskursu przez amerykańskiego politologa J.S. Nye'a jr. w 1990 r. w książce *Bound to Lead: The Changing Nature of American Power*. Co prawda pojęcia te tłumaczone są zazwyczaj z wykorzystaniem polskiego określania „siła", ale odnoszą się zarówno do siły, jak i potęgi, wedle przytoczonego powyżej rozróżnienia. Podział na *hard* i *soft power* odnosi się bowiem zarówno do zasobów, które znajdują się w dyspozycji danego podmiotu, jak i do natury jego zachowania. Sam Nye poczynił rozróżnienie na tzw. *behavioural power*, czyli zdolność do osiągania pożądanych rezultatów, oraz *resource power*, czyli posiadanie zasobów mogących stanowić podstawę do zdolności osiągania pożądanych rezultatów. Możliwość wdrożenia określonych rodzajów *behavioural power* jest uwarunkowana posiadaniem odpowiednich zasobów *resource power*. Nye lokuje twardą i miękką siłę po 2 stronach kontinuum wyznaczającego różne rodzaje *behavioural power*. Pomiędzy przymusem, będącym podstawą twardej siły, i przyciąganiem, warunkującym użycie →*soft power* [t. 3], Nye umieszcza jeszcze nakłanianie (*inducement* – bliżej *hard power*) oraz kształtowanie agendy (*agenda-setting*, bliżej *soft power*).

Hard power opiera się na zdolności do wymuszenia na innych uczestnikach stosunków międzynarodowych oczekiwanego przez dany podmiot działania. Jest to więc potęga o charakterze nakazowym, opierająca się na przymusie, oznaczająca zdolność do wymuszania na innych podmiotach konkretnych zachowań, które są oczekiwane i pożądane, w odróżnieniu od *soft power*, będącej potęgą o charakterze kooptacyjnym, opierającej się na zdolności do wpływania na inne podmioty wpływu bez użycia siły lub jej groźby, np. przez atrakcyjność kulturową czy ideologiczną.

Hard power to zbiór cech pozwalających państwu na wywieranie bezpośredniego wpływu na politykę innych podmiotów stosunków

międzynarodowych w celu realizacji własnych celów strategicznych. Termin potocznie rozumiany jest jako siła militarna, pozwalająca na odniesienie jednoznacznego zwycięstwa i pokonanie przeciwnika w potencjalnym konflikcie zbrojnym. Jednak możemy wyróżnić jeszcze kilka elementów niezbędnych do zdefiniowania *hard power* – siłę ekonomiczną, zasoby naturalne, demografię, położenie geograficzne wraz z wielkością terytorium, możliwości technologiczno-gospodarcze. Elementy te definiują siłę państwa, jego potęgę oraz zdolności koalicyjne we współczesnym świecie. Jak zwraca uwagę Nye jr. w książce *The Future of Power*, nie istnieje jedna definicja *hard power*, przyjęta przez wszystkich badaczy – używane definicje dotyczą możliwości wprowadzania lub opierania się zmianom, inne natomiast wskazują na możliwość wejścia w posiadanie określonych zasobów (nie tylko materialnych).

Do instrumentarium *hard power* należy przede wszystkim przymus, rozumiany nie tylko jako zastosowanie lub groźba zastosowania siły militarnej, ale także użycie np. środków ekonomicznych (sankcje, cła i inne narzędzia → w o j n y [t. 4] handlowej). Stosowanie siły militarnej należy określić jako radykalną wersję *hard power*.

Wśród uczestników stosunków międzynarodowych trwa nieprzerwana rozgrywka o dominację – lokalną, regionalną czy też światową. Jak zauważa Kleinowski, państwo może wybrać dominujący charakter swojej aktywności na arenie międzynarodowej – może to być współpraca, rywalizacja lub walka. Wybór konkretnej ścieżki zdeterminuje, w jakim stopniu potrzebna jest twarda siła dla realizacji celów i obrony własnych interesów. W sytuacji wyboru współpracy jako dominującego charakteru aktywności państwo w małym stopniu będzie polegać na sile militarnej, w większym natomiast na elementach podnoszących możliwość kooperacji i wspólnego rozwiązywania problemów. Jednak wybierając rywalizację, a w skrajnych przypadkach walkę, państwo w znaczącym stopniu będzie musiało oprzeć się na twardej sile. Można dodatkowo założyć, że państwo posiadające strategiczne złoża surowców naturalnych również będzie musiało oprzeć się na *hard power* w celu stworzenia warunków do obrony terytorium przed potencjalnym atakiem z zewnątrz. Budowanie potęgi państwa rywalizującego będzie się opierać głównie na zasobach naturalnych, położeniu i wielkości terytorium, poziomie rozwoju technicznego

oraz sile demograficzno-ekonomicznej. Ma to zapewnić realizację własnych celów nawet kosztem innych podmiotów stosunków międzynarodowych.

Podział pomiędzy twardą i miękką siłą jest nieostry. Granica między stosowaniem instrumentów należących do tych kategorii jest płynna. Często mamy też do czynienia z przechodzeniem od *hard power* do *soft power* i odwrotnie lub z ich łącznym stosowaniem (np. kampania militarna sprzęgnięta z kampanią propagandową).

Przykładem państwa mającego mocno rozwinięty potencjał w dziedzinie twardej siły są USA, których możliwości w zakresie wywierania nacisku wykraczają daleko poza ramy militarne – jest to największa nominalnie gospodarka na świecie: PKB na poziomie ok. 20 bln USD (ok. 25% światowej gospodarki), wydatki na zbrojenia sięgające 650 mld USD rocznie (ok. 35% wydatków światowych i ok. trzykrotnie więcej niż drugie państwo w rankingu – Chiny, które wg szacunków Stockholm International Peace Research Institute [SIPRI] w 2018 r. wydały na ten cel 250 mld USD; oficjalny budżet obronny Chin jest zauważalnie mniejszy). Stany Zjednoczone, choć nie są największym państwem na świecie pod względem demograficznym, mają ogromny potencjał gospodarczy/finansowy oraz militarny, które niewątpliwe wzmacniają amerykańską politykę zagraniczną poprzez znaczące wywieranie wpływu czy to na własnych sojuszników, czy konkurentów. Posiadanie dobrze rozwiniętej twardej siły to nie tylko możliwości ofensywne lub defensywne w aspekcie czysto militarnym, które odstraszają potencjalnych agresorów. To również umiejętne uzależnienie od własnych możliwości gospodarczych innych podmiotów, które mogą zostać w późniejszym czasie zmuszone do realizacji celów silniejszego partnera w zamian za nieprzerwane dostawy dóbr. Chociaż, jak zaznacza L. Pastusiak, na bazie amerykańskich doświadczeń historycznych można zauważyć, że użycie *hard power* nie zawsze gwarantuje sukces, to jednak wciąż ma ono swoich zwolenników wśród amerykańskich polityków głoszących tezę o szybszym osiąganiu celów politycznych przy zastosowaniu twardej siły.

Rafał Kopeć, Maciej Kulczycki

R. Keohane, J.S. Nye jr., *Power and Independence in the Information Age*, „Foreign Affairs" 1998, vol. 77 (5); M. Kleinowski, *Czynniki budujące siłę i potęgę państwa*

na arenie międzynarodowej, [w:] *Świat Idei i Polityki*, J. Waskan (red.), Wydawnictwo Adam Marszałek, Toruń 2010; R. Kopeć, *Hard power*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J.S. Nye jr., *Bound to Lead: The Changing Nature of American Power*, Basic Books, New York 1991; tenże, *Przyszłość siły*, tłum. B. Działoszyński, Wydawnictwo Naukowe PWN, Warszawa 2012; tenże, *Soft Power. Jak osiągnąć sukces w polityce światowej*, tłum. J. Zaborowski, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2007; L. Pastusiak, *Trzy rodzaje siły w polityce USA*, 11.03.2017, PrzegladDziennikarski.pl (dostęp 28.04.2019); J. Sadłocha, *Pomiędzy miękką a twardą siłą*, „Wrocławskie Studia Politologiczne" 2012, nr 13.

HEALTHIZM – system przekonań, w którym zdrowie postrzegane jest jako własność i odpowiedzialność jednostki, stawia na pierwszym miejscu osobiste dążenie do zdrowia ponad wszystko inne; to również nadmierna, obsesyjna troska o zdrowie, zjawisko obserwowane w ciągu ostatnich dekad w społeczeństwach krajów zachodnich. Jest szczególnym rodzajem koncentracji na zdrowiu jako wartości zależnej od jednostki i jej poczynań, które stanowi podstawę definiowania i osiągania dobrostanu, a jednostka może je sobie zapewnić przez zmianę stylu życia.

Kluczowa dla ideologii healthizmu jest koncepcja odpowiedzialności indywidualnej, czyli poglądu, wg którego zdrowie jednostki zależy od podejmowanych przez nią starań. Po raz pierwszy terminu *healthism* w 1980 r. użył R. Crawford i zdefiniował go jako „zajęcie się zdrowiem osobistym, nacisk na określenie i osiągnięcie dobrego samopoczucia; cel, który należy osiągnąć przede wszystkim poprzez zmianę stylu życia". Dotyczył nowej świadomości zdrowotnej Amerykanów opierającej się głównie na rosnącym zainteresowaniu własnym zdrowiem, budzenia się kultury zdrowego trybu życia, a także rosnącego przekonania o osobistej odpowiedzialności za zdrowie, poglądu, wg którego troska o zdrowie staje się nadrzędną ideą kierującą życiem.

Fundamentem dla rozwoju healthizmu stały się postępujące procesy → m e d y k a l i z a c j i [t. 3] i nasilającego się kultu zdrowia, przenoszącego się z obszarów medycznych w obszary związane np. z edukacją prozdrowotną czy też tworzeniem się nowych grup społecznych. Rozwój internetu i budowanie wirtualnych społeczności znacznie ułatwiają propagowanie zdrowego stylu życia i kultu zdrowia. Współczesne wzorce

zachowań kreowane są często właśnie na podstawie ideologii. Ludzie wyznający healthizm uważają, że zdrowie jest ważniejsze niż inne wartości i jest celem samym w sobie, a nie środkiem do osiągania celów. Healthizm nie może być nazwany jedynie troską o zdrowie, ponieważ bardziej przypomina on uzależnienie i często również ciągnie za sobą negatywne skutki. Jest to ideologia osób traktujących ciało jako symbol będący wskaźnikiem zdrowia. Polega na przesadnym dbaniu o swoje zdrowie i zdrowe odżywianie się. Uzależnienie od zdrowia odsuwa na dalszy plan realizowanie i wypełnianie innych obowiązków życiowych, równoważnych z aspektem zdrowia.

W ideologii healthizmu zdrowie przyjmuje się za wartość autoteliczną i nadrzędną w stosunku do pozostałych. Pojęcie zdrowia staje się tym samym wartością aksjonormatywną, oznaczającą wprowadzenie do społeczeństwa określonych, akceptowalnych społecznie norm zachowań prozdrowotnych oraz krytykę zachowań negatywnie wpływających na zdrowie (jak np. nikotynizm), prowadzących do wykluczeń społecznych.

Przeciwnicy ideologii healthizmu odnoszą się głównie do kwestii wywierania presji na bycie zdrowym, upatrując wręcz w healthizmie → z a g r o ż e n i a [t. 4] o charakterze behawioralnym. Healthizm jest uznawany za formę medykalizacji, w pełni związaną z przenoszeniem troski o zdrowie we wszystkie obszary życia człowieka. Współczesny healthizm wzmocniony zostaje przez technologie, które często dzięki ubieralnym urządzeniom (ang. *wearable technologies*) umożliwiają jednostce dostęp do szeregu danych na temat swojego zdrowia. Medykalizacja mająca progresywny charakter często przenosi kwestie do tej pory zarezerwowane dla środowiska medycznego na grunt społeczny. Trafia ona do coraz szerszego grona odbiorców dzięki narzędziom umożliwiającym partycypację w badaniach medycznych. Dane te za pomocą aplikacji mobilnych jednostka może samodzielnie przetwarzać i analizować (ang. *self tracking*). Healthizm wraz z postępem technologicznym wciąż się rozwija i poszerza swój zakres.

Cezary Krawczyk, Edyta Sadowska

A. Borowiec, I. Lignowska, *Czy ideologia healthismu jest cechą dystynktywną klasy średniej w Polsce?*, „Kultura i Społeczeństwo" 2012, nr 3; R. Crawford, *Healthism*

and the Medicalization of Everyday Life, „International Journal of Health Services" 1980, vol. 10, no. 3; K. Dzwonkowska-Godula, *Stosunek młodych ludzi do własnego zdrowia a ideologia healthismu*, „Acta Universitatis Lodziensis. Folia Sociologica" 2016, nr 58; D. Lizak, M. Seń, M. Kochman, *Healthizm – afirmacja promocji zdrowia czy współczesne zagrożenia behawioralne*, [w:] *Człowiek w zdrowiu i chorobie. Promocja zdrowia. Leczenie i rehabilitacja*, R. Żarow (red.), Wydawnictwa Państwowej Wyższej Szkoły Zawodowej, Tarnów 2014; M. Pollan, *Unhappy Meals*, „New York Times Magazine" 28.01.2007; M. Wróblewski, *Nowe szaty healthismu. Self-tracking, neoliberalizm i kapitalizm kognitywny*, „Acta Universitatis Lodziensis. Folia Sociologica" 2016, nr 58.

HEJTING (z ang. *hate* – nienawiść, nienawidzić) – działanie/czynność określająca:

- krytykowanie kogoś lub czegoś najczęściej anonimowo lub pod pseudonimem;
- obraźliwe lub agresywne komentowanie w internecie lub wrogie i agresywne mówienie na jakiś temat lub o jakiejś osobie;
- obrażanie i wyśmiewanie, artykułowanie niechęci czy niekonstruktywne pomówienia;
- nawoływanie do nienawiści i dyskryminacja na tle religijnym, seksualnym lub politycznym.

Hejting to tak naprawdę nie nowe zjawisko, ale w czasach cyfrowych zyskujące zupełnie nową formę – to wszelkie formy uderzenia w kogoś lub coś, w większości pełne nienawiści, często artykułowane w sposób wulgarny, chamski, niepoparty żadnymi argumentami. Znaczeniowo najbliżej temu zjawisku jest „obelga", choć polega ona na używaniu słów nacechowanych emocjonalnie, obraźliwych, a hejtować można bez uciekania się do obelg. Hejting może być więc często wynikiem pewnej → a g r e s j i [t. 1], która rodzi się w człowieku, kiedy nie radzi sobie ze swoimi emocjami. Dotyczy nie tylko mowy nienawiści, ale też wszelkich rodzajów wypowiedzi agresywnych, przekraczających granice kultury i dobrego wychowania, których nie da się identyfikować jako mowy nienawiści.

Hejting jako forma dewiacyjnych zachowań podczas publicznych dyskusji internetowych (wynika z właściwości internetu, który umożliwił biernym odbiorcom stanie się równocześnie twórcami treści, szczególną rolę odgrywają tu → m e d i a s p o ł e c z n o ś c i o w e [t. 3], które

udostępniły potężne narzędzia do dystrybucji nienawiści – stały się mimowolnie rodzajem interfejsu do hejtu) może być skierowany zarówno do konkretnej osoby, jak i przedstawicieli danego narodu, płci, osób o innym światopoglądzie, wyznawców danej religii czy grupy politycznej, a nawet znajomych osoby hejtującej – obiektem hejtu może stać się każdy. Na hejt w internecie zdecydowanie najbardziej narażone są znane osoby, przede wszystkim politycy, a także reprezentanci niektórych grup społecznych (np. nauczyciele, przedsiębiorcy, bezrobotni itp.). Należy zauważyć, że zjawisko to odnosi się głównie do słownej agresji, krytyki i szeroko pojętej negacji mającej miejsce w stosunku do innych osób oraz ich działań, aczkolwiek może wystąpić pod postacią grafiki (memy, gify) czy filmu i w takich przypadkach łatwiej zapada w pamięć.

Hejter – jak czytamy w *Miejskim słowniku slangu i mowy potocznej*, tworzonym przez samych użytkowników – to zazdrosny koleś, który nie potrafi cieszyć się sukcesem kogoś innego, dlatego próbuje wytknąć mu jego wszystkie możliwe wady. To osoba zamieszczająca obraźliwe, agresywne, prowokacyjne lub skrajnie krytyczne komentarze w internecie, której brakuje pewności siebie, zdecydowania i pasji w życiu, dlatego swoją wartość opiera na deprecjonowaniu osiągnięć innych ludzi. Polski hejter – wg agencji badań rynku i opinii SW Research – to najczęściej mężczyzna (53% hejterów) w wieku od 16 do 24 lat (73%), który ma wykształcenie średnie ogólnokształcące (35%, tylko co piąty ma wykształcenie wyższe), mieszka na wsi lub w małym bądź średniej wielkości mieście i najchętniej hejtuje osoby publiczne.

Najczęściej obraźliwe komentarze piszą osoby sfrustrowane, dysponujące dużą ilością wolnego czasu albo silnie związane ze skrajnymi ruchami (radykalni narodowcy, członkowie ONR). Hejterami jednak mogą też być osoby, których nigdy byśmy nie posądzili o podobne zachowania, np. wykształceni, dobrze sytuowani trzydziestolatkowie czy dyrektorzy dużych korporacji z wieloma sukcesami na koncie. Internetowym hejterem może być każdy. Niewiele jest bowiem osób, które z ręką na sercu mogą powiedzieć, że nigdy nie zdarzył im się komentarz wykraczający poza normy kultury wypowiedzi.

Wśród hejterów obserwujemy także osoby znacznie mniej emocjonalne i bardziej profesjonalne. Ci tzw. profesjonalni hejterzy pozostają

w głębokim cieniu, a doprowadzone przez nich do perfekcji hejtowanie traktują jako zawód. Najczęściej są związani z agencjami świadczącymi usługi marketingu szeptanego oraz z wielkimi portalami poświęconymi różnorodnej tematyce. Podchodzą do hejtu instrumentalnie i traktują go oportunistycznie, zwracając uwagę nie na negatywne emocje jako takie, lecz na możliwość zarobku na nich.

Hejtujemy w internecie, gdyż:

- hejtowanie przynosi ulgę – perspektywa zhejtowania osoby, która najczęściej nie wyrządziła nam realnej krzywdy, ale np. śmiała mieć inne zdanie na jakiś temat, ładniej wyglądać, mieć więcej pieniędzy, wywołuje siłę, euforię, ulgę i poczucie sprawiedliwości (reaguje wtedy jądro ogoniaste, czyli część tzw. układu nagrody znajdującego się w mózgu);
- każdy jest zdolny do czynienia zła – gdy widzimy, że inni hejtują np. poprzez udostępnianie postu osoby hejtowanej, dołączamy do nich, mimo że w oderwaniu od grupy innych internautów sami takiej treści byśmy nie stworzyli ani jej nie przekazywali dalej;
- internet umożliwia rozpowszechnianie nienawistnych treści w sposób szybki, ale jednocześnie anonimowy i niebezpośredni – nie „prosto w twarz";
- osoby, które hejtują, posługują się uproszczonymi schematami myślowymi – kieruje nimi strach przed innością religijną, kulturową, seksualną oraz poczucie →zagrożenia [t. 4] i krzywdy wywołane obecnością „obcych";
- czujemy zazdrość, niezadowolenie ze swojej sytuacji życiowej, targają nami przykre doświadczenia.

Konsekwencje hejtu mogą być ogromne, a mianowicie w przypadku ofiar tego zjawiska mogą doprowadzić do:

- obniżenia poczucia własnej wartości;
- mniejszej odporności na czytane w internecie treści i przekonania, że stawianie oporu nie ma sensu;
- bezsenności, życia w ciągłym stresie, obawy przed wyrażaniem własnego zdanie w sieci;
- izolowania się od reszty społeczeństwa, nerwicy, depresji, prób samobójczych.

Walcząc z hejtem, przede wszystkim należy unikać czytania negatywnych opinii, a zwłaszcza odpowiadania na nie. Kolejnym wyjściem jest zgłoszenie hejtu administratorowi danej strony, który nie tylko może usunąć konkretny komentarz, ale i zablokować konto danej osoby. Ważna jest również profilaktyka – prowadzonych jest wiele akcji społecznych, warsztatów z zakresu →przemocy [t. 3] w internecie, skierowanych przede wszystkim do młodzieży (m.in. #jestnaswiecej, HejtSTOP, Przytul Hejtera, #TrollingIsUgly, Nie ma zgody dla tej mowy).

Zamieszczanie obraźliwych lub agresywnych komentarzy w internecie wbrew pozorom nie jest bezkarne. Konsekwencje prawne takiego zachowania mogą okazać się dla sprawcy bardzo dotkliwe. Grozi za nie kara grzywny, ograniczenia, a nawet pozbawienia wolności. Należy pamiętać, że wg kodeksu karnego ścigane są zniesławienie i znieważenie innej osoby, propagowanie →faszyzmu i →totalitaryzmu [t. 4], znieważenie grupy lub osoby z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo jej bezwyznaniowości oraz znieważenie narodu lub Rzeczpospolitej. Wobec powyższego za zniesławienie i zniewagę w internecie można otrzymać karę grzywny lub usłyszeć wyrok ograniczenia lub pozbawienia wolności do roku. Za nawoływanie do nienawiści i dyskryminacji również grozi kara grzywny, ograniczenia wolności lub jej pozbawienia do lat 2.

Ponadto ofiara hejtu może z własnej inicjatywy wnieść pozew o naruszenie jej dóbr osobistych przez hejtera (warto zrobić zrzut ekranu i załączyć go do zawiadomienia, które należy złożyć w wybranej jednostce →Policji [t. 3] lub →Prokuratury [t. 3]). Dobra osobiste, które najczęściej narusza hejter, dotyczą dobrego imienia, czci, godności lub nazwy firmy (jeżeli atak kierowany jest przeciwko firmie). Naruszenie któregoś z dóbr powoduje, że mamy prawo do ich obrony oraz usunięcia zaistniałych negatywnych konsekwencji, np. zaniechania określonego działania czy zadośćuczynienia pieniężnego na swoją rzecz.

Emilia Musiał

J. Bralczyk, *Hejtować*, 7.04.2014, Wyborcza.pl (dostęp 14.01.2020); A. Gawenda, *Hejt jako przejaw patologicznych zachowań i konsekwencja rozwoju technologicznego*, „Bezpieczeństwo Obronność Socjologia" 2018, nr 9/10; K. Gawrol, *Hejt*

w Internecie – analiza zjawiska, „Edukacja – Technika – Informatyka" 2016, nr 4; M. Juza, *Hejterstwo w komunikacji internetowej: charakterystyka zjawiska, przyczyny i sposoby przeciwdziałania*, „Profilaktyka Społeczna i Resocjalizacja" 2015, nr 25; J. Kuś, *Nowe imię nienawiści: hejt*, SWPS.pl (dostęp 14.01.2020); Miejski.pl (dostęp 14.01.2020); E. Musiał, *Hejt*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; NoweWyrazy.uw.edu.pl (dostęp 14.01.2020); K. Rosińska, *Zjawisko hejtingu wśród młodzieży oraz sposoby przeciwdziałania*, „Kultura – Media – Teologia" 2017, nr 29; SJP.pl (dostęp 14.01.2020); S. Stasiewicz, *Hejt – zło odwieczne czy kulturowy nowotwór?*, [w:] *Hejterstwo. Nowa praktyka kulturowa? Geneza, przypadki, diagnozy*, J. Dynkowska i in. (red.), Wydawnictwo UŁ, Łódź 2017; S. Urbańczyk, *Encyklopedia języka polskiego*, Wydawnictwo Ossolineum, Wrocław–Warszawa–Kraków 1991.

HOLOKAUST (z gr. *holokaustos* – dosłownie całopalenie, ofiara całopalna, hebr. שואה, Szoa – „całkowita zagłada, zniszczenie", „katastrofa") – →ludobójstwo [t. 3] dokonane w czasie II wojny światowej przez III Rzeszę Niemiecką na większości europejskich Żydów. Pojęcie czasem błędnie używane jako nazwa dla innych ludobójczych akcji wymierzonych przeciwko innym narodom czy grupom (np. „Holokaust Romów").

Termin Holokaust, ze względu na kwestionowanie go współcześnie przez wielu badaczy, którzy interpretują „całopalenie" jako męczeństwo, ofiarę, zastępowany jest przez wspomniane słowo Szoa, Zagłada, które ma jednoznaczny wydźwięk. Wśród Żydów posługujących się językiem jidysz używany jest także termin *Hurban* (lub *Churban*), oznaczający zniszczenie, katastrofę, a historycznie związany ze zniszczeniem Świątyni Jerozolimskiej (w 586 r. p.n.e. i w 70 r. n.e.).

Zagłada Żydów składała się z kilku etapów. Pierwszym z nich było wprowadzenie paragrafów aryjskich (aktów prawnych ogłoszonych w III Rzeszy w kwietniu 1933 r., wykluczających „nie-Aryjczyków", tzn. Żydów, z uczestnictwa w życiu społecznym – zabraniających przynależności do partii politycznych, udziału w instytucjach gospodarczych, członkostwa w stowarzyszeniach akademickich, związkach sportowych itd.; paragrafy te stosowane były jako *numerus clausus* także w Rumunii, na Węgrzech i Słowacji jako regulacje państwowe; w Polsce lat 1935–1939 proponowane były jako skutek wpływu →faszyzmu niemieckiego przez ugrupowania

nacjonalistyczne, m.in. ONR, OZON, przez niektóre organizacje gospodarcze, izby adwokackie, a uczelnie wyższe również stosowały je w postaci getta ławkowego) oraz ustaw norymberskich (państwowych przepisów prawnych, które skierowane były przeciw niemieckim Żydom; 15 września 1935 r. Reichstag uchwalił ustawę o obywatelstwie Rzeszy oraz ustawę o ochronie krwi i czci niemieckiej), w których zdefiniowano i określono „Żyda" (zgodnie z zarządzeniem wykonawczym do ustaw norymberskich z 15 listopada 1939 r. Żydem był każdy, kto miał min. troje dziadków Żydów, ale „żydowskość" dziadków stwierdzana była na podstawie przynależności do gminy wyznaniowej, zatem przyjmowano kryterium religijne, a nie, jak zakładano, rasowe).

Drugim etapem było wprowadzenie oznakowania ludności żydowskiej, np. poprzez noszenie opasek żydowskich – np. w Generalnej Guberni (GG) ów nakaz dotyczył wszystkich Żydów powyżej 12. roku życia, którzy od 1 grudnia 1939 r. byli zobligowani do noszenia opasek na prawym ramieniu, które zawsze charakteryzowały się znakiem gwiazdy Dawida, ale miały różne kolory i rozmiary.

Trzecim etapem były wywłaszczenia, zapoczątkowane przez noc kryształową (niem. *Kristallnacht*), tj. pogrom ludności żydowskiej w Niemczech, przeprowadzony w nocy z 9 na 10 listopada 1938 r., połączony z grabieżą mienia tej ludności. Pretekstem dla akcji było zabójstwo dyplomaty ambasady niemieckiej we Francji, dokonane przez H. Grynszpana. Noc kryształowa została zorganizowana na polecenie szefa Głównego Urzędu Bezpieczeństwa Rzeszy (RSHA) R. Heydricha przez Gestapo i → p o l i c j ę [t. 3]. W jej wyniku zabito 91 niemieckich Żydów, a 20 tys. wysłano do obozów koncentracyjnych. Dokonano również profanacji i zniszczono 101 synagog, a 76 zostało zburzonych. Zdewastowano 7,5 tys. sklepów, a na Żydów nałożono kontrybucję, która miała być karą za zabójstwo dyplomaty, odszkodowania od ubezpieczycieli przejął Tamilijskimi Tygrysami aparat państwowy.

Kolejnym etapem była koncentracja ludności oraz uśmiercanie jej. Jeśli chodzi o pierwszy element tego etapu, był on częścią eksterminacji pośredniej (np. skupianie Żydów w gettach; które, jak się ocenia, pochłonęło ok. 500 tys. żydowskich istnień), czyli pierwszego z 2 etapów (obok eksterminacji bezpośredniej) hitlerowskiej polityki eksterminacyjnej. Polityka ta

stosowana była wobec ludności żydowskiej, która znalazła się na terenach Polski. Niemcy widzieli tutaj możliwość przeprowadzenia swoich zamierzeń na jednym terenie, ze względu na liczącą ok. 3 mln społeczność polskich Żydów oraz sytuację wojenną, która dawała na ziemiach polskich możliwość zrealizowania zamierzeń ideologii rasistowskiej. Początkowe założenia, sygnowane przez Heydricha, z września 1939 r. mówiły o natychmiastowej koncentracji wszystkich polskich Żydów, stopniowo także z innych terenów, ewentualnej ich emigracji (np. na Madagaskar, gdzie zakładano stworzenie „Wielkiego Getta" dla 4 mln Żydów), dobrowolnej lub przymusowej, a później o koncentracji w jednym określonym miejscu, nazywanym rezerwatem. Dopiero w połowie 1940 r. zaczęto mówić o wykorzystaniu żydowskiej siły roboczej dla III Rzeszy. To dało początek włączeniu administracji cywilnej w nadzór nad pracą przymusową i tworzeniem szopów (niemieckich manufaktur, powoływanych do życia w ramach organizacji produkcji, np. w getcie warszawskim). Upadek koncepcji emigracyjnej oraz stworzenia rezerwatu, a także niemożność tworzenia gett na obszarach zajętych po ataku Niemiec na Związek Radziecki oraz skutki masowych egzekucji dokonywanych przez Einsatzgruppen spowodowały kolejny etap Zagłady, eksterminację bezpośrednią.

Jej początek datuje się na lato 1941 r. Prawdopodobnie na ustny rozkaz A. Hitlera przystąpiono do tzw. ostatecznego rozwiązania czy też „ostatecznego rozwiązania kwestii żydowskiej" (niem. *Endlösung der Judenfrage*), określanego też jako „całościowe rozwiązanie" – kryptonimu niemieckiego programu wymordowania Żydów europejskich. Pisemne rozkazy wychodziły od H. Göringa i H. Himmlera bezpośrednio do Heydricha, a później do E. Kaltenbrunnera. Na wydanie rozkazu wymordowania wszystkich Żydów wpłynęła bezpośrednio eskalacja działań Einsatzgruppen, istnienie systemu obozów koncentracyjnych, skuteczność programu eutanazji (np. z wykorzystaniem Cyklonu B), praktyka w organizacji → d e p o r t a c j i dużych grup ludzi, a także świetnie działająca niemiecka administracja. Za początek ostatecznego rozwiązania przyjmuje się masowe egzekucje Żydów w Wilnie i Rydze, a także uruchomienie na przełomie 1941 i 1942 r. ośrodków zagłady w Chełmnie (niem. Kulmhof) i Bełżcu oraz dokonywanie mordów na Wschodzie, gdzie uśmiercano transporty Żydów z III Rzeszy i Protektoratu Czech i Moraw.

Chełmno nad Nerem było pierwszym niemieckim ośrodkiem zagłady, utworzonym bezpośrednio przed podjęciem decyzji o planie „ostatecznego rozwiązania". Obóz działał w 2 etapach, od 8 grudnia 1941 r. do 11 kwietnia 1943 r. i od 26 czerwca do 14 lipca 1944 r., a ludobójstwa dokonywano w nim w ciężarówkach pełniących funkcję komór gazowych, do których gaz dostawał się przez rurę wydechową skierowaną do wnętrza samochodu. Dziennie mordowano w nim ok. 700–1000 osób, ogółem zamordowano w nim 180–200 tys. Żydów z Polski oraz Niemiec, Austrii, Czech i Luksemburga, a także ok. 4 tys. Romów. Zamordowano tam także Polaków i sowieckich jeńców wojennych. Proces uśmiercania trwał ok. 10 min. W Bełżcu między 17 marca a czerwcem 1943 r. działał niemiecki ośrodek zagłady, stworzony początkowo „tylko" dla polskich Żydów (akcja Reinhardt). Ludobójstwa dokonywano w nim w komorach gazowych zasilanych silnikami diesla. Komory umiejscowione były w barakach z podwójną, izolowaną warstwą piasku ścianą. Proces uśmiercania w komorach w Bełżcu trwał ok. 30 min. Liczbę tamtejszych ofiar ocenia się na ok. 600 tys. Żydów z Polski, Niemiec, Austrii, Czechosłowacji i kilka tysięcy Romów. Po ekshumacji zwłok i ich spaleniu, na specjalnie do tego przygotowanych rusztach z szyn kolejowych, zlikwidowano pozostałości po ośrodku, zacierając wszelkie ślady jego istnienia.

Decyzje dotyczące realizacji „ostatecznego rozwiązania" zostały podjęte mimo wielu okoliczności utrudniających te plany, ale i przy braku oporu i sprzeciwu w krajach przez Niemcy okupowanych oraz w państwach wolnych, a także wśród społeczeństwa niemieckiego. Przypieczętowane zostały i wstępnie ustalone w styczniu 1942 r., podczas konferencji w Wannsee. Głównymi etapami „ostatecznego rozwiązania" było: wymordowanie Żydów z GG (akcja Reinhardt), później pozostałych Żydów z okupowanych krajów w Europie, a ostatnim zgładzenie Żydów węgierskich (ponad 434 tys.) latem 1944 r., w ostatnim jeszcze wówczas działającym ośrodku zagłady, Oświęcim II-Brzezinka (niem. Auschwitz II-Birkenau). Był to największy z niemieckich ośrodków zagłady, wchodzący w skład obozu koncentracyjnego KL Auschwitz-Birkenau, który w 1944 r., a więc w szczytowym okresie, składał się z 3 części: Auschwitz I, Auschwitz II-Birkenau, Auschwitz III, przy czym cały kompleks obozów Auschwitz składał się z 40 obozów i podobozów. Oświęcim II-Brzezinka był największy

z części KL Auschwitz-Birkenau, znajdował się na terenie wsi Brzezinka, w całości zaadaptowanej na potrzeby obozu. Działał między marcem 1942 i październikiem 1944 r. Decyzja o jego powstaniu podjęta została przez Himmlera, wydana ustnie i w tajemnicy R. Hessowi, komendantowi obozu w Oświęcimiu latem 1941 r. W trakcie wizyty A. Eichmanna ustalono sposób mordowania zgromadzonych ofiar. Pierwotnie była to komora gazowa umiejscowiona w zagrodzie chłopskiej za lasem. Ale jeszcze w 1941 r. zbudowano nowe komory gazowe. W obozie zginęło ok. 90% wszystkich ofiar KL Auschwitz, ok. 1 mln ludzi. Ponad 90% z nich to Żydzi, ok. 70 tys. to Polacy, a 20 tys. Cyganie, Romowie oraz inni, tacy jak jeńcy radzieccy i inni więźniowie różnych narodowości. Ludobójstwo dokonywane było więc nie tylko w ośrodkach (obozach zagłady), ale także w obozach koncentracyjnych (niem. *Konzentrationslagers*, KZ), które definiowane są nie tylko jako miejsca odosobnienia, niewolniczej pracy, ale i masowej zagłady, zarówno mieszkańców nazistowskich Niemiec, jak i krajów przez nie okupowanych. Za działanie i organizację obozów odpowiadało SS (niem. Schutzstaffel der NSDAP). Termin KZ określa zatem wszystkie obozy niemieckie, tzn. pracy przymusowej, przejściowe, które administrowane były przez Sipo (niem. Sicherheitspolizei, policję bezpieczeństwa), ale i przedsiębiorstwa prywatne. W tej kategorii mieszczą się także obozy jeńców wojennych (zarządzane przez Wehrmacht) i ośrodki zagłady, mimo że nie były one obozami koncentracyjnymi *sensu stricto*, natomiast niektóre obozy koncentracyjne pełniły funkcję ośrodków zagłady.

Po stłumieniu buntu żydowskich więźniów z Sonderkommando w Oświęcimiu 7 października 1944 r. udało im się podpalić i uszkodzić jedno krematorium, ale śmierć podczas pościgu poniosła cała 250-osobowa grupa, w wyniku represji ukarano śmiercią kolejnych 200 więźniów z Sonderkommando oraz 4 Żydówki, które kradły i dostarczały buntownikom materiał wybuchowy z zakładów zbrojeniowych Union-Werke). Himmler wydał rozkaz zatrzymania procesu ludobójstwa na Żydach. W wyniku tej decyzji rozebrano także komory gazowe i zniszczono krematoria. W trakcie całego programu „ostatecznego rozwiązania" Niemcy zamordowali, w większości na terenach ziem polskich, gdzie tworzyli wcześniej ośrodki zagłady, ok. 6 mln Żydów z wielu europejskich krajów. O takiej liczbie Żydów mówi się też, kiedy mowa o ofiarach całego Holokaustu/Zagłady.

Podkreślić tutaj trzeba, że większość ofiar tego ludobójstwa stanowili polscy Żydzi, a proceder odbywał się głównie na terenach Polski pod niemiecką okupacją.

Katarzyna Pabis-Cisowska

M. Adamczyk-Grabowska, H. Duda, *Terminy Holokaust, Zagłada i Szoa oraz ich konotacje leksykalno-kulturowe w polszczyźnie potocznej i dyskursie naukowym*, [w:] *Żydzi i judaizm we współczesnych badaniach polskich*, t. III, K. Pilarczyk (red.), Wydawnictwo Antykwa, Kraków 2003; Auschwitz.org (dostęp 14.01.2020); *Holokaust: lekcja historii: zagłada żydów w edukacji szkolnej*, J. Chrobaczyński, P. Trojański (red.), Wydawnictwo Naukowe Akademii Pedagogicznej, Warszawa 2004; Jewish Historical Institute, *Polski słownik judaistyczny*, JHI.pl/PSJ/ (dostęp 14.01.2020); T. Snyder, *Czarna ziemia. Holokaust jako ostrzeżenie*, Wydawnictwo Znak, Kraków 2015; R. Szuchta, *Zrozumieć Holokaust: książka pomocnicza do nauczania o zagładzie Żydów*, Ośrodek Rozwoju Edukacji, Warszawa 2012; R. Szuchta, P. Trojański, *Holokaust: zrozumieć dlaczego*, Oficyna Wydawnicza „Mówią wieki", Warszawa 2003; A. Ubertowska, *Holokaust: auto (tanato) grafie*, Instytut Badań Literackich PAN, Warszawa 2014; A. Żbikowski, *Żydzi, antysemityzm, holokaust*, Wydawnictwo Dolnośląskie, Wrocław 2001.

HOŁODOMOR (ukr. Голодомор; Wielki Głód w Ukrainie) – masowa śmierć ludzi z głodu w ZSRR (głównie w Ukraińskiej SRR), spowodowana umyślnymi działaniami Stalina i władz ZSRR i skierowana na →ludobójstwo [t. 3] rdzennej ludności. Najbardziej znanym i uznanym na całym świecie głodem jest masowe wymieranie Ukraińców w latach 1932–1933. Termin jest używany w przypadku klęsk głodu w latach 1921–1923 i 1946–1947. Sztucznie wywołana klęska głodu w latach 1932–1933 zabiła miliony Ukraińców. Jest również znany jako terror głodem oraz ludobójstwo głodem Ukraińców. Od 2006 r. Hołodomor jest uznawany przez Ukrainę i 15 innych krajów za ludobójstwo narodu ukraińskiego dokonane przez rząd radziecki.

Termin podkreśla celowość wywołania klęski głodu, której zamierzenie wyrażało się poprzez odrzucenie pomocy humanitarnej z zewnątrz, konfiskatę wszystkich artykułów gospodarstwa domowego i ograniczenie przemieszczania się ludności. To, czy Hołodomor był ludobójstwem, wciąż jest przedmiotem debaty akademickiej, podobnie jak przyczyny

głodu i liczba zmarłych. Niektórzy uczeni uważają, że głód został zaplanowany przez J. Stalina w celu wyeliminowania ukraińskiego ruchu niepodległościowego. Pod względem liczby ofiar Wielki Głód porównuje się z →Holokaustem.

Wczesne szacunki liczby ofiar śmiertelnych badaczy i urzędników państwowych były bardzo zróżnicowane: uważano, że w wyniku głodu zginęło od 3,5 do 10 mln etnicznych Ukraińców. ONZ we wspólnym oświadczeniu podpisanym przez 25 krajów w 2003 r. stwierdziło, że zginęło 7–10 mln osób. Od tego czasu badania zawęziły szacunki do 3,3–7,5 mln ofiar. Według ustaleń Sądu Apelacyjnego w Kijowie z 2010 r. straty demograficzne spowodowane głodem wyniosły 10 mln, 3,9 mln bezpośrednich zgonów z głodu i dalszych 6,1 mln deficytów urodzeniowych.

W pamięci Ukraińców i innych narodów Hołodomor w latach 1932–1933 w Ukrainie na zawsze pozostanie jedną z najokropniejszych tragedii XX w. Hołodomor jest faktem historycznym, który miał miejsce w określonym czasie, w określonym miejscu i był rezultatem działania konkretnych ludzi.

Od 2018 r. Hołodomor jest uznawany za ludobójstwo narodu ukraińskiego w 24 krajach świata, fakt ludobójstwa jest bezdyskusyjny i uznany przez społeczność międzynarodową, w tym także państwo polskie. Inaczej w Rosji, gdzie tematyka Hołodomoru nie istnieje, a przypomnienie o tej stalinowskiej polityce ludobójstwa jest ocenianie jako wroga agitacja. Za →zbrodnię przeciwko ludzkości [t. 4] uznały Wielki Głód Zgromadzenie Ogólne ONZ (listopad 2003 r.), Parlament Europejski (23 grudnia 2008 r.) i Zgromadzenie Parlamentarne Rady Europy (28 kwietnia 2010 r.). W 2016 r. Parlament Ukrainy zaapelował do państw demokratycznych z prośbą uznania Wielkiego Głodu w latach 1932–1933 za ludobójstwo narodu ukraińskiego. 20 września 2017 r. prezydent Ukrainy P. Poroszenko zaapelował na 72. sesji Zgromadzenia Ogólnego ONZ w Nowym Jorku o powszechne, ogólnoświatowe uznanie Hołodomoru za ludobójstwo dokonane na narodzie ukraińskim.

W 85. rocznicę Wielkiego Głodu w Ukrainie Senat USA uznał go za ludobójstwo. Rezolucja w tej sprawie jest pierwszym w historii aktem prawnym Kongresu USA poświęconym tej tragedii. Do dokumentu dołączono wnioski w sprawie Głodu w Ukrainie (z 22 kwietnia 1988 r.) mówiące

o tym, że Stalin i jego otoczenie dokonali w latach 1932–1933 zbrodni ludobójstwa na narodzie ukraińskim. W przyjętej rezolucji potępiono systematyczne łamanie przez sowieckie rządy → p r a w c z ł o w i e k a [t. 3], w tym prawa do samookreślenia i wolności słowa w Ukrainie.

24 listopada 2018 r., w 85. rocznicę Hołodomoru, Ukraińcy na całym świecie zapalili świeczki jako symbol pamięci o najstraszliwszej tragedii w historii Ukrainy, która pochłonęła miliony niewinnych istnień. Były to ofiary Hołodomoru z lat 1932–1933, głodu wywołanego przez człowieka, zaplanowanego i wdrożonego przez komunistów i → r e ż i m [t. 3] Stalina. Przez dziesięciolecia ten przerażający akt nieludzkości i ogromna narodowa tragedia była utrzymywana w tajemnicy przez Związek Radziecki oraz stanowczo zaprzeczał jej reżim komunistyczny. Miliony ludzi, głównie chłopi – kręgosłup ukraińskiej tożsamości, kultury i tradycji – w ciągu 2 lat zostały dosłownie zagłodzone na śmierć przez politykę stalinowskiego reżimu, który dążył do rozwiązania kwestii ukraińskiej. Wyniki prac przeprowadzonych w Ukrainie świadczą, że 93% ze wszystkich ofiar było mieszkańcami wsi. W czasie Wielkiego Głodu Związek Radziecki sprzedał 1,7 mln ton zboża na rynkach zachodnich.

W okresie istnienia ZSRR przez Ukrainę przetoczyły się aż 3 fale głodu – tuż po rewolucji bolszewickiej, w latach 1921–1923, w latach 1932–1933 i po II wojnie światowej w latach 1946–1947. Pierwsza klęska głodu w Ukrainie w latach 1921–1923, podobnie jak 2 późniejsze, była efektem polityczno-ideologicznych decyzji bolszewików, którzy z jednej strony chcieli „spacyfikować" niepokornych Ukraińców, a z drugiej zdobyć pieniądze pozwalające zainstalować na całym świecie komunizm. Owa „pacyfikacja" nie była niczym innym jak morderczym terrorem. Jego celem było zniszczenie w zarodku ukraińskich aspiracji narodowo-niepodległościowych. Bolszewicy uznali, że wsadzanie do więzień, przymusowa praca, publiczne egzekucje i masowa konfiskata produktów rolnych przekona Ukraińców do → k o m u n i z m u i zatrzyma wszelki opór przeciwko nowej władzy, a co najważniejsze, wyeliminuje ze społeczeństwa ludzi zamożnych.

Najtragiczniejszy w skutkach był jednak głód w latach 30., o którym nic nie mówiono, a był to akt ludobójstwa (genocyd) narodu ukraińskiego. Kolektywizacja ukraińskiego rolnictwa, rekwizycja żywności, akcje

represyjne, które miały stworzyć nowy ustrój rolny, wywołały masową klęskę głodu na najbardziej urodzajnych terenach Europy.

Wielki głód z lat 1932–1933 długo znajdował się wśród białych plam sowieckiej i ukraińskiej historii. Katastrofa ta nie była jednak podobna do innych klęsk głodu, była ona bezpośrednią konsekwencją nowego systemu wyzysku chłopstwa. W latach 1921–1922 władza sowiecka przyznała, że panuje głód, prosząc otwarcie o pomoc międzynarodową, jednak zaprzeczała klęsce lat 1932–1933 i zagłuszała → p r o p a g a n d ą [t. 3] głosy zagranicznej → o p i n i i p u b l i c z n e j [t. 3], zwracającej uwagę na tragedię.

Dla lepszego zrozumienia tego, czym był Hołodomor, należy podkreślić, że kiedy naukowcy mówią o Hołodomorze w latach 1932–1933, odnosi się to do okresu od kwietnia 1932 do listopada 1933 r. Właśnie w trakcie tych 17 miesięcy, ok. 500 dni, w Ukrainie zginęły miliony ludzi; liczby bezpośrednich i pośrednich ofiar Hołodomoru nie ma możliwości dokładnie wskazać. Między historykami wciąż toczy się debata, ile osób zginęło: 5, 7, 9 czy 10 mln ludzi, tak czy inaczej – co należy możliwie stanowczo podkreślić – mowa o milionach niewinnych ofiar. Jeśli wziąć pod uwagę straty pośrednie, np. dzieci, które nie urodziły się wskutek Hołodomoru, liczbę ofiar szacuje się na 14 mln.

Wielki Głód nastąpił w jednym z najżyźniejszych krajów Europy w czasie pokoju, podczas gdy ZSRR eksportował ogromne ilości zboża. W Ukrainie zboże, a następnie cała żywność, były konfiskowane przez władze. W 1932 r. w ZSRR wprowadzono prawo o ochronie własności państwowej, które pozwalało na rozstrzelanie człowieka nawet za zabranie tylko jednego kłosa z należącego do kołchozu pola. Obowiązywał także dekret o całkowitej blokadzie wsi z powodu rzekomego sabotowania obowiązkowych dostaw zbóż. Pragnąc przeżyć, wielu chłopów łamało zakaz opuszczania wsi i uciekało do miast, gdzie obowiązywały przydziały żywnościowe dla pracujących. Podejmowano próby ucieczki do Rosji, jednak ukraińskie granice administracyjne obstawione były przez wojsko. W ocenie historyków głód wywołano sztucznie, by złamać opór chłopstwa wobec kolektywizacji. W Ukrainie opór ten był największy.

Sowieckie władze starannie zacierały ślady ludobójstwa. GPU (Państwowy Zarząd Polityczny – sowiecka → p o l i c j a [t. 3] polityczna, następczyni utworzonej przez F. Dzierżyńskiego Czeki, a poprzedniczka NKWD)

zabraniała urzędnikom podawania głodu jako przyczyny zgonów. Gdy na wiosnę 1933 r. śmiertelność przybrała masowy charakter, zaniechano wystawiania aktów zgonu, a zmarłych po prostu zakopywano. W najgorszym okresie Wielkiego Głodu umierało 25 tys. ludzi dziennie, 1 tys. – co godzinę, 17 osób – co minutę. Głód pustoszył całe wsie. Zdarzały się liczne przypadki kanibalizmu. Szczególnie cierpiały dzieci: ocenia się, że 1/3 z nich straciła życie. Często rodzice, nie wytrzymując już męczenia głodem, zabijali siebie i swoje dzieci. Zginęli najbardziej uczciwi, pracowici ludzie. Zmieniły się i stosunki między ludźmi. Kiedy tylko głód się zaczął, chłopi pomagali sobie nawzajem, ale z jego nasileniem każdy myślał tylko o sobie, o tym, jak wyżyć.

W arsenale środków represji decydującą rolę odgrywało słynne prawo o ochronie własności państwowej ogłoszone 7 sierpnia 1932 r., a więc w najgorętszym momencie → w o j n y [t. 4] między chłopstwem a reżimem, które przewidywało 10 lat obozu lub karę śmierci „za wszelką kradzież lub roztrwonienie socjalistycznej własności". Termin wydania dekretu nie był przypadkowy. Miał przeciwdziałać próbom nielegalnego gromadzenia w czasie żniw zboża przez głodujące rodziny chłopskie. W obliczu zbliżającej się zimy ludzie – widząc, że plony w całości są wywożone do centralnych magazynów – pod osłoną nocy usiłowali zbierać na polu choćby kłosy. Prawo pozwalało rozstrzelać człowieka za zabranie kłosa z kołchozowego pola. Lud znał je pod nazwą „prawa o kłosach", gdyż skazani na jego podstawie winni byli najczęściej kradzieży kilku kłosów pszenicy lub żyta na kołchozowych polach. Nastąpiła fala migracji głodowych, na które władze odpowiedziały wprowadzeniem paszportów i zakazem podróży koleją.

Kolejnym posunięciem władz było odizolowanie obszarów wiejskich objętych głodem od reszty kraju. Prawną podstawą był tu dekret z 22 stycznia 1933 r., podpisany przez Stalina i Mołotowa, zobowiązujący lokalne władze i GPU do „całkowitego uniemożliwienia wyjazdów ludności wiejskiej z miejsca zamieszkania" z powodu rzekomego sabotowania obowiązkowych dostaw zbóż. W celu wykonania narzuconych, nierealnych norm produkcyjnych chłopom bezwzględnie rekwirowano zboże, nie pozostawiając ziarna na zasiew ani na mąkę. Na mocy tego dokumentu na terenach objętych głodem zakazano sprzedaży biletów kolejowych,

a na drogach ustawiono specjalne blokady i wojskowe posterunki zaporowe. Dzięki dokładnym kontrolom rekwirowano żywność wwożoną na tereny ogarnięte głodem. Cały obszar objęty był patrolami specjalnych oddziałów wojska i milicji uniemożliwiających wieśniakom ucieczkę z konających wsi. Władze zaprzeczały, że ludność w Ukrainie głoduje, a w tym samym czasie odmawiały przyjmowania pomocy z zagranicy.

Grozę tych danych potęguje fakt, że w 1933 r., w czasie, gdy z powodu głodu konały miliony mieszkańców Ukrainy, Związek Sowiecki wyeksportował na Zachód miliony ton zboża. Jak podaje rosyjski historyk R. Miedwiediew, z powodu → k r y z y s u ekonomicznego w Europie Zachodniej zboże to sprzedawano praktycznie za bezcen. Tymczasem nawet połowa zboża wyeksportowanego przez ZSRR w latach 1932–1933 wystarczyłaby do uratowania ludności Ukrainy od skutków głodu.

Wygrana bolszewików byłaby niemożliwa bez prasy. Za pieniądze niemieckiego Sztabu Generalnego powstało 75 gazet bolszewickich o łącznym nakładzie 600 tys. egz., które rozdawane były wśród → ż o ł n i e r z y [t. 4] i robotników. Nowy ustrój był, jak to określił A. Ossendowski, „dyktaturą dziennikarzy"; a dokładnie → p r z e m o c ą [t. 3] w służbie kłamstwa. „Naszą najważniejszą bronią jest druk" – stwierdził Stalin w 1921 r. Według większości dokumentów archiwalnych, *Wielkiej księgi wspomnień* i badań historyków Wielki Głód w Ukrainie był atakiem przede wszystkim na inteligencję i chłopstwo, w których to – zapewne słusznie – widziano zaplecze ukraińskiego ruchu niepodległościowego. Oprócz terroru głodu wobec Ukraińców stosowano masowe → d e p o r t a c j e, niszczenie inteligencji i indywidualne prześladowania, wyludnione wsie często zasiedlano przybyszami z Rosji.

Był to także skutek przebudowy wsi – niszczenie kułaków i chłopów indywidualnych, w większości dobrych gospodarzy, dzięki którym trzymała się wieś. Nowo organizowane kołchozy miały słabą wydajność, bo chłop nie był zainteresowany tym, by dobrze pracować na cudzej ziemi. Natomiast według planów partyjnych produkcja rolna miała rosnąć. To za zboże sprzedane na Zachód ZSRR kupował wszystko, co jest niezbędne dla wzrostu przemysłu ciężkiego. Ta hiperindustrializacja odbywała się kosztem wsi. Z chłopa Stalin wyciągał wszystko, aż do ostatniego ziarenka zboża. Stalin uruchomił swój plan przeciwko kułakom, lecz konsekwencje

dotknęły także ukraińską kulturę i duchowość, te najważniejsze wartości. Plan Wielkiego Głodu skierowano właśnie przeciwko chłopom ukraińskim, dlatego że to oni – 90% mieszkańców wsi było Ukraińcami – byli przedstawicielami tradycji i ducha narodu. Hołodomor złamał grzbiet etnosu, podcięto korzenie narodu ukraińskiego – eksterminując chłopów, niszcząc wieś, wyeliminowano tę warstwę, od której zależał rozwój społeczeństwa.

Skazanie na śmierć milionów ludzi na ziemiach słynących z urodzaju wymagało całego szeregu posunięć o charakterze prawno-organizacyjnym. Nie tak łatwo przecież zagłodzić mieszkańców obszarów, gdzie dosłownie każda uprawa przynosiła plony kilka razy bardziej obfite niż na innych terenach. Rosja zawsze patrzyła na Ukrainę tylko jak na kolonię, którą pod różnymi pretekstami można było nieustannie rabować, a właśnie głód bolszewicy uważali za najlepszą metodę zniszczenia pragnienia niezależności narodu Ukrainy. System totalitarny, który istniał za czasów ZSRR, podporządkował sobie wszystkie strefy życia społecznego.

O planowym charakterze Wielkiego Głodu świadczą kroki Kremla w przededniu masowego ludobójstwa – Stalin przygotowywał się do tej tragedii i próbował zapobiec rozpowszechnianiu → i n f o r m a c j i na jej temat: wzmocniono kontrolę graniczną, wysiedlano nielojalnych obywateli, wzmożono propagandę na Zachodzie, nastąpiły zmiany w polityce międzynarodowej, w tym podpisanie szeregu umów. Moskwa zorganizowała Wielki Głód i podjęła działania z wyprzedzeniem, aby zmniejszyć negatywne konsekwencje rozpowszechniania informacji o tragedii.

Ukrytym celem ludobójstwa w Ukrainie było zmniejszenie liczby Ukraińców, aby zasiedlić na ich miejscu ludzi z innych części ZSRR, a tym samym zabić wszelkie idee niepodległościowe.

Problem międzynarodowego uznania Wielkiego Głodu 1932–1933 w Ukrainie za ludobójstwo narodu ukraińskiego był istotny przez cały czas, poczynając od 1934 r., kiedy Kongres USA wezwał do potępienia tego aktu unicestwienia Ukraińców, a wiele krajów i instytucji oraz wielu badaczy poparły uznanie zbrodni Hołodomoru za skierowaną przeciwko narodowi ukraińskiemu.

Już R. Lemkin, autor terminu „ludobójstwo" i jeden z inicjatorów powstania prawnej definicji ludobójstwa, uważał głód w latach 1932–1933

w Ukrainie za klasyczny przykład sowieckiego ludobójstwa, najdłuższej i najszerszej próby rusyfikacji i zniszczenia narodu ukraińskiego. Był on pierwszym zachodnim naukowcem analizującym Wielki Głód w kontekście konwencji o ludobójstwie. Jak podkreślał profesor R. Serbin, Lemkin w 1953 r. wezwał ONZ „do uznania ZSRR i jego satelitów winnymi naruszenia konwencji o ludobójstwie poprzez planowaną kampanię na rzecz zniszczenia mniejszości za żelazną kurtyną". Jak twierdził Lemkin w tym samym roku w artykule *Investigation of Soviet Genocide by U.N.*:

> ironią historii jest to, że 8 milionów Ukraińców musiało zginąć z ludobójczego głodu, że tysiące Ukraińców musiało zostać zniszczonych w Winnicy, a niezliczona ilość ukraińskich kobiet i dzieci musiała być pochowana w kopalniach soli przed tym, jak sumienie świata zostało zszokowane.

Naród ukraiński był zbyt ludny, aby można go było całkowicie zniszczyć. Natomiast religijne, intelektualne i polityczne elity były raczej dość nieliczne i mogły być łatwo wyeliminowane, dlatego władza radziecka stosowała masową zagładę, deportację, pracę przymusową, wygnania i głód. Dopóki Ukraina – uważał Lemkin – zachowa swoją jedność narodową, swój język i kulturę, a Ukraińcy będą nadal uważać się za Ukraińców i szukać niepodległości, tak długo Ukraina będzie stanowić poważne →zagrożenie [t. 4] dla Sowietów. Nic dziwnego, że przywódcy komunistyczni przywiązywali największą wagę do rusyfikacji tego niezależnego narodu i postanowili go zmienić tak, aby pasował do ich wzoru jedynego narodu rosyjskiego. Ukrainiec nie jest i nigdy nie był Rosjaninem. Jego kultura, jego temperament, język, religia – wszystko jest inne. Ukraińcy odmówili Moskwie kolektywizacji, akceptując deportację, a nawet śmierć.

Lemkin uważał problem ludobójstwa za szerszy niż w przyjętej później definicji ONZ. W tekście *Radzieckie ludobójstwo w Ukrainie* przedstawił ukraińskie ludobójstwo jako sowiecką intencję zniszczenia narodu ukraińskiego w 4 etapach:

- Zniszczenie elity narodowej, czyli „mózgu" narodu, aby sparaliżować „ciało" narodu. Najistotniejsze uderzenie przeprowadzono w latach 1920, 1926 i 1932–1933, kiedy nauczyciele, pisarze, artyści, myśliciele,

przywódcy polityczni zostali zlikwidowani, uwięzieni lub deportowani. W 1931 r. na Syberię wysłano 51 713 intelektualistów. Przynajmniej 114 najwybitniejszych poetów, pisarzy i artystów, przywódców kulturalnych narodu, spotkał ten sam los. Ocenia się, że co najmniej 75% ukraińskich intelektualistów z Ukrainy Zachodniej, Karpat i Bukowiny zostało brutalnie eksterminowanych przez Rosjan.

- Zniszczenie Kościoła narodowego; ofensywa przeciwko Kościołom, kapłanom i hierarchii, likwidacja Ukraińskiego Autokefalicznego Kościoła Prawosławnego (UAKP) – „duszy Ukrainy". W latach 1926–1932 zlikwidowano UAKP, jego metropolitę i 10 tys. duchownych. W 1945 r., kiedy Sowieci zajęli Zachodnią Ukrainę, podobny los spotkał Ukraiński Kościół Katolicki. O tym, że rusyfikacja była jedynym problemem, wyraźnie świadczy fakt, że przed jego likwidacją Kościołowi zaoferowano możliwość przyłączenia się do patriarchy rosyjskiego w Moskwie, będącego politycznym narzędziem Kremla.
- Eksterminacja dużej części ukraińskich chłopów – strażników ukraińskiej kultury, języka, tradycji itp. Ukraińskie chłopstwo zostało złożone w ofierze celem utworzenia jednorodnego narodu radzieckiego.
- Kolonizacja Ukrainy przez inne grupy ludności, wymieszanie Ukraińców z innymi narodowościami poprzez przesiedlenia dla radykalnej zmiany składu ludności, rozproszenie narodu po całej Europie Wschodniej.

Jak podkreślał R.Lemkin, na wszystkich etapach zagłady Ukraińców decydujący był narodowy charakter operacji. Główne ofiary ludobójstwa – zagłodzeni na śmierć ukraińscy chłopi – zostały przedstawione jako repozytorium ducha narodowego i tych cech, które czynią ich „kulturą i narodem" (*that make them „a culture and a nation"*). Jak podkreśla Serbin, ta analiza 4-stopniowego zniszczenia narodu ukraińskiego jest głównym wkładem Lemkina w badania nad ukraińskim ludobójstwem. Podobne środki, wg Lemkina, zostały zastosowane wobec innych mniejszości narodowych Związku Radzieckiego. Środki te stały się elementem ekspansji imperium sowieckiego, ponieważ szybko zapewniły homogeniczność wieloetnicznej ludności Związku Radzieckiego.

Hołodomor 1932–1933 r. w Ukrainie wg Konwencji ONZ w sprawie zapobiegania i karania zbrodni ludobójstwa z dnia 9 grudnia 1948 r. nosi wszystkie oznaki genocydu jako działań będących próbą zniszczenia całkowicie lub częściowo grupy narodowej, etnicznej, rasowej lub religijnej.

W 1982 r. w Izraelu na konferencji międzynarodowej ws. Holokaustu i ludobójstwa mało znany wówczas badacz Harvard Ukrainian Research Institute James E. Mace był pierwszym spośród zachodnich historyków, który scharakteryzował Wielki Głód lat 1932–1933 w Ukrainie jako akt genocydu, celem którego była „likwidacja nacji ukraińskiej jako aktora politycznego i organizmu społecznego". Dopiero w 1983 r. milczenie dotyczące Wielkiego Głodu przerwali Amerykanie, powołując komisję specjalną Kongresu w celu zbadania zbrodni ludobójstwa i przyczyn głodu w Ukrainie w latach 1932–1933, wywołanego przez działania rządu radzieckiego. Deklaracją prezydenta USA 4 listopada 1984 r. oficjalnie stał Dniem Pamięci Wielkiego Głodu w Ukrainie w latach 1932–1933.

Wśród międzynarodowych aktów dotyczących Wielkiego Głodu w latach 1932–1933 jednym z pierwszych był Raport końcowy Międzynarodowej Komisji Śledczej Głodu z lat 1932–1933 w Ukrainie, utworzony 14 lutego 1988 r. z inicjatywy Światowego Kongresu Wolnych Ukraińców, w skład którego weszli uznani prawnicy międzynarodowi.

Komisja została utworzona jako całkowicie niezależny organ pozarządowy. Badała czas trwania głodu, jego przyczyny, geografię, liczbę ofiar Hołodomoru i jego skutki. Fakt sztucznie wywołanego głodu w Ukrainie w latach 1932–1933 został bez wątpienia przyznany, władza sowiecka, choć wiedziała o głodzie, nie zapobiegała mu i doprowadziła do śmierci milionów ludzi. Komisja doszła do wniosku, że Ukraina niewątpliwie była brutalnie głodzona w latach 1932–1933, a władze lokalne i centralne wiedziały o braku jedzenia wśród ludności. Nie było wątpliwości, że chociaż władze radzieckie wiedziały o dramatycznych warunkach w Ukrainie, powstrzymały się od udzielenia pomocy aż do lata 1933 r. Komisja stwierdziła również, że władze sowieckie podjęły różne środki prawne, które pogłębiły katastrofalne skutki głodu, uniemożliwiając ofiarom poszukiwanie jakiejkolwiek żywności, a także możliwości opuszczenia dotkniętych głodem regionów. Stwierdzono, że władze radzieckie zaprzeczyły istnieniu głodu w tym czasie, a mimo przytłaczających dowodów nie uznawały faktów

historycznych przez ponad 50 lat, z wyjątkiem prywatnych wspomnień Chruszczowa. Komisja podkreśliła, że władze sowieckie celowo wykorzystały głód dla ukończenia swojej nowej polityki denacjonalizacji.

W 1988 r. w Waszyngtonie został opublikowany raport komisji Kongresu USA, w którym podkreślono, że wg norm prawa międzynarodowego Hołodomor w Ukrainie w latach 1932–1933 ocenia się jako ludobójstwo. Oprócz tego Komisja zatwierdziła 19 punktów, w których potępiła brak podejmowania jakichkolwiek działań i świadome milczenie ówczesnego rządu USA oraz potwierdziła, iż głód w Ukrainie był zaplanowaną akcją władzy w Moskwie skierowaną przeciwko Ukraińcom. Badanie miało na celu także rozpowszechnienie w świecie informacji o Wielkim Głodzie po to, by dać mieszkańcom Stanów Zjednoczonych możliwość zrozumienia systemu radzieckiego i pokazać negatywną rolę rządu sowieckiego w planowaniu głodu w Ukrainie. W związku z działalnością diaspory ukraińskiej upamiętnienie ofiar Wielkiego Głodu, z poparciem reprezentantów władz USA, stało się akcją o charakterze politycznym, wywołującą reakcje na świecie.

Spośród innych międzynarodowych aktów dotyczących Wielkiego Głodu można wyróżnić wspólne oświadczenie z okazji 70. rocznicy Hołodomoru z lat 1932–1933 w Ukrainie, przyjęte na 58. sesji Zgromadzenia Ogólnego ONZ w 2003 r., podpisane przez 64 państwa, w którym Wielki Głód jest definiowany jako narodowa tragedia Ukraińców, która pochłonęła od 7 do 10 mln niewinnych istnień. 1 listopada 2007 r. odbyła się 34. sesja Zgromadzenia Ogólnego → U N E S C O [t. 4], na której 193 kraje jednogłośnie przyjęły rezolucję o upamiętnieniu ofiar Hołodomoru w Ukrainie (Remembrance of victims of the Great Famine (*Holodomor*) in Ukraine) w 75. rocznicę Wielkiego Głodu, w której stwierdza się, że Wielki Głód był wynikiem totalitarnego reżimu stalinowskiego. W rezolucji wyrażono przekonanie, że tragedia Hołodomoru, spowodowana przez brutalne działania i totalitarny stalinowski reżim polityczny, powinna być przestrogą dla obecnych i przyszłych pokoleń co do dotrzymania wartości demokratycznych, praw człowieka i praworządności.

W marcu 1993 r. z okazji 60. rocznicy Hołodomoru 1932–1933 L. Krawczuk, prezydent niezależnej już Ukrainy, podpisał uchwałę o szacunku do pamięci zamordowanych głodem ludzi, uporządkowaniu masowych

pogrzebów, ustanowieniu krzyży, uporządkowaniu cmentarzy, a w cerkwiach i kościołach odprawieniu modlitw i nabożeństw żałobnych. Właśnie po tej uchwale w większości miast Ukrainy ofiarom Hołodomoru zostały postawione krzyże i pomniki. We wrześniu 1993 r. Krawczuk wystąpił na międzynarodowej konferencji z okazji 60. rocznicy Hołodomoru, gdzie podkreślił, że w trakcie sztucznie wywołanego głodu niektóre regiony Ukrainy straciły prawie 1/3 swej ludności, a w obwodzie kijowskim śmiercią głodową zmarła co piąta osoba.

W listopadzie 1998 r. prezydent L. Kuczma podpisał uchwałę o ustanowieniu Dnia Pamięci Ofiar Hołodomoru. W tym czasie opublikowano szereg dokumentów, które potwierdziły, że Hołodomor ukraińskich rolników 1932–1933 był świadomie zaplanowanym zabójstwem milionów niewinnych ludzi, wśród których najwięcej było dzieci i osób starszych.

70. rocznica Wielkiego Głodu w Ukrainie 1932–1933 stała się wydarzeniem o globalnym znaczeniu. 10 listopada 2003 r. na posiedzeniu ONZ z okazji 70. rocznicy Wielkiego Głodu wygłoszono wspólną rezolucję 36 państw, w której po raz pierwszy w historii ONZ Hołodomor 1932–1933 w Ukrainie nazwano tragedią narodu ukraińskiego. Trochę wcześniej, 20 października, Kongres USA przyjął krótką rezolucję, w której podkreślono: „Hołodomor został zorganizowany i wprowadzony przez reżim radziecki jako zaplanowany akt terroru i masowego zabójstwa, skierowanego przeciwko narodowi ukraińskiemu". Jednak w związku z pozycją Rosji w obu dokumentach nie nazwano Hołodomoru 1932–1933 ludobójstwem.

Profesor J.E. Mace, autor raportu z 1988 r. specjalnej komisji Kongresu USA powołanej w celu zbadania Wielkiego Głodu, stwierdził jednoznacznie, że zgromadzenie 16 dowodów kwalifikuje w świetle prawa międzynarodowego Wielki Głód w Ukrainie lat 1932–1933 jako zbrodnię przeciwko ludzkości. Dokumenty, które zostały opublikowane po rozpadzie ZSRR, dodają tylko nowe detale do już nakreślonego przebiegu całej zbrodni. Analizując skutki głodu w Ukrainie, Mace uważa, że są one odczuwalne po dziś dzień i wraz z innymi katastrofami Ukrainy XX w. doprowadziły do wytworzenia się *postgenocidal society*, społeczeństwa ostatecznie niezdolnego do transformacji, której jednak konieczność odczuwa większość obywateli.

W maju 2003 r. parlament Ukrainy nazwał wydarzenia z lat 1932–1933 aktem ludobójstwa (genocydu) wobec narodu ukraińskiego, ale za takim stwierdzeniem głosowało tylko 226 z 450 deputowanych. W specjalnym posłaniu podkreślono, że po raz pierwszy w historii metoda konfiskowania żywności została zastosowana przez państwo jako broń masowego zniszczenia przeciwko własnemu narodowi w celu osiągnięcia pewnych celów politycznych. Według deputowanych celem eksterminacji z lat 1932–1933 było złamanie ducha narodowego Ukraińców, wyniszczenie elit i likwidacja chłopstwa jako elementu gospodarczej niezawisłości kraju.

26 listopada 2005 r. po raz pierwszy w skali całej Ukrainy obchodzono dzień pamięci ofiar sztucznie wywołanego głodu w latach 1932–1933 oraz represji politycznych →totalitaryzmu [t. 4] sowieckiego. Odbyły się wiece i demonstracje, w czasie których wspominano te straszne wydarzenia. Na cześć wielu milionów niewinnych ofiar zapalano świece. Hołodomory lat 1921–1923, 1932–1933 i 1946–1947 zostały ogłoszone ludobójstwem narodu ukraińskiego, prezydent Ukrainy W. Juszczenko podpisał 4 listopada 2005 r. rozporządzenie nr 1544 „O poszanowaniu ofiar i poszkodowanych w następstwie Hołodomorów w Ukrainie". Oprócz tego prezydent Ukrainy złożył do parlamentu projekt ustawy, w której Wielki Głód 1932–1933 kwalifikowano jako akt ludobójstwa.

W Polsce przyjęto Uchwałę Senatu Rzeczypospolitej Polskiej z dnia 16 marca 2006 r. w sprawie rocznicy Wielkiego Głodu na Ukrainie, gdzie podkreślono:

> Senat Rzeczypospolitej Polskiej pragnie przypomnieć, że Wielki Głód „Hołodomor" został specjalnie wywołany przez rządzący Związkiem Sowieckim despotyczny reżim bolszewicki i miał doprowadzić do osłabienia i wyniszczenia narodu ukraińskiego, a tym samym stłumić jego dążenia do wolności i odbudowania własnego niepodległego państwa. […] Senat Rzeczypospolitej Polskiej solidaryzuje się ze stanowiskiem ukraińskim, aby uznać Wielki Głód w latach 1932–1933 za zbrodnię ludobójstwa oraz wymienić odpowiedzialnych za tę zbrodnię zarówno głównych winowajców, jak również szeregowych wykonawców. Za śmierć milionów niewinnych ludzi odpowiadają także państwa,

> które kupowały w tym czasie od Związku Sowieckiego żywność, oraz dziennikarze, politycy i intelektualiści, którzy w tym czasie odwiedzali Ukrainę i nie tylko nie dostrzegli mającego miejsce powszechnego ludobójstwa, lecz kłamliwie zapewniali o bezpodstawności tego rodzaju oskarżeń. […] Za tego rodzaju kłamstwa niektórzy dziennikarze otrzymywali prestiżowe międzynarodowe nagrody. Ten ponury rozdział cynizmu i serwilizmu powinien zostać dokładnie zbadany i opisany, a przyznane wówczas nagrody unieważnione.

W sierpniu 2006 r. Służba Bezpieczeństwa Ukrainy (SBU) opublikowała w internecie, dostępne dotąd tylko dla historyków, 5 tys. stron dokumentów radzieckiego GPU dotyczących Wielkiego Głodu z lat 1932–1933. Według ujawnionych dokumentów NKWD Wielki Głód był zaplanowany polityką władz Związku Sowieckiego jako akcja wymierzona w niepodległościowe dążenia Ukrainy i „klasowych wrogów", za jakich reżim komunistyczny uznawał chłopów posiadaczy ziemi, którzy walczyli przeciwko przymusowej kolektywizacji. Jak podkreślił dyrektor SBU I. Driżczanyj, umniejszenie skali Hołodomoru w Ukrainie jest nie tylko bezsensowne, lecz również nieuczciwe i niesprawiedliwe z punktu widzenia historii. Dokumenty były zbierane przez kilka lat, wcześniej zaś chronione w zbiorach KGB pod hasłem „ściśle tajne", schowane przed społeczeństwem w specjalnych magazynach.

28 listopada 2006 r. Rada Najwyższa Ukrainy przyjęła na wniosek prezydenta Juszczenki ustawę uznającą Wielki Głód w latach 1932–1933 za zbrodnię ludobójstwa. Niestety, z prezydenckiego projektu wykreślona została m.in. odpowiedzialność prawna za negowanie Wielkiego Głodu jako ludobójstwa. 29 listopada 2006 r. prezydent podpisał ustawę, wg której Hołodomor w latach 1932–1933 uznano za ludobójstwo przeciwko narodowi ukraińskiemu.

Po Wielkim Głodzie praktycznie cała wschodnia Ukraina została zaludniona osiedleńcami z całego Związku Sowieckiego, dla których jedynym znanym językiem był język rosyjski, zaś – po upływie dziesięcioleci i nadejściu nowych pokoleń – jedyną identyfikacją była ta sowiecka. Miasta na wschodzie Ukrainy już uprzednio były zrusyfikowane.

Dziś postsowiecka ludność zarówno wschodniej Ukrainy, jak i czarnomorskiego Pomoria i Taurydy, nie mówiąc już o Krymie, który Kreml anektował, są ostoją wpływów partii prorosyjskich w Ukrainie. Rosja wykorzystuje tę ludność jako narzędzie nacisku na Kijów, by ów na powrót znalazł się w strefie wpływów rosyjskich. Tworzenie państwowości ukraińskiej w tych regionach nie wzbudza większego zainteresowania. Prasa lokalna i rosyjska zamiast tego przyciąga uwagę do takich idei jak Braterstwo Słowiańskie, Szczerze Prawosławie, Wielka Ruś, walka z amerykańskim imperializmem i banderowcami, którzy rzekomo objęli władzę w Kijowie. Tym bardzo rozpowszechnionym światopoglądom towarzyszy również dosyć ciekawy bukiet symboli historycznych. Tak np. czapka Monomacha (książę Rusi Kijowskiej w XI w.) znajduje się obok flagi czerwonej, orzeł z dwiema głowami obok gwiazdy pięcioramiennej, sierpa i młota, a ikona cara Mikołaja Romanowa obok portretu przywódcy bolszewickiego Stalina. Co ciekawe, tacy obywatele są przekonani co do zasadności tych mozaik i nie odczuwają niechęci do dawnych symboli. Podobna sytuacja występuje i w Rosji, gdzie pokojowo współistnieją biały car i czerwony zabójca cara, przedstawicieli Armii Białej i Czerwonej, święty Mikołaj na ikonach i mumifikowany Lenin na placu Czerwonym, obywatele jednakowo oddają hołd ostatkom gen. Denikina, do walki z którymi wzywał Lenin.

Wielki Głód odgrywa rolę jednego z głównych symboli, który ma połączyć świadomość historyczną wszystkich Ukraińców – i tak się dzieje, bo pamięć o Głodzie jest obecna w każdej ukraińskiej rodzinie. 80% obywateli Ukrainy uważa Wielki Głód w latach 1932–1933 za ludobójstwo narodu ukraińskiego. Prawie połowa ankietowanych uważa za winnego organizacji Wielkiego Głodu osobiście Stalina. 1/3 badanych obarcza winą za ludobójstwo takie organy jak NKWD, co czwarty respondent – najwyższe kierownictwo Ukraińskiej SRR.

Sowiecki reżim uparcie zaprzeczał istnieniu głodu w Ukrainie. Milczenie na temat tej wielkiej zbrodni ogarnęło cały świat. Przez pół wieku żadne z wpływowych państw nie chciało zadzierać z tego powodu z supermocarstwem, a temat Hołodomoru był tematem zamkniętym. Jakakolwiek próba badania Hołodomoru uważała była za próbę zniszczenia władzy radzieckiej, a względem badaczy stosowane były różnego rodzaju represję.

W ZSRR o Wielkim Głodzie wiedzieli wszyscy, ale nikt na ten temat nie rozmawiał. Wspomnienie w mass mediach o Głodzie było traktowane jako antyradziecka propaganda. W tym czasie żadne państwo nie pospieszyło z pomocą umierającym, nie było żadnej pomocy humanitarnej. Skala i stopień okrucieństwa tej zbrodni przekraczają wszystko, co dotąd człowiek wymyślił i zrealizował. Liczba ofiar określana jest przez badaczy tematu szacunkowo, ze względu na ukrywanie i fałszowanie wszelkich danych statystycznych przez reżim stalinowski. Prawda o Hołodomorze zaczęła przebijać się do europejskiej opinii publicznej dopiero po upadku ZSRR (np. Komunistyczna Partia Ukrainy do dzisiaj neguje ten fakt historyczny). Wszelkie wypowiedzi na ten temat były karane jako przestępstwa „propagandy antyradzieckiej".

Oprócz tego po śmierci Stalina u ludzi został strach, głęboko zakorzeniony wewnątrz: wszyscy wiedzieli o tym, co można mówić, a o czym w ogóle nie warto wspominać. W kodeksie karnym Ukraińskiej SRR znajdował się artykuł 62 (antyradziecka agitacja i propaganda), wg którego ludziom groziło nie tylko więzienie, ale i szpital psychiatryczny. Nawet wspomnienia o tej tragedii system totalitarny próbował wykreślić z pamięci narodu. Ujawnienie tragedii zawdzięcza najwięcej badaczom diaspory ukraińskiej. Do dziś w Ukrainie występują historycy, którzy umniejszają skalę Wielkiego Głodu.

O ludobójstwie Ukraińców w latach 1932–1933 napisano prawie 15 tys. prac, w których autorzy wyrazili własne obiektywno-naukowe oceny. Ponad 10 tys. książek i artykułów liczy bibliografia, którą opublikował kanadyjski badacz M. Carynnyk na początku lat 90. XX w.; listę ponad 12 tys. prac zamieszczono w książce L. Buriana i I. Rikuna z 2014 r. Tak duża liczba prac świadczy o wielkim zainteresowaniu tematyką i wielkim wysiłku na rzecz dogłębnego zbadania tej ukraińskiej tragedii narodowej, którą zajmuje się kilka pokoleń historyków, pisarzy, artystów i działaczy obywatelskich w Ukrainie i poza nią.

Na znak pamięci o wszystkich zmarłych w tych latach w każdą ostatnią sobotę listopada o 16:00 cały ukraiński naród milknie na minutę. W tej chwili ciszy wspomina się tych, którzy mieszkali na obszarze nazywanym spichlerzem Europy i umierali z głodu. Wspomina się tych, którym odebrano cały majątek i jako wrogów narodu zesłano na Syberię.

Wspomina się tych, którzy przeżyli i nosili te wspomnienia ze sobą przez całe życie.

Olga Wasiuta

Głód i represje wobec ludności polskiej w Ukrainie 1932–1947. Relacje, R. Dzwonkowski (red.), Towarzystwo Naukowe KUL, Lublin 2005; D. Irvin-Erickso, *Raphael Lemkin and the Concept of Genocide*, University of Pennsylvania Press, Philadelphia 2016; C. Rajca, M. Łesiów, *Głód w Ukrainie*, Wydawnictwo Werset, Lublin 2005; R. Serbyn, *Lemkin on the Ukrainian Genocide*, „Journal of International Criminal Justice" 2009, no. 7; tenże, *Raphael Lemkin's Conceptualization of the Crime of Genocide and his Analysis of the Ukrainian Genocide*, [w:] tegoż, *Soviet Genocide in Ukraine*, R. Serbyn (ed.), Maisternia Knyhy, Kyiv 2009; tenże, *Raphael Lemkin papers 1947–1959*, Archives.NYPL.org (dostęp 14.01.2020); tenże, *Soviet Genocide in the Ukraine*, Kashtan Press, Kingston 2014; L. Luciuk, *Holodomor: Reflections on the Great Famine of 1932–1933 in Soviet Ukraine*, The Kashtan Press, Kingston 2008; *The Genocide by Famine in Ukraine 1932–1933*, L.M. Burian, I.E. Rikun (eds.), Odessa National Research M. Gorky Library, Institute of the History of Ukraine of the National Academy of Sciences of Ukraine, Odessa 2014; O. Wasiuta, *Czy zbrodnia ludobójstwa w Ukrainie w latach 1932–1933 to mit?*, „Forum Politologiczne" 2007, nr 6; О. Веселова, В. Марочко, О. Мовчан, *Голодомори в Україні, 1921–1923, 1932–1933, 1946–1947: злочини проти народу*, Видавництво М.П. Коць, Київ 2000; А. Куліш, *Голодомор 1921–1923 років в Руси-Україні як продовження етнічной війни 1917–1921 років*, Асоціація дослідників голодоморів в Україні, Київ 2003; *Національні процеси в Україні: історія і сучасність. Документи і матеріали. Довідник*, Ч. 2, Київ 1997; С. Кульчицький, *Голодомор 1932–1933 рр. як геноцид: труднощі усвідомлення*, „Наш час", Київ 2008; Я. Папуга, *«Змова мовчання»: як Захід реагував на Голодомор українців 1932–1933 років. Видавець Олег Філюк*, Київ 2018; М. Дорошко, В. Головченко, *Голодомор 1932–33 рр. в Україні як геноцид: проблема міжнародного визнання*, „Актуальні проблеми міжнародних відносин" 2017, Випуск 1 (46); А. Куліш, *Геноцид. Голодомор. 1932–1933. Причини, жертви, злочинці*, Полтава, 2000; *Матеріали Міжнародної науково-практичної конференції «Голодомор 1932–1933 років: втрати української нації» (Київ, 4 жовтня 2016 року)*, Національний музей «Меморіал жертв Голодомору», Київ 2017.

I

IDEOLOGIZACJA PRZEKAZU – zjawisko lub proces związany ze wzbogacaniem, modyfikowaniem i przekształcaniem treści komunikatu lub →informacji adresowanej do konkretnego odbiorcy (lub grupy odbiorców) poprzez nadawanie im silnie zsubiektywizowanego, nierzadko zafałszowanego znaczenia. Proces ten w jawny bądź niejawny sposób zniekształca oraz redefiniuje podstawowy cel i fundamentalną wręcz funkcję przekazu, jaką jest funkcja informacyjna. Ideologizacja przekazu wiąże się także z przenikaniem określonych idei, poglądów, opinii, sądów i wartości (aksjologiczno-normatywnego porządku charakterystycznego dla danej ideologii) do treści transmitowanych za pośrednictwem środków masowego przekazu. Jawność bądź niejawność podszytego ideologicznie komunikatu wynika wprost z intencji jego nadawcy, natomiast przebieg procesu komunikowania zależy od stopnia świadomości w zakresie →manipulacji medialnej [t. 3] i propagandowego oddziaływania na jednostki poszczególnych jego uczestników. Oczywiście zjawisko ideologizacji, podobnie jak sama ideologia, może mieć zarówno negatywny, jak i pozytywny wydźwięk, jednak jego stopniowa pejoratywizacja sprawia, że ideologizacja przekazu często bywa utożsamiana ze zwerbalizowanym dążeniem do realizacji partykularnych interesów politycznych czy ekonomicznych, co ma wydatny wpływ na poziom →bezpieczeństwa informacji [t. 1], narażonych na ich ideologiczne zniekształcenie.

Zideologizowany przekaz (będący wynikiem procesu ideologizacji) nie musi nieść ze sobą wyłącznie treści mających w założeniu destabilizację określonego porządku (aksjologicznego, społecznego, politycznego itd.). Wektor zmiany, w stosunku do opisywanej i analizowanej rzeczywistości, może mieć charakter ujemny bądź dodatni, ale nigdy obojętny. Wykorzystanie potencjału ideologii w celu konstrukcji przekazów medialnych – np. do ferowania wyroków na rządzących i tworzenia nowych koncepcji dotyczących „idealnego świata" – samo w sobie nie może być zobojętnione, ponieważ ulegający wpływowi ideologii nadawca zawsze zajmuje mniej lub bardziej konkretne stanowisko w danej sprawie. Cechami charakterystycznymi ideologizacji przekazu są m.in.:

- przyznawanie pierwszeństwa niektórym wartościom, ideom i teoriom nad innymi, konkurencyjnymi względem nich (np. stwierdzenie wyższości idei wolnorynkowej nad scentralizowanym systemem gospodarki państwowej);
- nadawanie różnych znaczeń faktom oraz zdarzeniom o, wydawałoby się, sprecyzowanym wydźwięku oraz dostarczanie wyjaśnień spornych kwestii światopoglądowych (np. dychotomiczne określanie aborcji „zabijaniem nienarodzonych dzieci" lub „prawem kobiet do decydowania o własnym ciele");
- wykorzystywanie wolności słowa i pluralizmu rynku medialnego do konstrukcji przekazu o silnie zsubiektywizowanym obrazie świata, opozycyjnym lub konkurencyjnym względem innych, w założeniu bezstronnych, środków masowego przekazu (np. tworzenie wydawnictw, periodyków, audycji, relacji, komunikatów, programów telewizyjnych lub *stricte* politycznych o wyraźnie ideologicznym zabarwieniu i stronniczym charakterze);
- świadome wykorzystywanie przez twórcę przekazu nieświadomości → o p i n i i p u b l i c z n e j [t. 3] odnośnie do technik i narzędzi manipulacji oraz podatności społeczeństwa na pozornie atrakcyjne propozycje rozwiązania konkretnych problemów życia codziennego, które proponuje ideologia, do osiągania celów nierzadko politycznych (np. komunikacyjne oddziaływanie na odbiorcę poprzez posługiwanie się nośnymi hasłami i populistycznymi propozycjami dotyczącymi m.in. kwestii zabezpieczenia społecznego czy

ochrony rodzimego rynku pracy przed →zagrożeniami [t. 4] współczesnej migracji);

- dążenie do nieustannego utrzymywania swoistego monopolu na prawdę, który ma uwiarygodniać intencje twórcy określonych treści i legitymizować ideologię, która legła u ich podstaw (np. dla fundamentalistów religijnych za prawdziwe uznaje się słowo objawione przez pozaziemski byt absolutny, charakteryzujący się wszechwładzą, wszechwiedzą i wszechobecnością).

Proces intensywnej ideologizacji, jak podaje R. Tokarczyk, był charakterystyczny szczególnie w okresie XX w., kiedy to uwydatnił się →kryzys idei postępu promującej optymistyczną wizję rozwoju naukowego w kierunku możliwości wcielania pewnych rozwiązań do praktyki życia społecznego. Ideologia miała spełniać określoną funkcję poznawczą odpowiadającą za opis rzeczywistości społecznej i tworzenie zrozumiałych, aczkolwiek kompleksowych, propozycji dróg zmiany na lepsze w sposób prosty (często lakoniczny) w przekazie. Problem stanowić może jednak swoisty dualizm zideologizowanego przekazu, który z jednej strony odpowiada za racjonalizację, opis, przekonanie, informowanie, wyjaśnianie i integrowanie ludzi wokół tworzonego przezeń obrazu świata, a z drugiej strony wzbudza emocje, postuluje, apeluje, dezinformuje, oślepia i dezintegruje grupy społeczne, czyniąc z proponowanych rozwiązań iluzoryczny porządek oparty na wspólnocie celów i interesów wszystkich uczestników komunikowania (politycznego, publicznego, masowego). Zatem „przemycanie" treści nacechowanych ideologią do procesu komunikowania międzyludzkiego w znaczący sposób wpływa na:

- charakterystykę i interpretację roli jednostek i całych wspólnot w kreowaniu społeczno-politycznej rzeczywistości;
- dyskusję dotyczącą strategicznego wykorzystania tworzonych komunikatów medialnych w celu wpływania na wiedzę, wierzenia, postawy, zachowania i działanie uczestników komunikowania;
- poziom dyskursu uczestników procesu komunikowania (np. instytucji władzy, mediów, obywateli) w kwestii znaczenia medialnych przekazów dla konstrukcji i implementacji polityki państwa w określonym obszarze.

Wspomniane wzbogacanie, modyfikowanie i przekształcanie treści komunikatu, związane z ideologizacją przekazu i jej istotą, jawi się (najczęściej) jako poważne zagrożenie dla bezpieczeństwa informacyjnego, →bezpieczeństwa medialnego [t. 1] oraz →bezpieczeństwa ideologicznego [t. 1] współczesnego państwa. Pewne zastrzeżenie do powyższego stwierdzenia należy jednak odnotować w kontekście jego odniesienia do bezpieczeństwa medialnego, które to pojęcie R. Klepka definiuje jako „stan niezakłóconego funkcjonowania systemu medialnego w danym państwie", na który składa się wiele czynników, m.in.: gwarancja wolności wypowiadania się i formułowania opinii na dany temat, funkcjonowanie w państwie gwarantującego pluralizm systemu medialnego, możliwość swobodnego wyrażania poglądów czy brak monopolizacji rynku medialnego. Fakt występowania elementów ideologicznego dyskursu w przekazie medialnym w żaden sposób nie narusza bowiem ani wspomnianych gwarancji i prawa do swobodnej wypowiedzi, ani pluralizmu systemu medialnego. Wykorzystywanie wolności słowa i pluralizmu rynku medialnego do konstrukcji przekazu oraz dążenie do nieustannego utrzymywania swoistego monopolu na prawdę są cechami charakterystycznymi ideologizacji przekazu, ale nie stanowią zagrożenia dla bezpieczeństwa medialnego.

Inaczej jest w przypadku bezpieczeństwa informacyjnego i ideologicznego. Priorytetem pierwszego z wymienionych rodzajów bezpieczeństwa, wg H. Batorowskiej, jest ochrona zasobów informacyjnych, procesu ich wytwarzania i wykorzystywania oraz zapewnienie stabilnego ich funkcjonowania w każdych warunkach. Bezpieczeństwo informacyjne wiąże się także ze społecznym zaufaniem do treści przekazywanych za pośrednictwem środków masowego przekazu, dostępnością do nich oraz jakością dostarczanych informacji. Zagrożeniem może być w tym przypadku asymetria w dostarczaniu informacji tożsamych treściowo, ale odmiennych jakościowo oraz możliwość działania grup, które świadomie manipulują przekazem informacji. Na poszczególnych etapach zapewniania tak rozumianego bezpieczeństwa informacyjnego istnieje zatem ryzyko ideologizacji przekazu, a więc jego modyfikowania i zniekształcania, nierzadko również w celach indoktrynacyjnych, manipulacyjnych, propagandowych czy dezinformacyjnych, co w znacznym stopniu wpływa

na poziom jakości oferowanych komunikatów, stopień ich zafałszowania i decyduje o utracie zaufania społecznego do transmitowanych zasobów informacyjnych. Nierzadko ideologizację przekazu łączy się z jego propagandyzacją. Informacja jest budulcem działania propagandowego, środki i metody komunikacji są narzędziem w rękach → p r o p a g a n d y [t. 3] wykorzystywanym do przejmowania władzy nad jednostką lub społeczeństwem. Jeżeli więc propagandę określa się wywieraniem wpływu na społeczeństwo za pomocą określonych idei i wartości w celu realizacji interesów twórcy przekazu, to z ideologizacją przekazu ma ona rzeczywiście wiele wspólnego.

W nawiązaniu do bezpieczeństwa ideologicznego oraz ideologizacji przekazu, która wydatnie wpływa na możliwość jego zapewnienia, należy odnieść się do podziału na perspektywę wewnętrzną i zewnętrzną w jego definiowaniu. Oba ujęcia kładą nacisk na ochronę porządku ustrojowego państwa oraz ładu aksjologicznego przed sprzecznym z przyjętym systemem wartości oddziaływaniem innych ideologii. Chodzi tu przede wszystkim o ograniczenie wpływu na społeczeństwo partii politycznych, grup społecznych, grup nacisku politycznego oraz grup religijnych, realizujących partykularne interesy oraz propagujących i rozpowszechniających ideologie niezgodne z zasadami ustrojowymi państwa, a także o ograniczenie działania różnych podmiotów szerzących skrajne ideologie i deprawujących ustanowiony porządek moralny i aksjologiczny. Wychodząc z założenia, że tworzenie przekazów medialnych (zdeformowanych, zakamuflowanych lub zmanipulowanych przez ideologiczne odniesienia do określonego zespołu idei czy światopoglądu) trudne jest do kontrolowania, a ów przekaz jakościowo odbiega od tego „nieskażonego" ideologią procesu przesyłu informacji, należy jednoznacznie stwierdzić, że ideologizacja przekazu stanowi również znaczne zagrożenie dla bezpieczeństwa ideologicznego współczesnego państwa.

Istotnym zagadnieniem wydaje się także spojrzenie reprezentantów, wyznawców danej ideologii na jej rolę w procesie przekazywania (zideologizowanych) informacji. J. Brynkus zaznacza, że ideologizację wybranej płaszczyzny życia społecznego (np. procesu komunikowania, edukacji historycznej czy wyznaczania jednostce celów do realizacji) winno się rozpatrywać z perspektywy ideologizacji całego społeczeństwa

oraz jej wpływu na przekazywanie informacji o przeszłości i teraźniejszości. Przykładem mogą być komuniści, którzy ideologię traktowali jako nieuznające kompromisu narzędzie wpływu na społeczeństwo, pozwalające na dostosowanie kultywowanych idei do istniejącej rzeczywistości społecznej. Przy czym podstawą ideologizacji uczyniono m.in.: egalitaryzm, sprawiedliwość, socjalistyczne stosunki produkcji, internacjonalizm, pierwszorzędną rolę proletariatu i kierowniczą rolę partii komunistycznej. Przekładając spojrzenie na ideologię z punktu widzenia wyznawców jej różnych odmian, zaprezentowane przez A. Heywooda, na poziom ideologizacji treści przez nich prezentowanych można dojść do ciekawych konstatacji. Dla liberałów ideologia stanowiła oficjalny system przekonań i wartości, roszczący sobie prawo do monopolu na prawdę (pomimo swej nienaukowości), a jej represyjność i totalitarny wręcz charakter (zdaniem liberałów) skłania do twierdzenia, że najbardziej niebezpieczni pod względem skali ideologizacji są reprezentanci → k o m u n i z m u i → f a s z y z m u. Z kolei konserwatyści to socjalistów i liberałów uważali za „ideologicznych" i „ideologizujących" w myśl nieracjonalnych, aroganckich, oderwanych od rzeczywistości – i przez to niebezpiecznych – haseł i zasad oscylujących wokół porządku, którego nie można osiągnąć. Socjaliści, uznający liberałów za wyrazicieli negatywnie definiowanej ideologii klasy panującej, ideologizację traktowali jako przekazywanie treści skrywających sprzeczności występujące w społeczeństwie klasowym i sprzyjających bierności klas podporządkowanych. Dla faszystów, którzy odrzucali ideologię jako teorię systematyczną, to „obraz świata" stanowił odnośnik do ferowania realnych postulatów wprowadzania w państwie zmian, który wolny był od ideologizowania przepełnionego pasją, wolą i nadmiernym intelektualizowaniem wizji przyszłości. Dla zwolenników ekologizmu superideologia, jaką jest industrializm, oraz liberalizm i socjalizm jako wyrosłe na gruncie dążenia do wzrostu ekonomicznego i nadmiernego rozwoju humanizmu, są uznawane za najbardziej niekorzystne dla środowiska naturalnego ideologie współczesnego świata. Natomiast dla fundamentalistów religijnych wszystkie świeckie ideologie są aksjologicznie i moralnie puste, zatem muszą być odrzucone jako bezwartościowe i religijne obojętne. Ogólnie rzecz ujmując, wskazany powyżej subiektywnie negatywny stosunek do ideologii świadczyć

może generalnie o negatywnym (ujemnym) wektorze ideologizacji jako procesu związanego z przekazywaniem informacji.

Paweł Łubiński

H. Batorowska, *Bezpieczeństwo informacyjne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; J. Brynkus, *Komunistyczna ideologizacja a szkolna edukacja historyczna w Polsce (1944–1989)*, Wydawnictwo Antykwa, Kraków 2010; B. Dobek-Ostrowska, *Podstawy komunikowania społecznego*, Wydawnictwo Astrum, Wrocław 2004; P. Łubiński, *Bezpieczeństwo ideologiczne (ideological security)*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Ideologizacja przekazu*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; R. Klepka, *Bezpieczeństwo medialne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Heywood, *Ideologie polityczne. Wprowadzenie*, Wydawnictwo Naukowe PWN, Warszawa 2008; T.H. Qualter, *Propaganda and Psychological Warfare*, Literary Licensing, LLC, New York 1965; R. Tokarczyk, *Współczesne doktryny polityczne*, Wolters Kluwer Polska, Warszawa 2010; A. Urbanek, *Państwo jako podmiot bezpieczeństwa narodowego – ujęcie dziedzinowe*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, A. Urbanek (red.), Wydawnictwo Społeczno-Prawne, Słupsk 2013; D. Welch, *Powers of Persuasion*, „History Today" 1999, vol. 49, no. 8; W. Werner, *O (nie)rzeczywistości propagandy. Cechy charakterystyczne propagandowych obrazów świata*, [w:] *Uwikłania historiografii. Między ideologizacją dziejów a obiektywizmem badawczym*, T. Błaszczyk, K. Brzechczyn, D. Ciunajcis i in. (red.), IPN Oddział w Poznaniu, Poznań 2011; L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, „Obronność. Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2014, nr 2 (10).

ILS (ang. *instrument landing system*) – system nawigacyjny działający na podstawie fal radiowych, wykorzystywany w lotnictwie cywilnym w celu precyzyjnego wspomagania lądowania samolotów w warunkach o ograniczonej widzialności pasa w dzień i w nocy (warunki ograniczonej i niskiej podstawy chmur). W zainstalowanym systemie → i n f o r m a c j e są przesyłane w sposób ciągły na linii nadajnik – samolot w celu wytyczenia trafnej i rzetelnej drogi podejścia samolotu do lądowania. Systemem podejścia do lądowania nazywa się zespół urządzeń radiotechnicznych,

naziemnych oraz zainstalowanych na pokładzie, które umożliwiają wykonanie manewru podejścia przy ograniczonej widoczności.

Pierwowzory systemów nawigacyjnych ILS oraz pierwsze testy i symulacje rozpoczęły się w USA w 1929 r. Obecny system ILS został stworzony na podbudowie niemieckiego systemu Lorenza, skonstruowanego w 1932 r., który pracował na częstotliwościach fal krótkich i pozwalał uzyskać dużą dokładność w wyznaczaniu kursu podejścia do lądowania, kąta wymaganego do precyzyjnego schodzenia samolotu oraz odległości od punktu przyziemienia. Podobnym mechanizmem charakteryzował się radziecki SP-50. Sukcesem testów było pierwsze lądowanie samolotu pasażerskiego lecącego z Waszyngtonu do Pittsburgha 26 stycznia 1938 r., kiedy w ogromnej śnieżycy pilot wylądował, używając jedynie informacji zaczerpniętych z systemu ILS. Wraz z precyzją, jaka charakteryzowała ILS, Civil Aeronautics Administration (CAA) podjęła decyzję w 1941 r. o instalacji systemu w 6 miejscach na świecie. Pierwszy w pełni automatycznie wykonany ruch lądowania samolotu przy użyciu ILS odbył się w marcu 1964 r. na lotnisku w Bedford w Wielkiej Brytanii.

Dla zapewnienia → b e z p i e c z e ń s t w a [t. 1] stosowane są różne rozwiązania radiotechniczne przy wsparciu odpowiednich urządzeń wysyłających informacje, umożliwiające kontrolowanie maszyny i prowadzenie jej po określonym torze. Najtrudniejszą fazą lotu jest start i lądowanie samolotu, przy czym lądowanie w utrudnionych warunkach meteorologicznych, przy złej widoczności może stanowić wyzwanie dla pilotów w komunikacji człowiek – maszyna.

Obecnie stosowane są również dużo bardziej zaawansowane systemy nawigacyjne, np. MLS (Microwave Landing System) czy TLS (Transponder Landing System), a także systemy oparte na globalnej strukturze nawigacji satelitarnej GNSS. Jednakże ILS nadal jest podstawowym systemem precyzyjnego podejścia do lądowania samolotów cywilnych, pozwalającym na manewry statkami powietrznymi w niesprzyjających warunkach pogodowych. W systemach precyzyjnych systemów nawigacyjnych wyróżniamy:

- Instrument Landing System – ILS – lądowanie samolotu wg wskazań przyrządów; odbieranie informacji z urządzeń naziemnych umożliwia prowadzenie samolotu zgodnie z określonym kursem po ścieżce schodzenia. W skład architektury naziemnej ILS wchodzą:

nadajnik kierunku, nadajnik dla ścieżki schodzenia oraz markery. System ILS posiada 2 zestawy radiolatarni kierunkowych oraz system, za pomocą którego mierzona jest odległość. Radiolatarnia kierunkowa, która ustawiona jest za pasem lądowania, wysyła 2 wiązki informacji, z których jedna jest odchylona w lewo, a druga w prawo od osi pasa. Przykładowo dla lotniska w Pyrzowicach (Katowice Airport) wykorzystano radiolatarnię kierunku, radiolatarnię ścieżki schodzenia oraz urządzenia, które pozwalają na określenie odległości od punktu przyziemia – są to markery (Outer Marker – OM, Middle Marker – MM i Inner Marker – IM). Zatem w skład systemu ILS wchodzą: radiolatarnie typu *localizator* – odpowiadają za ustalenia odchylenia kursu; radiolatarnia typu *gildeslope* – odpowiadająca za kąt podejścia do lądowania oraz 3 markery – punkty charakterystyczne pasa. Zwykle, aby wytyczyć precyzyjnie drogę schodzenia, wystarczą 2 markery OM i MM, które wytyczą odległość i wysokość od pasa startowego. Dodatkowo wsparciem dla markerów lub też ich uzupełnieniem jest radioodległościomierz (DME) – zainstalowany zwykle na maszcie nadajnika dla ścieżki schodzenia (określa odległość od transpondera na podstawie sumy czasów przebiegu informacji radaru).

- Microwave Landing System – MLS – lądowanie za pomocą informacji przekazywanych poprzez mikrofale; następca ILS.
- Global Navigation Satellite System – GNSS – lądowanie za pomocą systemów globalnej nawigacji satelitarnej, opierającej się na istniejących systemach: GPS – Global Positioning System oraz GLONASS – Global Orbital Navigation Satellite System, a także Inmarsat – International Maritime Satellite (stworzony początkowo na potrzeby komunikacji morskiej, obecnie system obsługuje 12 sztucznych satelitów umieszczonych na orbicie geostacjonarnej).

Z uwagi na dostosowanie precyzyjności pomiarów ILS jest najbardziej rzetelnym systemem sprowadzania samolotów na tor podchodzenia do lądowania, zapewniając przy tym względne bezpieczeństwo wykonywania manewrów w powietrzu przy ograniczonej widoczności (przekazywane informacje dotyczą pozycji pionowej oraz poziomej). Z uwagi na kosztowność instalacji zarówno na lądzie, jak i w samolocie niewiele lotnisk

posiada systemy MLS. Od czasu wprowadzenia sygnałów GPS wiele systemów MLS zostało wyłączonych na lotniskach w Ameryce Północnej, jednakże systemy GPS nie są pozbawione wad. Działanie nawigacji systemu GPS nie pozwala precyzyjnie określić położenia i toru podejścia do lądowania, uzyskując tym samym margines błędu od 3 do 5 metrów, co w przypadku takiej pomyłki czyni lądowanie procesem bardziej niebezpiecznym, niejednokrotnie mogącym doprowadzić do katastrofalnych skutków w przypadku zerowej widoczności przestrzeni w niesprzyjających warunkach pogodowych. Pomimo przyjęcia rozwiązań technologii MLS przez Organizację Międzynarodowego Lotnictwa Cywilnego i prób wdrożenia jej do światowych rozwiązań nawigacyjnych ILS nadal jest najbardziej popularnym instalowanym systemem wspomagającym proces lądowania.

W zależności od dokładności systemu ILS wyróżnić można 3 jego kategorie: od najmniej precyzyjnej CAT I, poprzez standardową – CAT II, po najbardziej dokładną – CAT III A, B, C:

- CAT I – wskazania przyrządów do precyzyjnego podejścia do lądowania przy wysokości decyzji (to wysokość, która umożliwia widoczność świateł na drodze podejścia) nie mniejszej niż 60 m (tj. 200 stóp) nad pasem startowym oraz widzialności nie mniejszej niż 550 m. Przykładem lotniska wykorzystującego kategorię I jest Międzynarodowy Port Lotniczy im. Jana Pawła II Kraków-Balice (EPKK), Port Lotniczy Poznań-Ławica im. Henryka Wieniawskiego (EPPO).
- CAT II – wskazania przyrządów do precyzyjnego podejścia do lądowania przy wysokości decyzji mniejszej niż 60 m (tj. 200 stóp), ale nie mniejszej niż 30 m (100 stóp) oraz widzialności pasa startowego nie mniejszej niż 300 m. Przykładem lotniska wykorzystującego kategorię II jest Międzynarodowy Port Lotniczy Katowice w Pyrzowicach – Katowice Airport (EPKT), Port Lotniczy Gdańsk-Rębiechowo im. Lecha Wałęsy (EPGD), Port lotniczy Rzeszów-Jasionka (EPRZ).
- CAT III A – wskazania przyrządów do precyzyjnego podejścia do lądowania przy wysokości decyzji mniejszej niż 30 m (tj. 100 stóp) lub braku wysokości decyzji oraz widzialności drogi startowej nie

mniejszej niż 200 m. Lotnisko Chopina w Warszawie w 2018 r. po przeprowadzonej modernizacji otrzymało certyfikat prezesa Urzędu Lotnictwa Cywilnego, który uprawnia do wykonywania operacji lądowania w warunkach ograniczonej widzialności w kategorii III ILS – droga startowa 3 na kierunku 33.

- CAT III B – wskazania przyrządów do precyzyjnego podejścia do lądowania przy wysokości decyzji mniejszej niż 15 m (50 stóp) lub braku wysokości decyzji oraz widzialności pasa startowego nie mniejszej niż 200 m. System zainstalowany jest w porcie lotniczym Londyn-Heathrow (EGLL).
- CAT III C – wskazania przyrządów do precyzyjnego podejścia do lądowania przy całkowitym braku wysokości decyzji i braku widzialności wzdłuż drogi startowej.

W momencie podejścia do lądowania samolotu procedury można podzielić na 2 rodzaje:

- nieprecyzyjne (inaczej zwane klasycznym) – sterowanie samolotem odbywa się przy wykorzystaniu kompasów radiowych, systemu VOR (VHF Omni-directional Range – najpopularniejszy system kątowy w nawigacji lotniczej, wykorzystujący informacje azymutalne poprzez sygnały radiolatarni, wadą systemu jest duża możliwość występowania zakłóceń z uwagi na ukształtowanie terenu przy usytuowaniu lotnisk) oraz naziemnego urządzenia korespondencyjnego.
- precyzyjne – sterowanie statkiem powietrznym podczas podchodzenia do lądowania odbywa się na podstawie utworzonej przez systemy trójwymiarowej ścieżki, z zachowaniem odpowiedniego kąta i wysokości prowadzonej w locie maszyny. Zadaniem precyzyjnych systemów jest ustalenie i wyznaczenie ścieżki podejścia i kierunku lądowania samolotu. Z uwagi na manewr lądowania, który jest procesem krytycznym w ostatniej fazie lotu, wymagania techniczne zarówno dla urządzeń naziemnych, jak i pokładowych są bardzo wysokie (instalowane są podwójne urządzenia bezpieczeństwa);

Instalowane systemy ILS na lotniskach są elementami, które wspomagają proces podejścia do lądowania i bezpieczne prowadzenie maszyny

do momentu uziemienia. Układ systemów musi spełnić szereg wymagań, aby móc prowadzić operacje w sposób bezpieczny. Porównując stosowane systemy, MLS charakteryzuje się blisko 100% niezawodnością, a ILS – 98%. Przy czym należy zwrócić uwagę, że MLS jest mniej wrażliwy na warunki zewnętrzne oraz ukształtowanie terenu lotniska. Wytyczne dla bezpieczeństwa dotyczą przede wszystkim procesu przekazywania informacji pomiędzy funkcjonującymi urządzeniami: ich dokładności, dostępności, zasięgu działania, wiarygodności i niezawodności przy użyciu fal radiowych, a także pojemności gromadzenia danych.

Poprawa oprzyrządowania, skuteczność i precyzja w przesyłaniu rzetelnych informacji oraz wsparcie techniczne dla już istniejących kategorii ILS sprawiają, że jest to system wykorzystywany do nawigacji lotniczych na całym świecie. Koszty, jakie niesie za sobą instalacja systemów MLS, skłaniają międzynarodowe środowisko lotnicze do modernizowania oraz ulepszania systemów ILS. Pomimo użytkowania sygnałów z wykorzystaniem GPS ILS nadal jest jedną z najlepszych pomocy nawigacyjnych w systemie lotnictwa cywilnego.

Justyna Rokitowska

Civil Aviation Safety Authority, *Instrument Landing System Operational Notes Contents*, Department of Aviation, 2005; P. Czuj, *Analiza istniejących systemów nawigacji lotniczej. Obsługa metrologiczna testera TACAN AN/ARM-188*, „Biuletyn WAT" 2012, vol. 61, nr 2; M.M.A. Eltahier, K. Hamid, *Review of Instrument Landing System*, „Journal of Electronics and Communication Engineering" 2017, vol. 12, iss. 2, ver. III; International Virtual Aviation Organisation, *Navigation Instrumentation – ILS,* IVAO HQ Training Department, 31 May 2017; J. Merkisz, M. Galant, M. Bieda, *Analysis of Operating Instrument Landing System Accuracy under Simulated Conditions,* „Scientific Journal of Silesian University of Technology. Series Transport" 2017, no. 94; Nordian Aviation Training Systems, Koninklijke Luchtvaart Maatschappij Flight Academy, *Instrument Landing System*, [w:] *Radio Navigation 7.1: Navigation*, Nordian Aviation Training Systems–Eelde–KLM Flight Academy, Sandefjord 2017; J. Rokitowska, *ILS (Instrument Landing System)*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. Siergiejszyk, K. Krzykowska, R. Kruszyna, *Analiza porównawcza systemów precyzyjnego lądowania*, „Prace Naukowe Politechniki Warszawskiej" 2014, z. 102; Z. Skorupka,

Automatyczne układy wspomagania procesu lądowania statku powietrznego, „Logistyka" 2014, nr 6; M. Stołtny, *Instrument Landing System as an Example of a Precision Approach System*, „Scientific Journal of Silesian University of Technology. Series Transport" 2016, nr 93.

IMPREZA MASOWA – impreza artystyczna lub rozrywkowa kierowana do dużej liczby osób. Cechą charakterystyczną imprez masowych jest duża liczba ludzi zgromadzonych w jednym miejscu. Najczęściej są to obiekty sportowe: stadiony, hale sportowe i widowiskowe, a także centralne punkty miast i drogi publiczne. Osoby uczestniczące w nich spotykają się w celu uczczenia czegoś, świętowania, wyrażenia swoich poglądów lub po prostu spędzenia miłych chwil na wspólnej zabawie. Imprezy takie to jednak nie tylko zabawa i relaks, ale także szereg →zagrożeń [t. 4], które już na etapie planowania, a następnie realizacji organizatorzy powinni brać pod uwagę, podejmując czynności je minimalizujące. Organizacja imprezy masowej musi uwzględniać wiele potencjalnych zagrożeń: zamach terrorystyczny, katastrofę budowlaną, użycie środków pirotechnicznych, pożar, rozboje. Akty chuligaństwa podczas rozgrywek piłkarskich należą do najbardziej znanych i najczęściej występujących zagrożeń. Zaplanowanie i zabezpieczenie imprezy masowej stanowi duże wyzwanie organizacyjne. To szereg skoordynowanych działań obejmujących zapewnienie →bezpieczeństwa [t. 1] zarówno uczestnikom, jak i widzom. Zabezpieczenie imprezy masowej wymaga wdrożenia i zastosowania wielu procedur mających na celu zwiększenie bezpieczeństwa i zapewnienie ochrony (zdrowia, życia, mienia) jej uczestników. Taki obowiązek spoczywa nie tylko na organizatorze, ale także na innych podmiotach, jak wójt, burmistrz, prezydent miasta, wojewoda, →Policja [t. 3] czy →Państwowa Straż Pożarna [t. 3] wraz z zespołami i służbami wykonującymi zadania na rzecz bezpieczeństwa i porządku publicznego.

Zasady organizowania i przeprowadzania imprez masowych oraz obowiązki i uprawnienia organizatora określa ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych. Ustawa określa:

- zasady postępowania konieczne do zapewnienia bezpieczeństwa imprez masowych;
- warunki bezpieczeństwa imprez masowych;

- zasady i tryb wydawania zezwoleń na przeprowadzanie imprez masowych;
- zasady przetwarzania →informacji dotyczących bezpieczeństwa imprez masowych, w tym danych osobowych;
- zasady odpowiedzialności organizatorów za szkody wyrządzone w związku ze zorganizowaniem imprez masowych.

Zgodnie z postanowieniami ustawy „imprezą masową jest impreza masowa artystyczno-rozrywkowa, masowa impreza sportowa, w tym mecz piłki nożnej". Pojęcie to nie obejmuje imprez realizowanych cyklicznie w obiektach kultury i edukacji i organizowanych dla określonej grupy osób. Nie są więc imprezami masowymi imprezy organizowane w teatrach, operach, operetkach, filharmoniach, kinach, muzeach, bibliotekach, domach kultury i galeriach sztuki lub w innych podobnych obiektach. Nie są też nimi imprezy organizowane w szkołach i placówkach oświatowych przez zarządzających tymi szkołami i placówkami, organizowane w ramach współzawodnictwa sportowego dzieci i młodzieży, sportowe organizowane dla sportowców niepełnosprawnych, sportu powszechnego o charakterze rekreacji ruchowej, ogólnodostępne i nieodpłatne, organizowane na terenie otwartym, zamknięte i organizowane przez pracodawców dla ich pracowników. Przepisów ustawy o bezpieczeństwie imprez masowych nie stosuje się do nieodpłatnych imprez masowych organizowanych na terenach zamkniętych podległych (nadzorowanych bądź podporządkowanych) ministrowi obrony narodowej, ministrowi sprawiedliwości oraz ministrom właściwym do spraw wewnętrznych, do spraw oświaty i wychowania, do spraw szkolnictwa wyższego oraz do spraw kultury fizycznej, jeżeli jednocześnie są oni ich organizatorami (art. 2).

Ustawa definiuje precyzyjnie także poszczególne rodzaje imprez masowych, jednocześnie określając próg ilościowy miejsc udostępnionych dla uczestników, od którego możemy mówić o imprezie masowej.

Wedle ustawy imprezą masową artystyczno-rozrywkową jest impreza o charakterze artystycznym, rozrywkowym lub zorganizowane publiczne oglądanie przekazu telewizyjnego na ekranach lub urządzeniach umożliwiających uzyskanie obrazu o przekątnej przekraczającej 3 m, która ma się odbyć na stadionie, w innym obiekcie niebędącym budynkiem lub na terenie umożliwiającym przeprowadzenie imprezy

masowej (w których liczba udostępnionych przez organizatora miejsc dla osób, ustalona zgodnie z przepisami prawa budowlanego oraz przepisami dotyczącymi ochrony przeciwpożarowej, wynosi nie mniej niż 1 tys.) albo w hali sportowej lub w innym budynku umożliwiającym przeprowadzenie imprezy masowej (w których liczba udostępnionych przez organizatora miejsc dla osób, ustalona zgodnie z przepisami prawa budowlanego oraz przepisami dotyczącymi ochrony przeciwpożarowej, wynosi nie mniej niż 500). Zakwalifikowanie danej imprezy jako imprezy masowej jest zależne od wypełnienia następujących przesłanek: przedsięwzięcie musi spełniać warunki wynikające z definicji imprezy masowej, liczba miejsc udostępnionych dla uczestników przez organizatora nie może być niższa niż określona w ustawie oraz nie mogą wystąpić okoliczności wyłączające stosowanie ustawy.

Masowa impreza sportowa to impreza mająca na celu współzawodnictwo sportowe lub popularyzowanie kultury fizycznej, organizowana na stadionie lub w innym obiekcie niebędącym budynkiem (na którym liczba udostępnionych przez organizatora miejsc dla osób, ustalona zgodnie z przepisami prawa budowlanego oraz przepisami dotyczącymi ochrony przeciwpożarowej, wynosi nie mniej niż 1 tys., a w przypadku hali sportowej lub innego budynku umożliwiającego przeprowadzenie imprezy masowej – nie mniej niż 300) albo na terenie umożliwiającym przeprowadzenie imprezy masowej, na którym liczba udostępnionych przez organizatora miejsc dla osób wynosi nie mniej niż 1 tys. Mecz piłki nożnej to masowa impreza sportowa mająca na celu współzawodnictwo w dyscyplinie piłki nożnej, organizowana na stadionie lub w innym obiekcie sportowym, na którym liczba udostępnionych przez organizatora miejsc dla osób, ustalona zgodnie z przepisami prawa budowlanego oraz przepisami dotyczącymi ochrony przeciwpożarowej, wynosi nie mniej niż 1 tys.

Biorąc pod uwagę zdiagnozowane i potencjalne zagrożenia dla bezpieczeństwa uczestników imprezy lub → b e z p i e c z e ń s t w a p u b l i c z n e g o [t. 1] ustawodawca wprowadził do przepisów definicję imprezy o podwyższonym ryzyku, określając jednocześnie jej organizatorom surowsze wymogi organizacyjne zapewniające bezpieczeństwo. Zgodnie z ustawą taką imprezą jest impreza masowa, w czasie której, zgodnie z informacją o przewidywanych zagrożeniach lub dotychczasowymi doświadczeniami

dotyczącymi zachowania osób uczestniczących, istnieje obawa wystąpienia aktów →przemocy [t. 3] lub →agresji [t. 1]. Biorąc pod uwagę możliwe zakłócenie porządku publicznego i potencjalne akty agresji ustawodawca zmniejszył próg limitu miejsc dla uczestników imprezy pozwalający zakwalifikować ją jako imprezę masową, i tak limity te wynoszą nie mniej niż: 300 dla stadionu, innego obiektu niebędącego budynkiem lub terenu umożliwiającego przeprowadzenie imprezy masowej, 200 dla hali sportowej lub innego budynku umożliwiającego przeprowadzenie imprezy masowej, oraz 200 dla meczu piłki nożnej.

Ustawa o zabezpieczeniu imprez masowych ściśle narzuca organizatorowi imprezy masowej minimalną liczebność służby porządkowej (której głównym zadaniem jest dbanie o bezpieczeństwo i porządek podczas imprezy) oraz służby informacyjnej (której głównym zadaniem jest informowanie uczestników o zasadach bezpieczeństwa). W przypadku organizowania imprezy masowej niebędącej imprezą masową podwyższonego ryzyka organizator zapewnia minimum 10 członków służb (porządkowej i informacyjnej) na 300 osób, które mogą być obecne na imprezie masowej. W przypadku większej liczby uczestników organizator ma obowiązek zapewnić proporcjonalnie większą ilość służb. Na każde następne 100 osób mogących uczestniczyć w imprezie powinien zapewnić co najmniej 1 członka służby porządkowej lub służby informacyjnej, z zastrzeżeniem, że służby porządkowe powinny stanowić minimum 20% służb organizatora.

Zdecydowanie wyższe wymogi są stawiane wobec organizatora w przypadku przygotowywania imprezy masowej podwyższonego ryzyka. W takiej sytuacji ma on zapewnić co najmniej 15 członków służb: porządkowej i informacyjnej na 200 osób, które mogą być obecne na imprezie masowej. W przypadku większej liczby osób powinni zapewnić co najmniej 2 członków służb: porządkowej lub informacyjnej na każde następne 100 osób. Wymogiem jest w tym przypadku znaczne zwiększenie progu udziału członków służb porządkowych. Ich ilość nie powinna być mniejsza niż 50% ogólnej liczby członków służb organizatora.

Służbami informacyjnymi i służbami porządkowymi zarządza w imieniu organizatora imprezy kierownik do spraw bezpieczeństwa. Jego podstawowym zadaniem jest zapewnienie bezpieczeństwa uczestnikom imprezy masowej.

Uprawnienia służb porządkowych i informacyjnych pozwalają im na skuteczne podejmowanie działań związanych z zapewnieniem bezpieczeństwa na imprezie masowej. Ustawa o bezpieczeństwie imprez masowych (art. 20) nadała im uprawnienia do legitymowania osób w celu ustalenia ich tożsamości, sprawdzania i stwierdzania uprawnień osób do uczestniczenia w imprezie masowej oraz wezwania ich do opuszczenia imprezy, jeżeli nie posiadają stosownych uprawnień, przeglądania zawartości bagaży i odzieży osób w przypadku podejrzenia, że osoby te wnoszą lub posiadają broń lub inne niebezpieczne przedmioty, materiały wybuchowy, wyroby pirotechniczne, materiały pożarowo niebezpieczne, napoje alkoholowe czy też środki odurzające lub substancje psychotropowe. Posiadają uprawnienie do wydawania poleceń porządkowych osobom, które podczas imprezy zakłócają porządek publiczny lub zachowują się sprzecznie z regulaminem imprezy masowej (lub regulaminem obiektu, terenu), oraz do niewpuszczenia na teren imprezy osób posiadających orzeczony zakaz wstępu. W przypadku niestosowania się do poleceń służb porządkowych i informacyjnych mają prawo do wezwania takich osób do opuszczenia imprezy masowej. W przypadkach stwierdzenia osób stwarzających bezpośrednie zagrożenie dla dóbr powierzonych ochronie mają prawo do stosowania siły fizycznej w postaci chwytów obezwładniających lub innych technik obrony, a także kajdanek oraz miotaczy gazu, a w stosunku do osób dopuszczających się → c z y n ó w z a b r o n i o n y c h [t. 1] służby organizatora mają uprawnienie do ich ujęcia i niezwłocznego przekazania Policji.

Zapewnienie bezpieczeństwa podczas trwania imprezy masowej po stronie organizatora zawiera: spełnienie wymogów wyrażonych w przepisach prawa budowlanego, w przepisach sanitarnych i ochrony przeciwpożarowej; zapewnienie udziału służb informacyjnych i porządkowych oraz kierownika ds. bezpieczeństwa; zapewnienie pomocy medycznej; zapewnienie zaplecza higieniczno-sanitarnego; wyznaczenie dróg ewakuacyjnych; zapewnienie łączności; zapewnienie odpowiedniego sprzętu ratowniczego oraz gaśniczego; wyznaczenie miejsca dla służb kierujących zabezpieczeniem. Organizator musi opracować oraz udostępnić osobom uczestniczącym w imprezie masowej regulamin obiektu (terenu) oraz regulamin imprezy masowej. Jeżeli na imprezę wstęp jest odpłatny, musi też

posiadać ubezpieczenie od odpowiedzialności cywilnej za szkody wyrządzone osobom w niej uczestniczącym. W przypadku stwierdzenia szkód, które poniosły Policja, Żandarmeria Wojskowa, straż gminna (miejska), Państwowa Straż Pożarna i inne jednostki ochrony przeciwpożarowej oraz służba zdrowia, w związku z ich działaniami w miejscu i w czasie trwania imprezy masowej organizator odpowiada za ich równowartość.

Organizator imprezy masowej, nie później niż na 30 dni przed planowanym terminem rozpoczęcia imprezy masowej, ma obowiązek powiadomienia najbliżej położonego od miejsca odbywania imprezy masowej szpitala posiadającego szpitalny oddział ratunkowy albo szpitala posiadającego co najmniej: oddział anestezjologii i intensywnej terapii, chirurgii ogólnej z częścią urazową i oddział chorób wewnętrznych, podając lokalizację, rodzaj oraz przewidywaną liczbę uczestników organizowanej imprezy masowej. W przypadku imprezy masowej z udziałem ponad 10 tys. uczestników organizator imprezy masowej musi ponadto wyznaczyć koordynatora medycznego imprezy. Dodatkowo, w przypadku organizacji meczów piłki nożnej lub masowych imprez sportowych podwyższonego ryzyka, organizator do wniosku o wydanie zezwolenia załącza oświadczenie o spełnieniu wymogów w zakresie dodatkowego wyposażenia obiektu w elektroniczne systemy służące do: identyfikacji osób, sprzedaży biletów, kontroli przebywania w miejscu i w czasie trwania imprezy, kontroli dostępu do określonych miejsc oraz weryfikacji informacji o osobach, wobec których wydane zostało stosowne orzeczenie (zakazujące wstępu na imprezę masową, zobowiązujące do powstrzymania się od przebywania w miejscach przeprowadzania imprez masowych, wobec których wydany został zakaz zagraniczny lub zakaz klubowy).

Zezwolenie na przeprowadzenie imprezy masowej wydaje w drodze decyzji administracyjnej wójt, burmistrz albo prezydent miasta właściwy ze względu na miejsce przeprowadzenia imprezy masowej. W tym celu organizator imprezy masowej składa do uprawnionego organu wniosek o wydanie takiego zezwolenia. Wniosek powinien być złożony nie później niż 30 dni przed planowaną datą rozpoczęcia imprezy. Do wniosku powinny być dołączone opinie komendantów powiatowych Policji, Państwowej Straży Pożarnej, kierownika pogotowia ratunkowego i państwowego inspektora sanitarnego, dotyczące niezbędnej wielkości sił i środków na

zabezpieczenie imprezy masowej (art. 25 §1 pkt 2), regulamin i program imprezy, regulamin obiektu, a także informację o liczbie miejsc oraz liczbie służb porządkowych i informacyjnych. Organizator winien także wskazać zainstalowane urządzenia rejestrujące dźwięk i obraz. Opinie służb zachowują ważność przez 6 miesięcy od dnia ich wydania, a ich podstawą są przedłożone przez organizatora informacje oraz dokumentacja, a także lustracja obiektu (terenu), na którym ma być przeprowadzona impreza masowa. Komendant powiatowy (rejonowy, miejski) Policji wydaje opinię dodatkowo na podstawie analizy ryzyka, określającej przewidywane → z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4] i porządku publicznego mogące wystąpić w związku z imprezą masową.

Uprawniony organ wydaje zezwolenie albo odmawia jego wydania w terminie co najmniej 7 dni przed planowanym terminem przeprowadzenia imprezy masowej. Kopię decyzji organ wydający zezwolenie na przeprowadzenie imprezy masowej przekazuje niezwłocznie, nie później jednak niż w terminie 3 dni odpowiednim służbom oraz wojewodzie.

Na podstawie dokumentacji dołączonej do wniosku, w szczególności opinii komendanta powiatowego (rejonowego, miejskiego) Policji, informacji o przewidywanych zagrożeniach, czy też wniosku podmiotu zarządzającego rozgrywkami organ wydający decyzję może stwierdzić, że jest to impreza masowa podwyższonego ryzyka. Decyzja taka obliguje organizatora do weryfikacji założeń organizacyjnych i podniesienia poziomu zabezpieczenia imprezy zgodnie z wymogami ustawy. Jeżeli ocena bezpieczeństwa imprezy masowej wypadnie negatywnie, możliwe jest też jej przeprowadzenie bez udziału publiczności. Organ wydający zezwolenie na przeprowadzenie imprezy masowej kontroluje zgodność przebiegu imprezy masowej podwyższonego ryzyka z warunkami określonymi w zezwoleniu.

Wójt, burmistrz albo prezydent miasta odmawia wydania zezwolenia na przeprowadzenie imprezy masowej, gdy organizator: nie dołączy do wniosku wymaganych załączników lub opinii albo nie spełni innych narzuconych mu przez ustawę obowiązków i wymogów związanych z zapewnieniem bezpieczeństwa podczas trwania imprezy (art. 29 § 4). Organizatorowi przysługuje odwołanie od decyzji organu do samorządowego kolegium odwoławczego, którego termin rozpatrzenia wynosi 4 dni.

W przypadku stwierdzenia naruszenia warunków bezpieczeństwa imprezy masowej przez jej organizatora odpowiednie służby mogą wnioskować do organu, który wydał zezwolenie na przeprowadzenie imprezy masowej, o jej przerwanie. Organ wydaje taką decyzję w przypadku stwierdzenia niespełnienia przez organizatora warunków określonych w zezwoleniu, nadając jej rygor natychmiastowej wykonalności, o czym niezwłocznie powiadamia właściwego wojewodę. Decyzję doręcza się organizatorowi w terminie 7 dni od dnia przerwania imprezy.

W 2018 r. przeprowadzono 7822 imprezy masowe w Polsce, w związku z którymi Policja prowadziła działania zabezpieczające. Wśród nich 210 zakwalifikowanych zostało jako imprezy masowe podwyższonego ryzyka, stanowiąc 2,7% ogółu imprez masowych.

Krzysztof Dymura

Komenda Główna Policji, *Raport – Bezpieczeństwo imprez masowych w 2018 roku*, Warszawa 2019; S. Parszowski, A. Kruczyński, *Imprezy masowe, organizacja, bezpieczeństwo, dobre praktyki*, Wydawnictwo Difin, Warszawa 2015; A. Popławski, *Bezpieczeństwo imprez masowych – wybrane zagadnienia*, „Colloquium Wydziału Nauk Humanistycznych i Społecznych AMW" 2016, nr 3; J. Struniawski, *Dowodzenie w trakcie operacji policyjnych w zakresie imprez masowych i zgromadzeń publicznych*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2014; P. Suski, *Zgromadzenia i imprezy masowe*, Wydawnictwo LexisNexis, Warszawa 2010; B. Wiśniewski, R. Socha, M. Gracz, *Zasadnicze problemy prawno-organizacyjne bezpieczeństwa masowych imprez sportowych*, Wydawnictwo Wyższa Szkoła Administracji, Bielsko-Biała 2010; Ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, Dz. U. 2009, nr 62, poz. 504.

INDYWIDUALNE ŚRODKI OCHRONY LUDNOŚCI – najczęściej stosuje się w celu ochrony przed skażeniami, zwłaszcza przed wnikaniem środków trujących, biologicznych czy też pyłu radioaktywnego do wnętrza organizmu. Środki te służą ochronie całej powierzchni ciała, a także dróg oddechowych i oczu. Indywidualne środki ochrony przed skażeniami są stosowane przez →ludność cywilną [t. 3] i zapewniają jej →bezpieczeństwo [t. 1] w strefach objętych skażeniem oraz przez członków →formacji obrony cywilnej, którym umożliwiają prowadzenie

akcji ratowniczych na terenach skażonych. Środki tego typu są również wykorzystywane w określonych zakładach pracy.

Do indywidualnych środków → o c h r o n y l u d n o ś c i [t. 3] zaliczamy środki ochrony dróg oddechowych oraz środki ochrony skóry. Ochronę dróg oddechowych zapewniają maski przeciwgazowe filtracyjne i izolacyjne oraz respiratory. Działanie masek filtracyjnych polega na oczyszczaniu skażonego powietrza, które przechodzi przez specjalny pochłaniacz do układu oddechowego człowieka. Przeciwgazowa maska filtracyjna oczyszcza powietrze, ale nie wytwarza tlenu, zatem użycie takiej maski jest możliwe jedynie w sytuacji, gdy w atmosferze znajduje się minimum 17% tlenu. Standardowy pochłaniacz nie chroni przed tlenkiem węgla i nie można go stosować w czasie pożarów przestrzennych. Możemy wyróżnić maski przeciwgazowe filtracyjne wojskowe, cywilne, a także przemysłowe.

Do niedawna w wojsku polskim stosowano maski MP-4 i SzM-41, które zostały zastąpione nowoczesnymi maskami MP-5 oraz MP-6. Warto nadmienić, że nowelizacja doktryny obronnej z 2004 r., dokonana w 2014 r., rozszerzyła nieco zakres indywidualnych środków ochrony przed skażeniami stosowanych w wojsku. Mianowicie, → ż o ł n i e r z e [t. 4] oprócz masek i odzieży ochronnej zostali wyposażeni dodatkowo w indywidualne pakiety do likwidacji skażeń, sprzęt dozymetryczny oraz pakiety do udzielania → p i e r w s z e j p o m o c y [t. 3].

W przypadku masek cywilnych w użyciu są maski filtracyjne MC-1 – MS-3, składające się z części twarzowej i pochłaniacza. Na podstawie odpowiednich pomiarów głowy należy dopasować część twarzową. Maska jest prawidłowo dobrana i dopasowana, gdy górny brzeg przylega do czoła poniżej linii włosów, natomiast dolny obejmuje z łatwością podbródek i nie wrzyna się w krtań, obrzeża boczne maski nie dotykają małżowin usznych, a oczy znajdują się w połowie wysokości szkieł okularowych.

Kolejnym rodzajem indywidualnych środków ochrony dróg oddechowych, obok masek wojskowych i cywilnych, są maski przemysłowe, pochłaniacze przeciwgazowe oraz respiratory, stosowane na terenie większych przedsiębiorstw, hut, kopalń, a także zakładów, produkujących lub wykorzystujących w procesie produkcyjnym substancje niebezpieczne dla życia i zdrowia człowieka. W niektórych zakładach przemysłowych

na pracowników został nałożony bezwzględny obowiązek stosowania środków ochrony układu oddechowego w trakcie pracy, zwłaszcza w sytuacji, gdy zawartość tlenu w wydychanym powietrzu utrzymuje się na poziomie poniżej 17% jego składu, gdy stężenie groźnych substancji w powietrzu przekracza najwyższe dopuszczalne stężenia dla tych substancji, a także gdy temperatura wdychanego powietrza przekracza dopuszczalną normę umożliwiającą wykonywanie obowiązków zawodowych. Sprzęt wykorzystywany do ochrony dróg oddechowych m.in. w zakładach pracy został określony Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/425 z dnia 9 marca 2016 r. w sprawie środków ochrony indywidualnej oraz uchylenia dyrektywy Rady 89/686/EWG. Na mocy przepisów rozporządzenia za środki ochrony indywidualnej uznano środki zaprojektowane i wyprodukowane do noszenia bądź trzymania przez osobę w celu ochrony przed jednym lub większą liczbą → z a g r o ż e ń [t. 4] dla zdrowia lub bezpieczeństwa tej osoby; wymienialne elementy składowe tychże środków, implikujące ich funkcję ochronną; systemy przyłączy do środków, które nie są noszone ani trzymane przez osobę, są zaprojektowane do łączenia tych środków z urządzeniem zewnętrznym lub ze stabilnym punktem kotwiczącym, nie są przeznaczone do trwałego przymocowania i nie wymagają przeprowadzenia prac montażowych przed użyciem. Natomiast norma PN-EN 133 (Sprzęt ochrony układu oddechowego. Podział) określiła klasyfikację sprzętu, uwzględniając niedobór tlenu w powietrzu oraz obecność szkodliwych substancji (pyłów, gazów, oparów itp.). W konsekwencji ochrona dróg oddechowych polega na dostarczeniu powietrza z czystego źródła, wykorzystując sprzęt izolujący, a także na oczyszczaniu wdychanego powietrza dzięki sprzętowi oczyszczającemu. Sprzęt izolujący zapewnia dopływ świeżego powietrza z niezależnego źródła. Najczęściej akcesoria izolujące stosuje się przy zbyt niskiej zawartości tlenu w powietrzu, w przypadku wysokiego stężenia substancji szkodliwych (bądź jeśli stężenie nie jest nam dokładnie znane), gdy groźna substancja w postaci gazu nie posiada zapachu i nie można jej zidentyfikować, gdy proces filtracji powietrza okazuje się niewystarczający. Wśród sprzętu izolującego występują urządzenia autonomiczne (aparaty butlowe i regeneracyjne) oraz stacjonarne w postaci wężowych aparatów sprężonego powietrza.

Do sprzętu oczyszczającego zalicza się akcesoria umożliwiające oczyszczanie wdychanego powietrza ze szkodliwych substancji chemicznych oraz pyłów. Są nimi pochłaniacze zatrzymujące substancje chemiczne w gazowym stanie skupienia; filtry zatrzymujące cząsteczki stałe (pyły i kropelki cieczy w formie aerozolu – mgły); filtropochłaniacze stanowiące połączenie pochłaniaczy i filtrów. Wymieniony sprzęt oczyszczający jest skuteczny wyłącznie w połączeniu z częścią twarzową (z wyjątkiem przeciwpyłowych półmasek jednorazowych).

W przypadku ewakuacji ze strefy zagrożonej możemy również wskazać na sprzęt ucieczkowy. Akcesoria należące do sprzętu ucieczkowego stosuje się wyłącznie w nagłych sytuacjach wymagających natychmiastowego opuszczenia skażonej strefy.

Maski przemysłowe chronią drogi oddechowe pracowników narażonych bezpośrednio na kontakt m.in. z toksycznymi środkami przemysłowymi, substancjami chemicznymi oraz pyłami. Są wykorzystywane także w czasie likwidacji awarii oraz w trakcie akcji ratowniczych. Pochłaniacze przeciwgazowe można stosować zarówno do masek typu wojskowego i cywilnego, jak i do masek przemysłowych. Pochłaniacze służą do ochrony przed szkodliwym działaniem określonych środków toksycznych. Pochłaniacze są opatrzone oznakowaniem barwnym, które ułatwia ich identyfikację. Każdy pochłaniacz ma termin ważności. Używając pochłaniacza w sytuacji zagrożenia bronią masowego rażenia, należy wykazać się dokładną znajomością właściwości ochronnych konkretnych rodzajów pochłaniaczy. Nie wszystkie te środki gwarantują jednoczesną ochronę przed pyłem promieniotwórczym, aerozolem biologicznym oraz środkami trującymi.

Aby dobrać optymalną ochronę dróg oddechowych pracownika, należy uwzględnić określone czynniki, do których zaliczamy:

- ilość tlenu we wdychanym powietrzu;
- formę zanieczyszczeń;
- rodzaj oraz poziom stężenia niebezpiecznej substancji (w przypadku braku wiedzy na ten temat należy zastosować sprzęt izolujący);
- woń niebezpiecznej substancji (w sytuacji niewyczuwalnego zapachu należy skorzystać ze sprzętu izolującego, gdyż przy akcesoriach oczyszczających użytkownik nie będzie w stanie ocenić, czy doszło do uszkodzenia pochłaniacza);

- intensywność pracy;
- temperaturę i wilgotność otoczenia;
- czas pracy (czas użytkowania sprzętu ochrony dróg oddechowych jest zazwyczaj uzależniony od parametrów tego sprzętu);
- widoczność;
- komunikację;
- mobilność;
- szczelność maski;
- współdziałanie z innymi akcesoriami ochrony indywidualnej.

Przy dobieraniu właściwego filtru jest obligatoryjne obliczenie minimalnej wartości wskaźnika ochrony poprzez podzielenie stężenia substancji szkodliwej przez odpowiadające jej najwyższe dopuszczalne stężenie. Najwyższe dopuszczalne stężenie jest średnią ważoną wartością stężenia, którego oddziaływanie na pracownika przez 8 godzin dziennie przy przeciętnym tygodniowym wymiarze pracy (określonym w kodeksie pracy) przez okres jego aktywności zawodowej nie powinno powodować negatywnych zmian w jego stanie zdrowia oraz stanie zdrowia jego dzieci. Po obliczeniu minimalnej wartości wskaźnika ochrony należy wybrać klasę i rodzaj sprzętu, tak aby posiadał on wyższy poziom wskaźnika ochrony AFP (Assigned Protection Factor – spodziewany wskaźnik ochrony). Gdy w zakładzie pracy zostanie wykryta substancja zanieczyszczająca w formie pyłu o stężeniu 4,8 mg/m^3, a najwyższe dopuszczalne stężenie wynosi 0,6 mg/m^3, to minimalny wskaźnik ochrony wynosi 8 (4,8 : 0,6 = 8). Wówczas wybiera się sprzęt, dla którego AFP jest większe niż 8. Po dokonaniu właściwej identyfikacji substancji szkodliwej należy wybrać typ pochłaniacza, dobierając jednocześnie tzw. klasę ochrony pochłaniacza. Warunkiem jest pewność, że konkretny pochłaniacz podlegał testom wykonanym przez producenta, uzyskując akceptację pracy z konkretną substancją. Wówczas można dokonać obliczenia minimalnej wartości wskaźnika ochrony, dzieląc stężenie substancji przez jej najwyższe dopuszczalne stężenie. Następnie wybieramy rodzaj sprzętu, aby posiadał on wyższy poziom ochrony AFP. Jeśli substancją jest np. aceton, a jego stężenie wynosi 3000 mg/m^3, to należy podzielić to stężenie przez najwyższe dopuszczalne stężenie, które wynosi 200 mg/m^3 (3000 : 200 = 15). Minimalny poziom ochrony wynosi 15, zatem AFP sprzętu powinno być większe niż 15.

Drugim rodzajem masek przeciwgazowych, obok filtracyjnych, są maski izolacyjne, które pozwalają użytkownikowi oddychać powietrzem lub tlenem zgromadzonym lub wytworzonym w specjalnych urządzeniach znajdujących się na wyposażeniu masek izolacyjnych. Maski tego typu zapewniają całkowitą izolację dróg oddechowych, twarzy i oczu od skażonego powietrza. Powietrze służące do oddychania posiada zdolności regenerujące dzięki znajdującemu się w masce zapasowi tlenu i wchłanianiu dwutlenku węgla, który wydziela się w trakcie oddychania. Wśród masek przeciwgazowych izolacyjnych można dokonać jeszcze klasyfikacji na maski z chemicznym źródłem tlenu, maski z tlenem sprężonym oraz maski zawierające inne mieszanki oddechowe.

W ramach indywidualnych środków ochrony dróg oddechowych wyróżnia się dodatkowo tzw. środki zastępcze. Są one zazwyczaj wykorzystywane przez ludność cywilną, która nie ma dostępu do środków profesjonalnych. Należy jednak pamiętać, że środki zastępcze nie chronią przed działaniem bojowych środków trujących, a jedynie zabezpieczają drogi oddechowe przed skażeniami pyłem promieniotwórczym, pyłem nietoksycznym oraz częściowo przed bakteriami chorobotwórczymi. Chcąc ochronić drogi oddechowe, można użyć tamponów (opasek z gazy), opasek tkaninowych, respiratorów, masek przeciwpyłowych, półmasek przemysłowych, szala wełnianego lub ręcznika.

Kolejnym typem środków ochrony indywidualnej są środki ochrony skóry. Środki te gwarantują ochronę powierzchni ciała przed szkodliwym działaniem ciekłych substancji trujących i ich par, środków biologicznych, substancji promieniotwórczych oraz przed promieniowaniem cieplnym wybuchów jądrowych i środkami zapalającymi. Odzież ochronna występuje w wariancie hermetycznym i niehermetycznym. Do hermetycznych środków ochrony skóry zalicza się lekką odzież ochronną dwuczęściową (L-1) oraz jednoczęściową (L-2), wykonaną z podgumowanej tkaniny. Natomiast przykładem odzieży niehermetycznej jest ogólnowojskowa odzież ochronna.

Odzież ochronna lekka (L-1) jest wykorzystywana głównie w trakcie rozpoznania skażeń chemicznych i promieniotwórczych. L-1 składa się z bluzy z kapturem, spodni zaopatrzonych w pończochy ochronne i rękawic ochronnych. Wszystkie te elementy są umieszczone w odpowiedniej torbie.

Odzież ochronną lekką jednoczęściową (L-2) stosuje się w terenie silnie skażonym środkami trującymi lub substancjami promieniotwórczymi. Odzież L-2 składa się z kombinezonu, rękawic ochronnych i torby. Kombinezon tworzą kalosze, bluza i kaptur scalone w jedną całość.

Na ogólnowojskową odzież ochronną, stosowaną głównie przez jednostki ratownicze →obrony cywilnej [t. 3], składa się płaszcz ochronny, pończochy oraz pięciopalcowe rękawice ochronne. Ogólnowojskowa odzież ochronna jest stosowana w razie napadu chemicznego z użyciem →broni biologicznej [t. 1], a także przy opadaniu substancji promieniotwórczych z obłoku wybuchu jądrowego, w trakcie prowadzenia działań i zabiegów specjalnych na obszarze skażonym. Płaszcz może służyć również jako narzutka lub kombinezon. Płaszcz ochronny użyty wraz z rękawami może być wykorzystywany w trakcie przebywania w rejonie skażonym pyłem promieniotwórczym bądź skażonym środkami biologicznymi, w trakcie odkażania, dezaktywacji i dezynfekcji. W trakcie opadania pyłu promieniotwórczego płaszcz ochronny jest stosowany jako narzutka.

W Wojsku Polskim izolacyjna odzież ochronna OP-1 została zastąpiona odzieżą filtracyjną FOO-1, która wraz z maską przeciwgazową chroni żołnierza przed skażeniami chemicznymi, biologicznymi i promieniotwórczymi, stanowiąc jednocześnie efektywną barierę dla promieniowania alfa oraz częściowo dla promieniowania beta. Celem poprawy ochrony przed ciekłymi środkami trującymi oraz opadem promieniotwórczym na FOO-1 należy dodatkowo założyć narzutkę ochronną. Narzutka ochronna NO-1 wraz z filtracyjną odzieżą ochronną i maską przeciwgazową ma chronić żołnierza przed kroplami bojowych środków trujących, środków biologicznych, pyłem promieniotwórczym, ciekłymi wysokotoksycznymi substancjami przemysłowymi, produktami ropopochodnymi, a także opadami atmosferycznymi.

Ponadto żołnierze Wojska Polskiego zostali wyposażeni w lekką izolacyjną odzież ochronną LIOO-1 (w komplecie z maską przeciwgazową), przeznaczoną do ochrony skóry i układu oddechowego przed działaniem bojowych środków trujących oraz toksycznych środków przemysłowych, również biologicznych, w postaci par, aerozoli, pyłu czy też kropel. Odzież ochronna LIOO-1 zabezpiecza przed promieniowaniem alfa oraz

częściowo – przed promieniowaniem beta. Jest wykonana z materiału posiadającego właściwości samogasnące.

Jako środki zastępcze ochrony skóry można wykorzystać:

- płaszcze i peleryny przeciwdeszczowe z płótna impregnowanego lub podgumowanego, gumy, tkaniny z włókien sztucznych, plastyków;
- gumowe obuwie wykonane z tworzyw oraz skóry z długimi cholewami, śniegowce;
- okulary ochronne (przemysłowe, motocyklowe, gogle narciarskie);
- nakrycia głowy wykonane ze skóry, gumy lub tworzyw.

Wykorzystując zastępcze środki ochrony skóry, uzupełnione maską lub półmaską, można w warunkach skażeń przemieszczać się po niewielkich odcinkach terenu, aby wydostać się ze strefy skażonej, docierając do ukryć, lub podjąć obligatoryjne, niezbyt czasochłonne czynności ratownicze.

Julia Anna Gawęcka

R. Kalinowski, *Obrona cywilna w Polsce*, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce 2011; tenże, *Ochrona ludności – bezpieczeństwo – nauka i edukacja*, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce 2011; tenże, *Monitorowanie zagrożeń*, Wydawnictwo Akademii Podlaskiej, Siedlce 2003; W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilne. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny*, Wydawnictwo Towarzystwa Wiedzy Obronnej, Warszawa 2010; P. Maciejewski, W. Robak, *Indywidualne środki ochrony przed skażeniami w Wojsku Polskim*, „Bezpieczeństwo i Technika Pożarnicza" 2015, vol. 37, iss. 1; B. Michailiuk, *Miejsce ochrony ludności i ratownictwa w systemie bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, „Zeszyty Naukowe WSEI. Seria: Administracja" 2015, nr 5 (1); tenże, *Podsystem ratownictwa i ochrony ludności*. „Zeszyty Naukowe AON" 2013, nr 4 (93); E. Najbert, K. Sipowicz, T. Pietras, *Wielowymiarowy aspekt kryzysu w teorii i praktyce*, Wydawnictwo e-bookowo, Będzin 2017; *Obrona narodowa w tworzeniu bezpieczeństwa Polski w XXI w.*, R. Jakubczak, A. Skrabacz, K. Gąsiorek (red.), Wydawnictwo Bellona, Warszawa 2008; *Ochrona dróg oddechowych – podstawowe informacje*, Glovex.com.pl (dostęp 30.01.2020); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/425 z dnia 9 marca 2016 r. w sprawie środków ochrony indywidualnej oraz uchylenia dyrektywy Rady 89/686/EWG; P. Szmitkowski, *System ochrony ludności w Polsce – historia i współczesność*, „Colloquium Wydziału Nauk Humanistycznych i Społecznych AMW" 2012, nr 4.

INFORMACJA – pojęcie pierwotne, niedefiniowalne w sensie normatywnym. Należy do konstytutywnych własności otaczającej nas rzeczywistości, takich jak energia czy materia. Wszystkie występujące w niej obiekty oddziałują na siebie w sposób materialny, energetyczny lub informacyjny. Konstatacja ta nie ułatwia opisania pojęcia, które interpretowane jest na tyle sposobów, ile jest dyscyplin i badaczy reprezentujących w uprawianych przez siebie domenach zindywidualizowane podejście do fenomenu informacji. M.J. Schroeder proponuje wybór definicji wyjaśniającej istotę znaczenia pojęcia informacji opartej na „tożsamościowej koncepcji informacji", wg której informacja jest identyfikacją wielości (nadanie wielości charakteru jedności). Dochodzi do niej na podstawie analizy sporu prowadzonego w nauce na temat wyboru optymalnej konwencji dotyczącej nazwy dyscypliny, której system pojęciowy dotyczy informacji. Spory te dotyczą analizowanego pojęcia głównie w wymiarze epistemologicznym i ontologicznym. W podejściach tych uwaga skoncentrowana jest na ilościowej analizie informacji lub na analizie sposobu istnienia informacji, na traktowaniu informacji jako zjawiska naturalnego lub artefaktu, na rozumieniu informacji w terminach selekcji lub w terminach struktury.

W najogólniejszym ujęciu, proponowanym przez filozofię, informację postrzega się jako odbicie (odwzorowanie) różnorodności cechującej otaczającą rzeczywistość (obiekt, zdarzenie, proces, zjawisko). Większość definicji i interpretacji informacji odnosi ją do otoczenia, w którym występuje pewien odbiorca – adresat treści. Może nim być zarówno człowiek, jak i dowolny system, np. informacyjny, w którym są wykorzystywane technologie informatyczne do zarządzania →procesami informacyjnymi [t. 3]. Definicje najczęściej ukazują informację jako coś, co istnieje, lecz – jak zaznacza B. Stefanowicz – nie operacjonalizują tego pojęcia, tj. nie podają żadnych wskazówek, jak ją można analizować, organizować procesy jej przetwarzania, jak ową treść rejestrować lub realizować inne stosowne operacje. Jest ono opisywane zarówno przez ilościową, jak i jakościową teorię informacji.

Ilościowa teoria informacji stworzona przez C.E. Shannona zajmuje się badaniem zjawisk informacyjnych w aspekcie wykrywania w nich zmian stopnia nieokreśloności w zależności od wyróżnionego stanu danego układu. Teoria ta nie zajmuje się kwestiami dotyczącymi znaczenia

informacji, a jej związek z informacją wynika z przekonania, że gdy znamy rozkład prawdopodobieństwa wyboru elementów pewnego zbioru, możemy określić miarę czegoś, co może być interpretowane jako informacja „wyprodukowana" przez taki wybór. Wielkość tej wyprodukowanej informacji – entropia – oznacza miarę przenoszonej przez wiadomość informacji i wyznacza stopień nieokreśloności informacyjnej układu (miara niewiedzy o układzie). Informacja jest więc otrzymanym i zinterpretowanym komunikatem (zbiorem znaków danego kodu nadawanych i odbieranych). Obszarem zainteresowania jakościowej teorii informacji, a właściwie infologicznej teorii informacji, której podwaliny stworzyli B. Langefors i B. Sundgren, są własności informacji i znaczenie informacji postrzeganej w aspekcie użytkowym. Informacja jest definiowana jako nazwa treści zaczerpniętej ze świata zewnętrznego lub znaczenie (treść), jakie przypisuje się danym z uwzględnieniem czynników psychologicznych (wpływ osobowości na kształtowanie znaczenia), socjologicznych (wpływ rodzaju siły i kierunków interakcji między ludźmi na znaczenie informacji), językowych (wpływ języka) i semantycznych (proces nadawania sensu i istotności).

Wg infologicznej koncepcji informacji opisanej przez Stefanowicza informacja (jako treść zawarta w komunikatach) cechuje się następującymi własnościami:

- informacja jako treść komunikatu nie istnieje poza tym komunikatem i jej nośnikiem;
- informacja o obiekcie wymienionym w komunikacie istnieje niezależnie od podmiotu, który ją odbiera, wyjątek stanowią obiekty myślowe, powstające w umyśle człowieka – każda informacja jest informacją obiektywną;
- te same informacje mają różne znaczenie dla różnych odbiorców (użytkowników) zależnie od ich potrzeb informacyjnych, zainteresowań, rozwiązywanych problemów, dotychczasowej wiedzy, doświadczenia oraz czasu, w jakim są wykorzystywane;
- każda jednostkowa informacja ukazuje tylko pewien wycinek otoczenia;
- informacja przejawia cechę synergii powstającą na skutek obserwowania wybranego obiektu z kilku perspektyw i sprawia, że

łączne rozpatrywanie pozyskanych informacji sprzyja pełniejszemu, głębszemu i szerszemu poznaniu świata oraz ułatwia podjęcie racjonalniejszych decyzji nawet przy ograniczonych zasobach informacyjnych i mniejszych kosztach;

- odebrana przez użytkownika informacja o obiekcie jest przez niego łączona ze znanymi mu wcześniej informacjami na ten temat – ostateczny obraz obiektu, który po odebraniu tej samej informacji powstanie u 2 różnych odbiorców, może różnić się bardziej, niż to wynika z dostarczonej informacji; uzasadnia to potęgowanie się różnic w poglądach różnych osób na temat tych samych faktów, zdarzeń, zjawisk i procesów pod wpływem tych samych odbieranych informacji;
- własnością informacji jest jej różnorodność, wynikająca z odmienności i zróżnicowania rozpatrywanych obiektów, rozmaitości źródeł informacji oraz subiektywnego ich interpretowania przez użytkowników;
- informacja może być przetwarzana, powielana i przenoszona w czasie i przestrzeni i może w tym procesie ulec rozmaitym deformacjom i zniekształceniom z powodu czynników zakłócających (szumów);
- informacja jest zasobem niewyczerpywalnym;
- informacja kosztuje;
- rozkład informacji w otoczeniu jest nierównomierny, co wywołuje jej asymetrię i wpływa na kształtowanie się struktury społecznej.

W koncepcji infologicznej informacja spełnia następujące funkcje: informacyjną, sterującą, opiniotwórczą, demokratyzującą, wychowawczą, integracyjną, motywacyjną, terapeutyczną, czynnika kulturotwórczego, śladu ludzkiego bytowania, kapitału, towaru przeznaczonego do wymiany, zasobu do wykorzystania w przyszłości, „łagodnej siły", atrybutu władzy itd. Znaczenie informacji jest więc ściśle związane z osobą twórcy lub odbiorcy informacji. Niemożliwe jest dokładne przewidywanie przyszłych potrzeb informacyjnych, bo nie można przewidzieć, jakie znaczenie użytkownik nada informacji w przyszłości. Nie jest też możliwe poznanie znaczenia informacji wejściowych bez znajomości celu, który sobie wytyczył jej użytkownik.

J. Unlod optuje za datalogiczną interpretacją informacji, zgodnie z którą pomijane są czynniki socjopsychologiczne, a jej źródłem są dane ustrukturyzowane niosące informację użyteczną. Oznacza to, że informacja pełni funkcję poznawczą, decyzyjną, wykonawczą w określonym systemie zarządzania informacją. Autor umiejscawia informacje na poziomie całego systemu informacyjnego w organizacji i uznaje, że podstawowym kryterium użyteczności systemu informacyjnego zarządzania jest jego zdolność do ograniczania rozbieżności pomiędzy infologicznym a datalogicznym znaczeniem informacji.

W tym miejscu konieczne jest ustosunkowanie się do relacji, jakie łączą informacje z danymi, wiedzą i mądrością. Obrazuje ją funkcjonująca w literaturze tzw. piramida informacji, hierarchia wiedzy, trójkąt niematerialnych zasobów organizacji, model T.S. Eliota, które sytuują dane i informacje na najniższym poziomie piramidy jako te, które mogą być zbierane przez komputery i gromadzone w stworzonych do tego celu bazach danych, ponieważ poddawane są głównie takim procesom jak przechowywanie i przetwarzanie. Natomiast mądrość i wiedza zarezerwowane są dla ludzi, gdyż wymagają one umiejętności podejmowania decyzji, umiejętności osądu, rozumienia zasad i mentoringu. Ponieważ wiedza traktowana jest jako nieodłączny element ludzkiego umysłu i ludzkiego poznania, transformacja informacji w wiedzę może zachodzić tylko w umyśle człowieka. Natomiast transformacja danych w informacje wymaga szeregu działań, takich jak kontekstualizacja, kategoryzacja danych, kalkulacja i obliczanie, korygowanie czy kondensacja danych. Jak podsumowuje K. Materska, „poprzez każdą z tych transformacji dodajemy do danych pewną wartość dodaną, tworząc z nich informacje". Wartość dodana przy transformacji danych w informacje łączy się z procesami organizacji danych i syntezą informacji, transformacja informacji w wiedzę wymaga łączenia procesów syntezy z procesami osądu, a przy transformacji wiedzy w mądrość konieczne jest przechodzenie od procesów osądu do procesów decyzyjnych. Dostrzegalny jest zatem brak wyraźnych granic pomiędzy przemianą danych w informację a informacji w wiedzę. Dlatego Materska proponuje przyjęcie modelu kontinuum: dane – informacja – wiedza, w którym granice przechodzenia z jednego stanu do drugiego są rozmyte i ciągle „stają się", ponieważ wykorzystanie wiedzy powoduje konieczność

pozyskania nowych danych i nowej informacji, co uzasadnia zamknięcie cyklu transformacji: organizacja danych – zarządzanie informacją – tworzenie wiedzy – organizacja nowych danych – zarządzanie nowymi danymi – tworzenie nowej wiedzy – organizacja kolejnych danych itd.

Do dyskursu dotyczącego pojęcia informacji włączyli się także M. Grabowski i A. Zając, określając informację jako dane zawarte w komunikacie, zinterpretowane przez odbiorcę, mające dla niego znaczenie i wnoszące do jego świadomości element nowości, czyli zmniejszające jego niewiedzę. Ponieważ informacja zależy od zdolności interpretacyjnych odbiorcy, ma ona charakter subiektywny. Dla odbiorcy informacji ważna jest jej jakość, która wynika z takich cech, jak: celowość, rzetelność, aktualność, kompletność, wszechstronność, odpowiednia dokładność, uzasadnione nakłady finansowe. Oczekuje się więc informacji, która powinna być efektywna, wydajna, poufna, integralna, dostępna, zgodna i wiarygodna. Z kolei dla W. Babika informacje to ustrukturyzowane strumienie danych rejestrowane przez zmysły człowieka, a następnie przetwarzane intelektualnie i wpuszczane w obieg społeczny. K. Krzysztofek postrzega ją jako dostrzeżone i zinterpretowane dane o faktach i bytach, M. Próchnicka informację traktuje jako odpowiedź na pytania użytkowników skierowane do systemu informacyjnego, będące podstawą dialogu zmierzającego do pozyskania informacji zlokalizowanych w otoczeniu słów kluczowych. J. Kossecki definiuje informację jako bodziec, za pomocą którego można sterować społeczeństwem, a Materska postuluje rozpatrywanie informacji w kategorii manipulacji zachowaniami i postawami ludzi, podmiotów gospodarczych i społecznych. Rosnące znaczenie jej funkcji sterującej i konsumpcyjnej świadczy o tym, że w coraz mniejszym stopniu wypełnia ona swoją funkcję podstawową, czyli odwzorowującą rzeczywistość.

Informacja wpisuje się do tezaurusa pojęć badaczy problemów → zagrożeń [t. 4] generowanych przez → społeczeństwo informacyjne [t. 4] oraz procesy globalizacyjne. Konteksty pozyskiwania przewagi za pomocą informacji H. Batorowska odnosi m.in. do postrzegania jej jako fetyszu społeczeństwa (nie)wiedzy, patogenu → infosfery, broni masowej manipulacji, tworzywa inwigilacji, potencjału → wywiadu [t. 4] gospodarczego i politycznego, oręża walki informacyjnej, DNA → cyberzagrożeń [t. 1] itd. Rodzi to uzasadnione pytanie, czy społeczeństwo

informacyjne jest społeczeństwem poinformowanym, źle informowanym czy dezinformowanym. W dyskursie tym P. Sienkiewicz wskazuje na wagę zagrożeń systemowych wynikających z dominacji elit niekorzystających z wiedzy eksperckiej.

Hanna Batorowska

Analiza pojęcia informacji, J.J. Jadacki (red.), Wydawnictwo Naukowe Semper, Warszawa 2003; H. Batorowska, *Konsumpcja informacji a sztuka jej przetwarzania*, [w:] *Człowiek – Media – Edukacja*, J. Morbitzer, D. Morańska, E. Musiał (red.), Wyższa Szkoła Biznesu, Dąbrowa Górnicza 2015; H. Batorowska, B. Czubała, *Wybrane zagadnienia nauki o informacji i technologii informacyjnej*, Wydawnictwo Naukowe WSP, Kraków 2000; M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe UE w Krakowie" 2009, nr 798; M. Hetmański, *Świat informacji*, Wydawnictwo Difin, Warszawa 2015; tenże, *Epistemologia informacji*, Copernicus Center Press, Kraków 2013; J. Kossecki, *Cybernetyka społeczna*, Państwowe Wydawnictwo Naukowe, Warszawa 1981; K. Krzysztofek, *Obszary i konteksty informatologii w epoce cyfrowej: sieci – informacja – dane – software*, „ZIN" 2014, nr 1; K. Materska, *Informacja w organizacjach społeczeństwa wiedzy*, Wydawnictwo SBP, Warszawa 2007; J. Mikułowski-Pomorski, *Informacja a komunikacja*, Ossolineum, Wrocław 1987; G. Nowacki, *Działania informacyjne w operacjach połączonych*, AON, Warszawa 2004; M. Próchnicka, *Człowiek i komputer. Dialogowy model wyszukiwania informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2004; Z. Ryznar, *Nieodzowny wstęp do informacji*, „CXO Magazyn Kadry Zarządzającej" 2001, nr 1; M.J. Schroeder, *Tożsamościowa koncepcja informacji*, „Studia Metodologiczne" 2015, nr 34; P. Virolio, *Bomba informacyjna*, Wydawnictwo Sic!, Warszawa 2006; B. Stefanowicz, *Informacja*, Oficyna Wydawnicza SGH, Warszawa 2010; tenże, *Informacja, wiedza, mądrość*, GUS, Warszawa 2013; J. Unlod, *System informacyjny a jakościowe ujęcie informacji*, [w:] *SWO – Systemy Wspomagania Organizacji*, Prace Naukowe AE w Katowicach, Katowice 2007.

INFORMACJE NIEJAWNE – wg polskiej ustawy o ochronie informacji niejawnych to → i n f o r m a c j e, których „nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania".

Informacja obecnie jest cennym towarem, często decydującym nie tylko o rozwoju gospodarczym danej społeczności, ale także wpływającym na stabilność funkcjonowania i → b e z p i e c z e ń s t w a [t. 1] całego państwa. Według *Słownika języka polskiego PWN* informacja jest tym, co powiedziano lub napisano o kimś lub o czymś, to także zakomunikowanie czegoś. Informacja jest zjawiskiem społecznym, służy do społecznego komunikowania się.

Wolność informacyjna jest istotnym warunkiem funkcjonowania systemu demokratycznego. Przedmiotem wolności informacyjnej są wszelkie informacje, do których dostęp nie został ustawowo ograniczony, w tym również informacje publiczne. Konstytucja Rzeczypospolitej Polskiej w art. 54 zasadę wolności informacyjnej definiuje szeroko, zapewniając każdemu wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji, oraz wprowadza zakaz stosowania → c e n z u r y [t. 1] prewencyjnej czy też koncesjonowania prasy. Dodatkowo w art. 61 Konstytucji RP określono, że każdy obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Ograniczenie tego prawa może nastąpić wyjątkowo w sytuacjach opisanych w ustawie. Dopuszczalność ograniczenia dostępu do informacji publicznych może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa (art. 61 ust. 3 Konstytucji RP).

Należy zauważyć, że bezpieczeństwo funkcjonowania państwa wymaga chronienia informacji szczególnie istotnych dla jego interesów i sprawnego działania. Ochrona informacji niejawnych w dobie rosnącego znaczenia → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o [t. 1] to jeden z najważniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa. W związku z tym zarówno zaznaczona w art. 54 Konstytucji RP wolność wyrażania poglądów, jak i wynikające z art. 61 Konstytucji RP prawo dostępu do informacji publicznej nie mają charakteru absolutnego i mogą podlegać ograniczeniom. Zagadnienie to ze względu na konieczność ograniczenia powszechnego dostępu do danych i informacji wrażliwych dla bezpieczeństwa państwa zostało uwzględnione w systemie prawnym Rzeczypospolitej Polskiej. Art. 31 ust. 3 Konstytucji RP zawiera 3 kryteria

oceny dopuszczalności ograniczeń praw i wolności: zasadę wyłączności ustawy, zasadę proporcjonalności (wyrażoną w sformułowaniu: „gdy są konieczne w demokratycznym państwie") oraz obowiązek poszanowania (zachowania) istoty wolności i praw.

Dla ustalenia pojęcia tajemnicy w znaczeniu normatywnym w doktrynie oraz orzecznictwie sądów administracyjnych proponuje się wyróżnienie tajemnicy prawnie chronionej oparte na łącznym współistnieniu 2 przesłanek: materialnej i formalnej. Materialne przesłanki obejmują zakres podmiotowy, w tym wskazanie podmiotów zobowiązanych i beneficjentów tajemnicy, zakres przedmiotowy oraz zakres czasowy utajnienia. Przesłanka formalna to wola utajnienia przejawiająca się poprzez określoną formę utajnienia (z mocy ustawy, poprzez czynność nadania klauzuli tajności, umowę) lub odtajnienia informacji (zgoda beneficjenta tajemnicy, postanowienie sądu).

W 2013 r. opublikowano →*Białą Księgę Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* [t. 1], która wskazuje zagadnienia związane z ochroną informacji niejawnych jako jeden z najważniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa (jako istotny element *Podsystemu ochronnego*) w dobie rosnącego znaczenia bezpieczeństwa informacyjnego. Główne zadania w podsystemach ochronnych obejmują zapewnienie warunków dla utrzymywania ładu konstytucyjnego, wewnętrznej stabilności państwa oraz bezpieczeństwa ludności. W szczególności zadania te dotyczą ochrony instytucji państwa, obywateli, wspólnych i indywidualnych zasobów materialnych i niematerialnych przed →zagrożeniami [t. 4] niemilitarnymi. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* stała się podstawą do stworzenia Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej jako dokumentu określającego priorytety państwa w zakresie szeroko pojętego zagadnienia bezpieczeństwa. Określono w nim, że bezpieczeństwo informacyjne, w tym ochrona informacji niejawnych, to jeden z najważniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa. Kluczowe zadania w tym zakresie obejmują zapewnienie bezpieczeństwa informacyjnego państwa poprzez zapobieganie uzyskaniu nieuprawnionego dostępu do informacji niejawnych i ich ujawnieniu, zapewnianie personalnego, technicznego i fizycznego bezpieczeństwa

informacji niejawnych, akredytację systemów teleinformatycznych służących przetwarzaniu tych informacji oraz zapewnienie realizacji funkcji krajowej władzy bezpieczeństwa w celu umożliwienia międzynarodowej wymiany informacji niejawnych.

Podstawowym aktem prawnym regulującym tematykę ochrony informacji niejawnych w Polsce jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Ustawa ta zastąpiła wielokrotnie i obszernie nowelizowaną ustawę o ochronie informacji niejawnych z 1999 r., która wprawdzie przez 10 lat obowiązywania pozwoliła stworzyć współczesny system ochrony informacji niejawnych oraz odegrała istotną rolę w okresie akcesji Polski do → NATO [t. 3], ale poddawana była krytyce za niespójność, niekonsekwencję, a nawet sprzeczność z Konstytucją RP. W obecnie obowiązującej ustawie przedmiotem ochrony są informacje o szczególnym charakterze i zakresie, które ze względu na specyfikę podlegają ochronie. Wyłączenie jawności tych informacji ma ścisły związek z interesami państwowymi. Zapewnienie bezpieczeństwa tym zasobom informacji ma wykluczać nieuprawnione ujawnienie, które mogłoby przynieść szkody dla Rzeczpospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne. Ustawa w sposób kompleksowy określa zasady ochrony informacji niejawnych, w szczególności klasyfikuje informacje niejawne, określa zasady organizowania ochrony i przetwarzania informacji niejawnych (w tym w systemach teleinformatycznych), organizacji kontroli stanu zabezpieczenia informacji niejawnych i stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych. Ustawa określa także sposób prowadzenia postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy (wprowadzając 2 rodzaje postępowań – sprawdzających i kontrolnych postępowań sprawdzających) oraz postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych (postępowanie bezpieczeństwa przemysłowego).

Zakres podmiotowy obowiązywania ustawy o ochronie informacji niejawnych ma bardzo szerokie zastosowanie obejmujące organy władzy publicznej (Sejm i Senat, Prezydenta Rzeczypospolitej Polskiej, organy administracji rządowej, organy jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie

nadzorowanych, sądy i trybunały, organy kontroli państwowej i ochrony prawa), jednostki organizacyjne podległe ministrowi obrony narodowej lub przez niego nadzorowane, Narodowy Bank Polski, państwowe osoby prawne i jednostki organizacyjne, jednostki organizacyjne podległe organom władzy publicznej lub nadzorowane przez te organy, a także przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

Ustawa o ochronie informacji niejawnych z 2010 r. określa rodzaj klauzuli tajności i definiuje je. Klauzula, zgodnie ze Słownikiem języka polskiego, to zastrzeżenie lub warunek w umowie, układzie, traktacie. W ustawie zostały określone 4 kategorie informacji sklasyfikowanych ze względu na istotność w zakresie bezpieczeństwa i interesów państwa: „ściśle tajne", „tajne", „poufne", „zastrzeżone".

Najwyższą obowiązującą klauzulą informacji niejawnych w Polsce jest klauzula „ściśle tajne". Nieuprawnione ujawnienie informacji nią opatrzonych spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- zagrozi niepodległości, → suwerenności [t. 4] lub integralności terytorialnej Rzeczypospolitej Polskiej;
- zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
- zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- osłabi gotowość obronną Rzeczypospolitej Polskiej;
- doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, → żołnierzy [t. 4] lub pracowników służb odpowiedzialnych za realizację zadań → wywiadu [t. 4] lub → kontrwywiadu, którzy wykonują → czynności operacyjno-rozpoznawcze [t. 1], jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
- zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności

operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
- zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w Ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka, albo świadków, o których mowa w art. 184 (świadek anonimowy) Ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, lub osób dla nich najbliższych.

Klauzulą „tajne" oznacza się informacje niejawne, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:
- uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- zakłóci przygotowania obronne państwa lub funkcjonowanie → Sił Zbrojnych Rzeczypospolitej Polskiej [t. 4];
- utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

Informacjom niejawnym nadaje się klauzulę „poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:
- utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;

- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie →obrony narodowej [t. 3], polityki zagranicznej, →bezpieczeństwa publicznego [t. 1], przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej, której nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej.

Dokumenty niejawne posiadają cechy polegające na oznaczeniu, nadaniu i fizycznym naniesieniu odpowiednich klauzuli tajności. Zasady tworzenia dokumentów niejawnych zostały określone w Rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności. Zgodnie z tymi wytycznymi na dokumentach niejawnych nanosi się symbole oznaczenia klauzul tajności: dla klauzuli „ściśle tajne" – symbol „oo"; dla klauzuli „tajne" – symbol „o"; dla klauzuli „poufne" – symbol „Pf"; dla klauzuli „zastrzeżone" – symbol „Z".

System prawny ochrony informacji niejawnych w Polsce określił, że za ochronę informacji niejawnych odpowiedzialni są kierownicy jednostek organizacyjnych. To właśnie ich zadaniem jest zorganizowanie i zapewnienie funkcjonowania tej ochrony. Zobowiązani zostali do utworzenia kancelarii tajnych do przetwarzania informacji niejawnych o klauzuli tajne i ściśle tajne oraz poinformowania o tym →Agencji Bezpieczeństwa Wewnętrznego [t. 1] lub →Służby Kontrwywiadu

Wojskowego [t. 4]. Kancelaria tajna podlega pełnomocnikowi ochrony i jest obsługiwana przez pracowników pionu ochrony. Kancelarie tajne odpowiedzialne są za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom. Wedle ustawy o ochronie informacji niejawnych kierownik jednostki organizacyjnej, gdzie przetwarzane są informacje niejawne, powołuje pełnomocnika do spraw ochrony informacji niejawnych, który bezpośrednio odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Pełnomocnik podlega bezpośrednio kierownikowi jednostki. Pełnomocnik do spraw ochrony informacji niejawnych zobowiązany jest do sporządzenia dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem (bądź ich utratą) do informacji niejawnych o klauzuli „poufne" lub wyższej. Sporządza on instrukcję sposobu i trybu przetwarzania informacji niejawnych o klauzuli zastrzeżone oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony. Wszystkie wymienione dokumenty zatwierdza kierownik jednostki organizacyjnej. Jeżeli w jednostce organizacyjnej funkcjonują systemy teleinformatyczne do przetwarzania informacji niejawnych o klauzuli od „poufne" i wyżej, konieczne jest wykonanie akredytacji bezpieczeństwa teleinformatycznego. Do nadzoru nad funkcjonowaniem systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa kierownik jednostki organizacyjnej powołuje inspektora bezpieczeństwa teleinformatycznego. Kierownicy jednostek mogą polecić łączenie funkcji pełnomocnika do spraw informacji niejawnych z funkcją inspektora bezpieczeństwa teleinformatycznego.

W sytuacji, gdy dochodzi do naruszenia przepisów o ochronie informacji niejawnych, pełnomocnik ochrony danej jednostki zawiadamia kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności naruszenia oraz dąży do ograniczenia jego negatywnych skutków. W przypadku, gdy nieprawidłowości dotyczą informacji niejawnych o klauzuli „poufne" lub wyższej, pełnomocnik ochrony zawiadamia również niezwłocznie odpowiednio Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego o naruszeniach przepisów.

Pełnienie funkcji pełnomocnika do spraw ochrony informacji niejawnych wymaga ścisłej współpracy z kierownikiem jednostki w celu

skutecznego rozpoznawania i rozwiązywania problemów organizacji ochrony, a także inicjowania nowych rozwiązań zmierzających do eliminacji potencjalnych zagrożeń. Należy podkreślić, że stwierdzone uchybienia i nieprawidłowości w ochronie informacji niejawnych mogą skutkować odpowiedzialnością karną nie tylko dla pełnomocnika do spraw ochrony informacji niejawnych, ale również dla kierownika jednostki organizacyjnej.

Zgodnie z art. 21 ustawy o ochronie informacji niejawnych dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej może nastąpić w przypadku uzyskania poświadczenia bezpieczeństwa i odbycia szkolenia w zakresie ochrony informacji niejawnych. Zgodnie z ustawą o ochronie informacji niejawnych pełnomocnik ochrony przeprowadza zwykłe postępowania sprawdzające lub poszerzone postępowania sprawdzające. Pozytywne zakończenie zwykłego postępowania sprawdzającego upoważnia do dostępu do informacji niejawnych o klauzuli „poufne", a poszerzonego postępowania sprawdzającego do dostępu do klauzuli „tajne" lub „ściśle tajne". Ustawowym wymogiem w zakresie dostępu, dopuszczenia do pracy lub pełnienia służby na stanowiskach albo zlecenia prac związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone" wystarczającym jest posiadanie pisemnego upoważnienia wydanego przez kierownika jednostki organizacyjnej i odbycie szkolenia w zakresie ochrony informacji niejawnych. Uzyskanie zaświadczenia nie wymaga przeprowadzenia postępowania sprawdzającego.

Przepisy prawa nadały wiodącą rolę organom nadzorującym system ochrony informacji niejawnych w Polsce. Należą do nich przede wszystkim Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, a także powołane w ostatnim czasie w ramach struktury MSWiA Biuro Nadzoru Wewnętrznego.

Na mocy ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i zarządzenia nr 73 Prezesa Rady Ministrów w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego służba ta realizuje swoje zadania w zakresie obronności państwa, pełni zadania służby ochrony państwa, sprawuje funkcję krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych,

wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej lub innych organizacji międzynarodowych. Szef Agencji Bezpieczeństwa Wewnętrznego organizuje współdziałanie z Szefem Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa. W zakresie niezbędnym do wykonywania funkcji krajowej władzy bezpieczeństwa Szef Agencji Bezpieczeństwa Wewnętrznego lub upoważnieni przez niego funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego oraz Szef Służby Kontrwywiadu Wojskowego lub upoważnieni przez niego żołnierze lub funkcjonariusze Służby Kontrwywiadu Wojskowego mają prawo do wglądu do dokumentów związanych z ochroną informacji niejawnych międzynarodowych, wstępu do obiektów i pomieszczeń przeznaczonych do przetwarzania informacji niejawnych międzynarodowych, dostępu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych, uzyskiwania wyjaśnień i informacji dotyczących ochrony informacji niejawnych międzynarodowych. Upoważnieni pisemnie funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego albo funkcjonariusze lub żołnierze Służby Kontrwywiadu Wojskowego w zakresie koniecznym do kontroli stanu zabezpieczenia informacji niejawnych mają prawo do wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są przetwarzane, wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej, żądania udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania tych informacji, przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji, żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień, zasięgania w związku z przeprowadzaną kontrolą informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek, powoływania oraz korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych, uczestniczenia w posiedzeniach

kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących ochrony tych informacji w kontrolowanej jednostce organizacyjnej.

Podstawowe zadania Służby Kontrwywiadu Wojskowego zostały określone w art. 5 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego. Należy do nich m.in. ochrona informacji niejawnych. Zakres zadań Służby Kontrwywiadu Wojskowego w zakresie ochrony informacji niejawnych został określony w art. 10 ust. 2 ustawy o ochronie informacji niejawnych. Służba Kontrwywiadu Wojskowego realizuje zadania wyłącznie w odniesieniu do Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych, ataszatów obrony w placówkach zagranicznych, żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych.

Na mocy Ustawy z dnia 9 listopada 2017 r. o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw w strukturach Ministerstwa Spraw Wewnętrznych i Administracji powstało Biuro Nadzoru Wewnętrznego (BNW). Inspektor Nadzoru Wewnętrznego jako organ sprawujący nadzór egzekwuje w służbach podległych MSWiA działania zgodne z przepisami prawa oraz zasadami etyki zawodowej, w związku z koniecznością zapewnienia przestrzegania → p r a w c z ł o w i e k a [t. 3], wykonuje zadania z zakresu bezpieczeństwa państwa oraz ujawnia nieprawidłowości w tym zakresie. Do uprawnień Inspektora Nadzoru Wewnętrznego należy m.in. dostęp do materiałów z prowadzonych czynności operacyjno-rozpoznawczych → P o l i c j i [t. 3], Straży Granicznej oraz dostęp do materiałów postępowań sprawdzających i kontrolnych postępowań sprawdzających prowadzonych (na podstawie Ustawy z dnia 5 sierpnia 2010 r. ochronie informacji niejawnych) przez Policję, Straż Graniczną, → S ł u ż b ę O c h r o n y P a ń s t w a [t. 4] oraz → P a ń s t w o w ą S t r a ż P o ż a r n ą [t. 3] wobec własnych funkcjonariuszy, strażaków i pracowników oraz dostęp do tych materiałów dokumentów.

Krzysztof Dymura

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2013; S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2010; M. Jaśkowska, *Materialne i formalne przesłanki tajemnic publicznoprawnych*, [w:] *Jawność i jej ograniczenia*, t. IV, *Znaczenie orzecznictwa*, M. Jaśkowska (red.), C.H.Beck, Warszawa 2014; *Jawność i jej ograniczenia. Struktura tajemnic*, wyd. 2, t. 6, G. Szpor, A. Gryszczyńska (red.), C.H.Beck, Warszawa 2016; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78, poz. 483; J. Oleński, *Elementy ekonomiki informacji*, Wydawnictwo UW, Warszawa 2000; Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. 2011, nr 288, poz. 1692 z późn. zm.); *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2014; K. Tarnacka, *Prawo do informacji w Polsce*, „Państwo i Prawo" 2003, nr 5; Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2002, nr 74, poz. 676 z późn. zm.); Ustawa z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz. U. 2015, poz. 21); Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. 2010, nr 182, poz. 1228 z późn. zm.; Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz. U. 1997, nr 89, poz. 555 z późn. zm.; Ustawa z dnia 9 listopada 2017 r. o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw, Dz. U. 2018, poz. 106, Zarządzenie nr 73 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego, M.P. 2002 nr 26, poz. 432 z późn. zm.

INFORMACYJNA REWOLUCJA W SPRAWACH WOJSKOWYCH (ang. *information revolution in military affairs*; informacyjna RMA) – termin opisujący zasadnicze zmiany w sposobie prowadzenia wojny i organizacji armii, jakie pojawiły się na przełomie lat 80. i 90. XX w. w siłach zbrojnych USA pod wpływem rewolucji informacyjnej, broni konwencjonalnej o wysokiej technologii oraz poglądach na temat → w o j n y [t. 4] i jej postrzegania w społeczeństwie amerykańskim.

Informacyjna RMA jest częścią debaty nad rewolucyjnymi zmianami w sposobie prowadzenia wojny obok innych rodzajów RMA wymienianych

przez historyków, politologów i wojskowych (rewolucji piechoty w XIV i XV w., rewolucji w fortyfikacjach, wczesnonowoczesnej europejskiej rewolucji militarnej, rewolucji →artylerii [t. 1] w marynarce w XVI w., rewolucji napoleońskiej na przełomie XVIII i XIX w., rewolucji w wojnie lądowej, rewolucji w mechanizacji, lotnictwie i →informacji czy rewolucji nuklearnej). Badania nad →rewolucją w sprawach wojskowych [t. 3] rozpoczęły się w latach 50. XX w. W styczniu 1955 r. na Uniwersytecie Królowej w Belfaście brytyjski historyk M. Roberts wygłosił wykład poświęcony rewolucji militarnej w latach 1560–1660. W kolejnych latach badania nad RMA były kontynuowane, największe zainteresowanie jej założeniami przypadło na okres lat 80. i 90. XX w., tzn. na radziecką rewolucję naukowo-techniczną oraz amerykańską informacyjną rewolucję w sprawach wojskowych.

Termin „rewolucja w sprawach wojskowych" jest ogólnym pojęciem opisującym fundamentalną zmianę charakteru i sposobów prowadzenia konfliktu zbrojnego. Większość rewolucji opierała się na rozwoju nowych technologii, jednak nie ograniczały się one do tego czynnika. Zazwyczaj rewolucje zawierały 3 elementy: zmianę technologiczną, innowacje w zakresie sposobu prowadzenia operacji wojskowych (zmianę doktrynalną) oraz przekształcenia struktury organizacyjnej sił zbrojnych (zmianę organizacyjną).

Kluczowym elementem ostatniej rewolucji jest zastosowanie technologii informacyjnej w technice wojskowej, stąd możemy mówić o informacyjnej rewolucji w sprawach wojskowych. Należy przy tym zaznaczyć, że od lat 90. XX w. ogólny termin RMA jest powszechnie kojarzony właśnie z rewolucją informacyjną. W 1993 r. A. Marshall, dyrektor Net Assessment w Pentagonie, zastąpił wcześniej używany termin *military-technical revolution* właśnie określeniem *revolution in military affairs*, by podkreślić całościowy charakter zmian – nieograniczający się tylko do sfery techniki, ale obejmujący również doktrynę i organizację.

Genezy informacyjnej RMA należy doszukiwać się w szeregu technologicznych innowacji zastosowanych przez USA oraz, w ślad za nimi, przez inne armie →NATO [t. 3] w latach 80. XX w. Wprowadzono je z myślą o znalezieniu drogi do przezwyciężenia dominacji, przede wszystkim ilościowej, armii Układu Warszawskiego. Wcześniej jedyną dostępną

metodą miało być użycie taktycznej →broni nuklearnej [t. 1], co jednak nieuchronnie zamieniłoby Europę w nuklearną pustynię. Nie zamierzano dorównywać armiom Układu Warszawskiego pod względem liczebnym, zamiast tego postanowiono skorzystać z najnowszych rozwiązań technologicznych. Dwa z nich były kluczowe – miniaturyzacja sprzętu komputerowego (postępująca od czasów skonstruowania pierwszego elektronicznego układu scalonego w 1958 r.) oraz rozwój zdecentralizowanych systemów przekazu informacji opartych na sprzęcie komputerowym (jego początkiem było powstanie w 1969 r. „przodka" internetu – sieci ARPANet). Założenia RMA polegają więc nie tylko na implementacji układów elektronicznych do systemów uzbrojenia w celu zwiększenia ich możliwości (np. komputerowe systemy kierowania ogniem zwiększają celność ognia prowadzonego przez czołgi), ale przede wszystkim na połączeniu poszczególnych elementów ugrupowania bojowego, aż do poziomu pojedynczego →żołnierza [t. 4], siecią wymiany informacji (tzw. system systemów). Po raz pierwszy na większą skalę koncepcja ta została wykorzystana w rozwijanym w latach 80. projekcie Follow-On Forces Attack (FOFA, zwalczanie drugiego rzutu wojsk nieprzyjaciela), na potrzeby którego rozwinięto szereg nowych typów uzbrojenia. Generalnie typy te można podzielić na 2 grupy: systemy rozpoznawcze (np. przenoszony przez samoloty radar JSTARS, Joint Surveillance Target Attack Radar System) oraz systemy uderzeniowe (np. wyrzutnia pocisków rakietowych MGM-140 ATACMS, Army Tactical Missile System). Systemy te, połączone wysokowydajnymi sieciami przesyłu informacji, miały stanowić nowatorski system rozpoznawczo-uderzeniowy. Stworzyły również podwaliny pod dalszą, zakrojoną na znacznie szerszą skalę transformację, którą w uproszczeniu można opisać jako przekształcenie całych sił zbrojnych w jeden wielki system rozpoznawczo-uderzeniowy dzięki synergii pomiędzy trzema sferami: pozyskiwania informacji, przetwarzania i przesyłania informacji oraz wykorzystywania informacji w celu potęgowania siły ognia.

M. O'Hanlon wskazywał na następujące zasadnicze kierunki transformacji sił zbrojnych w duchu RMA:

- rozwój technologii informatycznych i komunikacyjnych (C2, Computers and Communications);
- rozwój wszelkiego rodzaju sensorów;

- rozwój lżejszych, trudniej wykrywalnych platform bojowych dla wszystkich środowisk walki;
- rozwój całkowicie nowych rodzajów broni, jak broń o ukierunkowanej energii oraz broń kosmiczna.

Jak podkreślił Ł. Kamieński w książce *Technologia i wojna przyszłości*, informacyjną RMA tworzą 3 podstawowe elementy: rewolucja informacyjna, broń konwencjonalna typu *high tech* oraz poglądy na temat wojny i jej postrzeganie w społeczeństwie amerykańskim. Rewolucja informacyjna rozumiana jako połączenie komputerów i telekomunikacji doprowadziła do pojawienia się nowych narzędzi wojny, zmian w prowadzeniu wojny (taktyka, operacje, organizacja sił zbrojnych) oraz zmian w charakterze wojny (→ s t r a t e g i a [t. 4], cele, skala wojny). Systemy radarowe zlokalizowane na okrętach podwodnych Aegis, systemy satelitarne, zintegrowane platformy zbierające dane, takie jak AWACS i JSTAR, umożliwiały zdobywanie aktualnych i właściwych informacji, dając tym samym przewagę nad przeciwnikiem. Obok nich w siłach zbrojnych USA pojawiły się → s t e a l t h t e c h n i k i [t. 4] pozwalające uczynić część sił powietrznych niewidzialnymi dla radarów przeciwnika. Przykładem był m.in. samolot F-117A oraz B-2. Rosnąca świadomość sytuacyjna oddziałów na różnym szczeblu hierarchicznym dzięki wykorzystaniu technologii informacyjnych doprowadziła do działania czynników nieznanych wcześniej dużym organizacjom, jakimi są armie narodowe: obchodzenia hierarchii i konkurencji. Nawet niewielkie oddziały wojskowe uzyskały dostęp do niekontrolowanej wiedzy i informacji niemożliwej do kontrolowania i monopolizowania. Amerykański pluton piechoty morskiej mógł mieć z związku z tym wiedzę na temat lokalizacji, położenia oraz kierunków ruchu przeciwnika i wykorzystać ją, nie czekając na informacje od dowództwa brygady, których nie może zweryfikować. Świadomość ta dała również przewagę mniejszym oddziałom operujących na podstawie większej autonomii i niezależności od dużych zhierarchizowanych oddziałów o ograniczonej mobilności.

Dominującym elementem przemian stała się więc szeroko pojęta sieciocentryczność, a najważniejszym czynnikiem przesądzającym o sukcesie miały być już nie tradycyjne przymioty, taki jak siła ognia, odporność na uderzenia czy zdolność do manewru, ale tzw. świadomość sytuacyjna

(ang. *battlespace awareness*). W uproszczeniu jest to nieustannie aktualizowana „wiedza o tym, gdzie jestem, gdzie są moi towarzysze, gdzie jest nieprzyjaciel". Na kluczowy element starcia wyrosła informacja, a dążenie do uzyskania przewagi informacyjnej stało się motywem przewodnim transformacji amerykańskich sił zbrojnych. Rdzeniem rewolucji nie były więc nowe typy uzbrojenia (choć i one się pojawiły – zwłaszcza pod postacią uzbrojenia precyzyjnego), lecz spięcie wszystkich elementów ugrupowania bojowego siecią dystrybucji informacji. Najważniejszym elementem sił zbrojnych stał się więc system C4IRS (Command, Control, Communications, Computing, Intelligence, Surveillance, Reconnaissance – dowodzenie, kontrola, komunikacja, informatyzacja, → w y w i a d [t. 4], obserwacja, rozpoznanie), który koordynuje proces bodziec – reakcja (od sensora do efektora) w czasie niemal rzeczywistym. Ten schemat działania spowodować miał odejście w przeszłość podstawowej dotychczas bolączki walczących, czyli braku informacji (który C. von Clausewitz określał „mgłą wojenną"). Wyzwaniem stał się za to nadmiar informacji, niepozwalający na ich właściwą interpretację.

Efektem rewolucji informacyjnej w sferze wojskowości były także narodziny idei → w o j n y i n f o r m a c y j n e j [t. 4], netwojny i → c y b e r w o j n y [t. 1]. Wojna informacyjna została określona jako działania podjęte w celu osiągnięcia dominacji informacyjnej poprzez wpływ na informację adwersarza, jego procesy oparte na informacji, systemy informacyjne i sieci komputerowe, a jednocześnie uniemożliwienie tego samego przeciwnikowi. Netwojna odnosiła się do poziomu społeczeństw oraz państw. Opisywała świadomość grupową na temat wojny, jak również sposoby manipulowania nią. Cyberwojna z kolei oznaczała sposób prowadzenia wojny, tzn. zniszczenie lub przerwanie funkcjonowania systemów informacji i komunikacji przeciwnika.

Teoretycy RMA przywołują metaforę internetu, ukazując cechy charakterystyczne dla tego medium, będące jednocześnie również elementami leżącymi u podstaw zmian społecznych zmierzających w kierunku budowy społeczeństwa informatycznego, jak i sił zbrojnych opartych na zdobyczach RMA. Są to: brak centralnej kontroli nad systemem („kreatywna anarchia"), łatwy dostęp do informacji z niemalże każdego miejsca na świecie oraz łączność wszystkich ze wszystkimi (ang. *interconnectivity*).

Tak pojmowany system tworzy środowisko, w którym kluczowym zasobem jest informacja, zdolna do szybkiej transmisji i efektywnego zastosowania.

Drugim charakterystycznym elementem informacyjnej RMA jest broń konwencjonalna o wysokiej technologii, a szczególnie jej 3 rodzaje, tj. bezzałogowe statki latające, broń precyzyjna i broń laserowa. Broń precyzyjna jest jednym z symbolów informacyjnej RMA. Pojawiła się na większą skalę w czasie I wojny w Zatoce Perskiej (1991), jednak dopiero w II wojnie w Zatoce Perskiej (2003) stanowiła większość (68%) ogółu użytej amunicji przez wojska amerykańskie. Pociski precyzyjne pojawiły się nie tylko w siłach powietrznych i → m a r y n a r c e w o j e n n e j [t. 3], ale także w korpusie piechoty morskiej i → w o j s k a c h l ą d o w y c h [t. 4]. Użycie ich było możliwe za pomocą wyrzutni rakietowych, artylerii, moździerzy, samolotów i → o k r ę t ó w w o j e n n y c h [t. 3]. Przykładem były m.in.: rakiety Hellfire, HARM, GBU-24, JDAM, JASSM.

Dzięki broni precyzyjnej możliwe stało się trafianie w cel z niespotykaną wcześniej dokładnością. Takie możliwości niosą za sobą wiele implikacji. Jedną z nich jest fakt, iż postęp technologiczny doprowadził do zmniejszenia „nakładów materiałowych" – do porażenia celu wystarczy znacznie mniejsza niż dawniej ilość środków bojowych. Jest to odpowiednik trendu obserwowanego w gospodarce cywilnej, gdzie informacja jest substytutem zasobów materiałowych i transportowych, dzięki niej bowiem można radykalnie zoptymalizować ich wykorzystanie. Broń precyzyjna umożliwiła także rozwiązanie tradycyjnego dylematu konstruktorów broni między zasięgiem a celnością. Dotychczas bowiem wraz ze wzrostem zasięgu zazwyczaj w sposób znaczny spadała celność systemów uzbrojenia. Broń precyzyjna pozwoliła na praktyczne wdrożenie koncepcji *stand-off* („pozostań w oddali"). Zamiast ryzykować bezpośrednie starcie, stosowane są środki rażenia odpalane z dużej odległości, co czyni nosiciela względnie niewrażliwym na przeciwdziałanie przeciwnika. Rezultatem jest generalne zwiększenie dystansu walki. Wojna staje się więc, przynajmniej w założeniach, przedsięwzięciem na podobieństwo gry komputerowej, gdzie bezpośredni kontakt z przeciwnikiem jest raczej wyjątkiem niż regułą.

Bezzałogowe statki powietrzne pojawiły się znacznie wcześniej niż idea informacyjnej rewolucji w sprawach wojskowych, tj. w czasie

wojny w Wietnamie, a pierwsze prototypy sterowanych radiowo pocisków nawet w czasie II wojny światowej. Podobnie jak broń precyzyjna, dopiero w latach 90. XX w. odegrały poważną rolę w operacjach militarnych prowadzonych przez USA. W 1991 r. chrzest bojowy przeszedł zaprojektowany przez Izrael samolot szpiegowski Pioneer. W 1994 r. loty rozpoczął jeden z najbardziej znanych i rozpoznawalnych na świecie dronów Predator. W kolejnych latach pojawiły się bezzałogowce, takie jak Global Hawk, Reaper, Shadow i inne. Obok misji obserwacyjnych, wykorzystywane były również do eliminacji celów za pomocą amunicji precyzyjnej oraz zapewniania →bezpieczeństwa wewnętrznego państwa [t. 1] (kontroli granicy państwowej, monitorowania obszarów, gdzie wystąpiły pożary lasów, powodzie, prowadzenia akcji humanitarnych, dostarczania leków itp.). W związku z prowadzeniem wojny z →terroryzmem [t. 4] w latach 2001–2011 Pentagon przeznaczył na rozwój bezzałogowych statków latających 6-krotnie większe fundusze niż latach 1991–2001. Do 2025 r. zaplanowano z kolei, że będą one wykonywać 35% wszystkich misji powietrznych realizowanych przez siły zbrojne USA. Badania nad bronią laserową prowadzone były zarówno w USA, jak również w ZSRR w czasie →zimnej wojny [t. 4]. Po jej zakończeniu, pomimo redukcji budżetów obronnych, Pentagon zdecydował się na kontynuowanie rozwoju tego rodzaju uzbrojenia. Charakter broni laserowej, technologia oraz skutki jej użycia czytelnie wpisywały się w idee informacyjnej rewolucji w sprawach wojskowych. Po pierwsze jest to broń wielokrotnego użytku, znacznie tańsza od pocisków precyzyjnych. Po drugie może ona być wykorzystana jako →broń nieśmiercionośna [t. 1], czego przykładem jest SMU-100 Laser Dazzler służący do obrony statków handlowych przed atakiem piratów, czy Green Laser Interdiction System, który może być wykorzystywany przez żołnierzy sił ONZ w czasie misji utrzymania pokoju.

Trzecim elementem informacyjnej RMA są poglądy na temat wojny i jej postrzeganie w społeczeństwie amerykańskim. Społeczeństwo amerykańskie pod wpływem bolesnych doświadczeń wojny w Wietnamie oraz świadomości możliwych skutków zastosowania broni atomowej w czasie zimnej wojny opisanych w doktrynie wzajemnego gwarantowanego zniszczenia niechętnie akceptowało prowadzenie wojny oraz ofiary wśród żołnierzy. „Syndrom wietnamski" doprowadził do powstania doktryny

Weinbergera i doktryny Powella w ramach amerykańskiej polityki zagranicznej, mówiących o kluczowym znaczeniu → o p i n i i p u b l i c z n e j [t. 3] w decydowaniu o zaangażowaniu wojskowym USA. Sukces I wojny w Zatoce Perskiej oraz interwencji NATO w Kosowie w 1999 r. wynikał m.in. z niewielkiej liczby ofiar w szeregach oddziałów amerykańskich. W czasie I wojny w Zatoce Perskiej zginęło zaledwie 147 żołnierzy wobec symulacji wskazujących na groźbę 10 tys. ofiar, w 1999 r. natomiast ani jeden amerykański żołnierz nie poniósł śmierci.

Cechami charakterystycznymi informacyjnej RMA była komputeryzacja, usieciowienie, informatyzacja, miniaturyzacja, precyzyjność i prędkość. Od okresu fascynacji w latach 80. i 90. XX w. w środowiskach amerykańskich wojskowych i naukowców zainteresowanie nią zaczęło spadać. Wynikało to m.in. z rozczarowania przebiegiem operacji militarnej w Afganistanie, misji stabilizacyjnej w Iraku oraz trudności Izraela w starciu z oddziałami Hezbollahu w Libanie w 2006 r. Konflikty te osłabiły entuzjastyczne podejście do nowych technologii wojskowych i przeświadczenia o możliwości zwycięstwa w każdej wojnie za pomocą *high tech*. Uwidoczniły one nadmierny optymizm, dostrzegalny w generalnych założeniach informacyjnej RMA. Szczególnie wyraźny był on w twierdzeniach o możliwości osiągnięcia przez jedną ze stron konfliktu (w praktyce przez Siły Zbrojne USA) niekwestionowanej supremacji informacyjnej, a także w założeniu, wedle którego informacja miała stać się w dużej mierze alternatywą dla tradycyjnych elementów przewagi militarnej, w tym dla siły ognia oraz odporności na ciosy zadawane przez przeciwnika.

O'Hanlon, odnosząc się do swoich prognoz sprzed 20 lat, w eseju *A Retrospective on the So-called Revolution in Military Affairs, 2000–2020* stwierdził, że postęp w dziedzinie rozwoju uzbrojenia przebiegał generalnie zgodnie z wcześniejszymi przewidywaniami, ale równocześnie nie wprowadzono jednak żadnych przełomowych rozwiązań. Zwraca uwagę przede wszystkim szybki rozwój technologii komputerowych i komunikacyjnych, obecnie w dużej mierze napędzanych przez rynek cywilny. Tempo rozwoju nowych sensorów było jednak skromne, podobnie jak w przypadku nowych platform. Rozwinięto i upowszechniono takie technologie jak stealth czy napędy niezależne od powietrza (AIP – Air Independent Propulsion) dla okrętów podwodnych, ale jest to tylko dalszy

rozwój rozwiązań opracowanych i wdrożonych już w XX w. Całkowicie nowe rodzaje broni, chociaż będące przedmiotem obiecujących prac badawczo-rozwojowych, pozostają jak na razie głównie w laboratoriach, a ich operacyjne użycie w większym wymiarze nadal jest kwestią przyszłości. Zwracają przy tym uwagę 2 zjawiska. Po pierwsze, zaawansowana technologicznie broń precyzyjna nadal pozostaje silną stroną USA, tak jak było to przed 20 laty, ale inne kraje, w tym Rosja i Chiny, poczyniły na tym polu znaczące postępy. Po drugie, RMA nie przyniosła zdecydowanego przełomu w prowadzeniu operacji przeciwrebelianckich i → a n t y t e r r o r y s t y c z n y c h [t. 1], które pozostają niezmiernie trudne nawet dla najbardziej zaawansowanych armii na świecie. Wykrywanie i identyfikacja nieprzyjacielskich bojowników wtopionych w → l u d n o ś ć c y w i l n ą [t. 3] nadal jest dużym wyzwaniem, a nowoczesna technologia z trudem znajduje rozwiązania niwelujące → z a g r o ż e n i e [t. 4] wynikające z szerokiej dostępności prostej, ale groźnej broni typowej dla działań nieregularnych (jak → b r o ń s t r z e l e c k a [t. 1] czy improwizowane ładunki wybuchowe – ang. *improvised explosive devices*, IED).

Równocześnie zdominowana przez technologie z obszaru matematyki i fizyki informacyjna RMA zaczęła ustępować biotechnologicznej RMA skupionej na badaniach z zakresu nanotechnologii, medycyny, genetyki i ulepszania człowieka.

Rafał Kopeć, Tomasz Wójtowicz

Ł. Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009; R. Kopeć, *Information-Based Revolution in Military Affairs*, [w:] *Encyclopedia of Information Science and Technology*, M. Khosrow-Pour (ed.), IGI Global, Engineering Science Reference, Hershey 2018; tenże, *Informacyjna rewolucja w sprawach wojskowych*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *Rewolucja w sprawach wojskowych w kontekście zachodniego sposobu prowadzenia wojen*, „Kultura i Polityka" 2014, nr 16; M. O'Hanlon, *A Retrospective on the So-called Revolution in Military Affairs, 2000–2020*, Foreign Policy at Brookings, 2019; tenże, *Technological Change and the Future of Warfare*, Brooking Institution Press, Washington 2000; T. Wójtowicz, *Rewolucja w sprawach wojskowych (RMA). Porównanie koncepcji Alvina Tofflera, Andrew Krepinevicha*

i Jeremy'ego Blacka, [w:] *Od wojny sprawiedliwej do wojny robotów. Rozważania o stałości i zmienności fenomenu wojny*, A. Nyzio (red.), Wydawnictwo Kontekst, Kraków 2018.

INFOSFERA – ma charakter metaforyczny, nawiązuje do pojęć z dziedziny ekologii, takich jak biosfera, hydrosfera, stratosfera itd. Pojęciem tym określa się środowisko → i n f o r m a c j i (łac. *informatio* – informacja; gr. σφαῖρα, *sfaira* – środowisko) obejmujące wszelkie relacje i procesy, jakie zachodzą pomiędzy użytkownikami informacji a zbiorami informacji. Pojęcie to podlega nieustannej transformacji, od postrzegania jej w wymiarze ściśle technologicznym, wirtualnym (→ c y b e r p r z e s t r z e ń [t. 1]) do globalnego → ś r o d o w i s k a i n f o r m a c y j n e g o [t. 4], i chociaż powszechnie występuje w literaturze, używane jest przez autorów bardziej intuicyjnie, a interpretacja dokonywana jest najczęściej w kontekście badanej domeny. Często infosfera, → p r z e s t r z e ń i n f o r m a c y j n a [t. 3], środowisko informacyjne, cyberprzestrzeń, otoczenie informacyjne, czasoprzestrzeń informacyjna, krajobraz informacyjny, informacyjny świat, informacyjny horyzont traktowane są zamiennie, a nawet jako wyrażenia synonimiczne. Powoduje to błędną interpretację i złe zrozumienie problemów i działań podejmowanych w tym środowisku.

Infosfera wg włoskiego filozofa etyki informacji L. Floridiego (info-Sfera) to semantyczna przestrzeń całości dokumentów, agentów i operacji użytkowania informacji, gdzie dokumenty to wszelkie dane, informacje i wiedza realizowane w dowolnym semiotycznym formacie; agenci to każdy system zdolny do interakcji z dokumentem; operacje to każdy rodzaj działania, interakcji i transformacji, które mogą być wykonywane przez agenta i przedstawione w dokumencie. Oznacza to, że infosfera obejmuje wszelkie relacje i procesy, jakie zachodzą pomiędzy użytkownikami informacji a zbiorami informacji.

Termin infosfery wprowadził do polskiej literatury naukowej w 1978 r. J.L. Kulikowski. Wyróżnił w „infosferze człowieka" (antropoinfosferze) 2 warstwy: wewnętrzną i zewnętrzną. Pierwsza z nich stanowi sumę informacji, które są utrwalone w pamięci człowieka, takich jak życiowe doświadczenie człowieka, wiedza, wspomnienia o przeżytych zdarzeniach oraz informacje utrwalone w pamięci krótkotrwałej, odbierane zmysłami.

Druga warstwa obejmuje te informacje, które są dostępne człowiekowi potencjalnie, jeżeli podejmie wysiłek pozyskania ich zgodnie z jego możliwościami fizycznymi, psychicznymi i społecznymi uwarunkowaniami materialnymi. Antropoinfosfera ma charakter zmienny, uzależniony od warunków społecznych, jak również od dostępności informacji wchodzących w skład infosfery zewnętrznej. W ewolucji antropoinfosfery Kulikowski wyodrębnił fazy uzależnione od możliwości komunikacyjnych podmiotu, które w początkowym okresie rozwoju człowieka koncentrowały się na warstwie wewnętrznej, następnie w wyniku wzbogacenia procesów komunikacyjnych i rozwoju technologii informacyjnych coraz częściej eksploatowały zawartość infosfery zewnętrznej, aż po dominację infosfery zewnętrznej, która naruszyła równowagę pomiędzy infosferą wewnętrzną a zewnętrzną. Zachwianie tej równowagi spowodowane zostało nadprodukcją informacji i → przeciążeniem informacyjnym [t. 3] uniemożliwiającym człowiekowi przetwarzanie informacji w tempie dostosowanym do jego biologicznych możliwości, w sytuacji dostarczania mu ich coraz szybciej i w coraz większej ilości za pośrednictwem coraz doskonalszych technologii informacyjnych. Te dysproporcje zmuszają człowieka do wypracowania racjonalnej organizacji infosfery zewnętrznej. Badacz proponuje utworzenie buforu → bezpieczeństwa [t. 1] pomiędzy infosferą wewnętrzną a zewnętrzną, której zadaniem będzie m.in. rozwój infosfery w selektywnie wybranych kierunkach, racjonalna wybiórczość zbiorów, regulacja stopnia rozpowszechnienia informacji zgodnie z kryteriami jej wartości poznawczych lub użytkowych, stworzenie warunków organizacyjnych i technicznych dla swobodnego przepływu informacji i możliwości jej przenikania do infosfery wewnętrznej, rozwój informacji pochodnych, reorganizacja programów nauczania na rzecz modelu, w którym nabywa się umiejętność samodzielnego przyswajania wiedzy i utrzymywania kontaktu z infosferą zewnętrzną. Autor już ponad 40 lat temu założył, że do tego celu zostaną wykorzystane sieci teleinformatyczne, które będą przetwarzać owe strumienie informacji, w ramach automatyzacji → procesów informacyjnych [t. 3]. Współcześnie zadania buforu bezpieczeństwa spełniają wyspecjalizowane, inteligentne programy zarządzania informacją i wiedzą (SIW, PIM, PKM, menadżery bibliografii itp.) oraz działania podejmowane na rzecz kształcenia

kompetencji informacyjnych (ang. *information literacy*) i kształtowania →kultury informacyjnej społeczeństwa ze szczególnym naciskiem na rozwijanie jego postaw proinfoekologicznych. W tej perspektywie infosfera obejmuje dynamiczne procesy zmierzające do zachowania równowagi w infosystemie (jak w ekosystemie).

A. Lepa, twórca pedagogiki medialnej, w centrum środowiska informacyjnego umieszcza człowieka. Środowisko to jest zindywidualizowane, odbierane i przeżywane inaczej przez każdą inną osobę i składa się z 4 części tworzących mediosferę człowieka, tj. z ikonosfery (środowiska obrazu), logosfery (środowiska słowa), sonosfery (środowiska dźwięku) i galenosfery (środowiska ciszy). W każdym z tych podzbiorów człowiek wchodzi w interakcje z mediami, które wpływają na rozwój jego osobowości. Natomiast wg W. Babika antropoinfosfera to ogół informacji dostępnych człowiekowi poprzez jego świadomość, które potencjalnie może on zużytkować dla realizacji swych życiowych celów. Jest miejscem aktywnego odbiorcy w sferze informacji uwikłanego w różnego typu relacje z informacją. To także, jak sugeruje M. Kisilowska, wielowymiarowy, dynamiczny, otwarty zbiór treści (danych i informacji), ich nośników oraz użytkowników. Istotne jest dookreślenie tej przestrzeni, np. do środowiska pracy systemu informacyjnego, do środowiska informacyjnego generowanego przez określone medium (książka, dokument, blog, serwis społecznościowy), do zestawu źródeł wykorzystywanych przez daną osobę, do środowiska relacji z użytkownikiem informacji (opisywanych w systemach architektury informacji) itp. Według definicji Kisilowskiej:

> użytkownicy informacji są w tej przestrzeni elementem aktywnym. Korzystając z odpowiednich narzędzi i metod docierają do poszukiwanych informacji, bądź eksplorują nowe dla nich źródła. To ich świadomość dotycząca dostępności tychże, jak również ciekawość, chęć poznania, są warunkiem koniecznym dla określenia przestrzeni i korzystania z niej.

Przyjmując ten punkt widzenia, można uznać, że w środowisku informacyjnym funkcjonuje wiele przestrzeni informacyjnych związanych bądź z daną osobą, z medium, rodzajem relacji między elementami tej

przestrzeni, bądź ze stosowanymi w niej narzędziami technologicznymi itp. Tworzy je suma indywidualnych przestrzeni informacyjnych poszczególnych użytkowników lub grup użytkowników, których informacyjne światy to podzbiory ogólnoświatowego zbioru informacji. B. Kamińska-Czubała podobnie interpretuje infosferę jako sumę indywidualnych przestrzeni informacyjnych poszczególnych użytkowników informacji lub ich grup. Sytuując człowieka jako aktora informacyjnego świata w jego centrum, opisuje indywidualne światy informacyjne ograniczone różnymi horyzontami informacyjnymi, których wielkość i zasięg uzależnione są od podejmowanych przez podmiot działań informacyjnych, użytkowanych źródeł informacji, kompetencji informacyjnych uczestników danego świata, postawy wobec informacji sterowanej przez kulturę informacyjną, a także od sytuacji i praktyk informacyjnych. W opracowanym przez nią modelu pozyskiwania i użytkowania informacji w życiu codziennym odwołała się do pojęcia małych światów wprowadzonego do literatury przez E. Chapman i horyzontu informacyjnego zaproponowanego przez D. Sonnenwald, uwzględniając je w strukturze infosfery. Również Babik jest skłonny do utożsamiania terminu infosfery z przestrzenią informacyjną odnoszącą się do pojedynczych użytkowników lub środowiska lokalnego, uwzględniając funkcję wyznaczania granic, ale dostrzega też jego wymiar globalny. Wąskie lub szerokie podejście do fenomenu infosfery łączone jest z położeniem środka ciężkości w definiowaniu tego pojęcia na „intensywności" działań podejmowanych przez człowieka w infosferze lub na jego kontekście przestrzennym, geograficznym.

W szerokim znaczeniu infosfera rozumiana jako globalne środowisko informacyjne człowieka jest czymś więcej niż tylko przestrzenią wirtualną, cyfrowym przedłużeniem realnej rzeczywistości człowieka. Jest miejscem rzeczywistym, w którym wspólnie funkcjonują ludzie, informacje oraz systemy informacyjne. Relacje, jakie pomiędzy nimi zachodzą, odnoszą się do procesów informacyjnych zachodzących w świecie analogowym, offline, jak i online, których sposób realizacji wpływa na zachowania podmiotów uczestniczących w tych procesach. W zachowaniach tych coraz częściej dominuje element gry interesów i walki o informację, a jak konkluduje M. Hetmański, we współczesnym świecie informacji dominują reguły twórców i nadawców informacji, a nie jej użytkowników i adresatów

emitowanych treści. W infosferze dochodzi do konwergencji takich zjawisk jak internet, społeczeństwo i kultura, a wg Floridiego jest ona:

> kompletnym środowiskiem informacyjnym złożonym z informacyjnych bytów, o określonych własnościach, wzajemnych zależnościach i relacjach, oraz procesów, co równoważy ją z istotą samego Bytu, pozwalając rozpatrywać infosferę w kategoriach ontologii informacyjnej.

Podsumowując, infosfera to środowisko informacyjne, w którym żyją ludzie zespoleni z nim w wymiarze wirtualnym i realnym, w których oddziałują na informację, a informacja oddziałuje na nich, w którym uczestniczą oni w różnych działaniach związanych z realizacją procesu informacyjnego i w którym wchodzą w różne relacje z elementami infosfery. Można zatem za P. Sienkiewiczem uznać, że współczesna infosfera jest dynamicznie rozwijającym się systemem, w którym na równi eksponowane są zarówno jego aspekty technologiczne, informacyjne, jak i społeczne i kulturowe, w którym dochodzi do konwergencji systemów informacyjnych, telekomunikacyjnych i masowego komunikowania. Tworzą ją ludzie, zbiory i źródła informacyjne, kanały informacyjne, narzędzia pozwalające na obustronny przepływ informacji między nadawcą a odbiorcą. Infosfera zawiera więc elementy struktury systemu informacyjnego (nadawca ↔ informacja ↔ odbiorca), którego główną funkcją jest realizacja procesu informacyjnego rozumianego jako gromadzenie, selekcjonowanie, przechowywanie, przetwarzanie, opracowanie, generowanie, wyszukiwanie, przesyłanie i udostępnianie informacji. Podejście holistyczno-systemowe w interpretacji świata jako systemu globalnego skłania Sienkiewicza do analizy interakcji zachodzących pomiędzy jego podsystemami, takimi jak socjosfera, technosfera, biosfera, ekonosfera, infosfera lokalna i globalna. W modelowaniu globalnym podkreśla wagę analizy strategicznej, np. w dokonywaniu oceny szansy lub ryzyka pomyślnej realizacji → s t r a t e g i i [t. 4] trwałego → z r ó w n o w a ż o n e g o r o z w o j u [t. 4]. Aby zrealizować ten scenariusz, świat powinien być zgodnie z teorią M. Mazura (*Cybernetyka i charakter*) systemem autonomicznym, czyli posiadającym zdolność sterowania i przeciwdziałania

utracie zdolności sterowania. W systemie takim istotną funkcję spełnia homeostat, czyli organ do przeciwdziałania przepływom informacji i energii zmniejszający zdolność oddziaływania systemu na otoczenie dzięki dodatnim i ujemnym sprzężeniom zwrotnym.

Infosferę błędnie utożsamia się z cybernetyczną przestrzenią i traktuje się ją jako synonim cyberprzestrzeni (ang. *cyberspace*) nieposiadającej przestrzennych, politycznych i geograficznych granic. Jest ona, jak podsumowuje Sienkiewicz: wirtualną rzeczywistością generowaną przez komputer, sieć i internet; społeczną megasiecią – „siecią sieci", której uczestnicy indywidualni i grupowi (społeczności) eksploatują zasoby globalne dostarczane przez internet; jest ewoluującym dynamicznym systemem złożonym i takim go należy przede wszystkim postrzegać, bez względu na to, czy eksponowane będą jego techniczne, informacyjne czy społeczne aspekty. To przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania) zapewniające przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne. Cyberprzestrzeń jest obszarem zarówno kooperacji pozytywnej, jak i kooperacji negatywnej. Ta pierwsza oznacza wzrost możliwości wszechstronnego zaspokojenia potrzeb społecznych, natomiast niebezpieczna przestrzeń cybernetyczna jest źródłem → z a g r o ż e ń [t. 4] dla bezpieczeństwa, takich jak cyberprzestępstwa, cyberinwigilacja, → c y b e r t e r r o r y z m [t. 1] i → c y b e r w o j n a [t. 1].

Cyberprzestrzeń to tylko fragment infosfery, w której ludzkość od zarania cywilizacji doskonaliła różnorodne sieci komunikacyjne odzwierciedlające coraz bardziej złożone relacje społeczne i technologiczne. J. Unlod pełną realizację koncepcji cyberprzestrzeni dostrzega we wszechobecnym przetwarzaniu informacji dokonującym się wszędzie, tj. w połączeniu internetu z hipermedialną siecią WWW oraz innymi mediami, głównie TV, telefonią komórkową i z internetem rzeczy (tj. przedmiotów codziennego użytku wspomaganych techniką komputerową, podłączonych do sieci, które w nieprzerwany i niezawodny sposób potrafią monitorować różne aspekty życia człowieka).

Chociaż środowisko informacyjne powinno być dla podmiotu środowiskiem bezpieczeństwa, to jednak infosfery nie można utożsamiać

z pojęciem infosfery bezpieczeństwa. Infosfera bezpieczeństwa to autonomiczne i odmienne pojęcie, różniące się zasadniczo od infosfery. Jak uzasadnia S. Jarmoszko, nie stanowi ono naturalnego środowiska, w którym funkcjonuje człowiek, lecz jest miejscem, w którym informacje są wykorzystywane świadomie i celowo pozyskiwane, zdobywane i aplikowane do skutecznego zarządzania ryzykiem i tworzenia pozytywnych stanów bezpieczeństwa. Można uznać, że infosfera bezpieczeństwa to obszar, w którym obowiązują zasady →ekologii informacji, który chroniony jest przed informacją niespełniającą kryteriów jakości, w którym →dezinformacja i →manipulacja informacją [t. 3] jest demaskowana, a środki przeciwdziałania zakłócaniu informacji są skuteczne, w którym panuje informacyjny ład oparty na informacyjnej inkluzji wszystkich podmiotów. Przedmiotem zainteresowania badaczy problemów infosfery bezpieczeństwa jest zapewnianie bezpieczeństwa informacyjnego za pomocą informacji. Jej istnienie i działanie opiera się wg Jarmoszki na 3 mechanizmach: pozyskiwania informacji (rutynowe poznawanie rzeczywistości, detekcja zagrożeń, systemy wczesnego ostrzegania, monitoring zagrożeń, odbiór ostrzeżeń intencjonalnych, analiza big data, →audyt bezpieczeństwa [t. 1], konsulting, →wywiad [t. 4] i →kontrwywiad), obróbki i zastosowania informacji (interpretacja informacji, ukrywanie, kamuflaż, szyfrowanie, →steganografia [t. 4], utajnianie, uwierzytelnianie, depozyt informacji, →cyberbezpieczeństwo [t. 1]) oraz emisji informacji (wołanie o pomoc, przekaz i ekspresja ostrzeżeń, dezinformacja, telesterowanie bezpieczeństwem, telemonitoring ochronny). →Bezpieczeństwo informacyjne [t. 1] zapewniane innymi środkami niż informacja wykracza poza istotę infosfery bezpieczeństwa. Bezpieczeństwo to dotyczy zarówno biernej infosfery bezpieczeństwa, która odnosi się do odbioru (ze zrozumieniem) sygnałów zagrożeń i intencjonalnych ostrzeżeń o nich, jak i czynnej infosfery bezpieczeństwa, która dotyczy aktywnego poszukiwania, przetwarzania tych sygnałów oraz wspierania procesów służących ogólnemu bezpieczeństwu.

Hanna Batorowska

L. Floridi, *Infosfera*, [w:] *Internet & Net Economy*, Vito di Bari (a cura di), Il Sole 25-Ore Libri, 2002; tenże, *La quarta rivoluzione. Come l'infosfera sta trasformando*

il mondo, Cortina Raffaello, Milano 2017; tenże, *Philosophy of Computing and Information: 5 Questions*, Automatic Press, 2008; M. Hetmański, *Świat informacji*, Difin, Warszawa 2015; S. Jarmoszko, *Antroposfera bezpieczeństwa wobec zagrożeń współczesnego świata (antropologiczna próba systematyzacji)*, [w:] *Bezpieczeństwo współczesnego świata. Wyzwania i zagrożenia*, A. Kusztelak (red.), Wydawnictwo Wyższej Szkoły Handlu i Usług, Instytut Wydawniczy Maiuscula, Poznań 2011; tenże, *Bezpieczeństwo informacyjne a casus infosfery bezpieczeństwa*, [w:] *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, M. Kubiak, R. Białoskórski (red.), Pracownia Wydawnicza Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Warszawa–Siedlce 2016; B. Kamińska-Czubała, *Zachowania informacyjne w życiu codziennym. Informacyjny świat pokolenia Y*, Wydawnictwo SBP, Warszawa 2013; Z. Kierzkowski, *Infosfera komunikacji bezpośredniej*, [w:] *Wymiana informacji i interaktywne komunikowanie medialne*, Z. Kierzkowski, S. Kluska-Nawarecka, A. Sielicki (red.), Wydawnictwo Sorus, Poznań 2003; J.L. Kulikowski, *Człowiek i Infosfera*, „Problemy" 1978, nr 3 (384); A. Lepa, *Pedagogia infosfery człowieka*, „Łódzkie Studia Teologiczne" 2011, nr 20; K. Materska, *Informacja w organizacjach społeczeństwa wiedzy*, Wydawnictwo SBP, Warszawa 2007; P. Sienkiewicz, *Ewaluacja strategii rozwoju społeczeństwa informacyjnego*, [w:] P. Sienkiewicz, *25 wykładów*, AON, Warszawa 2013; tenże, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, no. 13, vol. 9; tenże, *Społeczeństwo informacyjne jako system cybernetyczny*, [w:] *Społeczeństwo informacyjne. Wizja czy rzeczywistość?*, t. 1, H. Haber (red.), Akademia Górniczo-Hutnicza im. S. Staszica w Krakowie, Kraków 2003; J. Unlod, *Zarządzanie informacją w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa 2015.

INFOSFERA A INFOSFERA BEZPIECZEŃSTWA – →infosfera jest często używanym przez przedstawicieli różnych dyscyplin naukowych pojęciem stosowanym zamiennie z takimi terminami jak →środowisko informacyjne [t. 4] człowieka, antropoinfosfera lub →przestrzeń informacyjna [t. 3], która obejmuje →cyberprzestrzeń [t. 1] będącą zaledwie fragmentem infosfery.

Infosfera określa środowisko →informacji, w którym zachodzą wszelkie relacje i procesy zachodzące między użytkownikami informacji a zbiorami informacji. Pojęcie to podlega nieustannej transformacji, od postrzegania jej w wymiarze ściśle technologicznym, wirtualnym (cyberprzestrzeń) do globalnego środowiska informacyjnego odnoszącego się do procesów zachodzących w świecie analogowym, offline, jak i online.

Sposób prowadzenia refleksji nad znaczeniem infosfery w zapewnieniu →bezpieczeństwa [t. 1] współczesnego świata związany jest z umieszczeniem w jej centralnym miejscu albo informacji, albo człowieka, będącego twórcą i użytkownikiem tych informacji. Według W. Babika antropoinfosfera to ogół informacji dostępnych człowiekowi poprzez jego świadomość, które potencjalnie może on zużytkować dla realizacji swych życiowych celów. Jest miejscem aktywnego odbiorcy w sferze informacji uwikłanego w różnego typu relacje z informacją. To także, jak sugeruje M. Kisilowska, wielowymiarowy, dynamiczny, otwarty zbiór treści (danych i informacji), ich nośników oraz użytkowników. Użytkownicy informacji są w tej przestrzeni elementem aktywnym. To ich świadomość dotycząca dostępności źródeł informacji oraz chęć zapoznania się z nimi i wykorzystania, a także posiadane kompetencje informacyjne oraz podejmowane przez nich działania informacyjne są warunkiem koniecznym dla określenia ich indywidualnej przestrzeni informacyjnej. W środowisku informacyjnym funkcjonuje wiele przestrzeni informacyjnych związanych bądź z daną osobą, z medium, rodzajem relacji między elementami tej przestrzeni, bądź ze stosowanymi w niej narzędziami technologicznymi itp. Tworzy je suma indywidualnych przestrzeni informacyjnych poszczególnych użytkowników lub grup użytkowników, których informacyjne światy to podzbiory ogólnoświatowego zbioru informacji.

Infosfera jako globalne środowisko informacyjne człowieka jest czymś więcej niż tylko przestrzenią wirtualną. Jest miejscem rzeczywistym, w którym wspólnie funkcjonują ludzie, informacje oraz systemy informacyjne, miejscem, w którym równie duże znaczenie przypisuje się jego cechom technologicznym, informacyjnym, społecznym i kulturowym, w którym dochodzi do konwergencji systemów informacyjnych, telekomunikacyjnych i masowego komunikowania. Relacje, jakie pomiędzy nimi zachodzą, wpływają na zachowania podmiotów uczestniczących w tych procesach. W zachowaniach tych coraz częściej dominuje element gry interesów i walki o informację, a jak konkluduje M. Hetmański, we współczesnym świecie informacji dominują reguły twórców i nadawców informacji, a nie jej użytkowników i adresatów emitowanych treści. Środowisko informacyjne – w którym →procesy informacyjne [t. 3], przypisane im fazy i czynności mogą być analizowane jako działania pozwalające

zdobyć przewagę nad partnerem, konkurentem, podmiotem zaatakowanym, pozyskać jego aktywa, zdominować, odizolować od ośrodków decyzyjnych, doprowadzić do destrukcji, zniszczyć – jest środowiskiem permanentnej walki o informacje. Dlatego tak ważne są działania na rzecz zachowania równowagi w infosystemie polegające na „pełnej akceptacji hybrydowego środowiska informacyjnego, w którym nie dopuszcza się do dominacji ani środowiska naturalnego, ani sztucznego środowiska elektronicznego". Środowisko to powinno być tak zorganizowane, aby było wiadomo, kto jest nadawcą, a kto odbiorcą informacji, jaki ma ona status, jakie nadawca ma intencje, jaki jest cel informowania. Niestety, jak to określa Babik, coraz częściej dochodzi w tym środowisku do zlewania się informacji z → d e z i n f o r m a c j ą, nadmiernego zawierzania technologiom informacyjnym, podświadomego niedoceniania własnej interpretacji i oceny danych oraz niemożności oderwania się od ciągłej stymulacji napływających ze wszystkich stron bodźców informacyjnych prowadzącej do „zainformowania się człowieka na śmierć". Oznacza to, że środowisko informacyjne, postrzegane np. w kontekście ekologii środowiska przyrodniczego, może być światem interpretowanym w kontekście → z a g r o ż e ń [t. 4], patologii i → k r y z y s ó w cywilizacyjnych, w którym analiza procesu informacyjnego może być postrzegana także w kategoriach walki o informacje.

Infosferę błędnie utożsamia się z cybernetyczną przestrzenią i traktuje ją jako synonim cyberprzestrzeni (ang. *cyberspace*) nieposiadającej przestrzennych, politycznych i geograficznych granic. Cyberprzestrzeń jest wg Piotra Sienkiewicza wirtualną rzeczywistością generowaną przez komputer, sieć i internet; społeczną megasiecią – „siecią sieci", której uczestnicy indywidualni i grupowi (społeczności) eksploatują zasoby globalne dostarczane przez internet; jest ewoluującym dynamicznym systemem złożonym i takim go należy przede wszystkim postrzegać, bez względu na to, czy eksponowane będą jego techniczne, informacyjne czy społeczne aspekty. To przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania) zapewniające przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne. Stanowi konwergencję technologii informatycznych,

telekomunikacyjnych i mediów, charakteryzujących się cechami takimi jak sieciowość, wirtualność, interaktywność, multimedialność, hipertekstowość. Cyberprzestrzeń jest obszarem zarówno kooperacji pozytywnej, jak i kooperacji negatywnej. Ta pierwsza oznacza wzrost możliwości wszechstronnego zaspokojenia potrzeb społecznych, natomiast niebezpieczna przestrzeń cybernetyczna jest źródłem zagrożeń dla bezpieczeństw, takich jak cyberprzestępstwa, cyberinwigilacja, →cyberterroryzm [t. 1] i →cyberwojna [t. 1].

Cyberprzestrzeń to tylko fragment infosfery, w której ludzkość od zarania cywilizacji doskonaliła różnorodne sieci komunikacyjne odzwierciedlające coraz bardziej złożone relacje społeczne i technologiczne. J. Unlod pełną realizację koncepcji cyberprzestrzeni postrzega we wszechobecnym przetwarzaniu informacji dokonującym się wszędzie, tj. w połączeniu internetu z hipermedialną siecią WWW oraz innymi mediami, głównie TV, telefonią komórkową i z internetem rzeczy (tj. przedmiotów codziennego użytku wspomaganych techniką komputerową, podłączonych do sieci, które w nieprzerwany i niezawodny sposób potrafią monitorować różne aspekty życia człowieka).

Cyberprzestrzeń stała się obecnie nowym polem walki o wpływy i dominację pomiędzy narodami, państwami, korporacjami, co pociąga za sobą konieczność dokonania licznych zmian zarówno w pragmatyce, jak i w prawno-organizacyjnym wymiarze funkcjonowania systemów bezpieczeństwa w skali globalnej i lokalnej. W przestrzeni tej prowadzi się wiele form walki, których celem jest uzyskanie przewagi w dowodzeniu, wykorzystanie wiedzy rozpoznawczej, atakowanie systemów informacyjnych, blokowanie informacji w celu osiągnięcia przewagi ekonomicznej, stosowanie techniki radioelektronicznej i kryptograficznej, prowadzenie walki psychologicznej, prowadzenie →wojny [t. 4] w rzeczywistości wirtualnej.

Cyberprzestrzeń wg T.R. Aleksandrowicza jest przestrzenią operacyjną, w której prowadzone działania informacyjne skutkują realizacją celów usytuowanych zarówno w środowisku wirtualnym, jak i realnym. W przestrzeni tej prowadzona jest walka informacyjna o wpływ na sposób zachowania podmiotów będących celem ataku, o zakłócanie lub uniemożliwienie funkcjonowania zaatakowanego systemu informatycznego,

o fizyczne niszczenie infrastruktury informatycznej przeciwnika. Za pośrednictwem sieci teleinformatycznych wchodzących w skład cyberprzestrzeni można wpływać na →infrastrukturę krytyczną państwa. Oznacza to, że cyberprzestrzeń ma także wymiar militarny. Określa się ją piątym środowiskiem walki, poza lądem, morzem, przestrzenią powietrzną i kosmosem.

Ochrona cyberprzestrzeni staje się priorytetowym zadaniem rządów ze względu na powstałe →zagrożenia globalne [t. 4], do których M. Lakomy zalicza cyberterroryzm, działalność wywiadowczą, wykorzystanie cyberprzestrzeni do prowadzenia działań zbrojnych mających na celu uzyskanie przewagi informacyjnej. W ramach sieciowego paradygmatu bezpieczeństwa opisanego przez Aleksandrowicza państwa traktowane są jako węzły w sieci stosunków międzynarodowych, których obowiązkiem jest dostrzeganie szans i zagrożeń wynikających z funkcjonowania w cyberprzestrzeni i równocześnie reagowanie i przeciwdziałanie generowanym w tym środowisku zagrożeniom.

Chociaż środowisko informacyjne powinno być dla podmiotu środowiskiem bezpieczeństwa, infosfery nie można utożsamiać z pojęciem infosfery bezpieczeństwa. Jak uzasadnia S. Jarmoszko, nie stanowi ono naturalnego środowiska, w którym funkcjonuje człowiek, lecz jest miejscem, w którym informacje są wykorzystywane świadomie i celowo pozyskiwane, zdobywane i aplikowane do skutecznego zarządzania ryzykiem i tworzenia pozytywnych stanów bezpieczeństwa. Można założyć, że infosfera bezpieczeństwa powinna być obszarem, w którym obowiązują zasady →ekologii informacji, który chroniony jest przed informacją niespełniającą kryteriów jakości, w którym dezinformacja i →manipulacja informacją [t. 3] jest demaskowana, a środki przeciwdziałania zakłócaniu informacji są skuteczne, w którym panuje informacyjny ład oparty na informacyjnej inkluzji wszystkich podmiotów.

Jednak głównym przedmiotem zainteresowania badaczy problemów infosfery bezpieczeństwa jest zapewnianie →bezpieczeństwa informacyjnego [t. 1] za pomocą informacji. Jej istnienie i działanie opiera się wg Jarmoszki na 3 mechanizmach: pozyskiwania informacji (rutynowe poznawanie rzeczywistości, detekcja zagrożeń, systemy

wczesnego ostrzegania, monitoring zagrożeń, odbiór ostrzeżeń intencjonalnych, analiza big data, → a u d y t b e z p i e c z e ń s t w a [t. 1], konsulting, → w y w i a d [t. 4] i → k o n t r w y w i a d), obróbki i zastosowania informacji (interpretacja informacji, ukrywanie, kamuflaż, szyfrowanie, → s t e g a n o g r a f i a [t. 4], utajnianie, uwierzytelnianie, depozyt informacji, → c y b e r b e z p i e c z e ń s t w o [t. 1]) oraz emisji informacji (wołanie o pomoc, przekaz i ekspresja ostrzeżeń, dezinformacja, telesterowanie bezpieczeństwem, telemonitoring ochronny). Bezpieczeństwo informacyjne zapewniane innymi środkami niż informacja wykracza poza istotę infosfery bezpieczeństwa. Bezpieczeństwo to dotyczy zarówno biernej infosfery bezpieczeństwa, która odnosi się do odbioru (ze zrozumieniem) sygnałów zagrożeń i intencjonalnych ostrzeżeń o nich, jak i czynnej infosfery bezpieczeństwa, która dotyczy aktywnego poszukiwania, przetwarzania tych sygnałów oraz wspierania procesów służących ogólnemu bezpieczeństwu. Czynna infosfera bezpieczeństwa, jak konkluduje Jarmoszko, staje się coraz bardziej znaczącym elementem szeroko rozumianego systemu bezpieczeństwa, usytuowanym w → s t r a t e g i a c h [t. 4] bezpieczeństwa społeczności i w strategiach życiowych jej podmiotów.

Infosfera bezpieczeństwa uznawana jest za jedną z przedmiotowych kategorii antroposfery bezpieczeństwa odnoszącej się do informacyjnej płaszczyzny kreowania bezpieczeństwa. Przenika ona wszystkie składowe antroposfery bezpieczeństwa, definiowanej jako „całokształt ludzkich dyspozycji i dokonań w dziedzinie kreowania warunków zapewniających jednostce ludzkiej (oraz jej naturalnym zbiorowościom) bezpieczną i satysfakcjonującą egzystencję, rozwój i przetrwanie". Obejmuje zatem ogół wiedzy aktualnej i historycznej o biologii człowieka, jego społecznym działaniu oraz kulturowych wytworach w dziedzinie tworzenia bezpieczeństwa własnego oraz innych. Jak pisze Jarmoszko:

> antropologia bezpieczeństwa orientuje się na naturalne dyspozycje (właściwości) ochronne i obronne człowieka (indywidualne i zbiorowe), ale przede wszystkim na wykreowane przez niego technologie budowania bezpieczeństwa oraz całokształt ludzkich wytworów (artefaktów) wynikających z ich wdrażania.

Badacz wyróżnia 2 zasadnicze jej wymiary – diachroniczny (chronologiczny ciąg wydarzeń związanych z kreowaniem bezpieczeństwa) i synchroniczny (zależności i oddziaływania elementów systemu społeczno-kulturowego tworzących bezpieczeństwo w czasie teraźniejszym). Perspektywa synchroniczna reprezentowana jest przez antroposferę bezpieczeństwa, czyli technologię kształtowania bezpieczeństwa danego podmiotu we wszystkich przedmiotowych jego dziedzinach, np. bezpieczeństwa zdrowotnego, psychologicznego, ekologicznego, ekonomicznego, informacyjnego, międzynarodowego, społecznego, publicznego, narodowego itp. Podsumowując, antroposfera bezpieczeństwa jest ściśle związana z działalnością dotyczącą tworzenia, zapewnienia i utrzymania bezpieczeństwa danego podmiotu. Uzewnętrznia się w wytworach tej działalności i przygotowaniu podmiotu bezpieczeństwa do stałej gotowości na odpowiednie zareagowanie na powstałe zagrożenie, a w razie potrzeby na podjęcie odpowiednich działań zaradczych. Można zatem uznać za J. Piwowarskim, że produktem antroposfery bezpieczeństwa jest →kultura bezpieczeństwa rozumiana jako „konstrukt społeczny, możliwy do przeciwstawienia rozlicznym zagrożeniom, efekt wynikający z istnienia społecznych więzów, ze współzależności oraz interakcji zachodzących w danej zbiorowości ludzkiej, będącej jednym z podmiotów bezpieczeństwa".

Hanna Batorowska

T.R. Aleksandrowicz, *Świat w sieci. Państwa Społeczeństwa Ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Difin, Warszawa 2014; H. Batorowska, *Cyberprzestrzeń*; *Infosfera; Środowisko informacyjne* [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; W. Babik, *Środowisko informacyjne człowieka*, [w:] *Nauka o informacji*, W. Babik (red.). Wydawnictwo SBP, Warszawa 2016; M. Hetmański, *Świat informacji*, Difin, Warszawa 2015; S. Jarmoszko, *Bezpieczeństwo informacyjne a casus infosfery bezpieczeństwa*, [w:] *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, M. Kubiak, R. Białoskórski (red.), Wydawnictwo Naukowe UPH, Siedlce 2016; tenże, *Antroposfera bezpieczeństwa wobec zagrożeń współczesnego świata (antropologiczna próba systematyzacji)*, [w:] *Bezpieczeństwo współczesnego świata. Wyzwania i zagrożenia*, A. Kusztelak (red.), WSHiU, Poznań 2011; tenże, *Historyczne i merytoryczne „korzenie" antropologii*

bezpieczeństwa, [w:] S. Jarmoszko, C. Kalita, J. Maciejewski, *Nauki społeczne wobec problemu bezpieczeństwa (wybrane zagadnienia)*, Wydawnictwo Naukowe UPH, Siedlce 2016; M. Kisilowska, *Kultura informacji*, Wydawnictwo SBP, Warszawa 2016; M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations" 2010, nr 3–4 (t. 42); tenże, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015; A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON" 2013, nr 3 (92); J. Piwowarski, *Prolegomena do badań nad kulturą bezpieczeństwa*, „Scientific Journal for Students and PhD Candidates" 2013, nr 2; P. Sienkiewicz, *25 wykładów*, AON, Warszawa 2013; tenże, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka" 2009, t. 13, z. 2; tenże, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, no. 13, vol. 9; J. Unlod, *Zarządzanie informacją w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa 2015; J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

INFOTOKSYKACJA (zatrucie informacyjne) – termin zaadoptowany przez ekologów informacji (zob. → e k o l o g i a i n f o r m a c j i) do określenia działań związanych z zanieczyszczaniem → ś r o d o w i s k a i n f o r m a c y j n e g o [t. 4] człowieka → i n f o r m a c j a m i zniekształconymi, zmanipulowanymi, nadmiarowymi, patogennymi w celu wywarcia wpływu na zaatakowany podmiot i podporządkowania go woli dysponentów informacji. Informacjami toksycznymi mogą być informacje zniekształcone, fałszywe, → f a k e n e w s y, memy internetowe, → p a t o g e n y i n f o r m a c y j n e [t. 3] itp. Te ostatnie definiowane są jako informacje o „zainfekowanej" treści i/lub w nadmiernej ilości wprowadzone w obieg i wymierzone w ofiarę (jednostkę lub strukturę społeczną). Ich zadaniem jest zainicjowanie „choroby", której przejawem jest lęk i poczucie utraty kontroli i bezradności. Funkcjonują one w przestrzeni → p o s t p r a w d y [t. 3], w której kłamstwa wynikają ze wzajemnego wzmacniania się informacji prawdziwych, półprawd i kłamstw medialnych, w którym zanika umiejętność odróżniania komentarza od faktu, w którym prawda przestaje istnieć jako synonim obiektywności, ponieważ nastąpiło zobojętnienie na prawdę samą w sobie.

Jak pisze W. Babik, informacje patogenne muszą być usuwane lub neutralizowane przez człowieka, aby mógł on zachować stan równowagi

informacyjnej, tzw. homeostazy informacyjnej. Jeżeli zostanie ona naruszona, człowiek popada w chorobę. Uzewnętrznia się ona za pośrednictwem czynnika chorobotwórczego, którym może być np. słaba jakość informacji (informacja dotknięta patologią, czyli taka, która jest nieprawdziwa, niewiarygodna, niekompletna, nieaktualna). Reakcje obronne użytkownika informacji na ten stan uaktywniają się w zależności od indywidualnych cech podmiotu, jego potrzeb informacyjnych, kompetencji informacyjnych, →świadomości informacyjnej [t. 4], →kultury informacyjnej. Niestety w środowisku nadmiarowości informacji →choroby informacyjne [t. 1] stają się zjawiskiem powszechnym i często są bagatelizowane przez osoby nimi zainfekowane, chociaż świadczą o ich niedomaganiu zarówno w sferze fizycznej, jak i psychicznej.

Infotoksykacja →przestrzeni informacyjnej [t. 3] informacjami celowo zniekształconymi i zmodyfikowanymi (ale potencjalnie wiarygodnymi i logicznymi, tworzącymi w umyśle zainfekowanych podmiotów wrażenie wiarygodności) w celu wywołania określonego zachowania jednostki lub grupy jest przedmiotem zainteresowania głównie badaczy współczesnych problemów walki informacyjnej. Ich punkt widzenia na patologię środowiska informacyjnego wskazuje na wagę działań psychologicznych wspierających operacje militarne i ukazuje skalę →zagrożenia [t. 4] podmiotów, których kulturowe DNA zostanie uszkodzone. Gdy informacje zmanipulowane umieszczone w warstwie społeczno-kulturowej danej grupy łączą się z jej kulturowym DNA, dochodzi do zainfekowania społeczeństwa, ponieważ zostaje uszkodzony kulturowy gen zbiorowy zawierający wskazówki odnośnie do tworzenia się organizacji społecznych oraz funkcjonowania danej zbiorowości, przekazywane z pokolenia na pokolenie członkom grupy. Informacja kulturowa zapisana w postaci kodu zrozumiałego tylko przez członków danego społeczeństwa może pod wpływem różnych czynników – np. politycznych, militarnych, informacyjnych, socjalnych czy ekologicznych – ulec modyfikacji i doprowadzić do destabilizacji całej komórki społecznej. Zatruty zostaje cały system społecznej informacji, głównie w wyniku działań propagandowych i stosowania technik działań propagandowych. →Propaganda [t. 3] stanowi główne narzędzie

generowania patologii w środowisku informacyjnym. Nie odnosząc się do źródeł informacji, zmieniając fakty i metody komentowania dla potwierdzenia własnej pozycji, wykorzystując oszustwa, przekształcając przekonania, wykorzystując fikcję i kłamstwo, ukrywając cele, staje się maszyną do fabrykowania informacji patogennych. W propagandzie, jak pisze O. Wasiuta, „odrzuca się krytykę, zniekształca fakty, odwraca uwagę od głównego tematu, wpaja poczucie strachu i chaosu", czyli tworzy zatrute środowisko informacyjne, w którym niszczy się tradycyjne mechanizmy samoidentyfikacji i zastępuje je nowymi, niszczy podmiotowość całych grup etnicznych i narzuca obce modele życia społecznego, nową hierarchię wartości.

Zatrucie →infosfery stanowi poważne zagrożenie dla społecznego →bezpieczeństwa informacyjnego [t. 1], które powinno być budowane na społecznym ładzie informacyjnym. Infotoksykacja środowiska społecznego ładu informacyjnego skutkuje utratą poczucia społecznego bezpieczeństwa informacyjnego, ponieważ znika pewność egzekwowania przez podmiot swoich praw obywatelskich i gwarancja, że zasoby informacyjne zostaną wykorzystane zgodnie z intencją ich nadawców lub dysponentów.

Według R. Żuchowskiego infotoksykacja przestrzeni informacyjnej za pomocą patogenów informacyjnych jest bardzo niebezpieczna, także dlatego, że wpisuje się w szerszą technikę manipulacji zwaną kontrolą odbitą, polegającą na wykorzystaniu reakcji, często odruchowej, na podany patogen, w celu manipulacji emocjami i zachowaniami innych.

Podatność społeczeństwa na infekcję wzmacniana jest nadmiarowością informacji i możliwością dostępu do wielu kanałów informacyjnych oraz połączona jest z brakiem umiejętności selekcji informacji, krytycznego myślenia i niezależności sądów. Ponadto potencjał tworzenia fałszywych informacji dzięki narzędziom →technologii informacyjno-komunikacyjnych [t. 4] sprawia, że manipulacja staje się coraz łatwiejsza i skuteczniejsza, np. dzięki wykorzystaniu mediów syntetycznych, wirtualnej i rozszerzonej rzeczywistości, biometrycznego masowego nadzoru, technologii →deepfake oraz →big data [t. 1], które – jak piszą autorzy raportu *Jak nasz sposób myślenia napędza dezinformację* – pozwalają przenieść →dezinformację na wyższy poziom.

W tej sytuacji konieczne staje się podjęcie działań uświadamiających zagrożenia wynikające z uaktywniania patogenów informacyjnych w środowisku człowieka. Problem ten był przedmiotem raportu *Jak budować odporność społeczną w przestrzeni informacyjnej i cyberprzestrzeni: przeciwdziałanie propagandzie i dezinformacji* przygotowanego w 2017 r. przez → Centrum Analiz Propagandy i Dezinformacji [t. 1]. Stwierdzono w nim, że podejmowanie działań w celu neutralizacji zewnętrznych ingerencji i wpływów na krajową przestrzeń informacyjną wymaga systemowego i kompleksowego potraktowania problemu zagrożenia dla → bezpieczeństwa narodowego [t. 1] i społecznego Polski oraz budowania odporności społeczeństwa na owe manipulacje w przestrzeni informacyjnej i → cyberprzestrzeni [t. 1]. W tym celu zaleca się:

- budowanie i umacnianie świadomości polskiego społeczeństwa w zakresie występowania zagrożenia w postaci manipulacji oraz mechanizmów i technologii wykorzystywanych do ich implementacji w polskiej przestrzeni informacyjnej i cyberprzestrzeni;
- wzrost poziomu wiedzy i umiejętności społeczeństwa na temat pozyskiwania, weryfikacji, analizy informacji i krytycznego myślenia, osiągany w procesie obowiązkowej edukacji medialnej;
- wsparcie ze strony administracji państwowej i podmiotów odpowiedzialnych za bezpieczeństwo państwa działań mających zapobiegać zewnętrznej propagandzie;
- szkolenie dziennikarzy mediów publicznych i niepublicznych na temat zagrożeń i skutków propagandy i dezinformacji;
- szkolenie polityków i samorządowców na temat zagrożeń i skutków propagandy i dezinformacji;
- monitorowanie przez organy państwa odpowiedzialne za bezpieczeństwo w cyberprzestrzeni treści rozpowszechnianych w przestrzeni informacyjnej, m.in. kanałach informacji władz samorządowych, w tym gminnych, na których pojawiają się treści ksenofobiczne i radykalne, działające na emocje, a pochodzące z wątpliwych źródeł;
- większy udział behawiorystów, psychologów, antropologów i socjologów w monitorowaniu i definiowaniu zagrożeń wynikających

z zewnętrznych przekazów propagandowych i dezinformacyjnych oraz opracowywaniu sposobów przeciwdziałania;
- zaangażowanie istniejących już środowisk społecznych, medialnych i profesjonalnych do pracy w administracji państwowej w tym obszarze;
- implementacja mechanizmu weryfikującego groźne dla Polski materiały propagandowe lub dezinformacyjne we wszystkich podmiotach państwowych i komercyjnych odpowiedzialnych za tworzenie i rozpowszechnianie informacji;
- systemowe podejście do problemu, jednoczesne działania ukierunkowane na identyfikację propagandy i dezinformacji – *fact checking*, przeciwdziałanie i neutralizację, budowanie → komunikacji strategicznej i własnego pozytywnego przekazu;
- czerpanie z doświadczeń innych państw w obszarze wprowadzania i realizacji nowych rozwiązań prawnych, systemowych i edukacyjnych;
- nawiązywanie, zacieśnianie i intensyfikacja współpracy z partnerami i podmiotami zagranicznymi, wykorzystywanie istniejących możliwości do czerpania *know-how* i kształcenia lub podnoszenia kwalifikacji własnych ekspertów i pracowników administracji.

Podstawą poznania sposobów rozprzestrzeniania się patogenów informacyjnych jest wiedza na temat aspektów ludzkiej psychologii, które warunkują to, w jaki sposób jednostki i całe społeczeństwa podatne są na działanie infotoksyn. Wiedza ta musi być przekazywana w procesie permanentnej edukacji informacyjno-medialnej całego społeczeństwa i wzmacniana zasobami przykładów toksykogennych działań dezinformacyjnych ujawnianych np. przez organizacje factcheckingowe wykorzystujące technikę weryfikacji informacji do oceny komunikatów emitowanych przez polityków i osoby publiczne. W podsumowaniu przytoczonego raportu czytamy, że idealny ekosystem walki z dezinformacją powinien być oparty na dialogu i współpracy pomiędzy platformami społecznościowymi, podmiotami odpowiedzialnymi za tworzenie regulacji prawnych, podmiotami zajmującymi się factcheckingiem oraz podmiotami odpowiedzialnymi za edukację człowieka zmuszonego żyć w zatrutym środowisku informacyjnym. Nie ustalono jednak, czyim

obowiązkiem, ze względu na bezpieczeństwo narodowe, jest walka z dezinformacją.

Hanna Batorowska

H. Batorowska, *Patogeny informacyjne*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; taż, *Przeciążenie informacyjne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019; W. Babik, *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014; tenże, *Ekologia informacji a bezpieczeństwo człowieka i informacji we współczesnym świecie*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; tenże, *O niektórych chorobach powodowanych przez informacje*, [w:] *Komputer w edukacji*, J. Morbitzer (red.), Pracownia Technologii Nauczania AP, Kraków 2006; S. Gliwa, *Psychologia kluczem do zwalczania dezinformacji?*, 10.01.2020, CyberDefence24.pl (dostęp 10.01.2020); M. Kowalska, A. Lelonek, *Raport: Jak budować odporność społeczną w przestrzeni informacyjnej i cyberprzestrzeni: przeciwdziałanie propagandzie i dezinformacji*, Fundacja Centrum Analiz Propagandy i Dezinformacji, 2017; A. Lewandowska, *Patologia informacji – jeden z elementów wojny hybrydowej*, „Ante Portas. Studia nad Bezpieczeństwem" 2016, nr 1 (6); taż, *Patologia informacji i jej związek z wojną informacyjną. Prezentacja założeń teoretycznych*, „Ante Portas. Studia nad Bezpieczeństwem" 2016, nr 2 (7); taż, *Wojna informacyjna a teoria patologii przestrzeni informacyjnej*, [w:] *Technologie morskie dla obronności i bezpieczeństwa*, Akademia Marynarki Wojennej, Gdańsk–Gdynia 2018; P. Pawełczyk, J. Jakubowski, *Postprawda i nowe media. Czy potrzebujemy postprawdy?*, „Środkowoeuropejskie Studia Polityczne" 2017, nr 1; J. Sala, H. Tańska, *Społeczno-gospodarcze bezpieczeństwo informacyjne w kontekście zatrucia informacyjnego*, „Roczniki Kolegium Analiz Ekonomicznych" 2016, nr 40; J. Woźnak-Kasperek, *Przeciążenie informacyjne – wprowadzenie do tematu*, „Fides. Biuletyn Bibliotek Kościelnych" 2018, nr 47 (2); R. Żuchowski, *Wojska Obrony Terytorialnej w działaniach antydezinformacyjnych*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 3.

INFRASTRUKTURA INFORMACYJNA (ang. *information infrastructure*; *networking and information infrastructure*) – to pojęcie różnie definiowane, stosowane m.in. w ekonomii, informatyce, →naukach o bezpieczeństwie [t. 3], administracji, logistyce i →informacji naukowej.

Niekiedy jest ono, nie do końca słusznie, utożsamiane z infrastrukturą informacji. Weszło do obiegu naukowego w pierwszej połowie lat 90. XX w. Przyczyną były szeroko nagłośnione, programowe dokumenty m.in. władz USA i Unii Europejskiej. Dotyczyły one różnych zagadnień związanych z przemianami cywilizacyjnymi wynikającymi ze wzrostu znaczenia informacji.

Badacze zajmujący się naukami o bezpieczeństwie zgodnie uznają, że do infrastruktury informacyjnej należą powiązane ze sobą infrastruktury: informatyczna i telekomunikacyjna. Odnośnie do innych aspektów związanych z omawianym pojęciem nie są już tak zgodni. W latach 90. w USA do infrastruktury informacyjnej badacze zaliczali informacje, dane, systemy telekomunikacyjne, sprzęt, wyposażenie pomocnicze oraz wykwalifikowany personel. D.E. Denning w 1999 r. uznała, że infrastruktura informacyjna to zasoby informacyjne i systemy komunikacji działające w przemyśle, instytucjach oraz pozostałe, którymi posługują się ludzie. Podobnie jak wielu późniejszych badaczy słusznie wskazała, że można wyróżnić różne rodzaje infrastruktury informacyjnej. Odnoszą się one do całego świata, poszczególnych krajów, wybranych ważnych zagadnień w skali ogólnokrajowej, poszczególnych przedsiębiorstw. Tytułem przykładu wyróżniła krajową infrastrukturę informacji (ang. *national information infrastructure*); infrastrukturę informacji obrony (ang. *defence information infrastructure*); globalną infrastrukturę informacji (ang. *global information infrastructure*) oraz infrastrukturę informacyjną danej firmy.

W 1997 r. M. Goliński, podobnie jak część naukowców na Zachodzie w XXI w., ograniczał omawiane pojęcie do najnowszych osiągnięć techniki w zakresie informatyki, a także telekomunikacji i mediów elektronicznych. Nieco inne stanowisko zajął J. Lubacz, podkreślając w 1998 r. (a później w 2002 r.), że infrastruktura informacyjna obejmuje usługi oraz środki, zarówno techniczne, jak i instytucjonalne, które służą świadczeniu usług. Mają one wspierać funkcjonowanie głównie życia społecznego i działalności ekonomicznej społeczeństw. Uznał techniczną część infrastruktury informacyjnej za konglomerat różnorodnych sieci. Słusznie wskazywał, że infrastruktura informacyjna jest stopniowo integrowana i podlega regulacjom wprowadzanym przez władze państwowe, a niekiedy także ponadpaństwowe.

G.J. Rattray w 2001 r. definiował infrastrukturę informacyjną jako działający łącznie zbiór. Ma on obejmować: sprzęt, oprogramowanie komputerowe, urządzenia przeznaczone do przechowywania i generowania danych, informacje wraz z ich zastosowaniami, pracowników o odpowiednich kwalifikacjach i połączenia pomiędzy wymienionymi składnikami. W 2005 r. A. Żebrowski doliczał do tego także internet, publiczne i wojskowe sieci danych, inne sieci (m.in. telefoniczne, rozgłośni telewizyjnych i radiowych, satelitarne komercyjne, transportowe, zasilania w energię, →bezpieczeństwa publicznego [t. 1]), satelitarne systemy telewizyjnej transmisji bezpośredniej, usługi (np. bankowe, nawigacyjne, wydawnicze, meteorologiczne, rozrywkowe), serwisy online oraz urządzenia szyfrujące. Jak wynika z powyższego wykazu, możliwości wpływu informacyjnego i technicznego na infrastrukturę informacyjną w celach wojskowych są istotne m.in. dla sił zbrojnych.

Niektóre z powyższych poglądów podzielił w 2006 r. J. Oleński. Jego zdaniem infrastruktura informacyjna to jednak pojęcie wyraźnie szersze. Stanowi ona zbiór wzajemnie uzupełniających się instytucji i jednostek organizacyjnych, zasobów i systemów informacyjnych oraz technologii informacyjnych. Warunkują one funkcjonowanie odpowiednich systemów m.in. społecznych, politycznych oraz ekonomicznych, a także zasobów informacyjnych. Według niego infrastruktura informacyjna służy do gromadzenia, przechowywania i udostępniania informacji w takich ilościach, by odpowiadało to oczekiwaniom danego społeczeństwa. Równocześnie chodzi tu o informację, niezbędną dla funkcjonowania innych systemów zarówno społecznych, jak też gospodarczych, politycznych i tych systemów informacyjnych, które obsługują konkretne podmioty (społeczne lub gospodarcze).

Zdaniem Oleńskiego kluczowym elementem infrastruktury informacyjnej jest to, że warunkuje ona istnienie innych obiektów, systemów i procesów oraz determinuje ich działanie i sprawność. W odróżnieniu od Lubacza Oleński podkreśla inny charakter powiązań między elementami składowymi infrastruktury informacyjnej. To już nie jest konglomerat, ale kompleks. Powyższa zmiana wynika z odnotowanej już przez Lubacza postępującej integracji, jak też coraz wyższego stopnia regulacji wprowadzanych przez poszczególne państwa i struktury ponadpaństwowe

(np. UE). Wprowadzane przy tej okazji procedury umożliwiają coraz większą zgodność powiązanych ze sobą systemów, coraz łatwiejsze gromadzenie i wymianę danych.

Do cech charakterystycznych omawianego pojęcia Oleński zaliczył trwałość, powszechność, dostępność, kompleksowość i integralność. Oczywiście infrastruktura informacyjna ma, jego zdaniem, także spełniać określone normy w zakresie informacji.

Częściowo zbieżny z powyższym jest wyrażony w tym samym 2006 r. pogląd K. Liedela. Zalicza on do infrastruktury informacyjnej zespół niezbędnych do funkcjonowania państwa i jego gospodarki podstawowych urządzeń, instytucji i systemów. Natomiast Żebrowski podkreślał rolę usługową infrastruktury informacyjnej. Według tego badacza łączy ona, zabezpiecza i (w następstwie tego) wpływa na inne infrastruktury.

Z punktu widzenia funkcji i zakresu Oleński w 2006 r. wyróżnił i zdefiniował 7 rodzajów infrastruktury informacyjnej: globalną, państwa, gospodarki, społeczną, polityczną, branżową oraz regionu. Ze względu na zauważane w literaturze przedmiotu zwiększenie roli czynników ekonomicznych w budowie i utrzymywaniu bezpieczeństwa większość z wymienionych niewątpliwie wchodzi w zakres zainteresowań nauk o bezpieczeństwie. Z wyjątkiem infrastruktury informacyjnej państwa oraz globalnej infrastruktury informacyjnej wymienione rodzaje infrastruktury informacyjnej są jednak, nawet w Polsce, bardzo rzadko stosowane przez badaczy. Być może w praktyce ich przydatność w badaniach naukowych okazała się ograniczona.

Infrastrukturze informacyjnej państwa Oleński poświęcił ponad 700-stronicową książkę. Jego zdaniem to znajdujący się na terytorium określonym umowami międzynarodowymi zbiór takich wzajemnie powiązanych infrastrukturalnych zasobów oraz informacyjnych systemów, które warunkują postrzeganie państwa. Infrastruktura informacyjna państwa składa się z systemów informacyjnych, zasobów informacji i stosowanych wobec nich norm, informacyjnych instytucji, struktur organizacyjnych, a także urządzeń technicznych. Wymienione wspomagają gromadzenie, przechowywanie, przetwarzanie oraz przekaz informacji w ramach procesów i systemów informacyjnych. W 2008 r. niemal identycznie zdefiniowała omawiane pojęcie H. Świeboda. Zdecydowanie częściej

jednak używa się, nawet w polskiej literaturze przedmiotu, innej, równie trafnej nazwy: krajowa infrastruktura informacyjna (lub jej wariantów). W 2018 r. stosuje ją także sam Oleński. Definiuje ją jednak nieco inaczej niż jej odpowiednik kilkanaście lat wcześniej. Uznaje, że jest to zespół wzajemnie powiązanych elementów, który warunkuje funkcjonowanie z jednej strony państwa, z drugiej gospodarki, społeczeństwa, a także generalnie systemów i→procesów informacyjnych [t. 3]. W skład tego zespołu wchodzą: normy, zasoby, procesy, systemy oraz podmioty informacyjne. Są one kształtowane z jednej strony przez najważniejsze organy administracji państwowej; z drugiej zaś przez, jak to określił, komercyjne podmioty informacyjne. Odbywa się to zgodnie z obowiązującymi w danym kraju regulacjami prawnymi. Tak jak przed kilkunastu laty Oleński przyznaje, nie bez racji, wyróżnionemu przez siebie zespołowi elementów ogromne znaczenie. Według niego poziom jakości oraz integralności (spójności) infrastruktury informacyjnej danego kraju decyduje nie tylko o sprawności samego państwa. Dotyczy to również gospodarki, jakości życia społecznego i poziomu bezpieczeństwa informacyjnego ogółu obywateli, a także podmiotów zarówno społecznych, politycznych, jak i gospodarczych.

Jak trafnie zauważył – budowa zintegrowanej infrastruktury tego rodzaju stanowi obecnie podstawę dla działania sprawnego aparatu państwa. Za poziom integralności infrastruktury informacyjnej jego zdaniem odpowiada: spójność podstaw prawnych, praw i obowiązków informacyjnych, spójność informacyjna i organizacyjna norm, zasobów oraz procesów i systemów, a także ich bazy technicznej i organizacyjnej, redukcja redundancji do niezbędnego poziomu w ramach całej infrastruktury informacyjnej kraju oraz kontrola jakości informacji.

Tylko częściowo przydatna dla nauk o bezpieczeństwie jest definicja infrastruktury informacyjnej państwa autorstwa B. Szafrańskiego. Kładzie on nacisk na procedury, modele oraz zarządzanie informacją i jej przekazywanie. Pomija natomiast instytucje i niemal całe zasoby infrastrukturalne, które znajdują się na terytorium danego państwa.

Definicję notowanej np. przez Rattraya (w 2001 r.) globalnej infrastruktury informacyjnej na gruncie polskim podaje w 2006 r. Oleński. Uznaje ją za zespół wzajemnie powiązanych zasobów infrastrukturalnych

i operacyjnych systemów, które warunkują funkcjonowanie procesów mających zasięg globalny. To jego zdaniem zespół tych wzajemnie powiązanych ze sobą procesów oraz systemów i zasobów informacyjnych, które są w skali ponadpaństwowej tworzone, udostępniane lub upowszechniane. Zaliczył tu m.in. obejmujący teoretycznie cały świat system statystyki publicznej, globalne systemy informacyjne sektora finansowego oraz globalne systemy alertowe. Jest ona kształtowana przez organizacje i korporacje międzynarodowe.

Wyróżniono kilka poziomów tego rodzaju infrastruktury (m.in. regionalny i krajowy). Opisano co najmniej 3 modele globalnej infrastruktury informacyjnej – implementacyjny, strukturalny i funkcjonalny. Centralna administracja rządowa nadzoruje i zarządza poziomem krajowym, obejmującym m.in. → i n f r a s t r u k t u r ę k r y t y c z n ą danego państwa. Na tym poziomie na infrastrukturę informacji wpływają także komercyjne podmioty informacyjne krajowe i zagraniczne.

W globalnej infrastrukturze poszczególne państwa mogą aktywnie uczestniczyć poprzez generowanie i udostępnianie informacji. W związku z postępem technologicznym wpływają jednak na wymienione w ograniczonym stopniu. W obrębie globalnej infrastruktury głównymi instrumentami upowszechniania informacji są środki masowej komunikacji.

Z punktu widzenia nauk o bezpieczeństwie istotna będzie także stosowana w literaturze przedmiotu sektorowa infrastruktura informacyjna. Żebrowski zaliczył do niej m.in. informacyjne infrastruktury bezpieczeństwa: wewnętrznego państwa, obrony, → w y w i a d u [t. 4] i → k o n t r w y w i a d u, instytucji antykorupcyjnych, sądów oraz służb informacyjnych i ratowniczych. Warto dodać, że sektorowa infrastruktura informacyjna jest analogiczna do mającej tę samą nazwę części składowej wspomnianej wyżej, zdefiniowanej przez Oleńskiego branżowej struktury informacyjnej.

Tomasz Skrzyński

J. Chęć, *Realizacja Globalnej Infrastruktury Informacyjnej*, „Zeszyty Naukowe Wydziału ETI Politechniki Gdańskiej. Technologie Informacyjne" 2008, vol. 15; D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002; K. Kuźniar-Żyłka, *Badania naukowe a rozwój infrastruktury informacyjnej w gospodarce opartej na wiedzy*, „Studia

Ekonomiczne" 2013, nr 145; K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006; J. Lubacz, *Infrastruktura informacyjna – opcje i dylematy rozwoju*, „Raporty. Instytut Rozwoju i Studiów Strategicznych" 1998, nr 67; J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Wydział Nauk Ekonomicznych Uniwersytetu Warszawskiego, Warszawa 2006; tenże, *Strategie rozwoju e-państwa w perspektywie 2030 roku*, „Roczniki Kolegium Analiz Ekonomicznych" 2018, nr 48; G.J. Rattray, *Strategic Warfare in Cyberspaces*, Massachusetts Institute of Technology, Cambridge 2001; T. Skrzyński, *Infrastruktura informacyjna*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; T. Stupak, R. Wawruch, *Telecommunication Infrastructure of the Polish National Maritime Safety*, „Archives of Transport System Telematics" 2016, vol. 9; H. Świeboda, *Zagrożenia informacyjne bezpieczeństwa narodowego*, [w:] *Badania operacyjne i systemowe a zagadnienia społeczeństwa informacyjnego, bezpieczeństwa i walki*, J. Kacprzyk, A. Najgebauer, P. Sienkiewicz (red.), Instytut Badań Systemowych PAN, Polskie Towarzystwo Badań Operacyjnych i Systemowych, Warszawa 2008; A. Żebrowski, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego. Wybrane problemy*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016.

INFRASTRUKTURA KRYTYCZNA – fizyczne i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa.

Pojęcie infrastruktury krytycznej, mimo że zostało użyte po raz pierwszy dopiero kilkadziesiąt lat temu, istnieje, odkąd można mówić o rozwiniętej cywilizacji, a więc już od czasów starożytnych. Na terenie każdego państwa znajduje się infrastruktura krytyczna (IK), która ma duże znaczenie dla funkcjonowania państwa i obywateli, a także dla gospodarki, stąd też ochrona IK jest jednym z priorytetów stojących przed każdym państwem, także przed państwem polskim. Istota zadań związanych z IK sprowadza się nie tylko do zapewnienia jej ochrony przed →zagrożeniami [t. 4], lecz dotyczy również tego, by ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki.

IK jest stosunkowo nowym elementem branym pod uwagę przy tworzeniu →strategii [t. 4] →bezpieczeństwa [t. 1] państwa. Szczególne

zainteresowanie decydentów w tym obszarze należy wiązać z sytuacją międzynarodową i pojawiającymi się zagrożeniami i ich konsekwencjami w przypadku uszkodzenia kluczowych dla gospodarki państwa obiektów oraz urządzeń. Zagrożenia te mają zarówno charakter egzogenny i odnoszą się do uszkodzenia IK przez bezpośrednią lub pośrednią działalność międzynarodowych organizacji terrorystycznych, jak również charakter endogenny, związany z wystąpieniem szeroko rozumianej awarii technicznej, np. uszkodzeń spowodowanych katastrofą naturalną.

Do wskazanej kategorii należy również zaliczyć zagrożenia → cyberterroryzmem [t. 1]. Nie jest to zamknięta lista sytuacji mających wpływ na bezpieczeństwo IK. Natomiast istota zagrożeń dla IK odnosi się do konsekwencji spowodowanych jej zniszczeniem lub uszkodzeniem. Związane są one z zakłóceniami funkcjonowania państwa we wszystkich jego wymiarach. Mając na uwadze szybki rozwój techniczny, nie bez znaczenia pozostaje fakt rosnącej w sposób lawinowy zależności elementów tworzących IK.

W warunkach Polski zagadnienia te reguluje przyjęta w 2007 r. ustawa o zarządzaniu kryzysowym. Na jej podstawie za infrastrukturę krytyczną uważa się systemy oraz połączone ze sobą funkcjonalnie obiekty (w tym obiekty budowlane, urządzenia, instalacje i usługi), konieczne i ważne, aby zapewnić bezpieczeństwo państwa i jego obywateli, oraz służące zagwarantowaniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Jednym z elementów → zarządzania kryzysowego [t. 4] związanego ochroną IK jest współpraca administracji publicznej. Ma ona polegać na wspólnych działaniach, których celem jest poprawa warunków bezpieczeństwa. Ważnym elementem zapewnienia bezpieczeństwa jest również współpraca z przedsiębiorcami. Jej celem jest wypracowanie przejrzystych zasad i procedur między administracją a właścicielami samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Wynika to z faktu, iż znaczna część infrastruktury mającej kluczowe znaczenie dla bezpieczeństwa państwa znajduje się obecnie w rękach prywatnych.

W skład elementów tworzących IK wchodzą następujące systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,

- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- →ochrony zdrowia [t. 3],
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Powszechnie wskazuje się następujące rodzaje ochrony IK:

- Ochrona fizyczna – ochrona osób (zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej). Realizowana jest przez pracowników ochrony, którzy bronią dostępu do obiektów, urządzeń, instalacji lub usług IK.
- Ochrona techniczna – ogół przedsięwzięć związany z budową i eksploatacją obiektów, urządzeń, instalacji i usług IK, w tym również techniczne środki ochrony, minimalizujące zagrożenia IK.
- Ochrona osobowa – ma na celu minimalizację ryzyka będącego skutkiem działań pracowników oraz usługodawców, którzy mogą dopuścić do zakłóceń w funkcjonowaniu infrastruktury krytycznej.
- Ochrona teleinformatyczna – zespół przedsięwzięć i ich procedur, które mają na uwadze minimalizację zakłóceń w funkcjonowaniu IK związanych z wykorzystaniem do użytkowania tego typu infrastruktury systemów i sieci teleinformatycznych.
- Ochrona prawna – związana z kształtem współczesnej gospodarki rynkowej, w której dochodzi do zagrożeń ze strony innych podmiotów państwowych lub prywatnych.

Próba identyfikacji obiektów, urządzeń, instalacji lub usług, których zniszczenie bądź problemy w ich funkcjonowaniu doprowadziłyby do →sytuacji kryzysowej [t. 4], jest kluczowym zadaniem w jej ochronie. W tym celu rozgranicza się 2 grupy kryteriów:

- Kryteria systemowe (sektorowe) – można je określić jako parametry ilościowe lub funkcjonalne infrastruktury; charakteryzują

parametry wchodzące w skład systemów IK obiektów, urządzeń oraz instalacji lub funkcje realizowane przez te obiekty i zapewniające identyfikację IK.

- Kryteria przekrojowe – określają skalę skutków zniszczenia, jak również zaprzestania funkcjonowania wskazanej infrastruktury, w tym m.in. skalę:
  - ofiar w ludziach,
  - skutków finansowych,
  - konieczności ewakuacji,
  - utraty usługi,
  - czasu odbudowy,
  - efektów międzynarodowych,
  - unikatowości.

Przedstawione elementy ochrony IK są ze sobą bardzo silnie powiązane i tylko poprzez łączne ich stosowanie mogą przynosić rezultaty. Aby ochrona IK była skuteczna, powinna być realizowana na każdym poziomie i stanowić wspólny wkład zarówno administracji rządowej, samorządowej oraz operatorów, jak i niepublicznych właścicieli infrastruktury. Pozwoli to na zwiększenie znacznego poziomu bezpieczeństwa w państwie.

Pojęcie IK jest znane w polskim systemie prawnym od 2007 r., jednak należy tu zaznaczyć, iż do 2007 r. obiekty IK zaliczane obecnie do tej grupy były poddane ochronie. W tym kontekście na uwagę zasługuje ustawa o powszechnym obowiązku obrony RP oraz rozporządzenie Rady Ministrów w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, wprowadzające pojęcie ochrony szczególnie ważnych dla bezpieczeństwa i obronności państwa obiektów.

Do wskazanej kategorii obiektów zaliczono zakłady produkujące oraz remontujące i magazynujące uzbrojenie oraz sprzęt wojskowy i środki bojowe, magazyny rezerw państwowych, obiekty jednostek organizacyjnych, które podlegają ministrowi obrony narodowej, obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, zapory wodne, elektrownie. Należy również zauważyć, że zbieżny katalog obiektów został wskazany w ustawie o ochronie osób i mienia, przy czym wprowadzono we wspomnianym dokumencie bardziej szczegółowy podział na kategorie obiektów.

Dodatkowo ustawodawca w ramach bezpieczeństwa zewnętrznego, bezpieczeństwa państwa i sprawowania ogólnego kierownictwa w dziedzinie obronności państwa powierzył Radzie Ministrów określenie obiektów szczególnie ważnych dla bezpieczeństwa państwa, obronności, a także przygotowanie planów ich szczególnej ochrony. Pojęcia ochrony szczególnej i ochrony obowiązkowej stały się podstawą do zdefiniowania infrastruktury krytycznej w polskim ustawodawstwie. Mniej więcej w tym samym czasie powstały podwaliny prawne ochrony IK w państwach UE oraz →NATO [t. 3]. Szczególnie tragiczne wydarzenia z 2001 r. w Nowym Jorku przyspieszyły prace nad stworzeniem formalnego systemu ochrony IK. Zgodnie z definicją przygotowaną przez grupę ekspertów Komitetu Ochrony Cywilnej NATO IK to obiekty, służby i systemy informacyjne, które są żywotne dla interesów państwa, których uszkodzenie lub zniszczenie mogłoby mieć niebagatelny wpływ na bezpieczeństwo państwa, krajową gospodarkę, zdrowie i bezpieczeństwo publiczne oraz prawidłowe funkcjonowanie rządu.

Prace związane z przygotowaniem europejskiego programu ochrony IK były następstwem decyzji podjętej w czerwcu 2004 r. przez Radę Europejską, która zleciła Komisji Europejskiej opracowanie strategii dotyczącej ochrony IK. Komisja przygotowała komunikat, w którym zaproponowano przygotowanie nowych instrumentów – europejskiego programu ochrony infrastruktury krytycznej (EPOIK) oraz sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (SOZIK). W grudniu 2006 r. zaprezentowano komunikat Komisji w sprawie EPOIK określający zakres działań. Jednocześnie Komisja przedstawiła projekt dyrektywy w tym obszarze, który został przyjęty po poprawkach w 2008 r. W tym dokumencie po raz pierwszy do porządku prawnego UE wprowadzono definicję IK, europejskiej infrastruktury krytycznej (EIK), ochrony infrastruktury krytycznej oraz pojęcie właściciela (operatora) europejskiej infrastruktury krytycznej. W dyrektywie określono sposób rozpoznawania i wyznaczania EIK, a także obowiązki państw członkowskich i właścicieli tej infrastruktury. Dyrektywa definiuje IK jako składniki, systemy lub części infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego

ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji.

Ważnym elementem dyrektywy jest uwzględnienie w jej zapisach sektora prywatnego, w którego rękach znajduje się większość IK. Polska implementowała wspomniany akt prawa wspólnotowego do porządku prawnego, nowelizując ustawę o zarządzaniu kryzysowym. Zgodnie z nią dyrektor →Rządowego Centrum Bezpieczeństwa [t. 3] (RCB), razem z ministrami i kierownikami urzędów centralnych, na bieżąco rozpoznaje potencjalną EIK, a także tworzy narodowy program ochrony infrastruktury krytycznej (NPOIK). Celem NPOIK jest stworzenie warunków do poprawy bezpieczeństwa IK, w szczególności w zakresie zapobiegania zakłóceniom funkcjonowania IK, przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na IK, reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania IK, a także odtwarzania IK.

Należy tu jasno zaznaczyć, iż nie każdy strategiczny obiekt należy do IK. Wyodrębnienie tych systemów, instalacji, obiektów i usług jest prerogatywą dyrektora RCB. Opracowuje on niejawne kryteria pozwalające wyodrębnić IK i przekazuje je do uzgodnień ministrom i kierownikom urzędów centralnych.

Ustawa o zarządzaniu kryzysowym i akty wykonawcze do tejże ustawy to niejedyne zbiory przepisów w polskim systemie prawnym poruszające problematykę IK. Wskazane regulacje stały się jednak podstawą do tworzenia dalszych, bardziej szczegółowych regulacji prawnych w tym zakresie. Konieczność doprecyzowania regulacji w zakresie IK została podyktowana przez stały postęp technologiczny, który powoduje narastające współzależności pomiędzy poszczególnymi elementami IK na poziomie państwa, poziomie regionalnym oraz poziomie międzynarodowym. W praktyce oznacza to, iż uszkodzenie jednego z elementów IK powoduje straty w innych. Jest to związane z rozwojem połączeń między poszczególnymi elementami IK, które obecnie charakteryzuje wzajemne powiązania i uzależnienie i które na skutek informatyzacji są bardziej podatne na różnego rodzaju zagrożenia systemowe.

Do tego zbioru można również zaliczyć ustawę o szczególnych uprawnieniach ministra właściwego do spraw skarbu państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych

prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych. Akt ten określa szczególne uprawnienia (sprzeciw wobec decyzji władz spółki) przysługujące ministrowi właściwemu do spraw skarbu państwa w spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład IK, sporządzanym przez dyrektora RCB. Akt wykonawczy do wspomnianej ustawy nakazuje również powołanie pełnomocnika ds. ochrony IK. Pełnomocnik ten jest pracownikiem spółki, monitorującym jej działalność w zakresie dysponowania mieniem objętym ustawą i odpowiada za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony IK. Kolejnym przykładem mogą być przepisy traktujące o krajowym systemie →cyberbezpieczeństwa [t. 1]. Ustawa nakłada obowiązki służące zapewnieniu cyberbezpieczeństwa w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej państwa. Do tych sektorów zalicza się: energetykę, transport, bankowość, instytucje finansowe, sektor ochrony zdrowia, zaopatrzenie w wodę i infrastrukturę cyfrową. Ustawa o krajowym systemie cyberbezpieczeństwa i ustawa o zarządzaniu kryzysowym są więc komplementarne – uzupełniają się nawzajem. Jeden podmiot może być zarówno operatorem IK, jak i operatorem usługi kluczowej.

Większość autorów poruszających się w materii bezpieczeństwa IK definiuje jako rzeczywiste i cybernetyczne systemy niezbędne do minimalnego funkcjonowania gospodarki i państwa. IK ma kluczowe znaczenie dla istnienia państwa, a w jego ramach zorganizowanego społeczeństwa, gdyż jeżeli następuje zakłócenie w jej funkcjonowaniu, państwo i jego instytucje mogą utracić w całości lub części zdolność do wykonywania swoich podstawowych funkcji administracyjnych i usługowych, jak również możliwość sprawowania rzeczywistej kontroli nad całym swoim terytorium. Utrata infrastruktury uniemożliwia rozwój gospodarczy i społeczny, a w pewnych przypadkach może doprowadzić nawet do rozkładu życia społecznego.

Łukasz Szewczyk

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony; Z. Łukasik, W. Nowakowski, A. Kuśmińska-Fiałkowska, *Zarządzanie bezpieczeństwem infrastruktury krytycznej*, 2014; R. Piwowarczyk, *Kierowanie ochroną infrastruktury krytycznej*, [w:] *Kierowanie bezpieczeństwem narodowym*, B. Zdrodowski, B. Wiśniewski (red.), Warszawa 2008; RCB.gov.pl (dostęp 25.02.2020); Rozporządzenie Prezesa Rady Ministrów z dnia 22 marca 2017 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej, Dz. U. 2017, poz. 627; Rozporządzenia Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz. U. 2003, nr 116, poz. 1090; Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz. U. 2010, nr 83, poz. 542; K. Stec, *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce*, „Bezpieczeństwo Narodowe" 2011, nr 19; T. Szewczyk, M. Pyznar, *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2 (2); J. Trybulska, *Wybrane aspekty ochrony infrastruktury krytycznej w Polsce*, „Zeszyty Naukowe WSEI" 2015, nr 1; Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018, poz. 1560; Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, Dz. U. 2010, nr 65, poz. 404; Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz. U. 1967, nr 44, poz. 220; Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, Dz. U. 1997, nr 114, poz. 740; M. Żuber, *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, nr 2.

INFRASTRUKTURA WOJSKOWA (ang. *military infrastructure*) – celowo budowana i wykorzystywana przez siły zbrojne co najmniej od czasów imperium asyryjskiego, wg najszerszej interpretacji składa się z 4 części: stacjonarnych obiektów, stacjonarnych urządzeń, niewielkiej grupy ruchomych obiektów i urządzeń, które powstały w celu zaspokajania potrzeb armii oraz wojskowych oddziałów i struktur zapewniających wymienionym wyżej częściom zaopatrzenie i sprawność techniczną. Szczególnie chodzi o bieżące i przyszłe potrzeby wojska dotyczące dowodzenia, łączności, szkolenia, bytowania, magazynowania, dokonywania napraw

sprzętu wojskowego, przemieszczania sił zbrojnych oraz ich operacyjnego rozwinięcia.

W pojęciu infrastruktury wojskowej (IW) mieszczą się m.in. bazy wojskowe, koszary, lotniska wojskowe, magazyny wojskowe, obiekty szkoleniowe terenowe, parki sprzętu technicznego, składy wojskowe oraz bocznice kolejowe wojskowe.

Niektórzy badacze, raczej niesłusznie, usuwają spośród wymienionych potrzeb armii operacyjne rozwinięcie sił zbrojnych oraz łączność. Inni znawcy zagadnienia kwestionują obecność w definicji jednostek wojskowych albo zaliczają do IW obiekty i urządzenia logistyczne i inżynieryjne.

IW jest częścią infrastruktury obronnej, potencjału wojskowego (militarnego), logistycznego zabezpieczenia mobilizacyjnego rozwinięcia wojsk oraz bazy produkcyjno-usługowej zaspokajającej potrzeby obronne państwa (lub sojuszu państw).

W literaturze przedmiotu podkreśla się, że jakość IW i poziom dbałości o nią w sposób poważny wpływają na → b e z p i e c z e ń s t w o m i l i t a r n e [t. 1] państwa. Można nawet spotkać pogląd, że w razie konfliktu zbrojnego stan IW wpływa w decydujący sposób na jakość działania sił zbrojnych. Dla części badaczy stanowi ona podstawę utrzymania bezpieczeństwa w sferze militarnej. Nawet jeśli uznać te poglądy za nieco przesadne, to niewątpliwie IW w dużym stopniu wpływa na rolę danego państwa w sojuszach wojskowych.

Niektóre obiekty IW równocześnie wchodzą w skład innych pojęć składowych infrastruktury obronnej. W szczególności chodzi o niektóre obiekty infrastruktury techniczno-ekonomicznej i społecznej ważne dla obronności państwa. R. Radziejewski utożsamia je z infrastrukturą → o b r o n y c y w i l n e j [t. 3].

W tym wypadku ustalenia terminologiczne mają ścisły związek z rzeczywistością. Poza obiektami przeznaczonymi wyłącznie do celów wojskowych do IW zalicza się bowiem także obiekty służące społeczeństwu, a równocześnie także wymienionym celom wojskowym. Wymienia się tu równoczesne użytkowanie lotnisk wojskowych oraz budowli służących szkoleniu i bytowaniu → ż o ł n i e r z y [t. 4] (infrastruktura sportowa, rekreacyjna; oczyszczalnie ścieków). Nieprzypadkowo IW wznoszona jest

zarówno ze środków budżetowych, jak i lokalnych (szczególnie obiekty współużytkowane z obywatelami).

Jak słusznie zauważył R. Radziejewski, tylko najważniejsza część IW wchodzi w obręb → infrastruktury krytycznej. Znaczenie obiektów należących do infrastruktury wojskowej w odniesieniu do obronności państwa jest bowiem bardzo zróżnicowane. Trudno przyjąć, by w obrębie infrastruktury krytycznej mieściły się równocześnie stołeczny garnizon pułku ochraniającego dyktatora kierującego państwem autorytarnym i niewielka, zmodernizowana ze środków tamtejszego ministerstwa obrony oczyszczalnia ścieków niezbędna dla zapewnienia warunków bytowych w tym samym państwie żołnierzom jednego z prowincjonalnych garnizonów.

Nie można się zgodzić z poglądami utożsamiającymi IW z infrastrukturą terenową. W skład tej pierwszej wchodzi bowiem także infrastruktura wykorzystywana przez system kierowania obroną w skali państwa i dowodzenia całymi siłami zbrojnymi będącymi w dyspozycji władz centralnych. J. Tomaszewski nazywa tę część IW funkcjonalną infrastrukturą ochronną. Obejmuje ona zarówno obiekty adaptowane, jak i specjalnie do tego celu budowane. Musi ona spełniać podwyższone kryteria dotyczące odporności na środki rażenia potencjalnego przeciwnika.

Część IW zaliczana jest do infrastruktury bilateralnej. Obejmuje ona te obiekty wojskowe, które są finansowane na podstawie porozumienia między dwoma członkami sojuszu wojskowego. Przykładem mogą być urządzenia, z których korzysta głównie wojsko jednego państwa, a znajdują się w obrębie granic jego sojusznika.

Inną częścią IW jest infrastruktura wspólna. Składają się na nią obiekty istotne pod względem szkolenia wojsk danego sojuszu wojskowego lub wprowadzania w życie tych planów operacyjnych, które są wspólnie finansowane przez jego członków.

Funkcjonowanie IW wymaga dbałości o jej sprawność techniczną i funkcjonalną. Niekiedy utrzymanie infrastruktury obronnej wprost zalicza się do obowiązków państwa wobec obywateli. Zwykle władze dbają o nowe infrastrukturalne inwestycje wojskowe. Mniej są jednak skłonne do wydawania środków na konserwację i utrzymanie infrastruktury, która już jest.

Za planowanie, organizowanie i działanie IW w państwie odpowiadają określone struktury. Jej najważniejsza część składowa powstaje w ramach celów i priorytetów wyznaczanych przez programy obronne. Równocześnie jednak modernizacja IW w danym państwie jest ściśle powiązana z rozbudową tamtejszego systemu cywilnego transportu.

W szeregu państw planowaniem, modernizacją, rozbudową, przygotowaniem na wypadek konfliktu zbrojnego, zarządzaniem oraz użyciem w celach militarnych infrastruktury wojskowej zajmuje się podsystem IW w ramach systemu logistycznego armii. Niekiedy jest on wprost nazywany IW. Inni badacze utożsamiają elementy tego podsystemu z organami (jednostkami organizacyjnymi) IW. Te ostatnie są bardzo zróżnicowane szczególnie na szczeblu regionalnym i lokalnym. Przykładem odnośnie do Polski mogą być Terenowe Oddziały Lotniskowe czy Komendy Portów Wojennych.

Wspomniane plany dotyczące IW dotyczą modernizacji technicznej, inwestycji budowlanych, zakupu materiałów oraz inwestycji dokonywanych w ramach przynależności do sojuszu wojskowego. W obręb kompetencji podsystemu IW wchodzi także zabezpieczenie szkolenia wojsk oparte na IW.

Funkcjonowanie wspomnianego podsystemu opiera się na zasadach: stacjonarności, lokalnego zaopatrywania, rozdzielności funkcji dowódczych od gospodarczych, elastyczności w planowaniu oraz ochrony środowiska. Podsystem ten odpowiada także za dostarczanie do IW m.in. paliw grzewczych, benzyny, gazu ziemnego, energii cieplnej i elektrycznej oraz usług komunalnych.

S. Dworecki wskazuje na duże znaczenie dla sprawnego działania infrastruktury ustalenia odpowiednich jakościowych i ilościowych norm i wskaźników obsługi podmiotów. Ważniejsza od zapisów w instrukcjach i wytycznych wydaje się jednak strona praktyczna. Jak wskazują badania, bardzo duże → z a g r o ż e n i a [t. 4] dla IW mogą wynikać z błędów ludzkich. Podkreśla to konieczność dalszych szkoleń w jednostkach wojskowych odpowiedzialnych za bezpieczeństwo IW.

W czasie konfliktu zbrojnego głównym przedmiotem zainteresowania podsystemu IW jest zapewnienie sprawności omawianego rodzaju infrastruktury, a równocześnie jej przygotowanie oraz ewentualna odbudowa

i rozbudowa. Realizuje w tym zakresie polecenia władz państwa i wymagania wynikające ze zobowiązań sojuszniczych.

W zależności od planów władz nadrzędnych organy omawianej infrastruktury przygotowują przekazanie dla struktur cywilnych zbędnych elementów IW, a równocześnie pozyskują nieruchomości mające umożliwić rozbudowę jednostek wojskowych oraz poprawić ich działanie i szkolenie.

Warto tu za M. Sułkiem odnotować postulat, by działania związane z dbaniem o infrastrukturę „typowo" wojskową także częściowo przekazać sektorowi prywatnemu (np. remonty, utrzymanie). Do najważniejszych przeszkód należy ograniczona zdolność indywidualnych przedsiębiorców do odpowiedniej dbałości o ochronę → i n f o r m a c j i wojskowej. Ponadto, jak wskazuje M. Boulègue, bywają kraje i okoliczności, w których ze względów ekonomicznych władzom państwowym bardziej opłaca się przy rozbudowie infrastruktury wykorzystać struktury wojskowe.

Władze państwowe regulują ochronę omawianych obiektów w warunkach pokoju, → k r y z y s u i konfliktu zbrojnego. Odpowiada za nią kierownik jednostki bezpośrednio zarządzający obszarami, na których są rozmieszczone dane elementy składowe IW. Obiekty należące do IW mają z reguły przygotowane plany obrony szczególnej. Ma to przeciwdziałać i łagodzić skutki aktywności przeciwnika w odniesieniu do IW.

Dostęp do IW jest regulowany przy pomocy środków ochrony fizycznej. Mają one na celu zminimalizowanie ryzyka zakłóceń funkcjonowania elementów omawianej infrastruktury przez osoby niepowołane. Przykładem są działania zmierzające do uniemożliwienia wstępu na teren obiektów osobom nieupoważnionym czy zadbanie o ochronę techniczną i teleinformatyczną tych obiektów. Do ich ochrony oddelegowuje się pododdziały wojska lub niekiedy specjalnie w tym celu tworzone jednostki zmilitaryzowane.

W przypadku inwestycji realizowanych w związku z potrzebami bytowymi żołnierzy może zajść konieczność także ochrony prawnej IW. Ma ona na celu m.in. minimalizację zakłóceń w działaniu obiektów infrastruktury będących w posiadaniu prywatnym, związanych z wrogim przejęciem, fuzją lub sprzedażą tych elementów infrastruktury.

Z badań A. Tyburskiej dotyczących UE można wysnuć wniosek, że najczęściej zagrożenia dla IW wynikają z klęsk żywiołowych. Na innych

kontynentach jest podobnie. Przykładowo, jak podaje E. Babson, w 2019 r. 67% ocenianych obiektów IW USA było zagrożonych powodzią, 54% suszą, a 46% pożarem.

Nieprzypadkowo w literaturze można spotkać pojęcie zasobów infrastruktury wojskowej. Jak słusznie zauważył Tomaszewski, funkcjonowanie IW wymaga stworzenia i stałego utrzymywania odpowiednich do potrzeb rezerw (w tym strategicznych). Ważna jest także odpowiednia osłona techniczna dla najważniejszej części IW. W tym ostatnim przypadku chodzi szczególnie o gwarancję dostarczenia odpowiednich konstrukcji oraz urządzeń i materiałów.

O znaczeniu IW pośrednio świadczy też stosowanie w literaturze przedmiotu dość licznych synonimów: infrastruktura logistyczna; infrastruktura obronna; infrastruktura wojenna; czasem także infrastruktura militarna.

Ważne elementy IW wchodzą w skład podsystemu kierowania systemu kierowania →bezpieczeństwem narodowym [t. 1] oraz systemu obronności. Nie przeczy to równoczesnemu zaliczeniu licznych obiektów infrastruktury wojskowej do terytorialnej organizacji wojskowej. Niektóre obiekty IW stanowią w tym samym czasie część infrastruktury geoinformacyjnej. Warto też odnotować, że rozmieszczenie obiektów IW na terenie państwa wchodzi w zakres geografii wojskowej.

Omawiane pojęcie można uznać za pokrewne do →infrastruktury informacyjnej i logistyki wojskowej. Częściowo pokrywa się ono z infrastrukturą walki zbrojnej. Ta ostatnia, jak wskazuje S. Koziej, obejmuje jednak szeroko rozumiane środowisko konkretnego teatru wojny.

Tomasz Skrzyński

E. Babson, *Climate Change Impacts on National Security. Threats to American Military Infrastructure, Readiness, and Lives*, American Security Project, 2019; M. Boulègue, *Military Infrastructure and Logistics in the Russian Arctic*, [w:] tegoż, *Russia's Military Posture in the Arctic: Managing Hard Power in a „Low Tension" Environment*, Hatham House, The Royal Institute of International Affairs, London 2019; S. Dworecki, *Infrastruktura w bezpieczeństwie obywateli i państwa*, [w:] *Infrastruktura krytyczna w procesie zarządzania w sytuacjach kryzysowych*, t. 1, A. Gałecki, A. Kurkiewicz, S. Mikołajczak (red.), Wydawnictwo Wyższej Szkoły

Bezpieczeństwa, Poznań 2014; R. Jakubczak, K. Galicki, *Infrastruktura krytyczna w warunkach globalizacji*, [w:] *Wielowymiarowość obszaru bezpieczeństwa. Wybrane problemy bezpieczeństwa międzynarodowego*, W. Jakubczak, M.P. Podobny (red.), Wydawnictwo Wyższej Szkoły Agrobiznesu w Łomży, Łomża 2014; Z. Kamyk, *Doktrynalne i techniczne problemy force protection engineering w Wojsku Polskim*, [w:] *Inżynieria wojskowa problemy i perspektywy*, Z. Kamyk (red.), Wyższa Szkoła Oficerska Wojsk Lądowych, Wojskowy Instytut Techniki Inżynieryjnej, Wrocław 2008; S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011; R. Radziejewski, *Infrastruktura a bezpieczeństwo*, „Zeszyty Naukowe AON" 2013, nr 3 (92); M. Sułek, *Programowanie gospodarczo-obronne*, Bellona, Warszawa 2008; J. Tomaszewski, *Podsystem infrastruktury obronnej*, [w:] *System logistyczny Sił Zbrojnych Rzeczypospolitej Polskiej. Raport 2019*, T. Jałowiec, S. Mitkow, A. Radomyski i in. (red.), Akademia Sztuki Wojennej, Warszawa 2019; A. Tyburska, *Szanse i zagrożenia związane z uodparnianiem infrastruktury krytycznej*, [w:] *Infrastruktura krytyczna w procesie zarządzania w sytuacjach kryzysowych*, A. Gałecki, A. Kurkiewicz, S. Mikołajczak (red.), Poznań 2014.

INSPEKCJA TRANSPORTU DROGOWEGO – wyspecjalizowana, umundurowana i uzbrojona formacja kontrolna, powołana na mocy Ustawy z dnia 6 września 2001 r. o transporcie drogowym. Do podstawowych zadań Inspekcji Transportu Drogowego (ITD) należy m.in. kontrola i zapewnienie przestrzegania odpowiednich przepisów prawnych.

Transport drogowy jest jedną z najbardziej dynamicznie rozwijających się gałęzi gospodarki narodowej, przynosząc nie tylko zyski przedsiębiorcom, ale także wymierne korzyści dla budżetu państwa. → B e z p i e c z e ń s t w o [t. 1] w transporcie drogowym stanowi jeden z największych problemów współczesnej motoryzacji. Zapewnienie bezpieczeństwa w transporcie drogowym obejmuje przewóz osób, rzeczy oraz wszystkich uczestników ruchu drogowego. Jego skuteczność zależy od: środków transportu, uczestników ruchu drogowego, ruchu drogowego i przewożonych ładunków. Należy zaznaczyć, że transport drogowy (samochodowy) jest najczęściej wykorzystywaną gałęzią transportu w przewozach towarów. W porównaniu z innymi rodzajami transportu charakteryzuje się on cechami, które decydują o jego popularności: bezpośredniość przewozów, relatywnie duża szybkość przewozów, zdolność przewozów różnych towarów, duża dostępność środków transportowych, relatywna taniość

przewozów, krótkie i średnie odległości, niezawodność obsługi. Oprócz wielu pozytywnych aspektów transport drogowy wykazuje jednak tendencje do stałego obniżania kosztów transportu, co często odbywa się kosztem naruszania przepisów prawnych, zasad bezpieczeństwa i formalnych wymogów transportu.

W celu zapewnienia prawidłowości wykonywania transportu drogowego niezbędne było utworzenie instytucji kontrolnej, która działałaby w tym obszarze. ITD kieruje Główny Inspektor Transportu Drogowego jako centralny organ administracji rządowej, podległy ministrowi właściwemu do spraw transportu. Jest to wyspecjalizowana, umundurowana i uzbrojona formacja, której celem jest zapewnienie uczciwej konkurencji w ramach wykonywania transportu drogowego, polepszenie bezpieczeństwa w ruchu i ochrona środowiska. Utworzenie ITD było także realizacją jednego z wymagań akcesyjnych Unii Europejskiej. W jej utworzeniu pomagali specjaliści z Francji i Niemiec w ramach wykonanego w 2001 r. unijnego projektu współpracy bliźniaczej PHARE PL 9908.01 – „Przygotowanie podstaw prawnych i utworzenie Inspekcji Transportu Drogowego". Eksperci z tych 2 państw pomagali w stworzeniu struktury i prawnych podstaw funkcjonowania ITD. Dzięki ich wsparciu stworzono, na wzór istniejących w krajach UE bliźniaczych instytucji kontrolnych (m.in. niemieckiego BAG), strukturę ITD, określono jej kompetencje i szczegółowy zakres zadań. Eksperci pomagali też w szkoleniu kadry nowo powstającej instytucji. ITD zaczęła działania kontrolne na polskich drogach w dniu 1 października 2020 r.

Jej główne zadania zostały określone w art. 50 ustawy o transporcie drogowym. Należy do nich kontrola przestrzegania obowiązków lub warunków przewozu drogowego wskazanych w ustawie o transporcie drogowym, ale ITD także realizuje wiele zadań wynikających z innych przepisów prawa krajowego i dyrektyw unijnych regulujących transport osób i towarów. Do głównych zadań ITD należy kontrola: dokumentów związanych z wykonywaniem transportu drogowego lub przewozów na potrzeby własne oraz przestrzegania warunków w nich określonych; dokumentów przewozowych związanych z wykonywaniem krajowego i międzynarodowego transportu drogowego oraz niezarobkowego krajowego i międzynarodowego przewozu drogowego; przestrzegania przepisów

ruchu drogowego w zakresie krajowego i międzynarodowego transportu drogowego oraz niezarobkowego krajowego i międzynarodowego przewozu drogowego, w tym stanu technicznego pojazdów; przestrzegania przepisów dotyczących okresów prowadzenia pojazdu i obowiązkowych przerw oraz czasu odpoczynku kierowcy; przestrzegania szczegółowych zasad i warunków transportu zwierząt; przestrzegania zasad i warunków dotyczących przewozu drogowego towarów niebezpiecznych. Inne zadania to prowadzenie postępowań administracyjnych, w tym wydawanie decyzji administracyjnych na zasadach określonych w ustawie, a także podejmowanie innych czynności w niej przewidzianych. Inspekcja jest powołana także do kontroli przestrzegania przepisów socjalnych związanych z wykonywaniem transportu drogowego, poboru i prawidłowości uiszczenia opłaty elektronicznej za korzystanie z dróg i autostrad, kontroli rodzaju używanego paliwa, dokumentów związanych z wykonywaniem publicznego transportu zbiorowego, przestrzegania ustalonych cen za przewozy taksówkami, podejmowania czynności dotyczących zezwoleń zagranicznych i zezwoleń ministra właściwego do spraw transportu; wykonywania zadań związanych z monitorowaniem drogowego i kolejowego przewozu towarów oraz obrotu paliwami opałowymi, przestrzegania prawidłowości przewozu odpadów.

W celu realizacji ustawowych zadań inspektorzy ITD mają prawo do: wstępu do pojazdu; kontroli dokumentów; kontroli karty kierowcy i karty przedsiębiorstwa; kontroli zainstalowanych lub znajdujących się w pojeździe urządzeń pomiarowo-kontrolnych i tachografu; kontroli używanego w pojeździe urządzenia do elektronicznego poboru opłat drogowych; kontrolowania masy, nacisków osi i wymiarów pojazdu przy użyciu przyrządu pomiarowego; żądania od podmiotu wykonującego przewóz drogowy i jego pracowników pisemnych lub ustnych wyjaśnień, okazania dokumentów i innych nośników → i n f o r m a c j i oraz udostępnienia wszelkich danych mających związek z przedmiotem kontroli; wstępu na teren podmiotu wykonującego przewóz drogowy, w tym do pomieszczeń lub lokali, gdzie prowadzi on działalność lub przechowuje dokumenty.

W zakresie kontroli ruchu drogowego inspektorzy mają szerokie uprawnienia kontrolne, analogiczne do tych przysługujących policjantom.

Funkcjonariusze ITD, na podstawie art. 129 ust. 2 ustawy – Prawo o ruchu drogowym, są uprawnieni przede wszystkim do legitymowania osób i wydawania im wiążących poleceń, sprawdzania dokumentów, badania stanu trzeźwości kierowców i stanu technicznego pojazdów, sprawdzania zapisów urządzeń rejestrujących prędkość jazdy, czasu pracy i obowiązkowego odpoczynku kierowcy. Mają prawo do zatrzymywania w uzasadnionych przypadkach dokumentów, używania przyrządów kontrolno-pomiarowych, kontroli przewozów materiałów niebezpiecznych, występowania z wnioskiem o ocenę stanu zdrowia kierowcy i pilotowania określonych grup pojazdów. Inspektorom przysługuje prawo do kierowania ruchem drogowym. Należy podkreślić, że ITD ma także uprawnienia do kontroli samochodów osobowych w sytuacji, gdy inspektor stwierdzi rażące naruszenie przepisów ruchu drogowego lub spowodowanie → z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4].

Organami ITD są Główny Inspektor Transportu Drogowego (GITD) oraz wojewoda działający za pośrednictwem Wojewódzkiego Inspektora Transportu Drogowego. Główny Inspektor Transportu Drogowego ma kompetencje ministra infrastruktury w zakresie wydawania uprawnień (licencji, zezwoleń i zaświadczeń oraz świadectw kierowcy) w międzynarodowym transporcie drogowym. Organizację Głównego Inspektoratu Transportu Drogowego (GITD) określa statut nadany przez Prezesa Rady Ministrów, Zarządzeniem nr 92 Prezesa Rady Ministrów z dnia 26 października 2012 r. w sprawie nadania statutu Głównemu Inspektoratowi Transportu Drogowego. W strukturze jako komórki organizacyjne GITD wyszczególniono m.in. Biuro Elektronicznego Poboru Opłat; Biuro Nadzoru Inspekcyjnego; Biuro do spraw Transportu Międzynarodowego; Biuro Prawne; Biuro Spraw Wewnętrznych. W strukturze GITD wyodrębniono także Centrum Automatycznego Nadzoru nad Ruchem Drogowym jako jednostkę organizacyjną zarządzającą systemem ujawniania naruszeń przepisów ruchu drogowego związanych z przekraczaniem dopuszczalnej prędkości (za pomocą fotoradarów oraz odcinkowych i mobilnych pomiarów prędkości) oraz niestosowania się do sygnałów świetlnych, które to uprawnienia zostały kompetencyjnie przyznane ITD na podstawie przepisów prawa o ruchu drogowym (art. 129 g; art. 129 h).

W ramach struktury GITD funkcjonuje także 10 delegatur terenowych:

- Delegatura Północno-Zachodnia (obejmująca swoim zasięgiem obszary województw zachodniopomorskiego oraz lubuskiego bez powiatów: wschowskiego, żagańskiego, żarskiego);
- Delegatura Południowo-Zachodnia (województwo dolnośląskie oraz powiaty: wschowski, żagański, żarski);
- Delegatura Śląska (województwo śląskie oraz opolskie);
- Delegatura Południowa (województwo małopolskie i świętokrzyskie);
- Delegatura Północna (województwo kujawsko-pomorskie, pomorskie oraz powiaty: braniewski, elbląski i miasto Elbląg, ostródzki, iławski, nowomiejski, działdowski, nidzicki, ciechanowski, mławski, sierpecki, żuromiński);
- Delegatura Wielkopolska (województwo wielkopolskie);
- Delegatura Centralna (województwa łódzkie oraz mazowieckie bez powiatów: ciechanowskiego, mławskiego, sierpeckiego, żuromińskiego, przasnyskiego, makowskiego, ostrołęckiego i miasta Ostrołęki, ostrowskiego, węgrowskiego, sokołowskiego, łosickiego, siedleckiego i miasta Siedlce, mińskiego, garwolińskiego);
- Delegatura Północno-Wschodnia (województwo podlaskie bez powiatu siemiatyckiego oraz obszar województwa warmińsko-mazurskiego bez powiatów: braniewskiego, elbląskiego i miasta Elbląg, ostródzkiego, iławskiego, nowomiejskiego, działdowskiego, nidzickiego oraz powiaty: przasnyski, makowski, ostrołęcki i miasto Ostrołęka, ostrowski);
- Delegatura Wschodnia (województwo lubelskie bez powiatów: kraśnickiego, janowskiego, biłgorajskiego oraz powiaty: siemiatycki, łosicki, siedlecki i miasto Siedlce, garwoliński, węgrowski, sokołowski, miński);
- Delegatura Południowo-Wschodnia (województwo podkarpackie oraz powiaty: kraśnicki, janowski, biłgorajski).

Głównym zadaniem delegatur jest realizowanie zadań związanych z poborem opłat oraz uprawnieniami w zakresie przestrzegania przepisów prawa o ruchu drogowym (przekraczaniem dopuszczalnej prędkości oraz

niestosowaniem się do sygnałów świetlnych), w tym z obsługą i utrzymaniem urządzeń kontrolnych.

Na terenie każdego województw zadania kontrolne realizuje wojewoda działający za pośrednictwem Wojewódzkiego Inspektora Transportu Drogowego, jako kierownika Wojewódzkiego Inspektoratu Transportu Drogowego wchodzącego w skład wojewódzkiej administracji zespolonej. Wojewódzkie Inspektoraty Transportu Drogowego na terenie danego województwa realizują zadania kontrolne w zakresie szeroko pojętego transportu drogowego.

Krzysztof Dymura

P. Grabowski, *Kontrola ruchu drogowego jako element bezpieczeństwa na drogach*, „Kwartalnik Policyjny" 2017, nr 2; GITD.gov.pl (dostęp 22.01.2020); Krakow.witd.gov.pl (dostęp 22.01.2020); F. Odważny, A. Stasiuk-Piekarska, M. Drzewiecka, *Czynniki ryzyka w transporcie*, „Logistyka" 2014, nr 4; I. Pisz, I. Łapunka, A. Pakulska, *Działania Inspekcji Transportu Drogowego w celu eliminowania zagrożeń w transporcie drogowym*, „Logistyka" 2014, nr 6; D. Starkowski, K. Bieńczak, W. Zwierzycki, *Samochodowy transport krajowy i międzynarodowy. Kompendium wiedzy praktycznej. Zabezpieczenia ładunków oraz zagadnienia techniczno-eksploatacyjne w transporcie drogowym*, Wydawnictwo Systherm, Poznań 2010; M. Sudowski, B. Mrugalska, *Zapewnienie bezpieczeństwa transportu drogowego a manipulacje czasem pracy kierowców zawodowych*, „Zeszyty Naukowe Politechniki Poznańskiej" 2017, nr 73; Ustawa z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt, Dz. U. 2018, poz. 1967; Ustawa z dnia 14 grudnia 2012 r. o odpadach, Dz. U. 2019, poz. 701, 730, 1403 i 1579; Ustawa z dnia 15 listopada 1984 r. – Prawo przewozowe, Dz. U. 1984, nr 53, poz. 272; Ustawa z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym, Dz. U. 2018, poz. 2016 i 2435 oraz z 2019 r. poz. 730, 1495 i 1696; Ustawa z dnia 16 kwietnia 2004 r. o czasie pracy kierowców, Dz. U. 2019, poz. 1412 z późn. zm.; Ustawa z dnia 19 sierpnia 2011 r. o przewozie towarów niebezpiecznych, Dz. U. 2019, poz. 382, 534, 730 i 1123; Ustawa z dnia 21 marca 1985 r. o drogach publicznych, Dz. U. 1985, nr 14, poz. 60 z późn. zm.; Ustawa z dnia 21 sierpnia 1997 r. o ochronie zwierząt, Dz. U. 2019, poz. 122 i 1123; Ustawa z dnia 27 października 1994 r. o autostradach płatnych oraz o Krajowym Funduszu Drogowym, Dz. U. 2018, poz. 2014 i 2244 oraz z 2019 r. poz. 730 i 1123; Ustawa z dnia 29 czerwca 2007 r. o międzynarodowym przemieszczaniu odpadów, Dz. U. 2019, poz. 1162; Ustawa z dnia 5 lipca 2018 r. o tachografach, Dz. U. 2018, poz. 1480 oraz z 2019 r.

poz. 1123; Ustawa z dnia 6 września 2001 r. o transporcie drogowym, Dz. U. 2001, nr 125, poz. 1371 z późn. zm.; Ustawa z dnia 9 marca 2017 r. o systemie monitorowania drogowego i kolejowego przewozu towarów oraz obrotu paliwami opałowymi, Dz. U. 2018, poz. 2332 oraz z 2019 r. poz. 730, 1123 i 1556; Rozporządzenie wykonawcze Komisji (UE) 2016/799 z dnia 18 marca 2016 r. w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 165/2014 ustanawiającego wymogi dotyczące budowy, sprawdzania, instalacji, użytkowania i naprawy tachografów oraz ich elementów składowych, Dz. Urz. UE L 139 z 26.05.2016 z późn. zm.; Rozporządzenie wykonawcze Komisji (UE) 2017/548 z dnia 23 marca 2017 r. ustanawiające standardowy formularz pisemnego oświadczenia w sprawie usunięcia lub naruszenia plomby tachografu, Dz. Urz. UE L 79 z 24.03.2017; Decyzja Komisji nr 2007/230/WE z dnia 12 kwietnia 2007 r. w sprawie formularza dotyczącego przepisów socjalnych odnoszących się do działalności w transporcie drogowym, Dz. Urz. UE L 99 z 14.04.2007 z późn. zm.; Zarządzenie nr 92 Prezesa Rady Ministrów z dnia 26 października 2012 r. w sprawie nadania statutu Głównemu Inspektoratowi Transportu Drogowego (M.P. 2012 poz. 820); Zarządzenie nr 13 Prezesa Rady Ministrów z dnia 31 stycznia 2018 r. zmieniające zarządzenie w sprawie nadania statutu Głównemu Inspektoratowi Transportu Drogowego (M.P. 2018 poz. 150); Zarządzenie nr 179 Prezesa Rady Ministrów z dnia 7 października 2019 r. zmieniające zarządzenie w sprawie nadania statutu Głównemu Inspektoratowi Transportu Drogowego (M.P. 2019 poz. 1011); Rozporządzenie Rady (WE) nr 1/2005 z dnia 22 grudnia 2004 r. w sprawie ochrony zwierząt podczas transportu i związanych z tym działań oraz zmieniającego dyrektywy 64/432/EWG i 93/119/WE oraz rozporządzenie (WE) nr 1255/97, Dz. Urz. UE L 3 z 05.01.2005 z późn. zm.

INTEGRITY INITIATIVE (Inicjatywa na rzecz Uczciwości) – brytyjski program, partnerstwo kilku niezależnych instytucji kierowanych przez Institute for Statecraft, skupiający się na →przeciwdziałaniu dezinformacji i propagandzie [t. 3] ze strony Kremla i walce z nimi, mający na celu zwrócenie uwagi na →zagrożenie [t. 4] zachodnich demokracji ze strony Rosji; tajna organizacja informacyjna, w której biorą udział politycy, wojskowi i dziennikarze, zarządzana przez centrum analityczne w Londynie, które zajmuje się przeciwdziałaniem rosyjskiej →propagandzie [t. 3] i →wojnie hybrydowej [t. 4] Kremla. Inicjatywa na rzecz Uczciwości została uruchomiona jesienią 2015 r. przez Institute for Statecraft we współpracy z Wolnym Uniwersytetem Brukselskim, aby

zwrócić uwagę polityków, decydentów, liderów opinii i innych zainteresowanych stron na zagrożenie, jakie Rosja stwarza dla demokracji; działa jako środek zwalczania fałszywych wiadomości rozpowszechnianych z kont → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3] powiązanych z rosyjskim rządem. Deklarowanym celem programu było przeciwdziałanie → d e z i n f o r m a c j i i innym formom manipulacji, prowadzonym przez państwa i podmioty subpaństwowe, które próbują ingerować w procesy demokratyczne i zniszczyć zaufanie publiczne do krajowych instytucji politycznych, a także dostarczanie wiarygodnych → i n f o r m a c j i społeczeństwu, w tym w jęz. rosyjskim.

Projekt jest prowadzony przez społeczność dziennikarską, celem której jest weryfikacja informacji, wzrost wiedzy o mediach wśród społeczeństwa i walka o oddzielenie dziennikarstwa od propagandy; fachowców, którzy weryfikują fakty, redagują informacje, tłumaczą i rozpowszechniają je w różnych językach. Projekt przewiduje stworzenie klastrów ekspertów z różnych dziedzin, mających na celu śledzenie i analizowanie przykładów dezinformacji w różnych krajach.

Domena IntegrityInitiative.net została zarejestrowana po raz pierwszy 22 czerwca 2015 r. Projekt jest prowadzony przez Institute for Statecraft, który jest z kolei finansowany niemal wyłącznie przez rząd Wielkiej Brytanii. Ponadto jest on bezpośrednio połączony z brytyjskim → k o n t r w y w i a d e m i służbą bezpieczeństwa brytyjskiej MI5. Dyrektorem instytutu od 2010 r. i założycielem programu Integrity Initiative jest C.N. Donnelly, hasłem przewodnim organizacji jest „Obroń demokrację przed dezinformacją". Integrity Initiative robi to poprzez obalenie rosyjskiej dezinformacji dzięki pracy dziennikarzy w całej Europie i Stanach Zjednoczonych. Zarówno Instytut, jak i Inicjatywa twierdzą, że są niezależnymi organizacjami pozarządowymi. Obie są finansowane przez rząd brytyjski, → N A T O [t. 3] i innych darczyńców państwowych. Integrity Initiative to organizacja charytatywna finansowana przez Ministerstwo Spraw Zagranicznych, Armię Brytyjską i Ministerstwo Spraw Wewnętrznych Wielkiej Brytanii.

Institute for Statecraft oraz Integrity Initiative podkreślają, że rzeczywistością rosyjskiej doktryny nuklearnej jest to, że ona się nie wycofa, i wymieniają swoje 3 najważniejsze cele:

- Stworzenie różnych narodowych grup w rządach, wojsku, mediach i środowiskach akademickich, by koordynować działania przeciwdziałające propagandzie Kremla. Przykładem jest wyciszenie głosów prokremlowskich w serbskiej telewizji przez serbskiego analityka politycznego i dyrektora Centrum Studiów Euroatlantyckich J. Milica.
- Poszerzanie wiedzy; wykorzystanie istniejącej wiedzy fachowej; utworzenie sieci ekspertów, podmiotów opiniotwórczych i decydentów politycznych w celu edukowania krajowych grup docelowych w zakresie zagrożenia i pomocy w budowaniu zdolności krajowych w zakresie przeciwdziałania temu zagrożeniu; oświecenie społeczeństwa (przez rządy, ośrodki analityczne, wojsko, mass media), jakimi sposobami Kreml manipuluje i prowadzi → wojnę informacyjną [t. 4] i hybrydową.
- Zwiększenie szybkości reakcji, mobilizowanie sieci do tworzenia popularnych kampanii i niezależnych artykułów informacyjnych, które odkryją rosyjską dezinformację.

Postawione cele osiągają, nie tylko ujawniając i prostując fake newsy, ale także tworząc archiwum propagandy, analizując informacje, prowadząc szkolenia z weryfikacji informacji dla różnych grup, biorąc udział w tematycznych konferencjach i seminariach.

W kwietniu 2016 r. został uruchomiony nowy 4-letni program strategicznej komunikacji i rozwoju mediów, zatwierdzony przez Narodową Radę Bezpieczeństwa Wielkiej Brytanii, zwany Programem Przeciwdziałania Dezinformacji i Rozwoju Mediów. Program bada wpływ propagandy i dezinformacji na różne państwa – od krajów dawnego Związku Radzieckiego, przez Unię Europejską po Syrię i Turcję. Zadeklarowanym celem projektu jest informacyjne przeciwdziałanie Federacji Rosyjskiej.

O istnieniu Integrity Initiative świat usłyszał 5 i 29 listopada 2018 r., kiedy grupa → hakerów z Anonymous opublikowała dokumenty projektu Integrity Initiative, które Wielka Brytania mogła wykorzystać do prowadzenia wojny informacyjnej przeciwko Rosji. Z projektem ściśle współpracowali finansista B. Browder, a także W. Aszurkow, który jest współpracownikiem A. Nawalnego i I. Sutiagina – rosyjskich specjalistów ds. kontroli zbrojeń i → broni nuklearnej [t. 1], skazany w 2004 r.

za szpiegostwo na korzyść Wielkiej Brytanii i wymieniony w 2010 r. na szpiegów rosyjskich. Jak wynika z opublikowanych przez hakerów dokumentów, koszty związane z prowadzeniem projektu za rok finansowy oceniane są na 1,96 mln GPB (2,51 mln USD). Finansowanie pochodzi ze środków NATO, Departamentu Stanu USA, niemieckiej społeczności biznesowej, litewskiego Ministerstwa Obrony, amerykańskiego think tanku Smith Richardson Foundation i innych instytucji partnerskich.

Z opublikowanych dokumentów wynika, że projekt już działa we Francji, Grecji, Niemczech, Włoszech, na Litwie, w Czarnogórze, Holandii, Norwegii, Serbii i Hiszpanii. Planowane jest otwarcie w najbliższej przyszłości regionalnych biur w Armenii, Austrii, Belgii, Bułgarii, na Cyprze, w Danii, Finlandii, Islandii, Gruzji, Estonii, Kanadzie, Łotwie, Malcie, Mołdawii, Polsce, Portugalii, Rumunii, Republice Czeskiej, Słowacji, Szwajcarii, Szwecji, Turcji, Ukrainie, Stanach Zjednoczonych, na Węgrzech, na Bliskim Wschodzie i w Afryce Północnej.

Minister spraw zagranicznych Wielkiej Brytanii A. Duncan, odpowiadając na pytania parlamentarzystów o działalność Integrity Initiative w listopadzie 2018 r., wyszczególnił Rosję jako wroga numer jeden dla brytyjskiego → b e z p i e c z e ń s t w a [t. 1]. Wezwał do → s t r a t e g i i [t. 4] przeciwwagi dla Kremla, który wykorzystuje wszystkie możliwości: od ekonomicznych poprzez nowoczesne zasoby wojskowe, po szerszy wpływ dyplomatyczny i kulturowy na arenie światowej, dążąc do globalnych wpływów. Najistotniejszym celem Integrity Initiative jest przeciwdziałanie → R T [t. 3] (początkowo – Russia Today), która stoi na czele dezinformacji w Europie Zachodniej, w tym w Wielkiej Brytanii.

Integrity Initiative uczestniczy w skoordynowanej antyrosyjskiej ofensywie w krajach Europy Wschodniej: Ukraina, państwa bałtyckie, Mołdawia i Armenia są uważane za kluczowe obszary współpracy w przeciwdziałaniu rosyjskiej dezinformacji. Jednym z jego kluczowych partnerów w Ukrainie jest organizacja Stopfake, która została uruchomiona 2 marca 2014 r., głównym zadaniem której jest walka z nieprawdziwymi informacjami. Program umożliwia także litewskiemu zespołowi regularne przeprowadzanie szkoleń dla wszystkich chętnych dot. metodologii śledzenia i ujawniania rosyjskich wpływów i dezinformacji oraz wymianę praktycznych doświadczeń.

Integrity Initiative uważa, że istnieje potrzeba edukowania europejskiej publiczności, aby zrozumieć, w jaki sposób Rosja manipuluje i dezinformuje, prowadząc wojnę informacyjną w państwach zachodnich, podkreślając, że → a g r e s j a [t. 1] jest nieodłącznym elementem rosyjskiej polityki.

Po opublikowaniu przez grupę Anonymous dokumentów Integrity Initiative, skierowanych przeciwko Rosji jako największemu zagrożeniu dla pokoju na świecie, państwu, które według instytucji najprawdopodobniej może zdecydować się na użycie broni jądrowej, organizacja wyczyściła swoją witrynę i zablokowała konto na Twitterze w oczekiwaniu na dochodzenie w sprawie kradzieży danych.

Osoby zaangażowane w projekt Integrity Initiative oświadczyły, że część materiałów opublikowanych przez Anonymous oraz baza źródłowa informacji utraciły już aktualność albo nigdy nie były wykorzystywane, magazynowane były tylko jako potencjalnie przydatne. Wyniki wskazują, że kradzież była częścią kampanii mającej na celu podważenie pracy Inicjatywy na rzecz Uczciwości w badaniu, nagłaśnianiu i zwalczaniu zagrożenia dla europejskich demokracji przed dezinformacją i innymi formami wojny hybrydowej.

Po ataku hakerów uczestnicy projektu podtrzymują kontakt ze wszystkimi zaangażowanymi w działanie programu, także partnerami międzynarodowymi i władzami krajowymi, ale informacje o poszczególnych zadaniach w ramach programu nie są publikowane, ponieważ informacje te mogą zostać wykorzystane do aktywnej próby zakłócenia i osłabienia jego skuteczności.

Olga Wasiuta

Cyber Guerilla, *Institute for Statecraft: Integrity Initiative Part 3*, 15.12.2018, WilliamBowles.com (dostęp 12.02.2019); M. Elmaazi, M. Blumenthal, *The Integrity Initiative and the UK's Scandalous Information War*, The Carefully, 18.12.2018, MintPresNews.com (dostęp 16.03.2019); T. Hayward, *Integrity: Grasping The Initiative*, 15.12.2018, TimHayward.wordpress.com (dostęp 16.03.2019); *Integrity Initiative is the Biggest Story of 2018 – But Not Because of Anything It Did*, 23.12.2018, RT.com (dostęp 16.03.2019); D. Jamieson, *State-Backed Integrity Initiative Confirms Meeting with Herald Journalist for Scotland Briefing*, 19.12.2018, CommonSpace.com

(dostęp 16.03.2019); Moon of Alabama, *The „Integrity Initiative" – A Military Intelligence Operation, Disguised as Charity, to Create The „Russian Threat"*, 16.12.2018, WilliamBowles.info (dostęp 16.03.2019); T. Scripps, *Britain's Secret Propaganda „Integrity Initiative" Targets Russia*, 4.02.2019, WSW.org (dostęp 16.03.2019); TruNews Team, *Anonymous Hacktivists Release Secret UK Integrity Initiative Project Docs*, 14.12.2018, TruNews.com (dostęp 16.03.2019); O. Wasiuta, *Integrity Initiative*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

INTERESY NARODOWE (ang. *national interests*) – pojęcie z pogranicza →nauk o bezpieczeństwie [t. 3] i nauk o polityce. Współcześnie można spotkać się z dwojakim rozumieniem tego terminu: po pierwsze – interesy narodowe są kategorią charakterystyczną dla stosunków międzypaństwowych, która wiąże się z decyzjami podejmowanymi przez mężów stanu, wziąwszy pod uwagę motywy ich podjęcia (poglądy ideologiczne, interes jednostkowy, interes określonej grupy, ambicje dynastyczne, dobro obywateli, →bezpieczeństwo [t. 1] państwa); po drugie – interesy narodowe są rodzajem dyskursu politycznego prowadzonego przez elity zarządzające państwem i uzasadniającego ich działania odwoływaniem się do kategorii, mającego normatywny charakter, interesu narodowego. Analiza znaczenia terminu uwidacznia znaczną przewagę treści państwowo-politycznych nad narodowym wymiarem postrzegania tegoż interesu. Dlatego też rozdział na →rację stanu [t. 3] i interes narodowy (częstokroć w literaturze przedmiotu oraz dyskursie publicznym stosowane zamiennie) wydaje się stosowny, jeśli nie konieczny.

J. Wiatr definiuje interes narodowy jako posiadanie własnego państwa, które mając możliwość decydowania o własnym losie, jest zdolne do zapewnienia bezpieczeństwa własnym obywatelom (narodowi) na terytorium przez nich zamieszkałym. Można zatem mówić o interesie narodowym w kontekście publicznego (wspólnotowego) wymiaru oraz jego sfery prywatnej (indywidualnej). Interesy narodowe mogą być obiektywne lub subiektywne. Wreszcie, interes narodowy traktuje się jako zdefiniowanie pewnej potrzeby, określenie preferencji, skłonność do realizacji dążenia lub próbę ochrony określonej wartości, którą może być wolność, własność, prawda czy sprawiedliwość. Nierzadko też interes narodowy bywa rozumiany w kategorii interesu politycznego. Interes polityczny

w leksykalnym ujęciu jawi się jako wyrażanie zainteresowania dążeniem do osiągnięcia określonego celu abstrakcyjnego lub materialnego. Jednak pomimo tego, że obiektami wspomnianego pragnienia winny być przede wszystkim m.in. wolność czy równowaga społeczna, to w praktyce zazwyczaj chodzi o wyartykułowanie, wyrażanie oraz proces realizacji zamiarów i dążeń politycznych tych grup, które są zinstytucjonalizowane i mają bezpośredni wpływ na charakter i kierunek zmian zachodzących w państwie. Fakt posiadania sprecyzowanych i zindywidualizowanych interesów narodowych często przesądza o konflikcie interesów określonych frakcji w ramach danego państwa lub konflikcie interesów pomiędzy dwoma (lub więcej) uczestnikami stosunków międzynarodowych.

Dążenie do realizacji interesów narodowych może mieć zarówno partykularny, jak i uniwersalny charakter. Uniwersalizm interesów narodowych nie wynika jedynie z potrzeb definicyjnych bezpieczeństwa narodowego, stanowiącego zorganizowaną obronę państwa i ochronę obywateli przed szkodliwym działaniem czynników wewnętrznych i zewnętrznych, ale z różnorodności jego składowych. Otóż obok interesów militarnych, ekonomicznych, społecznych i politycznych oraz określonych uwarunkowań bezpieczeństwa wymienia się choćby interesy kulturowe – świadczące od możliwości utrwalania i pielęgnowania wartości, które decydują o tożsamości narodowej, oraz czerpania z doświadczeń nie tylko własnych, ale także z osiągnięć innych narodów. Wspomniane wartości, z którymi wiążą się interesy narodowe (i z których wynikają) zapisane są w Konstytucji Rzeczypospolitej Polskiej, należą do nich: niepodległość, nienaruszalność terytorialna, wolność, → prawa człowieka [t. 3] i obywatela, bezpieczeństwo obywateli, dziedzictwo narodowe, ochrona środowiska naturalnego oraz zasada → zrównoważonego rozwoju [t. 4].

W kontekście bezpieczeństwa swoisty uniwersalizm interesów narodowych znajduje odzwierciedlenie w Konstytucji Rzeczypospolitej Polskiej oraz w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (SBN RP z 2007 r. w sposób najbardziej systematyczny wyszczególnia katalog interesów narodowych). Zakres interesów narodowych wyartykułowany we wspomnianej → strategii [t. 4] podzielony został na 3 kategorie: interesy żywotne, interesy ważne oraz interesy istotne. Interesy żywotne wiążą się z przetrwaniem państwa i jego obywateli, a odnoszą

się w sposób bezpośredni do wartości: zachowania niepodległości i →suwerenności państwa [t. 4], ochrony integralności terytorialnej i nienaruszalności granic, zapewnienia bezpieczeństwa obywateli i ich podstawowych praw i wolności oraz umacniania demokratycznego porządku politycznego. Interesy te stanowią fundament polskiej polityki bezpieczeństwa. Interesy ważne to wedle strategicznego dokumentu: trwały i zrównoważony rozwój cywilizacyjny i gospodarczy, stworzenie warunków do wzrostu dobrobytu społeczeństwa, rozwoju nauki i techniki, ochrony dziedzictwa narodowego, tożsamości narodowej oraz środowiska naturalnego. Zaś w kategorii interesów istotnych można odnaleźć: umacnianie działania instytucji międzynarodowych, których członkiem jest Polska, rozwój stosunków międzynarodowych z poszanowaniem prawa, celów i zasad określonych w Karcie Narodów Zjednoczonych.

Natomiast w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2014 r. interesy narodowe przedstawiono jako fundament pod konstruowanie celów strategicznych w dziedzinie bezpieczeństwa. Wyszczególniono następujące interesy narodowe: dysponowanie skutecznym narodowym potencjałem bezpieczeństwa zapewniającym gotowość i zdolność do zapobiegania →zagrożeniom [t. 4], w tym →odstraszania [t. 3], obrony i ochrony przed nimi oraz likwidowania ich następstw; silna pozycja międzynarodowa Polski i członkostwo w wiarygodnych systemach bezpieczeństwa międzynarodowego; ochrona indywidualna i zbiorowa obywateli przed zagrożeniami dla ich życia i zdrowia oraz przed naruszeniem, utratą lub degradacją istotnych dla nich dóbr (materialnych i niematerialnych); zapewnienie swobody korzystania przez obywateli z wolności i praw, bez szkody dla bezpieczeństwa innych osób i bezpieczeństwa państwa, oraz zapewnienie tożsamości narodowej i dziedzictwa kulturowego; zapewnienie trwałego i zrównoważonego rozwoju potencjału społecznego i gospodarczego państwa, ze szczególnym uwzględnieniem ochrony środowiska naturalnego oraz warunków życia i zdrowia ludności jako podstawy bytowania.

Paweł Łubiński

P. Łubiński, *Interesy narodowe*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Komunikacyjny*

kontekst bezpieczeństwa. Interes narodowy w przekazie medialnym Ruchu Narodowego, [w:] *Bezpieczeństwo współczesnego świata. Historia, wyzwania, konflikty zbrojne*, J. Karwat (red.), Wydawnictwo Wyższej Szkoły Handlu i Usług, Poznań 2014; G. Łukomski, *Polityczna przestrzeń polskości w XX w. Bezpieczeństwo polityczne Rzeczypospolitej z perspektywy racji stanu*, Wydawnictwo Naukowe Silva Rerum, Poznań–Londyn 2013; W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, AON, Warszawa 2011; J. Kranz, *Jak rozumieć suwerenność? Próba opisu*, [w:] *Suwerenność państwa i jej granice*, S. Sowiński, J. Węgrzecki (red.), Wydawnictwo Uniwersytetu Kardynała Stefana Wyszyńskiego, Warszawa 2010; S. Musiał, *Strategie bezpieczeństwa i obronności Rzeczypospolitej Polskiej po 1989 roku*, [w:] *Unia Europejska a bezpieczeństwo Polski*, M.J. Malinowski, S. Musiał (red.), Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2011; J. Sadłocha, *Krytyczna analiza kategorii interesu w teorii stosunków międzynarodowych*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2015; J. Skrzyp, *Racja stanu, interesy narodowe i cele strategiczne jako podstawowe składniki bezpieczeństwa narodowego (państwa)*, [w:] *Podstawy bezpieczeństwa narodowego (państwa). Podręcznik akademicki*, J. Pawłowski (red.), Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2017; *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2007; *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego Warszawa 2014; J.J. Wiatr, *Polski interes narodowy: refleksje o historii i współczesności*, Wydawnictwo Instytutu Filozofii i Socjologii Polskiej Akademii Nauk, Warszawa 2012; tenże, *Refleksje o polskim interesie narodowym*, Wydawnictwo Instytutu Filozofii i Socjologii Polskiej Akademii Nauk, Warszawa 2004.

INTERNOWANIE – przymusowe umieszczenie określonych osób w wyznaczonym miejscu pobytu, bez prawa jego opuszczania. Internowanie jest środkiem pozbawienia wolności zarządzanym przez władze wykonawcze, gdy nie ma podstaw do przedstawienia danej osobie zarzutów karnych, ale istnieje powód, związany np. z wcześniejszą działalnością polityczną, uzasadniający ograniczenie wolności tej osoby. Internowanie jest zatem jedną z form pozasądowego, a jednocześnie legalnego – z punktu widzenia prawa międzynarodowego – pozbawienia wolności osób cywilnych w czasie konfliktu zbrojnego. Według interpretacji definicji pojęcia „internowanie", dokonanej przez Międzynarodowy Komitet Czerwonego Krzyża, internowanie nie jest karą, ale administracyjnym środkiem zapobiegawczym. Internowane mogą zostać tylko osoby, które brały udział w działaniach

zbrojnych i politycznych, a także osoby, co do których istniało przypuszczenie, że gdyby były pozostawione na wolności, to mogłyby przyczynić się do walki zbrojnej lub politycznej

W powszechnej świadomości termin ten wiązany jest z wydarzeniami historycznymi, takimi jak internowanie polskich legionistów przez Niemcy w 1917 r. w obozach w Szczypiornie i Beniaminowie, internowanie prezydenta I. Mościckiego oraz członków polskiego rządu w Rumunii w 1939 r. oraz internowanie działaczy opozycji w czasie stanu wojennego w 1981 r.

Internowanie członków sił zbrojnych walczących stron oraz →ludności cywilnej [t. 3] na terytoriach objętych konfliktem zbrojnym podlega regulacji konwencji wiedeńskich z 1949 r., które jednak nie zawierają definicji pojęcia internowania. Względem internowanych w państwach neutralnych, rannych, chorych, członków personelu sanitarnego oraz duchownego, należących do sił zbrojnych stron pozostających w konflikcie, należy stosować przepisy konwencji o polepszeniu losu rannych i chorych w armiach czynnych oraz konwencji dotyczącej losu rannych, chorych i rozbitków na morzu. Członków sił zbrojnych kraju okupowanego, internowanych przez okupanta, uważa się za jeńców wojennych. Identyczny status przyznaje się, co do zasady, osobom internowanym na terytorium państw neutralnych lub niebiorących udziału w konflikcie, jeżeli zgodnie z prawem międzynarodowym należałby się im status jeńców wojennych, gdyby znaleźli się we władzy nieprzyjaciela.

Internowanie jeńców wojennych zostało szczegółowo uregulowane w III konwencji genewskiej. Określono m.in. zasady przebywania internowanych w odosobnieniu, zwalniania ich na słowo, grupowania jeńców w obozach, wykonywania przez nich praktyk religijnych, odbywania zajęć intelektualnych i rekreacyjnych, posługiwania się stopniami i tytułami wojskowymi, utrzymywania kontaktów ze światem zewnętrznym, a także odpowiedzialności dyscyplinarnej i sądowej internowanych jeńców. Konwencja statuuje minimalne standardy w zakresie warunków, w jakich przebywać mają internowani – regulując kwestię pomieszczeń oddawanych do ich użytku, wyżywienia, odzieży, zasad utrzymania higieny oraz niesienia pomocy medycznej. Gwarantuje im ochronę przed niebezpieczeństwami →wojny [t. 4], takimi jak ostrzeliwanie lub bombardowanie, zastrzegając, że mają prawo korzystać na równi z ludnością

cywilną z odpowiednich pomieszczeń czy schronów. Ponadto internowani jeńcy nie mogą być przetrzymywani ani wysyłani do strefy walk. Określono także zasady, na jakich mogą wykonywać pracę, regulując kwestie wynagrodzenia i wypłaty żołdu.

Konwencja o ochronie osób cywilnych (tzw. IV konwencja genewska) wskazuje internowanie jako najsurowszy środek kontroli, jaki można stosować względem osób podlegających ochronie na podstawie konwencji, który może być stosowany tylko w przypadku, gdy wymaga tego bezwzględnie → b e z p i e c z e ń s t w o [t. 1] państwa, w którego władzy osoby te znajdują się, lub na żądanie osoby internowanej – w przypadku, gdy wymaga tego jej położenie. Decyzja o internowaniu podlega zaskarżeniu przez osobę internowaną do sądu lub do organu kontroli powołanego w tym celu przez państwo dokonujące zatrzymania. W przypadku utrzymania w mocy decyzji o internowaniu sąd albo organ kontrolny mają obowiązek co najmniej 2 razy w roku dokonywać sprawdzenia sytuacji internowanego pod kątem zaistnienia przesłanek do jego zwolnienia. Przesłankami do internowania zgodnie z konwencją są popełnienie przestępstwa w celu zaszkodzenia państwu okupacyjnemu oraz nagłe wymagania bezpieczeństwa. Konwencja reguluje szczegółowo zasady traktowania internowanych cywilów, w tym dotyczące miejsca internowania, zapewnienia im wyżywienia, odzieży, opieki medycznej, dostępu do praktyk religijnych, zajęć intelektualnych i rekreacyjnych, utrzymywania stosunków ze światem zewnętrznym czy odpowiedzialności dyscyplinarnej.

Zasady dotyczące zapewnienia humanitarnych warunków i należytego traktowania zostały uregulowane także w stosunku do ofiar niemiędzynarodowych konfliktów zbrojnych w II protokole dodatkowym do konwencji genewskich.

V konwencja haska reguluje obowiązkowe internowanie wojsk państw walczących na terytorium państwa neutralnego.

Instytucja internowania znana była prawu II Rzeczypospolitej i PRL. W myśl rozporządzeń z mocą ustawy z 1928 r. o stanie wojennym i o stanie wyjątkowym, internowanie przez władze administracji ogólnej bez polecenia władz sądowych było dopuszczalne w stosunku do osób zagrażających bezpieczeństwu państwa lub porządkowi publicznemu, przez okres do 3 miesięcy. Ustawy o stanie wyjątkowym z 1937 r. oraz

o stanie wojennym z 1939 r. utrzymały instytucję internowania w polskim porządku prawnym, przy czym w czasie stanu wyjątkowego było ono dopuszczalne tylko przez okres 3 miesięcy, zaś w czasie stanu wojennego przez czas jego trwania. W dekrecie o stanie wojennym z 1981 r. internowanie zostało przewidziane jako tzw. środek prewencyjny, który mógł być stosowany względem osób, które „pozostając na wolności, nie będą przestrzegać porządku prawnego albo będą prowadzić działalność zagrażającą interesom bezpieczeństwa lub obronności państwa". Ustawa o stanie wyjątkowym z 1983 r. dopuszczała internowanie na czas trwania stanu wyjątkowego. Przesłanki internowania w ustawie były identyczne jak wskazane w dekrecie o stanie wojennym.

W obecnie obowiązującej ustawie o stanie wyjątkowym ujęto możliwość zastosowania odosobnienia wobec osoby, co do której

> zachodzi uzasadnione podejrzenie, że pozostając na wolności, będzie prowadziła działalność zagrażającą konstytucyjnemu ustrojowi państwa, bezpieczeństwu obywateli lub porządkowi publicznemu albo gdy odosobnienie jest niezbędne dla zapobieżenia popełnienia czynu karalnego lub uniemożliwienia ucieczki po jego popełnieniu.

Mimo że internowanie jest stosunkowo łagodnym środkiem ograniczenia wolności, współczesna praktyka stosowania tego środka może budzić wątpliwości. Niejednokrotnie ten administracyjny instrument pozbawienia wolności osób cywilnych stosowany w celach prewencyjnych jest następnie wykorzystywany przez władze okupacyjne jako środek represjonowania. Tytułem przykładu wymienić należy politykę władz niemieckich i radzieckich względem ludności polskiej w czasie II wojny światowej. Przypomnieć jednak trzeba, że po zakończeniu II wojny światowej władze niektórych państw w Europie Środkowo-Wschodniej, w tym Polski, tworzyły obozy i miejsca odosobnienia dla cywilnej ludności niemieckiej. Podstawą internowania były narodowość lub obywatelstwo niemieckie. Współcześnie wskazuje się, internowanie może być jedną z metod represjonowania ludności ze względów etnicznych, czego liczne przykłady przyniosły wojny toczące się na terytorium byłej Jugosławii.

Natomiast przykładem państwa stale utrzymującego obozy internowania przede wszystkim dla własnych obywateli jest Korea Północna.

Anna Pacholska

Encyclopedia of Prisoners of War And Internment, J.F. Vance (ed.), Grey House Publishing, Millerton 2006; Konwencje o ochronie ofiar wojny, podpisane w Genewie dnia 12 sierpnia 1949 roku, Dz. U. 1956, nr 38, poz. 171; S. Manz, T. Dedering, *South Africa during World War I*, „South African Historical Journal" 2016, vol. 68, iss. 4; A. Pacholska, *Internowanie*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; M. Pietras-Eichberger, *Status prawny i zasady traktowania osób internowanych w czasie konfliktów zbrojnych i okupacji*, „Przegląd Prawa Publicznego" 2010, nr 6; R.C. Thurlow, *Internment in the Second World War*, „Intelligence and National Security" 1994, vol. 9, iss. 1; Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz. U. 2017.1928 t.j.

INTERPOL, Międzynarodowa Organizacja Policji Kryminalnych (ang. International Criminal Police Organization) – instytucja zapewniająca i promująca szeroką wzajemną pomoc zrzeszonych w niej →policji [t. 3], z uwzględnieniem ustawodawstwa obowiązującego w różnych państwach i przy zachowaniu zapisów Powszechnej deklaracji praw człowieka oraz wymogu nieprowadzenia działań o charakterze politycznym, militarnym, religijnym lub narodowościowym. Jej celem jest ustanawianie i rozwijanie narzędzi służących zapobieganiu i zwalczaniu przestępstw kryminalnych.

Interpol jest najstarszą i największą organizacją zapewniającą międzynarodową współpracę policyjną. Pomysł utworzenia takiej organizacji pojawił się już na początku ubiegłego stulecia, czyli na długo przed pojawieniem się zjawiska globalizacji. Społeczność międzynarodowa dostrzegła konieczność nawiązania współpracy, by móc skutecznie zwalczać →przestępczość [t. 3] międzynarodową. Z taką inicjatywą w 1904 r. wystąpiła policja francuska mająca problemy ze zwalczaniem zjawiska tzw. białego niewolnictwa, znanego także współcześnie, a polegającego na nakłanianiu kobiet do wyjazdu za granicę, w celu podjęcia legalnej pracy zarobkowej. Zamiast do pracy w kabaretach kobiety te wbrew swojej woli trafiały do domów publicznych na całym świecie. Francuscy policjanci zrozumieli, że konieczne jest w tym przypadku podjęcie współpracy z policjami innych krajów. Zaproponowali im utworzenie organizacji, która

stałaby się centralnym ośrodkiem koordynującym walkę ze zjawiskiem handlu ludźmi. Odzew nie był satysfakcjonujący, lecz powrót Francji do tej inicjatywy w 1910 r. zyskał już duże zainteresowanie.

W 1914 r. odbył się w Monako pierwszy Międzynarodowy Kongres Policji Kryminalnej, podczas którego zdefiniowano najważniejsze zadania potencjalnej współpracy, za które uznano wymianę → i n f o r m a c j i o przestępcach międzynarodowych oraz doskonalenie procedur ich aresztowania i ekstradycji. Drugi kongres potwierdzający te cele odbył się dopiero po zakończeniu I wojny światowej w 1923 r. Z inicjatywą wystąpił dr J. Schober, ówczesny komendant policji w Wiedniu, który zauważył, iż powstanie po → w o j n i e [t. 4] dużej liczby nowych państw skutkowało gwałtownym wzrostem dynamiki fałszerstw pieniędzy i oszustów finansowych. Na kongresie wiedeńskim powołano Międzynarodową Komisję Policji Kryminalnych, z główną siedzibą w Wiedniu i pod austriackim przewodnictwem. Każdorazowo komendant policji wiedeńskiej automatycznie stawał się prezydentem tej komisji. Koszty jej funkcjonowania oraz utrzymywania siedziby ponosili Austriacy. Ich poważnym atutem było posiadanie jednej z najlepszych na świecie kartotek policyjnych, która stanowiła bazę informacyjną Komisji.

W okresie dwudziestolecia międzywojennego głównym obszarem jej zainteresowań stały się najbardziej uciążliwe w tamtych czasach przestępstwa, takie jak fałszerstwa pieniędzy, czeków i papierów wartościowych, handel żywym towarem, handel narkotykami i kradzieże. Wtedy też Komisja skoncentrowała się na prowadzeniu identyfikacji sprawców przestępstw poprzez praktyczne stosowanie systemu identyfikacji daktyloskopijnej, który został stworzony w 1913 r. przez duńskiego kryminalistyka i policjanta H. Joergensena. Tuż przed wybuchem II wojny światowej, w 1938 r., po dokonaniu → a n e k s j i [t. 1] Austrii przez Niemcy, podczas zgromadzenia w Bukareszcie szef hitlerowskiej policji R. Heydrich zgłosił swoją kandydaturę na stanowisko prezydenta komisji. Jej przyjęcie stało się możliwe dopiero w 1941 r., kiedy organizacja ta wobec całkowitego upolitycznienia nie miała już żadnego znaczenia.

Interpol reaktywowano rok po zakończeniu II wojny światowej, z inicjatywy przedstawiciela belgijskiej policji F. Louwage'a. Nową siedzibą organizacji stała się Francja, co implikowało fakt, że sekretarzem generalnym

został Francuz – L. Ducloux, który przeszedł wszystkie szczeble policyjnej kariery, a w 1941 r. został zwolniony z policji za odmowę współpracy z niemieckim okupantem. Do nowych struktur wstąpiła większość państw, które należały do Interpolu przed II wojną światową, ale nie zaproszono do udziału w nich ZSRR. To spowodowało, że w 1952 r. z Interpolu wystąpiła Polska Rzeczpospolita Ludowa. Państwa obozu socjalistycznego, które traktowały Interpol jako organizację obcą ideowo, o charakterze kapitalistycznym, pomimo że nie wchodziły w jego skład, wielokrotnie z nim współpracowały i korzystały z jego pomocy.

Współczesny kształt organizacyjny Interpol uzyskał w 1956 r., wraz z przyjęciem nowego statutu zwanego konstytucją Interpolu. Podlegała ona kilkukrotnej modyfikacji, m.in. w 1967 r. w Kioto, w 1975 r. w Buenos Aires czy w 1983 r. w Cannes. Wynika z niej, iż Interpol nie jest międzynarodową policją, gdyż nie posiada żadnych własnych organów ścigania. To międzynarodowe narzędzie służące wymianie informacji o przestępstwach i umożliwiające współpracę policjom poszczególnych państw członkowskich w celu zwalczania międzynarodowej przestępczości. Opiera się na zasadach: respektowania → suwerenności państw [t. 4], egzekwowania przepisów prawa karnego, powszechności (wszystkie państwa członkowskie powinny ze sobą współpracować), egalitaryzmu – równości wszystkich państw, współpracy z innymi agencjami oraz elastyczności metod pracy.

Dzięki właściwej strukturze organizacyjnej terytorialny zasięg działania Interpolu obejmuje obecnie obszar 190 państw członkowskich wraz z terytoriami zależnymi. W szerokim ujęciu Interpol składa się z: Sekretariatu Generalnego w Lyonie, 7 biur regionalnych, 190 biur krajowych, 2 specjalnych przedstawicielstw oraz biura łącznikowego przy → Europolu. Sekretariat Generalny w Lyonie stanowi centralę Interpolu, która wykonuje zadania o charakterze operacyjnym, administracyjnym i technicznym. Biura regionalne mieszczą się na różnych kontynentach, w Argentynie (Buenos Aires), Salwadorze (San Salvador), Kamerunie (Jaunde), Kenii (Nairobi), Wybrzeżu Kości Słoniowej (Abidżan), Zimbabwe (Harare) oraz Tajlandii (Bangkok). Biura regionalne to zamiejscowe departamenty Sekretariatu Generalnego.

Zgodnie ze statutem Interpolu każde z państw członkowskich ustanawia lub wyznacza w strukturach krajowych organów ścigania własne

krajowe biuro Interpolu. To jedyna komórka organizacyjna, która na terenie danego kraju pośredniczy w kontaktach pomiędzy wszystkimi organami ścigania tego państwa a Sekretariatem Generalnym oraz krajowymi biurami Interpolu innych państw.

Zostały też otwarte specjalne przedstawicielstwa Interpolu, które działają przy Organizacji Narodów Zjednoczonych (Nowy Jork) i Unii Europejskiej (Bruksela). Taka struktura organizacyjna stwarza wyjątkowe możliwości udzielania wsparcia operacyjnego w poszukiwaniu osób podejrzanych, które ukrywają się przed organami ścigania i wymiarem sprawiedliwości. Wsparcie Interpolu jest systemem uzgodnionych przez państwa członkowskie metod i form współpracy policyjnej realizowanych przez upoważnionych funkcjonariuszy Sekretariatu Generalnego oraz pracowników właściwych krajowych służb policyjnych, które są ukierunkowane na identyfikację i lokalizowanie osób poszukiwanych, przebywających poza granicami danego państwa.

Głównym celem poszukiwań jest ujęcie i aresztowanie osoby ściganej lub zlokalizowanie jej miejsca pobytu. Najważniejszymi formami międzynarodowej współpracy wymiaru sprawiedliwości związanymi z poszukiwaniami podejrzanego są ekstradycja i Europejski Nakaz Aresztowania. Już w 1946 r. J. Nepote stworzył będący do dzisiaj w użyciu system tzw. kolorowych zawiadomień. Wyróżniamy następujące kolorystyczne kody zawiadomień:

- Czerwony – dotyczące osób poszukiwanych przez wymiar sprawiedliwości jednego z państw członkowskich lub międzynarodowy sąd lub trybunał karny w celu aresztowania i ekstradycji. Zawiadomienia te uwzględniają: nazwisko, imię, rysopis osoby wraz ze zdjęciem oraz, w miarę możliwości, odciskami daktyloskopijnymi. Wyróżnić można 2 typy not czerwonych: wydawane na podstawie decyzji krajowego organu wymiaru sprawiedliwości (prokurator/sąd) lub wydawane na podstawie decyzji międzynarodowego trybunału karnego.
- Zielony – informacje i ostrzeżenia o przestępcach, na których należy zwracać szczególną uwagę (np. objąć obserwacją lub powiadomić służby graniczne o konieczności odmowy wjazdu takiej osoby na teren danego kraju).

- Niebieski – zawierające adresowaną do policji krajów członkowskich prośbę o informacje dotyczące wskazanych osób (np.: prawdziwe nazwisko, popełnione przestępstwa).
- Żółty – informacje o osobach zaginionych, cierpiących na zanik pamięci.
- Czarny – informacje o niezidentyfikowanych zwłokach.

W Interpolu stworzono także specjalny mechanizm współpracy dotyczący poszukiwania zbiegów z placówek izolacji społecznej (zakładów karnych, aresztów). W Sekretariacie Generalnym Interpolu działa odrębny, odpowiadający za to zagadnienie wydział – Fugitive Investigative Service. Zajmuje się on opracowywaniem i publikowaniem not poszukiwawczych, koordynacją poszukiwań, upowszechnianiem najlepszych praktyk i wiedzy z obszaru poszukiwań. Aktualnie główna aktywność Interpolu dotyczy zagadnień związanych z narkotykami, przestępczością ekonomiczną i zaawansowanymi technologiami, poszukiwaniami, → terroryzmem [t. 4], handlem żywym towarem i → korupcją. Wskazane formy przestępczości w epoce globalizacji bardzo często nabierają charakteru zorganizowanego i transgranicznego. Stąd już w 1990 r. w Sekretariacie Generalnym utworzono Specjalną Grupę ds. Przestępczości Zorganizowanej, do której zadań należy: budowa baz danych z informacjami o organizacjach zajmujących się międzynarodową → przestępczością zorganizowaną [t. 3], przekazywanie do biur krajowych ważnych informacji w formie okólników i raportów oraz koordynowanie działań w zakresie różnych form przestępczości zorganizowanej, która coraz częściej ma również charakter multiprzestępczy.

Do istotnych przedsięwzięć dotyczących zorganizowanych grup przestępczych należą projekty: „Millenium" – dedykowany euroazjatyckim grupom przestępczym, „AOC" – wymierzony w zorganizowaną przestępczość na terenie Azji, „Scream" – zajmujący się seryjnymi mordercami i gwałcicielami czy „Bada" – zwalczający → piractwo morskie [t. 3].

Kardynalne znaczenie dla realizacji misji Interpolu ma bezwarunkowe uznanie jego statutu przez społeczność międzynarodową. Aby to osiągnąć, Zgromadzenie Ogólne Interpolu obradujące w dniach od 31 października do 3 listopada 2011 r. w Hanoi przyjęło rezolucję wzywającą do jednoznacznego unormowania formalnej przynależności państw członkowskich

do Interpolu. Rezolucja ta stanowiła prawny impuls do rozpoczęcia procesu ratyfikacji statutu we wszystkich państwach zrzeszonych w Interpolu. Oczywiście poszczególne zapisy statutu nie podlegają formalnym negocjacjom ze względu na to, iż obowiązują one już od 1956 r. i są powszechnie respektowane. Wystarczy więc sama ratyfikacja członkostwa.

Warto zwrócić uwagę na reperkusje prawne wynikające z zapisów kodeksu postępowania karnego. 27 września 2013 r. Sejm RP uchwalił jego nowelizację dodającą po art. 605 art. 605a stanowiący, że zatrzymanie osoby ściganej może nastąpić również na podstawie informacji o poszukiwaniach opublikowanych w bazie danych Interpolu. Ta regulacja prawna oznacza, iż jeśli osoba poddana policyjnej kontroli figuruje jako osoba poszukiwana do zatrzymania przez inne państwo członkowskie Międzynarodowej Organizacji Policji Kryminalnych, to można ją zatrzymać. Praktyka niestety dowodzi, że są takie państwa członkowskie, które wykorzystują ten system poszukiwań do ścigania swoich przeciwników politycznych, zwłaszcza tych walczących o zachowanie praw i wolności podstawowych. Dzieje się tak pomimo tego, że krajowe wnioski o zamieszczenie czerwonej noty są wcześniej poddawane sprawdzeniu przez Sekretariat Generalny pod kątem przestrzegania zakazu angażowania się Interpolu w działania o charakterze politycznym, wojskowym, religijnym lub rasowym. Zapis ten ma kluczowe znaczenie w konstytucji Interpolu, stąd przypadki jego łamania wymagają szybkiej reakcji naprawczej ze strony organów sprawiedliwości państwa, którego policja dokonuje takiego motywowanego politycznie zatrzymania. Pomimo takich incydentalnych sytuacji, po blisko 100 latach funkcjonowania Interpolu, trudno sobie wyobrazić skuteczne zwalczanie międzynarodowej przestępczości bez wypracowanego przezeń systemu poszukiwań i wymiany informacji.

Andrzej Czop

J.F. Blashfield, *Interpol. International organizations*, Gareth Stevens, New York 2004; M. Fooner, *Interpol: Issues in World Crime and International Criminal Justice*, Springer, New York 2013; A. Czop, *Europol*, *Interpol*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; I. Gawłowicz, A. Wasilewska, *Międzynarodowa współpraca w walce z przestępczością: (międzynarodowe trybunały karne, Interpol)*, Wydawnictwo

Naukowe Uniwersytetu Szczecińskiego, Szczecin 2004; W. Mądrzejowski, *Przestępczość zorganizowana: system zwalczania*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008; T. Safjański, *Prawne aspekty wykorzystania wsparcia Interpolu w poszukiwaniu osób podejrzanych w świetle art. 605a k.p.k.*, „Prokuratura i Prawo" 2016, nr 10; tenże, *Prawne, organizacyjne i techniczne uwarunkowania udziału Polski we współpracy międzynarodowej w ramach Interpolu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 14.

INTERWENCJA HUMANITARNA – interwencja zbrojna podejmowana przez państwo lub grupę państw (ewentualnie przez organizację międzynarodową) w innym państwie, bez konieczności zezwolenia tego państwa, mająca na celu zapobieżenie katastrofie humanitarnej. Termin pochodzi od łacińskiego *interventio* (wtrącanie się w jakąś sprawę; wywieranie na kogoś wpływu w celu uzyskania określonego efektu, np. zmiany decyzji; starania, zabiegi z tym związane) oraz *humanitas* (wykazujący troskę o człowieka, jego potrzeby, mający na celu jego dobro; ludzki). Przez katastrofę humanitarną rozumie się poważne i występujące na szeroką skalę naruszenia podstawowych →p r a w c z ł o w i e k a [t. 3].

O przesłankach do rozpoczęcia interwencji humanitarnej można mówić, gdy:

- państwo popełnia lub też dopuszcza do popełniania czynów takich jak: masakry, masowe zbrodnie czy też działania o charakterze ludobójczym;
- popełnia lub dopuszcza do popełniania zabójstw, tortur i innych działań, które prowadzą do masowych ucieczek →l u d n o ś c i c y w i l n e j [t. 3].

Interwencja humanitarna jest dopuszczalna, gdy:

- wyczerpały się inne środki polityczne i/lub ekonomiczne;
- istnieje prawdopodobieństwo, że przyniesie pożądany skutek;
- interweniujący zgłasza gotowość zakończenia misji, gdy cele humanitarne zostaną osiągnięte;
- stosuje się proporcjonalność podjętych środków wojskowych do zadania.

O interwencji humanitarnej możemy mówić w momencie, gdy występują 4 podstawowe elementy:

- faktyczne użycie siły;
- podmiot (organizacja międzynarodowa, państwo lub grupa państw);
- przyczyna (masowe naruszenie praw człowieka – kryterium ilościowe, musi dojść do „katastrofy humanitarnej");
- cel i motyw (powstrzymanie naruszeń praw człowieka, ochrona obywateli państwa, w którym następuje interwencja).

O ile interwencja humanitarna jest swoistym pogwałceniem → suwerenności państwa [t. 4], o tyle uważa się, że jest to forma → wojny sprawiedliwej [t. 4], stawiająca dobro ludzkości wyżej niż prawo państwa do samostanowienia. Doktryna taka wywodzona jest z nauk choćby Augustyna z Hippony, Tomasza z Akwinu, P. Włodkowica, H. Grocjusza czy E. da Vattela. Wojna jest zatem dopuszczalna, jeśli jej celem jest pokój, jest wypowiedziana i prowadzona zgodnie z prawem i jest uzasadniona obiektywnie (np. naprawienie szkód), jak i subiektywnie (godna intencja). Jest jednak ostatecznością, gdy inne środki zawiodły.

Interwencja humanitarna jest przewidziana przez Kartę Narodów Zjednoczonych, art. 42 gwarantuje możliwość przeprowadzenia, za zgodą → Rady Bezpieczeństwa [t. 3] (RB), akcji wojskowej – siłami powietrznymi, morskimi i lądowymi – jaką uzna się za konieczną do utrzymania lub przywrócenia międzynarodowego pokoju i → bezpieczeństwa [t. 1]. Akcja ta może obejmować demonstracje, blokadę i inne operacje sił zbrojnych, powietrznych, morskich lub lądowych członków ONZ.

Ze względu na stan prawny wyróżniamy:

- interwencję z upoważnienia RB ONZ;
- bez upoważnienia RB ONZ;
- na zaproszenie rządu.

Ze względu na podmiot interweniujący wyróżniamy interwencje:

- indywidualne;
- zbiorowe;
- regionalne.

Interwencja humanitarna często ma formę wymuszenia pokoju (ang. *peace enforcement*) – działania za zgodą lub bez zgody stron walczących, w celu zapewnienia utrzymania traktatu lub zawieszenia broni (zob. → misja pokojowa [t. 3]).

Historycznie za pierwsze interwencje humanitarne uznaje się amfiktionie ze starożytnej Grecji, gdy *polis* w sojuszu interweniowały w celu obalenia niesprawiedliwych tyranów. Kolejnym takim przykładem może być interwencja Francji w 1860 r. w celu powstrzymania rzezi chrześcijan na Bliskim Wschodzie (czego konsekwencją było powstanie Libanu). Po przyjęciu Karty Narodów Zjednoczonych takimi interwencjami były choćby Indii w Pakistanie Wschodnim (Bangladesz) czy Wietnamu w Kambodży. Wyraźny wzrost ilości tego typu działań można zanotować od upadku systemu bipolarnego, do takich można zaliczyć choćby: interwencję ECOWAS w Liberii (1990), interwencje w Iraku (1991), Somalii (1992), Bośni i Hercegowinie (1992–95), Rwandzie (1994) czy na Haiti (1993–1994). Kontrowersyjna jest druga wojna w Iraku (2003 r.), ale przede wszystkim w Kosowie (1999 r.) Niezależna Międzynarodowa Komisja ws. Kosowa uznała, że ta „interwencja militarna była nielegalna, ale legitymizowana".

Przemysław Mazur

D. Dróżdż, *Interwencje humanitarne a suwerenność państwa: realizowanie utopii – usprawiedliwianie użycia siły zbrojnej poprzez prowadzenie interwencji humanitarnych*, Wydawnictwo Społecznej Akademii Nauk, Łódź 2014; R. Kopeć, *Kryteria i praktyka interwencji humanitarnych w stosunkach międzynarodowych na przykładzie operacji EUFOR w Czadzie i Republice Środkowoafrykańskiej*, [w:] *Polska w Unii Europejskiej: wybrane aspekty polityki bezpieczeństwa w działalności edukacyjno-wychowawczej*, M. Campion, Z. Kwiasowski (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2013; P. Mazur, *Interwencja humanitarna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; D. Rudkowski, *Interwencja humanitarna w prawie międzynarodowym*, Wydawnictwo Sejmowe, Warszawa 2006; A. Szpak, *Interwencja humanitarna – aspekt prawny*, Wydawnictwo Adam Marszałek, Toruń 2005; J. Zajadło, *Dylematy humanitarnej interwencji*, Arche, Gdańsk 2005.

INWAZJA (łac. *invasio*) – w sprawach wojskowych i prawa międzynarodowego – zbrojne wtargnięcie nieprzyjacielskich sił zbrojnych jednego lub kilku krajów drogą lądową, powietrzną lub morską na terytorium innego państwa; najazd, napad wojsk na obce terytorium; działania o charakterze agresywnym z użyciem siły zmierzające do nielegalnego wjazdu na terytorium innego państwa w celu jego okupacji. Zazwyczaj odbywa się nagle

i znajduje odzwierciedlenie w szybkim przesuwaniu się przydzielonych sił do inwazji na inne państwo. Według prawa międzynarodowego inwazja stanowi akt → a g r e s j i [t. 1].

Inwazja to akcja wojskowa, która bezpośrednio zagraża niezależności państwa lub jego terytorium. Inwazje mogą być przeprowadzane w celu przywrócenia lub zmiany rządu. Taki rodzaj inwazji może być postrzegany przez jedną stronę jako akt uzurpacji, podczas gdy druga strona może postrzegać go jako akt wyzwolenia. Zwykle inwazje planowane są w celu szybkiego uzyskania przewagi terytorialnej i geopolitycznej. Do motywacji często należy możliwość grabieży i innych działań im towarzyszących.

Powody podawane jako → *c a s u s b e l l i* [t. 1] inwazji obejmują:

- odzyskanie terytorium utraconego w przeszłości;
- motywacje religijne;
- nabycie terytoriów kolonialnych;
- polityka → i n t e r e s ó w n a r o d o w y c h;
- prześladowanie wrogów lub ochrona sojuszników;
- oczekiwanie na atak w najbliższym czasie lub dostrzeganie możliwości takiego ataku w przyszłości;
- ochrona lub nabywanie szlaków transportowych lub zasobów naturalnych, w tym zaopatrzenie w wodę, ropę, gaz itd.;
- łagodzenie destabilizującego lub nieuzasadnionego konfliktu między sąsiadami;
- rozwiązywanie konfliktów destabilizujących lub uważanych za niemoralne.

Historycznie inwazja przybierała cechy operacji czysto wojskowej, zaplanowanej i przeprowadzonej zwykle ze względów ekonomiczno-politycznych, jeśli nie geostrategicznych, popartej wojną ideologiczną.

Dowody archeologiczne wskazują, że inwazje były częste od czasów prehistorycznych. W starożytności, przed komunikacją radiową i szybkim transportem, jedynym sposobem na zapewnienie odpowiedniego wsparcia było przeniesienie armii jako jednej potężnej siły. To z samej swojej natury doprowadziło do → s t r a t e g i i [t. 4] inwazji. Wraz z inwazją następowały zmiany kulturowe w rządach, religii, filozofii i technologii, które ukształtowały rozwój większości starożytnego świata.

Inwazja jest ofensywą militarną, w której siły zbrojne jednego podmiotu geopolitycznego agresywnie wchodzą na terytorium kontrolowane przez inny taki podmiot, na ogół w celu:

- podbicia terytorium;
- wyzwalania lub przywracania kontroli lub władzy nad terytorium;
- wymuszenia podziału kraju;
- zmiany istniejącego rządu lub uzyskania koncesji ze strony tego rządu;
- z różnych motywacji będących kombinacjami wyżej wymienionych celów.

Inwazja może być przyczyną → w o j n y [t. 4], może być wykorzystana jako część większej strategii zakończenia wojny lub może stanowić kompletną wojnę samą w sobie. Ze względu na dużą skalę operacji związanych z inwazjami są one zwykle strategiczne w planowaniu i realizacji. A ponieważ cele inwazji są często długoterminowe, to potrzebne są znaczne siły zbrojne do utrzymania terytorium i ochrony interesów strony dokonującej inwazji.

Inwazja była szeroko praktykowana we wszystkich okresach historii wojskowej do przejęcia obcych terytoriów, zniszczenia armii wroga i osiągnięcia innych celów agresywnych. Najbardziej znanymi inwazjami starożytności są inwazje wojsk Aleksandra Macedońskiego w Azji Mniejszej i Persji czy perskie inwazje na Grecję, z kolei w przypadku inwazji średniowiecznych należy wspomnieć ekspansję Franków w Europie Zachodniej, podbój przez Arabów państwa Sasanidów i krajów Azji Mniejszej, wielkie podboje Czyngis-chana i Batu-chana, zaś z czasów nowożytnych choćby inwazję Wielkiej Armii Napoleona na Rosję. Państwa z potencjalnie wrogimi sąsiadami zazwyczaj wykorzystywały środki obronne, aby opóźnić lub zapobiec inwazji. Oprócz wykorzystywania barier geograficznych, takich jak rzeki, bagna lub trudny teren, szeroko wykorzystywano fortyfikacje.

W XIX w. istniał również motyw, którym potężne państwa i supermocarstwa próbowały regulować światową politykę, np. zmieniając rząd lub → r e ż i m [t. 3] innego kraju. W takich przypadkach napastnicy często twierdzili, że chronią zaatakowany obszar i → l u d n o ś ć c y w i l n ą [t. 3].

W okresie między I a II wojną światową teoretycy wojskowi państw, które wyznawały pogląd o możliwości osiągnięcia decydującego zwycięstwa

w wojnie za pomocą szybkiego uderzenia, uzasadniali potrzebę utworzenia specjalnej grupy wojsk przeznaczonych do inwazji. Poglądy te były najpełniej realizowane przy budowie armii Niemiec, Włoch i Japonii. Nagła inwazja utworzonych wcześniej specjalnych grup na Europę i Azję stała się główną metodą ataku na inne kraje w II wojnie światowej.

Po II wojnie światowej armie wielu państw wielokrotnie przeprowadzały inwazje na kraje Azji, Afryki, Ameryki Łacińskiej i Bliskiego Wschodu, np.: inwazja izraelskich wojsk na terytorium Syrii i Egiptu w 1967 i 1973 r.; w 1980 r., po różnych konfliktach, Irak najechał sąsiedni Iran i rozpoczął krwawą wojnę, która trwała 8 lat; w 1991 r. wojska Saddama Husajna najechały na Kuwejt. Inwazja na Kuwejt doprowadziła do stworzenia międzynarodowego sojuszu, na czele którego stanęły Stany Zjednoczone; w 2003 r. prezydent USA G.W. Bush wydał rozkaz inwazji na Irak.

Istnieje wiele różnych metod, za pomocą których dokonywane są inwazje, są to:

- inwazja drogą lądową,
- inwazja drogą morską,
- inwazja drogą powietrzną,
- kombinacja tych metod.

Inwazja drogą lądową to bezpośrednie wejście sił zbrojnych na dany obszar, wykorzystując istniejące połączenia lądowe, zwykle przekraczając granice lub inne zdefiniowane strefy, takie jak strefa zdemilitaryzowana czy stanowiska obronne. Chociaż ta taktyka często prowadzi do szybkiego zwycięstwa, ruchy wojsk są stosunkowo powolne i podlegają zakłóceniom spowodowanym przez ukształtowanie terenu i pogodę. Co więcej, trudno jest ukryć plany dotyczące tej metody inwazji, ponieważ większość podmiotów geopolitycznych zajmuje pozycje obronne w obszarach najbardziej narażonych na metody wymienione powyżej.

W nowoczesnej wojnie inwazja lądem często ma miejsce po lub czasami równolegle do ataku na cel innymi środkami. Ataki lotnicze i pociski manewrujące wystrzeliwane z okrętów na morzu są powszechną metodą inwazji. Inne, bardziej subtelne przygotowania mogą wiązać się z potajemnym pozyskiwaniem poparcia, zamordowaniem potencjalnie groźnych liderów politycznych lub wojskowych i zamykaniem linii

zaopatrzeniowych tam, gdzie przekraczają granice sąsiednich krajów. W niektórych przypadkach te inne środki ataku eliminują potrzebę ataku naziemnego. Tak np. atak atomowy na Hiroszimę i Nagasaki w 1945 r. wykluczył potrzebę inwazji sił lądowych aliantów na Wyspy Japońskie. W miarę rozwoju bezzałogowej walki na dalekie dystanse liczba inwazji drogą lądową staje się mniejsza; często konwencjonalna walka dobiega końca, zanim piechota pojawi się w roli sił pokojowych.

Inwazja drogą morską polega na wykorzystaniu zbiornika wodnego w celu ułatwienia wejścia sił zbrojnych w obszar, który sąsiaduje z wodą lub wyspą. Zazwyczaj stosuje się ją albo w połączeniu z inną metodą inwazji, albo w przypadkach, w których nie ma innej metody wejścia na dane terytorium. Argumenty przemawiające za tą metodą zazwyczaj polegają na możliwości wykonania niespodziewanego ataku z morza. Jednakże duża ilość wymaganego specjalistycznego sprzętu takiego jak amfibie oraz trudność w ustanowieniu linii obrony – zwykle skutkująca wysoką liczbą ofiar – wobec stosunkowo niewielkich korzyści, są często używane jako argumenty przeciwko takiej metodzie inwazji. → Z a g r o ż e n i a [t. 4] podwodne i brak dobrej osłony to bardzo częste problemy podczas inwazji z morza. Tak np. jesienią 1943 r., podczas walk Amerykanów z Japończykami o atol Tarawa (niewielki archipelag na Pacyfiku, położony w środkowej części Oceanu Spokojnego w archipelagu Gilberta) amfibie amerykańskie utknęły na rafie koralowej i zostały ostrzelane z plaży. Inne zatonęły, zanim dotarły do brzegu, a czołgi, które niosły, utknęły w wodzie. Ogromna liczba zabitych → ż o ł n i e r z y [t. 4] skłoniła dowództwo USA do modyfikacji taktyk wojennych.

Inwazja drogą powietrzną to wynalazek XX w., który polega na wysłaniu wojsk powietrznodesantowych na terytorium wroga. Niejednokrotnie ataki powietrzne były wykorzystywane do utorowania drogi dla inwazji drogą lądową lub morską poprzez zajmowanie kluczowych pozycji głęboko za liniami wroga, takich jak mosty i skrzyżowania, ale inwazja oparta wyłącznie na powietrzu nigdy się nie udała. Przykłady inwazji powietrznej to: bitwa o Kretę – całokształt zmagań wojennych pomiędzy wojskami alianckimi a niemieckimi w maju 1941 r., których celem było panowanie nad grecką wyspą Kretą, mającą strategiczne znaczenie ze względu na centralne położenie we wschodnim basenie Morza Śródziemnego;

operacja Market Garden – największa operacja z udziałem wojsk powietrznodesantowych przeprowadzona przez aliantów we wrześniu 1944 r. na terytorium okupowanej Holandii, która miała za zadanie przyspieszyć klęskę Niemiec. W tym celu na okupowaną przez Niemców Holandię we wrześniu 1944 r. zrzucono na spadochronach i z wykorzystaniem szybowców prawie 35 tys. żołnierzy amerykańskich i brytyjskich. Jednak nawet przy tak ogromnej sile, która całkowicie zaskoczyła Niemców, atak był taktyczną porażką i po 9 dniach walk alianci odstąpili, a straty wyniosły blisko 17 tys. żołnierzy alianckich.

Wyniki inwazji mogą się różnić w zależności od celów zarówno najeźdźców, jak i obrońców. Najczęstszym typowym skutkiem jest utrata terytorium, której zwykle towarzyszy zmiana rządu, a często utrata bezpośredniej kontroli. W innych przypadkach wynikiem udanej inwazji może być po prostu powrót do *status quo*; można to zaobserwować w wojnach na wyczerpanie, w których głównym celem strategicznym jest zniszczenie zasobów i ludzi.

Pod koniec XX i na początku XXI w. pojawiły się wątpliwości co do skuteczności strategii inwazji w → wojnie czwartej generacji [t. 4]. W tym przypadku jedna lub więcej grup bojowych jest kontrolowana nie przez scentralizowany rząd państwowy, ale przez niezależnych przywódców i może składać się z cywilów, → agentów zagranicznych [t. 1], najemników, polityków, przywódców religijnych i członków regularnej armii. Grupy te działają w niewielkiej liczbie, nie są ograniczone granicami i niekoniecznie zależą od bezpośredniego wsparcia państwa. Takich grup nie można łatwo pokonać zwykłą inwazją, regularna armia państwa może zostać pokonana, a rząd zastąpiony, ale → wojnę asymetryczną [t. 4] grupy te mogą przedłużać w nieskończoność.

Wojny czwartej generacji są charakterystyczne dla ekstremistycznych ideologii i nieuczciwych rządów. Jeśli inwazja może zmienić rząd i zmienić nastawienie społeczeństwa, przedłużony opór jest mało prawdopodobny i można zapobiec przyszłej → przemocy [t. 3]. Takie zmiany mogą wymagać czasu – w niektórych przypadkach pokoleń – ale można uzyskać natychmiastowe korzyści poprzez zmniejszenie liczby bojowników w tajnych komórkach i zablokowanie ich linii zaopatrzenia. Zwolennicy strategii inwazji w wojnie czwartej generacji podtrzymują przekonanie, że

potężna siła okupacyjna może również odnieść sukces w realizacji swoich celów na poziomie taktycznym, odnosząc liczne małe zwycięstwa, jak w przypadku wojny na wyczerpanie.

Koncepcja wojny czwartej generacji jest dość nowa, więc żadna ze stron nie może twierdzić, że wie, jakie strategie ostatecznie rozwiążą problem. Przeciwnicy strategii inwazji wskazują na brak przykładów, w których siły okupujące lub siły pokojowe osiągnęły rozstrzygający sukces. Przytacza się także ciągłe konflikty, takie jak konflikt w Izraelu, Czeczenii i Iraku, oraz inne przykłady, które – jak twierdzą przeciwnicy strategii inwazji – są udowodnionymi niepowodzeniami, tak jak w przypadku konfliktów w Libanie i Afganistanie. Zwolennicy strategii inwazji twierdzą, że jest zbyt wcześnie, aby nazywać takie sytuacje niepowodzeniami, i że do realizacji planu potrzebna jest cierpliwość. Niektórzy uważają, że w rzeczywistości inwazje zakończyły się sukcesem, ale polityczni przeciwnicy i międzynarodowe media manipulują faktami poprzez sensację lub z uwagi na korzyści polityczne.

Olga Wasiuta

G. Bound, *Invasion 1982: The Falkland Islanders' Story*, Casemate Publishers, London 2007; J.M. Dorwart, *Invasion and Insurrection: Security, Defense, and War in the Delaware Valley, 1621–1815*, Associated University Press, Newark 2008; *Encyclopedia of Conflicts Since World War II*, J. Ciment (ed.), Routledge, London–New York 2015; T. Jarmoła, *Kreta 1941*, Bellona, Warszawa 2015; Ł. Kowalewski, *Iracka inwazja na Kuwejt w 1990 r.*, „Przegląd Historyczno-Wojskowy" 2012, nr 4; J. Ledwoch, *Zielone Diabły. Niemieckie wojska spadochronowe 1935–1945*, Militaria, Warszawa 1993; *The Invasion of the Dutch East Indies*, W. Remmelink (ed.), Leiden University Press, Leiden 2015; O. Wasiuta, *Inwazja*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; L.A. Yates, *The U.S. Military Intervention in Panama Origins, Planning, and Crisis Management June 1987–December 1989*, Center of Military History United States Army, Washington 2008; Д. Тимчук і in., *Вторгнення в Україну*: *хроніка російської агресії*, Брайт Букс, Київ 2016.

INŻYNIERIA SPOŁECZNA – inaczej socjotechnika (ang. *social engineering*) – zespół metod wywierania wpływu na ludzi w celu skłonienia ich do wykonania określonych czynności lub zmiany ich zachowania.

W kontekście →cyberbezpieczeństwa [t. 1] inżynieria społeczna może być definiowana jako naruszenie →bezpieczeństwa [t. 1] (np. organizacji) poprzez oddziaływanie na ludzi w taki sposób, aby złamali obowiązujące procedury bezpieczeństwa. Socjotechnika wykorzystywana jest m.in. w celu zdobycia poufnych →informacji (np. haseł dostępu). Metody inżynierii społecznej mogą być wykorzystywane w:

- manipulacjach podczas bezpośredniego kontaktu – np. poprzez podszywanie się pod inną osobę (ang. *impersonation*) w celu uzyskania informacji lub bezpośredniego dostępu do konkretnej osoby, firmy lub systemu komputerowego,
- wiadomościach mailowych – np. w formie →phishingu [t. 3], czyli wiadomościach mailowych spreparowanych w taki sposób, aby przypominały wiadomości od zaufanego nadawcy (np. z banku), w których nakłania się użytkownika do podania poufnych danych lub wykonania określonych czynności,
- wiadomościach otrzymywanych w →mediach społecznościowych [t. 3] – np. prośby o przelanie drobnej sumy pieniędzy na konto – lub w wiadomościach tekstowych SMS (ang. *smishing*, inaczej *phishing SMS*, rozsyłanie krótkich wiadomości tekstowych, które mają skłonić odbiorcę do wykonania określonych czynności, np. nieświadomego pobrania →złośliwego oprogramowania [t. 4], odwiedzenia zainfekowanej strony internetowej, połączenia z podanym numerem telefonu),
- rozmowach telefonicznych – np. praktyka polegająca na pozyskiwaniu informacji lub próbach wywierania wpływu na ludzi w trakcie rozmów telefonicznych (ang. *vishing*).

Metody inżynierii społecznej (w sposób świadomy lub nie i w różnym celu) wykorzystywane są przez różnorodne grupy osób, m.in. →hakerów (osoby włamujące się do systemów komputerowych), pentesterów (ang. *penetration testers*, osoby testujące systemy pod kątem bezpieczeństwa i podatności na →zagrożenia [t. 4]), szpiegów i wywiadowców, złodziei tożsamości, niezadowolonych/przekupionych pracowników danej organizacji, brokerów informacji, rekruterów, sprzedawców, w praktyce przez większość ludzi (np. w rozmowach rodziców z dziećmi, lekarzy z pacjentami).

Dla wyjaśnienia skuteczności działania inżynierii społecznej przytacza się różnorodne teorie dotyczące technik wpływu społecznego, m.in. „6 cech ludzkiej natury" R. Cialdiniego, „7 psychologicznych zapalników" (ang. *7 psychological triggers*) D. Gragga lub „7 zasad oszustwa" (ang. *7 principles of scam*) F. Stajano i P. Wilsona.

Według Cialdiniego ludzie są podatni na manipulacje ze względu na następujące cechy:

- Władza – ludzie mają tendencję do podporządkowywania się woli osoby, która ma „władzę". Socjotechnik może twierdzić, że jest z zarządu danej firmy, pracuje dla osób na wyższym stanowisku niż ofiara, lub podszywać się pod specjalistę (np. z działu informatycznego firmy).
- Sympatia – ludzie mają tendencję do podporządkowywania się woli osoby, która jest sympatyczna, ma podobne zainteresowania, poglądy, podejście do życia, doświadczenie. W kontekście wykorzystania tej socjotechniki możemy sprawdzić, czym interesuje się ofiara, jakie ma hobby, jaką szkołę ukończyła, z jakiego miasta pochodzi, a następnie na podstawie tych informacji dopasować atak i wykazać, że jesteśmy do tej osoby podobni.
- Wzajemność – ludzie chętniej podporządkowują się prośbie, jeśli obiecano im lub dano coś wartościowego. Prezent nie musi być materialny, może to być np. rada, pomoc lub nawet uśmiech czy komplement. Istotne jest, aby „prezent" był wartościowy dla ofiary. Przykładem tego typu działania jest np. zbieranie adresów mailowych w zamian za przesłanie interesujących materiałów (np. e-booków).
- Konsekwencja – ludzie mają tendencję do podporządkowywania się, jeżeli wcześniej publicznie ogłosili swoje poparcie i zaangażowanie w danej sprawie. Przykład ataku: socjotechnik przypomina pracownikowi, na jakie zasady zawarte w polityce bezpieczeństwa firmy się zgodził, a następnie „weryfikuje" jego hasło, które pracownik podaje zgodnie z tymi zasadami. Innym przykładem wykorzystania zasady konsekwencji mogą być ogólne pytania telemarketerów (np. pytanie „Czy uważa Pan, że jedzenie produktów ekologicznych sprzyja zdrowiu?), na podstawie których następnie

proponowana jest odpowiednia oferta (po uzyskaniu odpowiedzi pozytywnej dotyczącej jedzenia ekologicznego telemarketer może zaproponować zakup odpowiednich produktów).

- Przyzwolenie społeczne – ludzie chętniej spełnią prośbę, gdy wydaje im się, że ich zachowanie będzie zgodne z zachowaniem innych. Zasada ta może być wykorzystywana m.in. w procesie sprzedaży lub oferowania konkretnego produktu (np. poprzez hasła reklamowe typu „Zaufało nam już ponad 50 tysięcy klientów" lub „Dołącz do grupy 25 tysięcy zadowolonych subskrybentów newslettera"). Innym przykładem może być postępowanie ankietera, który informuje potencjalnego respondenta o tym, kto już wypełnił ankietę, a następnie zadaje pytania.
- Rzadka okazja – ludzie mają tendencję do zachowywania się w oczekiwany sposób, jeśli wierzą, że dany obiekt, produkt lub usługa występuje w ograniczonej ilości, jest limitowany lub ekskluzywny, pożądany przez innych lub dostępny tylko przez krótki czas lub dla wybranych osób. Przykładem ataku może być sytuacja wyłudzania danych osobowych, w której napastnik wysyła wiadomość mailową, że pierwsze 500 osób, które zarejestrują się na podanej stronie, otrzyma bon do wykorzystania na zakupy w określonym sklepie. Formularz rejestracyjny może wymagać podania takich danych jak np. imię i nazwisko, adres domowy (np. w celu przesłania bonu), numer telefonu i adres e-mail (np. w celu przesłania informacji o zdobyciu nagrody).

Gragg sformułował natomiast 7 psychologicznych zasad, wg których można wpływać na ludzi lub przekonywać ich do wykonania określonych działań:

- Silny wpływ (ang. *strong affect*) – wywołanie silnych emocji u ofiary (np. silne zdziwienie, gniew, panika) zakłóca zdolność logicznego myślenia i przeciwstawienia się sprawcy. Silne emocje mogą być wywołane np. obietnicą wysokiej nagrody, nieprzyjemnej kary lub groźbą utraty danych.
- Przeciążenie (ang. *overloading*) – podanie ofierze zbyt dużej ilości informacji w taki sposób, aby wywołać przeciążenie i ograniczyć czas potrzebny na przetworzenie informacji i podjęcie decyzji.

- Wzajemność (ang. *reciprocation*) – ofiara otrzymuje prezent lub obietnicę, więc czuje się zobowiązana do odwdzięczenia się za przysługę.
- Zwodnicze relacje (ang. *deceptive relationships*) – zbudowanie relacji z ofiarą w celu jej późniejszego wykorzystania. Zasada ta obejmuje także wzbudzanie sympatii u ofiary oraz wskazywania wspólnych cech (np. wspólnych zainteresowań i poglądów).
- →Rozproszenie odpowiedzialności [t. 3] i moralnego obowiązku (ang. *diffusion of responsibility and moral duty*) – ofierze łatwiej będzie podjąć decyzję lub wykonać określone działania, jeśli socjotechnik przekona ją, że nie będzie odpowiedzialna za daną czynność lub nie poniesie ewentualnych konsekwencji.
- Autorytet (ang. *authority*) – socjotechnik podszywa się pod osobę posiadającą władzę lub autorytet (np. będącą na wyższym stanowisku niż ofiara).
- Uczciwość i konsekwencja (ang. *integrity and consistency*) – ofiara będzie skłonna wykonać zaleconą czynność, jeśli socjotechnik przekona ją, że wcześniej ona (lub nawet np. ktoś ze współpracowników) obiecała wykonać dane zadanie.

Stajano i Wilson, na podstawie analizy wielu typów oszustw, opracowali 7 zasad wyjaśniających, dlaczego oszustwa są skuteczne:

- Zasada rozproszenia (ang. *distraction principle*) – odwrócenie uwagi lub rozproszenie ofiary sprawi, że będzie ona bardziej skłonna wykonać polecenia socjotechnika.
- Zasada zgodności społecznej (ang. *social compliance principle*) – normy społeczne nie pozwalają ludziom na kwestionowanie autorytetu, dlatego podszywanie się pod osobę o takich cechach jest skuteczną formą oszustwa.
- Zasada stada (ang. *herd principle*) – ludzie są skłonni postępować w sposób, w jaki postępują inni, lub usprawiedliwiać swoje zachowanie postępowaniem innych osób.
- Zasada nieuczciwości (ang. *dishonesty principle*) – skłonienie ofiary do wykonania nieodpowiednich lub nielegalnych czynności (np. pobrania nielegalnego oprogramowania lub darmowej pornografii) spowoduje, że w przypadku odkrycia przez nią oszustwa nie będzie mogła zwrócić się po pomoc (np. na →policję [t. 3]).

- Zasada oszustwa (ang. *deception principle*) – ludzie zapominają o możliwości, że „rzeczy i ludzie mogą nie być tym, czym się wydają", i nie przeprowadzają weryfikacji autentyczności.
- Zasada potrzeby i chciwości (ang. *need and greed principle*) – potrzeby i pragnienia ludzi (np. chęć zdobycia pieniędzy) sprawiają, że są bardziej podatni na manipulacje.
- Zasada czasu (ang. *time principle*) – ludzie pod presją czasu mają ograniczone możliwości podejmowania decyzji i logicznego myślenia.

Znajomość zasad psychologicznych oraz sposobów oszukiwania i manipulowania ludźmi jest niezbędna socjotechnikowi do przeprowadzenia skutecznego ataku z wykorzystaniem inżynierii społecznej.

Typowymi metodami inżynierii społecznej są m.in. podszywanie się pod pracownika tej samej firmy, firmy partnerskiej, agencji rządowej, udawanie nowego pracownika proszącego o pomoc, oferowanie pomocy w przypadku wystąpienia problemu (np. zainfekowania komputera złośliwym oprogramowaniem), wysyłanie złośliwego oprogramowania w załącznikach do wiadomości phishingowej, oferowanie aktualizacji oprogramowania, używanie firmowego żargonu w celu zdobycia zaufania, wymienianie nazwisk innych pracowników lub kierownictwa, okazywanie posiadania władzy, oferowanie nagrody za wykonanie określonej czynności, komplementowanie lub schlebianie.

Cykl socjotechniczny, mający na celu zdobycie informacji, może być podzielony na 4 główne etapy:

- Rozpoznanie – obejmuje ogólną analizę powszechnie dostępnych informacji (np. treści w mediach społecznościowych i na forach internetowych, zawartość stron internetowych, prasy, a nawet zawartości koszy na śmieci). Wiele informacji, które wydają się bez znaczenia i są powszechnie dostępne, może zostać wykorzystanych w dalszych etapach ataku, np. podczas podszywania się pod inną osobę.
- Budowanie więzi i zaufania – polega m.in. na użyciu wewnętrznych informacji, podawaniu się za kogoś innego, wspominaniu nazwisk znanych ofierze, zgłoszeniu pomocy (w tym momencie wykorzystywane są informacje zdobyte na etapie rozpoznania).

- Wykorzystanie zaufania – zmanipulowanie ofiary i bezpośrednie działanie (np. prośba o informację).
- Wykorzystanie informacji – jeżeli uzyskana informacja jest tylko kolejnym krokiem zbliżającym napastnika do celu, to wraca on do poprzednich etapów cyklu, aż do osiągnięcia sukcesu.

W literaturze przedmiotu można znaleźć stwierdzenia, że każdy człowiek – w odpowiedniej sytuacji, czasie i z wykorzystaniem dopasowanych technik – jest podatny na ataki oparte na inżynierii społecznej. Praktycznie nie jest możliwe, aby w zupełności zapobiec naruszeniom bezpieczeństwa spowodowanym przez tego typu ataki, jednak zastosowanie wielowarstwowych mechanizmów ochrony może zmniejszyć prawdopodobieństwo skuteczności ataku socjotechnicznego lub ewentualnie zminimalizować negatywne skutki ataku. Sygnałami ostrzegawczymi, na które należy zwrócić uwagę, np. podczas nietypowej rozmowy telefonicznej, mogą być m.in. osobliwe prośby, wyraźne okazywanie władzy i podawanie nazwisk, podkreślanie ważności i pilności sprawy, informowanie o konsekwencjach niewykonania prośby, niechętne odpowiadanie na pytania lub niechęć w podawaniu danych (np. zwrotnego numeru telefonu), pochlebstwa. Ochrona przed inżynierią społeczną w kontekście ochrony zasobów organizacji polega na:

- Zwiększeniu lub usprawnieniu fizycznej ochrony – zapewnienie bezpieczeństwa fizycznego i środowiskowego jest jednym z podstawowych elementów ograniczających lub uniemożliwiających dostęp do danych, informacji i systemów dla osób nieuprawnionych.
- Stworzeniu silnej polityki bezpieczeństwa (szczególnie polityki bezpieczeństwa informacji) – polityka bezpieczeństwa powinna być regularnie weryfikowana i aktualizowana, tak aby swoim zakresem obejmowała wszystkie kluczowe aspekty bezpieczeństwa informacji (np. udostępnianie informacji, uzyskiwanie dostępu, zmiana haseł, stosowanie identyfikatorów, niszczenie poufnych dokumentów).
- Kontroli reakcji na naruszenia bezpieczeństwa – pracownicy powinni zostać przeszkoleni w zakresie reagowania na wszelkie próby naruszeń bezpieczeństwa. Kontrola ta obejmuje również przeprowadzanie regularnych szkoleń przypominających o obowiązujących procedurach bezpieczeństwa oraz wdrożenie systemu kar za łamanie zasad i procedur.

- Wdrożeniu procedur postępowania w przypadku incydentów – oprócz wiedzy na temat inżynierii społecznej niezbędne jest także posiadanie praktycznych umiejętności w zakresie reagowania na próby naruszenia bezpieczeństwa (np. sposobów weryfikacji tożsamości rozmówcy poprzez oddzwanianie, poręczenie zaufanego pracownika, podanie specjalnego kodu, kontaktu ze zwierzchnikiem lub szefem, rozpoznawanie po głosie, osobiste spotkanie itd.).

Podstawowym sposobem ochrony przed inżynierią społeczną jest posiadanie wiedzy i świadomości na temat istniejących zagrożeń i sposobów manipulacji oraz wykształcenie odpowiednich nawyków, zachowań i reakcji na sytuacje zagrożenia.

W raporcie *2019 Data Breach Investigations Report* firmy Verizon zawierającym analizę ponad 40 tys. incydentów bezpieczeństwa, w tym ponad 2 tys. potwierdzonych naruszeń bezpieczeństwa danych, wskazano, że w 1/3 z nich wykorzystano ataki z wykorzystaniem inżynierii społecznej. W raporcie *Cyber-ruletka po polsku* firmy PwC, dotyczącym stanu przygotowania polskich firm do zapewnienia bezpieczeństwa informacji i danych, ataki socjotechniczne i zwiększanie świadomości pracowników w obszarze cyberbezpieczeństwa znalazły się wśród najważniejszych wyzwań dla bezpieczeństwa firm.

Paulina Motylińska

R. Cialdini, *Wywieranie wpływu na ludzi. Teoria i praktyka*, tłum. B. Wojciszke, Gdańskie Wydawnictwo Psychologiczne, Sopot 2016; A. Ferreira, L. Coventry, G. Lenzini, *Principles of Persuasion in Social Engineering and Their Use in Phishing*, [w:] *HAS 15, LNCS 9190*, T. Tryfonas, I. Askoxylakis (eds.), Springer, Cham 2015; I. Ghafir, V. Prenosil, A. Alhejailan i in., *Social Engineering Attack Strategies and Defence Approaches*, [w:] *Proceedings 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, M. Younas, I. Awan, W. Seah (eds.), IEEE Computer Society, Los Alamitos–Washington–Tokyo 2016; W. Gogołek, *Komunikacja sieciowa. Uwarunkowania, kategorie i paradoksy*, ASPRA-JR, Warszawa 2010; D. Gragg, *A Multi-Level Defense Against Social Engineering*, SANS Institute, 2003; K. Krombholz, H. Hobel, M. Huber i in., *Advanced Social Engineering Attacks*, „Journal of Information Security and Applications" 2015, vol. 22; K. Mitnick, W. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, tłum. J. Dobrzański, Wydawnictwo Helion, Gliwice 2016; P. Motylinska, *Inżynieria społeczna*, [w:]

Vademecum bezpieczeństwa informacyjnego, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; PwC, *Cyber-ruletka po polsku: dlaczego firmy w walce z cyberprzestępcami liczą na szczęście*, Pwc.pl/badaniebezpieczenstwa, 2018 (dostęp 15.02.2020); F. Stajano, P. Wilson, *Understanding Scam Victims: Seven Principles for System Security*, University of Cambridge Computer Laboratory, Technical Report no. 754, August 2009; *The Social Engineering Framework*, Social-Engineer.org (dostęp 15.02.2020); Verizon, *2019 Data Breach Investigations Report*, 2019, Enterprise.Verizon.com (dostęp 15.02.2020).

INŻYNIERIA WOJSKOWA (ang. *military engineering*) – należąca do nauk wojskowych dziedzina wiedzy i praktycznych umiejętności. Jest także działem ogólnych nauk inżynieryjnych. Jej początki sięgają starożytności.

Zajmuje się przystosowaniem terenu do prowadzenia przez siły zbrojne działań taktycznych (operacyjnych) oraz tworzeniem warunków dla efektywnego udzielania przez wojsko pomocy technicznej →ludności cywilnej [t. 3] w →sytuacjach kryzysowych [t. 4] (np. trzęsienie ziemi, powódź). Wchodzi w skład ochrony wojsk na wszystkich etapach ich przygotowania i wdrożenia.

W zakres inżynierii wojskowej wchodzą: budownictwo wojskowe, drogownictwo wojskowe, fortyfikacja, geologia wojskowa, hydrotechnika wojskowa, maskowanie techniczne (w tym organizacja i mechanizacja prac inżynieryjnych), minerstwo, mostownictwo wojskowe, prace inżynieryjno-wojskowe oraz zapory inżynieryjne. Częściowo się między sobą pokrywają znaczeniowo, stąd niektóre ze zbudowanych w XXI w. obiektów wojskowych można zaliczyć do kilku z wymienionych dziedzin.

Inżynieria wojskowa bywa też definiowana nieco szerzej. W takim ujęciu obejmuje także komunikację wojskową, →infrastrukturę wojskową, infrastrukturę portową i lotniskową, ratownictwo oraz wsparcie geograficzne.

Podobne rozbieżności definicyjne spotkać można także odnośnie do pojęć niższego rzędu wchodzących w skład inżynierii wojskowej. Przykładowo fortyfikację można zdefiniować jako projektowanie i opracowywanie konstrukcji obiektów budowlanych określonego typu (zwanych, wg W. Kawki, zespołami fortyfikacyjnymi) wraz z koncepcją ich wykorzystania, organizacją prac fortyfikacyjnych i wykorzystaniem tych obiektów do osłony działań bojowych wojsk oraz osłony bronionego

obszaru (państwa, jego części, państw połączonych sojuszem wojskowym). W węższym znaczeniu to jedynie zespół obiektów fortyfikacyjnych. Fortyfikacje tradycyjnie dzieli się na stałe i polowe, choć jak wskazują niektórzy specjaliści, w praktyce obecnie podział ten jest dość umowny.

W ramach inżynierii wojskowej przygotowywane są także projekty racjonalnych rozwiązań konstrukcyjnych. Aktualnie są one pod względem technologii oraz organizacji prac najczęściej związane z budową fortyfikacji, dróg i mostów wojskowych, a także zadaniami minerskimi i maskowaniem technicznym.

W XX w. części składowe inżynierii wojskowej takie jak minerstwo, fortyfikacja i maskowanie techniczne mają wyraźne cechy wojskowych nauk stosowanych, pozostałe stanowią działy ogólnych nauk inżynieryjnych. Zmiany w ramach inżynierii wojskowej są zdeterminowane tymi potrzebami operacyjnymi, które wynikają z realizacji głównych zadań wsparcia inżynieryjnego sił zbrojnych. To ostatnie jest kompleksem obejmującym przedsięwzięcia wraz z określonymi środkami i siłami przeznaczonymi do zrealizowania zadań inżynieryjnych. Jak pisze B. Bębenek, te ostatnie mają stworzyć jednostkom wojskowym na tyle dogodne warunki terenowe, by mogły one prowadzić skuteczne działania bojowe przy ograniczeniu czynników oddziaływania wykorzystywanych przez przeciwnika. W warunkach zbliżonych do optymalnych pod względem dowodzenia i finansów determinuje to nasilony rozwój określonych kompetencji w ramach wojsk inżynieryjnych. W XXI w. inżynieria wojskowa w coraz większym stopniu skupia się na doskonaleniu zdolności w zakresie zdolności przetrwania wojsk, mobilności oraz kontrmobilności.

Jak wskazuje Kawka, dziedziny wchodzące w skład inżynierii wojskowej ewoluują w związku ze zmianami wyposażenia (np. technicznych środków rażenia) i taktyki działania poszczególnych rodzajów wojsk. Przykładem jest system działań inżynieryjnych powiązany z systemem walki i jego zgrywaniem.

Niektórzy specjaliści wojskowi (jak np. Bębenek) utożsamiają analizowane pojęcie z wojskami inżynieryjnymi. Chodzi tu szczególnie o ich zmiany organizacyjne, etatowe, modernizację techniczną, organizację szkolenia oraz co najmniej częściowo taktykę szkolenia. Dla K. Wysockiego, M. Depczyńskiego i P. Szymczaka ta część armii jest gotowa realizować

tylko te zadania wchodzące w zakres inżynierii wojskowej, których realizacja wymaga specjalistycznego wyposażenia i wykwalifikowanego personelu. Zdaniem tych badaczy wojska inżynieryjne włączają w zakres swojej aktywności tylko część tematyki, którą obejmuje inżynieria wojskowa. Nic dziwnego – od strony podstawowych zadań inżynieryjnych sił zbrojnych do inżynierii wojskowej należy bowiem zabezpieczenie inżynieryjne i działanie inżynieryjne, którymi zajmują się wszystkie rodzaje wojsk. Jedynie wsparcie inżynieryjne z założenia wyłącznie jest realizowane przez jednostki wojsk inżynieryjnych.

W literaturze przedmiotu można spotkać pogląd, że w większości przypadków rozwiązywanie zagadnień inżynieryjnych wchodzących w zakres omawianego pojęcia sprowadza się do wypracowania oraz przyjęcia określonych organizacyjnych i technicznych sposobów wykonywania prac i budowy obiektów.

Do przyczyn ograniczonego wykorzystania w budownictwie wojskowym firm cywilnych można zaliczyć m.in. specyfikę zaplanowanych obiektów wojskowych, opór władz wojskowych, wymogi związane z przestrzeganiem tajemnicy wojskowej oraz sytuacje wspomniane przez M. Boulègue'a, gdy ze względu na poziom → k o r u p c j i w państwie władzom państwowym łatwiej jest wykorzystać → ż o ł n i e r z y [t. 4] jako tanią siłę roboczą.

Inżynieria wojskowa w dużym stopniu pokrywa się z pojęciem inżynierii → b e z p i e c z e ń s t w a [t. 1]. Inne pokrewne do analizowanego pojęcia to środki i urządzenia inżynieryjne oraz technika inżyniersko-saperska. Planowanie, organizacja oraz realizacja działań podejmowanych w ramach inżynierii wojskowej odnośnie do walk i operacji wojskowych wchodzi w zakres inżynieryjnego zabezpieczenia działań bojowych tych walk (lub operacji).

Tomasz Skrzyński

B. Bębenek, *Doświadczenia inżynierii wojskowej wynikające z operacji prowadzonych poza granicami kraju*, [w:] *Teoria i praktyka taktyki w XXI wieku*, red. W. Więcek, L. Elak, Warszawa 2016; tenże, *Nowe tendencje rozwojowe inżynierii wojskowej*, [w:] *Inżynieria Wojskowa problemy i perspektywy*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2014; M. Boulègue, *Military Infrastructure*

and Logistics in the Russian Arctic, [w:] tegoż, *Russia's Military Posture in the Arctic: Managing Hard Power in a „Low Tension" Environment*, Hatham House, The Royal Institute of International Affairs, London 2019; W. Kawka, *Działania inżynieryjne w ochronie ekspedycyjnych zgrupowań wojsk lądowych*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2012, dodatek; tenże, *Rozbudowa fortyfikacyjna terenu w działaniach militarnych*, AON, Warszawa 2011; *Rozwój, eksploatacja, przechowywanie oraz ochrona balistyczna środków transportu*, M. Szudrowicz, Z. Ciekot (red.), Wojskowy Instytut Techniki Pancernej i Samochodowej, Bel Studio, Warszawa 2016; *XXXIII Konferencja Naukowo-Techniczna „Ekomilitaris 2019". Inżynieria bezpieczeństwa – ochrona przed skutkami nadzwyczajnych zagrożeń*, Bel Studio, Warszawa 2019; K. Wysocki, M. Depczyński, P. Szymczak, *Współczesne wojska inżynieryjne Federacji Rosyjskiej*, Akademia Sztuki Wojennej, Warszawa 2017.

IRREDENTYZM (wł. *irredenta* – niewyzwolona) – roszczenia terytorialne oparte na wspólnych powiązaniach etnicznych między jednym państwem a mniejszością zamieszkałą w innym państwie. To również wszelkie działania zmierzające do uzyskania wolności (odzyskania niepodległości); ruch polityczny i społeczny dążący do połączenia w jeden organizm państwowy ziem zamieszkiwanych przez podobne grupy etniczne; dążenie do połączenia z państwem macierzystym części narodu i zamieszkałych przez nią terytoriów znajdujących się najczęściej w pobliżu granic państwa macierzystego; tendencje niepodległościowe, działania i ruch zmierzające do ustanowienia niepodległości (w rozumieniu potocznym). Ze swej istoty jest to koncepcja szeroko stosowana przez ideologie nacjonalistyczne, amerykański badacz J. Braille uważa irredentyzm za szczególną formę →nacjonalizmu [t. 3].

Irredentyzm jest bezpośrednio związany z procesem formowania się państw narodowych i można go rozumieć na 2 sposoby. Z jednej strony może to być pragnienie niektórych narodów, które żyjąc w pewnym państwie, chcą się od niego oddzielić, by utworzyć własne państwo narodowe, albo przyłączyć się do innego państwa, do którego uważają, że należą; z drugiej strony może to być roszczenie terytorialne państwa wysuwane wobec innego państwa. Spory terytorialne nie zawsze są irredentystyczne, ale często przedstawiane są jako takie, aby zdobyć poparcie społeczne i międzynarodowe.

W szerszym znaczeniu irredentyzm rozumiany jest jako każdy ruch polityczny lub ludowy, który stara się odzyskać i zająć ziemię, którą członkowie ruchu uważają za „zagubione" (lub „nieodkupione") terytorium przeszłości narodu z powodów kulturowych, historycznych, językowych, rasowych lub innych.

Irredentyzm ma źródła we włoskim ruchu politycznym z przełomu XIX i XX w., zapoczątkowanym ok. 1878 r., głoszącym konieczność przyłączenia do Włoch m.in. Trydentu, Triestu, Istrii i Dalmacji, które znajdowały się poza granicami Włoch, ale były zamieszkałe przez Włochów. Celem irredentystów było przyłączenie tych obszarów do ojczyzny. Zamiary te częściowo urzeczywistniono po I wojnie światowej. Ruch irredentystów silnie rozwijał się przed I wojną światową, później połączył się z ruchem faszystowskim. Czynnikiem sprzyjającym irredencie jest wspólnota pochodzenia, kultury, tradycji historycznej i świadoma wola zbiorowa.

W różnych częściach świata istnieją irredentystyczne ruchy polityczne, które są wspierane przez część grup etnicznych lub organizacje i partie polityczne, jednak nie są one oficjalnie uznawane przez państwo, rządy krajowe mogą je w niektórych przypadkach promować lub uznawać w pewnym okresie swojej historii. Np. rosyjski irredentyzm dąży do stworzenia tzw. „Wielkiej Rosji", która chce, aby dawne terytoria Związku Radzieckiego stały się częścią Federacji Rosyjskiej. Prezydent Rosji W. Putin promuje ideologię, która ma na celu wzmocnić wpływy Rosji w okupowanych regionach.

Irredentyzmy można podzielić na 2 grupy: na oficjalnie uznane i irredentyzmy bez oficjalnego lub historycznego uznania. Niektóre państwa mają dokumenty prawne, które formalizują ich irredentystyczne roszczenia, mogą to być konstytucje lub inne rodzaje dekretów.

Wiele państw formalizuje irredentystyczne roszczenia, włączając je do swoich dokumentów konstytucyjnych lub za pomocą innych środków prawnych. Takie roszczenia terytorialne są „uzasadnione" na podstawie rzeczywistych lub wyimaginowanych narodowych koncepcji historycznych powiązań terytorialnych, religijnych lub etnicznych. Polityka irredentystyczna może być popierana przez nacjonalistyczne i ogólnonarodowe ruchy i być cechą polityki tożsamości oraz kulturowej i politycznej geografii. Irredentyzm może działać jako narzędzie rządu, by przekierować niezadowolenie obywateli wobec osób z zewnątrz. Obszar, który może być

przedmiotem potencjalnego roszczenia, jest czasami nazywany irredentą; ale nie wszystkie irredenty są koniecznie zaangażowane w irredentyzm.

Irredentyzm może być inicjowany przez politycznie aktywnych członków lub przez ekspansjonistycznych bądź nacjonalistycznych przedstawicieli tytularnego narodu w państwie większości. Metody walki o zjednoczenie mogą mieć różny charakter i nie zawsze kończą się powodzeniem. W przypadku porażki część irredentów może wybrać ścieżkę → r e p a t r i a c j i [t. 3]. Należy podkreślić, że nie wszyscy irredenci są skłonni poprzeć ideę połączenia ziemi/terytorium, na której żyją, z ziemią ich tytularnego państwa z powodów ekonomicznych lub innych.

W przeciwieństwie do diaspory, której członkowie są rozproszeni na terytoriach państw odległych od ich historycznej ojczyzny, irredenci zwykle mieszkają zwarcie w państwach graniczących z ich historyczną ojczyzną, ze szczególnie wysoką koncentracją na przygranicznych, sąsiadujących terytoriach. Właśnie geograficzna bliskość i zwartość zamieszkania odróżniają irredentów od diaspory. Ale, podobnie jak diaspory, irredenci próbują stworzyć sieć instytucji społecznych w celu utrzymania i rozwoju zarówno własnej społeczności, jak i jej więzi z sąsiadującą większością i/lub innymi irredentami. Jednocześnie irredenci zwykle boleśnie podchodzą do naruszenia ich praw przez rząd, ponieważ uważają się za autochtonicznych mieszkańców terytorium, które zajmują. Jeśli przypadki dyskryminacji nabierają charakteru systematycznego, wśród irredentystów powstaje idea ponownego zjednoczenia z terytorium większości etnicznej.

Klasyczne przykłady irredentyzmu: Węgrzy w Rumunii i Ukrainie; Kazachowie w Rosji, Mongolii, Chinach i Uzbekistanie; Uzbecy w Kirgistanie, Afganistanie; Rosjanie w Ukrainie.

Upadek imperium doprowadza do podziału rodzin i przerysowania granic geograficznych. Nowi przywódcy obiecują powrót ludzi i terytoriów, które mogły zostać utracone w przeszłości, często opowiadając się za agresywną polityką zagraniczną, która może prowadzić do kosztownych i niszczycielskich → w o j e n [t. 4]. Ostatnim latom imperiów austro-węgierskiego i osmańskiego, końcowi europejskiej kolonizacji w Afryce i Azji oraz upadkowi Związku Radzieckiego towarzyszyły wojny i okrucieństwo.

Rozpad ZSRR i koniec → z i m n e j w o j n y [t. 4] doprowadziły do nowych impulsów wywołujących konflikty, takich jak nacjonalizm, napięcia

etniczne i irredentyzm. Wraz z upadkiem → k o m u n i z m u Rosja była prawdopodobnie najczęściej obserwowanym miejscem rewolucyjnego irredentyzmu w latach 90. XX w. Było to całkowicie właściwe, biorąc pod uwagę zarówno ciężar rosyjskiej historii jako imperium zbudowanego na ciągłym podboju terytorialnym, jak i znaczną liczbę Rosjan pozostawionych poza nowymi granicami Rosji.

Pomimo ogromnych trudności politycznych i gospodarczych, z jakimi borykają się wszystkie byłe państwa komunistyczne podczas przechodzenia na demokrację rynkową, tylko Rosja, Armenia, Chorwacja i Serbia próbowały zmienić istniejące granice.

Irredentyzm zaostrzył konflikty w następstwie rozpadu Jugosławii, ponieważ wysiłki na rzecz zjednoczenia wszystkich Serbów w Wielkiej Serbii i bośniackich Chorwatów w Wielkiej Chorwacji przedłużyły konflikt i spowodowały okrucieństwa i czystki etniczne. Po zakończeniu wojen jugosłowiańskich w 1995 r. okazało się, że gwałtowne irredentystyczne wysiłki, podczas których grupy etniczne chciały odzyskać utracone ziemie, stały się mniej częste i mniej ważne, przynajmniej w Europie. Jednak → a n e k s j a [t. 1] Krymu przez Rosję w 2014 r. i poparcie separatystycznych rebeliantów we wschodniej Ukrainie sprawiły, że znaczenie tego tematu znalazło się ponownie na pierwszym planie dyskusji politycznych. Te incydenty podkreśliły, że irredentyzm jest daleki od wymarcia, a zdecydowany przywódca może wykorzystać mniejszość jako pretekst do destabilizacji Europy na jej wschodniej granicy.

W książce S.M. Saidemana i R.W. Ayresa *For Kin or Country: Xenophobia, Nationalism, and War* autorzy proponują jasne i zwięzłe wyjaśnienie, dlaczego niektóre kraje stosują agresywną politykę wobec swoich sąsiadów, aby chronić swoje mniejszości, podczas gdy inne tego nie robią – chociaż polityka irredentystyczna może być kosztowna, a irredentyzm ryzykuje wojnę z sąsiadami, zaś sama wojna jest zawsze kosztownym procesem, niezależnie od wyniku. Wszelkie wysiłki na rzecz (re)unifikacji terytoriów zamieszkałych przez krewnych etnicznych z pewnością będą antagonizować sąsiadujące państwa. Co więcej, taka polityka zagraniczna prawdopodobnie zrazi sojuszników sąsiada, a być może nawet inne kraje stojące w obliczu podobnych → z a g r o ż e ń [t. 4].

Wysiłki irredentystyczne mogą przerodzić się w wojny, a takie konflikty mogą być jednymi z najbardziej trudnych i długotrwałych walk w polityce światowej. W rzeczywistości obie wojny światowe rozpoczęły się jako wojny irredentystyczne. Serbskie zamiary stworzenia Wielkiej Serbii doprowadziły do wybuchu I wojny światowej, a plan Hitlera, aby zjednoczyć Niemców, przyczynił się do wybuchu II wojny światowej. Innymi gorącymi punktami irredentyzmu są Kosowo, spór o Kaszmir między Indiami a Pakistanem, problemy związane z regionami przygranicznymi Afganistanu i Pakistanu, a także Irak.

Irredentyzm można częściowo wyjaśniać siłą nacjonalizmu i zdolnością przywódców do czerpania korzyści z pradawnych nienawiści, które przez lata utrzymywała przy życiu społeczność.

Olga Wasiuta

T. Ambrosio, *Irredentism: Ethnic Conflict and International Politics*, Greenwood Publishing Group, London 2001; G. Andreopoulos, *State and Irredentism: Some Reflections on the Case of Greece*, „The Historical Journal" 1981, vol. 24, no. 4; Ch. Farrington, *Reconciliation or Irredentism? The Irish Government and the Sunningdale Communiqué of 1973*, „Contemporary European History" 2007, vol. 16, no. 1; D. Horowitz, *Irredentas and Secessions: Adjacent Phenomena, Neglected Connections*, [w:] *Irredentism and International Politics*, N. Chazan (ed.), Lynne Rienner Publishers, Adamantine Press Limited, Boulder–London, 1991; M. Kornprobst, *Irredentism in European Politics. Argumentation, Compromise and Norms*, Cambridge University Press, Cambridge 2008; *Leksykon współczesnych międzynarodowych stosunków politycznych*, C. Mojsiewicz (red.), Wrocławskie Wydawnictwo Naukowe Atla 2, Wrocław 1998; T. Nałęcz, *Irredenta polska*, Książka i Wiedza, Warszawa 1992; J. Rak, *Irredentyzm i kontrirredentyzm jako typy postaw wobec ojczyzny*, „Principia" 2016, nr 63; S.M. Saideman, R.W. Ayres, *For Kin or Country: Xenophobia, Nationalism, and War*, Columbia University Press, New York 2015; ciż, *Determining the Causes of Irredentism: Logit Analyses of Minorities at Risk Data from the 1980s and 1990s*, „The Journal of Politics" 2000, vol. 62, no. 4; M. Suslov, *„Russian World": Russia's Policy towards its Diaspora*, „Russie Nei Visions" 2017, no. 103; O. Wasiuta, *Irredentyzm*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

ISACA (Information Systems Audit and Control Association) – międzynarodowe, niezależne stowarzyszenie o charakterze non profit, którego

celem jest opracowywanie wysokiej jakości standardów wiedzy i praktyk dla specjalistów w dziedzinie systemów informatycznych, zwłaszcza w aspekcie zarządzania →bezpieczeństwem [t. 1] w IT. Obecnie poprzez globalną działalność i wysoką jakość standaryzacji ISACA wyznacza kierunek rozwoju zarządzania →informacjami, ich kontroli, bezpieczeństwa oraz audytów.

Aktualnie ISACA ma ponad 200 oddziałów członkowskich w ponad 185 krajach oraz zrzesza ponad 140 tys. członków, wyszkoliła także i certyfikowała ponad 15 tys. osób niebędących członkami tejże organizacji. W swojej ofercie udostępnia profesjonalne, certyfikowane kursy, których ukończenie ma znaczną wartość na rynku pracy na całym świecie. W sposób ciągły zapewnia edukację członków, dostęp do zasobów wiedzy i opracowań orzecznictwa oraz możliwość konsultacji ze środowiskiem specjalistów na cyklicznie organizowanych konferencjach poświęconych problemom dotyczącym zawodów związanych z zapewnieniem bezpieczeństwa sieci, kontroli oraz ogólnym zarządzaniem IT. Ponadto ISACA wydaje czasopismo techniczne z tematyki kontroli informacji „ISACA Journal", a także organizuje międzynarodowe konferencje.

W Polsce zarejestrowane stowarzyszenie ISACA Warszawa dostało akredytację ISACA International w 2012 r., posiada oddziały w Warszawie i Katowicach.

Za nieformalny początek działalności stowarzyszenia można uznać 1967 r., kiedy wąska grupa specjalistów związanych z audytem bezpieczeństwa systemów komputerowych podjęła kroki na rzecz scentralizowania wiedzy, jej źródeł oraz norm implementacji odpowiednich praktyk. W 1969 r. działania grupy postanowiono sformalizować, rejestrując Stowarzyszenie Audytorów EDP. Następnie w 1976 r. w jego ramach utworzono fundację edukacyjną, której zadaniem była działalność badawcza mająca na celu poszerzanie wiedzy oraz rozpowszechnianie wypracowanych standardów w dziedzinie zarządzania, bezpieczeństwa oraz audytu w branży IT.

Warto zwrócić uwagę, iż proponowane przez tę instytucję standardy bezpieczeństwa są uniwersalne i mają zastosowanie w prawie wszystkich kategoriach przemysłu, finansów, bankowości oraz stanowisk sektora publicznego. Certyfikacja wydana przez stowarzyszenie jest poważnym atutem na rynku pracy, który zwiększa wiarygodność posiadanych

kompetencji. Od kandydatów wymaga się zdania egzaminu pisemnego z każdego z 4 podstawowych certyfikatów, są tylko 3 terminy egzaminu w roku. Jednym z wymogów członkostwa w stowarzyszeniu jest przestrzeganie kodeksu etyki zawodowej ISACA i wyrażenie zgody na spełnianie wymagań ustawicznego kształcenia zawodowego. Obecnie ISACA oferuje zdobycie 4 certyfikatów: CISA (Certified Information Systems Auditor), CISM (Certified Information Specialist Manager), CGEIT (Certified in the Governance of Enterprise IT), CRISC (Certified in Risk and Information Systems Control).

Piąta certyfikacja – CSX Practitioner (CSX-P) – została wprowadzona w 2015 r. i nie mieści się w ogólnych ramach, które dotyczą wyżej wymienionych zaświadczeń. Jest skierowana do praktyków bezpieczeństwa, którzy planują działania i reagują w odpowiedzi na incydenty związane z bezpieczeństwem.

CISA jest certyfikatem mającym na celu potwierdzenie umiejętności audytora systemów informatycznych, zaświadcza o wykwalifikowaniu w zakresie audytu i kontroli systemów informatycznych przedsiębiorstwa. Jest to najpopularniejszy certyfikat ISACA, do tej pory przyznano 115 tys. tego typu certyfikatów. Zagadnienia na egzaminie dotyczą: procesu audytu systemów informatycznych, kierowania i zarządzania IT, pozyskiwania, rozwoju i wdrażania systemów informatycznych, operacji systemów informatycznych, utrzymania usług i zarządzania usługami, ochrony zasobów informatycznych. Egzamin na certyfikat CISA składa się ze 150 pytań, warunkiem dopuszczenia do kursu i egzaminu jest przedstawienie dowodu doświadczenia zawodowego (minimum 5 lat audytu, kontroli lub bezpieczeństwa systemów informatycznych na poziomie zawodowym) oraz złożenie odpowiedniego wniosku. Warto wspomnieć, że brak wykształcenia informatycznego nie jest problemem dla stowarzyszenia – np. rok doświadczenia zawodowego jest odpowiednikiem 2 lat studiów.

Certyfikat CISM jest obecnie wiodącym zaświadczeniem dla kadry zarządzającej w IT, do tej pory wydano ponad 27 tys. takich certyfikatów. Posiadanie CISM świadczy o kwalifikacjach umożliwiających projektowanie, rozwijanie oraz nadzorowanie → b e z p i e c z e ń s t w a i n f o r m a c j i [t. 1] w przedsiębiorstwie. Zakres materiału na egzamin z tego certyfikatu obejmuje zarządzanie bezpieczeństwem informacji, → z a r z ą d z a n i e

ryzykiem informacyjnym [t. 4] i zgodność z przepisami, zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz opracowywanie i zarządzanie programem bezpieczeństwa informacji. Test składa się z 200 pytań, wymagane jest przedstawienie dowodu posiadania 5 lat doświadczenia zawodowego w bezpieczeństwie informacji, w tym przynajmniej 3 lat zajmowania stanowiska kierowniczego w bezpieczeństwie. Istotny jest również czas między uzyskaniem doświadczenia a zdaniem egzaminu – do 10 lat przed datą zgłoszenia. W przypadku braku doświadczenia w zakresie bezpieczeństwa informacji certyfikacja CISA, certyfikacja Certified Information Systems Security Professional (CISSP) lub studia podyplomowe są odpowiednikiem 2 lat doświadczenia. Certyfikaty takie jak Disaster Recovery Institute Certified Business Continuity Professional (CBCP), CompTIA Security +, Microsoft Certified Systems Engineer (MCSE), ANS Global Information Assurance (GIAC) lub ESL IT Security Manager są liczone jako rok doświadczenia.

Rzadkością na rynku pracy są osoby z certyfikatem CGEIT, który jest przeznaczony dla profesjonalistów posiadających zaawansowaną wiedzę i doświadczenie w zarządzaniu przedsiębiorstwem i zapewnianiu mu bezpieczeństwa, zajmujących się zagadnieniami relacji biznesu i IT, postępowaniem zgodnie z najlepszymi praktykami i standardami w zakresie operacji IT i zarządzania, zarządzaniem inwestycjami w IT. Zakres zagadnień egzaminu to: ramy zarządzania, zarządzanie strategiczne, realizacja świadczeń, optymalizacja ryzyka, optymalizacja zasobów. Wymagania są znacznie wyższe niż w przypadku wcześniej wspomnianych certyfikacji: egzamin składa się ze 150 pytań, ale konieczne jest przedstawienie dowodu doświadczenia zawodowego w profesjonalnym zarządzaniu przedsiębiorstwem, pełnieniu funkcji doradczej lub wspierającej zarządzanie. W tym rok doświadczenia musi być związany z ramami zarządzania IT w przedsiębiorstwie, natomiast pozostałe muszą dotyczyć zarządzania strategicznego, realizacji korzyści, optymalizacji ryzyka lub optymalizacji zasobów (przynajmniej 2 z wymienionych). Osoby wykładające na uczelniach przedmioty związane z zarządzaniem w IT mogą przeliczać 2 lata w pełnym wymiarze godzin na każdy rok doświadczenia zawodowego.

Statystyka ISACA wskazuje, że certyfikat CRISC zdobyło ponad 18 tys. osób, jego posiadanie charakteryzuje specjalistów IT, odpowiedzialnych

za wdrażanie programów zarządzania ryzykiem informacyjnym w całym przedsiębiorstwie. Obszary wiedzy na egzamin z tego certyfikatu to: identyfikacja ryzyka, ocena ryzyka, reakcja na ryzyko i ograniczanie ryzyka, monitorowanie oraz raportowanie ryzyka i kontroli. Egzamin składa się ze 150 pytań, wymagane jest posiadanie doświadczenia zawodowego (skumulowanego w obszarze profesjonalnego zarządzania i kontroli ryzyka oraz spełnianie co najmniej 2 z wymagań zawodowych z certyfikatu CRISC). W przypadku tego certyfikatu nie ma możliwości zastąpienia doświadczenia zawodowego wykształceniem czy innymi certyfikatami – ISACA daje 10 lat na zdobycie doświadczenia po złożeniu wniosku o certyfikację lub 5 lat od daty zdania egzaminu.

Oficjalnie nie ma formalnej, stopniowalnej ścieżki certyfikacyjnej, formalnie dostosowanej do struktury hierarchicznej w firmach, to ISACA sugeruje, by przede wszystkim do certyfikacji podchodziły osoby wcześniej zajmujące stanowiska kierownicze ds. informacji, statystyki, technologii lub dyrektora zarządzającego. Zalecane jest w pierwszej kolejności zdanie certyfikatu CISM, potem CGEIT, a na koniec CRISC. CISM doskonale nadaje się do ogólnego zarządzania bezpieczeństwem w przedsiębiorstwie, a certyfikaty CGEIT i CRISC obejmują zarządzanie i zagadnienie ryzyka.

W 2015 r. ISACA uruchomiła nowy program certyfikacyjny o nazwie Cybersecurity Nexus, w skrócie CSX. W planach jest dodanie zaświadczenia specjalistycznego i eksperckiego do oferty certyfikacyjnej; obecnie jedynym dostępnym certyfikatem CSX jest CSX Practitioner (CSX-P).

Certyfikat CSX-P jest przewidywany dla pracowników, którzy mogą działać jako osoby reagujące na incydenty bezpieczeństwa jako pierwsi. Specjaliści mieliby postępować zgodnie z ustalonymi procedurami i zdefiniowanymi procesami oraz pracować przede wszystkim ze znanymi problemami w jednym systemie. Kandydaci muszą wykazać się umiejętnościami i wiedzą w zakresie pracy z firewallami, tworzenia łatek bezpieczeństwa, działania programów antywirusowych, a także być w stanie wdrożyć wspólne kontrole bezpieczeństwa, wykonywać skanowanie w poszukiwaniu podatności i realizować podstawowe zadania analizy → z a g r o ż e ń [t. 4] i naruszeń. W zakres wymagań dla zdobycia certyfikatu CSX-P wchodzi zaliczenie 4-godzinnego egzaminu opartego na wydajności, dostępnego w centrach testowych Prometric. Podobnie jak w przypadku

innych certyfikatów ISACA, posiadacze CSX-P muszą stosować się do kodeksu etycznego organizacji i przestrzegać jej zasad ciągłego kształcenia i recertyfikacji. Jednak utrzymanie ważności tego poświadczenia znacznie różni się od wcześniej wspomnianych certyfikatów: posiadacze CSX-P muszą zgromadzić 30 godzin ciągłego kształcenia zawodowego (ang. *continuing professional education*, CPE) rocznie, z których 24 muszą obejmować szkolenia oparte na praktykach lub laboratoriach, a także dodatkowe 6 godzin na tradycyjnych zajęciach szkoleniowych. W trzecim roku posiadacz CSX-P musi ponownie przystąpić do egzaminu i zdać obecny certyfikat. Zakres materiału na egzamin obejmuje: identyfikację, obronę, wykrywanie, odpowiadanie, odzyskiwanie. Test ma wymiar praktyczny: kandydaci mają do czynienia z symulowanymi incydentami lub sytuacjami związanymi z bezpieczeństwem i muszą przeprowadzać analizy, diagnozować lub przeprowadzać różne naprawy i reagować na nie w celu ich rozwiązania.

Aby utrzymać ważność certyfikatu, posiadacze referencji muszą zdobyć 120 punktów CPE w okresie 3 lat od certyfikacji lub po odnowieniu (zdobywając co najmniej 20 CPE rocznie) i wnieść roczną opłatę za utrzymanie (45 USD dla członków i 85 USD dla osób niebędących członkami). W przeciwnym razie posiadacze certyfikatu muszą ponownie przystąpić do egzaminu, aby zachować jego ważność.

American National Standards Institute (ANSI) akredytował poświadczenia CISA, CISM, CGEIT i CRISC jako spełniające normę ISO/IEC 17024 dla jednostek obsługujących systemy certyfikacji osób.

W ustawodawstwie III RP certyfikat CISA jest wymieniany także w 2 aktach prawnych III RP: w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji na liście certyfikatów upoważniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych oraz w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, która uprawnia posiadacza certyfikatu do wykonywania zawodu audytora wewnętrznego.

Trzecią sferą rozwiązań, jakie proponuje ISACA, są programy dobrych praktyk związanych z zarządzaniem w firmach, wśród których aktualnie można wymienić: COBIT 4.1 (Control Objectives for Information and Related Technologies), który uwzględnia 34 wysokopoziomowe procesy,

obejmujące 210 celów kontrolnych; Risk IT, który odnosi się do zarządzania ryzykiem związanym z technologiami informatycznymi; Val IT i jego pochodne platformy programistyczne (ang. *frameworks*), który jest przeznaczony dla kadry zarządzającej na poziomie biznesowym; BMIS (Business Model for Information Security), który jest systemem zarządzającym bezpieczeństwem informacji.

Wojciech Cendrowski

D. Cannon, B.T. O'Hara, A. Keele, *CISA: Certified Information Systems Auditor Study Guide*, Sybex, Indianapolis 2016; W. Cendrowski, *ISACA*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *CISM Review Manual 2013*, ISACA, Illinois 2013; *COBIT 5. Enabling Processes*, ISACA, Illinois 2012; *History of ISACA*, ISACA.org (dostęp 29.04.2019); A. Kohnke, K. Sigler, D. Shoemaker, *Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Frameworks*, CRC Press, Boca Raton 2017.

ISLAMIZM (ew. polityczny islam) – ideologia, wg której postuluje się osiągnięcie przez islam dominacji w świecie, drogą do tego będzie rewolucja muzułmańska. Pierwszym krokiem ma być zjednoczenie wszystkich muzułmanów w jedną wspólnotę (arab. *umma*), która z czasem utworzy państwo (kalifat, arab. *daula islamijja*), w którym władza będzie pochodziła od Boga (*hakimijja*), jedynym prawem będzie prawo boskie (arab. *szari'at*), wszelkie problemy rozwiązywane będą w oparciu o religię, ostatecznie islam opanuje cały świat, inne religie będą mogły istnieć tylko, jeśli będą monoteistyczne i jeśli uznają prym islamu. Osiągnięcie takiego stanu będzie odbywało się przy sprzeciwie muzułmanów, którzy odeszli od prawdziwego islamu, poddając się wpływom złych nauczycieli lub ideologii obcych islamowi (arab. *takfir*) oraz niewiernych (arab. *kuffar*), dlatego niewykluczone będzie użycie siły i wypowiedzenie świętej → w o j n y [t. 4] (→ d ż i h a d).

Termin islamizm początkowo funkcjonował jako określenie religii muzułmańskiej. Takim sformułowaniem posługiwali się jeszcze Wolter, A. de Tocqueville czy E. Renan, termin był stosowany zamiennie z mahometanizmem (w jęz. pol. używał go choćby H. Sienkiewicz). Dopiero na

przełomie XIX i XX w. „islamismus" lub „islamism" zostały wyparte przez termin „islam", co ostatecznie zostało usankcjonowane w wydawanej przez Brill w latach 1931–1938 *Encyklopedii islamu* (*The Encyclopaedia of Islam*). Pojawienie się ponownie tego terminu, tyle że już w znaczeniu ideologii politycznej, miało miejsce w latach 70. XX w. Problem powiązania polityki i islamu w dyskursie naukowym zawdzięczamy artykułowi B. Lewisa *The Return of Islam* (1975). Termin zaczął być stosowany głównie we Francji w latach 80. XX w. Do najczęściej stosowanych pojęć zaliczamy: fundamentalizm islamski, polityczny islam, dżihadyzm, radykalny islam, islamski aktywizm (Q. Wiktorowicz), wojowniczy islam czy nawet militarny islam.

Nie ma konsensu terminologicznego, często terminy te stosowane są zamiennie. Zwłaszcza problematyczne jest rozróżnienie między fundamentalizmem a islamizmem. J.J.G. Jansen uważa, że fundamentalizm ma podwójną naturę religijną i polityczną, dlatego też jeśli islamizm jest fundamentalizmem, jest to tylko rozumienie węższe. G. Kepel nie rozróżnia tych terminów, stosując je zamiennie, nawet w przypadku pojęcia „radykalnego islamu". B. Tibi uważa, że mamy do czynienia z przenikaniem się religii i polityki, nie jest to zjawiskiem ekskluzywnym dla islamu. Sądzi, że jest reakcją świata islamu na → k r y z y s kulturowo-polityczny spowodowany kolonializmem i postępującą globalizacją. Islam i islamizm wpływają na siebie, religia została „upolityczniona" i służy legitymizacji przejęcia władzy. T. Ramadan uważa, że islamizm jest tożsamy z salafizmem, a więc jedną ze szkół określanych mianem fundamentalistycznych. Jednocześnie twierdzi, że to reakcja na kolonializm, porównując go do teologii wyzwolenia z Ameryki Południowej. Podkreśla, że ruch ten okazał się kluczowy poprzez zwrócenie uwagi na relacje religii i polityki (zwłaszcza problemu sekularyzacji). K. Hroub sądzi, że powstanie islamizmu jest wynikiem nałożenia się warunków historycznych oraz kontekstu społeczno-politycznego i gospodarczego, niemniej nie bez znaczenia były też podstawy religijne i ideologiczne. B.B. Lawrence zaproponował wprowadzenie terminu „fundamentalizm" dla odcięcia go od ruchu chrześcijańskiego, wnioskował o stosowanie arabskiego terminu *usulijja.* J.L. Esposito uważa, że osiągnięto efekt odwrotny od zamierzonego i fundamentalizm pozostał na stale w dyskursie, zwłaszcza politycznym, powiązany z islamem,

wg badacza błędnie. Na ogół przyjmuje się jednak, że fundamentalizm jest przede wszystkim ruchem religijnym, a islamizm to ruch polityczny. Osobnym zagadnieniem jest rozróżnienie między islamizmem a islamem politycznym, na ogół terminy te używane są zamiennie, ale islamizm ze względu na semantyczne zaakcentowanie bliskości do ideologii bardziej niż religii zaczyna być popularniejszym terminem.

Ideologia ta wywodzi się z jednej z sunnickich szkół koranicznych, tzw. hanbalickiej, zakładała ona konieczność odrzucenia obcych wpływów (religii, tradycji, filozofii) i powrotu do czystego objawienia Koranu i hadisów. W XIX w. na fali kolejnych porażek imperium osmańskiego i jednoczesnego wzrostu znaczenia zachodnich kolonizatorów narodził się ruch *salafijji* (dosłownie: przodek). Uznano, że należy zreformować sułtanat, a jedyną możliwością będzie powrót do prawdziwego islamu, kolejnym krokiem będzie stworzenie własnego systemu społecznego opartego na szariacie. Wreszcie, przypominając sukcesy islamu z jego początków, uznano, że obecne porażki nie wynikają z braku zdolności do osiągnięcia sukcesu, lecz z odejścia od prawdy. W tym kontekście publikowali i nauczali Dżamal ad-Din al-Afghani (1837–1897), Muhammad Abduh (1849–1905) i Raszid Rid (1865–1935). Ich nauki dotyczyły zarówno reformy religii, jak i stworzenia swoistej ideologii mającej uratować muzułmanów przed niewolą. Raszid Rida krytykował kalifat turecki jako ten, który zaprzeczał prawdziwej koncepcji kalifatu, uważał jednak, że celem będzie zbudowanie wspólnoty i stworzenie nowego kalifatu, zgodnego z zasadami szariatu. W swojej książce *Al-Chilafa au al-imama al-uzma* (*Kalifat albo wielki imamat*) skrytykował koncepcję sułtana, sądząc, że władza płynie od Boga i z jego nauki. Tymczasem sułtan okazał się tyranem, odchodzącym od wiary, co też skłaniało go do złego. Odrzucając takie przywództwo, sformułował koncepcję państwa islamskiego (arab. *daula islamijja*).

Koncepcję Raszida Ridy rozwijał Hassan al-Banna (1906–1949), założyciel Bractwa Muzułmańskiego (1928). Sprzeciwiał się demokracji jako sztucznemu tworowi Zachodu. Uważał, że istnienie partii politycznych służy jedynie interesom samych partii oraz poszczególnych grup społecznych, które stoją za tymi partiami. Tymczasem rządy islamskie mają dbać o interesy wszystkich warstw społecznych. Al-Banna i jego Bractwo Muzułmańskie opowiadało się za pełną implementacją prawa religijnego

do systemu prawa państwowego. Państwo islamskie to jedynie takie państwo, w którym obowiązuje jedynie islamskie prawo, czyli *szari'at*. Musi on obwiązywać na wszystkich poziomach zarządzania państwem i wspólnotą.

Kolejny ideologiem był Sajjid Abul ala al-Maududi (1903–1979). Jego kluczową pracą było *The Process of Islamic Revolution*. Jego zdaniem władza pochodzi od Boga, zatem w państwie islamskim władza jest boska (*hakimijja Allah*). W 1954 r. wydał pracę *Four Basic Qur'anic Terms*, zawarł w niej koncepcję jedności człowieka i Boga. Jeśli człowiek chce być sługą Boga, musi mu się oddać na każdej płaszczyźnie, również politycznej. Pojęcie suwerenności boskiej al-Maududiego było inspiracją dla Sajjida Kutby (1906–1966), który uznał, że jedyne, co legitymizuje państwo, to jego boskie pochodzenie i podporządkowanie Bogu. Kutba uznał, że państwo islamskie musi opierać się na następujących zasadach:

- Wprowadzenie rządów Boga – rząd ma kierować się zasadami religijnymi.
- Wprowadzenie instytucji kalifa jako symbolu jedności wszystkich muzułmanów.
- Wprowadzenie prawa boskiego (szariatu), a Koranu w miejsce świeckich konstytucji.
- Zlikwidowanie systemu partyjnego i utworzenie „muzułmańskiej organizacji ludowej".

Współczesne państwo jest zaprzeczeniem państwa islamu. Po pierwsze, jest to państwo bazujące na zachodniej myśli. Granice i ustroje państw islamskich często są narzucone i są pewną formą kolonializmu. Mają *de facto* służyć dalszemu zniewoleniu muzułmanów i próbie ich zniszczenia. Prawdziwe państwo islamu istniało tylko w początkach religii, czyli za czasów Mahometa i kolejnych 4 kalifów (632–661).

Jedną ze szczególnie niebezpiecznych idei Zachodu jest państwo narodowe i koncepcja nacji. Przywiązanie do narodu i terytorium jest wbrew islamowi. R. Scruton twierdzi, że to jeden z głównych problemów w relacji pomiędzy Zachodem a światem islamu. Terytorium i prawo zamknięte w obrębie tegoż jest nie do pogodzenia z koncepcją boskiego pochodzenia prawa. Ponadto zachodnia cywilizacja opiera się na koncepcji umowy społecznej, zatem i pewnej dobrowolności. Człowiek może kreować swoją rzeczywistość, w tym porządek polityczny i prawny. W świecie islamu jest

to zakazane. Kutb uważał obecnie istniejące ustroje społeczne, ekonomiczne czy polityczne za wyraz choroby cywilizacji Zachodu. → K o m u n i z m przez swój ateizm i materializm jest największym → z a g r o ż e n i e m [t. 4], ale i kapitalizm ze względu na atomizm społeczny jest nie do przyjęcia.

Arabowie są narodem wybranym, któremu zostało objawione, jak należy żyć, jakie wartości są istotne. To dzięki temu zasługują na „szacunek i przywództwo ludzkości". Arabowie nie mogą porzucić swojej misji, każdy naród ma jakieś swoje dzieło do uczynienia, a ten największy z narodów ma największe dzieło – zanieść światu islam. Bóg sprawdza swoich wybranych, poddaje ich wielu próbom, by oddzielić prawdziwie wierzących od tych, którzy nie zasługują na zbawienie. Oni pokonają swoje słabości i tak wbrew swoim ciemiężcom zwyciężą.

Według Kutby przyniesie nowy ład społeczny całej ludzkości:

> Islamski system społeczny jest dziś jedynym porządkiem na świecie, który opiera się na zasadzie internacjonalizmu w rzeczywistym tego słowa znaczeniu, ponieważ jest jedynym systemem pozwalającym na pokojowe życie pod swoimi rządami wszystkich ras, języków i wyznań.

Ów porządek zostanie zaprowadzony tylko dzięki woli boskiej. Zniesie on wszelki ucisk i rywalizacje między narodami, będzie gwarantem wiecznego pokoju.

> Ten nowy porządek będzie ludzki, ustanawiać będzie swoje stosunki międzynarodowe na bazie pokoju i przyjaźni z tymi, którzy nie walczą z nim. Powstanie takiego porządku na jakimkolwiek skrawku ziemi uważa się za gwarancję dla całej ludzkości powstrzymania dekadencji, regresu i burzenia.

Ideologia stworzona przez Kutbę nazywana jest też kutbizmem.

Koncepcja ta była dalej rozwijana, szczególnie duże było znaczenie dżihadu w latach 70. i 80. XX w. Muhammad Abd as-Salam Faradż (1954–1982) i Abd Allah Azzam (1941–1989) uczynili z niego kluczowy element. Podkreślali oni konieczność zjednoczenia muzułmanów i czynu

zbrojnego. To z tego nurtu powstała ideologia Al-Kaidy i → Państwa Islamskiego [t. 3] (Daesh, ISIS), a pewnym jego uwieńczeniem było ogłoszenie powstania kalifatu i wybrania kalifem Abu Bakra al-Bagdadiego (29 czerwca 2014 r.).

Do koncepcji islamizmu nawiązywali też Talibowie. Był to ruch sunnicki, którego głównym przywódcą był Mohammad Omar, nawiązywał on przede wszystkim do nauk al-Maududiego. Istnieją zresztą podejrzenia, że ten ruch był inspirowany przez pakistańskie → służby specjalne [t. 4]. Talibowie odrzucali demokrację, władza świecka była powiązana z religijną, wprowadzono również szariat w jego bardzo restrykcyjnej formie (widoczne były wpływy wahhabitów).

T. Osman zwraca uwagę na rozwijającą się wersję turecką islamizmu, jej propagatorami są Partia Sprawiedliwości i Rozwoju (tur. Adalet ve Kalkınma Partisi, AKP) i jej przywódca R.T. Erdoğan. Jest to swoiste połączenie wątków nacjonalistycznych z religią, jest zatem pewnym odejściem od koncepcji państwa laickiego Atatürka. Ruch początkowo zdobył znaczną popularność na prowincji tureckiej, bardziej konserwatywnej, która okazała się głównym elektoratem partii. Wraz z kolejnymi sukcesami wyborczymi mieszkańcy prowincji zaczęli wchodzić w skład administracji, część również migrowała do dużych miast. Turecka wersja islamizmu jest też pewną formą odseparowania Turcji od wpływu islamizmu arabskiego, głównie Bractwa Muzułmańskiego, poprzez adaptację pewnych metod i elementów doktryny.

Islamizm ma też swoją szyicką wersję. Za głównego ideologa można uznać Ali Shariati Mazinaniego, nawiązującego do Mohammada Ikbala, ideologicznego ojca założyciela Pakistanu. Jego koncepcja rewolucji islamskiej była raczej inspirowana filozofią Hegla czy marksistów, ale udało mu się ją powiązać z religią. Dzięki temu stworzył szyicką wersję rewolucji muzułmańskiej na wzór koncepcji Kutby czy Maududiego. Uważał, że należy naśladować proroka Muhammada (Mahometa) i jego następców, takich jak Ali, ponieważ przywrócenie prawa szariatu jest niezbędne dla uratowania się przed kolonializmem. Uważał, że westernizujący się muzułmanie są faktycznie agentami Zachodu i służą zachodnim interesom, wśród tych pseudomuzułmanów był oczywiście szach Iranu Mohammad Reza Pahlawi. Koncepcję Mazinaniego kontynuował Chomeini.

Ideologia ta bazowała na szyizmie, stąd też szczególne miejsce w niej przewidziano dla religijnych przywódców (arab. *ulama/alimi*), którzy interpretując prawo, wskazują właściwe postępowanie przywódcom państwa. Ich rządy będą obowiązywały do czasu nastania Mahdiego.

Islamizm nie jest ideologią spójną, zasadne jest mówienie o islamizmach. Nawet w nurcie Braci Muzułmanów widoczne są daleko idące podziały, część neguje zaangażowanie polityczne czy stosowanie → p r z e m o c y [t. 3]. Powołanie kalifatu ISIS zostało uznane przez większość Braci za świętokradztwo, również nurt Al-Kaidy nie zaakceptował tego faktu. Mimo znaczącej różnorodności wyraźne są jednak wspólne cechy, podobna diagnoza obecnej sytuacji społeczno-politycznej, te same cele. Wyraźne są też wzajemne inspiracje ideologów. Do innych ważniejszych przedstawicieli islamizmu można zaliczyć również ideologów takich jak Abu Bakr al-Baghdadi, Safar al-Hawali, Al-Hadżdż Muhammad Amin al-Husajni, Jusuf al-Kardawi, Muhammad Kutba, Usama ibn Ladin, Abu Bakr Naji (Muhammad Khalil al-Hakaymah), Said Ramadan i jego synowie Hani i Tariq, Abu Musab al-Suri, Muhammad Surur, Abu Musab al-Zarkawi, Ayman al-Zawahiri.

Przemysław Mazur

J.J.G. Jansen, *Podwójna natura fundamentalizmu islamskiego*, tłum. A. Łojek-Magdziarz, Wydawnictwo Libron, Kraków 2005; H.S. Jamsheer, *Reforma władzy i społeczeństwa w arabsko-muzułmańskiej myśli politycznej wieków XIX i XX*, Wydawnictwo Naukowe Ibidem, Łódź 2008; B. Lewis, *The Return of Islam*, „Commentary" 1976, vol. 61, no. 1; G. Kepel, *Fitna: wojna w sercu islamu*, tłum. K. Pachniak, Wydawnictwo Akademickie Dialog, Warszawa 2006; tenże, *Zemsta Boga: religijna rekonkwista świata*, tłum. A. Adamczak Wydawnictwo Krytyki Politycznej, Warszawa 2010; M. Kramer, *Coming to Terms, Fundamentalists or Islamists?*, „Middle East Quarterly" 2003, vol. 10/2; P. Mazur, *Czy dżihad to ideologia? O niekonsekwencjach terminologicznych wokół „walki na ścieżce Boga"*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 2; P. Mazur, O. Wasiuta, S. Wasiuta, *Państwo Islamskie ISIS: nowa twarz ekstremizmu*, Difin, Warszawa 2018; T. Osman, *Islamism: A History of Political Islam from the Fall of the Ottoman Empire to the Rise of ISIS*, Yale University Press, New Haven–London 2017; *Political Islam. Context versus Ideology*, K. Hroub (ed.), Soas Middle East Issues & London Middle East Institute, London 2010; T. Ramadan, *Islam: The Essentials*,

A Pelican Book, Penguin Random House UK, London 2017; R. Scruton, *Zachód i cała reszta*, tłum. T. Bieroń, Zysk i S-ka, Poznań 2002; B. Tibi, *Fundamentalizm religijny*, tłum. J. Danecki, Państwowy Instytut Wydawniczy, Warszawa 2001; B. Tibi, *Political Islam, World Politics and Europe: From Jihadists to Institutional Islamism*, Routledge, London–New York 2014; A. Zasuń, *Polityczny islam: między religią polityczną a instrumentalizacją religii w polityce*, Wydawnictwo im. Stanisława Podobińskiego Akademii im. Jana Długosza, Częstochowa 2018; J. Zdanowski, *Współczesna muzułmańska myśl społeczno-polityczna: nurt Braci Muzułmanów*, Wydawnictwo Naukowe ASKON, Warszawa 2009.

IWAR – termin używany przez →NATO [t. 3] do opisania formy →wojny [t. 4] w internecie oraz oznaczenia ataków przeprowadzanych w sieci, ukierunkowanych na infrastrukturę internetową konsumenta (np. strony internetowe zapewniające dostęp do usług bankowości internetowej). W tym rozumieniu iWar różni się od →cyberwojny [t. 1], →cyberterroryzmu [t. 1], →wojny informacyjnej [t. 4] czy walki informacyjnej, które dotyczą wykorzystania komputerów, internetu i innych środków przechowywania lub rozprzestrzeniania →informacji w celu przeprowadzania ataków na systemy informatyczne przeciwnika. Wykorzystują one do tego celu systemy i sieci teleinformatyczne; przejmują środki komunikacji, zdobywają dostęp do →infrastruktury wojskowej i →krytycznej, uciekają się do szpiegostwa elektronicznego oraz dowodzenia i kontroli pola walki, a ich polem bitwy są sieć łączności i →wywiad [t. 4] satelitarny.

iWar jest inna, ponieważ wykorzystuje wszechobecną infrastrukturę o niskim poziomie →bezpieczeństwa [t. 1], np. strony zapewniające dostęp do rozmaitych usług online. Podczas gdy same państwa narodowe mogą angażować się w cyberwojny i wojny informacyjne, iWar może być prowadzona przez jednostki, korporacje i społeczności. Małe „i" w nazwie wskazuje na jej wspólny rodowód z gadżetami i urządzeniami, które symbolizują nowe pokolenie osób korzystających z najnowszych technologii.

Koncepcja po raz pierwszy została przedstawiona zimą 2007 r. w przeglądzie NATO przez pracownika Instytutu Spraw Międzynarodowych i Europejskich J. Ryana. Również M. Andrejevic używa terminu iWar, aby uwzględnić istotne cechy współczesnej wojny. Mówi o interaktywnej stronie wojny z terrorem, która opiera się na nowych praktykach

monitorowania i zarządzania populacjami. Według niego nowe technologie mediów uczestniczących tworzą cyfrową obudowę konfliktu, w której każde działanie i transakcja generuje informacje o sobie, które następnie mogą być wydobywane i wykorzystywane do celów gospodarczych lub politycznych.

iWar prowadzi się za pomocą ataków typu odmowa usługi (ang. *denial of service*, DoS), które są znane od końca lat 80. XX w. Takie ataki mają na celu uniemożliwienie działania komputera lub systemu sieciowego poprzez bombardowanie go dużą ilością zapytań i zajęcie wszystkich wolnych zasobów. W razie powodzenia ataku obiekt nie będzie w stanie np. zapewnić dostępu do określonej witryny.

Przykładem iWar może być atak na Estonię 27 kwietnia 2007 r., kiedy to nastąpiły rozproszone ataki typu DDoS (ang. *distributed denial of service*) na ważne strony internetowe: prezydenta, parlamentu, wiodących ministerstw, partii politycznych, głównych serwisów informacyjnych i 2 dominujących banków w Estonii. Witryny zostały zablokowane i uniemożliwiono interakcję z klientami i użytkownikami. Ataki trwały do połowy czerwca. Estoński minister obrony nazwał ataki → z a g r o ż e n i e m b e z p i e c z e ń s t w a [t. 4] narodowego.

Atak DDoS działa na tej samej zasadzie, co DoS, ale zwielokrotnia swój wpływ, wykorzystując → b o t n e t [t. 1] komputerów w sieci, które zostały zdalnie przejęte, tak aby bombardować obiekt ataku wieloma żądaniami w tym samym czasie. Botnety mogą być kontrolowane przez jedną osobę. Niektóre botnety w atakach na Estonię składały się nawet ze 100 tys. maszyn.

Badacze wyróżniają 5 cech iWar, które wskazują, że może ona zrewolucjonizować konflikty:

- Potencjał do rozszerzenia działań ofensywnych – iWar rozszerza serię działań ofensywnych o bezprecedensową liczbę amatorów, których jedyną kwalifikacją jest połączenie z internetem. Atakujący w iWar, podobnie jak żołnierz z muszkietem, jest wyposażony w tani, potężny sprzęt, którego użytkowanie wymaga niewielkiego przeszkolenia.
- Nieograniczony zasięg geograficzny – iWar jest niedroga i łatwa do prowadzenia w sposób rewolucyjny. Po raz pierwszy w historii

wojna zostaje uwolniona od kosztów, przeszkód i wysiłków, które tradycyjnie powstrzymywały działania ofensywne przeciwko geograficznie odległym celom. Mobilność umożliwia użycie siły na coraz większe odległości od własnego terytorium. Konwencjonalna technologia ofensywna, polegająca na zdolności niszczenia celów za pomocą środków kinetycznych, jest kosztowna i stosunkowo powolna, np. samolot musi wykonać długi lot, aby zrzucić ładunek. W wojnie typu iWar można zadawać obrażenia z dowolnego punktu na ziemi, w dowolnym miejscu na ziemi, praktycznie bez żadnych kosztów.

- Trudność w wyjawieniu (rozpoznaniu) – prowadzenie iWar trudno rozpoznać, udowodnić i ukarać. Do dziś nadal nie jest jasne, czy Estonia padła ofiarą →cyberataków [t. 1] →hakerów bez zezwolenia ze strony Kremla, czy też zostały one oficjalnie usankcjonowane i skoordynowane przez inne, wrogie państwo. Nawet gdyby udowodnić winę jakiegoś państwa, nie jest jasne, w jaki sposób powinno zareagować państwo zaatakowane. Wojna typu iWar wykorzystuje rosnącą zależność wszystkich struktur państwowych od systemów komputerowych. Również śledztwo byłoby problematyczne – nawet jeśli wykryłoby komputer zarządzający botnetem i atakiem DDoS (który zwykle trwa tylko przez krótki, intensywny okres), jest mało prawdopodobne, aby można było podjąć skuteczne działania w celu wniesienia oskarżenia. Jeżeli nawet zostałby odnaleziony komputer, za pomocą którego zostało zaatakowane państwo, to „winny" komputer może znajdować się pod jurysdykcją państwa, z którym nie ma współpracy, wobec czego nie da się wyegzekwować prawa. Nawet gdyby nawiązano współpracę, istnieje możliwość, że komputer był obsługiwany z kafejki internetowej lub innej anonimowej publicznej sieci, co uniemożliwiłoby wskazanie osób zaangażowanych w atak DDoS.
- Łatwość proliferacji – iWar nie jest ograniczona geograficznie, co warunkowałoby rozprzestrzenianie się innowacji wojskowych, a zatem szybko rozprzestrzeniła się na całym świecie. Podczas gdy np. technologia produkcji prochu pojawiła się w Chinach w VII lub VIII w., ale debiutowała w Europie dopiero we Flandrii w 1314 r.,

narzędzia i wiedza niezbędne do prowadzenia iWar są dostępne w sieci. W 2007 r. informacje o atakach DDoS na Estonię rozprzestrzeniły się szybko na forach internetowych.

- Wpływ na cele „gotowe" – wpływ iWar wzrośnie, gdy internet będzie odgrywał coraz ważniejszą rolę w codziennym życiu politycznym, społecznym i gospodarczym. W ostatnim dziesięcioleciu rządy, społeczności, korporacje i osoby fizyczne nieprzerwanie wykorzystywały sieć jako środek dostarczania usług i kontaktów z obywatelami, klientami i rówieśnikami. Np. w Estonii, która zajęła 23 miejsce w rankingu e-gotowości, jest prawie 800 tys. klientów banków internetowych w populacji liczącej prawie 1,3 mln osób, a 95% operacji bankowych prowadzone jest elektronicznie. W wielu państwach dostarczanie treści medialnych za pośrednictwem sieci konkuruje teraz z konwencjonalną dystrybucją gazet i muzyki. Niezbędność technologii internetowych w wewnętrznej działalności organizacji biznesowych nabiera tempa. W Wielkiej Brytanii wydatki na reklamę w internecie są wyższe niż na reklamy w prasie krajowej.

Instytucje i organizacje mogą w coraz większym stopniu polegać na technologiach internetowych w swojej wewnętrznej działalności, wykorzystując aplikacje internetowe – np. Dokumenty Google (Google Docs) – i zastępować nimi konwencjonalne programy, takie jak te wchodzące w skład pakietu Microsoft Office. Dlatego iWar zagraża nie tylko interakcjom między organizacjami i ich klientami czy między państwem a obywatelem, ale także wewnętrznym działaniom organizacji.

Żadne państwo nie ma pełnej kontroli nad internetem. Jednostronne, „policyjne" inicjatywy nie będą skuteczne przeciwko iWar, ponieważ – podobnie jak piractwo przez wieki – jest to globalne zjawisko. Polityka ochrony mórz w przeszłości doprowadziła do opracowania międzynarodowych norm postępowania, często nieformalnych, zwyczajowych przepisów. Z czasem działalność w internecie może doprowadzić do skodyfikowania zasad oraz opracowania międzynarodowych norm zachowań w celu ochrony funkcjonowania i dostępu do sieci.

iWar może być wykorzystywana przez narody do wywierania nacisku na słabszych przeciwników, przez podmioty niepaństwowe do ataków na

infrastrukturę państwa narodowego. Pojawia się perspektywa anarchii i piractwa, które będą służyć i podważać interesy władzy. Aby sprostać temu zagrożeniu, potrzeba zarówno środków zaradczych w zakresie bezpieczeństwa, jak i odpowiednich ram prawnych.

Choć szkody powodowane przez iWar są niekonwencjonalne, agresorzy mogą wykonywać szybkie uderzenia z dowolnego miejsca, praktycznie bez kosztów. Udostępnianie informacji na poziomie NATO pozwoli na wczesne ostrzeganie o podejrzanych działaniach i profilowanie możliwych ataków. Niektóre państwa NATO zaczęły chronić się przed zagrożeniami związanymi z wiekiem internetowym, ustanawiając krajowe komputerowe zespoły reagowania kryzysowego (CERT). Koordynacja CERT na poziomie NATO we współpracy z Unią Europejską byłaby ważnym krokiem w ograniczaniu skutków ataków iWar w perspektywie krótkoterminowej, tak aby np. w razie wykrycia ataku na czeską stronę internetową dokonanego przez francuskiego użytkownika czeski CERT mógł poprosić swojego francuskiego odpowiednika o odcięcie połączeń używanych do ataku. Niestety, ale wiele rządów jeszcze nie ustanowiło własnych zespołów tego rodzaju.

Pojawienie się iWar jest konsekwencją, która zdominowała pierwszą dekadę XXI w.: rozprzestrzenienie się internetu, wzmocnienie pozycji jednostek i względny spadek władzy państwa w celu kontrolowania infrastruktury komunikacyjnej. Dostępność materiałów instruktażowych online, odpowiedniego oprogramowania i wszechobecna łączność z internetem umożliwiają praktycznie każdemu sprawnemu i zaangażowanemu graczowi atakowanie odległych przeciwników czy wrogów. iWar jako forma wojny internetowej może wybuchać w wielu miejscach na całym świecie i przybierać na sile w miarę wzrostu wykorzystania infrastruktury konsumenckiej przez gospodarki, rządy i społeczności. Jej wpływ może być ogromny, a członkowie NATO będą mieli mało czasu na rozważenie skutecznej reakcji.

iWar szybko się rozwinęła i stanowi rosnące zagrożenie dla członków NATO, ponieważ wzmacnia pozycję społeczności internetowych i nieprzyjaznych rządów. Dopiero się okaże, czy iWar stanie się narzędziem aktorów państwowych, czy też aktorzy niższego szczebla utrzymają zdolność do wykorzystywania iWar przeciwko państwom narodowym.

Ponieważ międzynarodowy konsensus jest mało prawdopodobny, NATO musi podejść do tego problemu jako bezpośredniego zagrożenia i dążyć do wypracowania praktycznej współpracy obronnej.

Terminu iWar używa się, aby uwzględnić istotne cechy współczesnej wojny. Jej powstanie stanowi głębokie odejście od fundamentalnych założeń systemu westfalskiego, który określił znaczenie wojny państwowej na ponad 300 lat od zakończenia wojny trzydziestoletniej. Ta historyczna chwila oznaczała ważny punkt przejścia z epoki prywatnych konfliktów najemników do nowoczesnej wojny, w której walczących zaczęto postrzegać jako instrumenty państwa. iWar ma niespotykaną dotąd dynamikę i skłania do krytycznego namysłu nad wykorzystaniem technologii sieciowych i komunikacyjnych. Ten typ wojny może być prowadzony przez każdego, kto posiada połączenie z internetem, co daje jednostkom możliwość zastraszania i ataków na rządy i duże korporacje – jest to zasadnicza zmiana w dotychczasowej równowadze sił.

Olga Wasiuta

M. Andrejevic, *iSpy: Surveillance and Power in the Interactive Era*, University Press of Kansas, Lawrence 2007; B. Gertz, *iWar: War and Peace in the Information Age*, The Institute of World Politics, Simon & Schuster, Washington 2017; A. Kiyuna, L. Conyers, *Cyberwarfare Sourcebook*, Lulu.com, United States 2015; H. Pötzsch, *The Emergence of iWar: Changing Practices and Perceptions of Military Engagement in a Digital Era*, „New Media & Society" 2015, vol. 17, no. 1; J. Ryan, *iWar: A New Threat, Its Convenience and Our Increasing Vulnerability*, „NATO Review" 2007; tenże, *iWar: Pirates, States and the Internet*, 6.02.2008, OpenDemocracy.net (dostęp 10.03.2019); G.J. Voelz, *The Rise of iWar: Identity, Information, and the Individualization of Modern Warfare*, Strategic Studies Institute, United States Army War College Press, Carlisle 2015; O. Wasiuta, *iWar – bezprecedensowa forma wojny internetowej*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 2; taż, *iWar*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

IZRAELSKA KRAJOWA DYREKCJA CYBERNETYCZNA – jest odpowiedzialna za wszystkie aspekty cyberobrony w sferze cywilnej, od formułowania polityki i budowania siły technologicznej po obronę operacyjną

w → c y b e r p r z e s t r z e n i [t. 1]; działa na rzecz promowania zdolności krajowych w cyberprzestrzeni i poprawy gotowości Izraela do radzenia sobie z obecnymi i przyszłymi wyzwaniami w cyberprzestrzeni. Ma za zadanie usprawnić obronę infrastruktur narodowych o kluczowym znaczeniu dla kontynuacji normalnego życia w kraju i chronić je, w miarę możliwości, przed atakiem cybernetycznym, jednocześnie promując pozycję Izraela jako centrum rozwoju technologii informatycznych i zachęcając do współpracy między środowiskiem akademickim, przemysłem i sektorem prywatnym, organami rządowymi i → ś r o d o w i s k i e m b e z p i e c z e ń s t w a [t. 4].

Dyrekcja jest odpowiedzialna za 3 główne obszary zadań:

- postęp w obronie i budowanie siły narodowej w dziedzinie cybernetycznej;
- budowanie wiodącej roli Izraela w dziedzinie cybernetycznej;
- postępowe procesy wspierające 2 pierwsze zadania.

Państwo Izrael było jednym z pierwszych krajów na świecie, które dostrzegły znaczenie obrony swoich krytycznych systemów komputerowych. W 1997 r. uruchomiono projekt Tehila (rządowa infrastruktura w epoce internetowej – izraelski projekt e-GOV) w celu ochrony połączenia urzędów państwowych z internetem i zapewnienia → b e z p i e c z e ń s t w a [t. 1] państwa. W 2002 r. rząd Izraela postanowił określić obszary odpowiedzialności za ochronę systemów komputerowych w kraju, definiując krytyczną infrastrukturę komputerową i ustanawiając Agencję ds. Bezpieczeństwa Informacji (ISA) w ramach Szin Betu (izraelskiej agencji bezpieczeństwa wewnętrznego). Jej zadaniem było zapewnienie bezpieczeństwa podstawowym organom państwa powiązanym ze sobą sieciami komputerowymi, a także wprowadzanie regulacji i doradztwo podmiotom związanym z → i n f r a s t r u k t u r ą k r y t y c z n ą w dziedzinie bezpieczeństwa → i n f o r m a c j i. Utworzenie ISA stało się przełomowym wysiłkiem rządu na poziomie globalnym w dziedzinie cyberobrony.

Biorąc pod uwagę rozwój cyberprzestrzeni i ekspansję → z a g r o ż e ń [t. 4] w tym obszarze, w listopadzie 2010 r. premier Izraela B. Netanjahu polecił utworzenie specjalnego zespołu, który miał pracować nad uczynieniem kraju globalnym liderem bezpieczeństwa w cyberprzestrzeni. Komitet pod nazwą National Cyber Initiative był kierowany przez Krajową

Radę ds. Badań i Rozwoju Cywilnego i prof. I. Ben-Izraela. Powołana grupa składała się z przedstawicieli głównych organów związanych z cyberprzestrzenią Izraela (badania, rozwój, obrona itp.), tworzyło ją kilka podkomitetów, które badały elementy niezbędne do skutecznego działania Izraela w cyberprzestrzeni. Komisja zbadała możliwości Izraela w zakresie konkurowania w cyberprzestrzeni i przeanalizowała korzyści ekonomiczne dla kraju, pożytki dla środowiska akademickiego i → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1]. Wyznaczony cel został osiągnięty – Izrael jest dziś uznawany za drugie państwo na świecie (po USA) w rozwoju sektora cyberbezpieczeństwa.

Głównym zaleceniem wydanym w ramach National Cyber Initiative było utworzenie Krajowego Biura ds. Cyberbezpieczeństwa (Israel National Cyber Bureau, INCB) jako instytucji odpowiedzialnej za budowę → c y b e r b e z p i e c z e ń s t w a [t. 1] w państwie, służącej jako organ doradczy premierowi, rządowi i jego komisjom w tworzeniu krajowej polityki cybernetycznej. W szczególności INCB zostało wyznaczone do opracowania krajowej → s t r a t e g i i [t. 4] bezpieczeństwa cybernetycznego. Główne działania prezydium dotyczą ogólnej polityki rządu i działań w sferze cybernetycznej, zarówno cywilnych, jak i wojskowych. 7 sierpnia 2011 r. rząd Izraela zatwierdził utworzenie (pod auspicjami premiera) INCB jako instytucji, która będzie odpowiedzialna za budowę ekosystemu cyberbezpieczeństwa w państwie. Jej celem będzie zapewnienie bezpieczeństwa funkcjonowania państwa w cyberprzestrzeni w sferze niemilitarnej na poziomie krajowym i koordynacja działań różnych organów, zwiększenie ochrony infrastruktury krajowej przed → c y b e r a t a k a m i [t. 1].

Biuro ds. Cyberbezpieczeństwa było odpowiedzialne za formułowanie krajowej polityki i strategii w dziedzinie cyberprzestrzeni, rozwijanie krajowych procesów obronnych i ich regulowanie, rozwijanie krajowych zdolności w cyberprzestrzeni oraz ustanawianie współpracy międzynarodowej i dążenie do statusu wiodącego kraju w tej dziedzinie. Celem Biura jest ochrona izraelskiej przestrzeni cybernetycznej, a jego głównym zadaniem zarządzanie wszystkimi operacyjnymi działaniami obronnymi w cyberprzestrzeni i wzmacnianie odporności całej gospodarki w tym obszarze.

Biuro ds. Cyberbezpieczeństwa miało tworzyć właściwe standardy, regulacje i ekosystem cyberbezpieczeństwa, m.in. finansując badania i rozwój oraz szkolenia. Warto wspomnieć, że cyberbezpieczeństwo jest od wielu lat jednym z przedmiotów do wyboru na maturze w Izraelu, jest też nauczane jako przedmiot w szkole średniej.

W 2015 r. premier Netanjahu podjął decyzję o przeniesieniu struktur zarządzania bezpieczeństwem infrastruktury krytycznej z Szin Betu do utworzonego wówczas Narodowego Urzędu ds. Bezpieczeństwa (NCSA). Dzięki temu wyeliminowano kolejne pole konfliktu między strukturami bezpieczeństwa, centralizując zdolności operacyjne w jednym ręku. Rząd zdecydował również w lutym 2015 r. o ustanowieniu NCSA centralnym organem operacyjnym ds. cyberbezpieczeństwa w Izraelu, który będzie współpracował z INCB w ramach Krajowej Dyrekcji Cybernetycznej (National Cyber Directorate, NCD). Decyzja o prowadzeniu 2 niezależnych jednostek w ramach jednej dyrekcji została podjęta w tym czasie ze względu na potrzebę wzmocnienia 2 oddziałów – zarówno zajmującego się prowadzeniem polityki cyberbezpieczeństwa (INCB), jak i działalnością operacyjną (NCSA). Na czele NCD stanął jako dyrektor generalny Y. Unna (nazywany przez media Cyber Guru). Szef Biura ds. Cyberbezpieczeństwa został również mianowany szefem dyrekcji i był odpowiedzialny za zatwierdzanie planów pracy urzędu i jego budżetu.

W 2017 r. wszystkie działania technologiczne Biura zostały zintegrowane z jednostką ds. technologii cybernetycznych, która jest krajowym organem służącym do rozwijania możliwości i technologii cybernetycznych na poziomie krajowym. W tym samym czasie jednostka identyfikacji i aplikacji biometrycznych została zintegrowana z Biurem ds. Cyberprzestrzeni.

W ten sposób powstała jednolita struktura, odpowiedzialna za całościowe, zintegrowane i scentralizowane działania organów państwa na rzecz bezpieczeństwa i obrony w cyberprzestrzeni. Zmiana ta jest pomyślana jako kolejny ewolucyjny krok w ramach konsekwentnie realizowanego procesu rozwoju ekosystemu cyberbezpieczeństwa. Jego istotą jest konsolidacja wysiłków wszystkich uczestników systemu w ramach holistycznego modelu, z fundamentalną rolą nowej dyrekcji. Założeniem kierownictwa na najbliższe lata jest zapewnienie techniczno-operacyjnej dominacji w cyberprzestrzeni.

Izraelska Krajowa Dyrekcja Cybernetyczna jest fundamentalną podstawą, która określa zasady i sposoby działania oraz zarządzania w cywilnej cyberprzestrzeni. Zapewnia ramy i pogłębia współpracę w zakresie →kryzysów cybernetycznych ministerstw, organów regulacyjnych, państwowych organizacji bezpieczeństwa cybernetycznego i całej gospodarki. Służy również jako narzędzie, które organizacje mogą wykorzystać w budowaniu gotowości i planu zarządzania kryzysami cybernetycznymi – każda na swoim poziomie, w celu utrzymania ciągłości funkcjonalnej i biznesowej.

Olga Wasiuta

Background for the Establishment of the Bureau, PMO.gov.il (dostęp 18.04.2019); D. Benoliel, *Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, „North Carolina Journal Of Law & Technology" 2015, vol. 16, no. 3; O. Danino, *An Overview of Israeli Efforts in the Cybernetics Field*, Article III.21, March 2015; *Israel National Cyber Bureau (INCB)*, CyberSecurityIntelligence.com (dostęp 18.04.2019); *About*, gov.il (dostęp 18.04.2019); A. Kozłowski, *Pułkownik Małecki: System cyberbezpieczeństwa Izraela to dobry wzór do naśladowania*, 19.03.2018, CyberDefence24.pl (dostęp 18.04.2019); *Mission of the Bureau*, PMO.gov.il (dostęp 18.04.2019); *National Cyber Concept for Crisis Preparedness and Management*, 6.11.2018, gov.il (dostęp 18.04.2019); E. Toch, *Smart City Technologies in Israel: A Review of Cutting-Edge Technologies and Innovation Hubs*, Inter-American Development Bank, 2018; O. Wasiuta, *Izraelska Krajowa Dyrekcja Cybernetyczna*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

K

KASPERSKY LAB (ros. Лаборатория Касперского, Laboratorija Kasperskogo) – międzynarodowa, globalna firma z branży → c y b e r b e z p i e c z e ń s t w a [t. 1] z centralą w Moskwie; największy na świecie producent oprogramowania antywirusowego; zrzesza ponad 500 firm w ponad 60 krajach na całym świecie. Przedsiębiorstwo zostało założone w 1997 r. w Moskwie, zajmuje się dostarczaniem rozwiązań zapewniających → b e z p i e c z e ń s t w o [t. 1] systemów informatycznych. Nazwa przedsiębiorstwa pochodzi od nazwiska współzałożyciela – J. Kasperskiego. Oprogramowanie antywirusowe firma sprzedaje w 200 krajach, jej klientami jest 400 mln użytkowników. Jest to jedna z pięciu największych firm antywirusowych na świecie. W 2017 r. firma zarobiła 698 mln USD i zatrudniała ok. 4 tys. pracowników.

Firma jest największym w Europie producentem systemów chroniących przed szkodliwym i niechcianym oprogramowaniem, atakami → h a k e r ó w i spamem. Firma do niedawna była jednym z czterech wiodących światowych dostawców oprogramowania do zapewnienia bezpieczeństwa → i n f o r m a c j i. Grupa ma biura w Wielkiej Brytanii, Chinach, Francji, USA, Niemczech, Rumunii, Japonii, Korei Południowej, Holandii, Polsce i Kanadzie. Tylko w Chinach produkty firmy mają 100 mln użytkowników, a oprogramowanie jest popularne również w Niemczech i oczywiście w Rosji.

Kasperski – współzałożyciel i dyrektor generalny firmy – w 1987 r. został absolwentem Wydziału Matematycznego Wyższej Szkoły KGB (od 1992 r. przemianowanej na Instytut Kryptografii, Komunikacji i Informatyki Akademii FSB) w Moskwie, gdzie studiował matematykę, kryptografię i technologię komputerową, specjalizując się w inżynierii matematycznej. Od 1987 r. Kasperski rozpoczął pracę w interdyscyplinarnym instytucie badawczym przy Ministerstwie Obrony ZSRR. Choć Kasperski nigdy nie ukrywał, że jego firma współpracuje z Federalną Służbą Bezpieczeństwa (FSB), przez wiele lat utrzymywał, że jest ona strukturą, która zajmuje się wyłączenie ściganiem przestępców, tak jak amerykańskie FBI.

Kaspersky Lab jest od samego początku działalności podejrzewane o współpracę z Kremlem, chociaż ich relacje nigdy nie były jasne. Zachodni eksperci uważają, że nie ma możliwości, aby Kasperski został miliarderem bez porozumienia z rządem. Zgodnie z rosyjskim prawem każda firma musi otworzyć swoje linie komunikacyjne na żądanie władz. Od 2012 r. zaś Kaspersky Lab opuszczali menedżerowie wysokiego szczebla, na których miejsce zatrudniano osoby utrzymujące bliskie kontakty z rosyjskimi agencjami wojskowymi lub wywiadowczymi. Kongres USA, brytyjski → w y w i a d [t. 4] i rządy państw demokratycznych zadawały pytanie o to, do jakiego stopnia firma współpracuje z rosyjską FSB i czy FSB nie wykorzystuje „laboratorium" Kasperskiego do szpiegostwa.

W lipcu 2012 r. amerykański magazyn „Wired" opublikował artykuł dziennikarza N. Shahtmana, w którym Kasperski był oskarżony o współpracę z rosyjskimi → s ł u ż b a m i s p e c j a l n y m i [t. 4]. Sam Kasperski wszystkiemu zaprzeczył. Jednak w marcu 2015 r. agencja prasowa Bloomberg opublikowała artykuł, w którym C. Matlak, M. Riley i J. Robertson ponownie oskarżyli Kaspersky Lab o współpracę z rosyjskimi służbami wywiadowczymi na podstawie tego, że rosyjscy agenci zostali celowo umieszczeni wśród personelu firmy w 2012 r., a także jednostronnego, selektywnego przedstawiania źródeł → z a g r o ż e ń [t. 4] hakerskich w swoich raportach i dołączanych do nich mapach, jak również na podstawie osobistych związków Kasperskiego z KGB, a później z FSB. Według Bloomberga dzięki oprogramowaniu antywirusowemu firmy rosyjski wywiad może stale monitorować ok. 400 mln ludzi na całym świecie.

Do zwrócenia uwagi na Kaspersky Lab zmusiły państwa demokratyczne → a n e k s j a [t. 1] Krymu przez Rosję oraz wywieranie wpływu na wybory prezydenckie w USA w 2016 r.

Pierwszym państwem, które zabroniło wykorzystywania produktów firmy była Ukraina. 25 września 2015 r. Rada Ministrów Ukrainy poleciła Państwowej Służbie Komunikacji Specjalnej i Ochrony Informacji zakazać nabywania i wykorzystywania w organach władz państwowych oprogramowania Kaspersky Lab. Rada Bezpieczeństwa Narodowego i Obrony Ukrainy zakazała używania rosyjskiego oprogramowania poprzez wprowadzenie sankcji wobec rosyjskich firm. Używanie produktów firmy przez ukraińskie władze jest niebezpieczne, ponieważ może zdalnie blokować pracę komputerów i przesyłać dane do rosyjskich służb specjalnych. Eksperci odkryli, że korzystanie z programów antywirusowych Kaspersky Lab jest ryzykowne. Powodem tego jest w szczególności niekontrolowane przesyłanie informacji z komputera na serwery firmy z możliwością dalszego wykorzystania tych danych, w tym przekazanie informacji służbom specjalnym FR.

Jesienią 2017 r. firma Kaspersky Lab naraziła się na ryzyko utraty większej części lukratywnego rynku amerykańskiego, gdyż jej produkty zostały zakazane przez amerykańskie agencje rządowe. Powodem było podejrzenie o bliskie związki z rosyjską FSB, a w szczególności informacja, że firma celowo ukradła tajne dokumenty Agencji Bezpieczeństwa Narodowego USA (National Security Agency, NSA), mianowicie kody źródłowe stworzone przez amerykańskich specjalistów w dziedzinie wirusów komputerowych (zob. → z ł o ś l i w e o p r o g r a m o w a n i e [t. 4]), co spowodowało większe szkody dla reputacji amerykańskiego wywiadu i → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1] USA niż E. Snowden. Kasperski powiedział, że firma otrzymała pliki przypadkowo i natychmiast je usunęła. Firma utraciła znaczną część rynku amerykańskiego i zachodnioeuropejskiego, które przynosiły jej ponad 60% zysków ze sprzedaży. Firma stała się „toksyczna" nie tylko dlatego, że stosunki między USA a Rosją są napięte, lecz również dlatego, że rosyjska firma od ponad 7 lat zbiera informacje o → c y b e r b r o n i [t. 1] USA, Izraela i Wielkiej Brytanii oraz publikuje raporty analityczne na ten temat i oferuje metody ochrony.

Stworzone przez firmę oprogramowanie było używane przez prawie 20 amerykańskich agencji rządowych, w tym Departamentu Stanu, Ministerstwo Obrony Narodowej, Ministerstwo Sprawiedliwości, wojsko, marynarkę i siły powietrzne. Sytuacja zmieniła się pod koniec wiosny 2017 r., gdy ujawniono prawdopodobną ingerencję rosyjskich hakerów w wybory prezydenckie w USA.

11 maja 2017 r. w senackiej komisji ds. wywiadu zostało przeprowadzone posiedzenie, na którym byli obecni dyrektorzy FBI, CIA, NSA i innych agencji bezpieczeństwa USA i gdzie omawiano ingerencje Kremla w proces wyborów w Stanach Zjednoczonych. 5 lipca Senat USA zaproponował, aby nie uwzględniać zakupu produktów firmy Kaspersky Lab w budżecie obronnym na 2018 r. 11 lipca agencja Bloomberg opublikowała badanie dotyczące udziału firmy w rozwoju systemów zapobiegających atakom DDoS (ang. *distributed denial of service*) na zlecenie FSB. Już 12 lipca General Services Administration, urząd odpowiedzialny w szczególności za zamówienia publiczne, wyłączyła Kaspersky Lab z listy autoryzowanych dostawców dla amerykańskich agencji rządowych. Na początku września produkty Kaspersky Lab zniknęły z półek amerykańskich sklepów Best Buy.

13 września 2017 r. Departament Bezpieczeństwa Wewnętrznego USA opublikował dyrektywę nakazującą wszystkim instytucjom rządowym i związanym z nimi firmom przystąpić w ciągu 3 miesięcy do realizacji działań, które doprowadzą do rezygnacji z programów Kaspersky Lab, bo zdaniem resortu mogą one być wykorzystywane ze szkodą dla bezpieczeństwa narodowego USA i ułatwić →cyberataki [t. 1], z uwagi na podejrzenie współpracy firmy z rosyjskimi służbami wywiadowczymi. W odpowiedzi na decyzję amerykańskich władz Kaspersky Lab zapewnił, że firma nie wspiera żadnego rządu w próbach szpiegostwa cybernetycznego czy też agresywnej działalności w →cyberprzestrzeni [t. 1].

Senat USA 18 września 2017 r. przegłosował zakaz używania przez wszystkie amerykańskie agencje federalne produktów Kaspersky Lab z uwagi na powiązanie firmy z Kremlem, które stanowi zagrożenie dla bezpieczeństwa narodowego. Taka poprawka została wprowadzona do budżetu obronnego USA na 2018 r.

13 grudnia 2017 r. prezydent D. Trump podpisał ustawę zabraniającą korzystania z produktów firmy zarówno w sieciach cywilnych, jak

i wojskowych. „Sprawa przeciwko Kasperskiemu jest dobrze udokumentowana i głęboko poruszająca" – powiedziała senatorka demokratów J. Shaheen i dodała, że oprogramowanie firmy stanowi „poważne zagrożenie" dla bezpieczeństwa narodowego USA.

Motywacją decyzji były obawy powiązania niektórych przedstawicieli Kasperskiego z rosyjskim wywiadem oraz rosyjskie prawo pozwalające władzom rosyjskim na wymuszenie współpracy i udostępnienie danych, które są w rosyjskich sieciach. W ręce dziennikarzy Robinsona i Rileya trafiła wewnętrzna korespondencja współpracowników Kaspersky Lab. W jednym z listów sam Je. Kasperski podkreślił, że projekt jest rozwijany na „wielką prośbę ze strony Łubianki". W firmie potwierdzono autentyczność listów, ale nie zaangażowanie w działalność FSB – na tej podstawie dziennikarze doszli do wniosku, że firmę łączą z rosyjskimi służbami znacznie bliższe relacje, niż przyznaje się to publicznie.

Od 5 do 11 października 2017 r. „The Wall Street Journal" i „The New York Times" opublikowały serię artykułów, w których stwierdzono, że rosyjscy hakerzy uzyskali dostęp do akt NSA poprzez programy antywirusowe Kaspersky Lab. Natomiast izraelskie służby jeszcze na początku 2014 r. złamały zabezpieczenia wewnętrznej sieci firmy i zawiadomiły USA o tym, że oprogramowanie Kaspersky Lab jest wykorzystywane do pobierania informacji poufnych na podstawie słów kluczowych, takich jak *top secret*. Przedstawiciele wywiadu USA uznali to za akt szpiegostwa przeciwko Stanom Zjednoczonym i zasugerowali, że tajne materiały zostały skradzione przez Kaspersky Lab na korzyść interesów rosyjskich służb specjalnych.

Zdaniem byłych programistów Kaspersky Lab przez ostatnie ok. 10 lat kierownictwo rosyjskiej firmy zmuszało ich do tworzenia złośliwego kodu. Za jego pomocą chciano wyeliminować z rynku głównych konkurentów – innych producentów oprogramowania antywirusowego. Podczas instalacji oprogramowania firmy Kaspersky Lab infekowano zdrowe pliki systemowe fragmentami kodu, na które produkty konkurentów reagowały jak na złośliwe. W rezultacie programy antywirusowe usuwały lub blokowały te pliki, a system operacyjny komputera przestawał działać, zaś oskarżenia kierowano przeciwko innym firmom. W ten sposób eliminowano konkurentów takich jak Avast, AVG Technologies, Microsoft i wielu innych. Ich sprzedaż spadała, a Kaspersky Lab przejmował klientów, chociaż firma

nie ulepszała swoich produktów, a główne wysiłki skupiały się na przygotowaniu nowych złośliwych kodów.

Kaspersky Lab zaprzecza wszelkim zarzutom, utrzymując, że zapewniała FSB jedynie pomoc techniczną. Ponadto firma sprzeciwiła się decyzji rządu amerykańskiego i pozwała Departament Bezpieczeństwa Wewnętrznego USA do sądu. Kaspersky Lab zaprzecza, że jego oprogramowanie stanowi zagrożenie dla amerykańskich komputerów.

Pod koniec 2017 r. Kaspersky Lab musiał zamknąć swój oddział w Waszyngtonie (Kaspersky Government Security Solutions).

W latach 2017–2018 wiele państw zachodnich i firm zrezygnowało z produktów Kaspersky Lab. W grudniu 2017 r. antywirus Kaspersky został zablokowany przez agencje rządowe w Wielkiej Brytanii i na Litwie. Rząd Litwy oświadczył, że oprogramowanie Kaspersky Lab stanowi potencjalne zagrożenie dla bezpieczeństwa kraju i musi zostać zastąpione innym. Ministerstwo Obrony Litwy poinformowało, że oprogramowanie rosyjskiej firmy zostało wyeliminowane z najważniejszych systemów w kraju w ciągu miesiąca, choć wyznaczono na to czas do 90 dni. Litwa zakazała również tego oprogramowania na komputerach używanych do zarządzania →infrastrukturą krytyczną. Brytyjska agencja ds. bezpieczeństwa cybernetycznego również ostrzegła biura rządowe, aby zaprzestały korzystania z produktów Kaspersky Lab, obawiając się, że jest on pod kontrolą rosyjskiego rządu. Także Barclays – jeden z największych brytyjskich banków – zrezygnował z programów antywirusowych rosyjskiej firmy.

Władze Holandii postanowiły odmówić korzystania z Kaspersky Lab na początku 2018 r. Według agencji Reuters rezygnacja z tego oprogramowania jest zalecana również prywatnym firmom w kraju. Szef holenderskiego Ministerstwa Sprawiedliwości i Bezpieczeństwa F. Grapperhaus wysłał do parlamentu list, w którym stwierdził, że zaprzestanie używania produktów firmy jest środkiem zapobiegawczym i że trzeba je usunąć z powodu obaw związanych z bezpieczeństwem. „Rząd Rosji ma ma ofensywny program cybernetyczny wymierzony m.in. w interesy Holandii" – cytuje Reuters. Serwis Twitter zakazał reklam Kaspersky Lab w kwietniu 2018 r. W czerwcu 2018 r. Parlament Europejski również wezwał do rezygnacji z używania produktów firmy. Rezolucja zatwierdzona przez PE 13 czerwca 2018 r. wzywa do poprawy współpracy między

państwami w zakresie cyberbezpieczeństwa. Rezolucja została przyjęta 476 głosami za, przy 151 przeciw i 36 wstrzymujących się. Dokument określił podejście PE do europejskiej polityki obrony cybernetycznej. W rezolucji produkty Kaspersky Lab nazwano „szkodliwymi", posłowie wezwali również do badania oprogramowania wykorzystywanego w różnych instytucjach.

Sergiusz Wasiuta

D.F. Poindexter, *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests*, McFarland & Company, Jefferson 2018; N. Shachtman, *Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals*, 23.07.2012, Wired.com (dostęp 31.01.2019); M.J. Strauss, *Hostile Business and the Sovereign State: Privatized Governance, State Security and International Law*, Routledge, London–New York 2019; D. Volz, *Trump Signs into Law U.S. Government Ban on Kaspersky Lab Software*, 12.12.2017, Reuters.com (dostęp 31.01.2019); S. Wasiuta, *Kaspersky Lab*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *Кабмін заборонив органам влади співпрацювати з російською „Лабораторією Касперського"*, 25.09.2015, UkraNews.com (dostęp 31.01.2019); В. Шаньгин, *Информационная безопасность*, Litres, Москва 2017.

KATASTROFY NATURALNE (ang. *natural disasters*) – zdarzenia, które powstają na skutek działania żywiołów i które są przejawem naturalnych procesów zachodzących w atmosferze oraz wnętrzu Ziemi. Pojęcie katastrofy naturalnej zostało zdefiniowane w prawodawstwie polskim i zgodnie z art. 3 ust. 2 ustawy o stanie klęski żywiołowej określane jest jako:

> zdarzenie związane z działaniem sił natury, w szczególności wyładowania atmosferyczne, wstrząsy sejsmiczne, silne wiatry, intensywne opady atmosferyczne, długotrwałe występowanie ekstremalnych temperatur, osuwiska ziemi, pożary, susze, powodzie, zjawiska lodowe na rzekach i morzu oraz jeziorach i zbiornikach wodnych, masowe występowanie szkodników, chorób roślin lub zwierząt albo chorób zakaźnych ludzi albo też działanie innego żywiołu.

Zagrożenia naturalne w większości przypadków występują sezonowo lub są zależne od innych czynników naturalnych, a także anomalii meteorologicznych (pewnych odchyleń od przyjętych norm światowych). W konsekwencji zachodzących po sobie wydarzeń katastrofa naturalna może doprowadzić do klęski żywiołowej, która w ustawie została zdefiniowana jako:

> katastrofa naturalna lub awaria techniczna, których skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach, a pomoc i ochrona mogą być skutecznie podjęte tylko przy zastosowaniu nadzwyczajnych środków, we współdziałaniu różnych organów i instytucji oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem.

Wystąpienie katastrofy naturalnej może również doprowadzić do katastrofy ekologicznej, której definicja brzmi następująco:

> trwałe (nieodwracalne w naturalny sposób) uszkodzenie lub zniszczenie dużego obszaru środowiska przyrodniczego, wpływające negatywnie, bezpośrednio lub pośrednio, na zdrowie, często życie ludzi oraz zdarzenie wynikające z działalności nieantropogenicznej: katastrofa naturalna, klęska żywiołowa, katastrofa ekologiczna wywołana przez czynniki niezależne od człowieka.

Wśród katastrof naturalnych należy wyróżnić: trzęsienia ziemi i erupcje wulkanów, huragany, tornada, powodzie, lawiny oraz susze.

Trzęsienia ziemi to pochodzące z wnętrza Ziemi naturalne i krótkotrwałe wstrząsy pokrywy skalnej rozchodzące się w postaci fal sejsmicznych, obserwowalne we wnętrzu oraz na powierzchni ziemskiej. Intensywność i rozmiar zniszczeń mierzone są w skali Richtera (gdzie < 2 to wstrząsy rzadko odczuwalne przez człowieka, a ≥ 9 to wstrząsy, które w epicentrum katastrofy mogą doprowadzić do zburzenia budynków na wielu tysiącach km^2). Trzęsienia ziemi można podzielić ze względu na przyczynę występowania:

- antropogeniczne – ściśle powiązane z działalnością górniczą człowieka,
- zapadliskowe,
- tektoniczne – związane z przemieszczaniem się płyt tektonicznych ziemi,
- wulkaniczne.

Zjawisko trzęsienia ziemi występuje najczęściej na połączeniach płyt tektonicznych oraz należy do najbardziej tragicznych w skutkach. Przykładowo jak dotąd najsilniejsze trzęsienie ziemi miało miejsce w Chile w 1960 r. Odnotowana magnituda wstrząsów sięgnęła 9,5 w skali Richtera. Równie silnym zjawiskiem było wydarzenie na Alasce w 1964 r., gdzie siła wstrząsów osiągnęła 9,2 w skali Richtera. Wstrząsy mające epicentrum pod pokrywą ziemską mórz i oceanów mogą powodować tsunami. W 2004 r. żywioł tsunami powstały w rejonie Oceanu Indyjskiego spowodował śmierć co najmniej 230 tys. osób, a w 2010 silne trzęsienie ziemi na Haiti było przyczyną śmierci ok. 223 tys. osób. W 2011 r. u wybrzeży Honsiu w Japonii niszczycielska fala oceaniczna zniszczyła obiekty elektrowni atomowej Fukushima, doprowadzając tym samym do drugiej pod względem wielkości katastrofy technicznej elektrowni atomowej po wydarzeniach w Czarnobylu w 1986 r.

Polska natomiast jest rejonem asejsmicznym, jednakże również na tym terenie dochodzi do sporadycznych wstrząsów tektonicznych. Zazwyczaj są one powodowane szkodami górniczymi, związanymi z działalnością człowieka w litosferze ziemskiej. Tąpnięcia górnicze niejednokrotnie sięgają magnitudy 4 w skali Richtera.

Pod względem przyczyn występowania z trzęsieniami ziemi silnie związane są erupcje wulkanów. Żywiołowość wulkaniczna występuje w strefie tzw. pacyficznego pierścienia ognia, gdzie odnotowano ok. 460 aktywnych wulkanów, oraz w basenie Morza Śródziemnego. Przemieszczanie się płyt litosfery to subdukcja, której zwykle towarzyszy aktywność sejsmiczna i wulkaniczna na ziemi. Z uwagi na umiejscowienie stożków wulkanicznych na połączeniach płyt tektonicznych litosfery zaobserwowano zależność między wstrząsami ziemi a aktywnością wulkaniczną. Erupcje wulkanów zwykle występują jako gwałtowne zjawiska, których naukowcy nie są w stanie do końca przewidzieć. Istotnym przykładem kataklizmu był wybuch

wulkanu Montagne Pelée na Martynice 8 maja 1902 r, podczas którego zginęło ok. 30 tys. osób. Niemniej jednak najbardziej znany jest wybuch Wezuwiusza we Włoszech, którego erupcja w 79 r. zniszczyła 3 miasta: Pompeje, Herkulanum i Stabie. Rozwój technologiczny oraz narzędzia pomiarowe XXI w. pozwalają precyzyjnie określać aktywność sejsmiczną, której wyniki przyczyniają się w znacznym stopniu do alarmowania ludności o możliwie występujących zagrożeniach. Obecnie ok. 500 mln ludzi żyje w strefie aktywności tektonicznej i wulkanicznej.

Huragany, czyli cyklony tropikalne, to bardzo silne zjawiska atmosferyczne, które rozwijają się najczęściej w ciepłych strefach klimatycznych nad ciepłymi wodami Oceanu Spokojnego (nazywane tajfunami) oraz Oceanu Atlantyckiego. Łączące się ze sobą masy powietrza powodują porywiste wiatry o sile 120 km/h i większej. Rok 2017 został określony mianem roku huraganów, gdyż cyklony tropikalne stanowiły ok. 86% wszystkich szkód poniesionych w wyniku działania niszczycielskich sił komórek burzowych: Harvey, Irma, Maria oraz Ophelia. Pierwszym niszczycielskim czynnikiem huraganów jest wiatr, który w rekordowym stadium może osiągać 85 m/s (305 km/h). Drugim czynnikiem jest opad deszczu, trzecim zaś fale przypływowe, które wywołują powodzie. Intensywność cyklonów mierzy się za pomocą skali Saffira-Simpsona w kategoriach od 1 do 5 (gdzie 1 oznacza niewielki poziom zniszczeń, natomiast 5 – katastrofalny). Prognozy rejestrowane przez radary i dane satelitarne są wykorzystywane na całym świecie przez służby →obrony cywilnej [t. 3] do działań ochronnych przed siłą niszczycielskiego żywiołu. Najbardziej rzetelne →informacje oraz komunikaty pogodowe i alarmowe są prezentowane przez amerykańskie Narodowe Centrum Huraganów (National Hurricane Center and Central Pacific Hurricane Center).

Tornada to intensywne wiry powietrzne, sięgające zwykle powierzchni ziemi, związane z superkomórkami burzowymi, mieszającym się wzajemnie powietrzem zimnym oraz ciepłym na morzach, oceanach i lądach. Zwykle wewnątrz burzy obserwuje się typową chmurę w kształcie lejka lub igły. Wirujące masy powietrza najczęściej występują w Alei Tornad w USA w stanach Teksas, Oklahoma, Kansas, Iowa, Nebraska i Dakota Południowa. Trąby powietrzne spotykane są na wszystkich kontynentach z wyjątkiem Antarktydy. Rozmiary tornad są określane na podstawie

szerokości ścieżki zniszczeń w momencie wędrowania leja burzowego i wynoszą zwykle od kilku do kilkuset metrów (rzadko osiągają 1,5 km). Meteorolodzy określają intensywność występowania tornad za pomocą skali Fujity (od niewielkich zniszczeń – F0 – do niewyobrażalnie dużych – F5) oraz dwunastostopniowej skali TORRO (gdzie T0 to najniższy stopień, a T11 najwyższy). Sprzyjające warunki powstawania tornad to ośrodki burzowe. W przypadku silnej aktywności ośrodków burzowych może pojawić się skupienie kilku superkomórek generujących tornada, tak jak np. 31 maja 1981 r. w Ohio i Pensylwanii, gdzie zanotowano wystąpienie jednocześnie 41 trąb powietrznych.

Powodzie to klęska geograficzno-społeczna, powodująca zalanie terenów na skutek wystąpienia wód z koryt rzecznych. Zgodnie z Ustawą z dnia 20 lipca 2017 r. – Prawo wodne za powódź:

> rozumie się czasowe pokrycie przez wodę terenu, który w normalnych warunkach nie jest pokryty wodą, w szczególności wywołane przez wezbranie wody w ciekach naturalnych, zbiornikach wodnych, kanałach oraz od strony morza, z wyłączeniem pokrycia przez wodę terenu wywołanego przez wezbranie wody w systemach kanalizacyjnych.

Przyczyną występowania mogą być masowe opady deszczu (powodzie opadowe), topniejące pokrywy śnieżne (powodzie roztopowe) lub spiętrzenie wód morza na skutek silnie wiejących wiatrów w kierunku lądu (sztormowe spiętrzenie wody w rzekach). Najbardziej spektakularnym przykładem powodzi opadowej była „powódź tysiąclecia" w Europie Środkowo-Wschodniej, która była następstwem podwójnej fali opadów między 5 lipca i 6 sierpnia 1997 r. Oszacowano straty na ponad 4,5 mld USD, a śmierć poniosło 114 osób. Najwięcej ofiar śmiertelnych – 3,5 tys. osób – spowodowała powódź w Chinach i Korei Południowej w 1998 r. W 2010 r. roztopowa fala powodziowa w maju oraz czerwcowe opady doprowadziły do silnego wezbrania wód w Polsce – w Krakowie poziom Wisły osiągnął punkt szczytowy wody określony jako najwyższy od 160 lat.

Susze są zjawiskiem bardziej rozciągniętym w czasie. Zazwyczaj są skutkiem długo utrzymującego się wysokiego ciśnienia na danym obszarze,

które nie pozwala na uformowanie się chmur opadowych. Konsekwencją braku opadów mogą być pożary oraz brak dostępu do wody pitnej. W XXI w. sukcesywnie odnotowuje się wzrost temperatury na Ziemi, co jest skutkiem ocieplenia klimatu. Mylnie więc interpretowane jest pojęcie suszy, które jak dotąd było dedykowane tylko dla obszarów podzwrotnikowych, gdzie występowały pustynie. Obecnie przejawy pustynnienia obserwowane są na wszystkich szerokościach geograficznych z mniejszą lub większą częstotliwością, zwykle sezonową, krótkotrwałą. Największa dotąd susza na terenach zurbanizowanych była przyczyną wielkiego głodu w Indiach w latach 1876–1878, przynosząc śmierć blisko 5,5 mln osób.

Trudno przewidzieć występowanie oraz zasięg katastrof naturalnych. W rezultacie podejmowane działania na całym świecie mają na celu opracowanie systemu ostrzegania, który w precyzyjny i szybki sposób uprzedzi ludność o zbliżającym się zagrożeniu. Jedynym sposobem na zmniejszenie strat materialnych i osobowych generowanych przez katastrofy naturalne jest opracowanie sprawnego systemu prognozowania zjawisk. Najczęściej występującymi zagrożeniami naturalnymi są powodzie, najwięcej ofiar powodują trzęsienia ziemi, natomiast największe straty materialne ponoszone są w wyniku występowania huraganów i tornad w przypadku, gdy katastrofą są objęte obszary wysoce zurbanizowane. Dokładne poznanie miejsc szczególnie narażonych na zagrożenia naturalne pozwala oszacować ryzyko wystąpienia potencjalnego zagrożenia oraz zminimalizować straty powstające na skutek działania niszczycielskich sił. Ważnym elementem jest również budowa schronów oraz wzmocnienie budynków, w których ludność mogłaby się ukryć w przypadku wystąpienia → z a g r o ż e n i a [t. 4].

Justyna Rokitowska

D. Alexander, *Natural Disasters*, Routledge, New York 2001; D. Drzewiecki, *Zagrożenia naturalne w Polsce,* AON, Warszawa 2016; B. Hołyst, *Bezpieczeństwo gatunku ludzkiego*, Wydawnictwo Naukowe PWN, Warszawa 2016; M. Kolińska, *Zagrożenia pochodzenia naturalnego i zagrożenia ekologiczne*, [w:] *Zagrożenia kryzysowe*, G. Sobolewski (red.), AON, Warszawa 2011; S. Malinowski i in., *Klęski żywiołowe*, [w:] *Katastrofy i zagrożenia we współczesnym świecie*, W. Baturo (red.), Wydawnictwo Naukowe PWN, Warszawa 2008; P. Manikowski, *Katastrofy naturalne a katastrofy spowodowane działalnością człowieka – analiza porównawcza*,

[w:] *Katastrofy naturalne i cywilizacyjne. Zagrożenia cywilizacyjne początku XXI wieku*, M. Żuber (red.), Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki, Wrocław 2007; W. Mizerski, M. Graniczny, *Geozagrożenia*, Wydawnictwo Naukowe PWN, Warszawa 2017; J. Rokitowska, *Katastrofy naturalne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz. U. 2002, nr 62, poz. 558; Ustawa z dnia 20 lipca 2017 r. – Prawo wodne, Dz. U. 2017, poz. 1566; *Zagrożenia meteorologiczne i hydrologiczne*, Instytut Meteorologii i Gospodarki Wodnej, Państwowy Instytut Badawczy, Warszawa 2011; О. Васюта, С. Васюта, Г.Філіпчук, *Екологічна політика*: *національні та глобальні реалії*, „Чернівці: Зелена Буковина" 2004, № 4.

KATASTROFY TECHNICZNE (ang. *technical disasters*) – to zdarzenia nagłe, często tragiczne w skutkach (cierpienie ludności, śmierć oraz ogromne straty materialne i ekologiczne). Węższe pojęcia mające związek bezpośredni z definicją katastrof to:

- wypadek – zdarzenie, które dotknęło niewielka liczbę osób oraz ma mały zasięg oddziaływania, jednakże przy szczególnie tragicznych konsekwencjach może przybrać miano katastrofy;
- awaria – podobnie jak wypadek może przybrać gwałtowny przebieg, a nieopanowana w odpowiednim momencie może być przyczyną katastrofy.

Zgodnie z art. 3 ust. 3 ustawy o stanie klęski żywiołowej w prawodawstwie polskim pojęcie katastrofy technicznej zostało ujęte w definicji awarii technicznej jako:

> gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie obiektu budowlanego, urządzenia technicznego lub systemu urządzeń technicznych powodujące przerwę w ich używaniu lub utratę ich właściwości.

Pojęcie awarii technicznej zostało ściśle powiązane z definicją klęski żywiołowej, wyjaśnionej jako:

> katastrofa naturalna lub awaria techniczna, których skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich

rozmiarach albo środowisku na znacznych obszarach, a pomoc i ochrona mogą być skutecznie podjęte tylko przy zastosowaniu nadzwyczajnych środków, we współdziałaniu różnych organów i instytucji oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem.

Pojęcie katastrofy najczęściej kojarzone jest ze szczególnymi wydarzeniami, jakie mogły nastąpić wskutek bezpośredniej działalności człowieka. Zwykle subiektywne odczucia świadków lub uczestników zdarzenia pozwalają na odpowiednią klasyfikację wydarzeń, bowiem trudno jest określić, które czynniki – antropogeniczne czy naturalne – miały duży, a niejednokrotnie decydujący wpływ na powstanie poważnych skutków. Bardzo często różne czynniki wywołują jedną katastrofę techniczną, która może być przyporządkowana jednocześnie do różnych kategorii. W takim przypadku wyróżnia się kilka typów klasyfikacji, np. katastrofy techniczne:

- wywołane czynnikami środowiskowymi: morskie, powietrzne, lądowe i rzeczne;
- powstałe na skutek panujących okoliczności: wojenne i terrorystyczne;
- mające miejsce w konkretnej lokalizacji: przemysłowe, górnicze, budowlane (inżynieryjne) oraz transportowe (drogowe, kolejowe, lotnicze i kosmiczne);
- niosące rodzaj konkretnego → z a g r o ż e n i a [t. 4] dla środowiska naturalnego i społecznego: chemiczne, nuklearne, epidemiologiczne, biologiczne lub pożarowe oraz mające skutki w kategoriach gospodarczych, ekologicznych i humanitarnych.

Pożar to „samorzutne, niekontrolowane rozprzestrzenianie się ognia, zawsze powodujące straty". Przez wieki pożary stanowiły zagrożenie zarówno dla ludzi, jak i środowiska naturalnego. Pożary mogą być sklasyfikowane ze względu na wielkość: małe, średnie, duże oraz bardzo duże; a także ze względu na źródło powstania: naturalne i powodowane działalnością człowieka. Rozprzestrzenianie się ognia na skutek czynności antropogenicznych to zdarzenia m.in. takie jak wypalanie traw – umyślne podpalenia; zaprószenia ognia; instalacja elektryczna mająca wady i jej zwarcia

oraz skutki wypadków komunikacyjnych. Do najważniejszych wydarzeń z udziałem ognia w ostatnich latach można zaliczyć: pożar w metrze w 1995 r. w Azerbejdżanie w Baku – zginęło 291 osób; pożary w Kalifornii w 2008 r., gdzie bezpośrednią przyczyną było podpalenie, a śmierć poniosło 14 osób; pożar wieżowca Grenfell Tower w Londynie w 2017 r. – bezpośrednio w budynku zginęło 71 osób.

Katastrofa lotnicza, inaczej wypadek lotniczy, to:

> zdarzenie związane z eksploatacją statku powietrznego, które zaistniało od chwili, gdy jakakolwiek osoba weszła na jego pokład z zamiarem wykonania lotu, do momentu, gdy wszystkie osoby znajdujące się na pokładzie opuściły ten statek powietrzny, i podczas którego: 1) jakakolwiek osoba doznała obrażeń ze skutkiem śmiertelnym lub poważnego obrażenia ciała […], 2) statek powietrzny został uszkodzony lub nastąpiło zniszczenie jego konstrukcji, […] 3) statek powietrzny zaginął lub znajduje się w miejscu, do którego dostęp jest niemożliwy.

Transport lotniczy jest najszybszym i najbezpieczniejszym środkiem transportu, jednakże podczas eksploatacji, ujawnienia się wad konstrukcyjnych czy zdarzeń losowych może dojść do incydentów, wypadków i katastrof. Jedną z najbardziej tragicznych w skutkach była katastrofa na Teneryfie w 1997 r., największa pod względem liczby ofiar w lotnictwie cywilnym. Podczas kołowania zderzyły się 2 samoloty Boeing 747, powodując śmierć 583 osób. Przyczyną była awaria świateł pasa oraz zakłócenia w przekazywaniu sygnałów z wieży kontrolnej. Na terenie Polski miały miejsce 2 inne poważne w skutkach katastrofy lotnicze. Pierwsza, 14 marca 1980 r., spowodowała śmierć 87 osób będących na pokładzie. Rozbił się samolot LOT „Mikołaj Kopernik", a przyczyną katastrofy było zniszczenie turbiny silnika, co uniemożliwiło sterowanie maszyną. Drugi wypadek lotniczy miał miejsce w 1987 r. w Lesie Kabackim. Samolot LOT „Tadeusz Kościuszko" z powodu awarii silnika rozbił się ze 183 osobami na pokładzie. W obu przypadkach w polskich katastrofach brały udział samoloty produkcji ZSRR typu IŁ-62, które po incydentach były sukcesywnie wycofywane ze służby.

Pod koniec 2018 r. i na początku 2019 r. doszło do 2 podobnych do siebie katastrof nowoczesnych samolotów Boeing 737 MAX. Boeing 737 uchodzi za najpopularniejszy samolot pasażerski świata, do lotów na całym świecie dostarczono ok. 10,5 tys. maszyn tego typu. Obie katastrofy miały miejsce w podobnych okolicznościach, na nowych maszynach wprowadzonych do służby w 2017 r. Boeing 737 MAX różnił się od poprzedników (np. od Boeing 737 Next Generation) – przede wszystkim wprowadzono nowe generacje silników (stal tytanowa, wytrzymalsze na temperaturę łopatki), przeprojektowaniu uległy skrzydła, wzmocniono podwozie oraz przeprojektowano układy cyfrowe. To właśnie programy cyfrowe nowoczesnego układu do zapobiegania przeciągnięciom maszyny (Maneuvering Characteristics Augmentation System, MCAS) zapewniające utrzymanie stabilności siły nośnej, stabilności parametrów fizycznych pomiędzy wysokością, prędkością i kątem natarcia w przypadku wnoszenia oraz opadania samolotu, według wstępnych analiz parametrów feralnych lotów były prawdopodobną przyczyną obu katastrof.

Katastrofa budowlana to:

> niezamierzone, gwałtowne zniszczenie obiektu budowlanego lub jego części, a także konstrukcyjnych elementów rusztowań, elementów urządzeń formujących, ścianek szczelnych i obudowy wykopów.

Skutki katastrof budowlanych to przede wszystkim zagrożenie dla życia i zdrowia ludzi oraz straty materialne. Do podstawowych przyczyn tego rodzaju incydentów zalicza się przede wszystkim błędy przy projektowaniu obiektów, błędy powstałe podczas prac wykonawczych, a także nieodpowiednią eksploatację budynków czy zdarzenia losowe, np. wyładowania atmosferyczne, silne trzęsienia ziemi, osuwiska, pożary lub wybuchy gazów. Przykłady takich wydarzeń to np. zawalenie się 3 biurowców w Brazylii w 2012 r., w wyniku którego zginęło 17 osób, a 5 zostało uznanych za zaginione. Bezpośrednią przyczyną katastrofy była wada konstrukcyjna oraz brak zgody na prowadzenie prac remontowych budynku. W 2013 r. wibracje wielkich generatorów spowodowały katastrofę budowlaną w Bangladeszu, gdzie w wyniku zawalenia się 8-piętrowego

budynku śmierć poniosło 540 osób (Szabhar, Rana Plaza). Największa katastrofa budowlana w historii Polski miała miejsce w 2006 r. w Chorzowie. Podczas Międzynarodowych Targów Katowickich śmierć poniosło 65 osób. Na skutek zaniedbań w użytkowaniu (duża grubość pokrywy śnieżnej na dachu) oraz wad projektowych konstrukcja utraciła stabilność, a w konsekwencji hala uległa zniszczeniu.

Katastrofy drogowe to wypadki z dużą liczbą ofiar. Związane ściśle z przemieszczaniem się ludności oraz towarów, gdzie najczęstszymi przyczynami zdarzeń tego rodzaju jest niedostosowanie prędkości do warunków oraz nieprzestrzeganie przepisów drogowych. We Francji w miejscowości Grenoble w 2007 r. w wyniku nieprzestrzegania przepisów oraz braku zgody na podróżowanie tą drogą autobus z polskimi pielgrzymami uderzył w barierę → b e z p i e c z e ń s t w a [t. 1] na zakręcie i stoczył się w dolinę rzeki. W rezultacie zginęło 26 osób. Najtragiczniejszą katastrofą drogową w Polsce był wypadek autokaru w Gdańsku w 1994 r. Bezpośrednią przyczyną zdarzenia było pęknięcie opony w pojeździe, po którym kierowca nie opanował nadmiernie przeciążonej maszyny, a autobus uderzył czołowo w drzewo. W rezultacie śmierć poniosły 32 osoby.

Katastrofy kolejowe, podobnie jak katastrofy drogowe i lotnicze, są związane z przemieszczaniem się ludności i towarów. Mogą być powodowane eksploatowaniem składów, niewłaściwym użytkowaniem, wadami technicznymi lub zdarzeniami losowymi. Najgroźniejsze skutki tych wydarzeń to przede wszystkim śmierć pasażerów, zniszczenia infrastruktury przyrodniczej, trakcji oraz towarzyszące im incydenty, np. wydostanie się materiałów mogących zanieczyścić środowisko (materiałów łatwopalnych, skażonych, promieniotwórczych lub gazów). Do najbardziej tragicznej w skutkach sytuacji doszło w 2004 r. na zachodnim wybrzeżu Sri Lanki. Fala tsunami całkowicie zniszczyła pociąg relacji Kolombo – Galla. Liczba pasażerów nie jest do końca znana, lecz przyjęto, że większość z 1,7 tys. podróżnych poniosła śmierć. Innym przykładem jest katastrofa pod Szczekocinami w Polsce w 2012 r. Czynnikiem sprawczym był błąd ludzki, w wyniku nieprawidłowego ustawienia zwrotnicy 2 składy jadące z naprzeciwka zostały skierowane na ten sam tor. Czołowe zderzenie pociągów relacji Przemyśl – Warszawa i Warszawa – Kraków doprowadziło do śmierci 16 osób.

Katastrofy przemysłowe powstają w sposób nagły, ale główne przyczyny zwykle są zależne od człowieka. Obszarem, który jest szczególnie narażony na wystąpienie takich awarii, są aglomeracje miejskie. Wraz z rozwojem technicznym nastąpiło zwiększenie gromadzenia oraz przewożenia materiałów niebezpiecznych do funkcjonowania fabryk. W przypadku uszkodzenia obiektów może dojść do uwolnienia się toksycznie niebezpiecznych substancji (chemicznych, biologicznych lub promieniotwórczych). Katastrofa może doprowadzić do skażenia terenów, śmierci lub silnego zatrucia osób oraz zwierząt przebywających w rejonie objętym zanieczyszczeniem. Awarie są następstwem niewłaściwego użytkowania instalacji i substancji przemysłowych, złego składowania odpadów oraz złego stanu technicznego urządzeń. Spośród najważniejszych katastrof tego typu można wymienić wybuch platformy wiertniczej BP Deepwater Horizon w 2010 r. w Zatoce Meksykańskiej w USA, w którym zginęło 11 osób. Wypadek doprowadził do niekontrolowanego wycieku ropy ze złoża Macondo. Bezpośrednią przyczyną awarii było niedostosowanie się do zaleceń obejmujących wzmocnienia odwiertu. Zastosowano 6 z 21 wskazanych obręczy wzmacniających.

Z przemysłem ściśle powiązane są katastrofy nuklearne. Promieniowanie jonizujące ma wpływ na środowisko naturalne i życie człowieka nie tylko w przypadku pracy elektrowni jądrowych. Społeczności mogą być narażone na zagrożenia z tym związane podczas eksploatowania złóż uranu, produkcji paliwa atomowego, jego uzdatniania, użytkowania, przewożenia czy składowania odpadów promieniotwórczych i ich pochodnych. Awaria nuklearna jest rzadkim zjawiskiem, definiowanym zamiennie z pojęciem wypadku lub incydentu. Według Ustawy z dnia 29 listopada 2000 roku – Prawo atomowe wypadkiem jądrowym nazywa się „jakiekolwiek zdarzenie lub serię zdarzeń mających to samo źródło pochodzenia, które powodują szkodę jądrową lub poważne i bezpośrednie zagrożenie jej powstaniem". Szkody jądrowe to skutki działania promieniowania jonizującego, mającego niekorzystny wpływ na otoczenie, ludzi, posiadane mienie oraz środowisko naturalne. Aby sklasyfikować wydarzenia mające związek z awariami i katastrofami nuklearnymi, Międzynarodowa Agencja Energii Atomowej (MAEA) oraz Agencja Energii Jądrowej (Nuclear Energy Agency, NEA) przy Organizacji Współpracy Gospodarczej

i Rozwoju (Organisation for Economic Co-operation and Development, OECD) stworzyły międzynarodową skalę zdarzeń jądrowych i radiologicznych (International Nuclear and Radiological Event Scale, INES). Siedmiostopniowa skala umożliwia szybką interpretację zagrożeń oraz merytoryczne i szybkie informowanie społeczeństwa o zaistniałych skutkach. Niższe poziomy skali (1–3) zostały nazwane incydentami, a wyższe (4–7) wypadkami lub awariami:

- Anomalia, chwilowa niesprawność urządzenia.
- Incydent, naruszenie niektórych barier bezpieczeństwa (np. w 1944 r. w Tennessee w USA doszło do wybuchu urządzenia służącego do wzbogacania uranu, w wyniku którego śmierć poniosły 2 osoby).
- Poważny incydent, poważne skutki zdrowotne dla pracowników.
- Awaria bez znaczenia dla otoczenia poza obiektem.
- Awaria z zagrożeniem występującym poza obiektem, działania mają na celu eliminację skutków zdrowotnych (np. podczas eksploatacji paliwa jądrowego w 1957 r. w miejscowości Windscale w Wielkiej Brytanii i próby pozyskiwania uranu spłonęło ok. 11 ton cząsteczek promieniotwórczych. Sprawę próbowano zatuszować, gdyż całe zdarzenie miało miejsce 8 dni po utworzeniu Międzynarodowej Agencji Energii Atomowej. Aby uniknąć konsekwencji, nazwa zakładu została zmieniona na Sellafield, a pod koniec roku zdecydowano się wyłączyć oba pracujące reaktory, gdyż obawiano się, że władze będą zakazywać prób uzdatniania uranu. Kategorię piątą skali wypadków jądrowych uzyskała również katastrofa w Three Mile Island w USA w 1979 r. Na skutek stopienia reaktora do gleby dostało się ok. 185 m^3 skażonej wody, a ok. 200 tys. ludzi zostało ewakuowanych. Tą samą klasyfikacją została objęta awaria reaktora prądotwórczego, który służył przy budowie łodzi podwodnej w 1970 r. w Niżnym Nowogrodzie. W rezultacie napromieniowanych zostało ok. 1 tys. pracowników, przez kolejne 25 lat utrzymywano w tajemnicy całe zdarzenie. Wskutek choroby popromiennej do 2005 r. śmierć poniosło ok. 620 pracowników.
- Poważna awaria – działania awaryjne na lokalnych terenach w celu ograniczenia skutków zdrowotnych, np. awaria z 1957 r. w elektrowni w pobliżu Czelabińska. Podczas pracy reaktora, na skutek awarii

systemów chłodzących, doszło do wybuchu zbiornika, w którym przechowywano odpady promieniotwórcze. Siła eksplozji była równa wybuchowi ok. 100 ton trotylu. Radioaktywna chmura objęła teren ok. 20 tys. km². Wiele → i n f o r m a c j i o awarii zostało utajnionych przez rząd ZSRR. Ewakuowano ludność z 22 wiosek, które zostały napromieniowane, a nazwy miejscowości zostały wykreślone z radzieckich map. Do wiadomości publicznej nie podano informacji o zaistniałym wypadku.

- Wielka awaria – ewakuacje, wyznaczenie stref, w których życie i przebywanie ludności nie jest możliwe, śmiertelność ludności, skażenie środowiska na ogromnym obszarze.

Zdarzenia niemające znaczenia dla bezpieczeństwa zostały nazwane odstępstwami i umieszczone poza skalą jako poziom 0. Skala INES dotyczy wszystkich obiektów jądrowych, zakładów produkcji i miejsc przetrzymywania paliwa jądrowego, składowisk odpadów promieniotwórczych oraz przede wszystkim elektrowni jądrowych.

Najpoważniejszymi awariami w dziejach energetyki jądrowej były katastrofa w Czarnobylu w 1986 r. oraz katastrofa w Fukushimie w 2011 r. Oba zdarzenia zostały zakwalifikowane jako wielkie awarie, czyli 7. stopień w skali INES. Ich skutkiem było uwolnienie dużej ilości materiału radioaktywnego poza obiekt przemysłowy oraz konsekwencje zdrowotne wywołane promieniowaniem przenikliwym na dużym obszarze. Przyczyny katastrofy w Czarnobylu to przede wszystkim wady techniczne konstrukcji reaktora oraz błędy w użytkowaniu i brawura przy przeprowadzaniu testu bezpieczeństwa. Silne wybuchy w elektrowni oraz pożar dachu spowodowały uwolnienie do atmosfery ok. 190 tys. ton materiału promieniotwórczego, powodując śmierć wielu tysięcy osób oraz skażenie terenu w bezpośrednim obszarze, a także wysiedlenie ludności w promieniu 30 km od miejsca zdarzenia. Na skutek wysokiego promieniowania jonizującego ewakuowano pobliskie miasto Prypeć. Radioaktywna chmura przemieszczała się nad Europą, okrążyła świat dwukrotnie.

Natomiast przyczyną awarii japońskiej elektrowni Fukushima było podziemne trzęsienie ziemi na Oceanie Spokojnym, które spowodowało falę tsunami. Fala z ogromną siłą uderzyła w linię brzegową i elektrownię,

zalewając nisko położone generatory oraz zbiorniki paliwa nuklearnego. W wyniku awarii do oceanu zostały uwolnione duże ilości skażonej wody, które wcześniej chłodziły rdzeń reaktora. Stopieniu uległy rdzenie reaktorów, które wydzieliły substancje promieniotwórcze bezpośrednio wydostające się do atmosfery.

Wydarzenia, które przyniosły podobne konsekwencje, klasyfikowane między 3. a 5. stopniem w skali INES, to wypadki takie jak:

- w 1967 r. w ZSRR przeniesienie przez wiatr skażonych osadów, których pył napromieniował ok. 1,8 tys. km² terenu zamieszkałego przez 40 tys. ludzi;
- w 1969 r. w Szwajcarii doszło do wycieku 50 kg paliwa nuklearnego;
- gaszenie pożaru w elektrowni Browns Ferry w Alabamie w USA w 1975 r., którego główną przyczyną było złe zachowanie pracownika usiłującego naprawić usterkę. Zamiast zastępczego oświetlenia użyto zwykłej świeczki, która doprowadziła do pożaru. Błąd kosztował 10 mln USD oraz dodatkowe koszty poniesione w wyniku wyłączenia generatorów na ponad rok;
- skażenie i napromieniowanie ludności w miejscowości Goiânii w Brazylii w 1987 r.

Awarie jądrowe związane są również ze składowaniem odpadów promieniotwórczych z przetworzonego paliwa nuklearnego. Globalnym problemem okazał się sam proces utylizacji substancji pochodnych pierwiastków radioaktywnych. Obecnie materiały nisko- i średnioaktywne są umieszczane głęboko pod ziemią, stwarzając zagrożenie dla środowiska naturalnego. Nieodpowiednio zabezpieczone pojemniki mogą doprowadzić do zanieczyszczenia wód gruntowych i gleby, a w konsekwencji do zatrucia ludności. Do 1993 r. zużyty materiał promieniotwórczy zamykany w odpowiednich pojemnikach zatapiano w głębinach mórz i oceanów. W konwencji londyńskiej zakazano stosowania tej metody ze względów ekologicznych oraz ochrony środowiska wodnego. Do popularnych metod przechowywania pozostałości wypalonego paliwa jądrowego zalicza się: prasowanie stałych materiałów oraz gromadzenie cieczy w odpowiednich zbiornikach umieszczanych w formacjach skalnych. Jednakże nawet minimalne uszkodzenie betonowych bloków niesie katastrofalne skutki dla środowiska naturalnego. Na świecie nie

dokonano jeszcze przełomowego odkrycia dotyczącego skutecznej utylizacji materiałów promieniotwórczych. Stosuje się najmniej inwazyjne dla środowiska i człowieka metody składowania odpadów, jednakże nie są one w pełni bezpieczne. Aby zminimalizować prawdopodobieństwo wystąpienia wielkich awarii, MAEA wydała odpowiednie wytyczne dotyczące oznakowania materiałów nuklearnych, ich przewożenia oraz składowania. Odpowiednie zalecenia zostały zaakceptowane przez ONZ na potrzeby transportu lotniczego, morskiego i drogowego.

Za najbardziej powszechnie występujące zagrożenia uznaje się pożary, następnie użytkowanie środków toksycznych przy procesach produkcyjnych, składowanie substancji promieniotwórczych na dnach mórz, oceanów i w formacjach skalnych oraz transport substancji niebezpiecznych przez gęsto zaludnione obszary. Zagrożeniem dla życia ludności są również katastrofy budowlane, powodowane zarówno przez działalność antropogeniczną, jak i przez czynniki naturalne (np. huragany). Wspomniane wypadki i incydenty w transporcie lądowym czy powietrznym są także czynnikiem degradacyjnym, a z uwagi na dużą liczbę poszkodowanych mogą być klasyfikowane jako katastrofy komunikacyjne. Każdy z wymienionych rodzajów katastrof może skutkować śmiercią wielu osób oraz przyczynić się do skażenia środowiska naturalnego.

Przemysł jądrowy jest powszechnie uważany za najbezpieczniejszą formę produkcji energii elektrycznej. Niezachowanie odpowiedniej → kultury bezpieczeństwa, zaniechanie przestrzegania podstawowych procedur eksploatacji, użytkowania i utylizacji materiałów nuklearnych może przyczynić się do awarii o poważnych skutkach dla środowiska naturalnego oraz społeczności międzynarodowych. Polityka działania powinna opierać się na zadaniach polegających na zapewnieniu bezpieczeństwa pracownikom i społeczności na całym świecie. W świetle zaistniałych awarii i incydentów nuklearnych należy przestrzegać zaawansowanych procedur zapewniających bezpieczne i higieniczne warunki pracy oraz dbać o urządzenia wysokiego ryzyka, minimalizując prawdopodobieństwo wystąpienia wypadków jądrowych.

Wraz z postępem technologicznym stwarza się czynniki, które ograniczają skutki występowania wypadków, oraz tworzy się systemy odpowiedzialne za bezpieczeństwo w pracy w obszarach najbardziej zagrożonych,

a przestrzeganie przez pracowników zasad bezpieczeństwa w zakładach produkcyjnych zmniejsza ryzyko wystąpienia awarii.

Justyna Rokitowska

J. Bolałek, *Ochrona środowiska morskiego. Od teorii do praktyki*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk–Sopot 2016; M. Borysewicz, *Katastrofy przemysłowe*, Centralny Instytut Ochrony Pracy, Warszawa 1997; J. Buczko, *Bezpieczeństwo w komunikacji publicznej i transporcie*, Państwowa Wyższa Szkoła Zawodowa im. Witelona, Legnica 2017; J.P. Christodouleas, R.D. Forrest, C.G. Ainsley i in., *Short-Term and Long-Term Health Risks of Nuclear-Power-Plant Accidents*, „The New England Journal of Medicine" 2011, no. 24 (364); G. Jezierski, *Energia jądrowa wczoraj i dziś*, Wydawnictwa Naukowo-Techniczne, Warszawa 2005; M. Kolińska, M. Witecka, *Zagrożenia wywołane działalnością człowieka i awarie techniczne*, [w:] *Zagrożenia kryzysowe*, G. Sobolewski (red.), AON, Warszawa 2011; L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, European Association for Security, Kraków 2016; M. Kowalski, *Katastrofy antropogeniczne*, [w:] *Katastrofy i zagrożenia we współczesnym świecie*, W. Baturo (red.), Wydawnictwo Naukowe PWN, Warszawa 2008; J. Kubowski, *Elektrownie jądrowe*, Wydawnictwo WNT, Warszawa 2013; tenże, *Nowoczesne elektrownie jądrowe – fizyka, budowa, technologia, bezpieczeństwo, ekologia, koszty*, Wydawnictwa Naukowo-Techniczne, Warszawa 2010; J. Rokitowska, *Awarie nuklearne*; *Katastrofy techniczne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Obawy społeczeństwa a bezpieczeństwo elektrowni atomowych*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civili IV" 2014, nr 166; J. Rokitowska, A. Wasiuta, *Ekonomiczne i społeczne aspekty bezpieczeństwa sektora energetycznego w kontekście zrównoważonego rozwoju*, Wydawnictwo Uniwersytetu Pedagogicznego im. KEN w Krakowie, Kraków 2019; J. Składzień, A. Ziębik, *Perspektywy rozwoju energetyki jądrowej w Polsce*, „Studia BAS" 2010, nr 1; A. Strupczewski, *Analiza korzyści i zagrożeń związanych z różnymi źródłami energii elektrycznej*, Polskie Towarzystwo Nukleoniczne, Warszawa 1999; tenże, *Awarie reaktorowe a bezpieczeństwo energetyki jądrowej*, Wydawnictwa Naukowo-Techniczne, Warszawa 1990; Ustawa z dnia 7 lipca 1994 r. – Prawo budowlane, Dz. U. 1994, nr 89, poz. 414; Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz. U. 2002, nr 62, poz. 558; Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe, Dz. U. 2001, nr 3, poz. 18; Ustawa z dnia 3 lipca 2002 r. – Prawo lotnicze, Dz. U. 2002, nr 130, poz. 1112; J. Waluszko, *Protesty przeciwko budowie elektrowni jądrowej Żarnowiec w latach 1985–1990*, Wydawnictwo Instytutu Pamięci Narodowej, Gdańsk 2013.

KOMUNIKACJA STRATEGICZNA (ang. *strategic communications*) – planowane i przemyślane działania komunikacyjne, nastawione na osiąganie długoterminowych interesów konkretnego podmiotu. Komunikacja strategiczna (KS) pozwala dotrzeć do konkretnych grup docelowych, aby wypromować własne przekonanie. Niejednokrotnie bywa słusznie utożsamiana z komunikacją zewnętrzną, a zatem z nową odsłoną *public relations*. KS odnosi się przede wszystkim do integracji działań komunikacyjnych. W przypadku państwowej KS daje się zauważyć swoisty dualizm, bowiem możemy wówczas mówić o komunikacji wewnętrznej (wobec własnych obywateli oraz pomiędzy instytucjami administracji publicznej), a także komunikacji zewnętrznej (odnoszącej się do innych państw i organizacji międzynarodowych). W ciągu ostatnich kilkunastu lat stała się przedmiotem burzliwych dyskusji w kręgach politycznych, naukowych oraz biznesowych.

W polskim porządku prawnym nie funkcjonuje spójna i zrozumiała definicja określająca specyfikę KS. Niemniej jednak na uwagę zasługuje projekt doktryny bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej z 24 lipca 2015 r., w którym za KS uznano:

> syntezę działań informacyjnych danego podmiotu strategicznego (np. państwa, sojuszu, koalicji) ukierunkowanych na kształtowanie poglądów, ocen, opinii itp. oraz decyzji innych podmiotów z otoczenia strategicznego (podległych, współdziałających, neutralnych, konkurujących, wrogich) w sposób korzystny dla własnych interesów strategicznych.

W zasadzie jedynym aktem prawnym, którego przepisy w sposób pośredni dotyczą KS, jest Decyzja Nr 284/MON Ministra Obrony Narodowej z dnia 8 lipca 2014 r. w sprawie powołania zespołu do spraw opracowania i wdrożenia systemu KS w resorcie → o b r o n y n a r o d o w e j [t. 3]. W dokumencie odnajdujemy tylko zapewnienie, że tworzony system KS będzie bazował na zasadach i procedurach właściwych dla → N A T O [t. 3].

Brak jasnej definicji KS dostosowanej do specyfiki, krajowego kontekstu oraz aktualnych możliwości państwa nie oznacza, że w Polsce nie stała się ona przedmiotem zainteresowań różnych kręgów politycznych,

naukowych itp. Jednak realizacja zadań z pogranicza KS ogranicza się w zasadzie do pojedynczych podmiotów działających w ramach poszczególnych resortów. Niestety daje się zauważyć brak wspólnych działań w tym zakresie na poziomie ogólnokrajowym, nie opracowano również żadnej →strategii [t. 4] ani procedur, na bazie których można byłoby koordynować działania we wszystkich sferach aktywności państwa. W konsekwencji polski system KS cechuje skomplikowana struktura i chaos kompetencyjny. Opisany stan może stać się przyczyną trudności w dotarciu do grup docelowych oraz uniemożliwić prowadzenie działań defensywnych. Jest to szczególnie istotne w obliczu licznych →zagrożeń [t. 4] polegających na →dezinformacji.

Za KS w ramach obronności odpowiada resort obrony narodowej, mający do dyspozycji Centrum Operacyjne Ministra Obrony Narodowej. Centrum zarządza procesem komunikacji społecznej – zewnętrznej i wewnętrznej ministerstwa – z wyłączeniem informowania o nastrojach w środowisku wojskowym. Zajmuje się również prowadzeniem spraw w zakresie badań społecznych dotyczących obronności. Centrum kształtuje wizerunek resortu oraz bada społeczne nastroje w kontekście prowadzonych przez ministerstwo działań.

Natomiast w Ministerstwie Spraw Zagranicznych, w Biurze Rzecznika Prasowego funkcjonuje odrębny referat ds. komunikacji strategicznej, który należy do sieci europejskiej współpracy w ramach systemu wczesnego ostrzegania Rapid Alert System (system do wymiany danych o zagrożeniach w →przestrzeni informacyjnej [t. 3], działający od marca 2019 r.). Ideą powołania referatu jest reagowanie na przypadki dezinformacji w obszarze polskiej polityki zagranicznej. W resorcie działa także Departament Dyplomacji Publicznej i Kulturalnej, zajmujący się działalnością strategiczną, koordynacyjną i wykonawczą w odniesieniu do kształtowania postaw społecznych i opinii społeczeństw innych państw na temat polskiej →racji stanu [t. 3] i priorytetów polskiej polityki zagranicznej.

Ze względu na nasilające się agresywne w skutkach zachowania Federacji Rosyjskiej w przestrzeni informacyjnej w działania z zakresu KS zaczęli angażować się przedstawiciele →Biura Bezpieczeństwa Narodowego [t. 1], a także Ministerstwa Spraw Wewnętrznych

i Administracji. Natomiast →operacje psychologiczne [t. 3] i informacyjne stały się domeną komórek struktury wojskowej. Oddział Komunikacji Strategicznej funkcjonuje nawet w Wojskach Obrony Terytorialnej, podejmując działania antydezinformacyjne. Na uwagę zasługuje także aktywność Polski w grupie zadaniowej East StratCom, funkcjonującej od 2015 r. w ramach Europejskiej Służby Działań Zewnętrznych. Grupa zajmuje się wykrywaniem przypadków dezinformacji oraz walką z nimi w państwach członkowskich UE oraz Partnerstwa Wschodniego.

KS jest domeną nie tylko nauk o mediach i komunikacji społecznej, ale termin ten jest również charakterystyczny dla nauk o zarządzaniu i jakości oraz →nauk o bezpieczeństwie [t. 3] i obronności. Jako zagadnienie interdyscyplinarne wymaga szczególnego podejścia z uwzględnieniem specyfiki dyscypliny naukowej, w której się pojawia. Nauki o mediach i komunikacji medialnej w kontekście KS podkreślają znaczenie mediów w procesie komunikowania i komunikowania się. Wraz z postępującą ewolucją cywilizacji i upowszechnieniem się swobodnego dostępu do →informacji media uzyskały monopol na manipulowanie informacjami, decydentami politycznymi, a także całymi społeczeństwami. W kontekście →wojny informacyjnej [t. 4] media stały się efektywnym narzędziem wroga w operacjach psychologicznych. Za pośrednictwem przekazu medialnego do przeciwnika dociera konkretna, spersonifikowana informacja, odwołująca się do emocji związanych z →bezpieczeństwem [t. 1] własnym oraz zdrowiem i życiem rodziny. W KS charakterystycznej dla nauk o mediach i komunikacji społecznej eksperci *public relations* oraz media kreują i promują wizerunek lidera danego państwa, przesądzając tym samym o sile danego podmiotu państwowego.

Nauki o zarządzaniu i jakości traktują KS jako konkretną →politykę informacyjną [t. 3] firmy lub podmiotu ukierunkowaną na kształtowanie przekonań, ocen, poglądów, a także decyzji innych podmiotów, w sposób uwzględniający korzyści dla własnych interesów. KS zapewnia prognozowanie kosztów i potencjalnych rezultatów działań wraz z osiągnięciem postawionych celów. Tak rozumiana KS ułatwia zrozumienie pomiędzy nadawcą a odbiorcą konkretnych informacji. Należy również zwrócić uwagę na sposób komunikowania z otoczeniem przedsiębiorstwa – spójna komunikacja danego przedsiębiorstwa ze środowiskiem,

w którym funkcjonuje, wpływa na strategię marki, kreuje wizerunek firmy oraz tworzy charakterystyczną kulturę organizacyjną. Strategiczne planowanie komunikacji warunkuje pożądane działania, dlatego tak istotne jest tworzenie dokumentu strategicznego, który określa dalszy rozwój przedsiębiorstwa.

Z perspektywy nauk o bezpieczeństwie i obronności KS stanowi syntezę działań informacyjnych podmiotu strategicznego (państwa, sojuszu lub koalicji), nastawionych przede wszystkim na kreowanie poglądów i decyzji innych podmiotów z otoczenia strategicznego (podmiotów podległych, współdziałających, neutralnych, konkurujących ze sobą lub wrogo do siebie nastawionych) w sposób zadowalający i pożądany dla własnych interesów strategicznych. KS warunkują zatem dyplomacja publiczna, komunikacja społeczna, operacje informacyjne i psychologiczne.

Bez wątpienia KS odzwierciedla społeczną naturę człowieka, której istotną potrzebą jest nawiązywanie i utrzymywanie relacji z przedstawicielami danej wspólnoty lub innych społeczności. Wspomniane relacje interpersonalne określiły miejsce człowieka w zbiorowości, a więzi informacyjne ukonstytuowały poniekąd istnienie danej wspólnoty i sens aktywności → s p o ł e c z e ń s t w a i n f o r m a c y j n e g o [t. 4].

Rozwój KS (StratCom) oraz wzrost zainteresowania nią nastąpił w XXI w., uwzględniając zarówno czynniki cywilne, polityczne, jak i militarne. Pierwsza definicja została zaproponowana w 2006 r. przez Departament Stanu USA, który określił KS jako:

> skoncentrowane procesy i wysiłki podejmowane w celu zrozumienia oraz zaangażowania kluczowych audytoriów (odbiorców) dla stworzenia, wzmocnienia lub utrwalenia warunków korzystnych dla realizacji narodowych interesów i celów poprzez zastosowanie skoordynowanych informacji, tematów, planów, programów oraz działań zsynchronizowanych z przedsięwzięciami realizowanymi przez pozostałe elementy władz państwowych.

Większość definicji przyglądających się KS przez pryzmat nauk o bezpieczeństwie skupiała się zazwyczaj na przekazie informacyjnym, działaniach podejmowanych na rzecz kształtowania pożądanego wizerunku

państwa, rozpowszechnianiu wiarygodnych informacji w zakresie podejmowanych decyzji i ich konsekwencji.

KS stanowi syntezę konkretnych działań, wskazanych przez Departament Obrony USA w 2004 r.:

- operacje informacyjne,
- dyplomację publiczną,
- międzynarodowe usługi w zakresie nadawania programów radiowych i telewizyjnych,
- działalność prasowo-informacyjną.

Operacje informacyjne skupiają się na doradztwie i koordynacji działań wojsk, aby osiągnąć pożądany efekt w sferze woli działania (walki), postrzegania i możliwości prowadzenia działań przez potencjalnego przeciwnika. Zadaniem dyplomacji publicznej jest wpływ na postawy społeczne i kształtowanie w tym aspekcie polityki zagranicznej danego państwa na arenie międzynarodowej. Dyplomacja publiczna kształtuje →opinię publiczną [t. 3] w innych państwach, wykorzystując mechanizmy zarezerwowane dla marketingu gospodarczego oraz politycznego. Natomiast międzynarodowe usługi w zakresie nadawania programów radiowych i telewizyjnych są sponsorowane przez organy władzy publicznej i polegają na aktywności medialnej – rozpowszechnianiu informacji, przekazów odpowiednich służb prasowo-informacyjnych wśród wyselekcjonowanych odbiorców (obiektów oddziaływania) za pośrednictwem radia, telewizji oraz internetu. Nie zawsze nadawane programy przybierają formę przekazu informacyjnego, wykorzystuje się również popularną rozrywkę medialną. Przykładami tego typu usług są np. →Głos Ameryki (Voice of America), a także →Radio Wolna Europa [t. 3] (Radio Free Europe) czy TV Biełsat. Działalność prasowo-informacyjna odnosi się do komunikacji społecznej, przekazywania informacji z konkretnych dowództw, tworzenia relacji ze społeczeństwem.

Potwierdzeniem istoty KS jest dokument NATO StratCom Policy z 2009 r., który uznał KS za podstawę starań Sojuszu Północnoatlantyckiego na rzecz osiągnięcia konkretnych celów politycznych i militarnych. Zgodnie z dokumentem KS NATO odnosi się do skoordynowanego i właściwego wykorzystania działań i zdolności komunikacyjnych NATO w obszarze dyplomacji publicznej, komunikacji społecznej, wojskowej

komunikacji społecznej, operacji informacyjnych i psychologicznych, w zależności od przypadku – w celu wspierania polityki, operacji i działań Sojuszu. Zapisy dokumentu wdrożyły nową politykę NATO z uwzględnieniem KS, która miała zapewnić podniesienie poziomu spójności mechanizmów wojskowych i cywilnych komunikacji społecznej Sojuszu oraz usprawnić komunikację z obiektami oddziaływania oraz innymi podmiotami i organizacjami międzynarodowymi.

Kolejnym dokumentem dotyczącym KS, jest przedstawiona w 2010 r. przez Sojusznicze Dowództwo ds. Transformacji (Allied Command Transformation, ACT) Wojskowa koncepcja komunikacji strategicznej NATO. Odwołano się tam do integracji planistycznej i wykonawczej przedsięwzięć charakterystycznych dla KS w odniesieniu do operacji wojskowych. Poruszono także kwestie przywództwa i odpowiedzialności dowódców za komunikowanie się z obiektami oddziaływania, a także konieczności rozpowszechniania przekazu do najniższego poziomu dowodzenia, wykorzystując wszystkie możliwe siły i środki. Permanentne zainteresowanie Sojuszu zagadnieniami KS potwierdzają liczne spotkania grup roboczych, warsztaty oraz szkolenia.

Zaproponowana w 2009 r. definicja StratCom ewoluowała w 2019 r., poszerzając swoje elementy składowe o zagadnienia charakterystyczne dla sfery pozarządowej i biznesowej. Konieczność poszerzenia obszarów zainteresowań KS w ramach NATO była podyktowana permanentnie i dynamicznie zmieniającym się → ś r o d o w i s k i e m i n f o r m a c y j n y m [t. 4], a także wzrastającym poziomem uzależnienia się sfery społecznej i politycznej od systemów wymiany danych, które każdego dnia gwarantują obieg informacji w skali globalnej. Tak skonstruowana definicja utożsamia KS jako całościowe podejście do komunikacji, oparte na wartościach i interesach, które obejmują wszelką aktywność podmiotu na rzecz osiągnięcia zamierzonych celów w spornym środowisku.

Julia Anna Gawęcka

H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019; Decyzja nr 284/MON z dnia 8 lipca 2014 r. w sprawie powołania zespołu do spraw opracowania i wdrożenia systemu komunikacji strategicznej w resorcie obrony

narodowej, Dz. Urz. MON 2014, poz. 236; L. Dušková, *Jak nie komunikować się strategicznie, czyli Republika Czeska i komunikacja strategiczna*, 22.11.2019, CAPD.pl (dostęp 30.01.2020); T. Kacała, J. Lipińska, *Komunikacja strategiczna i public affairs*, Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014; *Komunikacja strategiczna*, [w:] *(Mini)słownik BBN – propozycje*, BBN.gov.pl (dostęp 4.04.2019); A. Legucka, *Walka z rosyjską dezinformacją w Unii Europejskiej*, „Polski Instytut Spraw Międzynarodowych. Biuletyn" 2019, nr 111; A. Lelonek, *Potencjał słowa. Międzynarodowe stosunki i komunikacja. Stan i perspektywy*, Wydawnictwo Fundacja Centrum Badań Polska–Ukraina, Warszawa–Lwów 2016; M. Kowalska, Sz. Wigienka, *Komunikacja strategiczna w Polsce*, 28.10.2019, CAPD.pl (dostęp 30.01.2020); NATO Strategic Communications Policy, Annex to SG(2009)0794, 2009; J. Nowicka, W. Załoga, Z. Ciekanowski, *Komunikacja strategiczna w naukach o zarządzaniu i jakości oraz w naukach o bezpieczeństwie*, „Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach" 2018, nr 1 (14); *Projekt Doktryny Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej*, BBN, Warszawa 2015; *QDR Execution Roadmap for Strategic Communication*, U.S. Department of Defense, 2006; *Report of Defense Science Board Task Force on Strategic Communication*, U.S. Department of Defense, 2004; StratComCoE.org (dostęp 15.02.2020); O. Wasiuta, S. Wasiuta, *Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; R. Zgryziewicz, *Komunikacja strategiczna elementem kształtowania środowiska informacyjnego*, [w:] *Bezpieczeństwo a wyzwania współczesności*, M. Romańczuk, J. Pilżys, G. Ciechanowski (red.), WNUS, Szczecin 2018; R. Żuchowski, *Wojska Obrony Terytorialnej w działaniach antydeznformacyjnych*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 3.

KOMUNIZM (z łac. *communis* – wspólny, powszechny, ogólny, publiczny) – opowiada się za kolektywną własnością i kontrolą środków produkcji, ale także dystrybucji, transportu i komunikacji. Idea komunizmu ma korzenie w wizji społeczeństwa opartego na absolutnej równości ludzkich warunków i eliminacji indywidualnego wzbogacenia. Jest obecny w pracach wielu myślicieli od Platona po XVIII-wiecznych utopistów, sowieckich analityków i niektórych współczesnych teoretyków. Pojęcia komunizm i komunista zostały po raz pierwszy użyte we Francji w XI w. do określenia wspólnych praktyk, interesów i praw niektórych chłopów. Podczas rewolucji francuskiej niektórzy autorzy używali słowa „komunizm" w jego bardziej nowoczesnym znaczeniu, mówiącym o ogólnym

podziale dóbr w → r e ż i m i e [t. 3] ustanowionym w procesie rewolucyjnym. Inni, np. R. Owen, E. Cabet, W. Weitling i M. Hess, używali tego terminu do oznaczania utopijnych projektów społeczeństw opartych na nowym systemie wymiany i dystrybucji. Dopiero jednak w połowie XIX w. idea komunizmu stała się bardziej rozpowszechniona.

Współczesny komunizm wiąże się zwykle z ideami wysuniętymi przez niemieckich filozofów politycznych K. Marksa i F. Engelsa oraz rosyjskiego przywódcę i teoretyka komunistycznego W.I. Lenina. Intelektualne korzenie tej idei sięgają jednak *Państwa* Platona z IV w. p.n.e. Ogromne dysproporcje w zamożności i dystrybucji bogactwa w okresie rewolucji przemysłowej z przełomu XVIII i XIX w. dostarczyły impetu i inspiracji dla współczesnych koncepcji komunistycznych, które w głównym zarysie sprowadzają się do krytyki kapitalizmu oraz proponują zastąpienie go alternatywnym systemem społecznym i ekonomicznym, czyli komunizmem.

W *Manifeście komunistycznym* i innych pracach Marks i Engels krytykowali kapitalizm za alienację i eksploatację robotników (proletariatu), co wzbogacało kapitalistów (burżuazję) i zapewniało im rządy nad robotnikami. Cała ludzka historia, jak pisali, była historią zmagań między klasami, pomiędzy niewolnikami i ich właścicielami, poddanymi i panami, a w końcu proletariatem i kapitalistami. Według autorów walka ta miałaby być ostatnim rozdziałem w historii walki klasowej. Dzięki niej miałoby wyłonić się egalitarne, sprawiedliwe i bezklasowe społeczeństwo komunistyczne. Marks i Engels postrzegali kapitalizm jako historycznie niezbędny etap rozwoju, który przyniósł niezwykłe zmiany naukowe i technologiczne – zmiany, które znacznie zwiększyły władzę człowieka nad naturą. Kapitalizm również znacznie zwiększył łączną ilość bogactwa. Pod tym względem kapitalizm był siłą pozytywną i postępową. Problem polegał ich zdaniem na tym, że bogactwo, a także siła polityczna i szanse życiowe były nierówno i niesprawiedliwie rozdzielone. Pracownicy otrzymywali wynagrodzenie za długie godziny ciężkiej pracy. Co więcej to oni, a nie kapitaliści, byli twórcami bogactwa. Zgodnie z komunistyczną teorią wartości, prawdziwa wartość towaru zależy od ilości pracy wymaganej do jego wytworzenia. W kapitalizmie pracownicy nie otrzymywali sprawiedliwego wynagrodzenia za pracę. Kapitaliści odejmowali część, którą Marks nazywał „wartością dodaną", różnicę między tym, co otrzymywali

pracownicy, a ceną płaconą przez nabywców produktu. Ta nadwyżka była inwestowana, aby przynieść jeszcze większe zyski. To z kolei umożliwiało burżuazji gromadzenie ogromnego bogactwa, podczas gdy proletariat popadał w ubóstwo.

Marks zapowiadał, że seria → k r y z y s ó w gospodarczych przyniesie jeszcze większe bezrobocie, niższe płace i rosnącą nędzę proletariatu przemysłowego, a wtedy proletariat poddawany i motywowany rewolucyjną świadomością klasową przejmie władzę państwową i ustanowi swoje własne przejściowe państwo socjalistyczne, które Marks nazwał rewolucyjną → d y k t a t u r ą proletariatu. To znaczy, że proletariat będzie, tak jak wcześniej burżuazja, rządzić we własnym interesie klasowym, aby zapobiec kontrrewolucji ze strony pokonanej burżuazji. Według filozofa gdy to → z a g r o ż e n i e [t. 4] minie, państwa przestaną być potrzebne, co utoruje drogę do powstania bezklasowego społeczeństwa komunistycznego.

Wizja komunistycznego społeczeństwa zaproponowana przez Marksa była niejasna i ogólnikowa, myśliciel nie przedstawił szczegółowych planów budowy przyszłego społeczeństwa. Niektóre cechy, które opisał, takie jak bezpłatna edukacja publiczna dla wszystkich i powszechny podatek dochodowy, obie uważane za radykalne w jego czasach, są dziś obecne w wielu państwach, często jako oczywistość, zwłaszcza w Europie. Inne propozycje, takie jak własność publiczna czy kontrola głównych środków produkcji oraz dystrybucji towarów i usług zgodnie z zasadą „od każdego według jego zdolności, każdemu według jego potrzeb", okazały się bądź to niezwykle trudne do praktycznej realizacji, bądź też w dłuższej perspektywie przynosiły dramatycznie niskie efekty gospodarowania w państwach czy społeczeństwach próbujących wdrożyć te zalecenia.

Lenin dokonał 2 ważnych odstępstw od teorii i praktycznych dyrektyw dotyczących komunizmu w wersji Marksa. Pierwsze z nich wynikało z poglądu Lenina, że rewolucja komunistyczna nie rozpocznie się w zaawansowanych krajach kapitalistycznych, jak przewidział Marks, ponieważ tam robotnicy byli nasyceni reformatorską świadomością związkową, brakowało im zaś rewolucyjnej świadomości klasowej. To prowadziło ich do organizowania związków i partii politycznych robotników i odwracania się od idei rewolucji. W tej sytuacji wg Lenina rewolucja komunistyczna miałaby zacząć się w gospodarczo zacofanych państwach, takich jak Rosja,

i uciskanych oraz eksploatowanych państwach kolonialnych. Druga istotna zmiana wynikała z poglądu Lenina, że rewolucja nie może i nie powinna być spontanicznie przeprowadzana przez przemysłowy proletariat, jak utrzymywał to Marks, ale przez chłopstwo kierowane przez elitarną partię komunistyczną, złożoną z radykalnych intelektualistów klasy średniej. Partia ma za zadanie kierować masami. Było to konieczne, gdyż – jak twierdził Lenin – masy cierpiały na fałszywą świadomość i niezdolne były do rozeznania swoich prawdziwych interesów, by same mogły rządzić sobą. Lenin wskazywał także, że w toku krwawej i gwałtownej rewolucji i jej represyjnych konsekwencji nie może być miejsca na moralne skrupuły, ponieważ „nie można dokonać rewolucji bez łamania głów, ani łamania obietnic". Niemoralne działania były zatem usprawiedliwione w imię wyższej socjalistycznej moralności, która utrzymywała, że ostateczny cel – bezklasowe społeczeństwo komunistyczne – usprawiedliwia prawie wszelkie środki użyte do jego osiągnięcia.

Dalsza realizacja wizji bezklasowego społeczeństwa komunistycznego, którą próbowano wcielić w XX w., przyniosła krwawe reżimy rządzone przez J. Stalina w Związku Radzieckim i Mao Zedonga w Chinach. Komunizm został wprowadzony siłą po II wojnie światowej w wielu państwach Europy Środkowej i Wschodniej, a zakończył się wraz z pokojowymi rewolucjami z 1989 r. Od 1949 r. system komunistyczny panuje w Chinach, których populacja przekracza 1,4 mld ludzi; systemy komunistyczne istnieją również w Korei Północnej i na Kubie. Istnieje zatem grupa państw komunistycznych o różnych tradycjach i strukturach społecznych i etnicznych. Systemy komunistyczne w Europie były również dość zróżnicowane. Np. wariant rumuński, który utrzymywał pewną niezależność od Związku Radzieckiego, był znacznie bardziej represyjny niż wersje węgierska lub polska, podczas gdy wariant jugosłowiański z kolei silnie akcentował samozarządzanie pod kontrolą partii komunistycznej. Uwzględnienie wariantów azjatyckich jedynie pogłębia zróżnicowanie. Model chiński łączy potężną, prawie w pełni rynkową gospodarkę z kontrolą polityczną partii komunistycznej, natomiast model północnokoreański zbliża się do modelu totalitarnego w skali jego kontroli i represji. Pomimo różnic między systemami komunistycznymi określono ich granice, których próby przekroczenia spotkały się z daleko idącym sprzeciwem. Przejawiały się

one wyraźnie w interwencjach wojskowych armii radzieckiej na Węgrzech w 1956 r. i w Czechosłowacji w 1968 r., a także we wprowadzeniu stanu wojennego przez polskich komunistów w 1981 r. W każdym przypadku działania te były brutalnymi reakcjami na próby liberalizacji systemów komunistycznych.

Reżimy komunistyczne nie istnieją już w Rosji i Europie Wschodniej. Próby zreformowania komunizmu na Węgrzech, w Polsce, Czechosłowacji i Związku Radzieckim pod rządami Gorbaczowa nie powiodły się. Partie komunistyczne z Europy Zachodniej podupadają lub zmieniły swoją nazwę i tożsamość. Komunizm pozostawił ważną spuściznę. Dominacja komunistyczna odcisnęła piętno na dobrobycie w krajach, które skierowały się później ku demokratyzacji i gospodarce wolnorynkowej, co tłumaczy tęsknotę za równością i ochroną socjalną. W niektórych państwach komuniści są dobrze wspominani, ponieważ pamięć zbiorowa kojarzy ich z walką uciskanych klas społecznych i antyfaszyzmem. Sama doktryna komunistyczna przeżywa głęboki kryzys, ale niektórzy badacze odnajdują pewne zalety w marksizmie. Niektóre elementy kultury komunistycznej są wciąż żywe w postaci antykapitalizmu, dążenia do utopijnych ideałów, poszukiwania radykalnej alternatywy, kwestionowania zasad demokracji i wrogości wobec reformizmu. Komunizm może obecnie zostać uznany za nieistniejący jako scentralizowany politycznie i autorytarny ruch.

Rafał Klepka

T. Ball, *Communism*, [w:] *The Encyclopedia of Political Science*, G.T. Kurian (ed.), CQ Press, Washington 2011; R. Klepka, *Komunizm*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; L. Kołakowski, *Główne nurty marksizmu*, Wydawnictwo Naukowe PWN, Warszawa 2009; M. Lazar, *Communism*, [w:] *International Encyclopedia of Political Science*, B. Badie, D. Berg-Schlosser, L. Morlino (eds.), SAGE Publications, Los Angeles–London–New Delhi 2011; A. Rychard, *Communist system*, [w:] *International Encyclopedia of Political Science*, B. Badie, D. Berg-Schlosser, L. Morlino (eds.), SAGE Publications, Los Angeles–London–New Delhi 2011; A. Shlomo, *The Social and Political Thought of Karl Marx*, Cambridge University Press, Cambridge 1968; *The Cambridge History of Communism*, S. Pons i in. (ed.), Cambridge University Press, Cambridge 2017; S. White, J. Gardner, G. Schöpflin, *Communist Political Systems: An Introduction*, Macmillan Education, London 1987.

KONCEPCJA BEZPIECZEŃSTWA PUBLICZNEGO FR „MARTWA WODA" – jest rodzajem filozofii, pewnego rodzaju systemem poglądów dotyczących porządku świata, przekonaniem o wiedzy na temat rządzenia, miejsca rosyjskiej cywilizacji w historii i na świecie oraz kształtu sprawiedliwego społeczeństwa wolnego od pasożytnictwa. Koncepcja bezpieczeństwa publicznego FR „Martwa woda" jest ideą budowy społeczeństwa, którego członkowie będą godni tytułu człowieka, a jednocześnie będzie miało ono ogólnoświatowe zrozumienie umożliwiające wdrożenie tej idei w życie. Ma swój własny aparat terminologiczny (stabilne frazy) oraz podstawę filozoficzną. Koncepcja bezpieczeństwa publicznego poprzez analizy ewolucji biosfery i ludzkości, globalnego procesu historycznego, ekonomii, filozofii, socjologii i wielu innych nauk, za pomocą teorii zarządzania wyjaśnia procesy zachodzące we współczesnym świecie, początki globalnego kryzysu systemowego na ziemi, a także pokazuje sposoby wyprowadzenia Rosji i całej ludzkości (w tym każdej pojedynczej osoby) na ścieżkę bezkryzysowego, harmonijnego rozwoju w zgodzie z prawami natury (wszechświat, biosfera itp.). Podstawą koncepcji jest tzw. wystarczająca ogólna teoria zarządzania (DOTU). Jej zwolennicy twierdzą, że DOTU opiera się na czystej logice, a za jej pomocą można opisać każdy proces zarządzania.

Nazwa „Martwa woda" odnosi się do legend o cudownej mocy wód – „martwej" i „żywej". Kiedy „wody" się zmieniają, zmienia się także system poglądów na przeszłość, teraźniejszość i przyszłość, nieuchronnie przekształca się pod nieuniknionym wpływem „prawa czasu".

Twórcy koncepcji to grupa ideologów, anonimowy zespół autorów, który przyjął nazwę Wewnętrznego Predyktora ZSRR. Wyjaśniają swoją nazwę tym, że w matematyce obliczeniowej istnieje metoda „predyktor-korektor", polegająca na znalezieniu rozwiązania problemu poprzez kolejne przybliżenia. Predyktor to termin wykorzystywany w statystyce: zmienna modelu statystycznego stosowana w prognozowaniu, zmienna niezależna, zmienna objaśniająca. Ponadto algorytm metody jest cyklem, w którym 2 operacje są wykonywane jedna po drugiej: pierwsza to prognoza rozwiązania, a druga to weryfikacja prognozy pod kątem spełnienia wymagań dotyczących dokładności rozwiązania problemu – algorytm kończy się, gdy prognoza spełnia owe wymagania. Oznacza to, że jeśli

zarządzanie jest przeprowadzane zgodnie z powyższym schematem, osiągana jest wówczas wysoka jakość przebiegu wszystkich procesów. To znaczy, że autorzy koncepcji próbują przewidywać, co dzieje się czy będzie się działo ze społeczeństwem.

Według wyznawców koncepcji zachodnią cywilizacją rządzi Globalny Predyktor. Jaka to osoba, organizacja, grupa ludzi, skąd i z jakiego czasu pochodzi Predyktor, nie jest jasne. Zwolennicy filozofii są przekonani, że ten tajemniczy geniusz zmonopolizował banki, stworzył międzynarodowe korporacje, zorganizował „klub miliarderów" i utworzył praktykę udzielania kredytów, które zniewoliły ludność.

Cele globalnych wysiłków Predyktora ujawniane przez zwolenników koncepcji są alarmujące:

- zniszczenie granic państwowych;
- zniszczenie kultury narodowej i utworzenie „jednego stada niewolników";
- zmniejszenie populacji ziemi do „złotego miliarda" – najlepszych przedstawicieli ludzkości, którzy będą zarządzać zasobami naturalnymi (dla innych nie wystarczy).

Wiele uwagi koncepcja poświęca językowi – kulturze językowej mowy (mówionej i pisanej), która jest nie tylko środkiem wyrażania myśli, ale także jednym ze środków kształtowania kultury uczuć i myślenia nowych pokoleń wkraczających w życie. Kultura językowa oddziałuje nie tylko na poziom świadomości, ale także na nieświadome poziomy psychiki, których natura jest zasadniczo zaprogramowana genetycznie, biorąc tu pod uwagę też genetyczne predyspozycje osoby do posługiwania się takim czy innym językiem jako ojczystym.

Od 1987 r. inicjatywna grupa publiczna Wewnętrzny Predyktor ZSRR na podstawie badań ZSRR, ale również doświadczeń USA i → NATO [t. 3], zaczęła przygotowywać koncepcję bezpieczeństwa publicznego pod nazwą „Martwa woda" (wydania 1992, 1996, 1997, 1998, 2003, 2011, 2015, 2018). Od tego czasu ZSRR jako państwo zniknął, ale grupa kontynuuje prace pod tą samą nazwą. Jest tak nie tylko dlatego, że stała się ona specjalną marką, ale także dlatego, że jej członkowie nie dopuszczają (w sensie prawnym) likwidacji ZSRR zaistniałej na mocy dyrektyw „świata za kulisami", różnych lóż masońskich itp.

Każde społeczeństwo jest kontrolowane w taki czy inny sposób, a zatem globalny proces historyczny może być postrzegany jako globalny proces kontroli, który przede wszystkim obejmuje wiele procesów zarządzania regionalnego (polityki państw regionalnych i polityki międzynarodowe, siły, które nie są zinstytucjonalizowane w państwie, np. m a f i a [t. 3]). Podstawą teoretyczną koncepcji bezpieczeństwa publicznego jest wystarczająca ogólna teoria zarządzania i kontroli (wystarczająco ogólna, aby opisać każdy proces zarządzania lub proces kontroli na jej podstawie). Zgodnie z tą teorią wszystkie środki kontroli i zarządzania ludzkim społeczeństwem można podzielić na ogólne grupy, które są ułożone hierarchicznie od najbardziej efektywnych do najmniej skutecznych.

W koncepcji wojnę przedstawiono na 6 poziomach ujętych jako priorytety kontroli ludzkości. Z 6 priorytetów tylko jeden był wojskowy, a pozostałe to metody → w o j n y i n f o r m a c y j n e j [t. 4], zarazem potężne środki broni informacyjnej:

- priorytet ideologiczny: poglądy społeczeństwa na kluczowe pojęcia dobra i zła, życia i wszechświata; → i n f o r m a c j e o charakterze filozoficznym, metodologia, opanowanie, które ludzie budują – indywidualnie i publicznie – do rozpoznawania poszczególnych procesów w kompletności oraz integralności Wszechświata i określają ich hierarchiczne uporządkowanie we wzajemnym powiązaniu; stanowi podstawę kultury myślenia i kompletności działań kontrolnych, w tym wewnątrzwspólnotowej absolutnej władzy zarówno na poziomie regionalnym, jak i globalnym;
- priorytet chronologiczny: wg zasady „przepisz historię narodu, i ty podbijesz go"; np. Rosja wykorzystuje mity historyczne, aby uzasadnić swoje roszczenia do obszaru postsowieckiego i Europy Wschodniej; informacje o chronologicznej naturze wszystkich domen kultury i wiedzy; pozwala dostrzec kierunek rozwoju procesów i skorelować poszczególne dziedziny kultury jako całości oraz odpowiednich gałęzi wiedzy; dla tych, których światopogląd opiera się na poczuciu proporcji i jest zgodny ze światem, informacje te pozwalają zidentyfikować określone procesy, filtrując „chaotyczny" przepływ faktów i zjawisk przez „subiektywne" sito światopoglądowe – to subiektywna ludzka miara identyfikacji;

w tym kontekście kultura to wszelkie informacje, które nie są genetycznie przekazywane w ciągłości pokoleń;
- priorytet faktologiczny: opis poszczególnych procesów i ich wzajemnych powiązań; dogmaty, ideologia, kulty religijne, świeckie ideologie, technologie i fakty ze wszystkich dziedzin nauki, nawiązywanie do norm kultury, ideologii, sposobu życia (alkoholizm, łapówkarstwo, kult władzy państwowej);
- priorytet gospodarczy jako instrument wpływu poprzez finanse podporządkowane czysto informacyjnym środkom;
- →broń genetyczna [t. 1], praktyki →ludobójstwa [t. 3] lub →broń ekologiczna [t. 1], która wpływają nie tylko na dane pokolenie (zły stan zdrowia, włącznie z efektem śmiercionośnym), ale także przyszłe pokolenia (zmiany w genach następnych pokoleń): narkotyki, alkohol, tytoń i inne ludobójcze środki odurzające, dodatki do żywności, wszystkie zanieczyszczenia środowiska, niektóre leki; inżynieria genetyczna i biotechnologia;
- broń wojskowa, narzędzia destrukcji – broń w tradycyjnym tego słowa znaczeniu, zabijanie i okaleczanie ludzi, niszczenie i eksterminacja materialnych i technicznych przedmiotów cywilizacji, zabytków kultury i nosicieli ich ducha.

Chociaż nie ma jednoznacznych różnic między środkami wpływu, ponieważ wiele z nich ma cechy, które pozwalają przypisać je do różnych priorytetów, to hierarchiczne uporządkowanie ich klasyfikacji pozwala zidentyfikować dominujące czynniki wpływu, które można wykorzystać do kontroli, a zwłaszcza jako narzędzia tłumienia i eliminacji zjawisk w życiu społecznym, które są koncepcyjnie nieodpowiednie w sensie kontroli.

W przypadku stosowania tego zestawu w ramach jednego systemu społecznego są to ogólne sposoby zarządzania nim, a kiedy są używane przez system społeczny (grupę społeczną) w stosunku do innych, gdy koncepcje zarządzania nie pokrywają się w nich, jest to broń ogólna, tj. środki walki w najogólniejszym tego słowa znaczeniu.

Olga Wasiuta

O. Wasiuta, *Koncepcja bezpieczeństwa publicznego FR „Martwa woda"*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo

Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Arcana, Kraków 2017; Wewnętrzny Predyktor SSSR, *Martwa woda. Od „socjologii" do „Mowy Życia". Cz. 1. Esej historyczno-filozoficzny*, Kiteż 2004; *Мёртвая вода. От «социологии» к жизнеречению*, Концепция Общественной Безопасности, Издательство „КИТЕЖ", Державный град России, Москва 2015; Ю. Петухов, *Четвертая Мировая. Вторжение. Хроника оккупации Восточного полушария*, Издательство „Метагалактика", Москва 2004; Л. Шершнев, *Четвертая мировая война и ее исторические особенности*, МОФ „Фонд национальной и международной безопасности", Москва 2005.

KONCEPCJA DZIAŁAŃ SIECIOCENTRYCZNYCH (ang. *network centric warfare*, NCW) – strategia prowadzenia operacji militarnych bazująca na przewadze informacyjnej zbudowanej na podstawie właściwości sieci. Hołduje przekonaniu, że wzrost siły bojowej armii generowany jest poprzez połączenie w sieć informacyjną sensorów (czujników), decydentów (ośrodków decyzyjnych) i efektorów (środków rażenia i systemów walki) w celu osiągnięcia wspólnej świadomości sytuacyjnej, zwiększenia szybkości dowodzenia oraz tempa operacji, zwiększenia skuteczności uzbrojenia, wzrostu odporności na uderzenia przeciwnika oraz zwiększenia stopnia synchronizacji działań. Zdobywanie → i n f o r m a c j i to zadanie sensorów, ich przetwarzanie przez ośrodki kierowania to rola decydentów, a reakcja środkami rażenia na zdarzenia w obszarze operacji należy do efektorów. Ten trójelementowy system, oparty na nowoczesnych środkach teleinformatycznych, zapewnia bieżące monitorowanie sytuacji w obszarze działań operacyjnych przy wykorzystaniu rozpoznania satelitarnego, powietrznego, osobowego i elektronicznego. Wszystkie działania podejmowane w ramach operacji sieciocentrycznych zmierzają do szybkiego osiągnięcia przewagi informacyjnej nad przeciwnikiem przy wykorzystaniu dostępnej infrastruktury. Koncepcja NCW obejmuje zatem kombinację strategii, nowych taktyk, technik i procedur, a także rozwiązań organizacyjnych, które częściowo usieciowione siły zbrojne mogą zastosować, aby stworzyć decydującą przewagę na polu walki. Podczas prowadzenia operacji sieciocentrycznych wykorzystuje się wiedzę zgromadzoną w sieciach internetowych do formowania i stosowania wielorodzajowej siły, adekwatnie do sytuacji na polu walki wzmacniają efektywność i skuteczność działań zbrojnych. Punktem docelowym wszystkich tych działań jest pozyskanie,

integracja oraz wykorzystanie informacji w czasie zbliżonym do rzeczywistego, a w konsekwencji radykalne skrócenie czasu podejmowania decyzji i szybkie osiągnięcie pożądanego efektu. Jest to istota koncepcji działań sieciocentrycznych.

Koncepcja NCW uzyskała miano strategii rewolucyjnej z uwagi na nowatorski charakter, niespotykany dotychczas sposób prowadzenia działań zbrojnych i skalę wykorzystywania nowoczesnych rozwiązań technologicznych. Zwiększa ona bowiem zdolności bojowe armii poprzez uzyskanie wysokiego stopnia integracji we wszystkich wymiarach przestrzeni operacyjnej oraz ograniczenie ilości wojsk dzięki precyzyjnej informacji. Zmaterializowała się jako efekt dążenia do zwiększenia potencjału bojowego wojsk w sposób pozwalający dominować nad przeciwnikiem w sferze informacyjnej. Jej istotą jest przekonanie, że o przewadze informacyjnej w działaniu decyduje nie rozbudowa ilościowa środków i stanu liczebnego armii, a bardziej efektywne ich wykorzystanie przez decydentów (dowódców) dzięki posiadaniu i dystrybucji aktualnej i wiarygodnej informacji. Środki działające w systemie operacji sieciocentrycznych tworzą swoistą sieć informacyjną, zapewniającą pozyskanie, transmisję i przetwarzanie olbrzymich ilości danych oraz ich zobrazowanie na tle komputerowej mapy obszaru działań. Ważną cechą operacji sieciocentrycznych jest nielinearne pole walki – prowadzenie działań w wielowymiarowej przestrzeni, bez fizycznej obecności → ż o ł n i e r z y [t. 4] w każdym miejscu rejonu odpowiedzialności. Istotne jest także rozproszenie sił oraz wysoka dynamika i tempo działań własnej armii, które skutecznie utrudniają przeciwnikowi szybką reakcję. Rozproszenie sił nie jest postrzegane jako zjawisko świadczące o osłabieniu lub chaosie, a wręcz przeciwnie, jest zjawiskiem pożądanym, decydującym o dynamizmie działań wojsk własnych. Pozwala ono na bycie w gotowości na oddziaływanie przeciwnika w różnych uwarunkowaniach i z różnych kierunków. Małymi zgrupowaniami ponadto najlepiej manewruje się adekwatnie do zaistniałej sytuacji, siły rozproszone są mniej podatne na uderzenie przeciwnika.

Koncepcja działań sieciocentrycznych zrodziła się na gruncie amerykańskim w latach 90. XX w. jako połączenie nauki, techniki i nowoczesnych technologii, ale także umiejętności ich kompleksowego wykorzystania w praktyce, stając się dominującą metodą działań na polach walki

zbrojnej na przełomie XX i XXI w. Procesy globalizacyjne i doświadczenia uzyskane w latach 90. podczas wojny w Zatoce Perskiej oraz wyniesione z konfliktów zbrojnych w Iraku i Afganistanie wskazały, że osiągnięcie wysokiej sprawności w realizacji procesu dowodzenia uzależnione jest m.in. od dostępności zaawansowanych technologicznie środków dowodzenia. Pokazało to ogromny potencjał, jaki tkwi w odpowiednich metodach zarządzania informacją, oraz pozwoliło stworzyć nowe możliwości i sposoby wykorzystania tych środków na polu walki. Gwałtowny rozwój elektroniki i technologii informatycznych ujawnił nowe możliwości środków walki, precyzję i skuteczność rażenia, miniaturyzację środków rozpoznawczych, których zróżnicowanie i dokładność umożliwiła bieżące podglądanie przeciwnika z ziemi, powietrza i przestrzeni kosmicznej.

W powszechnej opinii I wojna w Zatoce Perskiej (1990–1991) i operacja Pustynna Burza (Desert Storm) to moment graniczny, w którym po raz pierwszy zastosowano sieciocentryczność w praktyce. Wówczas to obok klasycznej bitwy pancerno-powietrznej, w której brały udział ciężkie dywizje pancerne i zmechanizowane, zastosowano nowe rodzaje uzbrojenia oparte na zaawansowanej technologii. W strefie → w o j n y [t. 4] znajdowało się wówczas ponad 3 tys. komputerów połączonych z dowodzeniem w USA, a na polu walki permanentnie obecne były media. W większym stopniu elementy sieciocentryczne zastosowano podczas II wojny w Zatoce Perskiej (2003 r.). Doszło wtedy do kombinacji kilku prowadzonych jednocześnie, wzajemnie skoordynowanych operacji na lądzie, morzu i w powietrzu. Przykładem takiej operacji była Iracka Wolność (Iraqi Freedom) prowadzona przeciwko Saddamowi Husajnowi. Od tego momentu, w mniejszym lub większym stopniu, sieciocentryczność stała się sposobem działania sił zbrojnych wielu państw świata, dając początek nowej → d o k t r y n i e w o j s k o w e j.

Prekursorem naukowego oglądu idei sieciocentryzmu był amerykański adm. W. Owens, który w 1996 r. opublikował koncepcję „systemu systemów", w której przedstawił pierwowzór późniejszych koncepcji sieciocentrycznych w działalności militarnej. Samo określenie działań, walki, operacji sieciocentrycznych w języku angielskim – Network Centric Warfare – pojawiło się prawie równocześnie w kilku periodykach w 1997 r. w artykułach A.D. Campena, B. Brewina i E. Walsha Jr, jako wynik

obserwacji i analiz zebranych podczas I wojny w Zatoce Perskiej. W 1998 r. opublikowano artykuł amerykańskich oficerów polskiego pochodzenia – adm. A.K. Cebrowskiego oraz płk. sił powietrznych J. Garstki – *Network Centric Warfare: Its Origins and Future*. Uważa się go powszechnie za pierwszy opublikowany materiał dotyczący sieciocentryczności. Autorzy przedstawili w nim własne poglądy dotyczące nowych sposobów prowadzenia działań militarnych w warunkach →społeczeństwa informacyjnego [t. 4] i globalizacji, a ich poglądy i doświadczenia stały się początkiem nowej doktryny militarnej, która zakładała, że współczesne armie pokonają ewentualnego przeciwnika dzięki nowoczesnemu systemowi zbierania, przetwarzania i dystrybucji informacji obejmującemu wszystkie ogniwa dowodzenia. Pełniejszym rozwinięciem koncepcji →wojny sieciocentrycznej [t. 4] jest książka pt. *Network Centric Warfare: Developing and Leveraging Information Superiority* autorstwa D.S. Albertsa, J. Garstki i F.P. Steina.

Koncepcja działań sieciocentrycznych, która na dobre ugruntowała się w świadomości decydentów cywilnych i wojskowych, charakteryzuje się m.in.:

- szybkim i ciągłym przepływem informacji między różnymi poziomami i szczeblami dowodzenia, co przekłada się na zwiększenie tempa prowadzenia operacji, uprzedzanie przeciwnika w zdobywaniu informacji, utworzenie sprawnych i elastycznych zdolnych do szybkiego reagowania struktur dowodzenia, a także zwiększenie skuteczności dowodzenia i efektywności pracy sztabów dzięki dostępowi do wspólnego obrazu sytuacyjnego;
- zwiększeniem skuteczności ostrzegania przed atakiem przeciwnika;
- zwiększeniem efektywności broni precyzyjnego rażenia;
- efektywnym wykorzystaniem małych, rozproszonych geograficznie sił oraz sprawniejszym działaniem wielonarodowych sił umożliwiających siłom narodowym oferowanie specjalistycznych usług;
- umiejętnością integracji rozległej i różnorodnej struktury walki;
- możliwością redukcji kosztów działań na polu walki poprzez zmniejszenie ilości sił niezbędnych do wykonania zadania, które prowadzi do rozproszenia sił własnych, działających w niewielkich zgrupowaniach, co utrudnia przeciwnikowi lokalizację, identyfikację i rażenie;

- możliwością kontrolowania znacznie większego obszaru terenu przez relatywnie niewielkie siły własne;
- zmniejszeniem strat sił własnych dzięki znajomości lokalizacji wszystkich elementów własnego ugrupowania bojowego;
- doprowadzeniem do rzeczywistego połączenia działań różnych rodzajów sił zbrojnych na niskich poziomach dowodzenia oraz mniejsze i bardziej mobilne organy dowodzenia,
- wykorzystaniem na szeroką skalę narzędzi technologicznych, umożliwiających podejmowanie decyzji o mniejszym ryzyku;
- decentralizacją dowodzenia i przejęciem inicjatywy przez dowódców niższych szczebli, szybszym doprowadzeniem zadań do wykonawców, co w efekcie spowoduje, że zadania będą adekwatne do rzeczywistej sytuacji;
- zmianą natury wojny w odpowiedzi na zmieniające się realia prowadzenia działań zbrojnych w erze informatycznej, co sprawia, że przeciwnik zmuszony jest dostosować własne działania do naszych posunięć i prowadzić proces decyzyjny w sposób taki sam jak my.

Obserwacje praktycznego wykorzystania koncepcji NCW wyłoniły również wady wynikające głównie z barier natury technicznej, operacyjnej, strategicznej, kulturowej i finansowej. Należy tu uwzględnić całokształt problemów związanych z użytkowanym sprzętem, wyposażeniem, oprogramowaniem itd., wykorzystywanym w prowadzeniu działań o charakterze sieciocentrycznym, w tym także ograniczoną odporność sprzętu i oprogramowania na warunki fizyczno-geograficzne środowiska działań, tj. klimat, temperaturę, pogodę, a także podatność na zakłócenia i → c y b e r a t a k i [t. 1]. Problemem są również bariery informacyjne związane z nadmiarem informacji, który może zablokować systemy informacyjne i powodować obniżenie jej jakości, chaos i trudności w podejmowaniu efektywnych decyzji. Człowiek, który z jednej strony jest kreatorem efektywności działań sieciocentrycznych, z drugiej może być najsłabszym ogniwem. Błąd lub zaniedbanie człowieka może być przyczyną niepowodzeń, trudności i strat.

Do poważnych mankamentów należą także:

- wysokie koszty zastosowania innowacyjnych technologii, które stają się często barierą nie do przebicia dla mniej zamożnych państw,

uzależnionych od pozyskiwania sprzętu i wysokich technologii od innych;
- nadmierne faworyzowanie idei zmniejszania liczebności wojska, co nie przekłada się na zmniejszenie kosztów operacji, a zbyt duży nacisk kładzie na przyspieszenie cykli decyzyjnych;
- sieci informacyjne poprzez szeroki dostęp do internetu stają się naturalnym obiektem ataku dla strony przeciwnej, ale także przez osoby indywidualne oraz instytucje – w sieci mogą się zatem pojawić informacje sprzeczne lub nawet fałszywe; działania sieciocentryczne jako nowa forma aktywności militarnej w sposób niezamierzony wygenerowały nowy obszar zmagań w →cyberprzestrzeni [t. 1];
- negatywny wpływ na efektywność potencjału militarnego – operacje prowadzone są równolegle w ramach sojuszu lub w siłach zbrojnych potencjalnych sojuszników, podjęcie takich działań może prowadzić do swoistej izolacji państw i sojuszników spowodowanej brakiem kompatybilności sprzętowej i proceduralnej oraz natury mentalnej (np. różnice w szkoleniach);
- koncepcja sieciocentryczności umożliwia tylko bardziej efektywne wykorzystanie posiadanych informacji, potencjału bojowego i czynnika ludzkiego, ale mogą przecież wystąpić czynniki nieracjonalne, np. niekontrolowany wypływ technologii informatycznych, które mogą znaleźć się w niepożądanych rękach, niebezpieczeństwo wynikające z →zagrożeń [t. 4] asymetrycznych, np.: samobójcze ataki bombowe, cywile jako żywe tarcze, użycie →broni biologicznej [t. 1], →broni chemicznej [t. 1] itd. oraz narażenie na ataki w cyberprzestrzeni;
- przywiązywanie przesadnej wagi do informacji, przecenianie jej, niedocenianie potencjalnego przeciwnika oraz problemy z interoperacyjnością wojska, biorąc pod uwagę różnice, jakie dzielą poszczególne rodzaje;
- brak rzetelnej analizy ryzyka w zakresie rzeczywistego wprowadzenia w życie doktryny militarnej, opartej całkowicie na tak instrumentalnie zdobywanych i przesyłanych danych.

Błędne jest przekonanie, że działania sieciocentryczne wykonywane są wyłącznie przez siły zbrojne poszczególnych państw czy sojuszy.

Podmiotami realizującymi zadania w tym zakresie są także: → w y w i a d [t. 4] i → k o n t r w y w i a d, → p o l i c j a [t. 3], służby ochrony granic, ds. walki z narkotykami i → t e r r o r y z m e m [t. 4] oraz podmioty naruszające obowiązujące prawo krajowe i międzynarodowe. Każdy z nich posiada narzędzia pozwalające prowadzić działania sieciocentryczne. Władza wykonawcza także dysponuje wyspecjalizowanym aparatem zasilania w informacje (dyplomacja, → s ł u ż b y s p e c j a l n e [t. 4], policja, organizacje międzynarodowe, media itd.), rozbudowanym aparatem wspierającym proces decyzyjny (ośrodki analityczno-studyjne) i organami wykonawczymi (ministerstwa, siły zbrojne, służby specjalne, policja).

Pomimo istnienia wielu problemów i głosów krytycznych pod adresem koncepcji rozwój technologiczny i ewolucja współczesnych działań wojennych nieuchronnie prowadzą do usieciowienia sił zbrojnych i realizowanych przez nie zadań. Koncepcja działań sieciocentrycznych stopniowo implementowana do prawodawstwa państwowego i obronnego wielu państw cały czas podlega procesom rozwoju i modyfikacji, co czyni ją ideą niezwykle elastyczną i otwartą na zmiany, jakie niesie przyszłość. Wykorzystanie współzależności obszaru informacyjnego i obszaru działań bojowych w ramach walki zbrojnej wymaga zaawansowanej technologicznie wymiany informacji oraz łączenia jej w kompleksy danych, otrzymywanych z rozproszonych terytorialnie sensorów. Przodującą rolę w tym zakresie odgrywają największe i najnowocześniejsze armie zdolne do finansowania szeroko zakrojonych badań i programów naukowych związanych z rozwojem środków walki oraz podnoszeniem efektywności dowodzenia, m.in.: USA, Wielka Brytania i inne państwa strefy → N A T O [t. 3], w tym także Polska.

Sabina Olszyk

A.K. Cebrowski, *The Implementation of Network Centric Warfare*, Force Transformation, Office of the Secretary of Defense, Washington 2005; A.K. Cebrowski, J. Garstka, *Network Centric Warfare: Its Origins and Future*, „Proceedings Magazine" 1998, vol. 124, iss. 1; B. Grenda, *Sieciocentryczne zarządzanie siłami powietrznymi*, „Journal of KONBiN" 2011, nr 3; L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, „Myśl Wojskowa" 2005, nr 2; J. Kręcikij, *Działania sieciocentryczne: wybrane problemy*, AON, Warszawa 2008; J. Kręcikij, J. Posobiec,

Zarządzanie bezpieczeństwem militarnym w erze sieciowych powiązań informacyjnych. Dowodzenie, Międzynarodowa Fundacja „Scientia, Ars, Educatio", Kraków 2013; J. Kręcikij, J. Wołejszo, *Geneza i istota prowadzenia działań w środowisku sieciocentrycznym*, [w:] *Podstawy dowodzenia w aspekcie działań sieciocentrycznych*, J. Wołejszo, J. Kręcikij (red.), AON, Warszawa 2013; M. Majorek, S. Olszyk, M. Winiarska-Brodowska, *Cyberpolityka. Internet jako przestrzeń aktywności politycznej*, Texter, Warszawa 2018; J. Posobiec, *Dowodzenie w środowisku sieciocentrycznym. Rozprawa habilitacyjna*, „Zeszyty Naukowe AON" 2015, nr 1; J. Posobiec, J. Trembecki, A. Zarkowski, *System dowodzenia w działaniach sieciocentrycznych pk. „Układ"*, AON, Warszawa 2007; S. Olszyk, *Sieciocentryzm jako doktryna militarna,* „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 4; T. Szubrycht, *Sieciocentryczność – mity i rzeczywistość*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2004, vol. 40, nr 4; *Vademecum bezpieczeństwa informacyjnego*, t. 1–2, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. Wrzosek, *Wojny przyszłości. Doktryna, technika, operacje militarne*, Fronda, Warszawa 2018.

KONFLIKT MIĘDZYNARODOWY – bezpośrednie lub pośrednie starcie sprzecznych interesów 2 lub więcej stron (państw, grup państw, narodów, ruchów politycznych) wynikłe z istniejących sporów o subiektywnym lub obiektywnym charakterze, ukierunkowane na osiągnięcie celów przez strony konfliktu. Spory między państwami mogą być terytorialne, narodowe, religijne, ekonomiczne, wojskowo-strategiczne, naukowo-techniczne itd. Przedmiotami konfliktu międzynarodowego mogą być państwa, międzypaństwowe stowarzyszenia, organizacje międzynarodowe, zorganizowane siły społeczne i polityczne w kraju lub na arenie międzynarodowej. Konflikt międzynarodowy można interpretować jako przedłużający się stan aktywnej lub biernej walki między 2 lub kilkoma uczestnikami stosunków międzynarodowych w zakresie wdrażania ich interesów, które są niezgodne z interesami przeciwnej strony. Podczas konfliktu może zmienić się charakter zainteresowanych stron w konflikcie, zwiększać się liczba uczestników, mogą zmieniać się bezpośrednie albo drugorzędne podmioty konfliktu. Na ogół konflikt zawsze przybiera formę polityczną, ponieważ różnice między państwami są uświadamiane i rozwiązywane na polu polityki wewnętrznej, zagranicznej i wojskowej. Konflikty międzynarodowe są przejawem występujących sporów,

dowodem niemożności, a niekiedy niechęci odnalezienia satysfakcjonującego strony rozwiązania.

Na podstawie analizy struktur konfliktów międzynarodowych można wyróżniać ich charakterystyczne cechy, co pozwala przedstawić ich typologię. Jednocześnie należy podkreślić, że każdy konflikt jest specyficzny i niepowtarzalny. Żaden z istniejących lub już uregulowanych konfliktów nie był dokładną kopią innego, można więc mówić tylko o pewnych przybliżeniach w wyznaczaniu typowych cech konfliktów międzynarodowych, które służy uzyskiwaniu → i n f o r m a c j i i analizie innych, poszczególnych konfliktów.

Klasyfikacje konfliktów międzynarodowych uwzględniają: sferę działania, typy zaangażowanych stron; charakter stosunków społeczno-politycznych, stopień zorganizowania, poziom eskalacji itd. Wyjątkowo ważny jest podział międzynarodowych konfliktów na militarne i niemilitarne. Ponadto wśród konfliktów zbrojnych wyróżnia się „nowe" i „klasyczne". W szczególności amerykańska badaczka M. Kaldor przeciwstawiła nowe → w o j n y [t. 4] starym, uwzględniając cele, metody walki, a także sposoby ich finansowania.

Konflikt można uznać za międzynarodowy, gdy:

- odbywa się on z udziałem podmiotów stosunków międzynarodowych,
- ma wpływ na obecny stan międzynarodowych relacji.

W tym kontekście uwagę zwraca problem postrzegania konfliktów międzynarodowych jako rozgrywających się przede wszystkim między państwami, co ogranicza możliwość uznania za międzynarodowe konfliktów między innymi podmiotami. Tymczasem szerokie rozumienie konfliktu pozwala identyfikować całość związanych z nim czynników. W związku z tym klasyczne podejście C. von Clausewitza, który twierdził, że wojna jest niczym innym jak kontynuacją stosunków politycznych między państwami za pomocą innych środków, wymaga ponownego rozpatrzenia.

Z jednej strony, jeśli uznamy państwa za głównych uczestników stosunków międzynarodowych, to oprócz najbardziej radykalnej formy rozwiązania sporów, czyli konfliktu zbrojnego, dysponują one wieloma innymi środkami, takimi jak presja ekonomiczna, dyplomatyczne *démarche*, działalność agenturalna i wywrotowa, otwarta i niejawna propaganda, mechanizmy działalności organizacji międzynarodowych itp. Z drugiej

strony współczesne stosunki międzynarodowe charakteryzują się szerokim zakresem form współpracy pozapaństwowej, które wręcz wypierają państwo z niektórych sektorów działalności międzynarodowej. Zwłaszcza dziś walka zbrojna może toczyć się między nieregularnymi quasi-państwami, religijnymi lub etnicznymi organizacjami, separatystami, partyzantami, organizacjami terrorystycznymi czy gangami przestępczymi, prywatnymi jednostkami bojowymi itp. Zgodnie z tezą Barry'ego Buzana państwo nie występuje już jako główny podmiot wojny, chociaż nie można umniejszać jego statusu.

Przyczynami konfliktów międzynarodowych mogą być:

- sprzeczne interesy i możliwości (szczególne różnice społeczno-kulturowe i podobieństwa między stronami),
- znacząca zmiana układu sił,
- indywidualne spostrzeżenia i oczekiwania,
- zaburzona struktura oczekiwań,
- ubóstwo i nierówność,
- układ społeczno-ekonomiczny,
- ustrój polityczny,
- spory terytorialne,
- pragnienie konfliktu,
- ustrojem przynajmniej jednej ze stron jest → r e ż i m [t. 3] autorytarny lub totalitarny,
- zakłócenie *status quo*,
- nierozwiązane problemy międzynarodowe: surowcowo-energetyczne, ekologiczne, wykorzystanie mórz i oceanów, kosmosu,
- wiara w zwycięstwo w konflikcie,
- konflikty ról międzynarodowych państw, np. konflikty między rolami narzucanymi z zewnątrz i wybieranymi przez państwo,
- błędna ocena stanu stosunków międzynarodowych i stanu → b e z p i e c z e ń s t w a [t. 1] państw.

Są one potęgowane przez:

- odmienność społeczno-kulturową,
- nierówności w rozwoju gospodarczym, ekonomicznym i finansowym państw i narodów,
- zbrojenia i towarzyszący im wyścig zbrojeń,

- subiektywizm w formułowaniu celów polityki zagranicznej, zwłaszcza obecność w niej elementów egoizmu i → n a c j o n a l i z m u [t. 3],
- zdecentralizowaną lub słabą, narzuconą władzę państwową,
- różnicę statusu stron,
- naciski,
- polaryzację systemu (centralizacja siły przymusu),
- słabość *status quo*,
- zagrożoną wiarygodność,
- parytet siły,
- konflikty etniczne, narodowe, społeczne, klasowe,
- potęgę państwa – im większa potęga państwa, tym bardziej globalne są jego kontakty i interesy, tym większe również obawy władzy o swoją reputację.

Jedną z najbardziej wszechstronnych typologii konfliktów międzynarodowych zaproponowali P. Braillard i M.-R. Djalili. Autorzy porządkują konflikty wg przyczyn, motywacji ich uczestników oraz skali konfliktów: Do pierwszej grupy konfliktów międzynarodowych należą klasyczne konflikty międzypaństwowe, międzypaństwowe konflikty z tendencją do integracji, narodowo-wyzwoleńcze wojny itp. Druga grupa obejmuje zarówno terytorialne, jak i nieterytorialne konflikty o motywach społeczno-ekonomicznych, ideologicznych, statusowych lub innych. W zależności od skali konflikty dzieli się na wielkie, czyli takie, które są zdolne do rozwijania się w światowe konflikty i w których uczestniczy duża liczba państw, oraz regionalne, subregionalne i ograniczone (wg liczby państw).

Zrozumienie natury konfliktów międzynarodowych i znalezienie sposobów ich rozwiązania wymaga, oprócz wyjaśnienia ich przyczyn, ustalenia głębokości i charakteru poszczególnych konfliktów, w czym pomocne okazują się ich klasyfikacje. Najbardziej rozpowszechnioną na Zachodzie jest tradycyjna typologia konfliktów, zgodnie z którą wyróżnia się: → k r y z y s y m i ę d z y n a r o d o w e; konflikty o niskiej intensywności; → t e r r o r y z m [t. 4]; → w o j n y d o m o w e [t. 4] i rewolucje, które nabierają charakteru międzynarodowego; wojny i wojny światowe.

Kryzys międzynarodowy to sytuacja konfliktowa, w której:

- dotknięte zostają żywotne interesy podmiotów polityki międzynarodowej;

- na podjęcie decyzji podmioty mają bardzo ograniczony czas;
- wydarzenia rozwijają się zwykle w sposób nieprzewidywalny;
- sytuacja nie przeradza się jednak w konflikt zbrojny.

Taki → k r y z y s to zatem jeszcze nie wojna, lecz raczej przykład sytuacji „ani pokoju, ani wojny". Jest to rodzaj relacji pomiędzy podmiotami stosunków międzynarodowych, w których żadna ze stron nie chce wojny lub → p r z e m o c y [t. 3], ale obie uważają swoje cele za na tyle ważne, aby ryzykować dla nich ewentualnym wybuchem wojny.

Konflikty o niskiej intensywności to relacja między państwowymi i niepaństwowymi podmiotami na poziomie regionalnym lub państwowym. Stosunki między państwowymi i niepaństwowymi podmiotami dość często wiążą się z małymi potyczkami na granicach, indywidualną lub nieznaczną grupową przemocą. Ich niebezpieczeństwo zaczęto sobie uświadamiać właśnie teraz. Taki konflikt może zmienić się w pełnowymiarowy, ponadto nowoczesne uzbrojenie wojskowe nawet w konflikcie o niskiej intensywności może doprowadzić do poważnych zniszczeń. W warunkach ścisłego powiązania nowoczesnych suwerennych państw naruszenie pokoju w jednym regionie ma wpływ na wszystkie pozostałe.

Terroryzm jest formą przemocy politycznej, która jest skierowana przeciwko rządom poszczególnych państw, choć często cierpią przez niego zwykli ludzie, a jego celem jest wytworzenie atmosfery strachu. Wiele państw wspiera działalność terrorystyczną – np. Iran, Libia i Syria – jednocześnie zaprzeczając swojemu zaangażowaniu w działalność terrorystyczną.

Wojny domowe i rewolucje stają się konfliktami międzynarodowymi w przypadku, gdy państwo lub jedna z walczących stron uzyskuje wsparcie postronnych sił politycznych, państw lub organizacji, które często są żywotnie zainteresowane konkretnymi rezultatami. To konflikty w tym samym państwie między dwiema lub więcej stronami ze względu na różnice poglądów na temat przyszłego systemu politycznego lub różnic klanowych. Wojny domowe i rewolucje są nierzadko okrutne i krwawe, 10 z 13 najbardziej krwawych konfliktów XIX i XX w. było właśnie wojnami domowymi.

Wojna to konflikt na szeroką skalę pomiędzy państwami dążącymi do osiągnięcia swoich celów politycznych poprzez zorganizowane

walki zbrojne. Częstokroć instrumenty międzynarodowej reakcji, takie jak →Rada Bezpieczeństwa ONZ [t. 3] czy →Międzynarodowy Trybunał Karny [t. 3], pozostają bezsilne, są ignorowane lub dyskredytowane.

Wojna światowa zaczyna się, gdy do konfliktu wojskowego są zaangażowane grupy państw, które realizują swoje cele globalne, co prowadzi do znacznych strat ludzkich i materialnych.

Naukowcy twierdzą, że w ciągu ostatnich 5,5 tys. lat ludzkość żyła w pokoju łącznie tylko przez 300 lat, doliczono się ok. 14,5 tys. wojen (w tym dwóch światowych), w których zginęło 3,6 mld osób. Po zakończeniu II wojny światowej doszło do ponad 250 wojen, w które było zaangażowanych ponad 90 państw, a straty wyniosły ponad 35 mln osób.

Praktyka stosunków międzynarodowych pozwala twierdzić, że wojnę rzadko wywołuje jeden czynnik. Źródłem sporów są głównie interesy danych państw, unii gospodarczych i bloków polityczno-wojskowych. Ich przedmiotem są często terytoria i granice, chęć posiadania dominującej pozycji w regionie, sporne interesy ekonomiczne i polityczne krajów, negatywne stereotypy etniczne i religijne.

Artykuł 33 Karty Narodów Zjednoczonych wyznacza sposoby regulacji międzynarodowych sporów i konfliktów, które mogą doprowadzić do naruszenia pokoju między narodami. Dokument ten zobowiązuje państwa członkowskie ONZ do przestrzegania zasad sprawiedliwości i prawa. Dąży się do tego, by stosować negocjacje, kompleksowo badać występujące problemy, wykorzystywać doświadczenie i możliwości działania mediatorów i arbitrów, odnajdywać wyjście z sytuacji konfliktowych drogą pokojową przy pomocy służb dyplomatycznych. Do najsłynniejszych prób pokojowego rozwiązania sporów międzynarodowych należy mediacja ONZ w przypadku Afganistanu. Po długich i trudnych negocjacjach w Genewie w 1988 r. została podpisana umowa pokojowa z udziałem Afganistanu, Pakistanu i ZSRR o wycofaniu wojsk radzieckich (130 tys. żołnierzy) na początku 1989 r.

Szukając rozwiązań, strony konfliktu coraz rzadziej uciekają się do dyplomacji, coraz częściej do użycia siły. Rola dyplomacji, ONZ i innych organizacji międzynarodowych w zapobieganiu konfliktom i ich rozwiązywaniu jest coraz bardziej ograniczona. Napięte stosunki i nieufność

między stałymi członkami Rady Bezpieczeństwa ONZ zahamowały prace tego ważnego światowego forum na rzecz zachowania międzynarodowego pokoju i bezpieczeństwa.

Większość współczesnych konfliktów została rozdrobniona i spleciona z → ekstremizmem i międzynarodowym terroryzmem w takim stopniu, że trudno jest opracować metodę lub podjąć konkretne kroki w celu położenia kresu walkom i przemocy.

Konflikty zbrojne zwykle rozpoczynają się i rozwijają w krajach, w których instytucje rządowe są słabe i nie są w stanie sprostać ani wyzwaniom gospodarczym, ani dodatkowym czynnikom takim jak migracja, → przestępczość zorganizowana [t. 3], nielegalny handel bronią i narkotykami, terroryzm itp.

W takich okolicznościach państwa tracą legitymację i kontrolę nad sytuacją, stając się z reguły jedną ze stron konfliktu. Pojawienie się potężnych zbrojnych podmiotów niepaństwowych o znacznych zdolnościach finansowych i wojskowych, mających cele polityczne, gospodarcze lub kryminalne dodatkowo komplikuje sytuację, przedłużając konflikty zbrojne i stwarzając przeszkody dla odnalezienia rozwiązania politycznego. Szczególnie niebezpieczna jest zmowa między grupami takimi jak organizacje terrorystyczne i przestępcze oraz ich wspólne działania na szczeblu międzynarodowym. Dalszy niepokój budzi fakt, że brutalny ekstremizm rozprzestrzeniający się za pośrednictwem mediów, sieci regionalnych i poprzez sprawowanie kontroli nad terytorium stał się stałym elementem wielu konfliktów.

Masowe i – bardzo często – zorganizowane łamanie → praw człowieka [t. 3], praw uchodźców i międzynarodowego prawa humanitarnego to jedna z cech konfliktów zbrojnych mających miejsce we współczesnym świecie.

Międzynarodowe wysiłki dyplomatyczne i polityczne na rzecz zapobiegania, kontroli i pokojowego rozwiązywania konfliktów nadal pozostają jedyną możliwą odpowiedzią na problem konfliktów międzynarodowych. Zapobieganie musi leżeć u podstaw wszystkich podejmowanych starań. Wymaga to jednak znacznie wyższego poziomu jedności międzynarodowej, szczególnie w Radzie Bezpieczeństwa ONZ jako najwyższym organie zajmującym się utrzymaniem międzynarodowego pokoju i systemu

bezpieczeństwa zbiorowego. Konieczna jest także większa pomoc międzynarodowa dla słabszych krajów o podatnych na zranienie instytucjach, aby mogły skutecznie radzić sobie z problemami gospodarczymi i społecznymi. Ponadto potrzebne jest nawiązanie dialogu ze wszystkimi podmiotami zaangażowanymi w konflikty, w tym uzbrojonymi podmiotami niepaństwowymi, a także ustanowienie międzynarodowej kontroli nad stosowaniem nowych technologii, aby zapobiec ich nadużyciom. Rozstrzygając spory dotyczące konfliktów międzynarodowych, należy analizować je w świetle obowiązującego prawa międzynarodowego, nie kwestionując go i mając na uwadze przede wszystkim zasadę praworządności.

Stosunki międzynarodowe są bardzo podatne na nieporozumienia, co może mieć katastrofalne konsekwencje np. wtedy, gdy konflikt zbrojny nasila się właśnie z powodu zniekształconego lub selektywnego postrzegania sytuacji. Czynnikami przyczyniającymi się do eskalacji konfliktu mogą być normatywne wzmacnianie wojowniczych postaw w trakcie konfliktu oraz przekonania – często będące wynikiem manipulacji – uniemożliwiające osobom i grupom głęboko zaangażowanym w konflikt aktywne uczestniczenie w jego deeskalacji.

Olga Wasiuta

P. Boniface, *Atlas wojen XXI wieku. Konflikty współczesne i w przyszłości*, tłum. A. i Z. Dominik, Bellona, Warszawa 2001; K. Boulding, *Conflict and Defense. A General Theory*, Harper, New York 1962; P. Braillard, M.-R. Djalili, *Les relations internationals*, Presses Universitaires de France, Paris, 1988; B. Buzan, *Rethinking Security After the Cold War*, „Cooperation and Conflict" 1997, no. 32; Z. Cesarz, *Konflikty zbrojne jako problem międzynarodowy*, [w:] *Problemy polityczne współczesnego świata*, Z. Cesarz, E. Stadtmüller (red.), Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 1996; J. Dougherty, R. Pfaltzgraff, *Contending Theories of International Relations*, Longman, New York 2001; J. Galtung, *A Structural Theory of Agression*, „Journal of Peace Research" 1964, no. 2; M. Kaldor, *New and Old Wars: Organized Violence in a Global Era*, Polity, Cambridge 2001; K. Kubiak, *Wojny, konflikty zbrojne i punkty zapalne w świecie*, Trio, Warszawa 2007; J. Kukułka, *Zaspokajanie potrzeb i rozwiązywanie konfliktów w stosunkach międzynarodowych*, [w:] *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (red.), Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2006; W. Malendowski, *Spory i konflikty międzynarodowe*, [w:] *Stosunki międzynarodowe*,

W. Malendowski, C. Mojsiewicz (red.), Wrocławskie Wydawnictwo Naukowe Atla 2, Wrocław 2004; W. Malendowski, *Zbrojne konflikty i spory międzynarodowe u progu XXI wieku: analiza problemów i studia przypadków*, Wrocławskie Wydawnictwo Naukowe Atla 2, Warszawa 2003; K. Pawłowski, *Spory i konflikty międzynarodowe*, [w:] *Międzynarodowe stosunki polityczne*, M. Pietraś (red.), Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2006; O. Wasiuta, *Konflikt międzynarodowy*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017; Q. Wright, *The Study of International Relations*, Appleton-Century-Crofts, New York 1955.

KONFLIKT NIEMIĘDZYNARODOWY – współczesne konflikty zbrojne najczęściej mają charakter międzynarodowy, dlatego że państwa nie chcą być postrzegane jako naruszyciele prawa międzynarodowego. Starają się one osiągać swoje cele polityczne za pomocą tzw. →wojen zastępczych [t. 4] (ang. *proxy wars*), najczęściej wtedy można mówić o niemiędzynarodowym charakterze konfliktów.

By można było mówić o konflikcie zbrojnym o charakterze niemiędzynarodowym, musi zostać spełniona jedna podstawowa przesłanka – musi mieć miejsce konflikt zbrojny. Wymóg istnienia konfliktu zbrojnego przewiduje zarówno art. 3 wspólny dla konwencji genewskich, jak i II protokół dodatkowy z 1977 r. Konwencja stanowi, iż art. 3 stosuje się „gdyby na terytorium jednej z Wysokich Umawiających się Stron wybuchł konflikt zbrojny nieposiadający charakteru międzynarodowego".

W zależności od sytuacji mogą wystąpić działania zbrojne między rządowymi siłami zbrojnymi a niepaństwowymi grupami zbrojnymi lub tylko między tymi grupami.

Protokół dodatkowy II do konwencji genewskiej z dnia 12 sierpnia 1949 r. rozwija i uzupełnia art. 3 wspólnego, nie zmieniając istniejących warunków stosowania, wprowadza wymóg kontroli terytorialnej. Protokół dodatkowy II wyraźnie odnosi się tylko do konfliktów zbrojnych między siłami zbrojnymi państwa a innymi zorganizowanymi grupami zbrojnymi. W przeciwieństwie do art. 3 wspólnego protokół nie ma zastosowania do konfliktów zbrojnych występujących tylko między niepaństwowymi grupami zbrojnymi.

Profesor E. la Haye uznaje, że konflikt zbrojny w rozumieniu art. 3 ma miejsce w sytuacji zaistnienia wrogich działań zbrojnych na terytorium jednego państwa, pomiędzy regularnymi siłami zbrojnymi i zorganizowanymi grupami zbrojnymi lub też pomiędzy zorganizowanymi grupami zbrojnymi. Działania zbrojne muszą być poważne i przedłużające się. Podobne stanowisko zaprezentował Międzynarodowy Trybunał Karny dla byłej Jugosławii (MTKJ) w sprawie D. Tadzić, kiedy stwierdził m.in., iż konflikt zbrojny istnieje, gdy „następuje odwołanie się do sił zbrojnych państw lub dochodzi do przedłużających się działań wrogich pomiędzy rządem a zorganizowanymi grupami zbrojnymi lub też pomiędzy samymi grupami na terenie danego państwa". Przy określaniu wymienionych czynników wskazujących na zaistnienie konfliktu zbrojnego sąd winien analizować nie tylko stopień organizacji grup walczących, ale również czas trwania oraz intensywność działań zbrojnych. W tym samym orzeczeniu MTKJ stwierdził, że normy wynikające z art. 3 mają zastosowanie nie tylko w miejscu, w którym toczy się konflikt, ale na całym terytorium znajdującym się pod kontrolą stron walczących. Oznacza to, że art. 3 wspólny obowiązuje również w miejscu, gdzie nie są toczone walki.

Konflikt zbrojny powoduje zastosowanie → m i ę d z y n a r o d o w e g o p r a w a h u m a n i t a r n e g o k o n f l i k t ó w z b r o j n y c h [t. 3]. W takiej sytuacji w zależności od stopnia zorganizowania stron walczących oraz przestrzegania prawa humanitarnego możemy mieć do czynienia z konfliktem regulowanym przez:

- art. 3 wspólny dla konwencji genewskich z 1949 r. i prawa zwyczajowe,
- art. 3 i protokół dodatkowy II do konwencji genewskich z 1977 r. i prawo zwyczajowe.

Piotr Łubiński

A. Cassese, *The Status of Rebels under the 1977 Geneva Protocol on Non-International Armed Conflicts*, „International & Comparative Law Quarterly" 1981, vol. 30, iss. 2; A. Cullen, *The Concept of Non-International Armed Conflict in International Humanitarian Law*, Cambridge University Press, Cambridge 2010; H.-P. Gasser, *Internationalized Non-International Armed Conflicts: Case Studies of Afghanistan, Kampuchea, and Lebanon*, „American University Law Review"

1983, vol. 33; P. Łubiński, *Stosowanie MPHKZ w konfliktach międzynarodowych i niemiędzynarodowych. Kwestia stosowania praw człowieka w rejonie odpowiedzialności PKW*, [w:] *Międzynarodowe prawo humanitarne konfliktów zbrojnych. Materiał szkoleniowy dla oficerów*, Z. Falkowski (red.), Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014; W.A. Schabas, *Punishment of Non-State Actors in Non-International Armed Conflict*, „Fordham International Law Journal" 2002, vol. 26; S. Sivakumaran, *The Law of Non-International Armed Conflict*, Oxford Univeristy Press, Oxford 2012.

KONFLIKT ZAMROŻONY (także konflikt tlący się) – to sytuacja w stosunkach międzynarodowych, w której aktywne walki zakończyły się lub ustąpiły, ale nie ma porozumienia pokojowego poza niepewnym zawieszeniem broni; kiedy konflikt zbrojny między stronami zostaje zakończony bez podpisania traktatu pokojowego lub innego politycznego rozwiązania konfliktu. Dlatego legalnie konflikt może rozpocząć się od nowa w dowolnym momencie, tworząc środowisko niepewności i niestabilności. Konflikt zamrożony oznacza sytuację, w której nie ma aktywnej akcji militarnej między walczącymi stronami i z reguły kończy się naciskiem stron trzecich bez rozwiązywania sporów między stronami, a zatem bez zawarcia traktatu pokojowego, pogłębiając niezgodę, przekładając starcia między stronami konfliktu na poziom konfrontacji prawnej, ekonomicznej, publicznej (między społecznościami) i kulturowej. Z reguły zamrożone konflikty trwają latami i mogą od czasu do czasu prowadzić do otwartej konfrontacji zbrojnej. Sekretarz obrony USA A. Carter w wywiadzie z maja 2018 r. podkreślił, że „zamrożony konflikt" to wynalazek Rosji dla potrzeb wojskowo-politycznych, a nie koncepcja zachodnia.

Choć po zakończeniu II wojny światowej na kontynencie europejskim znacząco spadła częstotliwość dużych konfliktów zbrojnych, to pokój nie jest powszechny. Wiele → w o j e n [t. 4] o skali regionalnej i lokalnej po fazie „gorącej" przyjmuje formę konfliktów zamrożonych. Konflikty tego typu jako zjawisko polityczne można uznać za porażkę nowoczesnej dyplomacji, ponieważ ich pojawienie się stanowi podwaliny dla kolejnych konfliktów. W → g e o p o l i t y c e stały się one modelem rozwiązywania sporów terytorialnych, więc na współczesnej mapie Europy konflikty zamrożone pojawiają się coraz częściej.

Pojęcie konfliktu zamrożonego zyskało popularność w latach 90. XX w. po rozpadzie Związku Radzieckiego. Chociaż nie ma ustabilizowanej definicji, jest używane do opisania sytuacji pokonfliktowej, w której →przemoc [t. 4] zbrojna w dużej mierze dobiegła końca, ale napięcie leżące u podstaw konfliktu nadal się utrzymuje. Używane jest do opisu konfliktów w obszarze postradzieckim, konfliktu na Cyprze, w Abchazji, Osetii Południowej, Naddniestrzu czy Półwyspie Koreańskim. Faktyczna sytuacja konfliktu może nie odpowiadać oficjalnym roszczeniom wysuwanym przez strony, dobrym przykładem jest konflikt między Republiką Korei a Koreańską Republiką Ludowo-Demokratyczną – wysuwane są różne roszczenia, istnieje jednak dobrze określona granica między terytoriami obu państw.

Rozpad Związku Radzieckiego spowodował, że Rosja utraciła kontrolowaną strefę buforową. Wywoływanie zamrożonych konfliktów w pobliżu jej granic uniemożliwia dotkniętym państwom, takim jak Mołdawia i Gruzja, dołączenie do zachodnich instytucji i organizacji. Aby zapobiec zbliżaniu się krajów Europy Wschodniej do UE i →NATO [t. 3], Federacja Rosyjska celowo tworzy tam konflikty. Jak podkreślił gen. P.M. Breedlove, były głównodowodzący połączonych sił zbrojnych NATO w Europie:

> jeśli Rosja obawia się, że któryś z krajów pragnie zbliżenia z Zachodem, rozwiązaniem okazuje się inwazja, zamrożony konflikt, przez który NATO będzie obawiać się wzięcia tego kraju na pokład Sojuszu, ponieważ oznaczałoby to konflikt z Rosją.

Wykorzystywanie podziałów etnicznych i tworzenie kontrolowanej niestabilności w postaci zamrożonych konfliktów jest stosunkowo nowym sposobem osiągania celów geopolitycznych Rosji. Federacja Rosyjska dąży do kontrolowania procesów zachodzących w obszarze postradzieckim i niedopuszczenia do tego, aby państwa obszaru znalazły się poza orbitą jej wpływów. Utrzymanie napięcia w strefach zamrożonych konfliktów pozwala wpływać nie tylko na politykę wewnętrzną tych państw, ale także na politykę UE i NATO, do członkostwa w których te państwa aspirują.

Zamrożone konflikty występują w regionach krajów, nad którymi kontrolę utraciły władze centralne. Strefy takie podlegają jurysdykcji

separatystów, którzy prowadzą pokojowy dialog z urzędnikami państwowymi w celu wzmocnienia swoich rządów. Brak pokojowych rozwiązań problemu nie prowadzi do większych operacji zbrojnych, a konflikty skazane są na nierozwiązanie.

Główną cechą konfliktu „zamrożonego" jest unikanie najgorszych skutków, powiązanych z kontynuacją działań wojennych: ofiar wśród personelu wojskowego, →ludności cywilnej [t. 3], osób wewnętrznie przesiedlonych, strat materialnych i zniszczenia. Ponadto zamrożony konflikt umożliwia państwu, na którego terytorium konflikt ma miejsce, oszczędzanie środków wydawanych na utrzymanie niekontrolowanych przez nie regionów. Ostatecznie ta sytuacja pozwala skupić się na rozwiązywaniu problemów wewnętrznych, budowaniu konkurencyjnej gospodarki, sprawnej armii, przygotowując swój plan pokojowy. Tak np. rzeczywista utrata kontroli nad separatystycznymi regionami Gruzji nie przeszkodziła państwu (bardziej skutecznie) i Mołdawii (mniej skutecznie) w przeprowadzeniu ważnych reform w kierunku integracji europejskiej.

Konflikty tego typu przynoszą jednak szereg wyzwań dla państw:

- Zamrożone konflikty są skutecznym narzędziem nacisku ze strony zewnętrznych graczy. Np. konflikty w Abchazji, Osetii Południowej i Naddniestrzu pozostają najskuteczniejszą formą nacisku Rosji na Gruzję i Mołdawię, która od czasu do czasu przejawia się w formie prowokacji militarnych lub szantażu politycznego.
- Nieuregulowany konflikt oddala niekontrolowane regiony od państwa i sprawia, że ich ponowna integracja staje się coraz trudniejsza. W ciągu ostatnich prawie 30 lat w Abchazji, Osetii Południowej, Naddniestrzu i Górskim Karabachu wyrosły całe pokolenia, których tożsamość w dużym stopniu nie opiera się na związku z Gruzją, Mołdawią czy Azerbejdżanem.
- Zamrożone konflikty stają się przyczółkiem dla przemytu towarów, broni, handlu narkotykami i innych →zagrożeń [t. 4]. Zjawiska te stają się dochodowym biznesem dla obu stron konfliktu, jeśli linia frontu pozostaje niezmieniona przez długi czas.
- Nierozwiązane konflikty mogą wywołać ostre społeczne i polityczne spory dotyczące możliwości ich rozwiązania – od siłowego przejęcia władzy po odłączenie się podmiotów separatystycznych.

Praktycznie każdy z sąsiadów Rosji jest nękany przez → separatyzm [t. 4]. To nie przypadek. Mimo że znajdują się na peryferiach Europy, konflikty te mają daleko idący wpływ na lokalne, regionalne i międzynarodowe struktury → bezpieczeństwa [t. 1]. Wpływają na realia milionów ludzi i stawiają społeczność międzynarodową przed trudnymi wyzwaniami. Rosja utrzymuje bazy wojskowe na oderwanych terytoriach Abchazji, Osetii Południowej i Naddniestrza dla pogłębienia swoich wpływów.

Wpływ konfliktów zamrożonych na poziom bezpieczeństwa w Europie nie może pozostawać niezauważony i niedoceniany, zwłaszcza że jest on zdecydowanie negatywny. Brak działania i zaniechania w tym obszarze mogą mieć poważne konsekwencje zwłaszcza dlatego, że nie można przewidzieć, czy i kiedy ten czy inny konflikt z fazy „zamrożonej" przejdzie ponownie do fazy „gorącej" i jakie będą tego skutki, włącznie z możliwością rozprzestrzenienia się walki zbrojnej na kolejne kraje.

Wydaje się, że wiele krajów europejskich zwraca większą uwagę na utrzymywanie prawidłowych stosunków z Rosją niż na angażowanie się w spory peryferyjne. Rosja utrzymuje zamrożone konflikty w obszarze postradzieckim, utrudniając w ten sposób rozwój integracji euroatlantyckiej regionu. Rosja, która jest jednym z głównych graczy w tych konfliktach, najczęściej dyktuje swoje warunki, najpierw przejmując dane terytorium i tworząc → kryzys, a później deklarując konieczność rozwiązania tego kryzysu. Rosja faktycznie przejęła część Gruzji, teraz to samo dzieje się w Ukrainie. Zdaniem ekspertów nie należy oczekiwać, że obecne rosyjskie kierownictwo w przyszłości odmówi zastosowania zamrożonych konfliktów w swojej polityce zagranicznej. Ta polityka może być stosowana tak długo, jak długo będzie utrzymywał się obecny → reżim [t. 3] w FR.

1 października 2015 r. Parlament Europejski zorganizował konferencję „Jak rozwiązać zamrożone konflikty w Europie Wschodniej", skłaniając do omówienia obecnej sytuacji w „gorących punktach" regionu i sposobów jej ustabilizowania. UE widzi pilną potrzebę rozwiązania zamrożonych konfliktów w oparciu o wartości demokratyczne i → prawa człowieka [t. 3].

Okupacja zbrojna i zamrożenie konfliktów zaistniały wg podobnych scenariuszy w Mołdawii, Gruzji i Ukrainie. Wydarzenia te doprowadziły do przedłużającego się → kryzysu humanitarnego na okupowanych

terytoriach, nie ma jasnych zasad rozwiązywania takich konfliktów. Z powodu braku pełnej suwerenności nad prowincjami kraje wymienione nie mogą prowadzić w pełni niezależnej polityki zagranicznej. Jak dotąd Moskwa podjęła kroki w celu powstrzymania euroatlantyckich aspiracji tych państw, ponieważ ani NATO, ani UE nie zezwalają na członkostwo krajom, które nie są w stanie uzyskać pełnej władzy nad swoimi terytoriami. Szczególną uwagę należy zwrócić na sytuację w Górskim Karabachu jako interesujący przykład zamrożonego konfliktu bez bezpośredniego udziału Moskwy.

Pod rządami Putina Rosja utrwaliła lub wytworzyła zamrożone konflikty, które dotykają Armenię, Azerbejdżan, Mołdawię, Gruzję i Ukrainę. W każdym przypadku Kreml zachowuje zdolność do stłumienia lub eskalacji napięć w razie potrzeby, aby zmaksymalizować swój wpływ polityczny na dany kraj. Moskwa stosuje tę taktykę zgodnie ze swoimi celami dla określonego kraju lub regionu. W przypadku pobliskich państw członkowskich UE i NATO celem jest utrudnienie lub uniemożliwienie prozachodniego kursu oraz wyrwania się spod wpływów Rosji. Putin w gruncie rzeczy ustanowił doktrynę ograniczonej suwerenności sąsiadów Rosji, zwłaszcza tych państw, które były częścią Związku Radzieckiego. Taktyka Kremla ma na celu utrzymanie tych krajów w strachu i niepewności, wykorzystując destabilizację, propagandę i presję ekonomiczną, aż po bezpośrednią inwazję, a celem tych środków jest utrudnienie lub uniemożliwienie.

Rosja wykorzystywała również wydawanie rosyjskich paszportów, aby wciągnąć społeczeństwa uczestniczące w zamrożonych konfliktach lub potencjalnie zaangażowane w przyszłe konflikty w orbitę swoich wpływów i uzasadnić swoje ingerencje w sprawy sąsiednich państw. Zamiast podbić cudzoziemców, władze rosyjskie przekształcają ich w obywateli rosyjskich, a następnie domagają się prawa do obrony przed tym, co było ich własnym udziałem. Ok. 90% osób mieszkających w oderwanym regionie Gruzji, Osetii Południowej, ma rosyjskie paszporty, które są dostępne dla każdego, kto nadal ma radzieckie dokumenty lub przynajmniej jednego przodka, który był stałym rezydentem Rosji.

→ A g r e s j a [t. 1] Rosji na Ukrainę spowodowała po raz kolejny powrót dyskusji na temat konfliktów zbrojnych o niskiej intensywności. Zdaniem części analityków również konflikt w Donbasie zmierza do osiągnięcia statusu konfliktu zamrożonego, co uczyniłoby go kolejnym

potencjalnym punktem zapalnym na obszarze byłego ZSRR. Putin nie może również dopuścić do zakończenia konfliktu we wschodniej Ukrainie, ponieważ zagroziłoby to jego kontroli nad siłami bezpieczeństwa i wojskiem we własnym kraju. Jednocześnie nie może pozwolić rządowi w Kijowie odnieść sukcesu, ponieważ pokazałoby to narodowi Federacji Rosyjskiej skuteczną demokratyczną alternatywę. Wywołanie niestabilności ma kluczowe znaczenie dla strategii Kremla. Ukraina musi pilnie podjąć wysiłek reform, rosyjska inwazja w pewnym stopniu może służyć rządowi w Kijowie za katalizator wprowadzenia niezbędnych zmian. Z drugiej strony trwający konflikt odwraca od nich uwagę ukraińskich władz, zmuszając do poświęcenia walce dużej ilości czasu i zasobów.

W przeciwieństwie do konfliktu w Naddniestrzu sytuacja w Donbasie jest bardziej umiędzynarodowionym konfliktem. Konfliktu na wschodzie Ukrainy nie można uznać za konflikt zamrożony, przekonuje o tym przewodniczący Zgromadzenia Parlamentarnego OBWE G. Tsereteli oraz gen. armii USA, były szef CIA i głównodowodzący wojsk USA w Iraku oraz Afganistanie D. Petraeus. Kontynuowane są działania wojskowe, ukraińscy → ż o ł n i e r z e [t. 4] chronią → s u w e r e n n o ś ć [t. 4] swojego kraju i miejscowej ludności. Sankcje USA i UE wobec Rosji są związane z tym konfliktem, w związku z czym jego zamrożenie nie odpowiada interesom Kremla. Z kolei nierozwiązany kryzys w Ukrainie przeszkadza międzynarodowym graczom rozwijać współpracę z Rosją. Chociaż w przypadku innych konfliktów zamrożonych linia demarkacyjna odpowiada często geograficznym, administracyjnym lub etnicznym granicom, to w Donbasie linia ta została utworzona w rezultacie działań bojowych, sztucznie. Dlatego zamrożenie tego konfliktu będzie trudne z praktycznego punktu widzenia, ponieważ wiele rodzin ma krewnych, którzy znajdują się po różnych stronach linii rozgraniczenia. Ponadto w Donbasie wciąż istnieje jeden łańcuch produkcyjny, co jest dodatkową trudnością w próbach zamrożenia konfliktu.

Obecnie nie ma skutecznej platformy instytucjonalnej gwarantującej bezpieczeństwo, a wszelkie próby rozwiązania konfliktów w regionie odbywają się na poziomie porozumień między mocarstwami, po nieudanych bezpośrednich negocjacjach ze stronami konfliktu. Niepowodzenia w próbach rozwiązywania konfliktów polegające na zatrzymaniu ostrej

fazy konfrontacji i odroczeniu na czas nieokreślony ostatecznych decyzji wskazują na słabość i nieskuteczność systemu bezpieczeństwa zbiorowego w Europie. Do czasu ustanowienia (aktualizacji lub uzupełnienia) infrastruktury bezpieczeństwa instytucjonalnego liczba konfliktów międzynarodowych będzie się zwiększać.

Olga Wasiuta

T. Akopian, *Political Violence in Armenia (Sources, Public Perception, Ways to Overcome the Problem)*, „Central Asia and the Caucasus" 2002, no. 5; S.J. Byrne, *The Roles of External Ethnoguarantors and Primary Mediators in Cyprus and Northern Ireland*, „Conflict Resolution Quarterly" 2006, vol. 24, no. 2; J.J. Coyle, *Russia's Border Wars and Frozen Conflicts*, Palgrave Macmillan, London 2018; R. Czachor, *Abchazja, Osetia Południowa, Górski Karabach. Geneza i funkcjonowanie systemów politycznych*, Fundacja Instytut Polsko-Rosyjski, Wrocław 2014; K. Fedorowicz, *Konflikty na Kaukazie Południowym jako czynniki destabilizujące rzeczywistość społeczno-polityczną*, „Studia Europejskie" 2015, nr 4; A. Jarosiewicz, K. Strachota, *Górski Karabach – rozmrażanie konfliktu*, „Komentarze OSW" 2011, nr 65; *The International Spread of Ethnic Conflict: Fear, Diffusion and Escalation*, D.A. Lake (ed.), Princeton University Press, Princeton 1998; T. Kuzio, *Special Issue: Ukraine Between a Constrained EU and Assertive Russia*, „Journal of Common Market Studies" 2017, no. 1; R. Orttung, Ch. Walker, *Putin's Frozen Conflicts*, 13.02.2015, ForeignPolicy.com (dostęp 15.01.2020); O. Wasiuta, *Konflikt zamrożony*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; Є.О. Горюнова, *Європейський Союз І «заморожені конфлікти» на Південному Кавказі*, „Панорама політологічних студій" 2012, Випуск 8; О. Задорожній, *Міжнародне право в міждержавних відносинах України і Російської Федерації 1991–2014*, К.І.С., Київ 2014; Г.М. Перепелиця, *Генезис конфліктів на посткомуністичному просторі Європи*, Стилос – ПЦ „Фоліант", Київ 2003; М.Л. Плаксенко, *Роль та інтереси Росії в урегулюванні Придністровського конфлікту*, „Стратегічні пріоритети" 2008, № 3; В.Ф. Пряхин, *Региональные конфликты на постсоветском пространстве: (Абхазия, Южная Осетия, Нагорный Карабах, Приднестровье, Таджикистан)*, Гном и Д, Москва 2002; *Решение „замороженных конфликтов": трудности примирения*, „Per Concordiam" 2010, Т. 1, № 2.

KONTRREWOLUCJA W SPRAWACH WOJSKOWYCH (ang. *counter-revolution in military affairs*, CRMA) – pojęcie będące alternatywą dla

→rewolucji w sprawach wojskowych [t. 3] (RMA). Pojawiło się jako sprzeciw wobec bezrefleksyjnego podejścia niektórych badaczy i wojskowych do wiary w skuteczność nowych technologii militarnych. Pojęcia CRMA użył m.in. John Ferris w artykule *Conventional Power and Contemporary Warfare*, który ukazał się w książce *Strategy in the Contemporary World*. Zdaniem autora po 1989 r. RMA stała się głównym motorem amerykańskiej polityki wojskowej. Jej zwolennicy oczekiwali, że środki w postaci nowych technologii dokonają przełomu w sferze dostępu wojska do →informacji, głęboko przekształcając charakter sił zbrojnych. Konflikty zbrojne, do których dochodziło na przełomie XX i XXI w., wskazywały jednak na coraz większą liczbę mankamentów RMA. W Kosowie, pomimo zastosowania broni precyzyjnej i systemów C2 (Command and control), wojskom →NATO [t. 3] nie udało się zniszczyć zdolności obronnych Socjalistycznej Federacyjnej Republiki Jugosławii. Początkowy sukces w Iraku w 2003 r., jak twierdzi Ferris, nie wynikał natomiast z RMA, lecz z przewagi w powietrzu, niekompetencji dowództwa irackiego oraz efektu psychologicznego.

Pojęcia CRMA użył także G.S. Franch w publikacji *The Coming Counterrevolution in Military Affairs*, która ukazała się w ramach The Command and Control Research Program. Według autora technologie takie jak systemy C2, AWACS, JSTAR czy GPS nie gwarantują osiągnięcia zwycięstwa we współczesnej →wojnie [t. 4]. Przeciwnie – przesycenie technologiczne doprowadza do powstania wrażliwych punktów w infrastrukturze krytycznej państw wysokorozwiniętych. Strona słabsza – państwo rozwijające się, państwo upadłe lub organizacja terrorystyczna, przeprowadzając atak na →infrastrukturę krytyczną zaawansowanego technologicznie przeciwnika, może doprowadzić do czasowej utraty jego zdolności militarnych. W wyniku trudności, jakie napotkała armia amerykańska i jej sojusznicy w Iraku i Afganistanie, liczba krytyków RMA zaczęła rosnąć. W 2011 r. ukazała się książka brytyjskiego historyka J. Blacka *War since 1990*. Autor podał w wątpliwość skuteczność idei rewolucji w sprawach wojskowych. Zdaniem badacza:

- RMA była wojskowym narzędziem realizacji polityki unilateralnej przez administrację G. Busha zdominowaną przez środowisko neokonserwatystów.

- RMA służyła do wygrywania wojen z przeciwnikiem posiadającym konwencjonalne siły zbrojne, lekceważyła jednak przeciwników stosujących metody asymetryczne, czego przykładem były porażki USA w Iraku i Afganistanie oraz trudności Izraela w Libanie w 2006 r.
- Używana technologia wojskowa w praktyce okazała się zawodna. W czasie operacji Pustynna Burza w oddziałach amerykańskich wystąpiły trudności związane z synchronizacją działań lotnictwa i → wojsk lądowych [t. 4] podczas szybko zmieniających się warunków pola bitwy.

W ramach badań poświęconych CRMA oraz zawodności idei RMA wymieniane są następujące metody stosowane przez strony słabsze w konflikcie z zaawansowanym technologicznie przeciwnikiem:

- aktywna obrona;
- taktyka maskowania;
- ataki dywersyjne na wrogie „sanktuaria";
- doktryna wojny partyzanckiej (ang. *guerrilla doctrine*);

Aktywna obrona polega na podziale dostępnych sił lądowych na niewielkie oddziały celem uniknięcia ich zniszczenia przez lotnictwo przeciwnika w pierwszych dniach wojny. Metodę tę zastosowały wojska serbskie (jugosłowiańskie) w 1999 r. Przemieszczały się one w kolumnach składających się z 6 pojazdów oraz 80–150 → żołnierzy [t. 4] po terenie gęsto zalesionym i górzystym, utrudniając tym samym wykrycie z powietrza. Konsekwencje braku stosowania aktywnej obrony widoczne były w czasie operacji Pustynna Burza w Iraku, kiedy wycofujące się z Kuwejtu oddziały irackie przemieszczały się w dużych kolumnach po autostradzie nr 80. W dniach 26–27 lutego 1991 r. lotnictwo amerykańskie i sił sprzymierzonych przeprowadziło naloty na znajdujące się w tym miejscu wojska irackie, niszcząc, wg różnych szacunków, od 1,8 tys. do 2,7 tys. pojazdów.

Taktyka maskowania jest metodą polegającą na wykorzystaniu atrap czołgów, zestawów obrony przeciwlotniczej oraz pojazdów celem skłonienia strony przeciwnej do uznania ich za autentyczne cele, a następnie zniszczenia. Początkowe analizy prowadzone przez dowództwo amerykańskie w czasie operacji Allied Forces w Kosowie wskazywały na zniszczenie 120 serbskich czołgów i 220 bojowych wozów piechoty.

Po uwzględnieniu atrap nazywanych też wabikami (ang. *decoys*) szacunki zmniejszono do 13 czołgów i 100 bojowych wozów piechoty. Doszło w związku z tym do sytuacji, w której koszt pocisku i prowadzonej operacji powietrznej był znacznie wyższy niż koszt zniszczonego celu. Ponadto stosowanie wabików zwiększało ryzyko zestrzelenia samolotów przez zestawy obrony przeciwlotniczej. Aby potwierdzić zniszczenie obiektów naziemnych, piloci często obniżali pułap lotów, narażając się tym samym na wejście w promień rażenia systemów SA-9, SA-13 czy ZSU-23.

Kolejną metodą, jaką może stosować ugrupowanie pozapaństwowe lub strona dysponująca mniejszym potencjałem technologicznym, są ataki dywersyjne na „sanktuaria" przeciwnika. „Sanktuaria" to bazy wojskowe, lotniska oraz centra logistyczne położone daleko od miejsca prowadzonego konfliktu zbrojnego, które przeciwnik uznaje za bezpieczne, znajdujące się poza zasięgiem broni rakietowej i lotnictwa. Atak na nie może być jednak przeprowadzony przez siły specjalne, agenturę znajdującą się na terenie przeciwnika lub lokalne ugrupowania paramilitarne.

Doktryna wojny partyzanckiej polega na przygotowaniu państwa do odparcia ataku poprzez uzbrojenie społeczeństwa i ugrupowań paramilitarnych. Wyposażenie społeczeństwa w lekką broń osobistą, taką jak AK-47 czy ręczne granatniki przeciwpancerne RPG-7, umożliwia zadanie przeciwnikowi dużych strat na zajętych przez niego terytoriach oraz wywołanie sprzeciwu w społeczeństwach, które nie akceptują wysokich strat ponoszonych przez wojsko w czasie operacji militarnych.

Tomasz Wójtowicz

M. Andrew, *Revisiting the Lessons of Operation Allied Force*, 27.01.2014, AusAirPower.net (dostęp 2.01.2020); J. Baylis, J. Wirtz, C.S. Gray, E. Cohen, *Strategia we współczesnym świecie. Wprowadzenie do studiów strategicznych*, tłum. W. Nowicki, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009; J. Black, *Wojna od 1990 roku*, tłum. T. Pichór, Wydawnictwo Rambler, Warszawa 2011; J.T. Correll, *The Counter-Revolution in Military Affairs*, 1.07.2019, AirForceMag.com (31.12.2019); G.S. French, *The Coming Counterrevolution in Military Affairs*, dodccrp.org (dostęp 2.01.2020); J. Holmes, *The Counterrevolution in Naval Affairs*, 7.10.2019, NationalIntrest.org (dostęp 31.12.2019); J. Levich, *A Counter-Revolution in Military Affairs? Notes on US High-Tech Warfare*, 19.01.2007, MROnline.org (dostęp 31.12.2019);

T.R. McCabe, *The Counterrevolution in Military Affairs*, AirUniversity.af.edu (dostęp 30.12.2019); R. Peters, *The Counterrevolution in Military Affairs*, 7.02.2006, GEES.org (dostęp 31.12.2019).

KONTRWYWIAD – w sensie ogólnym może być rozumiany jako zorganizowana działalność wyspecjalizowanych komórek określonych podmiotów, która polega na ochronie ich najważniejszych zasobów informacyjnych oraz przeciwdziałaniu →zagrożeniom [t. 4] dla żywotnych interesów, niezakłóconego funkcjonowania oraz rozwoju tych podmiotów.

Przede wszystkim pojęcie kontrwywiadu dotyczy działalności wyspecjalizowanych służb państwowych, które chronią, pozyskują, gromadzą, opracowują, przetwarzają, analizują, a następnie przekazują najważniejszym organom władzy państwowej →informacje fundamentalne z punktu widzenia →bezpieczeństwa [t. 1] i podstawowych interesów państwa. Są istotnym elementem procesów decyzyjnych na najwyższym poziomie w państwie, którym z jednej strony zapewniają ochronę, a z drugiej je wspierają poprzez dostarczanie podstawowych informacji w celu prowadzenia polityki wewnętrznej i zewnętrznej, w tym m.in. gospodarczej, surowcowej, militarnej, migracyjnej, naukowej itp. Podobnie jak w przypadku służb wywiadowczych, mechanizm wypełniania tej podstawowej, informacyjnej roli w państwie, przedstawia się w ramach tzw. cyklu wywiadowczego. Często kontrwywiad jest też określany mianem →wywiadu [t. 4] wewnętrznego.

Z uwagi na charakter i wagę informacji będących przedmiotem zainteresowania kontrwywiadu (ochrony i pozyskiwania informacji fundamentalnych z punktu widzenia bezpieczeństwa, funkcjonowania państwa, a także zapewnienia bezpieczeństwa i pokoju na świecie), specyficzne miejsce w państwowych procesach decyzyjnych i pełnioną funkcję informacyjną w tym zakresie, a także umiejscowienie w przestrzeni walki informacyjnej między podmiotami państwowymi i niepaństwowymi i związanym z tym przeciwdziałaniem specyficznym kategoriom zagrożeń, wraz ze służbami wywiadu, często określane są w Polsce mianem →służb specjalnych [t. 4]. Poza fundamentalną rolą dla zapewnienia bezpieczeństwa, niezakłóconego funkcjonowania oraz rozwoju państwa oraz jego obronności służby kontrwywiadowcze

spełniają istotne funkcje w wymiarze międzynarodowym w zakresie wymiany informacji sojuszniczych (nadzór nad wymianą →informacji niejawnych międzynarodowych) oraz w zakrojonej na szeroką skalę współpracy międzynarodowej w zakresie przeciwdziałania →zagrożeniom globalnym [t. 4].

Przed służbami kontrwywiadowczymi (cywilnymi i wojskowymi) stawiane są zadania o najważniejszym znaczeniu w przedmiocie przede wszystkim →bezpieczeństwa politycznego [t. 1], →ekonomicznego [t. 1] i →informacyjnego [t. 1] państwa, w szczególności w następujących obszarach:

- przeciwdziałania aktywności obcych służb wywiadowczych (innych państw i podmiotów pozapaństwowych),
- przeciwdziałania →ekstremizmom politycznym i ideologicznym,
- ochrony porządku konstytucyjnego państwa,
- ochrony →bezpieczeństwa wewnętrznego [t. 1], obronności i żywotnych interesów państwa,
- ochrony interesów ekonomicznych państwa,
- ochrony tajemnic państwowych (informacji niejawnych),
- ochrony →infrastruktury krytycznej państwa,
- zwalczania →terroryzmu [t. 4] i →przestępczości zorganizowanej [t. 3],
- przeciwdziałania proliferacji broni masowego rażenia,
- przeciwdziałania nielegalnemu obrotowi bronią i amunicją oraz środkami wybuchowymi,
- przeciwdziałania obrotowi środkami odurzającymi i psychotropowymi.

W literaturze przedmiotu wskazuje się na następujące, podstawowe funkcje, jakie służby kontrwywiadowcze wypełniają w państwie:

- Funkcja informacyjna – dotycząca pozyskiwania, gromadzenia, przetwarzania, analizy i opracowywania podstawowych informacji z punktu widzenia bezpieczeństwa państwa, a następnie przekazywania ich najważniejszym organom władzy państwowej w celu wsparcia w zakresie realizacji polityki państwa. Realizowana jest na poszczególnych etapach tzw. cyklu wywiadowczego na podstawie

→czynności operacyjno-rozpoznawczych [t. 1] oraz analityczno-studyjno-informacyjnych.

- Funkcja ochronna – związana z ochroną najważniejszych zasobów informacyjnych, a także elementów infrastruktury krytycznej państwa. Podstawowe znaczenie mają tutaj czynności ochronno-kontrolne w odniesieniu do systemu ochrony informacji niejawnych (w wymiarze wewnętrznym i zewnętrznym, sojuszniczym), gdzie służby kontrwywiadu odgrywają często rolę tzw. służby ochrony państwa i krajowej władzy bezpieczeństwa. Zapewniają w tym obszarze →bezpieczeństwo informacji niejawnych [t. 1] wewnątrz państwa w odniesieniu do infrastruktury publicznej, jak również do działalności podmiotów prywatnych (w tym także w obszarze bezpieczeństwa systemów i sieci teleinformatycznych), sprawują kontrolę w tym zakresie, a także zapewniają bezpieczeństwo wymiany informacji i komunikacji w relacjach z innymi państwami.
- Funkcja policyjna (procesowa) – czasami stanowi uzupełniającą funkcję służb kontrwywiadowczych i polega na rozpoznawaniu i wykrywaniu określonej kategorii przestępstw oraz ściganiu ich sprawców. Ukierunkowana jest na wynik procesowy, a realizowana głównie za pomocą czynności dochodzeniowo-śledczych.

Nieodłącznym aspektem prowadzenia działalności kontrwywiadowczej jest tajność działania, zarówno w odniesieniu do form, metod i technik pracy, jak również do personaliów osób biorących w niej udział, tak funkcjonariuszy, jak i ich współpracowników (osobowych źródeł informacji, agentury). Co do zasady działalność kontrwywiadowcza prowadzona jest głównie wewnątrz państwa. Istotnym jej elementem jest tzw. ochrona porządku konstytucyjnego państwa, co świadczy o istnieniu ważnych powiązań systemowych w funkcjonowaniu tych służb z ustrojem państwa oraz instytucją władzy państwowej. Stąd też często służby tego typu umieszczane są w obszarze tzw. bezpieczeństwa ustrojowego (politycznego) państwa, a ich działalność nie odnosi się bezpośrednio do ochrony społeczeństwa, lecz raczej do ochrony państwa jako instytucji.

Warto zwrócić uwagę na poszerzenie się zakresu tradycyjnie pojmowanej działalności kontrwywiadowczej (odnoszonej głównie do

zwalczania działalności szpiegowskiej, dywersyjnej, sabotażowej, ekstremizmów politycznych i ideologicznych itp.) w ostatnim czasie, w związku ze zmianą porządku światowego po zakończeniu → z i m n e j w o j n y [t. 4], postępującymi procesami globalizacji i rewolucją technologiczno-informatyczną. Dotyczy to zmian zarówno w sferze podmiotowej – nowe podmioty zagrażające bezpieczeństwu państwa i międzynarodowemu lub zmiana charakteru ich działalności (transnarodowe organizacje przestępcze, międzynarodowe organizacje terrorystyczne, wielkie koncerny i korporacje działające w skali międzynarodowej itp.), jak również przedmiotowej – nowych rodzajów zagrożeń (przede wszystkim w sferze → c y b e r p r z e s t r z e n i [t. 1], jak → c y b e r t e r r o r y z m [t. 1] czy → c y b e r p r z e s t ę p c z o ś ć [t. 1]). Tę zasadniczą zmianę trafnie ujmuje również A. Żebrowski, charakteryzując działalność kontrwywiadowczą we współczesnym świecie w następujący sposób:

> Istotny obszar walki informacyjnej stanowi działalność kontrwywiadowcza ukierunkowana na pozyskiwanie i analizę informacji wykorzystywanych w przedsięwzięciach mających na celu zapewnienie bezpieczeństwa wewnętrznego państwa. Obecnie działania charakteru kontrwywiadowczego zdominowane zostały przez terroryzm międzynarodowy. Nie oznacza to, że pozostałe sfery jego zainteresowania zredukowano do niezbędnego minimum. Nadal kontrwywiad zajmuje się wykrywaniem i neutralizowaniem działalności szpiegowskiej, która obejmuje m.in. ochronę informacji niejawnych i struktur ważnych dla bezpieczeństwa państwa. Ma ona również ścisły związek z przeciwdziałaniem transnarodowym zagrożeniom związanym z nielegalnym wytwarzaniem, posiadaniem i obrotem bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi, proliferacją broni masowego rażenia i innymi formami zorganizowanej przestępczości międzynarodowej. W tym celu kontrwywiad (cywilny i wojskowy) podejmuje czynności operacyjno-rozpoznawcze, analityczne, a niekiedy procesowe (przy wyraźnych wskazaniach w przepisach prawa), co niewątpliwie wpływa na stan bezpieczeństwa wewnętrznego państwa.

W Polsce od przełomu lat 80. i 90. XX w., kiedy rozpoczęte zostały zasadnicze przemiany ustrojowe i systemowe, w obszarze kontrwywiadu najpierw utworzony został w 1990 r. → Urząd Ochrony Państwa (UOP) [t. 4], a w jego strukturach wyodrębniono Zarząd Kontrwywiadu, natomiast w sferze wojskowej powołane zostały w 1991 r. → Wojskowe Służby Informacyjne (WSI) [t. 4], w ramach których najpierw utworzono Zarząd Kontrwywiadu, a następnie – po 2003 r. – zadania kontrwywiadowcze realizowały komórki organizacyjne znajdujące się w stosownych pionach (głównie pion kontrwywiadu wojskowego). Później, w wyniku reformy służb cywilnych z 2002 r., nowo utworzona → Agencja Bezpieczeństwa Wewnętrznego (ABW) [t. 1] przejęła większość zadań oraz zasobów (w tym przede wszystkim dotyczących kontrwywiadu) po UOP, który uległ rozwiązaniu. W wyniku reformy służb w sferze wojskowej z 2006 r. rozwiązane zostały WSI, a zadania kontrwywiadu w tym zakresie przejęła nowo powołana → Służba Kontrwywiadu Wojskowego (SKW) [t. 4].

Do najbardziej znanych służb kontrwywiadowczych na świecie należą m.in.: Federalny Urząd Ochrony Konstytucji (BFV) w Niemczech, Dyrekcja Generalna Bezpieczeństwa Wewnętrznego (DGSI) we Francji, Federalne Biuro Śledcze (FBI) w USA, Federalna Służba Bezpieczeństwa (FSB) w Rosji, Służba Bezpieczeństwa (MI5) w Wielkiej Brytanii, Służba Bezpieczeństwa Ogólnego (Szin Bet) w Izraelu.

Piotr Swoboda

J. Barcz, B. Libera, *Urzędnik i biznesmen w środowisku międzynarodowym*, Wolters Kluwer Polska, Warszawa 2007; R. Faligot, R. Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie*, tłum. M. Stefańska-Matuszyn, K. Skawina, Wydawnictwo Iskry, Warszawa 2006; N. Polmar, T.B. Allen, *Księga szpiegów. Encyklopedia*, tłum. H. Białkowska i in., Wydawnictwo Magnum, Warszawa 2000; *Polskie służby specjalne. Słownik*, K.A. Wojtaszczyk (red.), Wydział Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2011; P. Swoboda, *Kontrwywiad*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *Wywiad i kontrwywiad w Polsce w procesie przemian systemowych (1989–2007)*, Wydawnictwo Avalon, Kraków 2016; R.C.S. Trahair, *Czarna księga szpiegów*, tłum. S. Kędzierski, Wydawnictwo Sensacje XX Wieku, Warszawa 2011;

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j. Dz.U. 2017, poz. 1920 z późn. zm.; Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, t.j. Dz. U. 2017, poz. 1978 z późn. zm.; A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej (Wywiad i kontrwywiad w latach 1989–2003)*, Oficyna Wydawnicza Abrys, Kraków 2005; A. Żebrowski, *Wywiad i kontrwywiad w XXI wieku*, Innovatio Press Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji, Lublin 2010.

KORUPCJA – żądanie lub przyjmowanie korzyści finansowych albo majątkowych przez pracowników instytucji za naruszenie prawa bądź wykonanie określonych czynności urzędowych; funkcjonuje także pod innymi określeniami, np. jako przekupstwo czy łapówkarstwo.

W kodeksie karnym wyróżniono 2 grupy przestępstw o charakterze korupcyjnym. Pierwsza (art. 228 kk) obejmuje przypadki polegające na przyjęciu korzyści majątkowej lub osobistej albo na złożeniu obietnicy przyjęcia takiej korzyści przez osobę pełniącą funkcję publiczną – określane są mianem łapownictwa czynnego. Druga (art. 229 kk) natomiast dotyczy sytuacji polegających na udzieleniu korzyści majątkowej lub osobistej lub też złożeniu obietnicy udzielenia takiej korzyści, a propozycja korupcyjna jest adresowana również do osoby pełniącej funkcję publiczną – nazywane łapownictwem biernym.

Zawarte w znamionach obu →czynów zabronionych [t. 1] sformułowanie „w związku z pełnioną funkcją publiczną" oznacza, że udzielona korzyść lub obietnica jej udzielenia dokonana została ze względu na pełnioną przez adresata funkcję publiczną. Związek ten może zachodzić nie tylko pomiędzy przyjęciem czy wręczeniem korzyści majątkowej (obietnicą) a konkretną czynnością służbową, lecz obejmuje on także faktyczne posiadanie możliwości podjęcia konkretnych czynności służbowych. Jeśli więc burmistrz otrzymał korzyść dlatego, że na podstawie przepisów szczególnych jest uprawniony do wydania decyzji administracyjnej, a jej adresat chce w ten sposób wpłynąć na jej treść lub sam burmistrz zażądał określonej korzyści w zamian za wydanie decyzji zgodnie z oczekiwaniami jej adresata, to niewątpliwie doszło do popełnienia przestępstwa. Odmiennie ocenić należy sytuację, gdy burmistrz otrzymał cenne prezenty w dniu swojego ślubu od osób obcych, które sądziły, że

w ten sposób zyskają jego przychylność na przyszłość. Wręczone korzyści nie pozostawały w związku z pełnioną funkcją publiczną, a fałszywe czy urojone wyobrażenie wręczającego nie stanowi realizacji znamion czynu zabronionego.

Pojęcie osoby pełniącej funkcję publiczną jest szersze niż termin →funkcjonariusz publiczny i zostało ono zdefiniowane w art. 115 § 19 kk. Należy też zwrócić uwagę, że kodeks rozciąga karalność także na czyny dotyczące osób pełniących funkcje publiczne w państwie obcym lub w organizacji międzynarodowej. Przestępstwo łapownictwa biernego ma zatem charakter indywidualny, podczas gdy przestępstwo łapownictwa czynnego ma charakter powszechny.

Korzyść majątkowa ma mieć wartość ekonomiczną, wyrażoną w pieniądzu, choć nie musi mieć postaci pieniędzy (np. wycieczka, telewizor, usługa gastronomiczna). Korzyścią osobistą będzie korzyść niewymierna w pieniądzu (np. awans, stosunek seksualny, powołanie do prestiżowego gremium). Obietnica korzyści może być wyrażona w każdy sposób mogący wywołać u adresata wrażenie, że zostanie ona spełniona i jest możliwa do spełnienia.

Rozwiązania przyjęte w kodeksie karnym w stosunku do obu grup przestępstw korupcyjnych są w większości analogiczne. Taka sama kara, od 6 miesięcy do 8 lat pozbawiania wolności, grozi za popełnienie obu czynów w typie podstawowym. Typ uprzywilejowany dotyczy przypadków tzw. mniejszej wagi, czyli sytuacji, gdy szkodliwość społeczna czynu jest niska i przewidziano za niego łagodniejszą karę. Typ kwalifikowany dotyczy sytuacji, gdy zachowanie osoby pełniącej funkcję publiczną będące lub mające być skutkiem korupcji stanowi naruszenie przepisów prawa. Drugi typ kwalifikowany odnosi się do przypadku, gdy korzyść majątkowa albo osobista była znacznej wartości.

W odniesieniu do łapownictwa biernego wprowadzono także dodatkowy typ kwalifikowany, odnoszący się do sytuacji uzależnienia przez osobę pełniącą funkcję publiczną wykonania czynności służbowej od otrzymania korzyści majątkowej lub osobistej albo jej obietnicy lub żądania takiej korzyści. Uzależnianiem jest danie do zrozumienia innej osobie, że sprawca czynności nie wykona jej wcale lub że wykona ją w sytuacji, gdy innej osobie zależy na niedokonywaniu czynności.

Szczególna regulacja – tzw. klauzula niekaralności sprawcy czynnej korupcji – dotyczy przypadków zawiadomienia przez sprawcę organu ścigania, zanim organ ten dowiedział się o fakcie przestępstwa z innego źródła, i ujawnienie wszystkich istotnych okoliczności przestępstwa. Jak wskazuje się w literaturze, ideą tego przepisu jest rozbicie solidarności przestępczej między udzielającym korzyści lub obietnicy a przyjmującym ją. Rozwiązanie to jest jednak krytykowane jako tworzące pole do nadużyć ze strony sprawców prawdziwych lub rzekomych czynnej korupcji.

Oba omawiane warianty przestępstw korupcyjnych mają charakter formalny, co oznacza, że do jego zaistnienia nie jest konieczne podjęcie lub zaniechanie czynności służbowej przez funkcjonariusza czy też jej przeprowadzenie w określony sposób.

Do grupy przestępstw korupcyjnych zaliczyć należy także płatną protekcję, która podobnie jak łapownictwo spenalizowana została w 2 wariantach (biernej – art. 230 kk) oraz czynnej (art. 230a kk). Pierwsze z wymienionych popełnia ten, kto powołując się na wpływy w instytucji państwowej, samorządowej, organizacji międzynarodowej albo krajowej lub w zagranicznej jednostce organizacyjnej dysponującej środkami publicznymi albo wywołując przekonanie innej osoby lub utwierdzając ją w przekonaniu o istnieniu takich wpływów, podejmuje się pośrednictwa w załatwieniu sprawy w zamian za korzyść majątkową lub osobistą albo jej obietnicę. Natomiast drugie dotyczy osoby, która udziela albo obiecuje udzielić korzyści majątkowej lub osobistej w zamian za pośrednictwo w załatwieniu sprawy w instytucji państwowej, samorządowej, organizacji międzynarodowej albo krajowej lub w zagranicznej jednostce organizacyjnej dysponującej środkami publicznymi, polegające na bezprawnym wywarciu wpływu na decyzję, działanie lub zaniechanie osoby pełniącej funkcję publiczną, w związku z pełnieniem tej funkcji.

Nadużycie uprawnień przez funkcjonariusza publicznego, który przekraczając swoje uprawnienia albo nie dopełniając obowiązków, działa na szkodę interesu publicznego lub prywatnego, działa w celu uzyskania korzyści majątkowej bądź osobistej, stanowi osobny czyn, ujęty w art. 231 § 2 kk.

Problematyce korupcji i jej zwalczaniu został poświęcony szereg aktów prawa międzynarodowego, tytułem egzemplifikacji należy wymienić:

2 konwencje międzynarodowe dotyczące korupcji z perspektywy prawa karnego i cywilnego, przyjęte w Strasburgu w 1999 r.; konwencję ONZ z 2007 r. Problematyki tej dotyczy także rządowy program zwalczania korupcji, realizowany przez zespół powołany przez premiera z szefem →Centralnego Biura Antykorupcyjnego [t. 1] na czele.

Jak wynika ze statystyk publikowanych przez Centralne Biuro Antykorupcyjne, najczęściej popełnianym przestępstwem o charakterze korupcyjnym jest poświadczenie nieprawdy w celu osiągnięcia korzyści majątkowej (art. 271 § 3 kk), a w dalszej kolejności: sprzedajność urzędnicza (art. 228 kk) oraz przekroczenie uprawnień lub niedopełnienie obowiązków w celu osiągnięcia korzyści majątkowej lub osobistej (art. 231 § 2 kk) i przekupstwo (art. 229 kk), liczba ujawnianych przestępstw korupcyjnych nadal wzrasta.

Indeks Percepcji Korupcji (Corruption Perceptions Index, CPI) to badanie prowadzone przez Transparency International, organizację międzynarodową działającą na rzecz przejrzystości i uczciwości w życiu publicznym i gospodarczym. W zestawieniu za 2019 r. Polska zajęła 41. miejsce, otrzymując 58 punktów. Średni wynik dla grupy Europa Zachodnia i Unia Europejska, do której należy Polska, wynosi 66 punktów. Spośród państw UE we wspomnianym rankingu Polska wyprzedziła Włochy (51. miejsce), Litwę (44. miejsce), Czechy (44. miejsce), Słowację (59. miejsce), Rumunię (70. miejsce) i Bułgarię (74. miejsce).

Anna Pacholska

Cywilnoprawna konwencja o korupcji, sporządzona w Strasburgu dnia 4 listopada 1999 r., Dz. U. 2004, nr 244, poz. 2443; C. Nowak, *Korupcja w polskim prawie karnym na tle uregulowań międzynarodowych*, C.H.Beck, Warszawa 2008; J. Lachowski, *Sprzedajność*, [w:] *Kodeks karny. Część szczególna*, t. 2: *Komentarz. Art. 222–316*, M. Królikowski, R. Zawłocki (red.), C.H.Beck, Warszawa 2017; Konwencja Narodów Zjednoczonych Przeciwko Korupcji, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych z dnia 31 października 2003 r., Dz. U. 2007, nr 84, poz. 563; A. Melezini, *Prawne instrumenty zapobiegania i zwalczania korupcji przez kontrolę skarbową*, Wolters Kluwer Polska, Warszawa 2012; A. Pacholska, *Korupcja*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; Prawnokarna Konwencja o korupcji sporządzona w Strasburgu dnia 27 stycznia 1999 r., Dz. U. 2005, nr 29, poz. 249;

Rządowy Program Przeciwdziałania Korupcji na lata 2018–2020, M.P. z 2018 r., poz. 12; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 2017, poz. 2204.

KRADZIEŻ TOŻSAMOŚCI – pojęcie potoczne, kojarzone ze wszystkimi przypadkami posłużenia się cudzymi danymi osobowymi przez osobę nieuprawnioną, przybraniem cudzej tożsamości, podszyciem się pod kogoś. Ochrona danych osobowych i wizerunku została uregulowana zarówno w prawie cywilnym, administracyjnym, jak i w prawie karnym, w którym czyn ten określony został mianem przestępstwa podszywania się.

Przestępstwo to (art. 190a § 2 kk) jest swoistym oszustwem, polegającym na podszywaniu się pod inną osobę poprzez wykorzystanie jej danych osobowych lub wizerunku w celu wyrządzenia jej szkody osobistej albo majątkowej.

Określenie podszywanie się, stanowiące jedno ze znamion przestępstwa, należy rozumieć jako fałszywe podawanie się za kogoś innego, bez wiedzy i zgody osoby, za którą sprawca się podaje, w taki sposób, aby osoby trzecie zostały wprowadzone w błąd co do jego tożsamości. Termin wizerunek należy natomiast ujmować szeroko jako każdy obraz czy efekt jego przetworzenia, który umożliwia identyfikację osoby na nim uwidocznionej. Zauważyć trzeba, że wizerunek podlega osobnej ochronie na podstawie ustawy o prawie autorskim i prawach pokrewnych oraz na podstawie kodeksu cywilnego. Pojęcie danych osobowych należy rozumieć w sposób zbieżny z definicją zawartą w ustawie o ochronie danych osobowych jako wszelkie → i n f o r m a c j e dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, czyli takiej, której tożsamość można określić bezpośrednio albo pośrednio, w szczególności za pomocą numeru PESEL, specyficznych czynników określających jej cechy fizyczne, umysłowe, kulturowe, społeczne. Wątpliwości budzi zaliczanie w poczet danych osobowych loginów, haseł, adresów e-mail itp. Wskazuje się na możliwość traktowania ich jako danych osobowych, których naruszenie mogłoby być uznane za popełnienie przestępstwa podszywania się tylko wówczas, gdy samodzielnie albo w powiązaniu z innymi danymi pozwalały one na jednoznaczną identyfikację osoby.

Szkodę majątkową, o której mowa w przepisie, ujmować należy, zgodnie z doktryną prawa cywilnego, jako uszczerbek w majątku pokrzywdzonego

(dobra, których nie uzyskał lub które utracił w związku z przestępstwem) albo jako utracone korzyści (które pokrzywdzony nabyłby, gdyby nie popełnienie przestępstwa). Wątpliwości interpretacyjne budzi natomiast termin szkody osobistej, który można interpretować jako synonim krzywdy (uszczerbek niemajątkowy, np. w dobrach osobistych) albo jako pojęcie szersze obejmujące zarówno krzywdę, jak i majątkową szkodę na osobie (np. rozstrój zdrowia generujący koszty leczenia).

Przestępstwo, o którym mowa, ma charakter powszechny, co oznacza, że może je popełnić każda osoba podlegająca odpowiedzialności karnej zgodnie z ustawą. Występek ten może zostać popełniony tylko przez działanie, nie zaś przez zaniechanie.

Przestępstwo podszywania może zostać popełnione wyłączenie umyślnie w zamiarze bezpośrednim kierunkowym. Oznacza to, że popełnienie przestępstwa można przypisać tylko osobie, która używając cudzych danych albo wizerunku, podszyła się pod pokrzywdzonego, obejmując swoją wolą (zamiarem) także wyrządzenie szkody. Odwrotnie, działanie polegające na podszywaniu się nieukierunkowanym na wyrządzenie szkody nie wyczerpuje znamion omawianego przestępstwa. Zaznaczyć trzeba, że zamiar sprawcy dotyczący wyrządzenia szkody musi być ukierunkowany na wyrządzenie jej tej samej osobie, pod którą sprawca się podszywa, nie zaś innej.

Konstrukcja strony podmiotowej przestępstwa oparta na zamiarze bezpośrednim kierunkowym krytykowana była już na etapie prac legislacyjnych nad przepisem i do chwili obecnej budzi wątpliwości ze strony przedstawicieli doktryny. Argumentowano, że ma miejsce niezasadne zawężenie kryminalizacji i udzielenie ochrony prawnej tylko tym pokrzywdzonym, których dobra zostały naruszone celowo. Skoro każdy człowiek ma prawo do tożsamości, a ustawodawca chce to prawo chronić, to niezasadne jest wprowadzanie dodatkowych warunków. Stąd też stale podnoszone są propozycje przeredagowania przepisu, przynajmniej poprzez zmianę zamiaru bezpośredniego na ewentualny. Wówczas odpowiedzialność karną ponosiłby każdy, kto posłużył się cudzymi danymi albo wizerunkiem, a liczył się przy tym lub powinien liczyć się z możliwością wyrządzenia w ten sposób szkody osobistej albo majątkowej.

Występek ten określany jest w literaturze przedmiotu jako formalny, czyli bezskutkowy. Oznacza to, że dla bytu przestępstwa nie jest istotne, czy

na skutek podszywania się sprawca rzeczywiście szkodę wyrządził, wystarczające jest, że działał w tym celu. Przyjęta konstrukcja budzi wątpliwości w doktrynie prawa jako prowadząca do nadmiernego ograniczenia kryminalizacji. W efekcie bowiem nie poniesie odpowiedzialności osoba, która wykorzystała wizerunek innej osoby albo jej dane, godząc się jedynie na to, że przy okazji może zostać wyrządzona szkoda.

Przykładem popełnienia przestępstwa podszywania się skutkującego wyrządzeniem szkody osobistej jest założenie konta na portalu społecznościowym z wykorzystaniem danych osoby pokrzywdzonej i jej zdjęć, a następnie rozpowszechnianie obraźliwych, poniżających lub ośmieszających informacji o pokrzywdzonej poprzez zamieszczanie wpisów czy wysyłanie wiadomości do innych użytkowników portalu. Natomiast popełnieniem tego przestępstwa w celu wyrządzenia szkody majątkowej jest zaciągnięcie kredytu przy wykorzystaniu cudzych danych osobowych w celu obciążenia koniecznością spłaty zobowiązania osoby, z którą sprawca był już uprzednio skonfliktowany.

Kodeks karny przewiduje także typ kwalifikowany przestępstwa, czyli wiążący się z surowszą odpowiedzialnością dla jego sprawcy. Charakteryzuje się on wystąpieniem następstwa w postaci targnięcia się przez pokrzywdzonego na własne życie – może być to dokonany albo usiłowany zamach samobójczy. Warunkiem przyjęcia odpowiedzialności za typ kwalifikowany jest ustalenie związku przyczynowego pomiędzy podszywaniem się a zamachem samobójczym ofiary. Należy zauważyć, że o ile przestępstwo podszywania się może zostać popełnione wyłącznie w zamiarze bezpośrednim, to za następstwo w postaci targnięcia się na życie odpowiada zarówno osoba działająca w zamiarze bezpośrednim, jak i ewentualnym. Sprawca, który podszywa się pod ofiarę, aby w ten sposób doprowadzić ją do śmierci, będzie odpowiadał także za przestępstwo zabójstwa w typie podstawowym albo w typie kwalifikowanym, jeżeli można uznać, że działał on z pobudek zasługujących na szczególne potępienie.

W literaturze wskazuje się, że przestępstwo podszywania się może być wymierzone jedynie przeciwko osobom fizycznym, aktualnie żyjącym i rzeczywiście istniejącym. Przemawia za tym m.in. umieszczenie omawianego przestępstwa w części kodeksu karnego dotyczącej przestępstw przeciwko wolności, które dotyczą naruszeń chronionych przez

prawo dóbr osób fizycznych. Wskakuje się także, że pojęcie wizerunku jest immanentnie związane z osobami fizycznymi, a nie odnosi się do osób prawnych. Tym samym z ochrony nie korzystają osoby prawne ani jednostki organizacyjne nieposiadające osobowości prawnej, mimo że zgodnie z art. 43 kc można odnosić względem nich pojęcie dóbr osobistych, a firma przedsiębiorcy podlega ochronie prawnej (art. 4310 kc).

Przestępstwa podszywania się nie można popełnić także, posługując się pseudonimem artystycznym, wizerunkiem scenicznym, danymi osoby już nieżyjącej czy osoby fikcyjnej (postaci literackiej). Wątpliwości budzić może także każdy przypadek stworzenia tożsamości fikcyjnej poprzez połączenie danych kilku osób albo połączenie danych pokrzywdzonego z danymi stworzonymi na potrzeby popełnienia → c z y n u z a b r o n i o n e g o [t. 1]. Tytułem przykładu można wskazać sytuację, gdy sprawca posługuje się danymi ofiary dla zawarcia umowy sprzedaży w sklepie internetowym, ale podaje swój adres jako miejsce odebrania zamówionego towaru. Jako miernik pozwalający na ustalenie, czy doszło do popełnienia przestępstwa podszywania się, przyjąć można odpowiedź na pytanie, czy obiektywnie oceniając, przeciętnie doświadczony człowiek, działając w normalnych okolicznościach, brał działającego sprawcę za osobę pokrzywdzoną.

Przestępstwo podszywania się w typie podstawowym ścigane jest na wniosek osoby pokrzywdzonej, natomiast w typie kwalifikowanym ściganie następuje z urzędu.

Przestępstwo podszywania się zostało ujęte w tym samym artykule, który dotyczy także przestępstwa nękania, określanego też mianem stalkingu i wprowadzonego razem z nim do kodeksu karnego w 2011 r. W literaturze wskazuje się, że kodeksowa regulacja podszywania się stanowić ma uzupełnienie kryminalizacji zjawiska stalkingu, w ramach którego dochodzić może do rozpowszechniania przez sprawcę wiadomości upozorowanych na pochodzące od ofiary, mających wyrządzić jej dodatkową przykrość czy szkodę, być dla niej uciążliwymi, np. poprzez rozpowszechnianie ofert matrymonialnych, anonsów erotycznych, nabywanie pod jej imieniem towarów czy usług. Zachowania takie nazywane są też cyberstalkingiem.

Dla zrealizowania znamion omawianego przestępstwa wystarczy jednokrotne wykorzystanie danych lub wizerunku ofiary w celu podszycia

się pod nią, nie jest konieczne, aby zachowania takie były podejmowane w sposób uporczywy, co odróżnia podszywanie się od stalkingu.

W praktyce często zdarza się, że sprawcy popełniający przestępstwo podszywania się swoim działaniem naruszają też przepisy kodeksu karnego inne niż tylko ten dotyczący nękania. Przestępstwo podszywania się może występować w zbiegu z przestępstwami przeciwko ochronie informacji (np.: zakładanie → p o d s ł u c h ó w [t. 3], uzyskiwanie dostępu do informacji, niszczenie, usuwanie, zmienienie danych informatycznych) oraz przeciwko wiarygodności dokumentów (np.: fałszerstwo, wyłudzenie poświadczenia nieprawdy, posługiwanie się dokumentem poświadczającym nieprawdę, posługiwanie się cudzym dokumentem).

Przepisy karne mające służyć zwalczaniu przestępstwa podszywania się ulokowane zostały także poza kodeksem karnym. Ustawa o dokumentach publicznych stanowi, że „Kto wytwarza, oferuje, zbywa lub przechowuje w celu zbycia replikę dokumentu publicznego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Ustawa o ochronie danych osobowych przewiduje system kar administracyjnych, nakładanych przez prezesa Urzędu Ochrony Danych Osobowych na podmioty nieprzestrzegające Rozporządzenia Parlamentu Europejskiego i Rady (UE) z 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Ustawa przewiduje także odpowiedzialność karną za nielegalne przetwarzanie danych osobowych lub udaremnienie przeprowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych.

Anna Pacholska

M. Królikowski, A. Sakowicz, *Art. 190a, uporczywe nękanie*, [w:] *Kodeks karny. Część szczególna*, t. 1: *Komentarz. Art. 117–221*, M. Królikowski, R. Zawłocki (red.), C.H.Beck, Warszawa 2017; A. Lach, *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Wolters Kluwer Polska, Warszawa 2015; A. Mozgawa, *Przestępstwa stalkingu (nękania) i podszywania się (art. 190a KK)*, [w:] *Przestępstwa przeciwko dobrom indywidualnym*, J. Warylewski (red.), C.H.Beck, Instytut Nauk Prawnych PAN, Warszawa 2016; A. Pacholska, *Kradzież tożsamości*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; K. Sowirka, *Przestępstwo kradzieży tożsamości w polskim prawie karnym*, „Ius

Novum" 2013, nr 1; Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz. U. 2017, poz. 459; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 2017, poz. 2204; A. Zoll, *Art. 190a*, [w:] *Kodeks karny. Część szczególna*, t. 2: *Komentarz do art. 117–211a*, W. Wróbel, A. Zoll (red.), Wolters Kluwer, Warszawa 2017.

KRAJOWA MAPA ZAGROŻEŃ BEZPIECZEŃSTWA (KMZB) – interaktywna mapa, która została wdrożona w październiku 2016 r. jako element procesu zarządzania →bezpieczeństwem publicznym [t. 1]. Mapa dostępna jest na pod adresem https://mapy.geoportal.gov.pl/iMapLite/KMZBPublic.html, w serwisie Policja.pl oraz w aplikacji mobilnej GeoportalMobile. Decyzja o utworzeniu tego narzędzia została podjęta w styczniu 2016 r. przez Ministerstwo Spraw Wewnętrznych i Administracji przy współpracy z Komendą Główną Policji (Biurem Prewencji KGP).

KMZB pozwala na identyfikację i czytelną wizualizację wybranych, określonych przez →Policję [t. 3] po konsultacjach społecznych, typów wykroczeń i →zagrożeń [t. 4] porządku publicznego, które w subiektywnym odczuciu mieszkańców negatywnie wpływają na ich poczucie →bezpieczeństwa [t. 1]. Autorzy projektu podkreślają, iż KMZB powstała w celu umożliwienia mieszkańcom przekazywania Policji →informacji o zagrożeniach, a tym samym przyczyniania się do podnoszenia ich poczucia bezpieczeństwa w zgłaszanych miejscach. Jej zadaniem jest również zaproszenie społeczeństwa do współpracy z Policją na rzecz ogólnej poprawy bezpieczeństwa oraz wytworzenie mechanizmu współpracy na linii mieszkańcy – Policja.

KMZB to jeden z instrumentów komunikacji społeczeństwa z Policją w dobie rozwoju technicznego i postępującej cyfryzacji. Celem projektu było stworzenie narzędzi, które pozwalają na prawidłowe, rzetelne i klarowne przedstawienie społecznościom lokalnym skali i rodzaju zidentyfikowanych zagrożeń przez instytucje współodpowiedzialne za bezpieczeństwo i porządek publiczny w formie wizualizacji stanu bezpieczeństwa. Jest to swoisty wykaz zagrożeń dla życia i zdrowia ludzkiego oraz mienia, sporządzony z uwzględnieniem ich lokalizacji czasoprzestrzennej. Takim narzędziem jest wizualizacja stanu bezpieczeństwa w formie tzw. map zagrożeń, tj. wykazów zagrożeń dla życia i zdrowia ludzkiego oraz mienia, sporządzonych przy uwzględnieniu ich rozkładu w przestrzeni i czasie.

Należy podkreślić, że proces wdrażania KMZB był wieloetapowy. Przed wprowadzeniem w życie projektu, w okresie od lutego do kwietnia 2016 r., zostały przeprowadzone ogólnopolskie konsultacje społeczne. Miały one bardzo szeroki zasięg. Ogółem na terenie całego kraju przeprowadzono 11,9 tys. konsultacji społecznych na poziomie wojewódzkim, powiatowym i gminnym. Uczestniczyło w nich w sumie 217,775 tys. obywateli. W trakcie tych spotkań wskazywano na nurtujące ich problemy, które w znacznym stopniu przyczyniły się do zdefiniowania sposobu określenia i prezentowania zagrożeń oraz sposobu jej funkcjonowania. Efekty pilotażowej realizacji KMZB były pozytywne. Pokazały pozytywny odbiór społeczny (społeczeństwo realnie uczestniczy w zapewnieniu bezpieczeństwa) i wymierny wpływ na poprawę poczucia bezpieczeństwa ludzi poprzez wnikliwą weryfikację każdego naniesionego zagrożenia. Pozytywnie to narzędzie pozyskiwania i wymiany informacji ocenili również policjanci odpowiedzialni za obsługę zgłoszeń, jak również korzystający z informacji przekazanych przez mieszkańców za pośrednictwem KMZB. Niewątpliwie ważnym aspektem była też integracja działań instytucji na rzecz bezpieczeństwa – eliminacja określonych zagrożeń realizowana jest przez podmioty pozapolicyjne. KMZB została wdrożona na terenie całego kraju po przeprowadzonych konsultacjach społecznych i pilotażu na terenie garnizonu podlaskiego, pomorskiego i stołecznego.

W wyniku przeprowadzonych konsultacji i późniejszych modyfikacji (na dzień 1 stycznia 2020 r.) funkcjonują 24 grupy zagrożeń, które są wskazywane na mapie przez społeczeństwo. Zagrożenia te zostały określone i pogrupowane jako: akty wandalizmu, osoba bezdomna wymagająca pomocy, dzikie wysypiska śmieci, grupowanie się małoletnich zagrożonych demoralizacją, kłusownictwo, nielegalna wycinka drzew, nielegalne rajdy samochodowe, nieprawidłowe parkowanie, niestrzeżone przejście przez tory, niewłaściwa infrastruktura drogowa, niszczenie zieleni, poruszanie się po terenach leśnych quadami, przekraczanie dozwolonej prędkości, spożywanie alkoholu w miejscach niedozwolonych, używanie środków odurzających, wałęsające się bezpańskie psy, wypalanie traw, zła organizacja ruchu drogowego, znęcanie się nad zwierzętami, żebractwo, niestrzeżony przejazd kolejowy, zdarzenia drogowe z udziałem zwierząt

leśnych, miejsca niebezpieczne na wodach, miejsce niebezpiecznej działalności rozrywkowej.

Za pomocą KMZB internauta może anonimowo, nie częściej niż raz na dobę, dokonać zgłoszenia, wskazując wybrany typ wykroczenia lub zagrożenia oraz określając jego dokładną lokalizację na mapie w dowolnym miejscu na terenie całej Polski. Informacje można nanosić na mapę za pomocą dowolnego urządzenia z dostępem do sieci – komputera, tabletu czy telefonu komórkowego. W celu dodania zgłoszenia należy wybrać ikonę „+" znajdującą się w lewym dolnym rogu serwisu. Następnie pojawią się ikony 24 uporządkowanych alfabetycznie kategorii zgłoszeń, spośród których należy wybrać jedną. Kolejną czynnością jest dodanie szczegółów zgłoszenia, tj. wskazanie miejsca na mapie, daty i godziny zaistniałego zdarzenia, dnia tygodnia i pory dnia oraz krótkiego opisu zagrożenia. Ponadto istnieje możliwość załączenia plików (w formatach .jpg, .pdf, .3gp, .mov, .doc, .txt) potwierdzających zdarzenie. Po zatwierdzeniu pojawia się informacja o przyjęciu zgłoszenia.

Każde zgłoszenie wywołuje reakcję Policji, która po interwencji nadaje mu odpowiedni status (zgłoszenie nowe, w trakcie weryfikacji, potwierdzone, potwierdzone – wyeliminowane, potwierdzone – przekazane poza Policję oraz niepotwierdzone).

Katalog wykroczeń oraz zagrożeń porządku publicznego ulegał zmianom w trakcie całego okresu funkcjonowania KMZB. Obecnie obejmuje on następujące obszary i kategorie:

- Bezpieczeństwo w ruchu drogowym:
  - nielegalne rajdy samochodowe,
  - nieprawidłowe parkowanie,
  - niestrzeżone przejście przez tory,
  - niestrzeżony przejazd kolejowy,
  - niewłaściwa infrastruktura drogowa,
  - przekraczanie dozwolonej prędkości,
  - zdarzenia drogowe z udziałem zwierząt leśnych,
  - zła organizacja ruchu drogowego.
- Wykroczenia oraz zagrożenia porządku publicznego:
  - akty wandalizmu,
  - spożywanie alkoholu w miejscach niedozwolonych.

- Bezdomność, →patologie społeczne [t. 3]:
  - grupowanie się małoletnich zagrożonych demoralizacją,
  - osoba bezdomna wymagająca pomocy,
  - używanie środków odurzających,
  - żebractwo.
- Bezpieczeństwo na terenach wodnych:
  - miejsca niebezpieczne na wodach.
- Ochrona środowiska:
  - dzikie wysypiska śmieci,
  - kłusownictwo,
  - nielegalna wycinka drzew,
  - poruszanie się po terenach leśnych quadami,
  - wałęsające się bezpańskie psy,
  - wypalanie traw,
  - znęcanie się nad zwierzętami.
- Inne:
  - miejsce niebezpiecznej działalności rozrywkowej.

Najważniejsze akty prawne regulujące funkcjonowanie KMZB to:

- Zarządzenie nr 768 Komendanta Głównego Policji z dnia 14 sierpnia 2007 r. w sprawie form i metod wykonywania zadań przez policjantów pełniących służbę patrolową oraz koordynacji działań o charakterze prewencyjnym – określa, „iż tworzy się mapy zagrożeń w oparciu o analizy stanu bezpieczeństwa i porządku, sporządzane na potrzeby dyslokacji służb wszystkich podmiotów działających na rzecz zapobiegania popełnianiu przestępstw, wykroczeń oraz zapobiegania zachowaniom aspołecznym". W § 15 zarządzenia wskazano, że „analiza stanu bezpieczeństwa i porządku na potrzeby dyslokacji służby patrolowej […] powinna opierać się na ocenie i monitorowaniu poszczególnych czynników mających wpływ na ten stan, w tym m.in. na bieżących i okresowych informacjach na temat poziomu poczucia bezpieczeństwa, opartych na opiniach społeczności lokalnej". W uzasadnieniu komendanta głównego Policji insp. T. Budzika nadmieniono ponadto, iż „zarządzenie w większym niż dotychczas stopniu kładzie nacisk na szeroko pojętą współpracę z podmiotami działającymi na rzecz

zapobiegania popełnianiu przestępstw i wykroczeń oraz zapobieganiu innym zjawiskom patologii społecznej".

- Wytyczne nr 3 Komendanta Głównego Policji z dnia 14 września 2016 r. w sprawie sposobu postępowania policjantów podczas realizacji zadań związanych z funkcjonowaniem Krajowej Mapy Zagrożeń Bezpieczeństwa oraz Wytyczne nr 1 z dnia 31 lipca 2017 r. zmieniające wcześniejszy dokument – określono w nich „zasady wyznaczania koordynatorów na poszczególnych szczeblach jednostek organizacyjnych Policji i ich zadania, tryb zapoznawania się z zagrożeniami naniesionymi na Krajową Mapę Zagrożeń Bezpieczeństwa oraz ich weryfikację, sposób zmiany statusów zagrożeń naniesionych na Krajową Mapę Zagrożeń Bezpieczeństwa, jak również sprawowanie nadzoru nad sposobem realizacji zadań związanych z funkcjonowaniem Krajowej Mapy Zagrożeń Bezpieczeństwa".

Zgodnie z danymi statystycznymi KMZB odwiedziło w 2016 r. 505 701 użytkowników, w 2017 r. 592 636 użytkowników, w 2018 r. 477 541 użytkowników, natomiast w 2019 r. 466 316 użytkowników. Najwięcej zgłoszeń było dokonywanych przez internautów w przedziale wiekowym 25–34 lat, natomiast najmniej w wieku 65+. Wyniki sondażu przeprowadzonego w 2017 r. przez Zespół ds. Analiz i Kontroli Zarządczej Gabinetu KGP pokazują, iż narzędzie to pozytywnie ocenia większość ankietowanych (57%). Do najczęściej zgłaszanych zagrożeń należą nieprawidłowe parkowanie, przekraczanie dozwolonej prędkości oraz spożywanie alkoholu w miejscach niedozwolonych. Najczęściej deklarowanym powodem wejścia na stronę mapy jest zamiar zgłoszenia zagrożenia (41,4% wskazań). Około 2-krotnie mniejszy odsetek badanych twierdzi, że głównym powodem wejścia na stronę jest chęć sprawdzenia, jakie zagrożenia zaznaczyli na mapie inni użytkownicy (23,6%). Ponad połowa ankietowanych uważa ponadto, że mapa → zagrożeń bezpieczeństwa [t. 4] poprawi skuteczność działań Policji, przyczyni się do spadku liczby przestępstw i wykroczeń szczególnie uciążliwych społecznie oraz podniesie poczucie bezpieczeństwa obywateli (odpowiednio 59,4%, 55,0% i 54,2% wskazań).

Korzyści z KMZB dostrzega również Biuro Prewencji KGP – wskazuje ono, iż zgłoszenia przekazywane przez społeczeństwo za pośrednictwem

mapy stały się istotnym źródłem informacji wykorzystywanym na potrzeby dyslokacji służb, zarówno kryminalnej, jak i prewencyjnej.

KMZB opiera się na informacjach pochodzących z 3 zbiorów: informacje gromadzone w policyjnych systemach informatycznych, informacje pozyskiwane od społeczeństwa (w trakcie bezpośrednich kontaktów z obywatelami, z przedstawicielami samorządu terytorialnego, organizacji pozarządowych i w trakcie realizowanych debat społecznych poświęconych bezpieczeństwu publicznemu) oraz informacje pozyskiwane od obywateli (internautów) z wykorzystaniem platformy wymiany informacji.

Pozytywne efekty konsultacji społecznych i pozytywne doświadczenia funkcjonowania KMZB w trakcie jej pilotażowego funkcjonowania spowodowały, że we wrześniu 2016 r. komendant główny Policji podjął decyzję o wdrożeniu KMZB do funkcjonowania na terenie całego kraju jako nowoczesnej platformy pozyskiwania informacji o lokalnie uciążliwych zagrożeniach bezpieczeństwa. Należy podkreślić, że KMZB nie służy do zgłaszania potrzeby pilnej interwencji Policji. Do tego służy numer alarmowy 112.

KMZB jest narzędziem informatycznym, które prezentuje społeczeństwu skalę i rodzaj zidentyfikowanych zagrożeń (mapa statystyczna), a także umożliwia mieszkańcom sygnalizowanie miejsc zagrożonych (mapa interaktywna) podlegających sprawdzeniu przez Policję. Aplikacja wykorzystuje Geoportal.gov.pl.

Moduł statystyczny pozwala każdemu obywatelowi zapoznać się ze skalą zagrożenia i poszczególnymi przestępstwami w pobliżu miejsca zamieszkania, w porównaniu z innymi regionami kraju (powiatami lub województwami). Stopień zagrożenia na mapie wyrażany jest w formie graficznej – odpowiednią kolorystyką. Jednocześnie w opisie określonego zagrożenia znajduje się opis kwalifikacji prawnej danego czynu. Obecnie (na dzień 1 stycznia 2020 r.) w panelu statystycznym można zapoznać się ze skalą występowania 25 zagrożeń i interwencji, są to: liczba wypadków drogowych; liczba ofiar śmiertelnych wypadków drogowych; liczba wypadków drogowych w przeliczeniu na 100 tys. mieszkańców; liczba ofiar śmiertelnych wypadków drogowych w przeliczeniu na 100 tys. mieszkańców; liczba ofiar śmiertelnych wypadków drogowych w przeliczeniu na 100 wypadków; liczba wypadków drogowych w przeliczeniu na 100 km

dróg publicznych; miejsca i odcinki dróg szczególnie niebezpieczne dla pieszych; kradzież z włamaniem (art. 279 kk); kradzież (art. 278 kk); rozbój (art. 280 kk); kradzież rozbójnicza (art. 281 kk); wymuszenie rozbójnicze (art. 282 kk); uszkodzenie rzeczy; bójka i pobicie; uszczerbek na zdrowiu (art. 156 kk; 157 kk); przestępstwa seksualne (art. 197 kk; 198 kk; 199 kk; 200 kk.; 200a kk; 200b kk.; 201 kk; 202 kk; 203 kk; 204 kk); liczba przestępstw w przeliczeniu na 10 tys. mieszkańców; kierowanie pojazdami mechanicznymi w stanie nietrzeźwym (art. 87 kw; 178a kk); posiadanie środków odurzających (art. 62 ustawy o przeciwdziałaniu narkomanii); udzielanie substancji psychotropowych (art. 58 i 59 ustawy o przeciwdziałaniu narkomanii); oszustwo „na wnuczka" (art. 286 kk); oszustwo „na policjanta" (art. 286 kk); interwencje Policji związane z zakłóceniem porządku publicznego; interwencje związane ze spożywaniem alkoholu w miejscach niedozwolonych; interwencje Policji związane z kradzieżą mienia; interwencje związane z uszkodzeniem mienia; liczba interwencji Policji łącznie. W każdej z wymienionych pozycji jest zamieszczony szczegółowy opis czynu i metodologii prowadzenia statystyk.

Mapa interaktywna umożliwiająca mieszkańcom sygnalizowanie miejsc zagrożonych jest narzędziem prostym w obsłudze i przez to przyjaznym użytkownikom w każdym wieku. Na stronie internetowej każdej jednostki Policji znajduje się zakładka „Krajowa Mapa Zagrożeń Bezpieczeństwa" w formie graficznego piktogramu i nazwy. Po kliknięciu na nią użytkownik jest przekierowany na stronę KGP, na podstronę KMZB. Znajduje się tam krótka informacja wyjaśniająca cel funkcjonowania i pouczenia związane z jej funkcjonowaniem. W przypadku wątpliwości administratorzy wskazali konkretny adres e-mail (kmzb@policja.gov.pl), każdy obywatel mający pytania i wątpliwości może je zadać za pośrednictwem poczty elektronicznej. Co istotne, opublikowano tam też materiał filmowy – czytelny instruktaż wskazujący, jak krok po kroku można dodać zgłoszenie w aplikacji KMZB. Ważne, że materiał ten jest przyjazny osobom niepełnosprawnym. Lektor opisuje kolejne czynności, a dodatkowo jest on tłumaczony na język migowy. To niewątpliwie poszerza zasięg potencjalnych odbiorców aplikacji. Dodatkowo na stronie znajduje się instrukcja obsługi KMZB do pobrania w formacie pliku .pdf. Ma ona formę przystępnego dokumentu, gdzie za pomocą grafik i krótkiego opisu

wskazano konkretne czynności pozwalające obywatelowi zgłosić niepokojące go zagrożenie. To wszystko powoduje, że obsługa aplikacji jest prosta i przystępna, co pozwala na jej powszechne wykorzystanie. Naniesienie zagrożenia na KMZB nie wymaga rejestracji i jest bezpłatne.

Przystępując do zgłoszenia zagrożenia, użytkownik musi zapoznać się z regulaminem KMZB i zaakceptować go. Po zatwierdzeniu regulaminu pojawia się okno mapy zawierające wszystkie dotychczasowe zgłoszenia dodane przez użytkowników. Aby zgłosić zagrożenie, należy w pierwszej kolejności wyszukać i przybliżyć konkretne miejsce występowania zagrożenia, kliknąć ikonę „Dodaj zgłoszenie", a następnie wybrać kategorię odpowiedniego zagrożenia i w pojawiającym się okienku wprowadzić opis zgłoszenia (można również dołączyć zdjęcie lub krótki film). Po uzupełnieniu tych informacji należy kliknąć ikonę „Zgłoś", co kończy procedurę zgłoszenia. Na ekranie pojawi się informacja o przyjęciu zgłoszenia przez system, a na mapie pojawi się ikona zgłoszenia w wybranym przez nas miejscu. Po dodaniu zgłoszenia nie może ono być modyfikowane i usuwane, a wszelkie błędy i pomyłki podczas zgłaszania powinny być zgłaszane administratorowi za pomocą poczty elektronicznej. Kolory piktogramów zgłoszeń na mapie świadczą o aktualnym statusie zagrożenia. Kolor zielony oznacza, że zagrożenie zostało naniesione na mapę przez użytkownika i jeszcze nie zapoznała się z nim Policja. W czasie do 3 dni (o ile zagrożenie nie zostanie uznane za żart lub pomyłkę) kolor zmieni się na żółty, co oznacza, że Policja zapoznała się z zagrożeniem i podjęła działania w celu weryfikacji, czy w istocie wskazane zagrożenie występuje na danym obszarze. Proces weryfikacji trwa do 7 dni od daty naniesienia zagrożenia na mapę (w szczególnie uzasadnionych przypadkach może być on dłuższy). W przypadku niepotwierdzenia zagrożenia piktogram przyjmuje kolor szary. Jest on widoczny na mapie przez 7 dni, po czym zostaje usunięty. Jeżeli natomiast zagrożenie zostało potwierdzone, piktogram jest czerwony. W przypadku zagrożenia, które zostało potwierdzone, a jego eliminacja jest zależna od innych podmiotów, piktogram przyjmuje kolor fioletowy, co oznacza, że zagrożenie takie jest eliminowane przez podmioty pozapolicyjne. W momencie wyeliminowania zagrożenia piktogram zmienia kolor na niebieski i jest widoczny na mapie przez 30 dni. Po tym czasie jest usuwany. Jak widać, zgłaszanie zagrożeń i obsługa KMZB

zostały maksymalnie uproszczone, a wprowadzenie zmian kolorystyki na piktogramach zgłoszeń jest czytelną informacją zwrotną dla użytkownika wskazującą kolejne kroki działania służb policyjnych i ich efekt.

Wdrożenie KMZB już od samego początku spowodowało aktywizację społeczeństwa na rzecz poprawy bezpieczeństwa w miejscach swojego zamieszkania. Ogółem od początku funkcjonowania KMZB (od grudnia 2016 r. do końca 2019 r.) obywatele nanieśli na mapę 1 357 714 zgłoszeń. Największa ich ilość została odnotowana na terenie województwa małopolskiego (177 727), śląskiego (155 717), dolnośląskiego (125 386) i wielkopolskiego (116 472).

Taki stan rzeczy nie byłby możliwy, gdyby nie odpowiednia promocja tego narzędzia komunikacji ze społeczeństwem. Począwszy od konsultacji społecznych, jak również po wdrożeniu projektu, policjanci z wielkim zaangażowaniem podeszli do tego projektu, upatrując w nim szansę na jeszcze lepszą współpracę z mieszkańcami i zdobywanie kolejnych danych poprawiających skuteczność w walce z naruszeniami prawa. Rozpowszechnianie informacji o KMZB odbywało się na wielu płaszczyznach. Zarówno w kontaktach bezpośrednich podczas organizowanych debat społecznych, przez dzielnicowych w ramach służby obchodowej, jak i za pośrednictwem środków masowego przekazu. Policjanci, uczestnicząc w spotkaniach z mieszkańcami, promowali tę możliwość komunikacji Policji ze społeczeństwem. Uzupełnieniem tego przekazu były plakaty KMZB umieszczane w jednostkach Policji, urzędach i obiektach użyteczności publicznej oraz gablotach parafialnych Kościoła rzymskokatolickiego. Służby prasowe jednostek Policji aktywnie współpracowały z lokalnymi i ogólnopolskimi mediami, przekazując informacje o funkcjonowaniu mapy przedstawicielom lokalnej prasy, radia, telewizji i portali internetowych.

Największą zaletą funkcjonowania KMZB jest możliwość współdziałania obywateli wraz z Policją w zapewnieniu bezpieczeństwa i porządku publicznego. Informacje przekazywane za pośrednictwem KMZB są bardzo dobrym uzupełnieniem wiedzy pozyskiwanej przez funkcjonariuszy w trakcie pełnienia codziennej służby. Szczególnie dzielnicowi dzięki mapie mają możliwość pogłębienia wiedzy o rejonie służbowym i jego skutecznego rozpoznania. Dane te nie tylko precyzują, w jakim dokładnie miejscu mogą występować zagrożenia, ale też w jakim stopniu są uciążliwe

dla społeczeństwa. Służą dzielnicowym do tworzenia planów działań priorytetowych, przede wszystkim na podstawie zdiagnozowanych oczekiwań społecznych oraz analizy zagrożenia w rejonie.

Ciągły rozwój KMZB sprawia, że nie tylko spełnia ona oczekiwania społeczne, ale również bardzo ułatwia pracę samych policjantów w procesie weryfikacji czy też eliminacji zagrożeń. Przykładem takim jest możliwość sygnalizowania problemów przez obywateli, poprzez funkcjonalność polegającą na możliwości dołączania opisów oraz zdjęć, które pozwalają na dokładniejsze określenie problemu oraz umożliwiają podjęcie precyzyjnych działań mających na celu ich wyeliminowanie.

Wszystkie działania służb w związku ze spływającymi sukcesywnie zgłoszeniami do KMZB wymagają rzetelnej weryfikacji, co z kolei przekłada się na potwierdzalność zgłoszeń. Potwierdzalność zgłoszeń na poziomie kraju z wynikiem 51,27% oznacza, że co drugie potencjalne zgłoszenie jest zgłoszeniem potwierdzonym, realnie wskazującym miejsca naruszenia prawa.

KMZB poprzez ilość zgłoszeń w poszczególnych kategoriach szybko zweryfikowała, jakie problemy najbardziej nurtują obywateli, a co za tym idzie, jakie działania trzeba podjąć, aby sprostać tym wyzwaniom. Największym wyzwaniem w obszarze Krajowej Mapy Zagrożeń Bezpieczeństwa w Małopolsce są kategorie związane z bezpieczeństwem i porządkiem w ruchu drogowym: przekraczanie dopuszczalnej prędkości (375 120 – potwierdzalność 65,5%) i nieprawidłowe parkowanie (352 048 – potwierdzalność 55,2%). W tym obszarze bezpieczeństwa znaczny odsetek zgłoszeń dotyczy także niewłaściwej infrastruktury drogowej (81 567 – potwierdzalność 63,9%) czy też złej organizacji ruchu drogowego (44 212 – potwierdzalność 35,2%). Ogółem można powiedzieć, że zgłoszenia związane z szeroko pojętym bezpieczeństwem i porządkiem w ruchu drogowym stanowią w skali kraju ok. 65% wszystkich zgłoszeń i jednocześnie mają one znaczną potwierdzalność. Z pozostałych kategorii na czołowe miejsca wysuwają się: używanie środków odurzających (43 615 – niewielka, zaledwie 11,6%, potwierdzalność), grupowanie się małoletnich zagrożonych demoralizacją (40 975 – potwierdzalność 31,1%), zgłoszenie dzikich wysypisk śmieci (36 525 – potwierdzalność 48,7%), akty wandalizmu (29 016 – potwierdzalność 36,1%).

Dotychczasowe doświadczenia związane z wykorzystywaniem KMZB pokazują, że pozwala ona nie tylko aktywizować społeczeństwo, ale także prowadzi do intensyfikacji współpracy Policji z innymi podmiotami. Do podmiotów pozapolicyjnych, które współpracują w zakresie KMZB, zaliczyć można m.in. straż gminną i miejską, które prowadzą zintegrowane działania z Policją mające na celu eliminację niekorzystnych zjawisk, przede wszystkim takich jak np. nieprawidłowe parkowanie. Kolejna grupa podmiotów, która współpracuje z Policją w zakresie eliminacji zagrożeń, to zarządcy dróg, którzy podejmują działania w przypadku potwierdzenia zgłoszeń dotyczących np. nieprawidłowego oznakowania lub nieprawidłowej organizacji ruchu. Ponadto współpraca w zakresie weryfikacji i eliminacji zagrożeń jest realizowana wraz ze Strażą Leśną, Strażą Rybacką oraz kołami łowieckimi. Wspólne działania podejmowane są na rzecz eliminowania zagrożeń dotyczących m.in. poruszania się po terenach leśnych quadami, kłusownictwem lub nielegalną wycinką drzew. W trakcie tych działań Straż Leśna kieruje do służby swoich funkcjonariuszy, którzy są wyposażeni w sprzęt umożliwiający sprawne poruszanie się po terenie leśnym, co daje możliwość skutecznej reakcji na zdarzenia, natomiast koła łowieckie ze względu na posiadaną wiedzę oraz doświadczenie potrafią trafnie określić, czy w danym miejscu dochodzi do wskazanych zdarzeń. Największą korzyścią, jaką można zauważyć we współpracy Policji z innymi służbami lub instytucjami, jest fakt, że takie współdziałanie często przenosi się na skuteczne realizowanie zadań dotyczących czynności mających na celu poprawę bezpieczeństwa w rejonach służbowych oraz w rozwiązywaniu problemów zgłaszanych przez mieszkańców. Bardzo dobrym rozwiązaniem, które się sprawdza w praktyce, jest organizowanie cyklicznych spotkań z podmiotami, które współpracują na co dzień z policjantami w zakresie obsługi KMZB. W trakcie takich spotkań określa się wspólne kierunki działań na rzecz eliminowania zagrożeń. Synergiczność działań w obszarze bezpieczeństwa wpływa na osiąganie lepszych efektów dla dobra lokalnych społeczności.

Właściwa i sprawna realizacja zadań związanych z funkcjonowaniem KMZB stała się możliwa dzięki wdrożeniu systemu informatycznego Karta Weryfikacji Zagrożenia, który służy do elektronicznego obiegu dokumentacji związanej z weryfikacją i eliminacją zagrożeń naniesionych

na KMZB. Takie rozwiązanie umożliwia gromadzenie jednolitych danych o wszystkich czynnościach związanych z funkcjonowaniem KMZB. Policjanci po wykonaniu zadania dokonują wpisu w aplikacji Karta Weryfikacji Zagrożenia, a kierownicy odpowiedzialni za realizację zadań związanych z weryfikacją na ich podstawie podejmują decyzję o nadaniu odpowiedniego statusu. Następnie karta pojawia się u koordynatora, który podejmuje dalsze decyzje, tzn. w przypadku nadania statusu niepotwierdzone dokonuje odpowiedniego wpisu i karta zostaje przeniesiona do archiwum, a w przypadku karty potwierdzonej wybiera z dostępnej listy odpowiedniego kierownika, któremu przesyła kartę do działań eliminacyjnych. Dzięki temu proces weryfikacji i eliminacji zagrożeń jest widoczny w systemie dla koordynatora wojewódzkiego i koordynatorów lokalnych, a zadania realizowane są na bieżąco z zachowaniem ogólnie przyjętych terminów oraz z zachowaniem właściwego nadzoru. Również dzięki funkcji dodawania komunikatów i powiadomień w systemie koordynatorzy każdego szczebla mają możliwość przekazania ważnych informacji oraz uwag wszystkim użytkownikom lub wybranej grupie oraz pewność, że informacja przez nich wygenerowana dotrze do adresatów, ponieważ jest ona widoczna na ekranie głównym zaraz po zalogowaniu się użytkownika do systemu.

Zarówno koordynatorzy lokalni, jak i kadra kierownicza mają możliwość bieżącego monitorowania określonych terminów weryfikacji zgłoszeń oraz realizacji zadań związanych z nimi. Generalnie przyjęto rozwiązanie, że zagrożenia, które dotyczą bezpieczeństwa w ruchu drogowym w podległych jednostkach, komendach powiatowych/miejskich, są nadzorowane przez naczelników Wydziału Ruchu Drogowego, natomiast nadzór nad pozostałymi zagrożeniami sprawują naczelnicy Wydziału Prewencji. Inną formą nadzoru związaną z prawidłowym funkcjonowaniem KMZB są patrole oficerskie realizowane przez policjantów przy współudziale innych komórek prewencyjnych (Sztab, Ruch Drogowy). Patrole takie w ramach wykonywania swoich obowiązków bardzo skrupulatnie sprawdzają poziom realizacji założeń zawartych w KMZB w jednostkach terenowych przez weryfikację zadań w Systemie Wspomagania Dowodzenia Policji i notatnikach służbowych. Również organizowane odprawy lub narady służbowe związane z tematem KMZB na

wszystkich szczeblach dowodzenia ukierunkowane są w szczególności na bieżącą analizę realizowanych zadań, problemów z tym związanych oraz kierunków jej działania.

KMZB okazała się narzędziem bardzo przydatnym, które nie tylko umożliwia mieszkańcom sygnalizowanie miejsc zagrożonych, lecz również ukazuje skalę i rodzaj zagrożeń dolegliwych dla lokalnych społeczności. Również dla samych policjantów informacje zawarte w KMZB przyczyniły się do pogłębienia wiedzy o występujących zagrożeniach. Jest to szczególnie przydatne dla dzielnicowych, którzy dzięki temu mają bardzo dobre rozeznanie, co dzieje się w ich rejonie służbowym na danym terenie. Wiedza taka pozwala na odpowiednią reakcję ze strony Policji, a społeczeństwu poprzez te działania daje poczucie większego bezpieczeństwa. Na uwagę zasługuje bardzo duża popularność tego narzędzia. Od początku działania KMZB obywatele z niej chętnie korzystają. Jest to zasługą nie tylko skutecznej akcji promocyjnej prowadzonej przez Policję, ale również zainteresowania społeczeństwa szybkimi i pragmatycznymi działaniami Policji, które mają na celu efektywną eliminację zagrożeń. Podkreślić należy, że utrzymująca się wysoka potwierdzalność zgłoszeń na poziomie 51,27% utwierdza w przekonaniu, że KMZB jest narzędziem, które rzetelnie diagnozuje dotkliwe społecznie zagrożenia i tym samym pozwala Policji skuteczniej ukierunkowywać działania prewencyjne.

Krzysztof Dymura, Agnieszka Polończyk

T. Guz, *Filozoficzne aspekty bezpieczeństwa człowieka*, [w:] *Społeczno-moralna potrzeba bezpieczeństwa i porządku publicznego*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin 2007; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78 poz. 483; E. Korzeniowski, *Bezpieczeństwo – wieloaspektowa forma istnienia w warunkach zagrożenia*, [w:] *Administracja, zarządzanie i handel zagraniczny w warunkach integracji. Materiały konferencyjne – Zarządzanie bezpieczeństwem*, K. Budzowski (red.), Krakowska Szkoła Wyższa im. Andrzeja Frycza Modrzewskiego, Kraków 2002; Krajowa Mapa Zagrożeń Bezpieczeństwa, Policja.pl (dostęp 12.02.2020); P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego"

2012, nr 7 (4); D. Minkiewicz, *Funkcje Krajowej Mapy Zagrożeń Bezpieczeństwa w kształtowaniu bezpieczeństwa społeczności lokalnej*, „Kwartalnik Policyjny" 2017, nr 3; D. Pater, *Społeczne wsparcie działań Policji mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym*, „Probacja" 2018, nr 12 (IV); „Policja 997" 2017, nr 9, wyd. spec.: *Krajowa Mapa Zagrożeń Bezpieczeństwa*; A. Polończyk, A. Leśniak, *A Spatial Analysis of Selected Categories of Offences in Kraków Based on Data from the National Safety Risk Map*, [w:] *Proceedings. 2018 Baltic Geodetic Congress (BGC Geomatics)*, IEEE Computer Society, Los Alamitos–Washington–Tokyo 2018; ciż, *The Impact of Generalised Spatial Data on the Incidence Density of Selected Offences in Kraków*, [w:] *Proceedings. 2018 Baltic Geodetic Congress (BGC Geomatics)*, IEEE Computer Society, Los Alamitos–Washington–Tokyo 2018; A. Polończyk, *Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa*, [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; J. Stawnicka, I. Klonowska, *Krajowa Mapa Zagrożeń Bezpieczeństwa nową formą dialogu polskiej Policji ze społecznością lokalną na rzecz bezpieczeństwa wewnętrznego. Aspekt społeczno-pedagogiczny*, Oficyna Wydawnicza „Humanitas", Sosnowiec 2018; J. Stawnicka, *Regulacje prawne i funkcjonowanie Krajowej Mapy Zagrożeń Bezpieczeństwa – istotnego elementu procesu zarządzania bezpieczeństwem publicznym przez polską Policję*, „Roczniki Administracji i Prawa" 2018, nr XVIII(1); Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. 1990, nr 30, poz. 179 z późn. zm.; Wytyczne nr 1 Komendanta Głównego Policji z dnia 31 lipca 2017 r. zmieniające wytyczne w sprawie sposobu postępowania policjantów podczas realizacji zadań związanych z funkcjonowaniem Krajowej Mapy Zagrożeń Bezpieczeństwa, Dz. Urz. KGP 2017, poz. 53; Wytyczne nr 3 Komendanta Głównego Policji z dnia 14 września 2016 r. w sprawie sposobu postępowania policjantów podczas realizacji zadań związanych z funkcjonowaniem Krajowej Mapy Zagrożeń Bezpieczeństwa, Dz. Urz. KGP 2016, poz. 58; Zarządzenie nr 5 Komendanta Głównego Policji z dnia 20 czerwca 2016 r. w sprawie metod i form wykonywania zadań przez dzielnicowego i kierownika dzielnicowych, § 38. 1, Dz. Urz. KGP z 2016 r., poz. 26 z późn. zm.; Zarządzenie nr 768 Komendanta Głównego Policji z dnia 14 sierpnia 2007 r. w sprawie form i metod wykonywania zadań przez policjantów pełniących służbę patrolową oraz koordynacji działań o charakterze prewencyjnym, Dz. Urz. KGP 2007 nr 15, poz. 119, z późn. zm.

KRAJOWY OŚRODEK ZAPOBIEGANIA ZACHOWANIOM DYSSOCJALNYM (również pod nazwą Regionalny Ośrodek Psychiatrii Sądowej) – zakład zamknięty należący do ogólnopolskiej sieci instytucji leczniczych

realizujących zadania w zakresie psychiatrii sądowej. Został utworzony na podstawie Ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających → zagrożenie [t. 4] życia, zdrowia lub wolności seksualnej innych osób. Pierwsza osoba została umieszczona w ośrodku w 2014 r., obecnie przebywa tam ponad 40 pacjentów. Ośrodek mieści się w Gostyninie w województwie mazowieckim.

Ideą przyświecającą utworzeniu ośrodka było stworzenie miejsc bezterminowego odosobnienia dla osób, które odbyły kary pozbawienia wolności za ciężkie przestępstwa, ale nadal są uznawane za stwarzające zagrożenie dla społeczeństwa, polegające przede wszystkim na wysokim prawdopodobieństwie popełniania przez nie kolejnych przestępstw po opuszczeniu zakładu karnego. Z założenia ośrodek miał być miejscem, gdzie byli więźniowie będą poddawani terapii. Motywacją podjęcia prac nad ustawą były nagłośnione w mediach przypadki osób skazanych za popełnienie ciężkich przestępstw na tle seksualnym, w tym czynów na szkodę małoletnich. Wyrokami wydanymi przed grudniem 1989 r. zostali oni skazani na karę śmierci, która została jednak zamieniona na karę 25 lat pozbawienia wolności w wyniku amnestii. Wobec bliskości terminu planowego opuszczenia przez nich zakładu karnego przedstawiciele mediów i świata polityki podjęli debatę nad koniecznością dalszego izolowania ich od społeczeństwa.

Zgodnie z ustawą osoby stwarzające zagrożenie mogą zostać umieszczone w ośrodku, jeśli odbywają prawomocnie orzeczoną karę pozbawienia wolności lub karę 25 lat pozbawienia wolności, wykonywaną w systemie terapeutycznym, w trakcie postępowania wykonawczego występowały u nich zaburzenia psychiczne w postaci upośledzenia umysłowego, zaburzenia osobowości lub zaburzenia preferencji seksualnych, a stwierdzone u nich zaburzenia psychiczne mają taki charakter lub takie nasilenie, że zachodzi co najmniej wysokie prawdopodobieństwo popełnienia → czynu zabronionego [t. 1] z użyciem → przemocy [t. 3] lub groźbą jej użycia przeciwko życiu, zdrowiu lub wolności seksualnej, zagrożonego karą pozbawienia wolności, której górna granica wynosi co najmniej 10 lat.

Bezterminowe umieszczenie w ośrodku następuje na podstawie orzeczenia sądu okręgowego, które wydawane jest na wniosek dyrektora zakładu karnego. W postępowaniu bierze udział skazany, który obligatoryjne

musi mieć obrońcę (w razie braku obrońcy z wyboru sąd przydziela mu obrońcę z urzędu). Podstawą do złożenia wniosku są negatywne opinie psychologiczna i psychiatryczna, wskazujące na ziszczenie się wcześniej wymienionych przesłanek uznania za osobę stwarzającą zagrożenie. Niezależnie od tego w toku postępowania opinię na temat skazanego wydają biegli sądowi – 2 biegłych psychiatrów oraz ewentualnie biegli psycholog i seksuolog.

Osoba stwarzająca zagrożenie umieszczona w ośrodku zostaje objęta odpowiednim postępowaniem terapeutycznym, którego celem jest poprawa stanu jej zdrowia i zachowania w stopniu umożliwiającym funkcjonowanie w społeczeństwie w sposób niestwarzający zagrożenia życia, zdrowia lub wolności seksualnej innych osób. Kierownik ośrodka sporządza indywidualny plan terapii dla każdej osoby umieszczonej w ośrodku. Nie rzadziej niż raz na 6 miesięcy sąd na podstawie opinii lekarza psychiatry oraz wyników postępowania terapeutycznego ustala, czy dalszy pobyt w ośrodku danej osoby jest niezbędny. Kierownik ośrodka co 6 miesięcy przesyła do sądu opinię lekarza psychiatry o stanie zdrowia i o wynikach postępowania terapeutycznego osoby umieszczonej w ośrodku. Opinię taką jest zobowiązany także przesłać bezzwłocznie, jeżeli w związku ze zmianą stanu zdrowia tej osoby uzna, że jej dalszy pobyt w ośrodku nie jest konieczny.

Od momentu uchwalenia ustawa budzi liczne i poważne wątpliwości. Zastrzeżenia co do zgodności jej przepisów z konstytucją zgłosił Rzecznik Praw Obywatelskich, kierując skargę do Trybunału Konstytucyjnego (TK). Podmiotami inicjującymi postępowanie przed TK byli również: prezydent, Sąd Okręgowy w Lublinie I Wydział Cywilny, Sąd Apelacyjny we Wrocławiu Wydział I Cywilny. 23 listopada 2016 r. Trybunał Konstytucyjny ogłosił wyrok (sygn. K 6/14), uznając większość zakwestionowanych przepisów za zgodne z konstytucją. Trybunał tylko co do jednego przepisu stwierdził naruszenie postanowień Konstytucji RP.

Obiekcje budzi jednak nadal szereg kwestii. W pierwszej kolejności wymienić należy bezterminowe odosobnienie i izolowanie osób, które odbyły już kary pozbawienia wolności zasądzone wyrokami sądu. Oznacza to, że przymusowo izolowane są osoby, które nie popełniły żadnego przestępstwa, bo za czyny uprzednio popełnione odbyły już karę, a dodatkowo

czas ich pobytu w ośrodku nie jest określany z góry. Można więc mówić o nielimitowanej karze bez przestępstwa i pozbawieniu wolności bez wyroku sądu.

Kolejna grupa zastrzeżeń dotyczy umieszczenia w ośrodku terapeutycznym osób chorych psychicznie, wobec których terapia nie może być prowadzona ze względu na stan ich zdrowia. Brak procedur pozwalających na przeniesienie pacjenta z ośrodka do szpitala psychiatrycznego, jeśli wymaga tego stan jego zdrowia lub został błędnie skierowany do ośrodka.

Z krytyką spotyka się także praktyka funkcjonowania ośrodka, w którym umieszczane są kolejne osoby. Pensjonariusze skarżą się na trudne warunki mieszkaniowe wynikające z przeludnienia oraz na rygory związane z kontrolami osobistymi i korespondencji, np. brakiem możliwości uzyskania przepustki na pogrzeb członków rodziny. Podkreślić należy, że nie są to osoby skazane, wobec których rygory naśladujące zakład karny mogłyby być rozumiane jako elementy kary. Nawet skazani osadzeni w więzieniach mają szereg praw, które w ośrodku nie są realizowane. Na pierwszym miejscu wymienić należy prawo do zachowania tajemnicy korespondencji z obrońcą. Podkreślić należy, iż ustawa, na podstawie której ośrodek został utworzony, nie określa jasno praw i obowiązków jego pensjonariuszy. W rezultacie ich prawa są niejednokrotnie bardziej ograniczone niż prawa skazanych przebywających w więzieniach. Regulacje pomijają sferę życia codziennego, warunków bytowych, zakupów, widzeń, korespondencji, rozmów telefonicznych, wyżywienia, kontroli osobistych, postępowania z pacjentami naruszającymi przepisy, możliwości wniosków, skarg i odwołań od decyzji dyrektora. Wobec osób przebywających w ośrodku stosowane są np. kary dyscyplinarne, które nie mają żadnej podstawy prawnej, nie istnieje bowiem żaden akt pozwalający na ich nakładanie, ustanawiający system kontroli nad nimi. W efekcie dochodzi np. do nakładania kar bezterminowych.

Z powodu przeludnienia i braków lokalowych utrudnione jest także prowadzenie terapii, a więc realizowanie głównego celu, dla którego ośrodek został powołany. Metody terapii stosowane w ośrodku, poza farmakoterapią, zostały ocenione krytycznie w opinii Krajowego Mechanizmu Prewencji Tortur, który przeprowadził wizytację ośrodka w 2019 r.

W raporcie z wizytacji wskazano, że podstawową formą jest terapia indywidualna zamiast grupowej. Zwrócono także uwagę na fakt, iż osadzeni nie mają zaufania do terapeutów, skoro nie jest przestrzegana zasada poufności, a podawane przez nich w czasie terapii → i n f o r m a c j e są później zamieszczane w aktach, dostępnych dla wielu osób.

Wątpliwości natury prawnej budzi sposób przedłużania pobytu w ośrodku. Obecnie nie jest wymagane wydanie w tym zakresie orzeczenia przez sąd ani też udział w posiedzeniu osadzonego czy jego obrońcy. Oznacza to, iż osadzony nie ma możliwości zaskarżenia decyzji sądu, albowiem środki odwoławcze przysługują wyłącznie w odniesieniu do orzeczeń. Standardy przyjęte w ustawie słabiej gwarantują ochronę praw i wolności osadzonych niż regulacje dotyczące pobytu niepoczytalnych sprawców przestępstw w szpitalach psychiatrycznych.

Od czasu utworzenia ośrodka na liczne mankamenty jego funkcjonowania oraz na konieczność uzupełniania i zmiany przepisów uwagę zwracał Rzecznik Praw Obywatelskich, do potrzebnych zmian jednak nie doszło.

Anna Pacholska

A. Depko, K. Eichstaedt, P. Gałecki, *Metodyka pracy biegłego psychiatry, psychologa oraz seksuologa w sprawach karnych, nieletnich oraz wykroczeń*, Wolters Kluwer Polska, Warszawa 2017; Raport przedstawicieli Krajowego Mechanizmu Prewencji Tortur z wizytacji Krajowego Ośrodka Zapobiegania Zachowaniom Dyssocjalnym w Gostyninie, RPO.gov.pl (dostęp 8.02.2020); Rozporządzenie Ministra Zdrowia z dnia 16 stycznia 2014 r. w sprawie Krajowego Ośrodka Zapobiegania Zachowaniom Dyssocjalnym, Dz. U. 2016.1480 t.j.; K. Żaczkiewicz-Zborska, *Bezterminowy pobyt w ośrodku dla groźnych przestępców zgodny z Konstytucją RP*, LEX/el. 2017; Ustawa z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób, Dz. U. 2019.2203.

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA – działa w Polsce od 28 sierpnia 2018 r. na mocy przepisów Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Próby wypracowania efektywnej polityki zapewnienia →b e z p i e c z e ń s t w a [t. 1] w →c y b e r p r z e s t r z e n i [t. 1] rozpoczęły się w Polsce w 2008 r. wraz z uchwaleniem

Rządowego programu ochrony cyberprzestrzeni RP na lata 2009–2011. Niewątpliwie asumptem do opracowania programu były ratyfikacja przez Polskę 16 maja 2005 r. konwencji Rady Europy o zapobieganiu → terroryzmowi [t. 4], a także ataki cybernetyczne wymierzone w Estonię w 2007 i Gruzję w 2008 r. Wówczas większość państw europejskich podjęła próbę wdrożenia → strategii [t. 4] i doktryn w zakresie → cyberbezpieczeństwa [t. 1]. Jednakże dopiero ustawa z 2018 r. nadała realny kształt systemowi i w pełni umożliwiła jego funkcjonowanie.

Zgodnie z art. 3 wspomnianego aktu prawnego polski system cyberbezpieczeństwa ma zapewnić bezpieczeństwo cyberprzestrzeni Rzeczypospolitej Polskiej. Generalnie chodzi głównie o zagwarantowanie ciągłości świadczenia usług kluczowych, a więc tych o szczególnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Usługi te zostały wskazane w załączniku do Rozporządzenia Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (generowanie i dystrybucja energii elektrycznej, administrowanie infrastrukturą energetyczną, produkcja paliw ciekłych bądź utrzymywanie rezerw strategicznych i zapasów ropy naftowej, produktów naftowych oraz gazu ziemnego itp.). Ponadto system cyberbezpieczeństwa odpowiada również za utrzymanie ciągłości świadczenia usług cyfrowych świadczonych elektronicznie (np. internetowe platformy handlowe, usługi przetwarzania w chmurze, wyszukiwarki internetowe). Ustawodawcy chodziło o stworzenie spójnego i efektywnego systemu odpowiedzialnego za szeroko pojęte cyberbezpieczeństwo. Przepisy ustawy wyraźnie sformułowały zakres odpowiedzialności podmiotów i instytucji, których aktywność w tym zakresie ma zapewnić lepszą wykrywalność, zapobieganie oraz minimalizowanie skutków wszelkich incydentów sieciowych, zarówno awarii, jak i ataków sieciowych. Na mocy ustawy z 2018 r. implementowano zatem zharmonizowany mechanizm pozwalający wykrywać, powiadamiać oraz reagować w obliczu potencjalnych → cyberzagrożeń [t. 1].

Bezpieczeństwo w cyberprzestrzeni jest pojmowane w kategoriach bezpieczeństwa przesyłu oraz wymiany danych i → informacji (rozumianych jako treści cyfrowe). Z cyberbezpieczeństwem wiąże się również bezpieczne świadczenie usług na odległość za pośrednictwem systemów

informatycznych. Wspomniane usługi są realizowane przez operatorów usług kluczowych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli oraz usług świadczonych na indywidualne żądanie użytkowników internetu przez dostawców usług cyfrowych.

W myśl przepisów ustawy z 2018 r. utrzymanie cyberbezpieczeństwa na poziomie krajowym mają zapewnić właściwie funkcjonujące systemy informacyjne, świadcząc usługi kluczowe i cyfrowe oraz zapewniające obsługę incydentów. Tak skonstruowany krajowy system cyberbezpieczeństwa pozwolił wygenerować swoistą przestrzeń, dzięki której jest możliwa skuteczna i skoordynowana współpraca pomiędzy podmiotami świadczącymi usługi cyfrowe a organami i instytucjami państwowymi właściwymi w zakresie cyberbezpieczeństwa. W ustawie w sposób enumeratywny wyszczególniono kilkanaście kategorii podmiotów krajowego systemu cyberbezpieczeństwa, do których zaliczono:

- operatorów usług kluczowych;
- dostawców usług cyfrowych;
- zespoły reagowania na incydenty bezpieczeństwa komputerowego (ang. Computer Security Incident Response Team, CSIRT), działające na poziomie krajowym, powołane w: Ministerstwie Obrony Narodowej (CSIRT MON), Naukowej i Akademickiej Sieci Komputerowej Państwowym Instytucie Badawczym (CSIRT NASK) oraz w → Agencji Bezpieczeństwa Wewnętrznego [t. 1] (CSIRT GOV);
- sektorowe zespoły cyberbezpieczeństwa (np. utworzone przez → organy właściwe do spraw cyberbezpieczeństwa [t. 3]);
- podmioty publiczne, w tym jednostki sektora finansów publicznych (organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasę Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; uczelnie

publiczne; Polską Akademię Nauk i tworzone przez nią jednostki organizacyjne, instytuty badawcze, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polską Agencję Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, spółki prawa handlowego realizujące zadania użyteczności publicznej na rzecz bieżącego i permanentnego zaspokajania zbiorowych potrzeb ludności w drodze świadczenia usług dostępnych na zasadzie powszechności;

- podmioty świadczące usługi z zakresu cyberbezpieczeństwa;
- organy właściwe do spraw cyberbezpieczeństwa;
- Pojedynczy Punkt Kontaktowy ds. cyberbezpieczeństwa;
- Pełnomocnika Rządu ds. Cyberbezpieczeństwa;
- Kolegium do Spraw Cyberbezpieczeństwa.

Za operatorów usług kluczowych uznano firmy działające w określonych sektorach:

- finansowym (banki krajowe i zagraniczne wraz z oddziałami, spółdzielcze kasy oszczędnościowo-kredytowe);
- energetycznym (przedsiębiorstwa z koncesją na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, przesyłania ropy naftowej, wytwarzania paliw syntetycznych, przetwarzania albo magazynowania energii elektrycznej, wydobywania gazu ziemnego);
- transportowym (firmy specjalizujące się w transporcie lotniczym i kolejowym oraz podmioty z zakresu transportu drogowego);
- →ochrony zdrowia [t. 3] (podmioty lecznicze, wytwórcy produktów leczniczych, przedsiębiorcy prowadzący apteki lub hurtownie farmaceutyczne);
- zaopatrzenia w wodę pitną (przedsiębiorstwa wodno-kanalizacyjne).

Aby krajowy system cyberbezpieczeństwa stanowił efektywny mechanizm zabezpieczający przed cyberzagrożeniami, powołano tzw. system zarządzania cyberbezpieczeństwem, który w Polsce obejmuje poziom roboczy, za który odpowiada Zespół ds. Obsługi Incydentów Krytycznych,

oraz poziom instytucjonalny, reprezentowany przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa i Kolegium ds. Cyberbezpieczeństwa.

Zespół ds. Obsługi Incydentów Krytycznych pełni funkcję pomocniczą w sprawach obsługi incydentów zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV. Jest również organem koordynującym działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV i → Rządowe Centrum Bezpieczeństwa [t. 3]. W gremium tym zasiadają przedstawiciele CSIRT MON, CSIRT NASK, szefa Agencji Bezpieczeństwa Wewnętrznego (ABW) realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa (RCB). Prace Zespołu są obsługiwane przez RCB, którego dyrektor przewodniczy tymże pracom.

Pełnomocnik Rządu ds. Cyberbezpieczeństwa koordynuje działania i realizuje politykę rządu w zakresie cyberbezpieczeństwa. Analizuje zatem i prowadzi ocenę funkcjonowania krajowego systemu cyberbezpieczeństwa. Sprawuje również nadzór nad procesem zarządzania ryzykiem systemu cyberbezpieczeństwa RP, opiniuje dokumenty rządowe, upowszechnia innowacyjne rozwiązania służące zapewnieniu cyberbezpieczeństwa, inicjuje krajowe ćwiczenia z zakresu cyberbezpieczeństwa oraz na wniosek CSIRT rekomenduje stosowanie określonych urządzeń informatycznych lub oprogramowania. Ponadto pełnomocnik współpracuje w zakresie cyberbezpieczeństwa z innymi państwami, instytucjami czy też organizacjami międzynarodowymi, wspiera badania naukowe z obszaru bezpieczeństwa w sieci oraz angażuje się w prace zmierzające do podniesienia poziomu świadomości społeczeństwa, zwłaszcza w zakresie bezpiecznego korzystania z internetu oraz ryzykownych działań z tym związanych.

Natomiast Kolegium ds. Cyberbezpieczeństwa jest organem opiniodawczo-doradczym w sprawach cyberbezpieczeństwa oraz aktywności CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa, a także organów właściwych do spraw cyberbezpieczeństwa. Kolegium składa się z: Prezesa Rady Ministrów (przewodniczącego Kolegium), Pełnomocnika Rządu ds. Cyberbezpieczeństwa, ministra ds. wewnętrznych, ministra ds. informatyzacji, ministra obrony narodowej, ministra ds. zagranicznych, szefa Kancelarii Prezesa Rady Ministrów, szefa → Biura Bezpieczeństwa Narodowego [t. 1], ministra odpowiedzialnego za koordynację → służb specjalnych [t. 4] lub

osoby przez niego upoważnionej (jeśli nie został wyznaczony odpowiedni minister, to jego miejsce zajmuje szef ABW). W obradach Kolegium uczestniczą również osoby bezpośrednio lub pośrednio odpowiedzialne za zapewnienie bezpieczeństwa państwa, m.in. dyrektor RCB, szef ABW (bądź jego zastępca), szef → Służby Kontrwywiadu Wojskowego [t. 4] (bądź jego zastępca), a także dyrektor NASK.

Struktura krajowego systemu cyberbezpieczeństwa wydaje się logiczna i uzasadniona, bowiem za efektywność systemu odpowiadają zespoły reagowania na incydenty bezpieczeństwa komputerowego funkcjonujące na poziomie krajowym, a zatem CSIRT MON, CSIRT NASK oraz CSIRT GOV. Każdy z tych zespołów realizuje swoje ustawowe obowiązki w konkretnym obszarze: CSIRT MON w obszarze wojskowym, a CSIRT NASK cywilnym. CSIRT GOV działa na poziomie administracji publicznej. Daje się jednak zauważyć deficyt zespołów reagowania na incydenty w obszarach bezpośrednio związanych z → infrastrukturą krytyczną, stanami nadzwyczajnymi oraz atakami terrorystycznymi. Wątpliwa jest także reakcja poszczególnych sektorów na potencjalne incydenty, zwłaszcza chodzi o sektor ochrony zdrowia, transportu czy też zaopatrzenia w wodę pitną.

Utworzenie krajowego systemu cyberbezpieczeństwa w Polsce było podyktowane koniecznością wdrożenia do polskiego porządku prawnego postanowień Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Network and Information Systems Directive, dyrektywa NIS). Jednak dyrektywa NIS nie ograniczała państw członkowskich UE konkretnymi rozwiązaniami w zakresie cyberbezpieczeństwa, pozwalając tym samym na dowolność w kwestii wyboru właściwego modelu organizacji systemu odpowiedzialnego za zapewnienie bezpieczeństwa w cyberprzestrzeni.

Powołane przepisami ustawy z 2018 r. zespoły ds. bezpieczeństwa komputerowego i reagowania na incydenty wywodzą się od zespołów uruchomionych pod koniec lat 80. XX w. W 1988 r. miała miejsce jedna z poważniejszych w skutkach epidemia tzw. robaka Morrisa (Morris Worm), który zainfekował globalne systemy informatyczne. W odpowiedzi na atak podjęto prace nad skonstruowaniem systemu właściwego

reagowania na incydenty w obszarze bezpieczeństwa informatycznego. Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (ang. Defence Advanced Research Projects Agency, DARPA) powołała w Uniwersytecie Carnegiego i Mellonów w Pittsburgu pierwszy specjalistyczny zespół CSIRT – Centrum Koordynacji CERT (Computer Emergency Response Team). Zespoły zaczęły również powstawać w Europie. Pierwszy z nich – SURFnet-CERT – został powołany w 1992 r. z inicjatywy holenderskiego dostawcy usług internetowych. Zespół funkcjonował w ramach ośrodków akademickich. Nowo powstające CERT coraz szybciej uzyskały miano prężnie działających jednostek specjalizujących się nie tylko w skutecznym reagowaniu na pojawiające się incydenty, ale również świadczące usługi prewencyjne i szkoleniowe. Ewolucja zespołów CERT i coraz wyższy poziom ich specjalizacji przyczyniły się do wprowadzenia nowego terminu – CSIRT.

Julia Anna Gawęcka

J. Gawęcka, *Krajowy system cyberbezpieczeństwa*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *Krajowy system cyberbezpieczeństwa*, gov.pl (dostęp 25.03.2019); *Krajowy system cyberbezpieczeństwa*, KSOIN.pl (dostęp 26.03.2019); M. Maj, *Pięć kluczowych wyzwań przy wdrożeniu Ustawy o krajowym systemie cyberbezpieczeństwa*, 13.07.2018, CyberSecurity.org (dostęp 23.03.2019); *The Morris Worm. 30 Years Since First Major Attack on the Internet*, 2.10.2018, FBI.gov (dostęp 25.03.2019); Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.

KRYMINALISTYKA – nauka, która przy zastosowaniu taktyki i techniki śledczej stawia sobie za cel optymalne wypracowanie metod ustalenia faktu popełnienia przestępstwa, sposobów działania sprawcy bądź sprawców, ich identyfikacji, zabezpieczenia i zebrania dowodów potwierdzających ich winę i określających stopień przyczynienia się do zaistnienia przestępstwa oraz zapobiegania czynom przestępczym i → patologiom społecznym [t. 3].

Przy tak szerokim spektrum zainteresowań badawczych w kryminalistyce można wyodrębnić kilka działów. Jednym z nich jest taktyka

kryminalistyczna obejmująca wiedzę o optymalnym, szybkim oraz zgodnym z etyką zawodową i prawem wykorzystywaniu sposobów i metod, głównie w sferze organizacji działań i ich efektywnej realizacji, ukierunkowanej bezpośrednio na walkę ze sprawcą czynu bezprawnego. Technika kryminalistyczna ma w swym zainteresowaniu metody, środki oraz sposoby wykorzystania zdobyczy nauk technicznych i przyrodniczych, a także własnych osiągnięć kryminalistyki, pomocnych głównie w obszarze badania → i n f o r m a c j i i ich źródeł pochodzących od dowodów rzeczowych i śladów. → S t r a t e g i a [t. 4] to wiedza typu prognostycznego pozwalająca na przewidywanie kierunków, metod i środków działania przestępców w przyszłości, a także wiedza przygotowująca nowe metody, środki i przedsięwzięcia, które umożliwią skuteczne zwalczanie tej przyszłej → p r z e s t ę p c z o ś c i [t. 3]. Ważnym działem jest także metodyka kryminalistyczna, która adaptuje osiągnięcia taktyki i techniki do konkretnej specyfiki zwalczania określonych grup przestępstw.

Kryminalistyka jest nauką relatywnie młodą, gdyż powstała dopiero w XIX w. Ma charakter interdyscyplinarny, gdyż korzysta z dorobku innych nauk, takich jak nauki techniczne (głównie mechanika, elektronika, metaloznawstwo), przyrodnicze (chemia, fizyka, biologia), medyczne (medycyna sądowa, psychiatria, anatomia), humanistyczne (psychologia, językoznawstwo), prawo karne, kryminologia czy nauki o → p o l i c j i [t. 3]. Kryminalistyka nie przejmuje jednak w sposób automatyczny metod badawczych z innych nauk, lecz dokonuje ich twórczej adaptacji do swych specyficznych celów. Absolutnie nie można zgodzić się z tezą Ch.E. O'Hary i J.W. Osterburga, że kryminalistyka ma charakter pasożytniczy i bazuje wyłącznie na tym, co wypracowały już inne dziedziny nauk. Podejście tych badaczy wynika z ich wąskiego postrzegania kryminalistyki, którą uważali za naukę o zastosowaniu metod fizycznych do wykrywania przestępstw.

Kryminalistyka wypracowuje własne metody, jak np. psychologiczne założenia gromadzenia i oceny materiału dowodowego lub daktyloskopia, bądź inspiruje podjęcie badań mających na celu wykorzystanie zdobyczy różnych dyscyplin nauki do osiągnięcia większej efektywności śledczej. To dziedzina wiedzy, która twórczo dostosowuje metody badawcze wypracowane przez inne nauki do optymalizacji własnych celów (wykorzystanie

rentgenografii, spektrografii, badań śladów w promieniach UV i UR). Kryminalistyka recypuje najnowsze metody wypracowane w naukach przyrodniczych i technicznych, ale coraz większego znaczenia nabiera jej funkcja prewencyjna, która polega na wskazywaniu, jak unikać → z a g r o ż e ń [t. 4] i jak skutecznie redukować ich negatywne skutki. Ten cel można osiągnąć dzięki poznaniu metod działania sprawców. Brak takiej wiedzy uniemożliwia nie tylko ich wykrycie, ale przede wszystkim zapobieganie podobnym czynom w przyszłości. Wiedział o tym już na początku XIX w. szef francuskiej policji kryminalnej E.-F. Vidocq. Rekrutował on funkcjonariuszy spośród przestępców, tak by mogli wykorzystać znajomość kryminalnych metod działania sprawców dla poprawy efektywności wykrywczej. Jednak postrzeganie kryminalistyki jako nauki kompleksowej i interdyscyplinarnej ewoluowało stopniowo, co ujawniało się w jej warstwie definicyjnej.

Według P. Horoszowskiego kryminalistyka bada sposoby i środki popełniania przestępstw, wypracowując narzędzia służące do ich wykrycia oraz identyfikacji i ujęcia sprawcy. Z kolei W. Gutekunst wskazywał, że kryminalistyka jest nauką o taktyce i technice dokonywania przestępstw, prowadzenia dochodzenia oraz zapobiegania czynom przestępczym. R.S. Biełkin dostrzega wprawdzie walor profilaktyczny kryminalistyki, ale zawęża jej obszar do procesu wykrywania przestępstw jedynie w aspekcie dowodowym. Według F. Meixnera kryminalistyka jest nauką o formach objawowych przestępczości, o metodach popełniania i zapobiegania oraz ujawniania, stwierdzenia i wyjaśnienia faktu przestępstwa, jak również ustalenia sprawcy. Zdaniem F. Kleinschmidta obszarem zainteresowań kryminalistyki są szczególne formy objawowe przestępczości, przyczyny przestępstw oraz metody ich zwalczania i zapobiegania. T. Tomaszewski i Z. Czeczot zwracają uwagę na fakt, iż kryminalistyka jest nauką praktyczną, która opracowuje zasady sprawnego działania, stosowanie środków technicznych i laboratoryjnych metod badawczych dla zapobiegania popełnianiu i wykrywania przestępstw oraz ustalania faktów mających znaczenie dowodowe w postępowaniu karnym.

Współczesna kryminalistyka zmierza do zapewnienia efektywności ścigania karnego oraz profilaktyki kryminalnej, stąd używa zarówno metody indukcji, jak i dedukcji. Wskazanie *modus operandi* odbywa się

w drodze badań empirycznych, a elementy taktyki śledczej są wynikiem ustalonych prawidłowości, czyli procesu rozumowania dedukcyjnego.

Kryminalistyka realizuje funkcję rozpoznawczą poprzez wypracowanie metod i środków służących do uzyskania możliwie największej liczby informacji o miejscach, przedmiotach, osobach oraz taktyce aktualnych i przyszłych działań kryminalistycznych. Informacje te mogą być zdobywane i przetwarzane poprzez pracę policjantów referatów patrolowo-interwencyjnych, obchód dzielnicowego czy pracę operacyjną polegającą na prowadzeniu rozpoznania osobowego, terenowego, środowiskowego i problemowego.

Ważnym źródłem tych danych są poufne, osobowe źródła informacji, często pozyskiwane w środowisku przestępczym. Funkcja wykrywcza kryminalistyki to ogół działań organów ścigania skierowanych na ujawnianie przestępstw oraz uzyskanie informacji umożliwiających indywidualizację sprawcy. Przedmiotem działań wykrywczych jest zdarzenie (przestępstwo), mechanizm powstawania określonych zjawisk (okoliczności towarzyszące przestępstwu) oraz rzeczy (narzędzia przestępstwa, przedmioty uzyskane w trakcie jego popełnienia). W procesie wykrywczym możemy wyróżnić 3 stadia: poszukiwanie przedmiotu wykrywania oraz dotyczących go informacji, ujawnianie tych informacji oraz weryfikację, czyli stwierdzenie, czy znaleźliśmy to, czego poszukiwaliśmy. Ustalenia wymaga: miejsce działania sprawcy przed zdarzeniem, miejsce zdarzenia, miejsce działania sprawcy po zdarzeniu, ofiara i jej środowisko, a zwłaszcza środowisko kryminogenne i skonfliktowane z ofiarą.

Kryminalistyka posługuje się zestawem 7 tzw. złotych pytań: co?, gdzie?, kiedy?, w jaki sposób?, dlaczego?, jakimi środkami?, kto? Analizując posiadane materiały, uzupełnione o wyniki → czynności operacyjno-rozpoznawczych [t. 1], należy szukać odpowiedzi na dodatkowe pytania mające charakter wykrywczy, z których najważniejsze to:

- Kto wiedział lub mógł wiedzieć?
- Kto chciał lub mógł chcieć popełnić czyn?
- Kto uzyskał lub mógł uzyskać jakąkolwiek korzyść ze zdarzenia?
- Kto obiektywnie mógł w danym czasie i miejscu popełnić czyn?
- Jaką osobowość mógł mieć sprawca czynu?

Kryminalistyka spełnia też funkcję dowodową, gdyż ma na celu udowodnienie sprawcy popełnienia przezeń → czynu zabronionego [t. 1].

Jest to możliwe poprzez zgromadzenie odpowiedniego materiału dowodowego uzasadniającego fakt popełnienia przestępstwa, jego okoliczności, sposób działania i motywację sprawcy oraz danych dotyczących sprawcy. Funkcja zapobiegawcza kryminalistyki zmierza do wypracowania metod i narzędzi uniemożliwiających lub utrudniających popełnienie przestępstwa. Ta funkcja może być realizowana poprzez różne praktyczne formy działania: rozmowę ostrzegawczą z potencjalnym sprawcą, prowadzenie obserwacji miejsc szczególnie zagrożonych, udzielanie porad co do form zabezpieczenia, sprawdzanie prawidłowości stosowanych zabezpieczeń, ochronę fizyczną i techniczną, wzmożone patrole policyjne, profilaktykę kryminalną, projektowanie bezpiecznych przestrzeni, społeczne → p r o g r a m y p r o f i l a k t y c z n e [t. 3] (takie jak np. „Bezpieczne Miasto"), zmianę wadliwego prawa czy kontrole stanu trzeźwości kierowców.

Nowoczesną metodą kryminalistyczną jest analiza kryminalna polegająca na konsekwentnym i zorganizowanym wyszukiwaniu i wykazywaniu związków pomiędzy danymi dotyczącymi przestępstwa a innymi możliwymi do wyróżnienia informacjami, które będą stanowiły podstawę do przygotowania wniosków wspomagających procesy decyzyjne organów ścigania. W kryminalistyce dużą uwagę poświęca się badaniu *modus operandi* będącego charakterystycznym i z reguły powtarzalnym sposobem zachowania sprawcy, który stanowiąc odbicie jego indywidualnych cech, właściwości i możliwości, wyraża się swoiście w czynie przestępczym i następstwach czynu. Manifestuje się w śladach, niekiedy także w zachowaniach poprzedzających czyn lub następujących po nim i pozwala na wstępną identyfikację grupową sprawcy, wersyjne typowanie sprawcy poprzez uformowanie kryterium łączenia kilku różnych czynów jako działania jednego sprawcy.

Nowoczesną metodą kryminalistyczną jest również profilowanie polegające na opracowanie krótkiej, dynamicznej charakterystyki sprawcy i przejawów jego zachowań. Powstaje portret psychologiczny sprawcy, na podstawie którego odbywa się wstępne, grupowe typowanie sprawcy. Profilowanie opiera się na racjonalnym, logicznym wnioskowaniu o cechach sprawcy przestępstwa i ma charakter pomocniczy.

Najważniejszym procesem badawczym w kryminalistyce jest analiza porównawcza. Jest to wyszukiwanie cech grupowych i indywidualnych

w materiale dowodowym, wyszukiwanie cech grupowych i indywidualnych w materiale porównawczym lub innym materiale dowodowym, porównywanie cech identyfikacyjnych obu materiałów. Porównywane są materiał dowodowy z materiałem wzorcowym, materiał dowodowy z materiałem porównawczym, ewentualnie z drugim materiałem dowodowym. Materiał porównawczy do badań jest uzyskiwany w drodze tzw. pobierania. Pobieranie indywidualne polega na uzyskiwaniu materiału porównawczego od jednej, konkretnej osoby. Materiał porównawczy może być pobierany od osób: podejrzanych, oskarżonych, stwarzających bezpośrednie zagrożenie dla życia lub zdrowia, do badań eliminacyjnych (wyeliminowanie śladów nieistotnych), nieletnich, cudzoziemców (nielegalne przekroczenie granicy). Można go również pobierać z nieznanych zwłok ludzkich i do tzw. trałowania, czyli pobierania masowego, od wielu osób, także niezwiązanych ze zdarzeniem, które są wyróżnione na podstawie kryteriów charakteryzujących domniemanego sprawcę zdarzenia, takich jak np. wiek, płeć, miejsce zamieszkania, w celu wykrycia tego sprawcy.

W kryminalistyce wyróżnia się identyfikację grupową pozwalającą na przypisanie śladu przedmiotu lub osoby do określonej kategorii bądź grupy oraz identyfikację indywidualną, gdy przedmiot lub osoba posiada cechę lub cechy tak charakterystyczne, że są one właściwe tylko dla niego i umożliwiają wyróżnienie go z grupy i nadanie mu desygnatu jednostkowego.

Podstawowymi metodami identyfikacyjnymi w kryminalistyce są: daktyloskopia, antropologia sądowa, badanie śladów biologicznych i analiza DNA, toksykologia sądowa, fizykochemia kryminalistyczna, mechanoskopia, badanie broni palnej i amunicji, badanie dokumentów i pisma ręcznego, fonoskopia, traseologia, osmologia, badanie reakcji psychofizjologicznych. Stosowane są również metody niekonwencjonalne, takie jak hipnoza, narkoanaliza, jasnowidztwo czy radiestezja.

Kryminalistyka jest więc nauką bardzo praktyczną, stosowaną (aplikacyjną), lecz nie stanowi wyłącznie uogólnienia praktyki śledczej, gdyż to hamowałoby jej rozwój. Jest teoretyczną bazą praktycznej działalności organów ścigania i musi adaptować zakres swoich dociekań do zakresu działania i potrzeb praktyki organów ścigania. Ważną jej funkcją jest także

wypracowywanie strategii przewidywania i przyszłego rozpoznawania i zwalczania zjawisk przestępczych i innych niekorzystnych społecznie, choć relewantnych prawnie zachowań. To nauka, która stale i dynamicznie się rozwija, dostosowując się do szybko zmieniającego się otoczenia przy wykorzystywaniu najnowszych zdobyczy także innych nauk.

Andrzej Czop

A. Czop, *Kryminalistyka*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Łośgraf, Warszawa 2011; T. Hanausek, *Kryminalistyka. Zarys wykładu*, Zakamycze, Kraków 1997; B. Hołyst, *Kryminalistyka,* Lexis Nexis, Warszawa 2010; tenże, *Wiktymologia,* Wydawnictwo Prawnicze PWN, Warszawa 2000; J. Kasprzak i in., *Kryminalistyka*, Difin, Warszawa 2006; J. Kasprzak, B. Młodziejowski, W. Kasprzak, *Kryminalistyka. Zarys systemu*, Difin, Warszawa 2015; *Kryminalistyka*, J. Widacki (red.), Wydawnictwo C.H.Beck, Warszawa 2018; *Kryminalistyka. Wybrane zagadnienia techniki*, G. Kędzierska, W. Kędzierski (red.), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2011; E. Skuza, M. Goc, J. Moszczyński, *Kryminalistyka czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.

KRYMINALISTYKA MEDIÓW CYFROWYCH (ang. Digital Visual Media Forensics, DVMF) – opiera się na szeregu badań naukowych, które wspierają procesy weryfikacji autentyczności i integralności obrazu cyfrowego i wideo. Ich podstawowym celem jest zachowanie danej treści w najbardziej oryginalnej formie, a jednocześnie prowadzenie ustrukturyzowanego badania, które umożliwia walidację i interpretację → i n f o r m a c j i, które przekazuje. → K r y m i n a l i s t y k a mediów cyfrowych służy zbieraniu dowodów, ich udoskonalaniu i uwiarygodnieniu, służy do analizy materiału dowodowego w postaci zapisu dźwięku i obrazu na potrzeby postępowań w sprawach cywilnych i karnych, m.in. w celu ustalenia autentyczności dowodów. Ich znaczenie wynika z faktu, że udokumentowane reprezentacje rzeczywistości, fotografie i filmy ułatwiają analizę przeszłego zdarzenia, stanowiąc istotne dowody sądowe, od których coraz częściej zależą doniosłe decyzje podejmowane w polityce, → w y w i a d z i e [t. 4], dochodzeniach, procesach sądowych oraz decyzjach dziennikarzy

oceniających autentyczność pozyskanych informacji. Zdjęcia i filmy są szczególnie ważne, ponieważ dostarczają wizualnego dowodu na wystąpienie prawdziwego wydarzenia, stanowiąc autorytet dla naszej percepcji, który przewyższa jedynie przeżycie samego wydarzenia w rzeczywistości. W świecie, w którym dowody wizualne mają takie znaczenie, konieczne jest posiadanie względnej pewności co do ich integralności i wiarygodności, zanim zostaną one zaakceptowane jako dokładne odzwierciedlenie rzeczywistości.

Analiza kryminalistyczna cyfrowej fotografii lub filmu rozpoczyna się od zebrania dowodów z nośnika pamięci takiego jak dysk optyczny, dysk flash, magnetyczny dysk twardy lub z urządzenia źródłowego, którym może być kamera monitorująca, kamera policyjna na desce rozdzielczej, kamera na ciele, osobista kamera wideo, aparat lub telefon komórkowy. W przypadku uszkodzenia nośnika lub urządzenia źródłowego dowody mogą wymagać prawidłowego odzyskania lub naprawy, aby zapewnić zachowanie ich integralności. Głównymi przyczynami, które powodują uszkodzenie nośnika pamięci lub urządzenia źródłowego, są upał, niewłaściwe użycie, warunki środowiskowe panujące w czasie rejestracji lub celowy sabotaż dokonany przez sprawcę. Powodzenie w odzyskiwaniu lub naprawie dowodów zależy od dokładnych okoliczności i stopnia uszkodzenia nośników danych lub urządzenia.

Udoskonalanie dowodów jest prawdopodobnie jednym z najczęściej wykonywanych zadań podczas analizy kryminalistycznej. Rzadko bywa, że zdjęcia lub nagrania wideo wydarzenia są dostępne w wysokiej jakości. Istotne staje się poprawienie ich jakości, aby szczegóły stały się wyraźne, a wydarzenia pokazane na zdjęciu lub filmie bardziej oczywiste dla śledczych, adwokatów czy sędziów. Najczęściej stosowane techniki ulepszania treści, które są dozwolone przez sąd, obejmują regulację kontrastu i jasności, korektę koloru, redukcję szumów, ostrego oświetlenia, wyostrzanie, stabilizację wideo, regulację szybkości klatek, maskowanie lub rozmazywanie twarzy, powiększanie, kadrowanie, rekonstrukcję obrazu w celu przeciwdziałania efektowi rozmycia ruchu i umieszczanie podtytułu oraz kodowania czasowego.

Operacje ulepszania treści są wykonywane przy użyciu nieniszczących technik, które zapewniają, że integralność danej treści jest zachowana

przez cały czas. Na zakres osiągalnego udoskonalenia mają wpływ czynniki takie jak początkowa jakość zdjęcia lub wideo, parametry techniczne urządzenia nagrywającego, warunki środowiskowe w czasie nagrywania oraz stopień kompresji.

Dowody wizualne są trudne do zakwestionowania, a twierdzenia, które z nich wynikają, niełatwo jest obalić, dlatego ilekroć jakiekolwiek dowody tego typu są wykorzystywane jako środek przekazywania ważnych informacji, kluczowe jest ustalenie wiarygodności dowodów. Zadania te realizuje się poprzez znalezienie odpowiedzi na pytania, skąd pochodzi zdjęcie lub film oraz czy zdjęcie lub film zostały przetworzone po ich wykonaniu. Pierwsze pytanie odnosi się do pochodzenia dowodu, podczas gdy drugie odnosi się do uwiarygodnienia jego treści. Każda operacja, która jest stosowana w odniesieniu do fotografii cyfrowej lub wideo i która w jakiś sposób zmienia zapis, pozostawia subtelne ślady. Są one ogólnie określane jako artefakty kryminalistyczne, mają one unikalny charakter dla każdej operacji przetwarzania treści. Identyfikujące ślady umożliwiają zarówno potwierdzenie pochodzenia, jak i uwierzytelnienie treści.

Postępowanie mające na celu ustalenie pochodzenia dowodu odnosi się do procesu stwierdzenia, czy zdjęcie lub film wideo zostały zarejestrowane przy użyciu urządzenia, o którym twierdzono, że je zarejestrowało, i czy nie zostały one przeniesione w nieautoryzowany sposób z jednego nośnika na inny, z wyjątkiem tych działań, których śledczy i analitycy sądowi byli świadomi. Proces kryminalistyczny, który łączy daną zawartość z określonym urządzeniem akwizycji, jest znany jako identyfikacja aparatu źródłowego (ang. *source camera identification*, SCI).

Ślady identyfikacyjne wykorzystywane przez różne techniki SCI są dostarczane przez sam proces generowania treści. Każdy składnik procesu generowania obrazu i wideo wpływa w unikalny sposób na cechy wynikowe treści, co oznacza np., że wideo przechwycone przez kamerę CCTV będzie wykazywać cechy inne niż rejestrowane przez ręczną kamerę, a także cechy filmów nagranych przez różne rodzaje kamer CCTV będą odmienne.

Różnice w sposobie, w jaki określony proces generowania obrazu lub wideo wpływa na charakterystykę zawartości, wynikają z obecności określonych elementów w urządzeniu rejestrującym oraz z powodu różnic

w ich sposobie wpływania na ostateczną treść. Dokładne zbadanie tych zmian pomaga wnioskować o szczegółach dotyczących danego urządzenia i procesu generowania treści, umożliwiając w ten sposób ustalenie pochodzenia dowodów. Przykładem takich zmian jest szum czujnika, który jest unikalnym rodzajem szumu, który kamera wprowadza w każdym zapisywanym obrazie lub wideo. Wzorce szumów czujnika różnią się w zależności od kamery, ale pozostają spójne dla całej zawartości nagranej przez konkretną kamerę.

Ponadto, ponieważ działanie różnych komponentów procesu generowania treści jest od siebie zależne, każdy komponent może zakłócać lub nawet usuwać ślady wprowadzone przez poprzedni komponent, co oznacza, że cechy wcześniejszego etapu mogą nie być obecne w ostatecznej treści. Analityk kryminalistyczny może ocenić pochodzenie danej treści nie tylko na podstawie obecności identyfikujących śladów, ale także na podstawie nieobecności oczekiwanych śladów.

Po ustaleniu pochodzenia obrazu lub wideo następnym krokiem jest sprawdzenie jego zawartości i upewnienie się, że nie zostały one naruszone od momentu zarejestrowania treści do chwili jej przedstawienia do uwiarygodnienia. Techniki kryminalistyczne, które pomagają wykryć obecność manipulacji semantycznych w obrazach cyfrowych i filmach, są wspólnie określane jako techniki wykrywania sabotażu lub fałszerstwa.

Każda operacja, która zostaje zastosowana w stosunku do obrazu cyfrowego lub wideo po jego wygenerowaniu, jest uważana za operację poprodukcyjną. Wszystkie takie operacje wpływają na charakterystykę treści cyfrowych i zmieniają jej istniejącą konfigurację, sprawiając, że atrybuty obrazu lub filmu, którego dotyczy takie działanie, wykazują cechy odbiegające od normalnego zachowania wyświetlanego przez atrybuty niezmodyfikowanego obrazu lub wideo. Te odchylenia i nietypowe zachowania są uważane za ślady identyfikujące, których ujawnienie umożliwiają techniki wykrywania manipulacji służące odróżnianiu autentycznej treści od treści zmodyfikowanej w procesie poprodukcyjnym.

Istotne z kryminalistycznego punktu widzenia pozostają różnice między ulepszaniem treści a modyfikowaniem zawartości. Chociaż głównym celem ulepszania treści jest poprawa jakości obrazu lub wideo i podkreślenie ważnych szczegółów sceny tak, aby ułatwić ich zrozumienie, sabotaż

jest szkodliwą operacją, która zmienia zdarzenia przedstawione na obrazie lub wideo i jego znaczenie, przez to czyniąc go szkodliwym dla celów podejmowania decyzji na jego podstawie. Typowe operacje manipulowania treścią obejmują fałszerstwa kopiowania i wklejania, w których dany obiekt jest wstawiany lub usuwany z obrazu lub klatki wideo, oraz fałszerstwa związane z klatkami, w których zestaw klatek jest usuwany z sekwencji wideo lub układ klatek jest zmieniany.

W zależności od cech charakterystycznych dla określonego scenariusza kryminalistycznego DVMF można podzielić na kryminalistykę aktywną i pasywną. W kryminalistyce aktywnej ślady identyfikujące są dołączane do treści w formie metadanych, takich jak *hash* (funkcja haszująca) lub podpis, albo są wstawiane bezpośrednio do treści tak jak znak wodny, na wczesnym etapie tworzenia treści. Aktywne metody kryminalistyczne są implementowane bezpośrednio w urządzeniu do pozyskiwania, a proces generowania treści nie może się rozpocząć, dopóki ślady identyfikujące nie zostaną wstawione do treści. Oznacza to, że aktywne metody kryminalistyczne nie pozwalają na ocenę wiarygodności dowolnych zdjęć i filmów nieznanego pochodzenia. W kryminalistyce biernej analityk nie ma kontroli nad procesem tworzenia obrazu lub wideo, typem i wyglądem śladów identyfikujących. Analityk jest również nieświadomy specyfiki procesu generowania treści i jego historii przetwarzania i ogranicza się do uwiarygodnienia treści poprzez sprawdzanie widocznych cech. Pasywne metody kryminalistyczne opierają się na 2 rodzajach śladów identyfikujących: właściwościach urządzenia i artefaktach przetwarzania.

Charakterystyka urządzenia odnosi się do wewnętrznych cech różnych urządzeń, które mogą występować np. dlatego, że producenci aparatów wykorzystują różne komponenty w swoich urządzeniach lub z powodu dostosowywania ustawień parametrów ich urządzeń na różne sposoby. Zmiany mogą również wystąpić z powodu niepożądanych niedoskonałości technologicznych takich jak wady czujnika. W związku z tym każde urządzenie pozostawia unikalne identyfikujące ślady na generowanych przez siebie treściach, a badając te ślady, można wysunąć wnioski na temat samego urządzenia.

Artefakty przetwarzania odnoszą się do tych śladów, które są wprowadzane przez różne operacje przetwarzania, które przechodzi obraz lub

wideo po jego wygenerowaniu. Takie artefakty są unikalne dla każdej operacji przetwarzania, a zatem służą jako ślady identyfikujące do rozpoznania konkretnej operacji.

Zarówno aktywne, jak i pasywne badania sądowe opierają się na wykrywaniu śladów identyfikujących, w przypadku aktywnych badań kryminalistycznych ślady te są osadzone lub dołączone są do danych celowo, a w przypadku pasywnych badań kryminalistycznych ślady te są wykrywane na podstawie analizy cech procesu pozyskiwania treści lub operacji poprodukcyjnych, którym materiał został poddany.

DVMF bywa określana jako ślepa, jeśli analityk pracuje bez kompletnej wiedzy *a priori* dotyczącej urządzenia nagrywającego, procesu generowania treści, oryginalnej sceny uchwyconej przez obraz lub wideo czy jakiejkolwiek operacji przetwarzania, która mogła zostać do niego zastosowana. Ślepe schematy kryminalistyczne badają identyfikujące ślady obecne w danej treści i próbują wywnioskować tożsamość urządzenia, które mogło zostać użyte do jego przechwycenia lub operacji poprodukcyjnych, którym mógł zostać poddany. W przeciwieństwie do ślepej kryminalistyki, nieślepe metody kryminalistyczne wykorzystują dodatkowe informacje o cechach generowania i przetwarzania treści. Mogą to być wiedza o tożsamości urządzenia rejestrującego lub informacje dotyczące historii przetwarzania treści. Chociaż nieślepe podejścia pomagają złagodzić niektóre z niepewności, z jakimi może się spotkać analityk w odniesieniu do tego, czy obraz lub wideo przeszło jakiekolwiek przetwarzanie poprodukcyjne, są one często niewykonalne w praktycznych sytuacjach. Np. nieślepe podejście nie może pomóc w określeniu pochodzenia obrazu lub wideo nieznanego pochodzenia, ponieważ dla takiego obrazu czy wideo nie ma żadnych dodatkowych informacji poza samą jego treścią.

Ostatnim ważnym zadaniem DVMF jest badanie elementów sceny przedstawionych na obrazie lub wideo, aby zidentyfikować zawarte w nim obiekty i zinterpretować ich znaczenie w odniesieniu do sceny. Podczas tej fazy analizy kryminalistycznej wykonywane są operacje takie jak wykrywanie obiektów, śledzenie i podświetlanie.

Po wstępnym wykryciu obiektu wykonuje się specjalistyczne badania, które są przeprowadzane w celu dokonania identyfikacji osób (ofiar, świadków lub podejrzanych) lub przedmiotów nieożywionych (plakietek,

tablic rejestracyjnych, nazw ulic i budynków, numerów domów itp.) przedstawionych na obrazie lub wideo. Typowymi technikami identyfikacji obiektów są mapowanie twarzy (tj. porównywanie jednego obrazu twarzy z innymi obrazami twarzy), gramatyka wideo (która jest przydatna do wykonywania pomiarów obiektów, np. w celu oszacowania wysokości sprawcy), identyfikacja innych charakterystycznych cech, takich jak blizny i tatuaże, oraz subiektywne metody kontroli, takie jak analiza kryminalistyczna chodu i analiza wzorca behawioralnego.

Dokładna interpretacja znaczenia danego dowodu ma kluczowy charakter. Podczas procesu dowody wizualne są często pozostawione, aby mówiły same za siebie, ponieważ oczekuje się, że dostarczą sądowi wiedzy o wszystkich faktach. Ta tendencja nie wyklucza jednak błędnej interpretacji dowodów. Wartościowy jest tu przykład z października 2003 r. z Florydy, gdzie niania C. Muro została oskarżona przez swoich pracodawców o znęcanie się nad dziećmi. W trakcie procesu jako dowód wykorzystano film z ukrytej kamery, który pokazał, że Muro gwałtownie potrząsa pięcioletnią córką. Uznano dowód za wystarczający, a Muro została skazana. W marcu 2006 r. sprawa została ponownie rozpatrzona, a materiał wideo został poddany analizie kryminalistycznej, która ujawniła, że dowody były w rzeczywistości mylące. Kamera nagrywała ok. 5,5 klatki na sekundę, co powodowało, że delikatne ruchy wydawały się gwałtowne, gdy wideo było odtwarzane z normalną częstotliwością klatek. To odkrycie uniewinniło Muro, która – mimo że była niewinna – spędziła 29 miesięcy w więzieniu. Przykład ten dowodzi roli, jaką odgrywa interpretacja dowodów fotograficznych i wideo, oraz tego, jak nawet najmniejsze błędy mogą prowadzić do pomyłki sądowej.

Jakub Idzik, Rafał Klepka

B. Dalrymple, J. Smith, *Forensic Digital Image Processing Optimization of Impression Evidence*, CRC Press, London–New York 2018; *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, E. Casey (ed.), Elsevier, Amsterdam–Boston–Heidelberg 2004; *Handbook of Digital and Multimedia Forensic Evidence*, J.J. Barbara (ed.), Humana Press, Totowa 2008; J. Idzik, R. Klepka, *Kryminalistyka mediów cyfrowych*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron,

Kraków 2019; K. Mancini, J. Sidoriak, *Fundamentals of Forensic Photography: Practical Techniques for Evidence Documentation on Location and in the Laboratory*, Routledge, London–New York 2018; R.D. Singh, *The Art and Science of Digital Visual Media Forensics*, „HSOA Journal of Forensic, Legal & Investigative Sciences" 2018, vol. 4, no. 1; taż, *Digital Visual Media Forensics*, [w:] *Cryptographic and Information Security Approaches for Images and Videos*, S. Ramakrishnan (ed.), CRC Press, Boca Raton–London–New York 2019.

KRYMINOLOGIA – nauka społeczna, której obszarem zainteresowań jest przestępstwo i przestępca, a także etiologia i przejawy → przestępczości [t. 3] i zjawisk → patologii społecznej [t. 3] z uwzględnieniem roli ofiary w zdarzeniach przestępczych, jak również profilaktyka kryminalna oraz prawidłowość działania systemu karnego.

Tak sformułowana definicja wytycza zadania kryminologii, spośród których najważniejsze to:

- poznanie przyczyn przestępczości i patologii społecznej,
- dostarczenie narzędzi do opisu tych zjawisk,
- poznanie przestępcy oraz procesów kryminalizacji,
- badanie funkcjonowania różnych dziedzin wymiaru sprawiedliwości,
- tworzenie wiedzy o sposobach zapobiegania przestępczości.

Kryminologia jest nauką interdyscyplinarną, multidyscyplinarną i wieloaspektową. Pojęciem tym po raz pierwszy posłużył się w 1879 r. P. Topinard, francuski antropolog zajmujący się biologią kryminalną. Nauką pomocniczą ważną w badaniach kryminologicznych jest psychologia, która pozwala na ustalenie właściwości psychicznych sprawcy → czynu zabronionego [t. 1], odtworzenie mechanizmów zachowania przestępczego oraz określenie wpływu czynników o charakterze psychicznym na sposób działania sprawcy. Psychologia daje również możliwość korygowania zachowań aspołecznych i ma walor naprawczy. Odgrywa również istotną rolę przy diagnozowaniu motywacji sprawcy i dostosowywaniu do jego charakteru odpowiednich środków karnych i kary. Z kolei pedagogika zajmuje się analizą możliwości skutecznego wpływania na zachowania człowieka i określa rolę wychowania w genezie zachowań przestępczych, badając uwarunkowania procesu socjalizacji i kontrsocjalizacji.

Daje możliwość wykorzystania nauczania jako środka oddziaływania w procesie resocjalizacji. Pedagogika resocjalizacyjna bada resocjalizacyjny cel kary pozbawienia wolności, wskazując, jak należy pracować ze skazanym, by go poprawić i zmotywować do prospołecznych zachowań.

Ważną gałęzią wiedzy jest dla kryminologii socjologia, zwłaszcza w aspekcie poszukiwania przyczyn przestępstw i przestępczości w środowisku społecznym, takim jak: struktury I stopnia (rodzina i grupa rówieśnicza), struktury II stopnia (sąsiedztwo, grupa lokalna), społeczeństwo globalne (państwo, struktura władzy). Socjologia bada też wpływ podkultur dewiacyjnych na przestępczość oraz analizuje zjawiska patologii społecznej, ze zwróceniem uwagi na dezorganizację życia rodzinnego, kryminogenny wpływ środowiska pozarodzinnego, negatywny wpływ mediów, ujemne skutki migracji, bezrobocie, alkoholizm czy narkomanię. Przedmiotem jej zainteresowań są społeczne mechanizmy kontroli przestępczości oraz sposób postrzegania w społeczeństwie zjawiska przestępczości. Pomocniczość psychiatrii sprowadza się do udzielenia odpowiedzi na ważne w procesie karnym pytania:

- Czy i na ile istnieje związek pomiędzy zaburzeniami psychicznymi a przestępstwem?
- Czy przestępca jest człowiekiem chorym psychicznie i czy w związku z tym może odpowiadać karnie?

To psychiatrzy zajmują się diagnozowaniem sprawcy przestępstwa. Medycyna sądowa wspierająca kryminologię bada mechanizm działania różnych urazów na organizm człowieka oraz zajmuje się problemem śmierci i zmian zachodzących w ciele po zgonie oraz ustalaniem przyczyn, rodzaju i czasu śmierci. Medycy sądowi badają też osoby żywe (pokrzywdzonych lub poszkodowanych) oraz dowody rzeczowe. Zajmują się problemem dziedziczenia układów grupowych krwi, oceną zdolności danej osoby do zapłodnienia, wyjaśniają wpływ alkoholu etylowego na organizm oraz badają stężenie tego alkoholu we krwi. W ramach badań toksykologicznych określają własności czynników toksycznych i ich negatywny wpływ na organizm człowieka.

Kryminologia korzysta z dorobku pokrewnej jej nauki, jaką jest →kryminalistyka zajmująca się taktycznymi zasadami i sposobami oraz technicznymi metodami i środkami rozpoznawania i wykrywania

prawnie określonych ujemnych zjawisk społecznych, w tym przestępstw i ich sprawców. Wspólnym przedmiotem zainteresowań tych nauk jest osoba ofiary przestępstwa. W kryminologii ważne jest posługiwanie się statystykami, które są źródłem → i n f o r m a c j i o rozmiarach, nasileniu, dynamice i strukturze przestępczości. Wśród nich są statystyki: policyjna, prokuratorska, sądowa i penitencjarna. Wyniki badań opracowuje się metodami statystycznymi, co pozwala na prognozowanie rozmiarów i rozwoju przestępczości. Powstał osobny dział – statystyka kryminalna – zajmująca się statystyką przestępczości oraz sposobami ich interpretacji. Z dorobku nauk ekonomicznych kryminologia korzysta przy określaniu rozmiarów: strat spowodowanych przestępczością, zysków z działalności przestępczej, nakładów finansowych potrzebnych na przeciwdziałanie przestępczości oraz wpływu → k r y z y s ó w ekonomicznych na przestępczość.

Dla wytłumaczenia przyczyn przestępczości kryminologia sformułowała szereg teorii, wśród których ważną rolę odegrały teorie biologiczne. Pierwszą z nich stworzył w ramach włoskiej szkoły pozytywnej C. Lombroso, który przyjął założenie deterministycznego pojmowania zachowań człowieka. W swoim dziele *Człowiek zbrodniarz w stosunku do antropologii, jurysprudencji i dyscypliny więziennej* wskazał, że przestępstwo jest warunkowane dziedzicznie. Uznał, że istnieje typ tzw. urodzonego przestępcy, którym jest jednostka wykazująca cechy atawistyczne, popychające ją do przestępstwa. Przestępca wg Lombroso stanowi odrębny typ człowieka – *homo delinquens* – który znajduje się na niższym poziomie ewolucyjnego rozwoju. Wykazuje on specyficzne cechy anatomiczne, takie jak odstające uszy, wystające kości policzkowe, rzadki zarost, asymetria czaszki, prognatyzm (wysunięcie szczęki do przodu), niewielka kość czołowa, silnie rozwinięte łuki nad brwiami, silnie rozwinięta dolna szczęka. Lombroso wskazywał, że przestępcy mają defekty psychiki, większą od przeciętnej sprawność zmysłów, brak wyrzutów sumienia. Cechuje ich cynizm, impulsywność, posługiwanie się gwarą. Z. Freud stworzył teorię psychoanalityczną, wg której człowiek jest wyposażony energetycznie w instynkt życia i miłości oraz instynkt śmierci. Ten ostatni stanowi podłoże agresywnych zachowań, musi zostać rozładowany, aby nie doszło do destrukcji organizmu. Rozładowanie może nastąpić poprzez sublimację pozytywną, taką jak twórczość, lub negatywną, którą jest agresja.

Trzy sfery psychiki człowieka: id – strefa instynktownych czynności (podświadomość), ego – uświadomiona osobowość, superego – sumienie (normy wytworzone w procesie socjalizacji). Id i superego pozostają wobec siebie w konflikcie. To z kolei rodzi poczucie winy i lęku, czego przejawem są zachowania substytucyjne, które mają go rozładować. Może to być zachowanie przestępcze, którego istotą nie jest samo wyrządzenie zła, ale podświadome dążenie do ukarania. To działanie ma zdaniem Freuda charakter kompensacyjny, w konsekwencji ma prowadzić do rozładowania istniejących kompleksów.

Poszukiwaniem wyjaśnienia zachowań dewiacyjnych bezpośrednio w strukturze społecznej zajęli się przedstawiciele teorii socjologicznych, z których najważniejszym był twórca tzw. anomii społecznej R.K. Merton. Według niego anomia jest stanem załamania, którego istotą jest silna rozbieżność pomiędzy normami i celami kulturowymi a możliwościami działania członków grupy zgodnie z tymi normami. Wyróżnił 5 typów przystosowania się jednostek do takiej sytuacji: konformizm, czyli akceptację zarówno celów kulturowych, jak też zinstytucjonalizowanych środków służących do jego realizacji; innowację, czyli zachowanie, w którym przy dążeniu do osiągnięcia celów kulturowych wykorzystuje się środki niezinstytucjonalizowane (zabronione, nieetyczne); rytualizm, który odrzuca cele kulturowe przy jednoczesnym zaakceptowaniu zinstytucjonalizowanych środków; wycofanie, rozumiane jako odrzucenie przez jednostkę zarówno kulturowych celów, jak i zinstytucjonalizowanych środków (norm postępowania), i bunt, który odrzuca zarówno cele kulturowe, jak i zinstytucjonalizowane środki przy jednoczesnym dążeniu do zastępowania ich nowym. To organizowanie nowej struktury poprzez zakwestionowanie tego, co stare.

A.K. Cohen ze szkoły chicagowskiej zajął się badaniem związku podkultury przestępczej z gangami młodzieżowymi warstw niższych. Wykazał, że braki w wychowaniu powodują niemożność skutecznego powstrzymywania się od zachowań agresywnych. Trudności w szkole i brak szacunku dla cudzej własności powodują, że młodzi ludzie nie wierzą w sukces poprzez pracę i edukację. Poczucie zablokowanych możliwości społecznego awansu przy rozbudzonych aspiracjach i potrzebie sukcesu rodzą frustrację, stany lękowe i niską samoocenę. Mogą one zostać zredukowane

poprzez reakcję pozorowaną, czyli odwrócenie wartości klas średnich i realizacji tego, co stanowi ich przeciwieństwo. Najlepszym środkiem realizacji celów staje się gang, w którym promowane są hedonizm, bezcelowość, negatywizm, nieużyteczność, złośliwość. W gangu występuje silne poczucie odrębności oraz solidarności grupy dewiacyjnej, amplifikowane przez wrogie reakcje ze strony instytucji formalnej kontroli społecznej.

Kryminologia zajmuje się też badaniami tzw. ciemnej liczby przestępstw (ang. *dark number*) w celu określenia rozmiarów przestępczości nieujawnionej. To liczba przestępstw niezgłoszonych i niezarejestrowanych przez organy ścigania. Podaje się ją w postaci pewnej relacji lub odsetka. Informacje o liczbie przestępstw rzeczywiście popełnionych zdobywane są z różnych źródeł i różnymi metodami. Są to to eksperyment, obserwacja uczestnicząca i → w y w i a d [t. 4]. Badania kryminologiczne wskazują, że Polska jest krajem o niskiej gotowości obywateli do zgłaszania o fakcie wiktymizacji. Największa ciemna liczba dotyczy przestępstw seksualnych, kradzieży własności osobistej i pobić, a najmniejsza występuje w kategorii kradzieży pojazdów i włamań. Według kryminologów → p o l i c j a [t. 3] nie wie o prawie 70% popełnianych na terenie Polski przestępstw.

Ważnym przedmiotem badań kryminologicznych jest kryminogeneza, czyli proces odbywający się w ludzkiej psychice, którego finałem jest popełnienie czynu zabronionego. Punktem centralnym zainteresowań kryminogenezy jest decyzja sprawcy czynu. Wymagane jest tu podejście syndromatyczne uwzględniające całokształt okoliczności istotnych dla jej podjęcia w ujęciu strukturalnym i dynamicznym. Kryminolodzy ustalają, jakie czynniki kryminogenne występowały, i pokazują je w historycznej sekwencji, wskazując kierunki tych uwarunkowań. Momentami kluczowymi kryminogenezy są więc zdarzenia zapoczątkowujące zainteresowanie przestępstwem lub utwierdzające sprawcę w słuszności jego decyzji, funkcjonujące na zasadzie wzmocnień. Finalnie ustalenia kryminogenezy wskazują czynniki prowadzące do przestępstwa, co pozwala na budowę odpowiedniej profilaktyki, oraz ułatwiają postępowanie ze sprawcą, określając najbardziej skuteczne środki indywidualnego oddziaływania, co ma duże znaczenie w przypadku wymiaru kary. To jest warunkiem spełnienia przezeń zakładanych celów naprawczych. Stosunkowo nową

dziedziną kryminologii jest wiktymologia, która zajmuje się badaniem roli ofiary w genezie przestępstwa, w aspekcie jej wpływu na powzięcie zamiaru przestępczego i jego realizację. Wiktymologia formułuje wnioski dotyczące → z a g r o ż e ń [t. 4] poszczególnych kategorii demograficznych i służy tworzeniu aktywnej polityki antywiktymizacyjnej.

Współczesna wiktymologia wykształciła orientację naukową, która bada zjawiska wiktymizacji, tworząc typologię ofiar i praktyczną mającą pomagać ofiarom przestępstwa w zakresie prawnym, medycznym, psychologicznym, terapeutycznym i materialnym. Jej celem jest redukowanie negatywnych skutków przestępstwa, a także zapobieganie wtórnej wiktymizacji. Badania wiktymizacyjne są alternatywą dla statystyk kryminalnych, gdyż pozwalają określić tzw. ciemną liczbę. Narzędziem są tu sondażowe badania ankietowe prowadzone w stosunku do sprawców i ofiar. Wyniki tych badań stanowią ważne, komplementarne źródło informacji o przestępczości. Kryminologia bada również poczucie → b e z p i e c z e ń s t w a [t. 1] rozumiane jako odzwierciedlony w świadomości stan bezpieczeństwa, który zakłada istnienie obok komponentu intelektualnego także komponentu o charakterze emocjonalnym. Poczucie bezpieczeństwa jest więc stanem subiektywnym wskazującym na stopień zaspokojenia potrzeby bezpieczeństwa. Według kryminologów na zwiększenie poczucia bezpieczeństwa i redukcję strachu pozytywny wpływ mają organizacja przestrzeni mieszkalnej, która daje możliwość kontroli tych miejsc; stwarzanie możliwości dogodnego zauważania sygnałów zagrożeń; gotowość społeczności do współpracy z agendami formalnej kontroli społecznej; czytelność reguł współpracy z policją; edukacja na rzecz bezpieczeństwa.

Kryminologia jest nauką, która dynamicznie się rozwija, korzystając z zasobów własnych i badań oraz odkryć dokonywanych w obrębie innych nauk.

Andrzej Czop

E. Drzaga, M. Grzyb, *Nowe kierunki w kryminologii*, Wydawnictwo Naukowe Scholar, Warszawa 2019; E. Delegacz-Jurgielewicz, E. Pływaczewski, *Współczesna przestępczość i patologie społeczne z perspektywy interdyscyplinarnych badań kryminologicznych*, C.H.Beck, Warszawa 2017; M. Grzyb, *Przestępstwa motywowane*

kulturowo. Aspekty kryminologiczne i prawnokarne. Reakcja krajów zachodnich na szkodliwe praktyki kulturowe, Wolters Kluwer Polska, Warszawa 2016; B. Hołyst, *Kryminologia*, Wolters Kluwer Polska, Warszawa 2016; tenże, *Wiktymologia*, Wydawnictwo Prawnicze PWN, Warszawa 2000; *Kryminalistyka. Wybrane zagadnienia techniki*, G. Kędzierska, W. Kędzierski (red.), Wydawnictwo WSPol w Szczytnie, Szczytno 2011; M. Kuć, *Kryminologia*, C.H.Beck, Warszawa 2015.

KRYZYS – pojęcie stosowane w →naukach o bezpieczeństwie [t. 3]; można o nim mówić w sytuacji, gdy zanika wyraźna granica rozdzielająca stan bezwzględnego →bezpieczeństwa [t. 1] i jego braku, co jednoznacznie wskazuje na jego znaczenie pojęciowe postrzegane za stan przejściowy, a nie docelowy. Z kryzysem jest związany stan i proces →zagrożenia [t. 4]. Nie można mówić o kryzysie, jeżeli nie zidentyfikuje się zagrożeń, które do jego powstania doprowadzają. Stąd zagrożenia i kryzys są nierozłączne i wzajemnie siebie definiują poprzez swoje specyficzne cechy. Jest to pojęcie wieloznaczne, używane w wielu obszarach, takich jak politologia, nauki wojskowe, nauki o organizacji i zarządzaniu, ekonomia czy nauki medyczne. Termin pochodzi od stgr. κρίσις, *krisis*, co oznacza punkt zwrotny, przesilenie, moment rozstrzygający, jakościową zmianę układu lub w układzie. W języku potocznym termin używany jest w sytuacjach, które kojarzą się z zagrożeniem. Używa się go, mówiąc o kryzysie politycznym, ekonomicznym, energetycznym, społecznym, środowiska naturalnego czy o kryzysie wartości.

Przyjmuje się, że kryzys jest kulminacyjną fazą narastającej →sytuacji kryzysowej [t. 4], powstającej w wyniku pojawiających się niespodziewanie okoliczności. W fazie tej dominującą rolę odgrywa fakt prawdziwej lub odczuwalnej utraty kontroli nad rozwijającą się sytuacją oraz braku koncepcji jej opanowania. Natomiast sytuacja kryzysowa to zespół okoliczności zewnętrznych i/lub wewnętrznych, w jakich znajduje się dany podmiot, jego część lub określona dziedzina jego działalności, wpływających na jego funkcjonowanie w taki sposób, iż zaczyna się w nim i jest kontynuowany proces zmian, w rezultacie czego dochodzi do zachwiania równowagi i utraty możliwości kontroli nad przebiegiem wydarzeń albo eskalacji zagrożenia jego interesów. Sytuacja kryzysowa może zakłócić wiele dziedzin funkcjonowania państwa, a w rezultacie

społeczeństwa. W wypadku kryzysów zewnętrznych zakłóceniu mogą ulec stosunki dyplomatyczne z innymi państwami, międzynarodowa wymiana handlowa, współpraca technologiczna, naukowa i wiele innych dziedzin, zaś w razie kryzysu o charakterze wewnętrznym zakłócone mogą być działania gospodarcze (inwestycje, rynek, usługi itd.), stosunki społeczne i polityczne, funkcjonowanie systemu oświaty, administracji publicznej i wiele innych dziedzin działalności państwa. W rezultacie to wszystko trzeba odbudować (przywrócić, odtworzyć, reaktywować).

Należy podkreślić, że kryzys jest często mylony i zamiennie stosowany z sytuacją kryzysową i na odwrót. Trzeba zauważyć, że pod pojęciem sytuacji kryzysowych ujmuje się wszelkie okoliczności doprowadzające podmiot działania do konieczności podjęcia rozstrzygnięć dotyczących zaistniałej sytuacji, natomiast kryzys stanowi apogeum nierozwiązanej sytuacji kryzysowej. Analiza tych 2 pojęć pozwala na stwierdzenie, że sytuacja kryzysowa jest zjawiskiem szerszym od kryzysu. Na sytuację kryzysową składa się szereg przyczyn, których wzajemny wpływ na siebie jest różny. Trudno określić, która zmienna decyduje o rozwoju sytuacji w kierunku kryzysu. Z chwilą zidentyfikowania sytuacji kryzysowej i określenia jej charakteru można poprzez właściwe przeciwdziałanie nie dopuścić do jej eskalacji w kryzys. Natomiast z chwilą osiągnięcia apogeum sytuacji kryzysowej wyodrębnia się czytelne zjawisko kryzysu o określonym charakterze i skutkach w stosunku do stanu lub sytuacji standardowej. Wynika z tego, że kryzys jest jedną z faz sytuacji kryzysowej.

W dziedzinie bezpieczeństwa kryzys jest rozmaicie definiowany w powiązaniu z tą dziedziną, naukowym podejściem oraz praktyczną działalnością. W różnych słownikach kryzys jest określany jako:

- sytuacja niekorzystna dla kogoś lub czegoś;
- sytuacja będąca następstwem zagrożenia, prowadząca w konsekwencji do zerwania lub znacznego osłabienia więzów społecznych przy równoczesnym poważnym zakłóceniu funkcjonowania instytucji publicznych, jednak w takim stopniu, że użyte środki niezbędne do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych przewidzianych w Konstytucji RP;

- sytuacja powstała w wyniku załamania się stabilnego dotąd procesu rozwoju, grożąca utratą inicjatywy i koniecznością godzenia się na przyjmowanie niekorzystnych warunków, wymagająca podjęcia zdecydowanych wszechstronnych kroków zaradczych;
- forma (faza) konfliktu, w wyniku którego dochodzi do gwałtownego wzrostu napięcia między stronami, które może doprowadzić do konfliktu zbrojnego.

Powyższe, słownikowe definicje kryzysu wydają się w wysokim stopniu ogólne, ponieważ nawet w potocznym rozumieniu nie każdy przełomowy, decydujący moment nazywa się kryzysem. Zjawisko to uznaje się natomiast za zaburzenie i zachwianie tego, co nazywamy stanem normalnym, stabilnym i przewidywalnym, jak również określa jako sytuacje, w których zagrożone jest życie, mienie i środowisko, co jest istotne w aspekcie → z a r z ą d z a n i a k r y z y s o w e g o [t. 4]. Należy podkreślić, że pojęcie kryzysu nie jest definiowane w polskich aktach prawnych, natomiast w pracach naukowych i publikacjach jest różnie określane przez naukowców oraz praktyków i zawiera zarówno wiele wspólnych, jak i odmiennych treści, w których definiuje się kryzys jako:

- sytuację, w której istnieje zagrożenie dla podstawowych wartości, interesów oraz celów instytucji i grup społecznych lub w której zagrożone są prawa i swobody obywateli, ich życie i mienie przez dłuższy czas i na znacznym obszarze;
- sytuację o charakterze niemilitarnym lub polityczno-militarnym, której skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach, środowisku na znacznych obszarach, bezpieczeństwu obywateli i porządkowi publicznemu oraz bezpieczeństwu i konstytucyjnemu ustrojowi państwa, a zapobieganie im i likwidacja ich skutków jest podejmowana z zastosowaniem zwykłych lub nadzwyczajnych środków, we współdziałaniu różnych organów administracji publicznej i instytucji oraz specjalistycznych służb i formacji, w tym sił zbrojnych, działających pod jednolitym kierownictwem;
- kulminację nagromadzonych zdarzeń, stanów rzeczy (zagrożeń, konfliktów, szans) w dziedzinie życia społecznego, gospodarczego, politycznego i innych dziedzinach działalności państwa (wielu

państw) oraz innych organizacji, będącą krytycznym rezultatem działalności człowieka przeciwko człowiekowi lub prawom natury, a także zjawisk wynikających z działania sił natury lub awarii technicznych, którym przeciwdziałanie przekracza możliwości rutynowych działań.

Interesujące są natowskie poglądy, według których, aby kryzys mógł zaistnieć, powinno zostać spełnionych kilka istotnych wymogów:

- musi stwarzać realne lub wiarygodne zagrożenie,
- musi być odpowiedniej wielkości,
- występuje nagle i jest nieprzewidywalny,
- występuje presja wydarzeń i deficyt czasu, brak pewności co do rozwoju sytuacji oraz pewności w zakresie sposobów, metod i techniki reagowania,
- musi nastąpić eskalacja wydarzeń.

Jednocześnie należy podkreślić, że kryzys jest szczególnym stanem lub procesem, zawsze oznacza przełom między dwiema fazami jakiegoś procesu, może być mniej lub bardziej dotkliwy, mieć różny zakres, czas trwania, ale zawsze kończy dotychczasowy stan rzeczy, jest naruszeniem stanu równowagi, niezakończony na czas powoduje przerwanie cyklu rozwojowego. Kryzys zawsze stanowi swoiste wyzwanie do podjęcia kroków zaradczych w sytuacji, która stanowi naruszenie podstawowych, powszechnie uznawanych za warte ochrony i obrony wartości i interesów danego podmiotu. Do mierzenia skali kryzysu używa się wielkości środków zastosowanych do jego opanowania, gdyż może się okazać, że zastosowane środki zaradcze nie zawsze muszą być wprost proporcjonalne do skali niebezpieczeństwa danej sytuacji. W innym ujęciu za miernik rangi (rozmiaru) kryzysu uważa się poziom zdezorganizowania procesów (więzi) społecznych, gospodarczych lub politycznych w danej organizacji. Kryzys może mieć zatem znaczenie subiektywne, wyrażając ocenę danego zjawiska poczynioną przez określony podmiot. Ma on też postać obiektywną, bowiem bez względu na jego subiektywne oceny istnieje i oddziałuje na daną organizację. Kryzys wreszcie ma charakter procesualny, rozwija się, ma postać niepowtarzalną i coraz bardziej złożoną.

W kryzysie czas odgrywa dominującą rolę. Zmienna czasu zwykle powoduje ekstremalny rozwój sytuacji. W niektórych przypadkach czas

jest czynnikiem, który obniża skalę zagrożenia po jego kulminacji. Stąd wynika, iż czas może wpływać pozytywnie i negatywnie na zjawisko kryzysu. Charakterystyczną cechą kryzysu jest stan zaskoczenia, wynikający z opóźnionego zidentyfikowania sytuacji. Jeżeli jednak symptomy kryzysu są odpowiednio wcześnie rozpoznane, wówczas stan zaskoczenia traci znaczenie. Natomiast w przypadku rozpoznania sytuacji dopiero w stanie kryzysu stan zaskoczenia trwa tak długo, jak długo nie zostanie podjęte racjonalne przeciwdziałanie. Stan zaskoczenia nasila się w sytuacjach rozwoju zagrożeń po eskalacji zjawiska, w przypadku błędnej ingerencji lub jej braku ze strony człowieka lub sił natury. Kryzys nie pojawia się nagle, mimo że może być gwałtowny, rozwija się również od zarodka do pełnej postaci. Stąd w sytuacjach kryzysowych można mówić o pewnej ewolucji przyczyn w kryzys. Jeżeli potrafimy zdefiniować przyczynę, to wówczas należy opracować plan zapobiegający eskalacji zdarzeń w kryzys. W ewolucji przyczyn w kryzys wyróżniamy fazę płynnego rozwoju sytuacji kryzysowej w gwałtowną. Rozwój sytuacji kryzysowej wynika z jej charakteru i podjętych działań zapobiegawczych. Kryzys poprzez działania zapobiegawcze zawsze wymusza potrzebę kolejnych zmian.

Należy podkreślić, że ocena kryzysu w znacznej mierze zależy od punktu obserwacji. Każde zdarzenie inaczej wygląda, gdy spojrzymy na nie z pewnej perspektywy czasu, inaczej, gdy obserwujemy je z zewnątrz w czasie jego trwania, a jeszcze inaczej, gdy jesteśmy jego uczestnikami i aktorami. Kryzys jako specyficzny proces lub też stan, posiadający swoje źródła i przyczyny, może być prognozowany, rozpoznawany, identyfikowany, analizowany i poddany ocenie, a zatem (na podstawie uzyskanych ocen i prognoz) mogą zostać podjęte określone kroki (czynności) zaradcze. Wobec tego kryzys, chociaż w ograniczonym zakresie, jest zjawiskiem sterowalnym.

W rozważaniach dotyczących pojęcia kryzysu należy również uwzględnić obowiązującą w literaturze problemu typologię kryzysu ze względu na następujące kryteria:

- usytuowanie źródła kryzysu: wewnętrzne, zewnętrzne;
- charakter kryzysu: polityczno-militarne, niemilitarne;
- skalę występowania: globalne, regionalne, lokalne;
- czas trwania: krótkotrwałe, długotrwałe, permanentne;

- zasięg geopolityczny: międzynarodowe, narodowe;
- częstotliwość występowania: jednorazowe, powtarzające się, cykliczne;
- symptomy zagrożeń: oczekiwane, nieoczekiwane;
- szybkość rozprzestrzeniania się: bardzo szybkie, szybkie, wolne;
- obszar zagrożenia: miejscowe, lokalne, na terytorium jednego lub większej liczby państw.

Konkludując, należy stwierdzić, że kryzys to również zachwianie dotychczasowego stanu stabilizacji, gdzie po usunięciu skutków jego działania powinna nastąpić ponownie stabilizacja, jakościowo inna, ale przede wszystkim spełniająca standardy bezpieczeństwa. Kryzys stanowi apogeum wszelkich sytuacji, gdzie w wyniku jego skutków następuje „zerwanie" dotychczasowych stosunków prawnych, organizacyjnych, społecznych lub innych. Wynika z tego, że zjawisko kryzysu jest raczej krótkotrwałe i stanowi pewien etap sytuacji doprowadzających do jego eskalacji oraz zakończenia. Do ważnych cech kryzysu należy zaliczyć kulminację negatywnych zdarzeń, okres przełomu, nagłość i nieprzewidywalność zjawiska, skutki zjawiska zagrażające cennym wartościom dla podmiotu, jednocześnie przeciwdziałanie zjawisku wymaga zastosowania nadzwyczajnych środków, a ponadto negatywne przyczyny zjawiska mogą wynikać z zewnątrz lub wewnątrz podmiotu.

Janusz Falecki

Z. Andrzejczak, *Koncepcja doskonalenia krajowego systemu zarządzania kryzysowego w aspekcie ustaw o stanach nadzwyczajnych*, „Myśl Wojskowa" 2005, nr 1; A. Bujak, *Zarys teorii kryzysu i reagowania kryzysowego*, „Zeszyty Naukowe WSOW Ląd" 2014, nr 3; A. Czupryński, B. Wiśniewski, J. Prońko, *Uwarunkowania kryzysów polityczno-militarnych*, „Problemy Ochrony Granic" 2006, z. 33; J. Falecki, *Kryzys*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Relacje między zagrożeniem a sytuacją kryzysową i jej apogeum kryzysem*, [w:], *Instytucje publiczne i prywatne w systemie zarządzania kryzysowego*, B. Wiśniewski, J. Prońko, P. Lubiewski, (red.), Szkoła Główna Służby Pożarniczej, Warszawa 2018; tenże, *Teoretyczne aspekty zarządzania kryzysowego*, [w:] *Zarządzanie kryzysowe. Teoria, praktyka, konteksty, badania*, J. Stawnicka, B. Wiśniewski, R. Socha (red.), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2011; tenże, *The Crisis and the Crisis Situation – Relations*, „Security Dimensions and Socio-Legal Studies" 2012, no. 7; tenże, *Zarządzanie*

kryzysowe w teorii i praktyce. Pojęcia – zagrożenia – system, Wyższa Szkoła Handlowa im. Bolesława Markowskiego, Kielce 2012; E. Jendraszczak, W. Kozłowski, *Zarządzanie w sytuacjach kryzysowych*, Wydawnictwo MON-DSO, Warszawa 1997; W. Kitler, *Zarządzanie kryzysowe w Polsce, stan obecny i perspektywy*, [w:] *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, G. Sobolewski, D. Majchrzak (red.), AON, Warszawa 2011; W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilnej. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny*, Towarzystwo Wiedzy Obronnej, Warszawa 2010; W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1990; T. Leszczyński, *Źródła kryzysów wymagających reagowania kryzysowego państwa*, „Myśl Wojskowa" 2005, nr 5; E. Nowak, *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, AON, Warszawa 2007; J. Rogozińska-Mitrut, *Podstawy zarządzania kryzysowego*, ASPRA-JR, Warszawa 2010; *Słownik języka polskiego*, M. Szymczak (red.), Wydawnictwo Naukowe PWN, Warszawa 1982; *Słownik terminów z zakresu bezpieczeństwa narodowego*, J. Kaczmarek, W. Łepkowski, B. Zdrodowski (red.), AON, Warszawa 2008; *Zarządzanie kryzysowe*, t. 1: *Uwarunkowania teoretyczne, prawne i organizacyjne*, B. Wiśniewski, B. Kaczmarczyk (red.), PWSZ im. Witelona w Legnicy, Legnica 2012.

KRYZYS HUMANITARNY – wywołany siłami przyrody albo działaniem ludzkim stan →zagrożenia [t. 4] dla poszanowania →praw człowieka [t. 3] na danym obszarze. Jako przykłady kryzysów humanitarnych podaje się m.in.: sytuację na Haiti po trzęsieniu ziemi w 2010 r., w Syrii, Jemenie w związku z konfliktami zbrojnymi na terenie tych państw, w Sudanie w związku z brakiem wody, w Kongu w związku z epidemią wirusa ebola. Za jeden z najdłużej trwających, złożonych kryzysów humanitarnych uznać można sytuację trwającą w Somalii od końca lat 80. XX w. Jako jego przyczyny wskazać należy recesję gospodarczą, →wojnę domową [t. 4], działalność grup terrorystycznych oraz piratów, a także długotrwałe susze. Efektem jest ogromna liczba ofiar śmiertelnych, szczególnie wśród dzieci oraz uchodźców, destabilizacja regionu Rogu Afryki. Klęska głodu jest źródłem kryzysu w Dżibuti, Etiopii i Kenii.

Wskazuje się, że na dotkliwość kryzysów humanitarnych ma wpływ kilka czynników, w tym m.in. zmieniający się charakter konfliktów, zmiany klimatu, rosnąca rywalizacja o dostęp do energii i zasobów naturalnych, poziom ubóstwa, stabilność rządów, osiedlanie się ludności w strefach zagrożenia. Jako skutki kryzysów humanitarnych wymienia się natomiast

zwiększenie liczby uchodźców, destabilizację sytuacji wewnętrznej państw, degradację środowiska naturalnego. Należy jednak uwzględnić to, iż niektóre ze wskazanych okoliczności mogą występować zarówno jako przyczyny zaistnienia kryzysu humanitarnego, jak i jako jego następstwa.

→ K a t a s t r o f y n a t u r a l n e, powodując poważne zakłócenie funkcjonowania społeczeństwa, a często i państwa, wpływają w pierwszej kolejności na faktyczny wymiar realizacji praw człowieka, przede wszystkim prawa do życia, prawa do zdrowia, pożywienia i odpowiednich warunków bytowych. Nie można też pomijać prawnego wymiaru katastrof, związanego z uprawnieniem jednostek do ochrony przed pewnymi niebezpieczeństwami oraz ich skutkami dla życia, zdrowia, własności i innych prawnie chronionych interesów.

Prawa człowieka powinny być brane pod uwagę przy kształtowaniu rozwiązań prawnych służących zarządzaniu → s y t u a c j a m i k r y z y s o w y m i [t. 4] i niwelowaniu ich skutków. Niewątpliwie bowiem wystąpienie kryzysu nie zwalnia dotkniętego nim państwa z obowiązku poszanowania praw człowieka i nie uprawnia do ich derogacji.

W ostatnich dekadach wyraźnie wzrosła częstotliwość występowania kryzysów humanitarnych, szczególnie o skutkach transgranicznych, oraz nastąpił wzrost zaangażowania międzynarodowego – państw i organizacji międzynarodowych – w udzielanie w związku z tym pomocy humanitarnej, mierzony przede wszystkim wysokością środków przeznaczanych na ten cel. Jednocześnie jednak stawiane są zarzuty, że powstał swoisty przemysł pomocy humanitarnej, albowiem jej beneficjentami przestały być rzeczywiste ofiary katastrof, a zamiast tego przyciąga ona żądnych zysku, którzy traktują ją jako źródło dóbr i dalszych dochodów.

Z pojęciem kryzysu humanitarnego ściśle związane jest pojęcie pomocy humanitarnej jako udzielanej w odpowiedzi na kryzys i zmierzającej do jego zażegnania, odróżnia to pomoc humanitarną od pomocy rozwojowej, która udzielana w dłuższej perspektywie czasowej ma na celu ułatwienie rozwoju społecznego, gospodarczego i politycznego.

Obok terminu kryzys humanitarny wyróżnia się także katastrofę humanitarną, którą można określić jako przypadek szczególnie dotkliwego, daleko idącego kryzysu, tragiczne zdarzenie lub serię zdarzeń, w wyniku których dochodzi do utraty życia na dużą skalę, wielkiego cierpienia

ludzkiego i niedoli albo rozległych szkód materialnych lub środowiskowych, i w ten sposób poważnie zakłócającego funkcjonowanie społeczeństwa.

W odniesieniu do katastrofy humanitarnej prawo międzynarodowe reguluje kilka grup zagadnień – są to prawo reagowania w sytuacji katastrofy, prawa i obowiązki państwa dotkniętego katastrofą oraz prawa i obowiązki państwa oferującego pomoc. W przypadku, gdy źródłem kryzysu jest konflikt zbrojny, regulacji tych kwestii należy poszukiwać przede wszystkim w konwencjach genewskich z 1949 r. i protokołach dodatkowych z 1977 r. oraz z 2005 r. Po II wojnie światowej przyjęto bardzo wiele umów dwustronnych oraz konwencji wielostronnych dotyczących niektórych aspektów współpracy w przypadku katastrof (np. konwencja o pomocy żywnościowej, konwencja o udostępnianiu zasobów telekomunikacyjnych do zapobiegania katastrofom i usuwania ich skutków), katastrof określonego typu (np. przemysłowych, nuklearnych, chemicznych), kompleksowej współpracy regionalnej w zakresie zwalczania skutków katastrof (np. Międzyamerykańska konwencja dotycząca ułatwiania pomocy w przypadku katastrofy z 6 lipca 1991 r., porozumienie ASEAN w sprawie zarządzania katastrofami i reakcji w stanach nadzwyczajnych). W literaturze przedmiotu wskazuje się jednak na niechęć państw do przyjmowania wiążących aktów prawa, które nakładałyby na nie jakiekolwiek obowiązki względem podmiotów zagranicznych. Stąd też w praktyce większą moc oddziaływania mają dokumenty formalnie niewiążące, które wpływają na kształtowanie się zwyczaju międzynarodowego. Zaliczyć należy do nich przede wszystkim – opracowane przez Komisję Prawa Międzynarodowego – Artykuły o ochronie osób w przypadku katastrof, a także – przyjęte przez Międzynarodową Konferencję Czerwonego Krzyża i Czerwonego Półksiężyca – Wytyczne dotyczące usprawnienia krajowego systemu reagowania oraz międzynarodowej pomocy w sytuacji klęsk i katastrof.

Anna Pacholska

M. Balcerzak, *Pomoc humanitarna a międzynarodowa ochrona praw człowieka*, [w:] *Pomoc humanitarna w świetle prawa i praktyki*, P. Grzebyk, E. Mikos-Skuza (red.), Wydawnictwo Naukowe Scholar, Warszawa 2016; *International Disaster Response Law*, A. de Guttry, M. Gestri, G. Venturini (eds.), T.M.C. Asser Press, Springer, Hague 2012; A. Pacholska, *Kryzys humanitarny*, [w:] *Vademecum bezpieczeństwa*,

O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; *The International Law of Disaster Relief*, D.D. Caron, M.J. Kelly, A. Telesetsky (eds.), Cambridge University Press, New York 2014.

KRYZYS MIĘDZYNARODOWY – punkt zwrotny w konfrontacji między państwami, który poprzedza albo pokojowe rozwiązanie konfliktu, albo rozpoczęcie działań wojennych. Pojęcie → k r y z y s u pochodzi od stgr. κρίσις, *krisis*, pierwotnie oznaczało moment przełomowy, punkt zwrotny, wyjście, koniec, współcześnie używane jest do oznaczenia punktu zwrotnego, wyboru, rozstrzygnięcia. Kryzys międzynarodowy to przesilenie, przełamanie dotychczasowego stanu funkcjonowania systemu międzynarodowego na skutek napięć i konfliktów między uczestnikami stosunków międzynarodowych.

Można wydzielić szereg specjalistycznych podejść do kryzysów międzynarodowych. Warte uwagi są te, które dotyczą kryzysów systemowych, kryzysów konfrontacyjnych i kryzysów decyzyjnych. Podejścia te różnią się definicjami, poziomami analizy i zainteresowaniami praktycznymi.

Kryzysy systemowe zakłócają stabilność systemu międzynarodowego i stwarzają warunki do jego upadku lub zmiany. Występują globalne i regionalne kryzysy systemowe. Globalne kryzysy miały miejsce na przełomie lat 80. i 90. XX w., a zakończyły się likwidacją Układu Warszawskiego i upadkiem ZSRR, faktycznie zakończyły prawie półwieczne istnienie dwubiegunowego porządku międzynarodowego z dwoma głównymi wrogimi mocarstwami – ZSRR i USA.

Nie wszystkie kryzysy systemowe są katastrofalne. Ponadto można sztucznie je tworzyć w regionie, aby zachęcić rządy odpowiednich regionów do podejmowania inicjatyw. Członkowie UE wielokrotnie wykorzystywali „kryzysy terminowe", aby zmusić rządy państw członkowskich UE do podjęcia kroków integracyjnych, czego przykładem może być traktat z Maastricht z 1992 r., który wyznaczył członkom UE termin spełnienia warunków niezbędnych do przyjęcia wspólnej waluty – euro.

Nie tak dawno temu przyczyną międzynarodowych kryzysów systemowych mogły być jedynie → w o j n y [t. 4] lub rewolucje, które całkowicie zmieniały podział władzy w krajach i na świecie. Jednak dziś, w obliczu globalnej współzależności gospodarczej krajów, załamanie waluty lub

hiperinflacja w wiodących krajach mogą być również początkiem kryzysu systemowego. Regionalna niestabilność finansowa w Azji pod koniec lat 90. wyraźnie zarysowała tę perspektywę.

Kryzysy konfrontacyjne powstają na skutek roszczeń (konfrontacji) jednego podmiotu systemu międzynarodowego wobec stanowiska drugiego. W odróżnieniu od kryzysów systemowych kryzysy konfrontacyjne nie niosą → z a g r o ż e n i a [t. 4] dla stabilności systemu międzynarodowego i/lub nie doprowadzają do jego upadku lub zmiany. Konsekwencje ich pojawienia się dla porządku międzynarodowego są odczuwalne tylko dla podmiotów, które prowadzą konfrontacje. Zazwyczaj po wyrażeniu przez jedną ze stron roszczeń wobec drugiej ze strony drugiej następuje odpowiedź wobec roszczeń pierwszej, a kryzys kończy się zawarciem porozumienia. Możliwy jest także scenariusz, gdy strony nie dojdą do porozumienia i zamiast zakończenia kryzysu ma miejsce jego eskalacja. Za przykład kryzysu konfrontacyjnego możemy uznać konflikt między Argentyną a Wielką Brytanią w 1982 r. Argentyna wysunęła roszczenia wobec Zjednoczonego Królestwa w sprawie przejęcia kontroli nad Falklandami. Argentyńskie roszczenia zostały odrzucone przez rząd Margaret Thatcher, kolejne negocjacje zakończyły się niepowodzeniem, co w konsekwencji przyczyniło się do rozpoczęcia wojny o Falklandy (wojny o Malwiny) między Argentyną i Wielką Brytanią.

Kryzysy konfrontacyjne często bazują na założeniach teorii gier, ich uczestnicy próbują przewidzieć, w jaki sposób prowadzić konfrontację, by zostać zwycięzcą, jednocześnie ponosząc jak najmniejsze straty.

Trzeci rodzaj kryzysów to kryzysy decyzyjne, dotyczą one poszczególnych decyzji (działań), które stanowią poważne zagrożenie dla przywódców danego państwa, a w większym zakresie także obywateli państwa. W ramach koncepcji podejmowania decyzji brane są pod uwagę 2 kwestie: w jaki sposób krytyczna sytuacja wpływa na jakość podejmowania decyzji i jakie cechy (umiejętności) podmiotów decyzyjnych przyczyniają się do mniej lub bardziej efektywnego przeciwdziałania kryzysom. Na tej podstawie tworzone są zalecenia i narzędzia zapobiegające kryzysom i wskazujące sposoby ich skutecznego rozwiązywania bez znaczących negatywnych konsekwencji. W tym celu na początku ustalany jest pożądany standard jakości rozwiązania (np. jego racjonalność lub zdolności

adaptacyjne, nietradycjonalny charakter lub uniknięcie niepożądanych skutków itp.). Następnie określane są czynniki polityczne, które działają na odchylenia podejmowanych decyzji od ustalonych standardów oraz stosowane są zalecenia dotyczące sposobu osiągnięcia pożądanego efektu.

Przykładem tego rodzaju kryzysu był kryzys w kręgach rządowych USA, gdy w październiku 1962 r. amerykańska agencja wywiadowcza stwierdziła, że Związek Radziecki w tajemnicy umieścił na Kubie pociski balistyczne średniego zasięgu, co stanowiło bezpośrednie zagrożenie dla terytorium USA. W latach 1959–1960 USA rozmieściły pociski w pobliżu ZSRR na terytorium Wielkiej Brytanii, Włoch i Turcji. Przed elitami rządzącymi USA stanęło zadanie, by w jak najkrótszym czasie podjąć racjonalne decyzje.

Możliwe jest ewoluowanie kryzysów od jednego typu ku drugiemu. Tak np. w 1962 r., gdy rząd USA zażądał wycofania radzieckich rakiet z terytorium Kuby, wprowadził kwarantannę morską Kuby (blokadę transportu środków bojowych) oraz embargo na handel z państwem, kryzys decyzyjny przekształcił się w kryzys konfrontacyjny między Związkiem Radzieckim i USA. Konfrontacją ze strony Związku Radzieckiego było wysłanie statków wiozących kolejne materiały militarne. W konsekwencji kryzys konfrontacyjny stał się kryzysem systemowym.

Kryzys międzynarodowy w zależności od tego, jakiego segmentu funkcjonowania systemu międzynarodowego dotyczy, może mieć wymiar kryzysu finansowego, gospodarczego oraz środowiskowego.

Kryzys finansowy wiąże się z poważnymi zakłóceniami na rynku finansowym, co przejawia się w znacznym spadku cen aktywów oraz upadłości wielu instytucji finansowych i niefinansowych. Kryzys finansowy powoduje niezdolność rynków do alokowania kapitału w gospodarce, rzutuje to na zmianę płynności oraz niewypłacalność uczestników rynku. Kryzys finansowy może przybierać formę kryzysu bankowego, kryzysu walutowego oraz kryzysu zadłużeniowego, w zależności od problemów dominujących na rynku finansowym. Kryzysy te są ze sobą w mniejszym lub większym stopniu powiązane, a ich sprzężenie nasila się w warunkach globalizacji i integracji rynków finansowych. Kryzys przyczynia się do pojawienia zagrożeń w sektorze bankowym, poprzez utratę płynności oraz pogorszenie się pozycji kapitałowej banków na mocy strat, które

ponoszą z tytułu niespłaconych kredytów. Kryzys bankowy jest także utożsamiany z tzw. paniką bankową (ang. *bank run*). Kryzys bankowy jest ściśle powiązany z kryzysem finansowym, gdyż konsekwencjami dla kryzysu finansowego jest upadek instytucji finansowych. Przesłankami dla wybuchu kryzysu walutowego jest polityka monetarna państwa, która przyczynia się do upłynnienia kursu walut i zaciągnięcia pożyczek zagranicznych w celu obrony kursu centralnego. Przyczynia się to do utraty zaufania inwestorów do danej waluty, a w konsekwencji do ataku spekulacyjnego. Kryzys walutowy jest częścią kryzysu finansowego, jednakże może on występować autonomicznie, nie doprowadzając w konsekwencji do powstania kryzysów w pozostałych ogniwach systemu finansowego. Kryzys zadłużeniowy wiąże się z niemożliwością spłacenia wcześniej zaciągniętych pożyczek, co oznacza niezdolność sektora publicznego i prywatnego do wywiązania się ze zobowiązań z długu. Kryzys ten dla sektora publicznego oznacza brak możliwości spłaty lub redukcji długu, który powstał na kanwie świadomego zawyżenia własnej waluty, może to doprowadzić do poważnych konsekwencji, takich jak niewypłacalność lub upadek państwa. Z kolei dla sektora prywatnego kryzys ten wywołany jest niespłaceniem zobowiązań finansowych, które pojawiły się poprzez odrzucenie lub restrukturyzację długu. Przykładem kryzysu finansowego może być kryzys meksykańskiego peso w 1994 r. wywołany nagłą dewaluacją peso w grudniu 1994 r. oraz zamieszkami spowodowanymi wysokim poziomem → k o r u p c j i w państwie. Administracja nowego prezydenta E. Zedillo, szukając rozwiązania problemów, podjęła decyzję o dewaluacji peso, spowodowało to rezygnację inwestorów zagranicznych, spadek PKB oraz wzrost inflacji. Z kolei przyczyną rosyjskiego kryzysu finansowego w 1998 r. była korupcja oraz brak efektywności reform państwowych, dewaluacja rubla i polityczna niestabilność. Spadki cen ropy i gazu dla państwa rosyjskiego jako światowego eksportera tych surowców dodatkowo pogłębiły kryzys. Kryzys przerzucił się na inne rynki, takie jak Ukraina czy Czechy.

Kryzys gospodarczy należy rozumieć jako gwałtowne załamanie się gospodarki w skali światowej, co powoduje, że dotyka on większość krajów rozwiniętych i krajów rozwijających się. Kryzys gospodarczy definiowany jest także jako głęboka i przedłużająca się recesja. Recesja gospodarcza

jest to okres, w którym przez co najmniej 2 następujące po sobie kwartały występuje zmniejszenie aktywności finansowej w państwie, co skutkuje spadkiem wartości PKB, tj. wartości wszystkich dóbr i usług wyprodukowanych w państwie skorygowanych o stopę inflacji. Nie tylko recesja gospodarcza, lecz również krach gospodarczy i depresja gospodarcza oznaczają zmniejszenie poziomu PKB w ujęciu realnym w co najmniej 2 kwartałach. Recesję i depresję gospodarczą odróżnia długość ich trwania i skala spadków. Krach gospodarczy oznacza nagłe i gwałtowne zmniejszenie tempa wzrostu PKB. Bazując na teorii cyklu koniunkturalnego, depresja jest jedną z faz klasycznego cyklu, w której następuje dno kryzysu i która charakteryzuje się zahamowaniem spadku produkcji oraz stabilizacją zatrudnienia, cen i stopy zysku. W cyklu koniunkturalnym w fazie kryzysu następują zmiany wskaźników makroekonomicznych, tj. spadek popytu na dobra i usługi, spadek produkcji i zatrudnienia oraz spadek cen i inwestycji. Załamanie cyklu koniunkturalnego może mieć zasadniczy wpływ na zmniejszenie tempa wzrostu gospodarczego. Skutki kryzysu na skalę światową powodują hamowanie inwestycji, ograniczenie dostępu do kredytów, ogłaszanie upadłości firm, co z kolei przyczynia się do zwiększenia bezrobocia, zniszczenia części sektora bankowego, spowolnienia wymiany międzynarodowej, ograniczania wpływów do budżetów państw bogatych. Zatem kryzys gospodarczy może mieć następujące objawy: wzrost inflacji, spadek produkcji, spadek płac i zatrudnienia, spadek inwestycji oraz PKB, wzrost deficytu budżetowego, spadek tempa rozwoju gospodarczego oraz spadek tempa eksportu.

Przykładem kryzysu gospodarczego jest argentyński kryzys gospodarczy z 1999 r., u podłoża którego leżały takie czynniki jak → d y k t a t u r a w o j s k o w a w państwie, klęska na Falklandach, załamanie gospodarcze oraz inflacja. Pogorszenie sytuacji związane z wzrostem poziomu korupcji i wzrostu długu spowodowało recesję, co przyczyniło się do utraty inwestycji oraz polityki rządowej związanej z zamrożeniem kapitałów na rachunkach. Doprowadziło to do pogorszenia sytuacji w państwie, krwawych zamieszek oraz upadku rządu F. de la Rúa. Do kryzysu gospodarczego jest zaliczany kryzys naftowy z 1973 r., określany także mianem kryzysu paliwowego czy szoku naftowego. Kryzys ten objął wszystkie państwa uzależnione od ropy naftowej, spowodował gwałtowny wzrost

ceny ropy naftowej na rynkach światowych. Przyczyną wybuchu kryzysu było spotkanie przedstawicieli OPEC w Kuwejcie, gdzie podjęto decyzję z inicjatywy Arabii Saudyjskiej i Iranu o zmniejszeniu wydobycia bez żadnego porozumienia z największymi koncernami, takimi jak Shell, BP, Texaco itd. Było to działanie wymierzone przeciw USA po wybuchu wojny izraelsko-arabskiej w 1973 r. Decyzja podjęta przez OPEC spowodowała gwałtowny wzrost cen ropy naftowej o 400%, z 3 USD do 12 USD. Indeks giełdowy Dow Jones w reakcji na podwyżkę cen ropy w ciągu kilku miesięcy stracił na wartości ok. 40%. W 1979 r. miał miejsce drugi szok naftowy, wywołany rewolucją islamską w Iranie. Na skutek przewrotu Iran całkowicie wstrzymał eksport ropy naftowej, co przyczyniło się do kolejnych drastycznych podwyżek cen ropy z 17 USD do ponad 40 USD.

Kryzys środowiskowy (ekologiczny) to stopień zanieczyszczenia środowiska, który uniemożliwia środowisku samooczyszczenie oraz samoodtworzenie ekosystemów i biocenoz. Pojawienie się kryzysu natury ekologicznej jest wywołane zachwianiem równowagi ekologicznej ekosystemów, zakłóceniami obiegu materii i przepływu energii w ekosystemie. Przyczyny kryzysu ekologicznego są związane z katastrofą ekologiczną, rozwojem cywilizacyjnym, gwałtownym przyśpieszeniem procesów urbanizacji, wzrostem liczby ludności i podnoszeniem standardów życia, wzrostem konsumpcji i rozwojem przemysłu, niedoskonałymi technologiami i szkodliwymi środkami używanymi w rolnictwie. Rozwój cywilizacyjny niesie negatywne skutki dla środowiska naturalnego poprzez zniszczenie naturalnych ekosystemów, zanieczyszczenie środowiska, nadmierną eksploatację zasobów naturalnych oraz pogłębianie się efektu cieplarnianego.

Bardzo istotną kwestią jest niski poziom wiedzy i świadomości społecznej na temat zagrożeń środowiska naturalnego wywołanych działaniami człowieka. Konieczne jest uwzględnienie międzynarodowego bezpieczeństwa ekologicznego poprzez wprowadzenie norm, zasad postępowania i wzajemnych zobowiązań gwarantujących wszystkim podmiotom stosunków międzynarodowych zachowanie i racjonalne wykorzystanie naturalnych zasobów oraz poprawę stanu środowiska. Wpływ kryzysu ekologicznego na kraje bogate i rozwijające się jest zróżnicowany. W przypadku tych pierwszych problem dotyczy zanieczyszczenia

środowiska i konsekwencji dla człowieka, w przypadku drugich problem jest związany także z nadmierną eksploatacją zasobów naturalnych.

Maryana Prokop

M. Bochenek, *Rozważania historyczno-semantyczne na temat kryzysów ekonomicznych*, „Acta Universitatis Nicolai Copernici. Ekonomia" 2012, nr 2 (43); *Kryzysy bankowe: przyczyny i rozwiązania*, M. Iwanicz-Drozdowska (red.), Polskie Wydawnictwo Ekonomiczne, Warszawa 2002; L. Leśniewski, *Przegląd teoretycznego ujęcia kryzysu finansowego*, „Studia i Prace Kolegium Zarządzania i Finansów" 2016, z. 151; W. Małecki i in., *Kryzysy walutowe*, Wydawnictwo Naukowe PWN, Warszawa 2001; W. Morawski, *Kronika kryzysów gospodarczych*, Wydawnictwo Trio, Warszawa 2003; *Ostatni światowy kryzys finansowy. Przyczyny, przebieg, polityka przedsiębiorstwa*, t. III, K. Piech, K. Wierus (red.), Instytut Wiedzy i Innowacji, Warszawa 2012; *Polityka makroekonomiczna w warunkach kryzysu i jej wpływ na gospodarkę*, Z. Dach (red.), Wolters Kluwer Polska, Warszawa 2011; A. Skowroński, *Filozoficzne i światopoglądowe implikacje kryzysu ekologicznego*, „Studia Ełckie" 2007, nr 9; A. Sławiński, *Rynki finansowe*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2006; M. Tomala, R. Zajęcki, *Impact of the 2008–2009 Financial Crisis on Democratisation Processes in the European Union*, „Rocznik Bezpieczeństwa Międzynarodowego" 2019, nr 2; A. Zielińska-Głębocka, *Współczesna gospodarka światowa*, Wolters Kluwer Polska, Warszawa 2012; *Zmiany instytucjonalne w reakcji na obecny kryzys*, A. Wojtyna (red.), Polskie Wydawnictwo Ekonomiczne, Warszawa 2013; F. Charles, О.В. Юркова, *Кризи, основні концептуальні підходи до аналізування суспільних криз (з досвіду міжнародної політології)*, [w:] *Енциклопедія історії України*, В.А. Смолій та ін. (ред.), Т. 5 (Кон – Кю), НАН України. Інститут історії України, Наукова думка, Київ 2008.

KULTURA BEZPIECZEŃSTWA – utożsamiana z kulturą obronności; klimat bezpieczeństwa lub securitologia stosowana jest przez przedstawicieli →nauk o bezpieczeństwie [t. 3] jako określenie ich domeny badawczej. L. Korzeniowski zalicza securitologię do nauk praktycznych, które w sposób naukowy wskazują perspektywę niwelowania →zagrożeń [t. 4] dla istnienia, rozwoju i normalnego funkcjonowania człowieka i organizacji społecznych. Definiowana jest ona w szerokiej lub w wąskiej perspektywie. W szerszym ujęciu obejmuje ona „utrwalony dorobek ludzkości w zakresie materialnym i pozamaterialnym, pozwalający na ratowanie, podtrzymywanie, a nawet podnoszenie poziomu

bezpieczeństwa określonych podmiotów – tak indywidualnych, jak i zbiorowych", wymagając od nich refleksyjności i „kultywowania ducha ludzkiego". M. Cieślarczyk, reprezentant holistycznego podejścia do rozumienia pojęcia kultury bezpieczeństwa, stwierdza, że do jej podstawowych komponentów zalicza się element mentalny (duchowy, niematerialny, etyczny, świadomościowy, aksjologiczny), racjonalno-organizacyjny (społeczny) i materialny. Według J. Piwowarskiego tylko pierwszy z nich decyduje o tym, czy rozwój człowieka będzie w sposób właściwy służył → b e z p i e c z e ń s t w u [t. 1] ludzkości. Dlatego kultura bezpieczeństwa koncentrować powinna się na człowieku, jego potrzebach, wyznawanych przez niego wartościach, przyjmowanych postawach i racjonalnych zachowaniach, aby systematycznie rozwiązywać problemy, z którymi przychodzi mu się mierzyć.

W tym kontekście kultura bezpieczeństwa jest bliższa pojęciu bezpieczeństwa humanitarnego, w którym akcent położony jest na ochronę człowieka i jego godności, a polityczny wymiar, jak stwierdza B. Bartz, łączy „perspektywę praw człowieka, rozwój ludzkości, zabezpieczenie pokoju i prewencję konfliktów". W koncepcji tej przedkłada się bezpieczeństwo ludności osiągane przez stały jej rozwój nad bezpieczeństwo terytorialne osiągane poprzez uzbrojenie.

Także termin klimatu bezpieczeństwa, wprowadzony przez D. Zoharę do piśmiennictwa z zakresu securitologii, pokrywa się w obszarze przedmiotu i metod badawczych z terminem kultury bezpieczeństwa, chociaż w podejściu do problemów bezpieczeństwa w większym stopniu obejmuje aspekt psychologiczny. Żeby móc odczuć ów klimat, nieodzowne jest dążenie do osiągnięcia przez społeczeństwo dojrzałości pozwalającej podejmować mądre decyzje w sferze politycznej, społecznej, kulturowej, technologicznej, informacyjno-komunikacyjnej i innych. Niewystarczające jest więc podejście do kultury bezpieczeństwa wyłącznie z pozycji działań obronnych. Dlatego, jak stwierdza Cieślarczyk, odchodzi się od stosowania pojęcia kultury obronności wyłącznie w wymiarze militarnym i przypisuje mu się rolę fundamentu, na którym można budować kulturę bezpieczeństwa.

Holistyczny wgląd w problemy kultury bezpieczeństwa, szczególnie w globalnym → s p o ł e c z e ń s t w i e i n f o r m a c y j n y m [t. 4], wymaga

prowadzenia badań nad jej fenomenem w sposób interdyscyplinarny. Społeczeństwo to generuje nowe zagrożenia, wynikające z nieodróżniania bezpieczeństwa, jakie daje człowiekowi „wolność do", od niezabezpieczonej i niekontrolowanej wolności wynikającej z braku wiedzy, kompetencji, przezorności, inteligencji, niechęci przestrzegania ustalonych norm i kodeksów oraz z braku kultury bezpieczeństwa całych systemów państwowych. Bezpieczeństwo jako kształtowanie pewności przetrwania, posiadania i swobód rozwojowych podmiotu wymaga od człowieka przyjęcia postawy obywatelskiej, aby mógł on przeciwdziałać zagrożeniom oraz świadomie podejmować wyzwania poprzez redukowanie ryzyka i wykorzystywanie szans. Nie jest to możliwe bez bycia świadomym istnienia ryzyka związanego z rozwojem i rozumienia, że bezpieczeństwo w dłuższym okresie nie może istnieć bez rozwoju. Dlatego właściwą postawę wobec problemów bezpieczeństwa Piwowarski utożsamia z wrażliwością i tzw. podwyższoną uważnością obywateli, związaną z przewidywaniem przez nich sytuacji zagrożenia, identyfikowaniem ich w porę i odpowiedniego na nie reagowania. Z tego względu należy zwrócić uwagę człowieka na różne obszary bezpieczeństwa, w tym indywidualnego (osobowego), grupowego (zawodowego, korporacyjnego), państwowego (lokalnego, terytorialnego, krajowego), międzynarodowego (globalnego, regionalnego), szczególnie odnoszące się do dziedzin jego aktywności ekonomicznej, społecznej, informacyjnej, ekologicznej, kulturalnej, zdrowotnej, finansowej itp.

Dążenie do bezpieczeństwa nie jest jednak możliwe bez wykształcenia kultury bezpieczeństwa, przez którą Cieślarczyk rozumie:

> zbiór podstawowych założeń, wartości, norm, reguł, symboli i przekonań charakterystycznych dla danego podmiotu, wpływających na sposób postrzegania przez niego wyzwań, szans i zagrożeń w bliższym i dalszym otoczeniu, sposób odczuwania bezpieczeństwa i myślenia o nim oraz związany z tym sposób zachowania i działania, wyuczony przez podmiot w procesach edukacji i tworzenia infrastruktury, np. informatycznej i informacyjnej, służącej osiąganiu przez podmiot najszerzej rozumianego bezpieczeństwa, z pożytkiem dla siebie i dla otoczenia.

Dlatego nie bez przyczyny istotę kultury bezpieczeństwa M. Lutostański upatruje w:

> praktycznym wytworzeniu i utrzymaniu takiego środowiska funkcjonowania jednostki i narodu, które pozwala im zdobyć i umożliwić realizowanie własnych spraw i osiąganie autonomicznych celów w akceptowanym komforcie psychicznym.

Wymaga to wykształcenia wrażliwości dostrzegania każdego negatywnego zjawiska oraz umiejętności oceny jego wpływu na realizację celów narodu.

Kultura bezpieczeństwa łączy się także z umiejętnością radzenia sobie przez podmiot z ryzykiem i ze sprawnością zarządzania nim. Deficyt umiejętności zarządzania ryzykiem sprawia, że jednostka nie potrafi zachować równowagi pomiędzy podejmowanymi działaniami kreatywnymi i innowacyjnymi a poczuciem odpowiedzialności za skutki tych działań i staje się źródłem generowania postaw zachowawczych i destrukcyjnych, a to stoi w opozycji do gotowości ponoszenia odpowiedzialności za siebie, innych i swoje otoczenie. M. Cieślarczyk i A. Filipek dostrzegają w kulturze bezpieczeństwa nie tylko indywidualną wrażliwość ludzi, stanowiącą cechę ich mentalności, nakazującą preferowanie bezpieczeństwa, względnie ryzyka, lecz również potrzebę podejmowania ryzyka i mądrego zarządzania nim w celu wprowadzania zmiany umożliwiającej rozwój, a w konsekwencji gwarantującej bezpieczeństwo podmiotu w dłuższym okresie. Cieślarczyk uważa, że radzenie sobie z ryzykiem oraz umiejętność zarządzania nim jest ściśle związana z → k u l t u r ą i n f o r m a c y j n ą podmiotu. Dlatego kształtowanie kultury bezpieczeństwa bez dbałości o kulturę informacyjną może nie przynieść oczekiwanych efektów i musi być połączone z podnoszeniem poziomu kultury informacyjnej wszystkich grup społecznych i zawodowych w kraju.

Pojęcie kultury zestawione z terminem bezpieczeństwa sprawia, że w naukach o bezpieczeństwie uwaga skoncentrowana jest na problemach budowania świadomości bezpieczeństwa wśród społeczeństwa, na pozyskiwaniu wiedzy o zagrożeniach, odpowiedzialności za utrzymywanie stanu bezpieczeństwa, na wartościach, na których można budować

bezpieczeństwo jednostki i narodu, na pozytywnych postawach ludności wobec problemów bezpieczeństwa, na ich emocjach związanych z dążeniem do przeciwdziałania zagrożeniom i wzmacniania więzi, na zachowaniach, które sprzyjają budowaniu poczucia bezpieczeństwa i niwelowaniu stanów zagrożenia. Kultura bezpieczeństwa – podobnie jak kultura – powinna kształtować w człowieku ideał człowieczeństwa, a wartości sprzyjające rozwijaniu tego ideału należy pielęgnować i przekazywać kolejnym pokoleniom.

Szerokie podejście do problemów kultury bezpieczeństwa jest szczególnie ważne we współczesnym świecie przesyconym technologiami informatyczno-komunikacyjnymi i ponoszącym konsekwencje procesów globalizacyjnych. Tym bardziej że funkcjonowanie w cywilizacji cyfrowej stwarza wiele problemów aksjologicznych, a globalne społeczeństwo ma problemy z odróżnianiem problemów bezpieczeństwa w skali lokalnej od bezpieczeństwa światowego.

Megatrendy rozwojowe, do których zaliczyć można m.in. rewolucję informacyjną i wynikającą z niej dominację społeczeństw informacyjnych, sprawiają, że problemy bezpieczeństwa przestają być domeną wyłącznie nauk o wojskowości, obronności i polityce. Rozumienie bezpieczeństwa w epoce płynnej nowoczesności, w epoce ryzyka i katastrof zyskuje szerszy wymiar – wymiar humanistyczny i społeczny – a kształtowanie jego poczucia możliwe jest tylko w sytuacji zaufania obywateli do państwa i decydentów. Bez tego zaufania trudno kształtować postawy odpowiedzialności za wspólne dobro, wytworzyć postawy zaangażowania i partycypacji społecznej, zintegrować grupy do podejmowania wspólnych przedsięwzięć na rzecz tworzenia warunków gwarantujących bezpieczeństwo całej wspólnoty. Niestety, jak konkluduje Bartz, chociaż kultura bezpieczeństwa koreluje z odpowiedzialnością państwa za los społeczeństwa, to władze polityczne, także krajów demokratycznych, podejmują zbyt często decyzje „nieuwzględniające egalitarnego i humanitarnego znaczenia bezpieczeństwa, w sposób relatywny identyfikując zagrożenia w zależności od interesów poszczególnych grup społecznych". Stanowisko to wzmacnia stwierdzenie U. Becka, że dopóki ryzyko nie zostanie potwierdzone, tak długo nie istnieje w sensie prawnym, pedagogicznym, ekonomicznym, społecznym, etycznym, psychologicznym,

medycznym i nie zapobiega się mu ani nie podejmuje w tym zakresie działań profilaktycznych.

Hanna Batorowska

B. Bartz, *Kultura bezpieczeństwa w epoce niepewności*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 2: *Bezpieczeństwo i kultura bezpieczeństwa w teorii, w badaniach naukowych i w praktyce*, A. Filipek, B. Gałek (red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2014; tenże, *Perspektywiczne znaczenie bezpieczeństwa humanitarnego*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 4: *Odkrywanie znaczeń w naukach o bezpieczeństwie*, A. Filipek (red.), Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2015; H. Batorowska, *Kultura bezpieczeństwa*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Wybrane problemy kultury bezpieczeństwa, kultury informacyjnej i bezpieczeństwa informacyjnego w refleksji nad funkcjonowaniem człowieka w świecie informacji*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym*, t. 2, H. Batorowska, Z. Kwiasowski (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2016; taż, *Wybrane aspekty kultury bezpieczeństwa w społeczeństwie informacji i wiedzy*, „Studia Politologica Ucraino-Polona" 2016, nr 6; M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Wydawnictwo Akademii Podlaskiej, Siedlce 2006; tenże, *Kultura informacyjna jako element kultury bezpieczeństwa*, [w:]: *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*, t. 1, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2015; M. Cieślarczyk, A. Filipek, *Kultura bezpieczeństwa – między kreatywnością a poczuciem odpowiedzialności*, [w:] *Bezpieczeństwo i edukacja dla bezpieczeństwa w zmieniającej się przestrzeni społecznej i kulturowej*, R. Rosa (red.), Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2012; *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 2: *Bezpieczeństwo i kultura bezpieczeństwa w teorii, w badaniach naukowych i w praktyce*, A. Filipek, B. Gałek (red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2014; L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2012; A. Pieczywok, *Kultura bezpieczeństwa człowieka i jej zagrożenia*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 2: *Bezpieczeństwo i kultura bezpieczeństwa w teorii, w badaniach naukowych i w praktyce*, A. Filipek, B. Gałek (red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2014; J. Piwowarski, *Podstawowe kategorie*

nauk o bezpieczeństwie, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 4: *Odkrywanie znaczeń w naukach o bezpieczeństwie*, A. Filipek (red.), Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2015.

KULTURA BEZPIECZEŃSTWA INFORMACYJNEGO – jako komponent →kultury bezpieczeństwa stanowi o kształcie obronności kraju. W szerokim podejściu do problemów kultury bezpieczeństwa, o którym traktują liczne prace M. Cieślarczyka, przedstawia się kulturę bezpieczeństwa informacyjnego jako czynnik kształtujący odporność społeczeństwa na ataki informacyjne i podnoszący jego świadomość na temat współczesnej →wojny informacyjnej [t. 4].

Kulturę tę należy analizować z perspektywy nadmiarowości →informacji i przyspieszenia technologicznego w świecie ponoszącym konsekwencje procesów globalizacyjnych. Tym bardziej że cywilizacja cyfrowa generuje problemy aksjologiczne, a jej przedstawiciele nie odróżniają problemów bezpieczeństwa w skali lokalnej od bezpieczeństwa światowego. Stąd zainteresowanie badaczy kultury bezpieczeństwa informacyjnego rewolucją informacyjną i wynikającą z niej dominacją →społeczeństw informacyjnych [t. 4]; →potopem informacyjnym [t. 3] przyczyniającym się do powstawania stresu informacyjnego utrudniającego lub uniemożliwiającego podejmowanie mądrych decyzji; skokowym postępem w dziedzinie technologii; powstawaniem sieci przetwarzania informacji; globalną ekspansją gospodarki opartej na wiedzy; globalizacją; homogenizacją kultury z dominacją konsumpcyjnego stylu życia; przewagą technopolu nad kulturą i absorpcją światopoglądu technokratycznego; rosnącą władzą mass mediów; wirtualizacją życia; przenikaniem się kultur; erupcją →cyberzagrożeń [t. 1]; postępującym procesem wykluczenia cyfrowego i pogłębiającym się wykluczeniem społecznym jednostek, grup, organizacji, narodów.

Żyjąc w środowisku „namnażania się informacji", w którym poddawane są one procesowi manipulacji i zniekształceniom w celu dezinformowania przeciwnika, uczestniczymy w permanentnej walce informacyjnej. Rozgrywa się ona zarówno w prywatnej, jak i publicznej →przestrzeni informacyjnej [t. 3]. Walka informacyjna toczy się o dostęp do dokumentów, źródeł i wiedzy, dzięki którym można uzyskać

przewagę nad nieprzyjacielem, można przejąć jego aktywa i uzależnić od własnych decyzji. W tej walce orężem jest informacja, a celem podporządkowanie umysłów zaatakowanej ludności.

Należy się do niej przygotować. W tym celu konieczna jest ciągła i powszechna edukacja społeczeństwa w zakresie →zagrożeń [t. 4] stwarzanych przez cywilizację cyfrową i problemów dotyczących →bezpieczeństwa informacyjnego [t. 1]. Rozwijanie świadomości społeczeństwa i wyczulanie go na zachowania zagrażające bezpieczeństwu informacyjnemu państwa należy do zadań priorytetowych. W →Doktrynie Cyberbezpieczeństwa RP edukacja w zakresie bezpieczeństwa informacyjnego traktowana jest jako ważne ogniwo wsparcia systemu →cyberbezpieczeństwa [t. 1], a umiejętności i świadomość indywidualnych użytkowników za jeden z filarów cyberbezpieczeństwa kraju. Kultura bezpieczeństwa informacyjnego w znaczącym stopniu przyczynia się do podnoszenia poziomu bezpieczeństwa informacyjnego kraju.

Posiłkując się definicją kultury bezpieczeństwa Cieślarczyka i →kultury informacyjnej H. Batorowskiej, można określić kulturę bezpieczeństwa informacyjnego jako sferę aktywności człowieka kształtowaną przez →świadomość informacyjną [t. 4] i sposób myślenia o bezpieczeństwie; wartości, normy i reguły wspierające potrzebę podwyższania poziomu kultury bezpieczeństwa pozwalającej dostrzegać wyzwania, szanse i zagrożenia w lokalnej i globalnej przestrzeni informacyjnej; postawy wpływające na uwrażliwienie społeczeństwa na znaczenie bezpieczeństwa i kształtowanie zachowań charakterystycznych dla dojrzałych informacyjnie użytkowników →infosfery, współodpowiedzialnych za to bezpieczeństwo. Zachowania te wynikają z oddziaływania na siebie wymienionych komponentów kultury. Odnoszą się one do przedmiotów i innych wytworów związanych z bezpieczeństwem informacyjnym i uczestnictwem podmiotów w procesie informacyjnym.

Komponenty kultury bezpieczeństwa informacyjnego o cechach mentalnych (wartości, normy, zasady), materialnych (→infrastruktura informacyjna) i organizacyjnych (działania, regulacje prawne, procedury, polityki bezpieczeństwa informacyjnego, struktury) przenikają się nawzajem, a kultura informacyjna łączy je także w odniesieniu do

poszczególnych sektorów bezpieczeństwa, takich jak bezpieczeństwo ekologiczne, zdrowotne, polityczne, społeczne, technologiczne, kulturowe itd.

Kluczowym komponentem tej kultury jest kultura informacyjna i rozwijane przez nią kompetencje informacyjne. Nie ograniczają się one do umiejętności rozpoznawania potrzeb informacyjnych, lokalizowania i oceny, zastosowania i tworzenia informacji w kontekście kulturowym i społecznym. Są to także kompetencje mające zasadnicze znaczenie dla uzyskiwania przewagi konkurencyjnej osób, przedsiębiorstw, regionów i narodów, wykraczające poza obecne technologie i obejmujące uczenie się, krytyczne myślenie i umiejętności interpretacyjne. Oznaczają posiadanie specyficznego rodzaju wiedzy wykorzystywanej we wszystkich sferach życia indywidualnego i społecznego do refleksyjnego podejmowania decyzji oraz stanowią podstawowy warsztat pracy dla specjalistów od zarządzania bezpieczeństwem informacyjnym. Bez kultury informacyjnej trudno jest kształtować kulturę bezpieczeństwa informacyjnego. Obie wzajemnie się przenikają i uzupełniają, żadnej z nich nie można analizować oddzielnie, przedmiotem obu jest człowiek funkcjonujący w przestrzeni informacyjnej, który może być przyczyną zagrożenia dla bezpieczeństwa informacji i infosfery, ale też sam wymaga ochrony przed niekorzystnym oddziaływaniem informacji i dychotomicznego → ś r o d o w i s k a i n f o r m a c y j n e g o [t. 4] (rzeczywistego i wirtualnego).

Komponentami kultury bezpieczeństwa informacyjnego są również kompetencje komunikacyjne, międzykulturowe, technologiczne, a także etyka informacyjna, prawo informacyjne, → e k o l o g i a i n f o r m a c j i, wychowanie do mass mediów i wychowanie do informacji, → p o l i t y k a i n f o r m a c y j n a [t. 3], profilaktyka informacyjna i inne.

Podsumowując, kultura bezpieczeństwa informacyjnego wymaga umiejętności

> skupiania się i poszukiwania odpowiedzi na pytania dotyczące tego, czy wykorzystywanie i posługiwanie się daną informacją, opieranie się na niej, będzie służyło bezpieczeństwu tego podmiotu i innych podmiotów: czy będzie pozytywnie oddziaływało na ich otoczenie, czy też będzie mogło powodować jego degradację […]

szczególnie w odniesieniu do obszaru wartości, norm i zasad. Wysoki poziom tej kultury A. Filipek łączy z nieobojętnością na inne wymiary przedmiotowych kultur bezpieczeństwa. W węższym znaczeniu kulturę bezpieczeństwa informacyjnego postrzega W. Józefowicz, tj. w kontekście wiedzy na temat kształtowania polityki bezpieczeństwa informacji, wyczulenia na nadużycia w tym przedmiocie i kształtowania zachowań pozwalających na ochronę informacji przed kradzieżą, deformacją, zniszczeniem, błędami ludzkimi i organizacyjnymi, awariami i skutkami katastrof oraz innymi atakami powodującymi zagrożenie prawidłowego funkcjonowania jednostki i grupy.

Odniesienie się do edukacji w zakresie kształtowania kultury bezpieczeństwa informacyjnego wynika z założenia części badaczy, że stanowi ona najskuteczniejszy sposób przeciwdziałania → z a g r o ż e n i o m b e z p i e c z e ń s t w a [t. 4] informacji rozumianego szeroko i wieloaspektowo jako bezpieczeństwo ludzi, zbiorów i zasobów informacji, danych i metadanych, usług informacyjnych i środowiska informacyjnego, w którym ludzie i systemy działają. Infosfera narażona na ciągłe świadome bądź nieświadome ataki, jako miejsce nieustannej walki informacyjnej, musi być chroniona przez system permanentnej edukacji całego społeczeństwa w zakresie bezpieczeństwa informacyjnego.

Zwracając uwagę na ekologię informacji, W. Babik proponuje podejmowanie działań praktycznych, polegających m.in. na:

> oparciu polityki informacyjnej na jej szerokim rozumieniu; dbaniu o świadomość informacyjną człowieka jako istotnego elementu w procesach informacyjnych; ochronie człowieka przed jego uprzedmiotawianiem za pomocą manipulacji informacją; rozwijaniu kompetencji informacyjnych; wychowaniu do odpowiedzialności za infosferę; równoważeniu rozwoju człowieka w świecie techniki, technologii i informacji; umiejętnym wykorzystywaniu informacji do budowania indywidualnej i zbiorowej wiedzy dla indywidualnego i wspólnego dobra ludzkości; zarządzaniu bezpieczeństwem informacji w środowisku informacyjnym człowieka.

Aby postulaty te zostały spełnione, konieczne jest dążenie do wychowania dojrzałych informacyjnie obywateli, bo tylko takie osoby są w stanie tworzyć kulturę bezpieczeństwa informacyjnego. Dojrzałość wymaga od nich refleksyjności, otwartości, racjonalności, odpowiedzialności, pracowitości, inteligencji, mądrości, generatywności, relatywizmu, mądrości, samokrytycyzmu i etyki. Dojrzałość informacyjna podmiotu jest warunkiem uzyskania nie tylko wysokiego poziomu kultury bezpieczeństwa informacyjnego, ale kultury bezpieczeństwa w ogóle. Edukację w tym zakresie należy traktować jako narzędzie umożliwiające świadome uczestnictwo w życiu społecznym oraz przygotowanie do odgrywania w nim obranej roli, jest więc środkiem w dążeniu do osiągnięcia wysokiego stopnia przystosowania społecznego i odpowiedzialności za rozwój i bezpieczeństwo przestrzeni, w której funkcjonuje.

Można stwierdzić, że obszarem zainteresowania kultury bezpieczeństwa informacyjnego są problemy:

- budowania świadomości bezpieczeństwa informacyjnego wśród społeczeństwa;
- pozyskiwania wiedzy o zagrożeniach generowanych przez cywilizację cyfrową;
- odpowiedzialności za utrzymywanie stanu bezpieczeństwa w infosferze;
- pielęgnowania wartości, na których można budować bezpieczeństwo jednostki i narodu;
- kształtowania postaw ludności wobec problemów bezpieczeństwa informacyjnego, ich emocji związanych z dążeniem do przeciwdziałania zagrożeniom i wzmacniania więzi;
- kształtowania zachowań, które sprzyjają budowaniu poczucia bezpieczeństwa informacyjnego i niwelowaniu stanów zagrożenia.

Należy przyjąć za Filipek, że kultura bezpieczeństwa informacyjnego jest związana z „opieraniem się na utrwalonym, akceptowanym, ogólnoludzkim systemie wartości w kwestii przekształcania rzeczywistości w oparciu o otrzymywane informacje". Oznacza to, że kompetencje podmiotu w zakresie rozumienia komunikatów, przetwarzania ich treści, analizy i interpretacji pozyskanych informacji, a następnie wykorzystania ich do podejmowania mądrych decyzji, wsparte procesami

zarządzania informacją i wiedzą oraz znajomością metod, technik i systemów zniekształcania informacji, działań manipulacyjnych, a także opór wobec nich, świadczą o dojrzałości informacyjnej człowieka, którą należy uznać za wyznacznik kultury bezpieczeństwa informacyjnego.

Hanna Batorowska

W. Babik, *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014; H. Batorowska, *Indywidualne zarządzanie informacją, zabezpieczeniem przed manipulacją w środowisku płynnej inwigilacji,* „Edukacja – Technika – Informatyka" 2018, nr 1; taż,, *Kultura bezpieczeństwa informacyjnego*, „Edukacja – Technika – Informatyka" 2018, nr 1; taż, *Kultura bezpieczeństwa informacyjnego*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2013; taż, *Wybrane problemy kultury bezpieczeństwa, kultury informacyjnej i bezpieczeństwa informacyjnego w refleksji nad funkcjonowaniem człowieka w świecie informacji*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*, t. 2, H. Batorowska, Z. Kwiasowski (red.), Wydawnictwo Uniwersytetu Pedagogicznego, Kraków 2016; M. Cieślarczyk, *Ekologia informacji, kultura informacyjna i kultura bezpieczeństwa informacyjnego w teorii i praktyce*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; tenże, *Kultura informacyjna jako element kultury bezpieczeństwa*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*, t. 1, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2015; tenże, *Kultura informacyjno-komunikacyjna a funkcjonowanie człowieka i grup społecznych w sytuacjach kryzysowych*, [w:] *Bezpieczeństwo człowieka a komunikacja społeczna*, t. 2: *Aspekty filozoficzne i polityczne*, E. Jarmocha, A. Świderski, I.A. Trzpil (red.), Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2011; A. Filipek, *Rola edukacji w kształtowaniu kultury bezpieczeństwa informacyjnego*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; W. Józefowicz, *Kształtowanie kultury bezpieczeństwa informacji*, „Wiedza Obronna" 2016, nr 1/2.

KULTURA BEZPIECZEŃSTWA NARODOWEGO – celnie nazywana przez J. Piwowarskiego „narodową kulturą bezpieczeństwa i mocy", co oznacza, że jest w niej siła, która jest w stanie uruchomić w narodzie

mechanizmy umożliwiające mu przetrwanie nawet w najbardziej trudnych warunkach, gdy siła ataku wroga przewyższa możliwości obronne zaatakowanego podmiotu. Przez kulturę tę badacz rozumie:

> trwały dorobek społeczeństwa zorganizowanego w państwo, będący przenikającymi się i wzmacniającymi nawzajem trzema strumieniami energii – mentalnym, społecznym i fizycznym (materialnym), […] który jest konieczny do utrzymywania bezpieczeństwa lub odzyskiwania go, kiedy zostanie utracone, oraz do podnoszenia go na wyższy poziom, zgodnie z aktualnymi potrzebami.

Autor proponuje powrót do „mocy obronności", która płynie z energii dostarczanej przez I i II strumień kultury bezpieczeństwa narodowego.

Konstatacja ta pozwala uznać, że →kultura bezpieczeństwa, zgodnie z koncepcją kultury bezpieczeństwa i obronności M. Cieślarczyka, umożliwia narodowi uodpornienie się na zewnętrzne i wewnętrzne →zagrożenia [t. 4] generowane przez środowisko, w którym żyje. Zyskaniu tej odporności (w rozumieniu czynnym, a nie pasywnym), czyli „aktywnego sposobu reagowania na pojawiające się zagrożenia", towarzyszyć powinna wrażliwość podmiotu pozwalająca mu na zapobieganie zagrożeniom i pomniejszanie ich skutków, utrzymanie godziwych warunków funkcjonowania w sytuacji powstałych zagrożeń oraz skuteczne zarządzanie odbudową po doznanych stratach. Wymaga to od podmiotu →bezpieczeństwa [t. 1] umiejętności radzenia sobie z ryzykiem i sprawności zarządzania nim. Brak kompetencji w tym zakresie sprawia, że jednostka nie łączy skutków podejmowanych decyzji i działań z poczuciem odpowiedzialności za nie i staje się źródłem generowania postaw zachowawczych i destrukcyjnych, a to stoi w opozycji do gotowości ponoszenia odpowiedzialności za siebie, innych i swoje otoczenie. Dlatego zadaniem kultury bezpieczeństwa jest:

> pobudzanie w społecznej i personalnej skali świadomości człowieka, przekonań o potrzebie ciągłego samodoskonalenia i trychotomicznego rozwoju oraz uaktywnienia motywacji i postaw

> skutkujących indywidualnymi i zespołowymi działaniami powodującymi komplementarny rozwój indywidualnych i grupowych podmiotów bezpieczeństwa, w tym ich autonomicznej obronności.

Kształtowanie w społeczeństwie podwyższonej wrażliwości i uważności na działania wymierzone w jego bezpieczeństwo oraz aktywnej odporności pozwalającej na przeciwstawienie się, złagodzenie i przezwyciężenie skutków zagrożenia odzwierciedla istotę pojęć kultury bezpieczeństwa i mocy oraz kultury bezpieczeństwa narodowego i mocy wprowadzonych do tezaurusa → n a u k o b e z p i e c z e ń s t w i e [t. 3] przez Piwowarskiego.

Odwołując się do prac badaczy takich jak K.R. Krause, N. Gnesotto, A. Wolfers, H. Plotkin czy M. Górka, wyeksponował w kulturze bezpieczeństwa narodowego (KBN) następujące elementy: tradycję, dzięki której można wyodrębnić i zrozumieć interesy i wartości wpływające na bezpieczeństwo państwa; integrację celów, narzędzi i środków służących do kreowania wspólnej polityki bezpieczeństwa; normy i wartości wspólne dla określonej społeczności; porozumienie zawarte w wybranej zbiorowości pozwalające na budowanie jednolitego myślenia i reagowania w ramach polityki bezpieczeństwa; ideę pokoju oznaczającą stabilną sytuację w państwie i stan braku obaw o utratę wartości (bądź ich zniszczenie), które są szczególnie ważne dla egzystencji człowieka.

Elementy te wskazują na wyjątkowe znaczenie czynnika mentalnego w kształtowaniu kultury bezpieczeństwa danego narodu. Chociaż w kulturze bezpieczeństwa Cieślarczyk dostrzega wagę wszystkich trzech strumieni jej siły (mentalnego, społecznego i materialnego), to jednak tylko pierwszy z nich może przesądzić o zwycięstwie narodu. Dlatego powinność narodu w zakresie pielęgnowania i przestrzegania reguł kulturowych oraz ponoszenia odpowiedzialności za podejmowane działania ma służyć ochronie „mocy bezpieczeństwa narodowego". Także J. Czaja uznaje, że właśnie sektor kulturowy KBN odpowiedzialny jest za stworzenie optymalnych warunków dla zachowania tożsamości kulturowej, ponieważ

> problem dla bezpieczeństwa narodowego pojawia się wtedy, gdy napływ nowych faktów i nowe zjawiska kulturowe negatywnie

wpływają, a nawet zagrażają tożsamości kulturowej społeczności lokalnych i narodowych, rodząc różne reakcje i postawy, z objawami wrogości wobec otoczenia międzynarodowego włącznie.

Tożsamość kulturowa nie oznacza tylko wspólnego pochodzenia grup czy narodów, ale głównie zespół wartości, reguł postępowania czy stylów życia łączących członków grupy. Stanowi newralgiczny punkt w systemie bezpieczeństwa państwa, ponieważ może być wykorzystywana do wzmacniania potencjału kraju poprzez kształtowanie silnego, spójnego narodu przygotowanego do obrony swojej tożsamości i → suwerenności [t. 4], albo stać się przedmiotem ataku wroga dążącego do uzyskania przewagi i pragnącego przejąć władzę.

Sytuacja ta wymaga od podmiotu bezpieczeństwa refleksyjności, dojrzałości informacyjnej i wysokiego poziomu → kultury informacyjnej, aby mógł on aktywnie uczestniczyć w działaniach na rzecz zachowania tożsamości narodowej. Aktywność podmiotu bezpieczeństwa łączy się z dokonywaniem przez niego właściwych wyborów zgodnych ze zdolnościami i możliwościami, wytrwałością w dążeniu do ich spełnienia i umiejętnościami wyrównywania strat. Nie można go uznać za dojrzałego informacyjnie, jeżeli w jego charakterystyce nie uwzględni się elementu kompetencji informacyjnych, poziomu tych kompetencji oraz jego kultury informacyjnej, będącej ważnym komponentem kultury bezpieczeństwa. Podstawowym elementem w jego edukacji musi być również wychowanie do → informacji i wychowanie dla refleksyjności, ograniczające pasywne zachowania podmiotów bezpieczeństwa w środowisku społecznym.

Trychotomiczne podejście do kultury bezpieczeństwa umożliwiło Cieślarczykowi wprowadzenie w obszar pojęcia terminów takich jak kultura informacyjna, kompetencje informacyjne, kultura komunikacyjna, → ekologia informacji, aby ukazać znaczenie sztuki komunikowania się jednostek i grup społecznych, znaczenie sprawnego obiegu informacji, wagę dążenia do → zrównoważonego rozwoju [t. 4] przez podmiot bezpieczeństwa i stosowania kompetencji informacyjno-komunikacyjnych w zarządzaniu bezpieczeństwem oraz sprawności informacyjnych w kształtowaniu kultury bezpieczeństwa i obronności podmiotów indywidualnych i zbiorowych.

Kultura bezpieczeństwa kształtująca w człowieku ideał człowieczeństwa, oparta na wartościach sprzyjających rozwijaniu tego ideału, wymaga jednak pielęgnacji i zaszczepienia jej kolejnym pokoleniom. Proces ten jest szczególnie ważny w czasach globalizmu, konsumpcjonizmu i technopolu. Nie bez powodu Piwowarski do zagrożeń, które negatywnie oddziałują na strumienie mocy narodowej kultury bezpieczeństwa, zalicza imperializm kulturowy, bezkrytyczny konformizm zwolenników globalizacji, szyderczy stosunek do wartości rodzinnych, patriotyzmu i duchowości. Przeciwstawienie się im widzi w systematycznej edukacji społeczeństwa w obszarze kultury bezpieczeństwa i w podnoszeniu poziomu świadomości narodowej mających na celu utrwalenie „mocnych mentalnie postaw". Jeżeli edukacja ta będzie prowadzona niewłaściwie, może być przyczyną groźnych dla rozwoju KBN zagrożeń i prowadzić do zachwiania ładu społecznego opartego na wspólnie wypracowanych przez pokolenia wartościach.

Kultura bezpieczeństwa utożsamiana z terminem kultury obronności, klimatu bezpieczeństwa lub securitologii koncentruje się zatem na człowieku, jego potrzebach, wyznawanych przez niego wartościach, przyjmowanych postawach i racjonalnych zachowaniach, aby mógł on systematycznie rozwiązywać problemy, z którymi musi się zmierzyć. Z kolei termin klimatu bezpieczeństwa, wprowadzony przez D. Zoharę do piśmiennictwa z zakresu securitologii, pokrywa się wprawdzie w obszarze przedmiotu i metod badawczych z terminem kultury bezpieczeństwa, ale w podejściu do problemów bezpieczeństwa w większym stopniu obejmuje aspekt psychologiczny.

Niewystarczające okazało się traktowanie kultury bezpieczeństwa wyłącznie z perspektywy działań obronnych, dlatego coraz więcej badaczy odchodzi od stosowania pojęcia kultury obronności wyłącznie w wymiarze militarnym i przypisuje mu rolę fundamentu, na którym można budować kulturę bezpieczeństwa.

Podsumowując, można odwołać się do sposobu ujmowania kultury bezpieczeństwa przez Piwowarskiego jako

> narzędzia badawczego, za pomocą którego bada się, np. charakter personalnego wymiaru kultury bezpieczeństwa narodowego u standardowego obywatela RP, regionalny wycinek rozmiarów i natury tego zjawiska czy wreszcie ocenia się całościowo poziom

oraz specyfikę społeczną kultury bezpieczeństwa narodowego w danym kraju.

Kultura bezpieczeństwa traktowana jest przez badacza jako model poznawczy, w przeciwieństwie do kultury bezpieczeństwa narodowego przyjmującego wymiar podmiotowy (obywatel, grupa społeczna, naród i jego państwo). KBN tworzoną przez państwo narodowe łączy on z przekonaniami, systemem wartości, postawami, obyczajami i fizycznymi efektami działań indywidualnych podmiotów przypisanych do danego narodu. Oznacza to, że KBN ma wymiar personalny i analizować należy ją z perspektywy człowieka, indywidualnego podmiotu bezpieczeństwa, jest kulturą tego podmiotu, wynikającą z kompetencji, które on nabył, oraz z jego indywidualnych cech oraz właściwości.

Ciekawym aspektem badań nad KBN jest podmiot bezpieczeństwa funkcjonujący w →cyberprzestrzeni [t. 1], narażony na szereg nowych zagrożeń lub sam stanowiący zagrożenie dla innych użytkowników tej przestrzeni. K. Trochowska, analizując motywy, racjonalności oraz zachowania jednostek i grup związanych z →bezpieczeństwem narodowym [t. 1] i międzynarodowym w cyberprzestrzeni, charakteryzujące się określonymi postawami, normami, wartościami, zgodnie z którymi podejmują one ryzyko i wyzwania czy też wykorzystują powstające szanse, podjęła próbę zrozumienia ich aktywności oraz opracowania metody kształtowania ich postaw i zachowań, które byłyby pożądane ze względów bezpieczeństwa. Jest to trudne zadanie, ponieważ kształtowanie kultury bezpieczeństwa podmiotu w cyberprzestrzeni zdeterminowane jest zasadami, którymi się to środowisko rządzi, a z punktu widzenia bezpieczeństwa narodowego główne atrybuty i zalety cyberprzestrzeni są również jej najsłabszymi punktami oraz źródłami licznych zagrożeń i wyzwań.

Hanna Batorowska

H. Batorowska, *The Informatological Context of Safety Culture*, „Przegląd Biblioteczny" 2019, wyd. spec.; taż, *Przeciążenie informacyjne wyzwaniem dla kształtowania kultury bezpieczeństwa*, [w:] *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*, H. Batorowska, P. Motylińska (red.), Wydawnictwo SBP, Warszawa 2020; M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*,

Wydawnictwo Akademii Podlaskiej, Siedlce 2006; tenże, *Ekologia informacji, kultura informacyjna i kultura bezpieczeństwa informacyjnego w teorii i praktyce*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; M. Cieślarczyk, A. Filipek, A.W. Świderski, J. Ważniewska, *Teoretyczne aspekty badania kultury bezpieczeństwa i systemu zarządzania kryzysowego*, „Kultura Bezpieczeństwa" 2014, nr 1–2; J. Czaja, *Kulturowy wymiar bezpieczeństwa. Aspekty teoretyczne i praktyczne*, Oficyna Wydawnicza AFM, Kraków 2013; J. Gierszewski, M. Kubiak, *Kultura bezpieczeństwa w teorii i praktyce*, Wydawnictwo Adam Marszałek, Toruń 2019; M. Górka, *Kultura bezpieczeństwa w kontekście znaczenia informacji jako elementu społeczno-kulturowego*, „Przegląd Politologiczny" 2018, nr 2; M. Lutostański, *Istota i rola kultury bezpieczeństwa w zarządzaniu bezpieczeństwem narodu i państwa*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 2: *Bezpieczeństwo i kultura bezpieczeństwa w teorii, w badaniach naukowych i w praktyce*, A. Filipek (red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2014; A. Pieczywok, *Kultura bezpieczeństwa człowieka i jej zagrożenia*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 2: *Bezpieczeństwo i kultura bezpieczeństwa w teorii, w badaniach naukowych i w praktyce*, A. Filipek (red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2014; J. Piwowarski, *Koncepcja zrównoważonego rozwoju jako ważny element kultury bezpieczeństwa w erze globalizacji*, [w:] *Wojna, etyka, kultura*, C. Kalita, S. Topolewski (red.), ASPRA-JR, Siedlce–Warszawa 2019; tenże, *Nauki o bezpieczeństwie. Między kulturą bezpieczeństwa a studiami bezpieczeństwa*, Difin, Warszawa 2018; tenże, *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*, Wydawnictwo Akademii Pomorskiej, Słupsk 2016; tenże, *Podstawowe kategorie nauk o bezpieczeństwie*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 4: *Odkrywanie znaczeń w naukach o bezpieczeństwie*, A. Filipek (red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2015; K. Trochowska, *Kultura bezpieczeństwa narodowego w cyberprzestrzeni – wprowadzenie*, „Kultura Bezpieczeństwa" 2016, nr 5.

KULTURA INFORMACJI I KULTURA INFORMACYJNA – pojęcia często używane zamiennie, obok utożsamianego z nimi terminu kultury informatycznej oraz terminu kompetencji informacyjnych (ang. *information literacy*). Najczęściej badacze posługują się pojęciem kultury informacyjnej, rozumiejąc przez nie zarówno sferę aktywności człowieka

wchodzącego w różne relacje z →informacją, jak i dążenie przez niego do osiągnięcia dojrzałości informacyjnej.

Rozróżnienia tych pojęć podjęła się M. Kisilowska, proponując, aby dla określenia sposobu świadomego i aktywnego funkcjonowania człowieka w →środowisku informacyjnym [t. 4] (→infosferze) oraz opisu konsekwencji funkcjonowania w nim używać pojęcia kultury informacji. Jak zakłada autorka, świadome funkcjonowanie w cywilizacji technicznej wymaga posiadania, rozwijania i zdobywania coraz to nowych kompetencji informacyjnych, korzystania z dostępnej oferty i aktywnej postawy polegającej na inicjowaniu działań i współtworzeniu środowiska informacyjnego. Kulturę informacji rozumie jako tworzenie się pewnej kultury wokół zjawiska, jakim jest informacja, w analogii do terminów kultury pisma, kultury druku, kultury książki itp., formę przymiotnikową – kultura informacyjna – łączy się z kompetencyjnym charakterem i posiadaniem wybranych umiejętności przez członków tej kultury informacji. Kultura informacji jest więc kulturą ludzi funkcjonujących w →przestrzeni informacyjnej [t. 3], bez narzucania im żadnych barier normatywnych i wartościującego charakteru ich kompetencji informacyjnych. To kultura, w której ludzie wypracowują zasady funkcjonowania w niej, co jest naturalnym efektem przebywania i korzystania z przestrzeni i obiektów informacyjnych, określa więc osiągnięty poziom rozwoju społeczeństwa, dla którego informacja odgrywa wyjątkową rolę i ma fundamentalne znaczenie.

Kultura informacyjna jest zawsze ściśle związana z użytkownikiem informacji oraz otoczeniem, w którym jednostka funkcjonuje oraz rozwija pożądane zachowania informacyjne, a jej kształtowanie powinno zakończyć się pozyskaniem przez zdolności do racjonalnego, efektywnego i etycznego funkcjonowania w →społeczeństwie informacyjnym [t. 4], a zatem oczekuje się od reprezentantów tej kultury odpowiednich postaw i zachowań. Dlatego, definiując kulturę informacyjną, zwraca się szczególną uwagę na ograniczenia normatywne, ustalając, że

> kultura informacyjna to sfera aktywności człowieka kształtowana przez jego świadomość informacyjną, wartości wspierające potrzebę alfabetyzacji informacyjnej, postawy emitujące

> zachowania charakterystyczne dla dojrzałych informacyjnie użytkowników, wynikające z oddziaływania na siebie wymienionych komponentów kultury. Zachowania te powstałe pod wpływem bodźców motywacyjnych i kompetencji informacyjnych oceniane są w procesie tworzenia wiedzy pozytywnie, będąc równocześnie podporządkowanymi społecznym wzorom opartym na etyce korzystania z informacji. Odnoszą się do przedmiotów i innych wytworów związanych z działalnością informacyjną lub uczestnictwem w procesie informacyjnym.

Kultura informacyjna człowieka odnosi się do jego kompetencji informacyjnych, ale rozumianych jako proces przygotowywania jednostki do racjonalnego funkcjonowania w społeczeństwie informacyjnym, oparty na edukacji i wychowaniu informacyjnym. Kompetencje informacyjne przyczyniają się bowiem do pobudzenia aktywności społecznej ludzi i są sumą ich umiejętności informacyjnych oraz postaw, jakie reprezentują wobec informacji, jej narzędzi i technologii.

Warto mieć świadomość, że obszar badań nad kulturą informacyjną na przełomie XX i XXI w. koncentrował się wokół teoretycznych zagadnień związanych z kompetencjami informacyjnymi i ich systematyką oraz w kręgu działań związanych z wypracowaniem metod zmierzających do efektywnego propagowania kultury informacji w społeczeństwie. C. Basili zjawisko kompetencji informacyjnych proponowała traktować w perspektywie nauki o informacji jako przejaw kultury informacyjnej, w perspektywie społeczno-politycznej jako swoisty cel polityki edukacyjnej, a w perspektywie kognitywnej jako specyficzny rodzaj indywidualnych kompetencji. Kompetencje informacyjne oznaczały zatem albo proces kształcenia umiejętności informacyjnych oraz rozpowszechniania ich znaczenia w społeczeństwie, aby osiągnęło ono minimalny poziom sprawności w zakresie wyszukiwania, ewaluacji i wykorzystywania informacji pochodzących z różnych źródeł, albo status będący rezultatem tego procesu, czyli stan bycia kompetentnym informacyjnie, tj. posiadania kompetencji do wyszukiwania, ewaluacji i wykorzystywania informacji.

Obecnie takie podejście jest niewystarczające, ponieważ kultura informacyjna stała się przedmiotem zainteresowania wielu dyscyplin,

które włączają ją jako istotny komponent do przedmiotu własnych badań. Funkcjonuje np. pojęcie kultury informacyjnej w kontekście szeroko rozumianej kultury, której głównym obszarem zainteresowania jest funkcjonowanie człowieka w cywilizacji cyfrowej, w świecie ryzyka i katastrof, w świecie o zaburzonym społecznym ładzie informacyjnym i zaburzonej równowadze pomiędzy podmiotowością a przedmiotowością jednostki. Łączy się ją ze →społeczeństwem sieci [t. 4] dostrzegającym znaczenie refleksji nad naturą samej informacji, jej kontekstem społecznym, filozoficznym, etycznym, politycznym, ekonomicznym, technicznym, kulturowym. Uznaje się kulturę informacyjną za nieodzowny czynnik postępu społecznego, drogę do wolności politycznej, poprawy jakości życia i ludzkiego szczęścia. T. Piątek definiuje ją jako:

> poziom rozwoju społeczeństwa w danej epoce historycznej uwarunkowany stopniem opanowania sił przyrody, osiągniętym stanem wiedzy i twórczości artystycznej oraz formami współżycia społecznego z wykorzystaniem technologii informacyjnych.

Z kolei B. Stefanowicz określa ją jako:

> wiedzę, nawyki i umiejętności odnoszące się do informacji traktowanej jako składnik rzeczywistości otaczającej człowieka, równie ważny jak materia i energia, jako czynnik wpływający na zachowania i osiągnięcia zarówno pojedynczych ludzi, jak i całych społeczeństw.

Przeniesienie akcentu na te elementy kultury informacyjnej, które odnoszą się do szeroko pojmowanej wiedzy na temat istoty informacji i jej funkcji oraz umiejętności informacyjnych, a także na →świadomość informacyjną [t. 4], pozwoliło badaczowi przedstawić strukturę kultury informacyjnej obejmującej kulturę myśli, kulturę języka i kulturę czynu, pozwalających na interpretację otaczającej rzeczywistości, wyrażanie myśli i kształtowanie postaw wobec informacji i związanych z nimi procesów i technologii informacyjnych. Doceniając znaczenie kształtowania kultury informacyjnej dla potrzeb demokracji i społeczeństw

obywatelskich, warto odwołać się do 4 imperatywów tej kultury sformułowanych przez Stefanowicza. Wskazują one, że:

- kultura informacyjna wymaga systemowego kształtowania świadomości jej roli i znaczenia w społeczeństwie, co wynika z przypisywanych jej cech i funkcji społecznych, w którym tworzy ona porządek społeczny, gwarantuje ciągłość społeczeństwa dzięki przyjętemu systemowi wartości i zasadom współżycia społecznego,
- kultura informacyjna zakłada myślenie informacyjne, to dbałość o prawdę i tylko prawdę,
- kultura informacyjna zakłada nieustanny proces rozwijania wiedzy o informacji w konfrontacji z działalnością człowieka funkcjonującego w społeczeństwie informacyjnym,
- kultura informacyjna wymaga jej kształtowania na każdym etapie życia współczesnego człowieka, poczynając od edukacji szkolnej.

Problematyka kultury informacyjnej jest więc związana bardziej z problematyką funkcjonowania społeczeństwa w ogólności, społeczeństwa o określonej kulturze, strukturze społecznej, systemie wartości, gospodarce, infrastrukturze technologiczno-informacyjnej itd. Wynika z tego, że odnoszące się do człowieka pojęcie kultury informacyjnej przenoszone jest na kraj, obszar lub inne obiekty, niebędące podmiotami. Dlatego Kisilowska zaproponowała wprowadzenie pojęcia kultury informacji, podobnie jak na gruncie badań francuskich zrobił to C. Baltz.

W świadomości społeczeństwa polskiego termin kompetencji informacyjnych nadal utożsamiany jest wyłącznie z elementarnymi umiejętnościami wyszukiwania informacji lub ze szkoleniem tych umiejętności, podczas gdy w literaturze światowej, głównie amerykańskiej, angielskiej i australijskiej, już dawno zyskał rangę dyscypliny. F. Machlup i U. Mansfield akcentują związek kultury informacyjnej z polami badawczymi dyscyplin takich jak nauki kognitywne, nauka o informacji i komputerach, →sztuczna inteligencja [t. 4], lingwistyka, bibliotekoznawstwo i informacja naukowa, cybernetyka, teoria informacji, teoria matematyki czy teoria systemów. Nie ograniczają zatem kultury informacyjnej do zagadnień użycia narzędzi informacji i szkolenia użytkowników w zakresie praktycznych umiejętności korzystania ze źródeł informacji. J.J. Shapiro i S.K. Hughes podążają dalej, zaliczając kompetencje informacyjne do

sztuk wyzwolonych, które dostarczają wiedzy nie tylko na temat tego, co i jak stosować, ale też dlaczego. Kulturę informacyjną łączą zatem z wiedzą o informacji i korzystaniu z niej, z umiejętnością dostrzegania społecznych, kulturowych i filozoficznych kontekstów korzystania z informacji, z refleksją nad kompetencjami informacyjnymi jako całością i wielowymiarową filozofią. Tak ujmowane zagadnienie według badaczy gwarantuje przygotowanie ludzi do funkcjonowania w społeczeństwie informacyjnym i jest podstawą ich humanistycznego wychowania. Służy także postępowi społecznemu i przeciwdziała procesowi wykluczenia społecznego.

Kompetencje informacyjne przyczyniają się do pobudzania aktywności społecznej ludzi, rozumienia idei kształcenia przez całe życie, uczenia się, aby wiedzieć, walki z wykluczeniem informacyjnym, → przeciążeniem informacyjnym [t. 3], smogiem informacyjnym itd. Zagraniczni teoretycy i praktycy problemów kultury informacyjnej są zgodni, że odpowiedzialność za rozwój świadomości informacyjnej obywateli ponosi rząd i to on kompetencje informacyjne winien uznać za priorytetowy cel polityki edukacyjnej i komponent polityki informacyjnej państwa. Jakość edukacji zależy nie tylko od inwestycji w technologie, ale głównie w programy edukacji informacyjnej rozwijającej kulturę informacyjną. Powinno się ją łączyć z dynamicznym procesem umożliwiającym doskonalenie intelektualnych zdolności użytkowników informacji, z działaniami, których celem jest wyposażenie ich w narzędzia i kompetencje konieczne do tworzenia wiedzy, a także umożliwienie im zwiększonej aktywności we wszystkich sferach życia (socjalizacja informacji) poprzez rozwój świadomości informacyjnej jednostki i całych społeczności. W porównaniu z dorobkiem światowym polska literatura poświęcona zagadnieniom teoretycznym kultury informacyjnej jest mniej imponująca. Tematyka ta początkowo dostrzeżona została przez badaczy interesujących się nauką o informacji, ekonomią, informatyką, techniką, pedagogiką i psychologią. Obecnie kultura informacyjna obejmuje pola badań różnych dyscyplin naukowych podejmujących rozważania nad współczesnymi zjawiskami informacyjnymi. Stała się ona przedmiotem zainteresowania także → nauk o bezpieczeństwie [t. 3].

Badacze problemów → kultury bezpieczeństwa traktują kulturę informacyjną jako integralny jej komponent, równie ważny jak

kultura organizacyjna i kultura komunikacyjna. Kształtowanie kultury bezpieczeństwa bez dbałości o kulturę informacyjną może nie przynieść oczekiwanych efektów i musi być połączone z podnoszeniem poziomu kultury informacyjnej wszystkich grup społecznych i zawodowych w kraju. Wysoki poziom kultury informacyjnej i →kultury bezpieczeństwa informacyjnego sprzyja osiąganiu poczucia podmiotowości i służy kształtowaniu się przekonania o wpływie tych czynników na jakość życia człowieka oraz na wyższy poziom jego bezpieczeństwa w wymiarze obiektywnym i subiektywnym.

W literaturze przedmiotu wskazuje się na ścisły związek kultury informacyjnej jednostki z bezpieczeństwem społecznym. Bezpieczeństwo to zależy w dużym stopniu od świadomości informacyjnej społeczeństwa, a tę należy rozwijać w procesie edukacji permanentnej. Wiedza i umiejętności związane ze sprawnym uczestniczeniem w procesie informacyjnym, a szczególnie możliwość dostępu do potrzebnej informacji we właściwym czasie, zapewnia jednostce i grupom nie tylko przewagę w dążeniu do władzy i dóbr materialnych, ale i bezpieczeństwo. Cenna jest tylko ta informacja, która charakteryzuje się wysoką jakością, jest dobrze chroniona i ma wartość strategiczną. Taką informację należy zabezpieczyć przed →zagrożeniami [t. 4] związanymi z nieuprawnionymi działaniami ludzi, z błędami ludzkimi i organizacyjnymi, ze skutkami katastrof i działań terrorystycznych, z awariami sprzętu i wadami oprogramowania. Dążenie do bezpieczeństwa wymaga wykształcenia kultury bezpieczeństwa, w tym zagwarantowania takiego poziomu kultury informacyjnej poszczególnych podmiotów, aby uniemożliwić jednej ze stron wykorzystanie przewagi kompetencyjnej w tym obszarze do osiągnięcia egoistycznych celów. M. Cieślarczyk twierdzi, że problematyka kultury bezpieczeństwa, a w niej kultury informacyjnej, zajmie należyte miejsce w systemie edukacji dopiero wtedy, gdy wiedza i konkretne fakty dotyczące walki i →wojny informacyjnej [t. 4] szerzej dotrą do świadomości obywateli. Wówczas model „piramidy bezpieczeństwa" budowany będzie na bazie bezpieczeństwa informacyjnego, w oparciu o które będą mogły rozwijać się kolejne, przedmiotowe obszary bezpieczeństwa, od ekologicznego i zdrowotnego, przez ekonomiczny po polityczny i kulturowy.

Tylko interdyscyplinarne spojrzenie na istotę kultury informacyjnej może pozwolić na zrozumienie roli, jaką odgrywa ona w zglobalizowanym świecie. Definicje kultury informacyjnej eksponują świadomy sposób i aktywne funkcjonowanie człowieka w środowisku informacyjnym i w cywilizacji technologicznej oraz przedstawiają konsekwencje takiego w nim funkcjonowania dla jednostki i grup społecznych. Kultura informacyjna jest kulturą osoby dojrzałej informacyjnie. Dojrzałość informacyjna jest więc środkiem w dążeniu do osiągnięcia wysokiego stopnia przystosowania społecznego. W świetle powyższego można przyjąć, że dojrzałość skłania się bardziej ku kulturze informacyjnej jednostki i jej samowychowaniu informacyjnemu niż kompetencjom informacyjnym i wykształceniu informacyjnemu. Osiągnięcie jej jest także jednym z gwarantów uzyskania przez podmiot pożądanego poziomu kultury bezpieczeństwa.

Hanna Batorowska

H. Batorowska, *Kultura informacyjna*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; taż, *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2013; taż, *Kultura informacyjna w perspektywie zmian w edukacji*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2009; taż, *Kultura informacyjna*, [w:] *Nauka o informacji*, W. Babik (red.), Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2016; taż, *Wpływ edukacji informacyjnej na jakość życia człowieka dorosłego*, „Praktyka i Teoria Informacji Naukowej i Technicznej" 2014, nr 2–3; taż, *Od edukacji informacyjnej ucznia do kultury informacyjnej człowieka dorosłego*, [w:] *Bibliotekarz 2.0. Nowoczesność na bazie tradycji*, S. Skórka, M. Rogoż, E. Piotrowska (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2015; taż, *Między dorosłością a dojrzałością informacyjną*, [w:] *Współczesne oblicza komunikacji i informacji. Problemy, badania, hipotezy*, E. Głowacka, M. Kowalska, P. Krysiński (red.), Wydawnictwo UMK, Toruń 2014; W. Babik, *Kultura informacyjna – spojrzenie z punktu widzenia ekologii informacji*, „Bibliotheca Nostra" 2012, nr 2 (28); M. Cieślarczyk, *Ekologia informacji, kultura informacji i kultura bezpieczeństwa informacyjnego w teorii i praktyce*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; tenże, *Kultura informacyjna jako element kultury bezpieczeństwa*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*, t. 1, H. Batorowska

(red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2015; tenże, *Kultura informacyjno-komunikacyjna a funkcjonowanie człowieka i grup społecznych w sytuacjach kryzysowych*, [w:] *Bezpieczeństwo człowieka a komunikacja społeczna*, t. 2: *Aspekty filozoficzne i polityczne*, E. Jarmocha, A. Świderski, I.A. Trzpil (red.), Wydawnictwo Naukowe UPH, Siedlce 2011; tenże, *Fenomen bezpieczeństwa i zjawisko kryzysów postrzegane w perspektywie kulturowej*, [w:] *Jedność i różnorodność. Kultura vs. kultury*, E. Rekłajtis, B. Wiśniewski, J. Zdanowski (red.), ASPRA-JR, Warszawa 2010; tenże, *Relacje między bezpieczeństwem i obronnością w kontekście wąskiego i szerokiego rozumienia tych zjawisk*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa. W poszukiwaniu relacji między bezpieczeństwem a obronnością*, J. Ważniewska (red.), Wydawnictwo Naukowe UPH, Siedlce 2017; W. Furmanek, *Kultura techniczna i kultura informacyjna. Eksplikacja pojęcia. Konsekwencje metodologiczne*, [w:] *Techniki komputerowe w przekazie edukacyjnym*, J. Morbitzer (red.), Wydawnictwo Naukowe AP, Kraków 2002; tenże, *Kultura informacyjna kategorią pedagogiki współczesnej*, [w:] *Nauka o wychowaniu w ponowoczesnym świecie*, „Chowanna" 2003, R. XLVI (LIX), t. 1 (20); S. Jaskuła, L. Korporowicz, *Kultura informacyjna w zarządzaniu międzykulturowym. Ujęcie transgresyjne*, [w:] *Kompetencje informacyjno-komunikacyjne i międzykulturowe w gospodarce. Od adaptacji do innowacji*, I. Sobieraj (red.), Wydawnictwo Naukowe Scholar, Warszawa 2012; M. Kisilowska, *Kultura informacji*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2016; B. Łukasik-Makowska, *Społeczny wymiar kultury informacyjnej*, [w:] *Koncepcje i narzędzia zarządzania informacją i wiedzą*, E. Niedzielska, K. Perechuda (red.), Wydawnictwo AE, Wrocław 2004; *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*, t. 1, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2015; *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*, t. 2, H. Batorowska, Z. Kwiasowski (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2016; T. Piątek, *Kultura informacyjna komponentem kwalifikacji kluczowych nauczyciela*, Wydawnictwo Oświatowe Foszcze, Rzeszów 2010; B. Stefanowicz, *Kultura informacyjna*, [w:] *Dydaktyka informatyki. Problemy teorii*, W. Furmanek, A. Piecuch (red.), Wydawnictwo UR, Rzeszów 2004; tenże, *Imperatywy kultury informacyjnej*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2015, nr 36 (863).

KULTURA STRATEGICZNA – pojęcie określające zasady zachowań wojskowych w stosunkach międzynarodowych przez poszczególne państwa, dotyczące kwestii takich jak decyzje o podjęciu działań zbrojnych, postrzeganie →zagrożenia [t. 4], sposób prowadzenia →wojny [t. 4],

dopuszczalna liczba ofiar, stosunek do wykorzystania nowych technologii czy zaufanie do sojuszników.

O wpływie kultury na prowadzenie działań wojennych pisał już Tukidydes w *Wojnie peloponeskiej*, wskazując różnice w podejmowaniu decyzji militarnych między Ateńczykami a Spartanami, mówił o tym także B.L. Hart, podkreślający istnienie narodowego (brytyjskiego) sposobu prowadzenia wojny. W XX w. pierwszym badaczem, który użył pojęcia kultury strategicznej, był J.L. Snyder w publikacji *The Soviet Strategic Culture: Implications for Limited Nuclear Operations* z 1977 r. Analizując → s t r a t e g i ę [t. 4] nuklearną USA i ZSRR, Snyder doszedł do wniosku, iż postęp techniczny w dziedzinie → b r o n i n u k l e a r n e j [t. 1] nie jest zasadniczym czynnikiem kształtującym strategię militarną. Jego zdaniem Związek Radziecki („człowiek radziecki") kieruje się odmienną logiką i kalkulacją strategiczną niż „człowiek racjonalny". Samo pojęcie kultury strategicznej zdefiniował z kolei jako: „sumę idei, uwarunkowanych emocjonalnie odpowiedzi i wzorców zwyczajowych zachowań, jakie członkowie narodowej wspólnoty bezpieczeństwa nabyli przez instrukcję lub imitację i podzielają w odniesieniu do strategii nuklearnej". Inny amerykański badacz, C.S. Grey, w książce *Modern Strategy* z 1999 r. opisał kulturę strategiczną jako:

> utrwalone, przekazywane społecznie idee, postawy, tradycje, zwyczaje i preferowane metody, które są mniej lub bardziej specyficzne dla określonej, umiejscowionej geograficznie wspólnoty bezpieczeństwa, cechującej się wyjątkowym doświadczeniem historycznym.

A. Johnston w artykule *Thinking about Strategic Culture* z 1995 r. przedstawił ją zaś jako:

> zintegrowany system symboli, który działa na rzecz ustanowienia dominujących i długotrwałych preferencji strategicznych poprzez sformułowanie koncepcji roli i skuteczności siły militarnej w międzynarodowych stosunkach politycznych i poprzez przybranie tych koncepcji w taką aurę faktyczności, że preferencje strategiczne wydają się unikalne, realistyczne i skuteczne.

W tym samym roku definicję kultury strategicznej przedstawił S. Rosen, wg którego są to:

> przekonania i założenia określające przyjmowane zasady zachowań wojskowych w stosunkach międzynarodowych, przede wszystkim dotyczące decyzji o podjęciu działań zbrojnych, preferencji co do sposobu prowadzenia wojny oraz dopuszczalnego podczas wojny poziomu ofiar.

W związku z pojawianiem się coraz większej liczby definicji kultury strategicznej Johnston zaproponował podział dotychczasowych badań prowadzonych nad kulturą strategiczną na pokolenia (generacje):

- pierwsza generacja badań nad kulturą strategiczną (przełom lat 70. i 80. XX w.),
- druga generacja badań nad kulturą strategiczną (lata 80. XX w.),
- trzecia generacja badań nad kulturą strategiczną (lata 90. XX w.),
- czwarta generacja badań nad kulturą strategiczną (pojawiła się na przełomie XX i XXI w., już po artykule Johnstona *Thinking about Strategic Culture* z 1995 r.).

Pierwsza generacja badań nad kulturą strategiczną koncentrowała się na kwestiach związanych ze strategią militarną USA i ZSSR, ze szczególnym uwzględnieniem broni atomowej. Naukowcy tacy jak Gray i D. Jones argumentowali, że różnice w strategii militarnej mocarstw wynikają z różnych doświadczeń historycznych, politycznych, kulturowych oraz położenia geograficznego. Druga generacja obejmowała badaczy (m.in. B. Kleina), którzy analizowali kulturę strategiczną jako narzędzie hegemonii w procesie podejmowania decyzji strategicznych oraz społeczną autoryzację użycia siły przez państwa w stosunkach międzynarodowych. Trzecia generacja postrzegała kulturę strategiczną jako zmienną niezależną wyjaśniającą zachowania państw w stosunkach międzynarodowych. W przeciwieństwie do dwóch poprzednich, trzecie pokolenie rozszerzyło pojmowanie kultury strategicznej z problematyki wojskowej na politykę międzynarodową. Z tego okresu pochodzi np. książka Johnstona *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. Do badaczy trzeciej generacji kultury strategicznej zaliczany

jest również I. Klein, autor *A Theory of Strategic Culture*. W efekcie obserwacji najnowszych publikacji poświęconych kulturze strategicznej, zdaniem niektórych badaczy, na przełomie XX i XXI w. pojawiła się czwarta generacja. Postrzega ona kulturę strategiczną jako zbiór subkultur w ramach danego państwa oraz ich wpływ na politykę zagraniczną i politykę obronną. Subkultury mogą powstawać wokół partii politycznych, instytucji wojskowych lub think tanków. Tworzą je profesjonaliści posiadający wiedzę z zakresu kultury strategicznej danego państwa oraz określone poglądy dotyczące roli i znaczenia tego państwa w stosunkach międzynarodowych.

Klasyfikacji kultury strategicznej podjął się również J. Glenn w artykule *Realism versus Strategic Culture: Competition and Collaboration*, która ukazała się w 2009 r. Autor wyróżnił w niej 4 koncepcje kultury strategicznej funkcjonujące w nauce o stosunkach międzynarodowych:

- epifenomenalną,
- konstruktywistyczną,
- poststrukturalistyczną,
- interpretatywistyczną.

W podejściu epifenomenalnym kultura strategiczna traktowana jest jako jeden z czynników kształtujących zachowanie się państw na arenie międzynarodowej. Orientacja ta przyjmuje główne założenia neorealizmu, a interpretacja kulturowa jest jedynie uzupełnieniem klasycznych nurtów analizy stosunków międzynarodowych. Przedstawiciele koncepcji epifenomenalnej koncentrują się, podobnie jak badacze pierwszej generacji badań nad kulturą strategiczną, na aspektach wojskowych – strategii militarnej, strategii → o d s t r a s z a n i a [t. 3] itp. Inne podejście charakteryzuje badaczy reprezentujących koncepcję konstruktywistyczną. Ich zdaniem kultura strategiczna nie jest wyłącznie jednym z zewnętrznych czynników oddziałujących na politykę zagraniczną i obronną państw, lecz ich bezpośrednią determinantą. Koncepcja poststrukturalistyczna jest zbliżona do drugiej generacji badań nad kulturą strategiczną. Wykorzystywana jest do legitymowania kierunku politycznego państwa, obieranego przez decydentów. Celem badaczy w ramach tej koncepcji nie jest prezentowanie stałych prawidłowości rządzących zachowaniem państw, lecz analizowanie każdego przykładu osobno.

Upadek ZSSR oraz klasyfikacje teoretyczne zaproponowane przez Glenna i Johnstona doprowadziły do dalszych dynamicznych badań nad kulturą strategiczną. C. Dryzd w artykule *Kultura strategiczna – geneza, definicja i praktyczne zastosowanie* przedstawił rolę kultury strategicznej w kontekście 3 funkcji poznawczych nauk:

- funkcji deskryptywnej,
- funkcji eksplanacyjnej,
- funkcji predykcyjnej.

Kultura strategiczna obejmuje wszystkie czynniki funkcjonowania państwa. Opisuje zarówno elementy →*hard power* (ustrój państwa, gospodarkę, system bezpieczeństwa), jak również soft power (→*soft power* [t. 4]) (historia państwa, kultura, typ społeczeństwa). Funkcja deskryptywna umożliwia porównanie poszczególnych czynników oraz wskazanie, który z nich ma znaczenie dominujące. Możliwe jest również poznanie ewolucji kultury strategicznej danego państwa, wpływu na nią czynników wewnętrznych oraz środowiska międzynarodowego. Funkcja eksplanacyjna pozwala wyjaśnić zachowanie się państwa w stosunkach międzynarodowych. Dzięki temu kultura strategiczna może być traktowana jako uzupełnienie lub alternatywa dla koncepcji reprezentowanych przez klasyczne teorie stosunków międzynarodowych. Funkcja predykcyjna z kolei może służyć do wychwytywania trendów i tendencji w ramach funkcjonowania danego państwa.

Spośród polskich badaczy na temat kultury strategicznej pisali m.in.: R. Wiśniewski, E. Olzacka, C. Dryzd, T. Wójtowicz, Ł. Smalec, ponadto J. Czaja w książce *Kulturowe czynniki bezpieczeństwa* czy K. Malinowski w pracy *Kultura bezpieczeństwa narodowego w Polsce i Niemczech*.

Badania prowadzone w tym obszarze pozwoliły udzielić odpowiedzi na szereg kluczowych pytań dotyczących polityki zagranicznej, polityki historycznej oraz polityki bezpieczeństwa Polski, takich jak powody nieufności Polski do sojuszników, ostrożność w obliczu współpracy rosyjsko-niemieckiej, wpływ tradycji insurekcyjnej na bieżącą politykę zagraniczną czy przyczyny dominacji tradycji romantycznej nad pozytywistyczną w polityce zagranicznej.

Tomasz Wójtowicz

J. Czaja, *Kulturowe czynniki bezpieczeństwa*, Krakowska Szkoła Wyższa im. Andrzeja Frycza Modrzewskiego, Kraków 2008; C. Dryzd, *Kultura strategiczna – geneza, definicja i praktyczne zastosowanie*, „Roczniki Studenckie Akademii Wojsk Lądowych" 2017, nr 1; C. Gray, *Modern Strategy*, Oxford University Press, Oxford 1999; A.I. Johnston, *Thinking About Strategic Culture*, „International Security" 1995, vol. 19, no. 4; T. Libel, *Explaining the Security Paradigm Shift: Strategic Culture, Epistemic Communities, and Israel's Changing National Security Policy*, „Defence Studies" 2016, vol. 16; K. Malinowski, *Kultura bezpieczeństwa narodowego w Polsce i Niemczech*, Instytut Zachodni, Poznań 2003; E. Olzacka, *Wojna a kultura. Nowożytna rewolucja militarna w Europie Zachodniej i Rosji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2016; J. Snyder, *The Soviet Strategic Culture*, Rand, Santa Monica 1977; R. Wiśniewski, *Kultura strategiczna, czyli o kulturowych uwarunkowaniach polityki zagranicznej i bezpieczeństwa*, „Przegląd Strategiczny" 2012, nr 1; T. Wójtowicz, *Kultura strategiczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Porównanie kultury strategicznej Stanów Zjednoczonych i Chińskiej Republiki Ludowej*, „Polityka i Społeczeństwo" 2018, nr 1 (16).

ISBN 978-83-66269-52-1

ISBN 978-83-66269-52-1

ENCYKLOPEDIA BEZPIECZEŃSTWA

TOM 2

ENCYKLOPEDIA
BEZPIECZEŃSTWA

TOM 2

D–K

REDAKCJA NAUKOWA
OLGA WASIUTA, SERGIUSZ WASIUTA

ENCYKLOPEDIA
BEZPIECZEŃSTWA

TOM 2
D–K

REDAKCJA NAUKOWA
OLGA WASIUTA, SERGIUSZ WASIUTA

ISBN 978-83-66269-52-1

Recenzenci:
prof. dr hab. Wojciech Jakubowski (Uniwersytet Warszawski)
prof. dr hab. Bogusław Pacek (Uniwersytet Jagielloński)

Redakcja:
Michał Pranke

Korekta:
Joanna Kłos

Projekt okładki i skład:
LIBRON

Publikacja s nansowana przez Uniwersytet Pedagogiczny
im. Komisji Edukacji Narodowej w Krakowie

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

Wykaz haseł

tom 1*

* Hasła na litery A–C i L–Ż znajdują się w osobnych tomach encyklopedii. Zob. *Encyklopedia bezpieczeństwa*, O. Wasiuta, S. Wasiuta (red.), t. 1, 3, 4, Wydawnictwo Libron, Kraków 2021.

Wykaz haseł

tom 2

tom 3

międzynarodowe prawo humanitarne kon iktów zbrojnych
międzynarodowe stosunki wojskowe
Międzynarodowy Trybunał Karny
Międzynarodowy Trybunał Sprawiedliwości
militarne działania nieregularne
militarne i niemilitarne metody prowadzenia wojny hybrydowej
militaryzacja przestrzeni kosmicznej
misja pokojowa
mobilizacja
morale
nacjonalizm
NATO
nauki o bezpieczeństwie
nawalizm
nawoływanie do popełnienia przestępstwa
negocjacje międzynarodowe
neokonserwatyzm
neonazizm
neutralność międzynarodowa
Niebieska Karta
obrona cywilna
obrona narodowa
obrona totalna
ochrona ludności
ochrona własności intelektualnej w sieci
ochrona zdrowia (system opieki zdrowotnej, system ochrony zdrowia)
oddziały cybernetyczne w Wojsku Polskim
odstraszanie
okno Overtona
okręt wojenny
operacje dezinformacji wojskowej
operacje propagandowe
operacje psychologiczne
opinia publiczna
Organizacja ds. Współpracy w Zakresie Uzbrojenia

tom 4

system obrony terytorialnej
System Państwowe Ratownictwo Medyczne
system powiadamiania ratunkowego
system zarządzania kryzysowego
System Zaufania Społecznego
sytuacja kryzysowa
szansa bezpieczeństwa
sztuczna inteligencja
sztuka wojenna
środki przymusu bezpośredniego i broń palna
środowisko bezpieczeństwa
środowisko cyberbezpieczeństwa
środowisko informacyjne
świadomość informacyjna
Światowa Komisja ds. Stabilności Cyberprzestrzeni
Światowa Organizacja Zdrowia
taktyczno-bojowa opieka nad poszkodowanym
technika wojskowa
technologie informacyjno-komunikacyjne
technowojna
teoria spiskowa
terroryzm
terroryzm a media
terroryzm islamski
ree Block War
totalitaryzm
triaż
trolle z Petersburga
trolling
Trybunał Sprawiedliwości UE
typologia zagrożeń
UNESCO
Unijny Mechanizm Ochrony Ludności
Urząd Ochrony Państwa
walka elektroniczna

D

Darknet (ciemna sieć) – część internetu najczęściej wiązana z pełną anonimowością i możliwością prowadzenia szeregu działań, w tym transakcji, które mają charakter nielegalny. W potocznych wyobrażeniach kojarzone z handlem bronią i narkotykami, pornografią dziecięcą i → przemocą [t. 3]*. Pojęcie darknetu zostało po raz pierwszy użyte w artykule P. Biddle'a, P. Englanda, M. Peinady i B. Willmana, pracowników korporacji Microsoft. W 2002 r. opublikowali opracowanie pt. *The Darknet and the Future of Content Distribution*, w którym przewidywali istnienie sieci typu darknet mających zwiększyć wygodę, przepustowość, wydajność i anonimowość w zakresie dzielenia się plikami. Choć wskazywali wówczas, że darknet może rodzić kontrowersje prawne, nie przewidzieli, w jakim kierunku będzie się rozwijać ten rodzaj aktywności w sieci.

W internecie – rozumianym jako globalny system sieci komputerowych, który obecnie rozszerzył się na inne urządzenia, takie jak smartfony i tablety – konieczne staje się wyróżnienie 2 warstw sieci: surface webu, zwanego też clearnetem, czyli internetu zindeksowanego lub inaczej

* Rozstrzelone słowa stanowią osobne hasła znajdujące się w *Encyklopedii bezpieczeństwa*. Oznaczenia „[t. 1]", „[t. 3]", „[t. 4]" informują, że hasło mieści się we wskazanych, odrębnych tomach encyklopedii.

powierzchniowego, oraz → deep webu, czyli ukrytej części sieci. Pierwsza z nich jest tym, co przeciętny użytkownik uważa za internet – zbiorem stron internetowych indeksowanych przez wyszukiwarki takie jak Google, Yahoo i Bing, do których to witryn można łatwo uzyskać dostęp za pomocą standardowych przeglądarek i protokołów internetowych. Choć można na nich odnaleźć ogromną ilość → informacji, to surface web jest tylko wierzchołkiem góry lodowej. Główną jej częścią pozostaje deep web. Jest to druga warstwa sieci, zdeniowana przez wymóg oddzielnego interfejsu potrzebnego do uzyskania dostępu do danych, ponieważ nie jest indeksowana. Wielu badaczy podkreśla, że ukryty internet jest znacznie większy niż internet zindeksowany. Z badań K. Finklei przeprowadzonych w 2017 r. wynika, że deep web jest większy ok. 4–5 tys. razy od internetu zindeksowanego. To właśnie w obszarze deep webu należy lokować → dark web oraz darknet, czyli ciemniejsze strony internetu.

W dyskusjach potocznych istnieje tendencja do traktowania pojęć „dark web" oraz „darknet" jako synonimów. Z technicznego punktu widzenia nie są one jednak tym samym. Cząstka „net" w wyrażeniu „darknet" pochodzi od słowa internet – globalnego systemu połączonych ze sobą sieci komputerowych. Z kolei słowo „web", skrót od World Wide Web, oznacza zestaw protokołów, które pozwalają korzystać z internetu, takich jak HTTP, TCP/IP czy UDP. Można je traktować jako rodzaj języka niezbędnego do tego, by wszystkie urządzenia mogły komunikować się ze sobą w ten sam sposób, aby proces przesyłania danych między nimi był skuteczny. Istnieje zatem wyraźna różnica pomiędzy darknetem a dark webem. Darknet to sieć komputerów, których zwykle nie można zobaczyć, a dark web to system, który pozwala na interakcję z nimi. Przykładami takich systemów są Tor lub Freenet, odpowiedniki usługi World Wide Web, umożliwiające korzystanie z ciemnej strony sieci.

Darknet jest niewielką częścią deep webu, do którego dostęp uzyskuje się za pomocą przeglądarek z maskowaniem tożsamości, takich jak e Onion Router (Tor), Freenet i I2P. Technologia zwiększająca poziom prywatności (ang. *privacy-enhancing technology* PET) wykorzystywana przez te przeglądarki zawdzięcza swoje początki amerykańskiemu laboratorium badawczemu → marynarki wojennej [t. 3] i Agencji Zaawansowanych Projektów Badawczych w Obszarze Obronności

(Defense Advanced Research Projects Agency, DARPA). PET i darknet zostały początkowo opracowane w celu ochrony internetowych komunikatów wywiadowczych USA przed zagranicznym nadzorem. Później zostały zmienione i wykorzystane przez The Tor Project do stworzenia platformy pozwalającej uniknąć monitorowania przez rządy i korporacje. Ze względu na silne szyfrowanie i wiele dostępnych technik maskowania tożsamości darknet jest używany przez cyberprzestępców.

Dostęp do darknetu może uzyskać każdy, kto zechce pobrać i zainstalować przeglądarkę Onion – np. Tor lub I2P. Jednak samo zainstalowanie przeglądarki typu Onion nie zapewnia anonimowości w darknecie. Usługodawca internetowy oraz instytucje nadzorujące korzystanie z sieci wiedzą, kiedy użytkownik korzysta z sieci takich jak Tor, chociaż niekoniecznie to, jakie treści przegląda. Właśnie dlatego niezbędne jest zwiększenie anonimowości użytkownika podczas korzystania z darknetu.

Wygląd przeglądarki typu Onion bazuje na popularnym, darmowym programie Mozilla Firefox. Cechą charakterystyczną adresów stron w tej sieci jest to, iż kończą się frazą *onion*. Jako przykłady takich adresów można podać następujące strony, które w 2014 r. zostały zamknięte przez FBI:

- sklepy narkotykowe: Blue Sky (blueskyplzv4fsti.onion), Hydra (hy-drampvvnunildl.onion), Pandora (pandora3uym4z42b.onion), Cloud Nine (xvqrvtnn4pbcnxwt.onion);
- sklep z bronią: Executive Outcomes (http://iczyaan7hzkyjown.onion);
- sklep z kartami kredytowymi: Fake Real Plastic (http://igvmwp3544wp nd6u.onion);
- sklep z fałszywymi dowodami osobistymi: Fake ID (http://23swqgocas65z7xz.onion);
- sklepy z fałszywymi banknotami: Fast Cash (http://5oulvdsnka55buw6.onion), Super Notes Counter, (http://67yjqewxrd2ewbtp.onion).

W przeglądarce poza możliwościami przeglądania specjalnej, kodowanej treści istnieje też możliwość przeglądania zwykłych, ogólnodostępnych stron internetowych. Dostęp do treści szyfrowanych nie zawsze jest możliwy, gdyż uzależnione jest to od tego, czy serwer z daną zawartością pozostaje włączony. Nie zawsze tak jest, ponieważ węzły komunikacyjne

zakładane są w dużej mierze przez osoby prywatne, zaś ich utrzymanie wiąże się z wysokimi kosztami. Sieci typu darknet działają znacznie wolniej niż zwykły internet, ponieważ możliwości przesyłu danych są ograniczone. Jest to także powodem, dla którego wygląd stron jest na ogół bardzo skromny, oszczędny w grafiki czy pliki filmowe, niejednokrotnie ograniczony tylko do tekstu. Ponadto węzły komunikacyjne najczęściej są tak zaprogramowane, aby domyślnie blokowały te sposoby wymiany i dystrybucji plików, które powodują zbyt duży przesył danych.

Tor jest bardzo popularną przeglądarką, której liczbę aktywnych użytkowników w styczniu 2018 r. oszacowano na 4 mln. Najwięcej jest ich w USA (19%), następnie w Rosji (11,9%), Niemczech (9,9%) i Zjednoczonych Emiratach Arabskich (9,2%).

Darknet jest używany do szerokiej gamy działań społecznych. Obejmują one formy aktywności od wyraźnie moralnie akceptowalnych, poprzez uznane za niedozwolone przez niektórych, aż po wyraźnie przestępcze w oparciu o krajowe lub międzynarodowe normy prawne. Działania te można podzielić na 3 główne kategorie:

> aktywizm, dziennikarstwo i informowanie o nieprawidłowościach;
> działalność przestępcza na wirtualnych rynkach;
> generowanie → zagrożenia bezpieczeństwa [t. 4] cybernetycznego, w tym tworzenie → botnetów [t. 1], → złośliwego oprogramowania [t. 4] i oprogramowania → ransomware [t. 3].

Anonimowość zapewniana przez darknet jest wykorzystywana do celów społecznych i politycznych. Użytkownicy mogą otwarcie dzielić się swoimi przekonaniami i wyrażać niezgodę na działania rządów lub oczekiwania wobec nich bez obawy o odwet. Ta możliwość nieskrępowanej afirmacji postaw jest szczególnie cenna w państwach o silnej → cenzurze [t. 1] państwowej i inwigilacji wobec działaczy politycznych, bojowników o wolność i dziennikarzy. Reporterzy, aktywiści i demaskatorzy w takich państwach mogą wykorzystywać darknet do komunikowania się ze światem zewnętrznym, zachęcać do zmian społecznych i reform politycznych, nie ujawniając swojej tożsamości. Prawie wszystkie organizacje tego typu zmierzają do prowadzenia elektronicznej wymiany informacji w bezpiecznych miejscach. Korzystanie z Tora jest zalecane przez Reporterów bez Granic – międzynarodową

organizację pozarządową propagującą i monitorującą wolność prasy na całym świecie – jako jeden z warunków przetrwania dziennikarzy i aktywistów pracujących w represyjnych państwach. Dobrym przykładem zastosowania Tora mogą być zamieszki w Egipcie, w czasie których dziennikarzom i aktywistom z całego świata udało się dzięki przeglądarce ominąć cenzurę rządu i skutecznie informować o bieżącej sytuacji. Sygnalizm, czyli zgłaszanie nieprawidłowości w działaniu państwa, jest aktem polegającym na działaniu ukierunkowanym na wyciekanie prywatnych informacji rządów lub firm do wiadomości publicznej. Pozostaje to zgodne z założeniem, że społeczeństwo ma prawo do informacji o działaniach zarówno swoich rządów, jak i dużych przedsiębiorstw. Niezależnie od tego w niektórych krajach wyciek prywatnych informacji z plików rządowych jest uważany za szkodliwy. Co więcej, wyciek informacji z firm jest nielegalny w niektórych krajach, np. w USA. E. Snowden, jeden z najbardziej znanych informatorów, ujawnił poufne informacje rządu Stanów Zjednoczonych – większość z nich dotyczyła NSA i armii amerykańskiej – za co został oskarżony na podstawie ustawy o szpiegostwie z 1917 r. Najprawdopodobniej do wysłania do wielu dziennikarzy tajnej informacji o amerykańskim programie szpiegowskim PRISM wykorzystał Tora.

Duża liczba wirtualnych rynków darknetu specjalizuje się w handlu nielegalnymi narkotykami. Skradzione tożsamości, informacje o kartach kredytowych, broń i morderstwa na zlecenie to także popularne „towary i usługi" w tej sieci. Model biznesowy jest podobny do rynku online eBay. Użytkownicy mogą zostawiać informacje zwrotne na temat produktów, a w celu ochrony sprzedawców i kupujących oraz rozwiązywania ewentualnych sporów został utworzony system o nazwie „escrow". Najczęściej spotykaną i gwarantującą największą anonimowość metodą płatności są bitcoiny. Są one jedną z wielu istniejących kryptowalut, rozproszonego systemu księgowości, który przechowuje informacje o stanie posiadania użytkownika w umownych jednostkach. Waluta przechowywana jest w portfelach, do których dostęp mają tylko ich użytkownicy, można ją wymieniać na zwykłe waluty zarówno elektronicznie na odpowiednich serwisach, jak i na gotówkę w specjalnych bankomatach.

Darknet jest także miejscem → zagrożeń [t. 4] cybernetycznych. Na niektórych rynkach przedmiotem obrotu są narzędzia hakerskie, które

mogą być bezpośrednio lub pośrednio wykorzystywane do atakowania rm lub osób. Twórcy szkodliwego oprogramowania wykorzystują darknet do komunikacji i wymiany pomysłów. Szkodliwe oprogramowanie ChewBacca wykorzystuje infrastrukturę Tora do uzyskiwania adresów IP swoich o ar i rejestrowania uderzeń klawiatury; z kolei złośliwe oprogramowanie i2Ninja jest znane z utrzymywania bezpiecznej komunikacji między zainfekowanymi urządzeniami a serwerem dowodzenia i kontroli poprzez ukrytą sieć I2P. Oprogramowanie ransomware uruchamia wirusy na zainfekowanych komputerach, szyfruje wszystkie dane, do których może uzyskać dostęp, a następnie żąda płatności w bitcoinach, aby uwolnić dane.

Ocena działania i funkcjonowania darknetu pozostaje niejednoznaczna. Anonimowe miejsce dyskusji, wymiany poglądów, protestów czy obywatelskiego buntu jawi się jako szczególnie wartościowe w dobie wszechobecnej kontroli państwa. Ciemna strona internetu jest jednak związana także z handlem ludźmi, bronią oraz pornogra ą dziecięcą. Z uwagi na anonimowość użytkowników darknetu ściganie działań niezgodnych z prawem jest tu o wiele trudniejsze niż w tradycyjnym internecie.

Jakub Idzik, Rafał Klepka

P. Biddle, P. England, M. Peinado i in., *e Darknet and the Future of Content Protection*, [w:] *Digital Rights Managment. DRM 2002*, J. Feigenbaum (ed.), Springer, Berlin–Heidelberg 2003; R. Broadhurst, D. Lord, D. Maxim i in., *Malware Trends on „Darknet" Crypto-markets: Research Review*, Australian National University, Cybercrime Observatory, Canberra 2018; J. Broséus, D. Rhumorbarbe, M. Morelato i in., *A Geographical Analysis of Tra cking on a Popular Darknet Market*, „Forensic Science International" 2017, vol. 277; K. Finklea, *Dark Web*, Congressional Research Service, 2017; L. Gayard, *Darknet: Geopolitics and Uses*, ISTE Ltd, Wiley, London–Hoboken 2018; J. Idzik, R. Klepka, *Darknet*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J. Kosiński, *Deepweb and Darknet – Police View*, referat wygłoszony na konferencji Archibald Reiss Days, Belgrad 2015; A. Krauz, *Mroczna strona internetu – TOR niebezpieczna forma cybertechnologii*, „Dydaktyka Informatyki" 2017, nr 12; M. Majorek, *Darknet. Ostatni bastion wolności w internecie?*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 4; M. Mirea, V. Wang, J. Jung, *e not so Dark Side of the Darknet: A Qualitative Study*, „Security Journal"

2019, vol. 32, no. 2; D. Moore, T. Rid, *Cryptopolitik and the Darknet*, „Survival Global Politics and Strategy" 2016, vol. 58, no. 1; H. Wojciechowski, *Darknet – wybrane aspekty kryminologiczne, kryminalistyczne i prawne szyfrowanych sieci komputerowych*, „Acta Universitatis Lodziensis. Folia Iuridica" 2018, nr 82.

Dark web (mroczna/ciemna sieć) – zbiór tysięcy stron internetowych, które istnieją w zaszyfrowanej sieci i nie można ich znaleźć lub odwiedzić przy użyciu tradycyjnych przeglądarek. Niektóre są publicznie widoczne, ale wykorzystują narzędzia anonimowości takie jak Tor i I2P, aby ukryć swój adres IP. Oznacza to, że każdy może odwiedzić witrynę sieci Web tego typu, ale ustalenie, gdzie jest ona hostowana – lub przez kogo – może być bardzo trudne. Dark web jest najczęściej używany do nielegalnych praktyk, np. sprzedaży narkotyków, broni palnej, pornogra i dziecięcej, umożliwia jednak również anonimowe informowanie o nieprawidłowościach i chroni użytkowników przed inwigilacją i → c e n z u r ą [t. 1].

W 2015 r. Komitet ds. Zwalczania Fałszerstw – organ jednej z Pod komisji Kongresu USA – przygotował raport *Fałszerstwo w Ciemnej Sieci* (*Anticounterfeiting on the Dark Web*), który opisał 3 części sieci interneto wej. Pierwsza z nich to *surfaceweb* – jest to część sieci znana większości użytkowników, składają się na nią wszystkie strony internetowe, które mogą być indeksowane przez typowe wyszukiwarki. Jako drugą część wyróżniono → d e e p w e b (głęboką sieć), czyli część internetu ukrytą przed konwencjonalnymi wyszukiwarkami np. poprzez szyfrowanie; zbiór nieindeksowanych stron internetowych; zawiera wszystko, do czego nie ma dostępu wyszukiwarka. Jako trzecią wskazano dark web – to mała część deep webu, która jest celowo ukryta i niedostępna dla standardo wych przeglądarek internetowych. Kiedy serwisy informacyjne błędnie opisują dark web jako 90% internetu, mylą go z deep webem – to ciemna sieć jest częścią głębokiej sieci. Deep web zawiera dark web, ale poza tym obejmuje również wszystkie bazy danych użytkowników, strony webmail, fora internetowe wymagające wcześniejszej rejestracji itp.

Większość stron dark webu korzysta z oprogramowania Tor, wywo dzącego się z amerykańskich prac badawczych w zakresie technologii obronnych. Jest ono zbudowane w oparciu o kod źródłowy popularnej przeglądarki Firefox zmody kowany tak, aby umożliwić użytkownikom

anonimowe przeglądanie sieci, blokując lub odradzając użytkownikowi czynności, które mogą ujawnić jego tożsamość (np. zmianę rozmiaru okna przeglądarki).

Oprogramowanie Tor szyfruje ruch sieciowy w warstwach i przekierowuje ten ruch dookoła sieci przez losowo wybrane komputery na całym świecie, z których każdy usuwa pojedynczą warstwę szyfrowania przed przekazaniem danych do następnego komputera w sieci. Teoretycznie uniemożliwia to szpiegom – nawet tym, którzy kontrolują jeden z tych komputerów w zaszyfrowanym łańcuchu – dopasowanie pochodzenia ruchu do miejsca przeznaczenia. Kiedy internauci uruchamiają przeglądarkę Tor, odwiedzane przez nich strony nie mogą łatwo zidentyfikować adresu IP użytkownika sieci. Tor zapewnia anonimowość także samym stronom internetowym i serwerom. Serwery skonfigurowane do odbierania połączeń przychodzących tylko przez Tor są nazywane „ukrytymi usługami". Aby odwiedzić witrynę w dark webie, która używa szyfrowania Tor, użytkownik sieci musi używać oprogramowania Tor. Tak jak adres IP użytkownika końcowego jest odbijany przez kilka warstw szyfrowania, aby wyglądać na inny adres IP w sieci Tor, tak też działa adres IP witryny. Dzięki temu strony w ciemnej sieci mogą być odwiedzane przez każdego, ale bardzo trudno jest ustalić, kto stoi za tymi witrynami. Przeglądarka Tor i witryny dostępne tylko dla niej są wykorzystywane przez użytkowników → darknetu i mogą być identyfikowane poprzez domenę (pseudodomenę) „.onion". Dostęp do dark webu jest możliwy z poziomu sieci darknet, składającej się z wielu rozproszonych, anonimowych węzłów.

Tożsamości i lokalizacje użytkowników darknetu pozostają anonimowe i nie można ich śledzić z powodu warstwowego systemu szyfrowania. Technologia szyfrowania darknetu kieruje dane użytkowników przez dużą liczbę pośrednich serwerów, co chroni tożsamość użytkowników i gwarantuje anonimowość. Przesyłane → informacje mogą zostać odszyfrowane tylko przez kolejny węzeł w schemacie, który prowadzi do węzła wyjściowego. Skomplikowany system uniemożliwia odtworzenie ścieżki węzła i odszyfrowanie informacji warstwa po warstwie. Ze względu na wysoki poziom szyfrowania strony internetowe nie są w stanie śledzić geolokalizacji i IP swoich użytkowników, a użytkownicy nie są w stanie uzyskać tych informacji o hoście. Komunikacja między użytkownikami

darknetu jest wysoce zaszyfrowana, co pozwala im na poufne porozumiewanie się, blogowanie i udostępnianie plików.

Gdy użytkownicy sieci uruchamiają Tora, wszystkie odwiedzane witryny nie mogą łatwo zobaczyć ich adresu IP. Ale strona internetowa, która sama uruchamia Tora – co jest znane jako usługa ukryta Tora – może być odwiedzana tylko przez użytkowników Tora. Fakt, że adresy IP tych witryn są ukryte, niekoniecznie oznacza jednak, że są one tajne. Ukryte usługi Tora, takie jak witryny sprzedaży narkotyków, miały setki tysięcy stałych użytkowników. W lipcu 2017 r. R. Dingledine, jeden z trzech założycieli projektu Tor, powiedział, że Facebook jest największą ukrytą usługą. Dark web zawiera tylko 3% ruchu w sieci Tor.

Nie wszystkie ciemne strony używają Tora. Niektóre korzystają z podobnego narzędzia o nazwie I2P (Invisible Internet Project), np. Silk Road (Jedwabny Szlak), który był globalnym rynkiem nielegalnych usług i przemytu, głównie narkotyków. Serwis został założony na początku 2011 r. i przez jakiś czas był najpopularniejszym spośród czarnorynkowych serwisów internetowych, z którym przez lata walczyły amerykańskie organy ścigania. Za jego pośrednictwem handlowano głównie narkotykami. Można było jednak kupić tam także broń czy zlecić zabójstwo. Z czasem Silk Road rozrósł się do ogromnych rozmiarów. Zaczęto go nazywać „narkotykowym Amazonem". Dostawcy nielegalnych substancji operowali w ponad 10 krajach na całym świecie. Od momentu uruchomienia witryny w styczniu 2011 r. ponad 100 tys. użytkowników wykorzystało ją do zakupu nielegalnych towarów, w tym narkotyków o wartości 1,2 mld USD. Szacuje się, że łączny przychód wyniósł 9,5 mln bitcoinów (wg średniego kursu z 2013 r. to równowartość ok. 3 mld USD). 2 października 2013 r., w bibliotece publicznej w San Francisco, agenci federalni zatrzymali administratora internetowego Silk Road, gdy był zalogowany do witryny za pośrednictwem tymczasowo zaszyfrowanego połączenia Tor, wykorzystując sieć WiFi biblioteki. Okazał się nim 29-letni R. Ulbricht, kryjący się pod pseudonimem DPR (Dread Pirate Roberts). Został oskarżony o pranie brudnych pieniędzy, piractwo komputerowe, umożliwienie handlu narkotykami oraz o zlecenie 6 zabójstw, w lutym 2015 r. został skazany na dożywocie w więzieniu za różne przestępstwa bez możliwości wcześniejszego zwolnienia.

W październiku 2013 r. została również zamknięta giełda, ale Silk Road (v. 2.0) reaktywowano w ciągu miesiąca od zamknięcia jego pierwszej odsłony. FBI potrzebowało kolejnego roku na odnalezienie kolejnego administratora i serwerów.

Na początku listopada 2014 r. skoordynowane działania FBI i → Europolu, znane jako operacja Onymous, zajęły dziesiątki ukrytych usług Tora, w tym 3 z 6 najpopularniejszych rynków narkotykowych w ciemnej sieci. Większość wymienianych towarów była nielegalna. Sposób, w jaki zlokalizowano te miejsca, pozostaje tajemnicą. Niektórzy analitycy → bezpieczeństwa spekulują, że rządowi → hakerzy wykorzystali tzw. ataki „odmowy usługi", które zalewają przekaźniki Tora niechcianymi danymi, aby zmusić witryny docelowe do korzystania z kontrolowanych przez nie przekaźników Tora, śledząc w ten sposób ich adresy IP. Mogli również zmienić administratorów w informatorów lub znaleźć inne podatne na atak luki w witrynach docelowych. Może to oznaczać, iż darknetowa implementacja sieci Tor zawiera kilka luk w zabezpieczeniach lub błędy w konfiguracji, które umożliwiają zdemaskowanie jej użytkowników. W 2016 r. specjaliści z firmy Intelliagg dokładniej sprawdzili, co kryje się w sieci Tor. Okazało się, że znajduje się tam maksymalnie 30 tys. stron o rozszerzeniu .onion (przypisanym do darknetu), ale tylko połowa z nich zawiera treści, które są zakazane prawem.

Dark web po raz pierwszy trafił na pierwsze strony gazet w sierpniu 2015 r., po tym jak doniesiono, że 10 GB danych skradzionych z Ashley Madison, serwisu randkowego i społecznościowego skierowanego do osób będących w związkach małżeńskich lub partnerskich, zostało umieszczonych w dark webie. Hakerzy ukradli dane i zagrozili, że przekażą je do sieci, jeśli witryna nie zostanie zamknięta. Później użytkownicy Ashley Madison otrzymali listy żądające zapłaty 2500 USD w bitcoinach lub ujawnienia niewierności. W ten sposób ciemna sieć wzbudziła ogromne zainteresowanie naukowców i rządów, starających się ujawnić tożsamość uczestników tych lukratywnych, ale nielegalnych rynków. Tradycyjne metodologie i techniki śledcze sprawdzające się w sieci okazały się nieudolne w demaskowaniu tych uczestników rynku.

W marcu 2015 r. rząd Wielkiej Brytanii uruchomił specjalną jednostkę ds. → cyberprzestępczości [t. 1], aby zająć się dark webem, ze

szczególnym naciskiem na zwalczanie poważnych przestępstw i pornografii dziecięcej. National Crime Agency (NCA) i brytyjski → wywiad [t. 4] Government Communications Headquarters (GCHQ) tworzą razem Joint Operations Cell (JOC).

Chociaż ciemna sieć jest najczęściej kojarzona ze sprzedażą narkotyków, broni, fałszywych dokumentów i pornografią dziecięcą – a wszystkie te mające swoich klientów branże rzeczywiście korzystają z usług Tora – nie wszystko w mrocznej sieci jest tak „ciemne". Dziennikarze korzystają z ciemnej sieci, aby chronić anonimowość swoich źródeł, a inni używają ciemnej sieci tylko dlatego, że mocno wierzą w swoje prawo do prywatności. Jedną z pierwszych wysokoprofilowych stron dark webu była usługa ukryta Tora stworzona przez WikiLeaks w celu akceptowania wycieków z anonimowych źródeł. Ten pomysł został od tego czasu dostosowany do narzędzia o nazwie SecureDrop, oprogramowania, które integruje się z ukrytymi usługami Tora, tak aby każda organizacja informacyjna mogła otrzymywać anonimowe zgłoszenia. Wielu aktywistów i dysydentów politycznych używa dark webu do swobodnego wyrażania swoich opinii lub jako sposób na wymianę i otrzymywanie informacji bez cenzury bądź kontroli. Sieć może służyć do ochrony urzędników przed identyfikacją i hakowaniem przez przeciwników. Może być też używana do prowadzenia tajnej lub ukrytej operacji sieci komputerowej, takiej jak likwidacja, atak typu „odmowa usługi" lub przechwycenie komunikacji. Nawet Facebook uruchomił wersję swojej strony w ciemnej sieci, aby „ułatwić dostęp do witryny z krajów, które ograniczają usługę, takich jak Chiny i Iran". Ma ona na celu lepszą obsługę użytkowników, którzy odwiedzają witrynę, używając Tora do unikania nadzoru i cenzury.

Olga Wasiuta

Anticounterfeiting Committee – U.S. Subcommittee Public Awareness Task Force, *Report: Anticounterfeiting on the Dark Web*, 13.04.2015, Inta.org (dostęp 31.07.2020); arma, *Did the FBI Pay a University to Attack Tor Users?*, 11.11.2015, Blog.TorProject.org (dostęp 31.07.2020); O. Catakoglu, M. Balduzzi, D. Balzarotti, *Attacks Landscape in the Dark Side of the Web* [w:] *Proceedings of the Symposium on Applied Computing*, ACM, New York 2017; M. Egan, *What is the Dark Web, What's on it*

& How to Access it, 25.10.2019, TechAdvisor.co.uk (dostęp 31.07.2020); K. Finklea, *Dark Web*, Congressional Research Service, 2017; A. Greenberg, *Hacker Lexicon: What Is the Dark Web?*, 19.11.2014, Wired.com (dostęp 31.07.2020); D. Hayes, J. Cardon, F. Cappa, *A Framework for More Effective Dark Web Marketplace Investigations*, „Information (Switzerland)" 2018, vol. 9, no. 186; G.F. Hurlburt, *Shining Light on the Dark Web*, „Computer" 2017, no. 50 (4); R. Jansen, T. Vaidya, M. Sherr, *Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor*, [w:] *Proceedings of the 28th USENIX Security Symposium*, USENIX Association, Berkeley 2019; T. Leżoń, *Darknet i deep web. Głęboko pod powierzchnią jest miejsce, o którym wołałbyś nie wiedzieć*, 27.04.2015, TVN24.pl (dostęp 31.07.2020); A. Nastiti, A. Wimmer, *Darknet, Social Media and Extremism: Addressing Indonesian Counter terrorism on the Internet*, „Deutsches Asienforschungszentrum Asian Series Commentaries" 2015, vol. 30; O. Wasiuta, *Dark Web*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J.M. Porup, *What is the Tor Browser? How It Works and how It Can Help You Protect Your Identity Online*, 12.07.2018, CSOOnline.com (dostęp 31.07.2020); T. Shim, *How to Access the Dark Web: Browsing Dark Web, TOR Browser, and .Onion Websites*, 10.04.2019, WebHostingSecretRevealed.net (dostęp 31.07.2020); J. Solomon, *The Deep Web Vs. The Dark Web*, 11.11.2015, Dictionary.com (dostęp 31.07.2020); M. Szpunar, *Imperializm kulturowy internetu*, Instytut Dziennikarstwa, Mediów i Komunikacji Społecznej Uniwersytetu Jagiellońskiego, Kraków 2017; M.P. Zillman, *Deep Web Research and Discovery Resources 2019*, 21.01.2019, LLRX.com (dostęp 31.07.2020).

Debunk (ang. demaskować, witryny: Debunk.eu, Demaskuok.lt w jęz. lit.) – to unikalna ogólnokrajowa litewska inicjatywa, która powstała w 2015 r., a jej celem jest monitorowanie i dementowanie → dezinformacji. Debunk łączy litewskie jednostki → komunikacji strategicznej i podmioty → społeczeństwa obywatelskiego [t. 4] – w tym media, dziennikarzy i wolontariuszy, a także podmioty biznesowe i medialne – w jednym celu: aby społeczeństwo było bardziej odporne na zorganizowane kampanie dezinformacyjne i ich obalanie, zanim fałszywe, wprowadzające w błąd lub niszczące zaufanie do państwa i jego demokratycznych instytucji informacje rozprzestrzenią się w kraju. Z inicjatywą współpracuje także litewska społeczność → elfów, naukowcy oraz doświadczeni informatycy. Wg organizatorów docierają one do 90% mieszkańców Litwy. Platforma jest krokiem w kierunku zwalczania wyzwań dezinformacyjnych z zagranicy,

jednak obserwatorzy twierdzą, że pomaga ona społeczeństwu radzić sobie z rosnącym strumieniem → informacji z samego kraju. Inicjatywa została sponsorowana i zrealizowana w ramach projektu Digital Innovation Foundation firmy Google oraz redakcji największego w regionie portalu informacyjnego Delfi Baltic. Na czele Debunk.eu stoi V. Daukšas.

Strona wykorzystuje zautomatyzowany system → sztucznej inteligencji [t. 4] do skanowania i analizy ok. 20 tys. artykułów dziennie w 3 językach w ciągu 2 minut od ich publikacji, w tym w mediach rosyjskich i litewskich, korzysta z ponad 1 tys. źródeł prasowych, biorąc pod uwagę podejrzane słowa kluczowe, zgłasza artykuły z określonymi słowami kluczowymi i wskazuje potencjalne źródło rozprzestrzeniania się dezinformacji, w tym również takich, że Litwa jest krajem upadłym lub jest ponownie zajęta przez → NATO [t. 3]. Wolontariusze filtrują treści oznaczone przez system, odczytują materiały i oceniają potencjalne → zagrożenie [t. 4]. Zgłoszone informacje docierają do dziennikarzy wraz z konkretnymi komentarzami i wiedzą wolontariuszy, którzy posiadają wiedzę na tematy poruszane przez → propagandę [t. 3], takie jak technologia, polityka lokalna i konflikt w Ukrainie. Inicjatywa Debunk.eu obnażyła np. nieprawdziwość doniesień o testach → broni biologicznej [t. 1] w krajach bałtyckich, obiektach pozaziemskich zestrzelonych na Litwie czy też fikcyjność historii → żołnierza [t. 4] NATO, który zabił rowerzystę.

Litewscy dziennikarze publikują analizy obnażające wyprodukowane przez rosyjskie media → fake newsy. Inicjatywa ta jest również otwarta dla czytelników portalu Delfi. Na głównej podstronie działu znajduje się formularz, w którym można zgłosić dany problem dziennikarzom lub poinformować o nowym fake newsie. Każdy użytkownik strony może sprawdzić, czy news, na który natknął się w sieci, został uznany za manipulację lub fake. Działanie witryny skupia się przede wszystkim na fake newsach istotnych z punktu widzenia państwa (a nie np. komercyjnych). Przykładami takich istotnych wiadomości mogą być fałszywe twierdzenia rosyjskich mediów państwowych o porwaniu 6 rosyjskich dzieci przez litewskie siły specjalne, aby zmusić rodziców do współpracy przeciwko Rosji, lub całkowicie nieprawdziwe informacje, wg których Łotwa wzniosła obozy koncentracyjne dla etnicznych Rosjan.

Liczba ludności rosyjskojęzycznej na Litwie wynosi zaledwie 6% ogółu, mniej niż w Estonii i na Łotwie. Jednak 8% ankietowanych Litwinów twierdzi, że poparło → aneksję [t. 1] Krymu. Ok. 97% ludzi ogląda tele wizję codziennie; z tej liczby 14% to odbiorcy rosyjskich stacji, z których wiele jest faktycznie zarejestrowanych w krajach europejskich i podlega przepisom UE dotyczącym transmisji. Popularność mediów rosyjskich jest większa wśród starszych pokoleń Litwinów, którzy dorastali z sowieckimi mediami i czują się lepiej, będąc informowani w swoim podstawowym języku. T. Kvedaras, attaché prasowy w litewskim Ministerstwie Spraw Zagranicznych, powiedział, że jego 85-letnia babcia nadal woli NTV lub Channel One od jakiejkolwiek stacji w języku litewskim.

Litwini starają się na różne wydarzenia reagować natychmiast. Kiedy na Litwie rosyjską firmę Lukoil przemianowano na Vijada, żeby zmylić społeczeństwo, w odpowiedzi natychmiast opublikowano i rozpowszechniono w → mediach społecznościowych [t. 3] zdjęcia z podpisem „To ta sama kakaszka, tylko z drugiej strony". Skuteczność takich memów była dość wysoka: dzięki humorowi można wiele przekazać społeczeństwu. Kiedy firma Adidas zaczęła produkować koszulki z symbolami ZSRR, Litwini uruchomili kampanię „Stop! Adidas", która okazała się bardzo udana, także w globalnej skali. W 19 krajach opublikowano 116 artykułów na ten temat, w tym 55 artykułów na Ukrainie, co zmusiło przedsiębiorstwo do oficjalnego zaprzestania takiej produkcji.

We wrześniu 2018 r. litewską inicjatywę Demaskuok.lt po raz pierwszy przedstawiono instytucjom i państwom członkowskim UE. Spotkanie z Europejską Służbą Działań Zewnętrznych i zagranicznymi dyplomatami odbyło się w Stałym Przedstawicielstwie Litwy przy UE w Brukseli. Skala problemu dezinformacji została również omówiona z europejską komisarz ds. gospodarki cyfrowej i społeczeństwa M. Gabriel. Podczas konferencji prasowej dla zagranicznych mediów lider inicjatywyDaukšas przedstawił inicjatywę Demaskuok.lt oraz możliwości zastosowania tego narzędzia w UE lub w poszczególnych krajach UE. Inicjatywa wzbudziła duże zainteresowanie instytucji UE i międzynarodowych mediów. We wnioskach uznano, że tylko wspólne media, działania pozarządowe i sektor publiczny tworzą dobrze poinformowane społeczeństwo, które może odnosić sukcesy w walce z dezinformacją.

Wykorzystując zasady niezależności, przejrzystości i skuteczności, Demaskuok.lt jest unikalną inicjatywą tego rodzaju nie tylko na Litwie, ale także prawdopodobnie na świecie. Inicjatywa krajowa Demaskuok.lt znalazła się w gronie nalistów konkursu zorganizowanego przez → Centrum Eksperckie NATO ds. Komunikacji Strategicznej [t. 1] i ambasadę USA pod koniec grudnia 2018 r. Debunk oferuje rozwiązania, które pomagają identy kować szkodliwą zawartość wideo i zdjęć używanych do rozpowszechniania dezinformacji w sieci. Do tej pory inicjatywa została już zaprezentowana w Brukseli dyplomatom państw UE, przedstawicielom biur Komisji Europejskiej i przedstawicielom NATO, została przedstawiona także w USA w 2018 r. przy okazji spotkań Rady Atlantyckiej.

Z pomocą elfów i unikalnych narzędzi opartych na algorytmach media mogą reagować na dezinformację i manipulację w czasie rzeczywistym i skutecznie. Rozwiązania stosowane przez Debunk.eu można aplikować zarówno w instytucjach litewskich, jak i międzynarodowych, automatyzując monitorowanie mediów, zmieniając fałszywe narracje i oceniając zakres rozpowszechnienia się dezinformacji, np. w kontekście nadchodzących wyborów do Parlamentu Europejskiego czy wyborów do parlamentów krajowych.

Litwa, podobnie jak inni sąsiedzi, ukształtowana przez komunistyczną dominację w czasach sowieckich, od dawna dążyła do twardego podejścia do dezinformacji zarówno w kraju, jak i na poziomie UE. → Strategia [t. 4] Wilna jest godna uwagi ze względu na sposób, w jaki opiera się na bliskiej współpracy między różnymi grupami w społeczeństwie, takimi jak media i wojsko.

Komisja Europejska zaproponowała przyjęcie wspólnego unijnego kodu dezinformacji, wsparcie dla niezależnej sieci wery katorów fak tograficznych i promowanie wysokiej jakości dziennikarstwa poprzez podniesienie umiejętności korzystania z mediów.

Sergiusz Wasiuta

Debunk, *Disinformation*, Debunk.eu (dostęp 10.03.2019); Embassy of the Republic of Lithuania to the United States of America and to the United Mexican States, *Lithuania shares its experience in countering disinformation*, 9.10.2018, USA.MFA.lt

(dostęp 10.03.2019); B. Gerdziunas, *Lithuania hits back at Russian disinformation* 27.09.2018, DW.com (dostęp 10.03.2019); Lrytas, *„Demaskuok.lt" – NATO konkurso nalę* 28.11.2018, Lrytas.lt (dostęp 10.03.2019); *Demaskuok.lt pristatyta Europos Komisijos atstovybėje*, 26.09.2018, Lrytas.lt (dostęp 10.03.2019); A. Kendall-Taylor, R. Rizzo, V. Daukšas, Giedrius, *Combatting Disinformation in Lithuania*, 19.10.2018, CNAS.org (dostęp 10.03.2019); S. Wasiuta, *Debunk*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

Deepfake (generowane komputerowo treści wideo, zbitka od ang. *deep learning* – głębokie uczenie – oraz *fake* – fałszywy) – to technika obróbki obrazów twarzy ludzkich oparta na działaniu → sztucznej inteligencji [t. 4]. Służy do zautomatyzowanego przez program komputerowy łączenia istniejących obrazów lub filmów oraz nakładania na siebie treści tak, aby w rezultacie wytworzyć przekonujące fotomontaże lub nagrania ze zmienionymi obrazami twarzy bohaterów. Technologia deepfake wykorzystuje sztuczną inteligencję do tworzenia lub modyfikowania odwzorowania twarzy, do tworzenia ultrarealistycznych fałszywych filmów, na których ludzie mówią i robią rzeczy, które w rzeczywistości nie się zdarzyły. Oprogramowanie do edycji zdjęć takie jak Photoshop od dawna było używane do fałszowania obrazów statycznych, jednak do niedawna trudno było edytować treści wideo bez użycia specjalistycznego oprogramowania, wysokich umiejętności i dużej ilości czasu. W związku z tym nagrania wideo często były uważane za dowód, że coś faktycznie się wydarzyło. Od innych technik manipulacji treściami wideo odróżnia deepfake jego potencjał do uzyskania wysoce realistycznych, przekonujących rezultatów.

Termin został utworzony od nazwy anonimowego użytkownika portalu Reddit o pseudonimie deepfakes, który w grudniu 2017 r. opublikował kilka filmów pornograficznych, na których twarze aktorek zostały podmienione na twarze celebrytek. Filmy typu deepfake są tworzone przez załadowanie do komputera złożonego zestawu instrukcji wraz z dużą ilością zdjęć i nagrań dźwiękowych. Następnie program komputerowy uczy się, jak naśladować i odtwarzać mimikę danej osoby, jej głos, ruchy, indywidualne maniery, intonację oraz rodzaj używanego słownictwa. Wystarczająca liczba filmów i zapisów dźwiękowych danej osoby umożliwia systemowi stworzenie nagrania z tą osobą. Bardzo często oszuści tworzący

materiały typu deepfake wykorzystują autentyczne nagrania, które łączą ze sztucznie wygenerowanym obrazem.

Nowa technologia pozwala każdemu stworzyć materiał wideo, w którym pojawiają się znane postaci, np. prezydent USA D. Trump czy wysocy rangą dyplomaci, wypowiadający się na kontrowersyjne tematy w sposób podburzający → opinię publiczną [t. 3]. Filmy typu deepfake zostały wykorzystane do fałszywego przedstawienia znanych polityków na portalach gromadzących treści wideo lub na czatach, np. twarz argentyńskiego prezydenta M. Macriego zastąpiła twarz A. Hitlera, w innym nagraniu twarz A. Merkel została zastąpiona twarzą Trumpa. W lipcu 2017 r. świat obiegł lmik, w którym B. Obama obrażał Trumpa. Okazało się, że byłego prezydenta USA wygenerowano w całości w aplikacji → FakeApp, a głosu użyczył mu komik J. Peele. Akcja miała na celu zwrócenie uwagi na problem fake newsów. W kwietniu 2018 r. Peele i J. Peretti stworzyli podróbkę, używając wizerunku Obamy do publicznego ogłoszenia o → zagrożeniach [t. 4] związanych z podróbkami.

W ostatnich latach technologia przetwarzania obrazu (aparaty cyfrowe, telefony komórkowe itp.) stała się wszechobecna, umożliwiając ludziom na całym świecie natychmiastowe wykonywanie zdjęć i tworzenie nagrań wideo. Odzwierciedleniem tego wzrostu liczby obrazów cyfrowych jest zdolność nawet stosunkowo niewykwali kowanych użytkowników do manipulowania i zniekształcania przekazu mediów wizualnych. Podczas gdy wiele manipulacji jest wykonywane dla zabawy lub dla wartości artystycznej, inne służą celom takim jak → propaganda [t. 3] lub → dezinformacja. Ta manipulacja multimediami wizualnymi jest możliwa dzięki szerokiej dostępności zaawansowanych aplikacji do edycji obrazu i wideo, a także dzięki zautomatyzowanym algorytmom umożliwiającym edycję w sposób bardzo trudny do wykrycia nieuzbrojonym okiem lub nawet poprzez analizę z wykorzystaniem specjalistycznych narzędzi. Słowo deepfake określa wykorzystanie algorytmów uczenia maszynowego i technologii mapowania twarzy do cyfrowej manipulacji głosami, ciałami i twarzami ludzi. Technologia rozwija się w tak dużym tempie, że coraz trudniej jest stwierdzić, co jest fałszywe. Z czasem, bez odpowiedniego sprzętu, lmy deepfake staną się nie do odróżnienia od prawdziwych zdjęć czy lmów. Deepfake'i mogą być wykorzystywane również

do tworzenia fałszywych wiadomości i złośliwych oszustw. Dysponując wystarczającą ilością obrazów obu aktorów i wystarczającą ilością czasu na szkolenie komputerowe, rezultaty mogą być niezwykle przekonujące. Filmy deepfake można zidenty kować na podstawie braku sygnałów zjologicznych właściwych człowiekowi: oddychania, mrugania oczami, braku widocznego pulsu.

Liderzy państw demokratycznych doceniają obecnie wagę problemu, jaki niesie ze sobą możliwość tworzenia treści, w których generowane komputerowo obrazy znanych postaci życia publicznego wypowiadają bulwersujące stwierdzenia i są nie do odróżnienia od prawdziwych osób. Materiały wideo tego rodzaju są potencjalnym zagrożeniem dla → b e z p i e c z e ń s t w a w e w n ę t r z n e g o [t. 1] każdego państwa, a także mogą stać się narzędziem wpływu na wybory. Kolejny sfabrykowany skandal może zagrozić → b e z p i e c z e ń s t w u n a r o d o w e m u [t. 1] lub wpły nąć na opinię publiczną, to pole do działania dla oszustów chcących in gerować np. w nastroje polityczne w społeczeństwie, a także nowa broń w → w o j n i e i n f o r m a c y j n e j [t. 4]. Technologia ta będzie narzędziem wykorzystywanym przez państwa w celu manipulowania opinią publiczną i przeprowadzania kampanii dezinformujących, a także podkopywania wiary w obecnie istniejące instytucje.

Masowa dostępność oprogramowania do tworzenia materiałów typu deepfake ma wiele niepokojących implikacji, które trudno ignorować. Dzięki tej technologii coraz trudniejsze będzie odróżnienie prawdy od kłamstwa. Technologia deepfake jest już szeroko stosowana w fałszywych lmach por nogra cznych i komediowych. Szybki postęp technologiczny może oznaczać jednak poważne konsekwencje. Realistyczne lmy deepfake można również wykorzystywać przy próbach szantażu, linkach → p h i s h i n g o w y c h [t. 3] i oszustwach służących wymuszeniu. Przy minimalnym nakładzie pracy mogą także dostarczać przestępcom narzędzi do tworzenia realistycznych, trudnych do wery kacji, przynajmniej bez dogłębnej analizy, nagrań wideo, na których osoby mogą podszywać się pod kogoś innego, prowadząc do oszustwa i unikając wyegzekwowania prawa. Mogłyby one zostać wyko rzystane np. do wplątania niewinnych ludzi w zbrodnie, a w postępowaniu cywilnym te sfałszowane lmy mogą być wykorzystywane do przeprowa dzania wszelkiego rodzaju oszukańczych roszczeń.

To narzędzie ma jednak znacznie większe możliwości, co właśnie wykorzystują Chińczycy. W listopadzie 2018 r. chińska państwowa telewizja Agencji Informacyjnej Xinhua stworzyła wygenerowanego komputerowo prezentera, który poprowadzi wieczorne wiadomości (jego sylwetka była wzorowana na pracowniku agencji, Z. Zhao). Xinhua planuje stworzenie mediów, które będą prowadzone na okrągło przez komputerowych prezenterów, a wiadomości widz będzie mógł usłyszeć w dowolnym języku. Treści, które ma przedstawiać cyfrowy prezenter, wprowadzane są do pamięci oprogramowania deepfake, a ruch jego warg jest synchronizowany ze słowami wypowiadanymi przez syntezator mowy. Stało się to, czego wielu obawiało się od dawna. Pierwszy raz w historii telewizji wiadomości ze świata relacjonuje prezenter, który został sztucznie wytworzony za pomocą technologii deepfake.

Technologia tworzenia zmanipulowanych wideo nie jest jeszcze doskonała i wytrawne oko dostrzeże mody kacje. Mechanizm konstruowania nagrań typu deepfake jednak cały czas się rozwija i za chwilę odbiorca być może nie zauważy, że materiał lmowy jest fałszywy.

W USA aktywnie rozwijana jest technologia służąca identy kacji lmów typu deepfake. Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (Defense Advanced Research Projects Agency, DARPA) rozpoczęła w 2016 r. projekt MediFor (ang. Media Forensics, media śledcze), którego celem jest opracowanie technologii do automatycznej oceny integralności zdjęć lub lmów i uczynienie jej częścią platformy wymiany materiałów pomiędzy użytkownikami końcowymi. W założeniach platforma MediFor automatycznie będzie wykrywać manipulacje, podawać szczegółowe informacje o tym, jak owe manipulacje zostały wykonane, a także oceniać ogólną integralność obrazów wizualnych, ułatwiając użytkownikom podjęcie decyzji o wykorzystaniu jakichkolwiek wątpliwych zdjęć lub lmów.

Opracowaniem oprogramowania do wery kacji autentyczności mediów zajmuje się także utworzona w 2017 r. amerykańska AI Foundation [t. 1]. Celem pierwszego produktu rmy o nazwie Reality Defender jest identy kowanie oszustw i złośliwej zawartości poprzez wykorzystanie uczenia maszynowego oraz ludzkiego umiarkowania i rozsądku. Naukowcy zapraszają użytkowników do wysyłania im fałszywych materiałów do

tworzenia spersonalizowanej sztucznej inteligencji, z której mogą korzystać wszyscy ludzie. W tym celu firma utworzyła własną Globalną Radę ds. Sztucznej Inteligencji (Global AI Council), która stara się przewidywać i przeciwdziałać negatywnym skutkom wykorzystania sztucznej inteligencji.

Olga Wasiuta, Sergiusz Wasiuta

J. Booth, A. Roussos, A. Ponniah i in., *Large Scale 3D Morphable Models*, „International Journal of Computer Vision" 2018, vol. 126, no. 2; A. Dodge, L. House, E. Johnstone, *Using Fake Video Technology To Perpetrate Intimate Partner Abuse*, 25.04.2018, WithoutMyConsent.org (dostęp 15.03.2019); W. Gogołek, *Komunikacja sieciowa. Uwarunkowania, kategorie i paradoksy* ASPRA-JR, Warszawa 2010; R. Heartfield, G. Loukas, *Protection Against Semantic Social Engineering Attacks*, [w:] *Versatile Cybersecurity. Advances in Information Security* M. Conti, G. Somani, R. Poovendran (eds.), Springer, Cham 2018; H. Kim, P. Garrido, A. Tewari i in., *Deep Video Portraits*, „ACM Transactions on Graphics" 2018, vol. 37, no. 4; D. Rivera, A. García, M.L. Martín-Ruiz i in., *Secure Communications and Protected Data for a Internet of things Smart Toy Platform*, „IEEE Internet of things Journal" 2019, vol. 6, no. 2; S. Suwajanakorn, S.M. Seitz, I. Kemelmacher-Shlizerman, *Synthesizing Obama: Learning Lip Sync from Audio*, „ACM Transactions on Graphics" 2017, vol. 36, no 4; A. Tewari, M. Zollhöfer, H. Kim i in., *MoFA: Model-based Deep Convolutional Face Autoencoder for Unsupervised Monocular Reconstruction*, [w:] *2017 IEEE International Conference on Computer Vision (ICCV)*, Wenecja 2017; J. Thies, M. Zollhöfer, M. Stamminger i in., *FaceVR: Real-Time Facial Reenactment and Eye Gaze Control in Virtual Reality*, „ACM Transactions on Graphics" 2018, vol. 37, iss. 2; O. Wasiuta, *Deepfake*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 3; Y. Zhu, R. Bridson, D.M. Kaufman, *Blended cured quasi-newton for distortion optimization*, „ACM Transactions on Graphics" 2018, vol. 37, iss. 4.

Deep web (także ang. *invisible web* – niewidzialna sieć, ang. *hidden web* – ukryta sieć), ukryty internet, głęboka sieć – obszar globalnej sieci, który nie jest indeksowany, a więc także nie jest wyszukiwany przez standardowe wyszukiwarki internetowe (ang. *search engines*); to część sieci ukryta przed konwencjonalnymi wyszukiwarkami, np. poprzez szyfrowanie; zbiór nieindeksowanych stron internetowych.

Termin *invisible web* („niewidzialna sieć") po raz pierwszy został użyty przez J. Ellsworth w 1994 r. na określenie tych zasobów sieciowych, których wyszukiwarki nie mogą lub nie chcą indeksować i które ostatecznie są dla użytkowników niewidzialne i niedostępne. Duży wkład w rozwój badań nad zagadnieniem wniósł G. Price – bibliotekarz i szef Online Information Resources w serwisie Ask.com. Stworzył również bezpłatną, dostępną online listę zawierającą wykaz rankingów firm, wybitnych ludzi i ich zawodowych osiągnięć, prowadzoną od 1998 r. Za pośrednictwem jego serwisu DirectSearch można było dotrzeć do wielu zasobów deep webu. Co ważne, ok. 95% głębokiej sieci stanowią zasoby, do których dostęp jest bezpłatny, a blisko połowa to specjalistyczne, dziedzinowe bazy danych – niezwykle cenne w poszukiwaniach bibliograficznych.

Deep web to pojęcie złożone. Można w nim wyróżnić 2 kategorie zasobów.

Pierwsza kategoria to każda → informacja trudna do uzyskania poprzez standardowe wyszukiwanie. Może to obejmować posty na Twitterze lub Facebooku, linki „schowane" w wielu warstwach lub wyniki, które znajdują się tak daleko w standardowych wynikach wyszukiwania, że typowi użytkownicy nigdy ich nie znajdą. Druga kategoria to ogromne repozytorium informacji, które nie są dostępne dla standardowych wyszukiwarek. Składa się z treści znalezionych na stronach internetowych, w bazach danych i innych źródłach. Często są one dostępne tylko za pośrednictwem niestandardowego zapytania skierowanego do poszczególnych stron internetowych, do których nie można dotrzeć za pomocą prostego wyszukiwania powierzchniowego. Deep web nie znajduje się w jednym miejscu. Składa się zarówno z treści ustrukturyzowanych, jak i niestrukturalnych, których ogromna ilość znajduje się w bazach danych.

Zawartość głębokiej sieci jest ogromna – jak szacuje firma Bright Planet, ok. 500 razy większa niż ta widoczna dla konwencjonalnych wyszukiwarek – i o znacznie wyższej jakości niż sieć powierzchniowa. Ukryty internet w dużej mierze składa się z niezwykle cennych i użytecznych źródeł informacji praktycznej i naukowej. Jak podkreśla N. Pamuła-Cieslak, mają one tę przewagę nad dokumentami widzialnego internetu

(ang. *surface web*), że w dużej części pozostają pod stałą kontrolą merytoryczną, faktograficzną, językową oraz bibliograficzną. Dzieje się tak dlatego, że powstają z inicjatywy lub przy współudziale ekspertów dziedzinowych. Gwarantuje to użytkownikom wiarygodność zdobytych w ten sposób informacji i danych. Aby dotrzeć do zasobów ukrytego internetu, należy zastosować pewne → strategie [t. 4] wyszukiwawcze – nie wystarczy tu skorzystać z jednego prostego narzędzia, jakim jest wyszukiwarka. Aby zastosować owe strategie, należy wiedzieć, że są one ściśle związane z rodzajem poszukiwanych źródeł.

Korzystając z internetu, mamy do dyspozycji ok. 1,5 mld zindeksowanych stron internetowych. Ta liczba robi wrażenie, ale to tylko wierzchołek góry lodowej – ok. 3–4% zawartości całej sieci. Reszta internetu kryje się pod powierzchnią na dynamicznie generowanych stronach, których nie można znaleźć poprzez standardowe wyszukiwarki. Są one dla nich po prostu niewidoczne, ponieważ stanowią sieć niezindeksowaną. Roboty wyszukiwarek nie docierają do większości zasobów zamieszczonych w głębokiej sieci, chociaż ok. 95% z nich to publicznie dostępne informacje. Zasoby sieci, które nie są indeksowane, powiększają się gwałtownie i przyjmują przeważnie postać baz danych – ponad połowa niewidocznej sieci znajduje się w bazach danych specjalistycznych. Warto dodać, że twórcy wyszukiwarek opracowują coraz lepsze algorytmy wyszukiwania, co powoduje, że zasoby widzialnego internetu i głębokiej sieci coraz bardziej się przenikają. Obecnie jesteśmy jednak dopiero na początku tej drogi, która ma na celu zindeksowanie jak największej części zasobów.

Deep web nie jest jednorodny, jego zawartość można łatwo zdefiniować. Zasoby te, ze względu na swoją rozległość, treść i uwarunkowania techniczne, są bardzo heterogeniczne. C. Sherman i G. Price proponują następującą typologię wg kryteriów podobnego typu i formatu dokumentów, podobnych problemów związanych z dotarciem do nich, podobnych sposobów ich znajdowania (strategii wyszukiwawczych):

> sieć nieprzezroczysta (ang. *the opaque web*) – zaliczają się do niej te zasoby internetowe, które bez trudu mogą być indeksowane przez wyszukiwarki, ale z kilku powodów indeksowane nie są i dlatego znajdują się w obszarze deep webu; tymi powodami są: „głębokość" ich znajdowania się w Internecie, częstotliwość przeszukiwania

sieci, maksymalna liczba rezultatów wyszukiwania w rankingu odpowiedzi, nieobecne w hipertekście adresy URL;
sieć zasobów prywatnych (ang. *the private web*) – zasoby prywatne mogą być zaindeksowane przez wyszukiwarki, coś jednak sprawia, że indeksowane nie są; przyczynami tego mogą być: hasło zabezpieczające stronę (w tym przypadku mechanizm skanujący nie ma do niej dostępu i nie może zindeksować jej zawartości), użycie przez autora strony pliku o nazwie robots.txt w katalogu, w którym witrynę zycznie umieszczono na serwerze (taki plik umieszcza się celowo, by określić, które strony i pliki mogą być indeksowane przez wyszukiwarki); zasoby znajdujące się w sieci prywatnej zwykle zawierają treści, które interesują osoby znające zarówno hasło, jak i adres konkretnej witryny;
sieć zastrzeżona (ang. *the proprietary web*) – zasoby internetu dostępne tylko dla tych użytkowników, którzy uzyskali zgodę na ich przeglądanie i wykorzystywanie; tego typu witryny wymagają rejestracji użytkownika, można mówić o bezpłatnej i komercyjnej części sieci zastrzeżonej, nawet zasoby bezpłatne są jednak niedostępne dla wyszukiwarek (roboty nie mają możliwości technicznych przejścia przez proces rejestracyjny, polegający zwykle na odpowiadaniu na pytania zawarte w formularzu – podaniu danych osobowych niezbędnych do identy kacji użytkownika, określeniu własnych preferencji); najrozleglejszą częścią sieci zastrzeżonej są komercyjne systemy płatnej rejestracji, oferujące dostęp do baz danych, które w większości zostały stworzone jeszcze przed powstaniem sieci WWW, potencjalnie udostępniane odbiorcom;
prawdziwie ukryty internet (ang. *truly invisible web*) – zasoby, które nie są skanowane i indeksowane przez wyszukiwarki z powodów technicznych i technologicznych. Takie postawienie problemu jest jednak nie do końca słuszne, gdyż na bieżąco powstają nowe, coraz bardziej zaawansowane technicznie wyszukiwarki, starające się indeksować choć część zasobów należących dotychczas do prawdziwie ukrytego internetu, a i te istniejące dotychczas starają się nadążać w tym względzie za konkurencją.

Z punktu widzenia przeciętnego użytkownika w deep webie znajduje się wszystko to, co nie pojawia się na pierwszej stronie rezultatów wyszukiwania wiodących serwisów (Google), czego nie ma w newsfeedzie na portalach społecznościowych (Facebook). Cały ruch sieciowy, czyli wszystkie dane, jest wielokrotnie szyfrowany w momencie przejścia przez poszczególne węzły. Ponadto żaden węzeł sieciowy nie zna ani źródła ruchu, ani jego punktu docelowego, ani zawartości. Sprawia to, że anonimowość jest na wysokim poziomie oraz w typowych warunkach niemal niemożliwe jest stwierdzenie, kto w rzeczywistości stoi za daną aktywnością sieciową. Cała zawartość jest przechowywana w różnych systemach o różnych strukturach. Deep web zawiera mnóstwo danych oraz bogactwo możliwości, m.in.:

- zasoby nieindeksowane przez uniwersalne wyszukiwarki, zwłaszcza Google – z różnych powodów, w tym technicznych (błędne metadane, czas działania, nietypowe formaty itp.), ale też związanych z polityką wyszukiwarek lub właścicieli serwisów WWW;
- zasoby indeksowane, do których nie tak łatwo dotrzeć, których odnalezienie i wykorzystanie wymaga rozwiniętej strategii wyszukiwawczej;
- wewnętrzne strony największych rm, stowarzyszeń i organizacji handlowych;
- dokumenty w nietypowych formatach, np. skompresowane;
- serwisy WWW zabezpieczone hasłem, np. fora, intranety (szkół, uczelni i uniwersytetów);
- listy dyskusyjne wymagające zalogowania się;
- serwisy WWW, do których nie prowadzą odsyłacze z innych witryn;
- strony wyłączone z procesu indeksacji przez twórców, czyli takie, których autorzy zabronili robotom indeksowania ich treści;
- treści generowane dynamicznie, w czasie rzeczywistym, np. w odpowiedzi na zapytanie użytkownika;
- zasoby *de facto* indeksowane przez wyszukiwarki uniwersalne, ale pojawiające się na odległych miejscach na liście wyników wyszukiwania (aspekt algorytmów rankingowych) albo takie, których odnalezienie wymaga zaawansowanej strategii wyszukiwawczej;

zawartość komercyjnych baz danych, czasopism, wypożyczalni online itd., wymagających dokonania rejestracji albo subskrypcji;
zawartość publicznie dostępnych baz danych, archiwów i repozytoriów typu Open Access, bibliotek cyfrowych, katalogów bibliotecznych itp.;
źródła, do których dociera się dzięki poleceniom innych;
bazy danych tworzone z reguły przez podmioty rządowe lub naukowe, w których wyszukiwanie za pomocą ich własnych interfejsów (a nie interfejsu Google czy innej wyszukiwarki globalnej) jest o wiele bardziej efektywne i których zawartość jest uważana za wiarygodną;
dane – badawcze, statystyczne i in. oraz zbiory takich danych;
gra ki, multimedia – a właściwie ich zawartość;
pełne teksty artykułów i książek;
zawartość portali społecznościowych.

Wspólne jest to, że informacje w nich zawarte nie są przeznaczone do konsumpcji publicznej. Właściciele treści mogą dołożyć wszelkich starań, aby były niedostępne, a także zapewnić, że nie pojawią one się w wynikach wyszukiwania.

Przyczyny istnienia deep webu to:

polityka i sposób działania wiodących serwisów WWW, zwłaszcza wyszukiwarek globalnych;
postępowanie dostawców treści/zasobów informacyjnych – dostęp restrykcyjny, w tym komercyjny;
brak kompetencji cyfrowych/informacyjnych użytkowników (ang. *digital literacy*/*information literacy*);
zasoby nieindeksowane i/lub nieudostępniane przez Google.

Warto zauważyć, że zawartość deep webu nie zawsze jest nielegalna, w jego obszarze istnieje wiele działań pozostających całkowicie w ramach prawa. Można tu wyróżnić np.:

→ media społecznościowe [t. 3], blogi, czaty głosowe;
międzynarodowe gry w stylu turniejowym, takie jak szachy i backgammon (tryktrak);
grupy typu „koniec świata”;
kluby książki, fankluby, kluby gier wideo;

ukryte odpowiedzi – popularna wersja Yahoo Answers;
rejestry publiczne i certy katy, indeksy systemu bibliotecznego;
komunikacja za pomocą szyfrowanego użycia w celu zapewnienia prywatności i ochrony;
konkursy karaoke i śpiewu;
grupy teoretyków spisku;
kursy z zakresu obsługi komputera i technologii.

Tradycyjne wyszukiwarki tworzą swoje indeksy przez przeglądanie lub indeksowanie powierzchniowych stron internetowych. Aby zostać odkryta, strona musi być statyczna i połączona z innymi stronami. Głębokie witryny sieci Web otrzymują średnio o 50% większy ruch miesięczny niż strony powierzchniowe i są bardziej powiązane z witrynami na powierzchni. Typowa (wg mediany) głęboka strona internetowa nie jest jednak dobrze znana użytkownikom sieci. Ponad połowa głębokich stron znajduje się w bazach tematycznych.

Deep web charakteryzuje się rozrostem, różnorodnością domen i licznymi ustrukturyzowanymi bazami danych. Rośnie w tak dużym tempie, że skuteczne oszacowanie jego wielkości może być trudne lub wręcz niemożliwe.

Olga Wasiuta, Sergiusz Wasiuta

P. Biddle, P. England, M. Peinado, *e Darknet and the Future of Content Distribution*, 2003; M.K. Bergman, *e Deep Web: Surfacing Hidden Value*, „ e Journal of Electronic Publishing" 2001, vol. 7, iss. 1; E. Dilipraj, *Cyber Enigma: Unravelling the Terror in the Cyber World*, Routledge, Milton 2019; K. Król, *Deep Web i Dark Web: niewidoczne zasoby internetu*, 9.05.2019, HomeProject.pl (dostęp 18.05.2019); T. Leżoń, *Darknet i deep web. Głęboko pod powierzchnią jest miejsce, o którym wołałbyś nie wiedzieć*, 27.04.2015, TVN24.pl (dostęp 31.07.2020); D. Midel, *Mappa mundi ukrytego internetu. Próba kategoryzacji kanałów komunikacji i treści*, „Praktyka i Teoria Informacji Naukowej" 2015, t. 23, nr 1; E. Morozov, *e Net Delusion: e Dark Side of Internet Freedom*, Public A airs, New York 2011; W. Orliński, *Internet. Czas się bać*, Wydawnictwo Agora, Warszawa 2013; N. Pamuła-Cieslak, *Typologia zasobów ukrytego internetu*, „Przegląd Biblioteczny" 2006, z. 2; taż, *Ukryty internet jako przedmiot edukacji informacyjnej*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2015; C. Sheils, *e Dark Web & Deep Web: How To Access e Hidden Internet Today* , 27.02.2019, Digital.com (dostęp 27.02.2019); Ch. Sherman,

G. Price, *The Invisible Web. Uncovering Information Sources Search Engines Can't See*, Information Today, Medford, New Jersey 2003; M. Szpunar, *Imperializm kulturowy internetu*, Instytut Dziennikarstwa, Mediów i Komunikacji Społecznej Uniwersytetu Jagiellońskiego, Kraków 2017; taż, *Sieć ukryta a sieć widzialna. O zasobach WWW nieindeksowanych przez wyszukiwarki*, „Przegląd Kulturoznawczy" 2014, nr 1 (19); D. Szumilas, *Kop głębiej! Google to nie wszystko*, „Magazyn Internet" 2005, nr 8; B. Świderski, *Najciemniejszy zakątek internetu naprawdę istnieje. Ukryta sieć TOR: Lewe papiery, pedofilia, przekręty i narkotyki*, 21.09.2012, NaTemat.pl (dostęp 18.05.2019); O. Wasiuta, *Deep web*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron Kraków 2019; O. Wasiuta, S. Wasiuta, *FakeApp jako nowe zagrożenie bezpieczeństwa politycznego i informacyjnego*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 3; J.A. Wood, *The Darknet: a Digital Copyright Revolution*, „Richmond Journal of Law & Technology" 2010, vol. 16, iss. 4.

Degradacja wojskowa – polega na odebraniu posiadanego → stopnia wojskowego [t. 4], co bywa dokonywane często w ceremonialny sposób, aby dodatkowo ukarać i upokorzyć degradowanego. Ceremonia taka odbywa się publicznie – na widoku wszystkich zgromadzonych odbiera się degradowanemu wszelkie odznaczenia i emblematy, zrywa się guziki i epolety, strąca czapkę i łamie białą broń przyboczną. Degradacji wojskowej dokonywano za różne czyny, przy czym zwykle była to kara za działania haniebne i uważane za niehonorowe i niegodne → żołnierza [t. 4]. Wśród znanych zdegradowanych wymienia się m.in. F.Mitchella (1621 r.), T. Cochrane'a (1814 r.), A. Dreyfusa (1894 r.), P. Pétaina (1945 r.), R. Kuklińskiego (1984 r.).

Obecnie w Polsce, zgodnie z art. 324 § 1 pkt. 3 kk, degradacja jest jednym ze środków karnych. Definicja legalna degradacji zawarta została w art. 327 § 1 kk, zgodnie z nią degradacja obejmuje utratę posiadanego stopnia wojskowego i powrót do stopnia szeregowego. Degradacja godzi w istotny sposób w prestiż ukaranego, a także pociąga za sobą restrykcje natury ekonomicznej takie jak utrata pracy, brak możliwości uzyskania dodatkowego uposażenia rocznego czy odprawy, a także odebranie prawa do zaopatrzenia emerytalnego.

Sąd może orzec degradację w razie skazania za przestępstwo umyślne, jeżeli rodzaj czynu, sposób i okoliczności jego popełnienia pozwalają

przyjąć, że sprawca utracił właściwości wymagane do posiadania stopnia wojskowego, a zwłaszcza w wypadku działania w celu osiągnięcia korzyści majątkowej. Oznacza to, że degradacja może zostać orzeczona w odniesieniu do każdego skazanego żołnierza, niezależnie od typu czynu, jaki popełnił. Sąd może orzec degradację tylko wobec osoby, która w chwili popełnienia → czynu zabronionego [t. 1] była żołnierzem, chociażby przestała nim być w chwili orzekania.

Ostatnim publicznie zdegradowanym angielskim rycerzem królestwa był Mitchell – został pozbawiony rycerstwa po uznaniu go winnym wyłudzania pieniędzy od licencjobiorców po tym, jak otrzymał monopol na licencjonowanie zajazdów przez G. Villiersa, pierwszego księcia Buckingham, i króla Jakuba I Stuarta. Z kolei Cochrane, brytyjski arystokrata, polityk i wojskowy, adm. Royal Navy, uczestnik wojen napoleońskich, został zdegradowany za udział w spekulacjach giełdowych. Marszałek Pétain został zdegradowany za zdradę narodową i kolaborację na rzecz hitlerowskich Niemiec.

Jednym z najbardziej znanych w historii zdegradowanych żołnierzy był kpt. Dreyfus, którego historia wywołała skandal polityczny we Francji pod koniec XIX wieku. Dreyfus był niezależnym, zamożnym Żydem pochodzenia niemieckiego, służył w Sztabie Generalnym Armii Francuskiej. Został oskarżony o szpiegostwo na rzecz Niemiec na podstawie dokumentu znanego jako „Bordereau" (fr. *bordereau*, wykaz, notka) znalezionego w niemieckiej ambasadzie. Wyraźnie antysemicki Sztab Generalny odmówił Dreyfusowi dostępu do dokumentacji użytej do osądzenia go w procesie przed sądem wojskowym w październiku 1894 r. Dreyfus został uznany za winnego i skazany na degradację i uwięzienie na Diabelskiej Wyspie. Płk G. Picquart wkrótce po procesie zdał sobie sprawę, że dokument „Bordereau" został napisany przez mjra F. Walsina Esterhazy'ego, którego pismo odpowiadało innym obciążającym dowodom. Picquarta szybko zastąpił komendant H.-J. Henry, który sfałszował dokumenty obciążające Dreyfusa, a gdy zostało to odkryte, popełnił samobójstwo. Sąd wojenny zwolnił Esterhazy'egoze wszystkich stawianych mu zarzutów. W sprawę niesłusznie oskarżonego i zdegradowanego Dreyfusa zaangażował się pisarz Emil Zola, który 13 stycznia 1898 r. opublikował list otwarty *J'Accuse…!* (*Oskrażam…!*), pod którym podpisało się wielu francuskich intelektualistów. M.in. za sprawą

listu miał miejsce nowy proces w Rennes 3 czerwca 1899 r., w którym Drey fus ponownie został uznany za winnego, ale z okolicznościami łagodzącymi. W 1903 r. Sąd Najwyższy stwierdził, że wyrok sądu wojskowego był błędny. Dopiero jednak 22 lipca 1906 r. przywrócono Dreyfusowi stopień kapitana, awansowano go na majora oraz odznaczono Legią Honorową.

Kontrowersje wywołuje niejednokrotnie pytanie o to, za co można ukarać żołnierza degradacją, aby kara odpowiadała popełnionemu czynowi. W 2012 r. ze stopnia sierż. sztab. piechoty morskiej USA do stopnia szeregowego został zdegradowany F. Wuterich. Dowodził on oddziałem, który dokonał masakry w Al-Hadisie w Iraku 19 listopada 2005 r. Wówczas to amerykańscy żołnierze brutalnie zamordowali 24 Irakijczyków, w tym kobiety i dzieci. Przyczyną wydarzenia był wybuch bomby pułapki, która zabiła jednego z żołnierzy marines. Koledzy zabitego w akcie desperacji zastrzelili cywilów w taksówce, a następnie wtargnęli do domów w pobliżu miejsca eksplozji. Tam zastrzelili kilkanaście kolejnych osób. Wśród 24 zabitych było 8 kobiet i 5 dzieci. Ciała zamordowanych nosiły ślady strzałów w głowę, jedno zaś było spalone. Świadkowie wydarzeń podkreślali, że nie było powodów dla tak brutalnego działania. Lokalna ludność żądała ukarania śmiercią żołnierzy, którzy dopuścili się masakry. Postępowanie wobec zdegradowanego następnie Wutericha trwało 6 lat.

Proces degradacji może być nie tylko następstwem wyroku sądowego, ale także konsekwencją decyzji politycznej. W Polsce w 2018 r. pojawił się projekt ustawy degradacyjnej, której założeniem było pozbawienie stopni wojskowych żołnierzy i oficerów służących w Wojsku Polskim w czasie PRL, w tym przede wszystkim odebranie stopni generalskich W. Jaruzelskiemu i C. Kiszczakowi. Zgodnie z projektem ustawy degradacja miała objąć oficerów wskazanych przez ministra obrony narodowej, który będzie mógł wszcząć stosowne postępowanie z inicjatywy własnej lub po uzyskaniu → informacji od Instytutu Pamięci Narodowej, Wojskowego Biura Historycznego oraz organizacji społecznych. Ustawa nie weszła jednak w życie w związku z odmową jej podpisania przez Prezydenta RP.

W 1984 r. zdegradowany ze stopnia pułkownika został Kukliński. Pozycja Kuklińskiego w Sztabie Generalnym Polskiej Armii Ludowej i jego rola jako oficera łącznikowego między Polską Armią Ludową a oddziałami Układu Warszawskiego dała mu dostęp do najtajniejszych dokumentów

wojskowych. W 1971 r. rozpoczął współpracę z CIA, która wg niektórych źródeł historycznych dostarczyła Amerykanom ok. 35 tys. stron ściśle tajnych materiałów, od specyfikacji technicznych najnowszej radzieckiej broni po plany operacyjne Układu Warszawskiego. W 1981 r, tuż przed ogłoszeniem przez gen. Jaruzelskiego stanu wojennego, kiedy ujawnienie Kuklińskiego było bliskie, wraz z rodziną z pomocą CIA opuścił PRL. Następnie mieszkał w USA pod zmienioną tożsamością. Zaocznie Kukliński został zdegradowany i skazany na śmierć przez polski sąd wojskowy, ale wyrok został uchylony w 1996 r. po upadku → komunizmu w Polsce.

Jakub Idzik

S. Cenckiewicz, *Atomowy szpieg. Ryszard Kukliński i wojna wywiadów*, Zysk i S-ka, Poznań 2014; G. Chapman, *The Dreyfus Case: A Reassessment*, Reynal, New York 1972; *Encyclopedia of Violence, Peace & Conflict*, L.R. Kurtz (red.), Elsevier, Oxford 2008; *Handbook of the Sociology of the Military*, G. Caforio, M. Nuciari (red.), Springer International Publishing, Cham 2018; M. Horoszewicz, *Sprawa Dreyfusa: ostrzeżenie sprzed wieku*, Bellona, Warszawa 2017; A. King, *The Combat Soldier. Infantry Tactics and Cohesion in the Twentieth and Twenty-First Centuries*, Oxford University Press, Oxford 2013; A. Richardson, *Dreyfus Affair (1894–1906)*, [w:] *Ground Warfare: An International Encyclopedia*, S. Sandler (ed.), ABC-CLIO, Santa Barbara–Denver–Oxford 2002; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 2019.1950 t.j.; B. Weiser, *Ryszard Kukliński. Życie ściśle tajne*, Świat Książki, Warszawa 2009.

Demilitaryzacja – w wąskim rozumieniu oznacza zobowiązanie do usunięcia wszelkich obiektów militarnych, broni oraz sił zbrojnych z danego terenu oraz zakaz ich lokowania, budowania czy utrzymywania na nim w przyszłości, wynikające z umów międzynarodowych i stanowiące jeden z typów ograniczenia zwierzchnictwa terytorialnego państwa. Takie ujęcie terminu zostało zawarte w załączniku XIII do traktatu pokojowego z Włochami, podpisanego w Paryżu dnia 10 lutego 1947 r. Zgodnie z dokumentem demilitaryzacja powinna być rozumiana jako:

> zakaz, na danym terenie i na danych wodach terytorialnych, wszelkich urządzeń lub fortyfikacji morskich, wojskowych i lotniczo-wojskowych, jak również ich zbrojenia, sztucznych zapór

wojskowych, morskich i powietrznych; korzystania z baz przez jednostki wojskowe, morskie i lotnictwa wojskowego lub stacjonowania stałego, jak również tymczasowego tych jednostek; szkolenia wojskowego w jakiejkolwiek bądź formie oraz fabrykacji sprzętu wojennego.

W I protokole dodatkowym do konwencji genewskich użyto natomiast terminu strefa zdemilitaryzowana, która spełnia następujące warunki:

a) wszyscy kombatanci, jak też broń i ruchomy sprzęt wojskowy powinni zostać z niej usunięci;
b) w strefie nie należy czynić użytku ze stałych urządzeń i obiektów wojskowych na szkodę nieprzyjaciela;
c) władza i ludność danego obszaru nie będą podejmować działań na szkodę nieprzyjaciela oraz
d) nie może być prowadzona żadna działalność na rzecz wsparcia wysiłku wojskowego.

Wyróżnia się demilitaryzację całkowitą i częściową. W pierwszym przypadku dany teren ma być wyłączony z wykorzystania w celach militarnych pod jakimkolwiek względem, w drugim zobowiązanie polega jedynie na ograniczeniu wykorzystania danego terenu do celów militarnych. Szczególnym przykładem częściowej demilitaryzacji jest denuklearyzacja, czyli zakaz utrzymywania → broni nuklearnej [t. 1] na określonym obszarze. Status stref wolnych od broni jądrowej ustanowiono np. w Ameryce Łacińskiej i na Karaibach (traktat z Tlatelolco z 1967 r.), na Południowym Pacyfiku (traktat z Rarotonga 1985 r.), w Azji Południowo-Wschodniej (traktat z Bangkoku z 1995 r.), w Afryce (traktat z Pelindaba z 1996 r.) i w Azji Środkowej (traktat z Semipałatyńska z 2006 r.).

Termin demilitaryzacja używany jest także w znaczeniu szerszym – jako dążenie do ograniczenia potencjału militarnego państw, przy czym nie oznacza całkowitego usunięcia z ich terytorium wszelkich obiektów czy sił militarnych, a jedynie ograniczenie liczebności sił zbrojnych czy arsenału posiadanego uzbrojenia. Przykładami może być demilitaryzacja Niemiec, Austrii i Japonii po II wojnie światowej.

Dążenie do wyłączenia określonych obszarów z wykorzystania w celach wojskowych jest zjawiskiem znanym od wieków, by wspomnieć np. tego rodzaju zapisy w traktatach pokojowych zawartych w Westfalii w 1648 r. czy w Utrechcie w 1713 r. Postanowienia tego rodzaju coraz częściej ujmowano w traktatach zawieranych od końca XIX wieku – demilitaryzacja Kanału Kilońskiego, Kanału Panamskiego, Kanału Sueskiego, demilitaryzacja Nadrenii, cieśniny Magellana, Dardanele, Bosfor, Gibraltarskiej. Status obszarów zdemilitaryzowanych mają także: Antarktyka (traktat antarktyczny z 1959 r.), dno morskie (traktat o dnie morza z 1971 r.), Wyspy Alandzkie (traktat paryski z 1856 r., potwierdzony w 1921 i ponownie w 1947 r.), koreańska strefa zdemilitaryzowana oddzielająca Koreę Północną i Koreę Południową (ustalona przez ONZ w 1953 r.).

Przestrzeń kosmiczną można uznać za przynajmniej częściowo zdemilitaryzowaną. Traktat o przestrzeni kosmicznej z 1967 r. przewiduje, że państwa-strony

> zobowiązują się nie wprowadzać na orbitę wokół Ziemi jakichkolwiek obiektów przenoszących broń nuklearną lub jakichkolwiek innych rodzajów broni masowego zniszczenia ani nie umieszczać tego rodzaju broni na ciałach niebieskich lub w przestrzeni kosmicznej w jakikolwiek inny sposób. […] Zakazuje się zakładania wojskowych baz, instalacji oraz forty kacji na ciałach niebieskich, dokonywania na nich prób z jakimikolwiek typami broni oraz przeprowadzania manewrów wojskowych. Korzystanie z personelu wojskowego w celu badań naukowych lub w jakichkolwiek innych celach pokojowych nie jest zabronione.

Analogicznego statusu nie nadano natomiast morzom i oceanom. Artykuł 88 Konwencji Narodów Zjednoczonych o prawie morza z 1982 r. wskazuje jedynie, że *morze pełne jest wykorzystywane wyłącznie do celów pokojowych*. Konwencja nie wprowadza więc ani częściowej, ani całkowitej demilitaryzacji czy też denuklearyzacji morza pełnego, nie zakazuje również działalności nawigacji wojskowej.

Anna Pacholska

T. Brańka, *Demilitarization and Neutralization – the Case of the Åland Islands*, „Przegląd Politologiczny" 2017, nr 4; R. Klepka, *Parlament w państwie federalnym na przykładzie Austrii, Belgii, Niemiec i Szwajcarii*, Wydawnictwo Sejmowe, Warszawa 2013; A. Makowski, *Konwencja o prawie morza – implikacje dla bezpieczeństwa polski*, „Prawo Morskie", t. XXVII; A. Pacholska, *Demilitaryzacja*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; J. Polit, *Kapitulacja i okupacja Japonii*, [w:] *Historia polityczna świata XX wieku*, M. Bankowicz (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2004; Protokół dodatkowy do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony o ar międzynarodowych kon iktów zbrojnych (Protokół I), sporządzony w Genewie dnia 8 czerwca 1977 r., Dz. U. 1992, nr 41, poz. 175.

Demobilizacja – w szerszym znaczeniu to szereg działań, które mają miejsce w państwie w przypadku zmiany jego sytuacji politycznej z wojennej na pokojową. W tym zakresie pojęcie jest przeciwstawne do mobilizacji oznaczającej zmianę sposobu funkcjonowania państwa w przypadku zmiany sytuacji pokojowej na wojenną. Zmiana demobilizacyjna polega na podjęciu szeregu działań odnoszących się do funkcjonowania armii, gospodarki, systemu ekonomicznego, przemysłu, rolnictwa, transportu, łączności oraz innych sfer. W węższym sensie demobilizacja wojskowa jest procesem rozumianym jako jeden z aspektów działania obejmującego rozbrojenie, demobilizację i reintegrację byłych → ż o ł n i e r z y [t. 4] oraz przemysłu nastawionego na prowadzenie działań wojennych. Odgrywa kluczową rolę w przechodzeniu od → w o j n y [t. 4] do pokoju. Powodze nie lub niepowodzenie tego przedsięwzięcia bezpośrednio wpływa na długoterminowe perspektywy budowania pokoju w każdym społeczeństwie po zakończeniu kon iktu. Procesy demobilizacji przyczyniają się do zaspokojenia natychmiastowych potrzeb w zakresie → b e z p i e c z e ń s t w a [t. 1] i umożliwiają rozwój silnych instytucji politycznych, dobrze funkcjonujących gospodarek oraz reintegrację społeczną i gospodarczą byłych uczestników walk w celu przyczynienia się do racjonalnych rządów, pojednania społeczeństwa, długofalowego rozwoju i trwałego pokoju.

Demobilizacja wojskowa jest zarówno procesem zycznym, jak i mentalnym. Aspekt zyczny polega na oddzieleniu elementu uzbrojonego, a więc żołnierza, od systematycznej struktury dowodzenia i kontroli sił zbrojnych lub grupy, zmniejszając w ten sposób liczbę walczących w siłach

zbrojnych albo rozwiązując grupy w całości. Mentalny aspekt procesu demobilizacji polega na przygotowaniu danej osoby lub grupy do znalezienia swojego miejsca w → społeczeństwie obywatelskim [t. 4]. Wojsko ma do odegrania ważną rolę zarówno w rozbrojeniu, jak i demobilizacji, jednakże równie istotny jest komponent cywilny – rozbrojenie jest przede wszystkim odpowiedzialnością wojska, zaś w pozostałych czynnościach, zwłaszcza w programie reintegracji, uczestniczy głównie ten drugi, przy czym strony udzielają sobie wzajemnego wsparcia. Współpraca cywilno-wojskowa jest kluczem do wydajności w tej części operacji.

Demobilizacja wojskowa odnosi się do szeregu interwencji w procesie → demilitaryzacji oficjalnych i nieoficjalnych grup zbrojnych poprzez rozbrajanie i rozwiązywanie grup niepaństwowych oraz ewentualnie zmniejszanie sił zbrojnych. Tradycyjnie alternatywą dla rozwiązania pokonanej grupy zbrojnej jest włączenie jej częściowo do zwycięskich sił zbrojnych. Polityczne i społeczne motywy demobilizacji obejmują poprawę jakości i efektywności sił zbrojnych, zapewnienie politycznej legitymizacji sił zbrojnych, co wiąże się z przesunięciem lojalności grupy zbrojnej z określonego podmiotu (politycznego), modernizację wojska, utrzymanie dokładnej reprezentacji mniejszości w grupie zbrojnej oraz zagwarantowanie bezpieczeństwa ludzi. Należy podkreślić, że demobilizacja jest przede wszystkim procesem cywilnym, choć wkład wojska ma kluczowe znaczenie dla decyzji metodologicznych i organizacyjnych.

W praktyce programy demobilizacyjne pomagają byłym uczestnikom walk odchodzić od ról i stanowisk, które określały ich w czasie konfliktu, aby identyfikowali się jako obywatele i członkowie lokalnych społeczności. Zakłada się, że doszło do rozbrojenia oraz że broń została zebrana, zmagazynowana lub w ostateczności zniszczona. Zorganizowanie zgrupowania byłych walczących jest zazwyczaj pierwszym krokiem dającym możliwość odzyskania kontroli nad wcześniej rozproszonymi oddziałami i ich bronią. Oprócz usunięcia symboli życia wojskowego walczących, takich jak broń, mundur i stopień, byli żołnierze są rejestrowani, liczeni i monitorowani przy użyciu dokumentów identyfikacyjnych, a jednocześnie zbierane są → informacje niezbędne do ich integracji ze społecznością. Osobom, które wcześniej brały udział w konfliktach, oferuje się medyczne badania przesiewowe i pomoc, zaopatrzenie i transport w celu powrotu do ich

rodzinnych regionów. Udzielanie pomocy materialnej lub nansowej rodzinom byłych uczestników walk jest również uważane za kluczowe w tym procesie, ponieważ ułatwia akceptację długo nieobecnych członków społeczeństwa przez ich macierzyste społeczności.

Po przeniesieniu się do społeczności lokalnych byli uczestnicy walk otrzymują szkolenie zawodowe do pracy poza dziedziną bezpieczeństwa, kredyty, stypendia, dystrybucję własności ziemi, a czasami znajdują zatrudnienie w nowej → p o l i c j i [t. 3] lub służbie bezpieczeństwa. Jednakże aby proces powrotu zakończył się sukcesem, społeczność lokalna, do której były żołnierz i jego rodzina są ponownie wprowadzani, musi być na to przygotowana. Jednocześnie byli uczestnicy walk muszą znać swoje obowiązki zgodne z prawem i zwyczajami panującymi w ich państwie oraz być świadomi zmian politycznych, które miały lub mają miejsce.

Demobilizacja może prowadzić do trwałej reintegracji z życiem obywatelskim w dłuższej perspektywie czasowej, jeżeli istnieje odpowiednia perspektywa ekonomiczna, funkcjonują instytucje państwowe zdolne do świadczenia podstawowych usług, ramy prawne i ścisła koordynacja ze społeczeństwem obywatelskim w celu zapewnienia, że byli żołnierze znajdą realne źródła utrzymania i nowy cel w życiu.

Doświadczenia międzynarodowe ilustrują wyzwania związane z wdrażaniem procesu demobilizacji, a także jej polityczny i złożony charakter. Proces ten w dużej mierze koncentruje się na byłych walczących i ogranicza się do stosunkowo krótkiego okresu po zakończeniu wojny. Proces reintegracji musi być jednak postrzegany jako zadanie długoterminowe, które wymaga gotowości podmiotów międzynarodowych do utrzymania politycznego rozmachu tego programu. W zależności od charakteru wojny społeczności mogą zdecydowanie sprzeciwiać się powrotowi walczących. Mogą upłynąć lata, zanim część z nich wróci do domu, tak jak np. w Rwandzie, gdzie w czasie kon iktu zaszły drastyczne zmiany prawne i polityczne. Ponadto, aby poradzić sobie z brakiem zaufania do zmian politycznych lub poczuciem marginalizacji, demobilizacja jest prowadzona w połączeniu z innymi działaniami reformującymi sektor bezpieczeństwa.

Dodatkowym problemem pozostaje kwestia tego, ilu byłych walczących trzeba zdemobilizować. Liczby pochodzące z list dowódców są często przeszacowane i w związku z tym muszą być zwery kowane innymi

sposobami. Co więcej, byli żołnierze mogą nie chcieć oddać całej swojej broni, a wówczas może dojść do wzrostu → przemocy [t. 3] i → przestępczości [t. 3]. W niektórych przypadkach dawni walczący nie chcą wrócić do swoich domów lub mogą obawiać się dezaprobaty bądź odrzucenia, a tym samym próbować zatrzymać proces.

Istnieje również duża trudność w ustaleniu tego, kto jest byłym walczącym i kto powinien kwalifikować się do wsparcia demobilizacyjnego. Zdefiniowanie osoby biorącej udział w konflikcie jako noszącej broń często prowadziło do wykluczenia z procesów demobilizacyjnych kobiet i dziewcząt. Nierzadko związane z siłami zbrojnymi, napotykają również szczególne trudności w ponownej integracji ze społeczeństwem, w którym podporządkowują się tradycyjnym poglądom na swoją rolę w społeczeństwie.

Demobilizacja może być postrzegana jako nowa umowa społeczna pomiędzy byłymi uczestnikami walk a ich środowiskiem po zakończeniu konfliktu. Od 1989 r. kompleksowe rozwiązania polityczne mające na celu zakończenie długotrwałych konfliktów wewnętrznych w Ameryce Środkowej, różnych częściach Afryki, Azji Południowo-Wschodniej i na Bałkanach Zachodnich zawierały szczegółowe przepisy dotyczące rozbrojenia i demobilizacji rebeliantów i sił rządowych. W tym kontekście kraje OECD uzgodniły wytyczne polityczne dotyczące pomocy rozwojowej, a Departament Operacji Pokojowych ONZ opublikował zasady i wytyczne dotyczące właściwych programów, które od tego czasu stały się obowiązkowym elementem operacji utrzymywania i egzekwowania pokoju. Oprócz zaangażowania ONZ Bank Światowy finansuje i pomaga w prowadzeniu i ocenie tego rodzaju programów, podczas gdy Unia Europejska od dawna wspiera procesy rozbrojenia, demobilizacji i reintegracji poprzez programy wspólnotowe, fundusze dwustronne państw członkowskich, a od 2005 r. poprzez misje w ramach Europejskiej Polityki Bezpieczeństwa i Obrony (EPBiO). Coraz częściej organizacje pozarządowe działające w lokalnych społecznościach otrzymują fundusze na prowadzenie pomocy reintegracyjnej oraz świadczenie usług socjalnych i szkoleń.

Jakub Idzik

K.M. Clark, *Fostering a Farewell to Arms: Preliminary Lessons Learned in the Demobilization and Reintegration of Combatants*, United States Agency for International Development, Washington 1996; G.A. Dzinesa, *Disarmament, Demobilization and Reintegration in Southern Africa: Swords into Ploughshares*, Palgrave Macmillan, Johannesburg 2017; A. Giustozzi, *Introduction*, [w:] *Post-conflict Disarmament, Demobilization and Reintegration: Bringing State-building Back In*, A. Giustozzi (ed.), Routledge, New York–London 2016; T. Kmiecik, *Problemy demobilizacji i przejścia Wojska Polskiego na stopę pokojową w latach 1945–1947*, „Słupskie Studia Historyczne" 2004, z. 11; M. Knight, A. Özerdem, *Guns, Camps and Cash: Disarmament, Demobilization and Reinsertion of Former Combatants in Transitions from War to Peace*, „Journal of Peace Research" 2004, vol. 41 (4); tenże, *Disarmament, Demobilization and Reintegration of Former Combatants in Afghanistan: Lessons Learned from a Cross-Cultural Perspective*, „Third World Quarterly" 2002, vol. 23 (5); J. Rak, *From Mobilization to Demobilization: Dynamics of Contention in the Austerity-driven Slovenia*, „Środkowoeuropejskie Studia Polityczne" 2018, nr 3; The World Bank, *Demobilization and Reintegration Programming in the World Bank*, Conflict Prevention and Reconstruction Unit, The World Bank, Washington 2003; N. Young, *Demobilisation after War*, [w:] *The International Encyclopedia of Peace*, Oxford University Press, Oxford 2009.

Demonopolizacja bezpieczeństwa – proces tworzenia → społeczeństwa obywatelskiego [t. 4] nierozerwalnie związany jest z decentralizacją władzy i przekazaniem części kompetencji, a co za tym idzie także odpowiedzialności, samorządom. Bardzo ważną kompetencją uzyskaną przez władze samorządowe stało się zapewnianie → bezpieczeństwa publicznego [t. 1]. Odbywało się to w sytuacji, gdy zmiany ustrojowe o charakterze ekonomiczno-politycznym, jakie rozpoczęły się w Polsce na początku lat 90. XX w., spowodowały nie tylko akcelerację procesów gospodarczych i cywilizacyjnych zapewniających dynamiczny rozwój w różnych dziedzinach życia, ale także gwałtowny wzrost → przestępczości [t. 3] i towarzyszących jej → patologii społecznych [t. 3]. To właśnie wtedy pojawiły się nieznane wcześniej rodzaje przestępstw, w tym te o charakterze zorganizowanym i międzynarodowym. Jednocześnie kontrola nad aktywnością obywateli uległa ze strony państwa osłabieniu, tworzyły się pierwsze prywatne fortuny, dając początek powstawaniu rodzimego kapitału. Nastąpił też międzynarodowy transfer aktywów finansowych, a granice stały się bardziej otwarte, także dla świata

przestępczego. Społeczeństwo zaczęło też, głównie dzięki przekazom medialnym, odczuwać zwiększony stan → zagrożenia [t. 4] przestępczością, którą uznało za poważną przeszkodę w osiągnięciu satysfakcjonującego poziomu życia. Państwo nie było już zdolne do zapewnienia szeroko rozumianego → bezpieczeństwa [t. 1], a to z kolei zapoczątkowało trwałą zmianę, jaką jest demonopolizacja bezpieczeństwa. Paradoksalnie kolejną determinantą zagrożenia stało się wejście Polski do koalicji antyterrorystycznej i udział Sił Zbrojnych RP zarówno w misjach stabilizacyjnych, jak i operacjach wojskowych poza granicami kraju, stworzyły one dla kraju realne zagrożenie ze strony ekstremistów. Przed organami państwa pojawił się wówczas problem skutecznego przeciwstawiania się nowym wyzwaniom skutkującym wzrostem dynamiki → zagrożenia bezpieczeństwa [t. 4].

W nowej sytuacji państwo szybko zorientowało się, że dotychczas scentralizowane zarządzanie bezpieczeństwem jest nieefektywne, gdyż nie zapewnia właściwej reakcji na nieznane dotąd w Polsce determinanty zagrożeń. Tak więc podzielenie się odpowiedzialnością za stan → bezpieczeństwa publicznego [t. 1] z innymi niż rządowe podmiotami wynikało z jednej strony z procesów demokratyzacji państwa, a z drugiej z niemożności samodzielnego zwalczania występujących zagrożeń. W ten sposób następowała stopniowa demonopolizacja bezpieczeństwa.

Słownik języka polskiego PWN słowo „monopol" definiuje jako „czyjeś wyłączne prawo do czegoś". Demonopolizacja oznacza więc likwidowanie istniejącego monopolu w określonej dziedzinie. Przez wiele lat sferą całkowicie zmonopolizowaną przez państwo było bezpieczeństwo. Jest ono powszechnie uznawane za jedną z podstawowych potrzeb człowieka, której zaspokojenie umożliwia mu korzystanie z innych wartości, dając możliwość przetrwania i rozwoju. Termin „bezpieczeństwo" pojawił się w piśmiennictwie polskim już w XIX w., a jednym z jego prekursorów był, w okresie międzywojennym, W. Kawka, który definiował je jako stan, w którym ogół społeczeństwa, jak również państwo ze swoimi celami, mają zagwarantowaną ochronę od szkód zagrażających im z jakiegokolwiek źródła. J. Zaborowski za bezpieczeństwo publiczne uważa taki realny stan wewnętrzny państwa, który pozwala mu, bez narażenia na szkody (spowodowane zarówno działaniem sił natury, techniki jak i zachowaniem

ludzkim), na prawidłowe funkcjonowanie organizacji państwowej i zapewnienie jej interesów, zachowanie życia i zdrowia obywateli oraz korzystanie przez nich z praw i swobód zagwarantowanych im konstytucją i innymi uregulowaniami prawnymi. Kwestią bezpieczeństwa publicznego zajął się także Sąd Najwyższy, który w uchwale z dnia 22 grudnia 1993 r. określił je jako *całość porządku i urządzeń społecznych, chroniących obywateli przed zjawiskami groźnymi dla życia, zdrowia lub grożącymi poważnymi stratami w gospodarce narodowej*

Biorąc pod uwagę przedstawione wyżej de nicje, można przyjąć, że demonopolizacja bezpieczeństwa to udzielenie przez państwo zgody oraz stworzenie odpowiednich warunków do zapewniania bezpieczeństwa także przez inne niż państwowe podmioty. To podzielenie się przez państwo kompetencjami, zadaniami i odpowiedzialnością w zapewnianiu bezpieczeństwa z podmiotami, które ustawodawca wyposażył w tym celu w określone uprawnienia i narzędzia, pozwalające im na prowadzenie efektywnych działań.

Zapewnianiu bezpieczeństwa publicznego służy system będący zorganizowanym zbiorem podsystemów współdziałających ze sobą i tworzących spójną całość, ukierunkowanych na realizację wspólnego celu, jakim jest uzyskanie i utrzymanie pożądanego stanu w państwie, rozumianego jako brak zagrożenia w życiu społeczeństwa i poszczególnych jego członków, umożliwiającego im stały i → zrównoważony rozwój [t. 4]. Podsystemy te funkcjonują na podstawie przyznanych im kompetencji, realizując różne zadania zmierzające do skutecznego przeciwdziałania wszelkim determinantom zagrożeń oraz zapobiegające czynom godzącym w dobro państwa, jego porządek publiczny, życie, zdrowie i mienie obywateli. Za stworzenie i sprawne funkcjonowanie systemu bezpieczeństwa publicznego odpowiada państwo, dla którego zapewnienie bezpieczeństwa jest jednym z podstawowych i najważniejszych zadań. Do czasu transformacji ustrojowo-politycznej państwa system bezpieczeństwa opierał się na organach administracji państwowej, a szczególna rola przypadała w nim tzw. służbom mundurowym do których zaliczamy: → Policję [t. 3], → Agencję Bezpieczeństwa Wewnętrznego [t. 1], → Agencję Wywiadu [t. 1], → Służbę Kontrwywiadu Wojskowego [t. 4], → Służbę Wywiadu Wojskowego [t. 4], → Centralne Biuro

Antykorupcyjne [t. 1], → Straż Graniczną [t. 4], → Służbę Ochrony Państwa [t. 4], → Państwową Straż Pożarną [t. 4] oraz → Służbę Więzienną [t. 4]. Także obecnie dział administracji rządowej „sprawy wewnętrzne" obejmuje zadania realizowane przez te formacje, z których najważniejsze to: ochrona bezpieczeństwa i porządku publicznego, ochrona granicy państwowej, → zarządzanie kryzysowe [t. 4], → obrona cywilna [t. 3], ochrona przeciwpożarowa, przeciwdziałanie skutkom klęsk żywiołowych, nadzór nad ratownictwem górskim i wodnym.

Demonopolizacja bezpieczeństwa implikowała wprowadzenie do systemu bezpieczeństwa, który do tej pory tworzyły organy administracji państwowej, 2 nowych podsystemów: samorządowego i prywatnego.

Podsystem prywatny tworzą firmy ochrony osób i mienia. Wspólna inicjatywa podjęta przez organy państwowe oraz samorząd gospodarczy prywatnego sektora bezpieczeństwa doprowadziła do uchwalenia przez Sejm 22 sierpnia 1997 r. długo oczekiwanej ustawy o ochronie osób i mienia. Tym samym administracja państwowa, odpowiedzialna za system bezpieczeństwa państwa, uznała, że jej partnerem na poziomie lokalnym będą przedsiębiorcy prowadzący koncesjonowaną działalność gospodarczą, spełniający wysokie, ściśle określone wymagania i zatrudniający pracowników mających odpowiednie kwalifikacje zawodowe. W ramach demonopolizacji bezpieczeństwa rozpoczął się także proces jego komercjalizacji.

Jednak najważniejszym skutkiem demonopolizacji bezpieczeństwa było powstanie podsystemu samorządowego, który stał się ważnym ogniwem w zapewnianiu porządku i bezpieczeństwa publicznego. By mogło to nastąpić, ustawodawca wprowadził nowe regulacje prawne. Kluczowa była Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, która w art. 7 uznała, że zaspokajanie zbiorowych potrzeb wspólnoty mieszkańców należy do zadań własnych gminy. Jako szczególnie ważne zadanie własne wskazała sprawy porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, w tym wyposażenia i utrzymania gminnego magazynu przeciwpowodziowego. Wiodącym partnerem Policji w realizacji zadań z zakresu poprawy stanu bezpieczeństwa i porządku publicznego w mieście stała się → straż miejska [t. 4].

Lokalne → strategie [t. 4] i programy bezpieczeństwa były przyjmowane w gminach, zarówno mających charakter wielkomiejskich aglomeracji, jak i w małych miejscowościach, których mieszkańcy i przedstawiciele samorządów uznali, że sama Policja nie zapewni im bezpieczeństwa. W wielu gminach zaczęły więc funkcjonować komisje ds. porządku i bezpieczeństwa publicznego. Podlegają one radzie gminy, które przedkładają plan pracy oraz okresowe sprawozdania ze swej działalności (art. 21 ustawy o samorządzie gminnym). W zakresie spraw nieuregulowanych w odrębnych ustawach lub innych przepisach powszechnie obowiązujących, rada gminy uzyskała również uprawnienia o charakterze legislacyjnym. Prawo wydawania przepisów porządkowych ma zastosowanie w sytuacji, gdy jest to niezbędne dla ochrony życia lub zdrowia obywateli oraz dla zapewnienia porządku, spokoju i bezpieczeństwa publicznego (art. 40 ust. 3 ustawy o samorządzie gminnym). Kolejnym etapem demonopolizacji bezpieczeństwa było uchwalenie przez Sejm w dniu 5 czerwca 1998 r. kolejnej ustawy rozszerzającej prerogatywy samorządowe w tym obszarze na poziom powiatowy. Powiatom powierzono wykonywanie określonych ustawami zadań publicznych, także w zakresie porządku publicznego i bezpieczeństwa obywateli (art. 4 ust. 1 pkt 15 ustawy o samorządzie powiatowym). Ważną prerogatywą rady powiatu jest uchwalanie powiatowego programu zapobiegania przestępczości oraz ochrony bezpieczeństwa obywateli i porządku publicznego. Do kompetencji komisji należy: ocena zagrożeń porządku publicznego i bezpieczeństwa obywateli na terenie powiatu; opiniowanie pracy Policji i innych powiatowych służb, inspekcji i straży, a także jednostek organizacyjnych wykonujących na terenie powiatu zadania z zakresu porządku publicznego i bezpieczeństwa obywateli; przygotowywanie projektu powiatowego programu zapobiegania przestępczości oraz porządku publicznego i bezpieczeństwa obywateli; opiniowanie projektów programów współdziałania Policji i innych powiatowych służb, inspekcji i straży oraz jednostek organizacyjnych wykonujących na terenie powiatu zadania z zakresu porządku publicznego i bezpieczeństwa obywateli.

W ramach demonopolizacji bezpieczeństwa państwo przyznało prawo administrowania porządkiem i bezpieczeństwem publicznym organom samorządowym, co jednak nie oznacza pozbawienia organów rządowych kompetencji w zakresie realizacji tych zadań. Nadal utrzymywanie

bezpieczeństwa pozostaje przede wszystkim w gestii służb i formacji należących do administracji rządowej, które wykonują podstawowe zadania w tym obszarze. Działalność podmiotów samorządowych i → specjalistycznych uzbrojonych formacji ochronnych [t. 4] należących głównie do sektora prywatnego, komercyjnego ma jedynie charakter uzupełniający i pomocniczy. Jest to spowodowane tym, że samorządy terytorialne, a tym bardziej prywatne firmy ochrony osób i mienia nie posiadają takich uprawnień jak organy rządowe. Stąd koncentrują one swoją uwagę głównie na działaniach o charakterze ochronnym. Najszerszy zakres uprawnień w zakresie bezpieczeństwa został przekazany na szczebel gminy, która realizuje te zadania głównie poprzez tworzenie straży gminnych (miejskich).

Andrzej Czop

A. Czop, *Prywatny sektor ochrony niedocenianym elementem w zarządzaniu bezpieczeństwem wewnętrznym w Polsce* [w:] *Współczesne uwarunkowania zarządzania bezpieczeństwem wewnętrznym państwa*, J. Falecki, R. Kochańczyk, P. Sowizdraniuk (red.), Szkoła Policji w Katowicach, Katowice 2018; tenże, *System bezpieczeństwa publicznego w Polsce*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2012, nr 12; tenże, *Udział firm ochrony osób i mienia w zapewnianiu bezpieczeństwa publicznego w Polsce*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Katowice 2014; M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, AON, Warszawa 2014; W. Kawka, *Policja w ujęciu historycznym i współczesnym*, Drukarnia „Zorza", Wilno 1939.

Deportacja (łac. *deportatio* – zesłanie) – przymusowe przeniesienie lub wydalenie osoby lub grupy osób ze stałego miejsca zamieszkania do innego państwa lub innej miejscowości, zwykle pod nadzorem; wygnanie przestępców, przeciwników politycznych lub całych grup etnicznych z → przemocą [t. 3] państwową w odległe miejsca na długie lub dożywotnie przymusowe pobyty. Deportacja całych grup etnicznych może mieć charakter „czystki etnicznej", mającej na celu ujednolicenie narodowościowe (lub wyznaniowe) danego terytorium.

Termin „deportacja" wywodzi się z ustawodawstwa karnego Francji w XVIII–XIX w. i odnosi się do określonych rodzajów wygnania. Po raz

pierwszy deportacja niewiarygodnych politycznie w Gujanie została ustanowiona na mocy ustawy o podejrzanych z 1791 r. Deportacja, w tym deportacja na całe życie, była przewidziana w kodeksie karnym z 1810 r. i polegała na wygnaniu i życiu poza terytoriami kontynentalnymi, w miejscach deportacji określonych ustawą z 23 marca 1872 r. Prawo to przewidywało utworzenie centralnego obozu deportacyjnego na wyspie Well oraz umocnionego miejsca (fortecy) dla deportowanych na półwyspie Duco w Nowej Kaledonii. Deportacja służyła nie tylko do karania przestępców i recydywistów po odbyciu kary w więzieniach metropolitalnych, ale także do radzenia sobie z rewolucjonistami (w 1872 r. schwytani komuniści zostali deportowani na wyspy archipelagu Nowej Kaledonii).

Deportacja jako forma kary była stosowana od czasów starożytnych w różnych kulturach i jest dobrze opisana, szczególnie w starożytnej Mezopotamii. Z ściśle historycznego punktu widzenia Biblia w kilku fragmentach odnosi się do masowych deportacji, obecnie uznawanych za historyczne: przeniesienie dużej części ludności Izraela do Babilonu, najwyraźniej wbrew ich woli i w celach niewolniczych. W czasach cesarstwa rzymskiego różne plemiona były zmuszane do przemieszczania się w kierunku imperium (Traków, Dalmacji) lub poza nie (Niemcy, Celtowie, Madziarowie), z woli armii rzymskiej lub aby uciec przed naporem swoich wrogów. W późnym średniowieczu całe populacje greckie, albańskie i starożytne imperium bizantyjskie zostały zmuszone do wycofania się ze swoich naturalnych granic w kierunku północno-wschodniej Europy ze względu na spotkania armii krzyżowców z Turkami.

Deportacje można podzielić na następujące rodzaje:

Deportacja więźniów do kolonii karnych – ma długą historię, więźniowie w koloniach mogli w pewnym zakresie swobodnie się przemieszczać. W czasach współczesnych były w dużym stopniu wykorzystywane przez Wielką Brytanię, Australię, Związek Radziecki z obozami karnymi (Gułag), Rosję, Francję, Włochy. W Rosji deportacja więźniów politycznych lub osób po prostu niewygodnych na Syberię była powszechną praktyką od czasów Iwana IV Groźnego i trwa w praktyce nadal, nawet w XXI wieku.

Deportacja niechcianych osób – obejmuje osoby, które nie popełniły żadnych przestępstw, ale nie chcą pozostać na miejscu.

Takie deportacje były przeprowadzane w różnym stopniu przez właściwie wszystkie → dyktatury.

Deportacja grup osób – w latach 1863–1880 miały miejsce masowe deportacje z Polski na Syberię. Konflikty narodowościowe dawały częste okazje do deportacji mniejszości.

Deportacje na podstawie umów – np. deportacje rdzennych Amerykanów oparte o ustawę o przeprowadzkach z 1830 r. oraz umowy o ich transporcie zawarte między USA a poszczególnymi plemionami indiańskimi, w szczególności przymusowe przesiedlenia z żyznych lasów południowo-wschodnich USA na dość jałowe ziemie mieszczące się w granicach współczesnej Oklahomy. Innymi przykładami mogą być: wymiana ludności między Grecją a Turcją na podstawie traktatu z Lozanny z 24 lipca 1923 r.; porozumienie w sprawie przesiedlenia Południowych Tyrolczyków między Niemcami a Włochami z czerwca 1939 r.; niemiecko-sowiecki traktat o granicy i przyjaźni po podziale Polski, kiedy uzgodniono wymianę mniejszości między Niemcami a Związkiem Radzieckim. Dotknęło to grup etnicznie niemieckich, a także Ukraińców i Białorusinów mieszkających w Niemczech i okupowanej przez Niemcy Polsce. Największym przesiedleniem z udziałem ok. 20 mln osób był podział Indii. W ramach negocjacji niepodległościowych uzgodniono przeprowadzenie relokacji z perspektywy religijnej. Muzułmanie powinni byli przenieść się do nowo powstającego Pakistanu, a Hindusi do Indii. Niewłaściwe przygotowanie, nieodpowiednie wsparcie i niesprawiedliwości związane z przesiedleniem doprowadziły do ataków, zamieszek, gwałtownego przesiedlenia i ucieczek, co poskutkowało około milionem ofiar śmiertelnych.

Deportacje z przyczyn ekonomicznych – przykładem deportacji z przyczyn ekonomicznych, ale również politycznych są tzw. *Highland Clearances* w Szkocji w XVIII i XIX wieku. W 1707 r. doszło do zawarcia unii pomiędzy Anglią i Szkocją i powstania Królestwa Wielkiej Brytanii. W latach 1715 i 1746 wybuchły krwawo stłumione powstania jakobitów, będące ostatnimi znaczącymi przejawami oporu Szkotów przeciwko dominacji angielskiej. Anglicy, obawiając się kolejnych zamieszek, rozpoczęli egzekucje i deportacje

mieszkańców regionu Highlands; przystąpili do likwidacji struktury klanów, zabronili również przestrzegania tradycyjnych obyczajów. Chłopi, pozbawieni ziemi, emigrowali do Ameryki. Na wyludnionych terenach Anglicy zakładali hodowle owiec. Dopiero wprowadzony w 1886 r. Cro ers' Holding Act, który chronił prawa drobnych posiadaczy ziemi, zakończył okres wyludnienia regionu.
Deportacje grup ludzi do pracy przymusowej – dotknęły obywateli we wszystkich krajach okupowanych przez nazistowskie Niemcy podczas II wojny światowej (niem.*Ostarbeiter*– robotnicy ze wschodu). Od grudnia 1944 r. radzieckie tajne służby NKWD deportowały setki tysięcy niemieckich cywilów do pracy przymusowej w obozie Związku Radzieckiego (Gułag), głównie kobiet. Te cywilne deportacje zostały uznane przez aliantów na konferencji w Jałcie jako reparacje w naturze. Około 1/3 deportowanych zmarło w wyniku uwięzienia z głodu, chorób i zimna lub podczas transportu w wagonach dla bydła. Szacuje się, że 1,7–2 mln ludzi w Kambodży zostało deportowanych do obozów śmierci z powodów polityczno-ideologicznych w czasach Czerwonych Khmerów pod rządami komunistycznego → r e ż i m u [t. 3] Mao Pol Pota, gdzie zostali zamordowani lub umarli podczas pracy przymusowej na polach ryżowych.
Deportacje jako sankcja – deportacja duńskich funkcjonariuszy → p o l i c j i [t. 3] do niemieckich obozów koncentracyjnych miała miejsce w 1944 r. podczas II wojny światowej po rozbrojeniu i rozwiązaniu duńskiej policji (operacja Möwe). Zatrzymani policjanci zostali najpierw deportowani do obozu koncentracyjnego Neuengamme, a następnie do obozu koncentracyjnego Buchenwald. Natomiast w ZSRR Koreańczykom nie wolno było podróżować poza Azję Środkową i służyć w wojsku, ale poza tym zachowali oni prawa obywateli radzieckich. Mniejszość koreańska to ok. 200 tys. mieszkańców Dalekiego Wschodu, którzy padli o arą represji państwowych w 1937 r. Podczas deportacji Koreańczycy zostali załadowani do wagonów bydlęcych, a także przetransportowani do Kazachstanu lub Uzbekistanu. W specjalnych lokalizacjach osadniczych byli wykorzystywani do pracy przymusowej i mieszkali w warunkach

ograniczonych praw i wolności. Większość z nich była wcześniej rolnikami i rybakami i miała trudności z przystosowaniem się do jałowego środowiska Azji Środkowej. Szacuje się, że w pierwszych latach po deportacji zmarło do 40 tys. Koreańczyków. Deportowani Koreańczycy etniczni nie mogli wrócić do domu. Szkoły koreańskie i używanie języka koreańskiego zostały zakazane.

Deportacje przeciwników politycznych – wiele osób, które opar-ło się nazistom, zostało deportowanych po dekrecie z 7 grudnia 1941 r., jeżeli nie zostali zabici. Z powodu złych warunków trans-portu (brak wody, brak powietrza itp.) duża część więźniów zginęła w pociągach w trakcie przewozu.

Deportacje ze względów religijnych – do XVIII w. deportacje z po-wodów religijnych miały miejsce w Szwajcarii: menonici zostali wydaleni, zwłaszcza w kantonie Berno, z pomocą państwowych anabaptystów w celu ochrzczenia terytorium. W XX w. w ZSRR w czasach Stalina deportowano na Syberię rosyjsko-niemieckich menonitów oraz Świadków Jehowy i członków ich rodzin.

Deportacje narodów – były szeroko stosowane w ZSRR, będąc formą represji, stanowiąc rodzaj narzędzia radzieckiej polityki demogra cznej i narodowej. Zarówno jednostki, jak i całe narody, uznane przez o cjalne władze za społecznie niebezpieczne, zostały poddane przymusowej migracji do odległych części kraju. Depor-tacja ludności była przymusową relokacją obywateli z przyczyn narodowych i społecznych do różnych regionów ZSRR. W zależ-ności od przyczyn przesiedlenia i potrzeb ekonomicznych państwa docelowe miejsca deportacji były różne – Syberia, miasta Uralu, Kazachstan, Azja Środkowa i in.

Deportacja osób – wszystkie kraje zastrzegają sobie prawo do deportacji osób bez prawa pobytu, nawet tych, które są rezyden-tami długoterminowymi lub posiadają stałe miejsce zamieszkania. Zasadniczo cudzoziemcy, którzy popełnili poważne przestępstwa, nielegalnie wjechali do kraju, przedłużyli lub złamali warunki wizy lub w inny sposób utracili status prawny umożliwiający pozostanie w kraju, mogą zostać administracyjnie wydaleni lub deportowani. W niektórych przypadkach nawet obywatele mogą

być deportowani. Niektóre kraje zachodnie mają również możliwość deportacji obywateli, jeśli mają inną narodowość lub nabywają obywatelstwo w wyniku oszustwa. Np. w latach 30. XX w., podczas Wielkiego Kryzysu, bardziej rygorystyczne egzekwowanie przepisów imigracyjnych doprowadziło do wydalenia nawet 2 mln obywateli Meksyku z USA. Deportacja często wymaga określonego procesu, który musi zostać zatwierdzony przez sąd, lub uprawnień wyższego urzędnika państwowego.

Począwszy od lat 20. XX wieku, deportacje osiągnęły szczyt w pierwszej połowie lat 30. XX wieku, kiedy to miliony chłopów z Ukrainy, Białorusi i Korei zostały deportowane na Syberię i na daleką północ ZSRR. Pierwsza deportacja w historii ZSRR, która miała miejsce ze względu na narodowość, dotyczyła Finów. W 1935 r. podjęto decyzję o wydaleniu ludności ńskiej z obszarów przygranicznych na północnym zachodzie. Kilkadziesiąt tysięcy Finów z Petersburga przeniesiono do obwodu wołogodzkiego. Była to jedna z pierwszych z serii operacji mających na celu „oczyszczenie" granic i przygotowanie się do działań wojennych.

Wraz z wybuchem II wojny światowej deportacja mniejszości etnicznych osiągnęła największy zasięg. Całe ludy zostały wspólnie „ukarane". Oskarżenie o „zdradę" sowieckiego systemu było regularnie podawane jako o cjalny powód deportacji. W wyniku przymusowych eksmisji w latach 1939–1940 ucierpiała ludność zachodniej Ukrainy, zachodniej Białorusi i państw bałtyckich. W czasie → w o j n y [t. 4] w latach 1941–1944 Niemcy zostali deportowani na odległe obszary Syberii, podobnie przedstawiciele narodów, których kraje były członkami koalicji hitlerowskiej (Węgrzy, Bułgarzy, Finowie).

Najbardziej brutalne były deportacje wojenne. W latach 1942–1945 Kałmucy, Niemcy, Finowie, Tatarzy krymscy, Karaczajowie, Czeczeni, Bałkani, Turcy meschetyńscy i inne ludy, mieszkańcy terytoriów radzieckich pod okupacją niemiecką, obywatele Europy Wschodniej, w tym rosyjscy emigranci, zostali deportowani. Po sowietyzacji Mandżurii w sierpniu i wrześniu 1945 r. chińscy, japońscy i rosyjscy emigranci również zostali deportowani. W 1944 r. pod zarzutem współpracy z Niemcami przymusowo zostali zmuszeni do eksmisji Tatarzy krymscy, Kałmucy, Inguszowie, Czeczeni, Karaczajowie, Bałkarzy, Nogajowie, Turcy meschetyńscy.

Szacuje się, że wewnętrzne przymusowe migracje w ZSRR dotknęły ok. 6 mln ludzi. Spośród nich zginęło ok. 1–1,5 mln osób. Deportacjom towarzyszyła likwidacja ich autonomii.

W wyniku deportacji narodów etnicznych z Kaukazu Północnego i Krymu ok. 870 tys. osób musiało opuścić swoje domy. Wraz z Niemcami liczba deportowanych obywateli w latach wojny 1941–1945 wynosiła ok. 2,3 mln osób. Opuszczone obszary zostały ponownie zaludnione przez rosyjskojęzycznych obywateli. Łącznie daje to ok. 3 mln ofiar całkowitej deportacji etnicznej.

Rehabilitacja deportowanych ludów w ZSRR rozpoczęła się w latach 1957–1958, a ograniczenia zostały ostatecznie zniesione 14 listopada 1989 r. Deklaracją Rady Najwyższej ZSRR.

Po „przymusowej emigracji" i wydaleniu Żydów z Niemiec po rozpoczęciu wojny niemiecko-radzieckiej 22 czerwca 1941 r. zaczęła się systematyczna deportacja i mordowanie wszystkich europejskich Żydów w obozach koncentracyjnych. Z tzw. względów higieny rasowej naziści zmuszali zarówno żydowskich Niemców, jak i żydowskich mieszkańców terenów okupowanych i kontrolowanych przez Niemcy w czasie II wojny światowej w Europie Zachodniej, a zwłaszcza w Europie Wschodniej (w tym w Belgii, Danii, Francji, Grecji, Luksemburgu, Holandii, Norwegii, Polsce i Węgrach).

Proces przymusowego wysiedlenia niemieckiej ludności krajów Europy Wschodniej do Niemiec i Austrii miał miejsce w latach 1945–1950 po klęsce Niemiec w II wojnie światowej. W sumie ok. 12–14 mln Niemców zostało poddanych przymusowej eksmisji. Procesowi wydalenia Niemców z Europy Wschodniej towarzyszyła zorganizowana przemoc o ogromnych rozmiarach, w tym konfiskata całej własności, umieszczanie niemieckich cywilów w obozach koncentracyjnych, pomimo uznania deportacji za → zbrodnię przeciwko ludzkości [t. 4] podczas trybunału wojskowego w Norymberdze w sierpniu 1945 r.

W przeciwieństwie do terminu deportacji istnieje definicja przymusowego wygnania, która opiera się głównie na ograniczeniach swobodnego rozwoju jednostki w pierwotnym miejscu zamieszkania. W nowo wybranym miejscu docelowym państwo odpowiedzialne za wygnanie nie nakłada ograniczeń ani sankcji na wolność osobistą. Termin „migracja

przymusowa", który obejmuje także przesiedlenia, dominował w latach 80. XX w., ponieważ miał zastosowanie do różnych rodzajów przemieszczeń ludności w XX w. i określał masową przemoc jako główną ich przyczynę.

Ochronę prawną przed deportacjami zapewnia Powszechna Deklaracja Praw Człowieka ONZ (art. 9 i 12) w czasach pokoju oraz art. 49 IV Konwencji genewskiej z 12 sierpnia 1949 r. w czasie wojny lub okupacji wojskowej. Jeżeli deportacja wiąże się z pracą przymusową, narusza ona art. 4 Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności (ETPC), zgodnie z którym nikt nie może zostać wydalony z terytorium państwa, którego jest obywatelem, i żadnemu obywatelowi nie może być zakazany wjazd na jego terytorium. Zgodnie z art. 7 Rzymskiego Statutu Międzynarodowego Trybunału Karnego z 17 lipca 1998 r. „deportacja lub przymusowe przemieszczanie ludności" odnosi się do zbrodni przeciwko ludzkości i pociąga za sobą międzynarodową odpowiedzialność karną. Deportacje są ścigane przez → Międzynarodowy Trybunał Karny [t. 3] w Hadze jako zbrodnie przeciwko ludzkości (w czasie pokoju) lub jako → zbrodnie wojenne [t. 4]. Już w prawie naturalnym XVIII w. lozofowie zgodzili się, że wydalenie narodu z terytorium, w którym historycznie zamieszkuje, jest niedopuszczalne. Pod koniec XX wieku Organizacja Narodów Zjednoczonych opracowała kodeks dotyczący zbrodni przeciwko ludzkości. Art. 18 kodeksu zbrodni przeciwko pokojowi i → bezpieczeństwu [t. 1] ludzkości określa arbitralną lub przymusową deportację na dużą skalę jako zbrodnię przeciwko ludzkości.

Obecnie termin deportacja jest równoznaczny z wydaleniem administracyjnym i oznacza rodzaj kary administracyjnej stosowanej wyłącznie wobec cudzoziemców lub bezpaństwowców, polegający na ich kontrolowanym, dobrowolnym wyjeździe lub przymusowym wydaleniu (w tym pod eskortą) z kraju przyjmującego.

Olga Wasiuta

S. Ciesielski, G. Hryciuk, A. Srebrakowski, *Masowe deportacje ludności w Związku Radzieckim*, Wydawnictwo Adam Marszałek, Toruń 2003; ciż, *Masowe deportacje radzieckie w okresie II wojny światowej. Prace Historyczne*, Instytut Historyczny Uniwersytetu Wrocławskiego, Wrocław 1994; S. Ciesielski, W. Materski,

A. Paczkowski, *Represje sowieckie wobec Polaków i obywateli polskich*, Ośrodek Karta, Warszawa 2000; P. Christensen, *e Decline of Iranshahr: Irrigation and Environments in the History of the Middle East, 500 B.C. to A.D. 1500*, Museum Tusculanum Press, Copenhagen 1993; R. Conquest, *e Nation Killers*, Macmillan, New York 1970; S. Coutin, *Exiled by Law: Deportation and the Inviolability of Life* [w:] *e Deportation Regime: Sovereignty, Space, and the Freedom of Movement* N. De Genova, N. Peutz (ed.), Duke University Press Books, Durham 2010; R. Daniels, *Coming to America: A History of Immigration and Ethnicity in American Life*, HarperCollins, New York 2002; R. Fischer, J.C. Leggett, *Stalin and German Communism: A Study in the Origins of the State Party*, Transaction Publishers, New York 2006; A.T. Fragomen, S.C. Bell, *Immigration Fundamentals: A Guide to Law and Practice*, Practising Law Institute, New York 1996; A. Gil, *Deportacja Ukraińców z Polski w latach 1944–1946 jako problem we współczesnych relacjach polsko-ukraińskich*, Instytut Europy Środkowo-Wschodniej, Warszawa 2004; B.O. Hing, *De ning America rough Immigration Policy* Temple University Press, Philadelphia 2004; A.M. Jaimoukha, *e Chechens: A Handbook*, Routledge, Florence 2005; E. Mawdsley, *e Stalin Years: e Soviet Union 1929–1953*, Manchester University Press, Manchester 2003; A. Radziwinowiczówna, *Doświadczenie deportacji: przemoc orężem suwerenności*, „Praktyka Teoretyczna" 2016, nr 3 (21).

Detektywistyka – to regulowana działalność gospodarcza prowadzona przez przedsiębiorcę posiadającego wpis do rejestru prowadzonego przez ministra właściwego do spraw wewnętrznych, polegająca na świadczeniu usług detektywistycznych.

Podstawowym aktem prawnym, który traktuje o prowadzeniu działalności gospodarczej, jest Konstytucja Rzeczypospolitej Polskiej, która w art. 20 stanowi, że społeczna gospodarka rynkowa jest oparta na wolności działalności gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych, będąc podstawą ustroju gospodarczego RP. Ograniczenie wolności działalności gospodarczej jest dopuszczalne wyjątkowo i może nastąpić jedynie w drodze ustawy, o ile wymaga tego ważny interes publiczny.

De nicja działalności gospodarczej określona w Ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej wskazuje, że jest to: zarobkowa działalność wytwórcza, budowlana, handlowa, usługowa oraz poszukiwanie, rozpoznawanie i wydobywanie kopalin ze złóż, a także działalność zawodowa, wykonywana w sposób zorganizowany i ciągły.

Ważnym desygnatem tej działalności jest jej charakter zarobkowy, co oznacza, że przedsiębiorca winien w swej aktywności dążyć do odniesienia zysku. Przedsiębiorcą może być osoba fizyczna, osoba prawna i jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznaje zdolność prawną – wykonująca we własnym imieniu działalność gospodarczą. *Expressis verbis* ustawodawca wskazuje, że dany podmiot, aby mógł zostać uznany za przedsiębiorcę, musi posiadać zdolność prawną. Przedsiębiorca prowadzi działalność gospodarczą w imieniu własnym, co świadczy o jego autonomii prawnej i nabywaniu bezpośrednim praw i obowiązków w stosunkach cywilnoprawnych.

Przedsiębiorca prowadzący firmę detektywistyczną świadczy usługi polegające na uzyskiwaniu, przetwarzaniu i przekazywaniu → informacji o osobach, przedmiotach i zdarzeniach. Są one realizowane na podstawie umowy zawartej ze zleceniodawcą, w formach i w zakresach niezastrzeżonych dla organów i instytucji państwowych. W szczególności działania te obejmują sprawy wynikające ze stosunków prawnych dotyczących osób fizycznych oraz sprawy wynikające ze stosunków gospodarczych. W tym obszarze mogą dotyczyć wykonania zobowiązań majątkowych, zdolności płatniczych lub wiarygodności w tych stosunkach, a także bezprawnego wykorzystywania nazw handlowych lub znaków towarowych. Przedmiotem usług detektywistycznych mogą być też przejawy nieuczciwej konkurencji lub kwestie ujawnienia wiadomości stanowiących tajemnicę przedsiębiorstwa lub tajemnicę handlową. Usługi mogą też dotyczyć wiarygodności informacji o szkodach zgłaszanych zakładom ubezpieczeniowym.

Osobnym obszarem aktywności detektywistycznej jest poszukiwanie osób zaginionych lub ukrywających się oraz poszukiwanie mienia. Detektywi mogą również zbierać informacje w sprawie, w której toczy się postępowanie karne, postępowanie w sprawach o przestępstwa skarbowe lub wykroczenia skarbowe, ale zleceniodawcą tych czynności nie mogą być organy prowadzące lub nadzorujące postępowania w tych sprawach. Wykonywanie działalności gospodarczej w zakresie usług detektywistycznych jest działalnością regulowaną w rozumieniu przepisów Ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej i wymaga uzyskania wpisu do rejestru działalności detektywistycznej. Działalność

regulowana to taka działalność gospodarcza, której wykonywanie wymaga posiadania określonych kwali kacji i dozwolona jest dopiero po uzyskaniu zezwolenia, które można zdobyć po spełnieniu wymogów określonych przepisami prawnymi danego państwa.

Wg Dyrektywy 2005/36/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. zawód regulowany to działalność zawodowa lub zespół działalności zawodowych, których podjęcie, wykonywanie lub jeden ze sposobów wykonywania wymaga posiadania specjalnych kwali kacji zawodowych. W szczególności używanie tytułu zawodowego zastrzeżone jest na mocy przepisów ustawowych, wykonawczych i administracyjnych dla osób posiadających odpowiednie kwali kacje zawodowe.

Polskie prawo stanowi, że tytułu zawodowego „detektyw" może używać wyłącznie osoba posiadająca licencję. Przedsiębiorca będący osobą zyczną może wykonywać działalność detektywistyczną, o ile posiada licencję detektywa lub ustanowił pełnomocnika, który ma taką licencję. W przypadku przedsiębiorcy niebędącego osobą zyczną licencję musi posiadać co najmniej jedna osoba uprawniona do reprezentowania rmy lub pełnomocnik ustanowiony przez przedsiębiorcę do kierowania działalnością detektywistyczną. Przedsiębiorca ten nie może być wpisany do rejestru dłużników niewypłacalnych Krajowego Rejestru Sądowego. Osoby nieposiadające licencji, wchodzące w skład organu zarządzającego przedsiębiorcy oraz ustanowieni przez ten organ prokurenci i przedsiębiorca będący osobą zyczną nie mogą być osobami wcześniej karanymi za przestępstwa umyślne lub umyślne przestępstwa skarbowe. Organem prowadzącym rejestr rm detektywistycznych jest minister właściwy do spraw wewnętrznych.

Przedsiębiorca jest zobowiązany do zachowania formy pisemnej umów w zakresie usług detektywistycznych. Musi też prowadzić oraz przechowywać dokumentację dotyczącą zatrudnianych detektywów oraz zawieranych i realizowanych umów. Jest zobowiązany do przedstawiania tej dokumentacji, na żądanie upoważnionego do kontroli organu. Ponadto ma zachować w tajemnicy źródła informacji oraz okoliczności sprawy, o których dowiedział się w związku z wykonywaniem zlecenia. Ponosi również, na zasadach określonych w kodeksie cywilnym, odpowiedzialność za wszelkie szkody wyrządzone podczas wykonywania usług

detektywistycznych oraz wskutek podania nieprawdziwych informacji. W związku z tym na przedsiębiorcy ciąży też obowiązek zawarcia umowy ubezpieczenia od odpowiedzialności cywilnej za takie właśnie szkody. Przedsiębiorca może sam wykonywać czynności detektywistyczne, o ile posiada licencję detektywa lub może przekazać ich realizację zatrudnionym pracownikom, którzy uzyskali takie licencje.

O wydanie licencji detektywa może ubiegać się osoba, która posiada obywatelstwo polskie lub obywatelstwo innego państwa członkowskiego Unii Europejskiej lub przysługuje jej, na podstawie umów międzynarodowych lub przepisów prawa UE, prawo do podjęcia zatrudnienia lub wykonywania działalności gospodarczej na terytorium RP. Musi mieć ukończone 21 lat i posiadać wykształcenie co najmniej średnie. Koniecznym warunkiem jest także pełna zdolność kandydata do czynności prawnych. Nie może toczyć się przeciwko niemu postępowanie o umyślne przestępstwo lub umyślne przestępstwo skarbowe. Nie może to być osoba skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe ani też zwolniona dyscyplinarnie z → Policji [t. 3], → Straży Granicznej [t. 4], → Agencji Bezpieczeństwa Wewnętrznego [t. 1], → Agencji Wywiadu [t. 1], → Służby Ochrony Państwa [t. 4], wojska, → prokuratury [t. 3], sądu lub z innego urzędu administracji publicznej w RP lub innym państwie, w okresie ostatnich 5 lat. Konieczne jest posiadanie pozytywnej opinii wydawanej przez komendanta powiatowego (rejonowego, miejskiego) Policji właściwego ze względu na miejsce zamieszkania kandydata. W toku badań lekarskich stwierdzana jest jego zdolność fizyczna i psychiczna do wykonywania czynności detektywa.

Przyszły detektyw musi legitymować się dokumentem potwierdzającym odbycie szkolenia w zakresie: zagadnień ochrony danych osobowych, ochrony → informacji niejawnych, przepisów regulujących prawa i obowiązki detektywa oraz zasad wykonywania działalności gospodarczej w zakresie usług detektywistycznych. Licencję w drodze decyzji administracyjnej wydaje lub odmawia jej wydania komendant wojewódzki Policji właściwy ze względu na miejsce zamieszkania osoby ubiegającej się o wydanie licencji. W przypadku osoby niemającej miejsca zamieszkania na terytorium RP organem właściwym jest Komendant Stołeczny Policji.

Wprawdzie licencję wydaje się na czas nieoznaczony, ale jej posiadacz jest obowiązany poddawać się okresowym badaniom lekarskim i psychologicznym. Detektyw powinien przy wykonywaniu czynności kierować się zasadami etyki, lojalnością wobec zlecającego usługę i szczególną starannością, aby nie naruszyć wolności i → prawa człowieka [t. 3] i obywatela. Wykonuje bowiem zawód zaufania publicznego. Trybunał Konstytucyjny w orzeczeniu z 7 maja 2002 r. (w sprawie SK 20/00) orzekł, że

> „zawód zaufania publicznego" to zawód polegający na obsłudze osobistych potrzeb ludzkich, wiążący się z przyjmowaniem informacji dotyczących życia osobistego i zorganizowany w sposób uzasadniający przekonanie społeczne o właściwym dla interesów jednostki wykorzystywaniu tych informacji przez świadczących usługi.

Nie ma żadnych wątpliwości, że detektyw spełnia wskazane w tym wyroku warunki.

W trakcie wykonywania czynności detektyw może uzyskiwać informacje zarówno od osób fizycznych i przedsiębiorców, jak i od instytucji, a także organów administracji rządowej lub samorządowej. Detektyw podczas pracy jest obowiązany do przestrzegania przepisów prawa oraz odmowy wykonania czynności niezgodnej z prawem lub nieetycznej. Musi także zachować należytą staranność i rzetelność, a zwłaszcza sprawdzać zgodność z prawdą uzyskanych informacji. Ma obowiązek zachować w tajemnicy źródła informacji oraz okoliczności sprawy, o których dowiedział się w trakcie wykonywania zleconych czynności. Ten obowiązek ciąży na nim także po zaprzestaniu pracy w zawodzie detektywa. Wykonując powierzone mu czynności, musi mieć przy sobie licencję oraz okazywać ją na żądanie osoby, której czynności dotyczą. Detektyw nie może stosować środków technicznych oraz metod i → czynności operacyjno-rozpoznawczych [t. 1] zastrzeżonych dla upoważnionych organów na mocy odrębnych przepisów. Oznacza to, że nie wolno mu stosować → podsłuchów [t. 3], gdyż naraża się wówczas na odpowiedzialność karną określoną w art. 267 kk § 3. Przepis ten przewiduje karę za uzyskiwanie informacji poprzez zakładanie lub posługiwanie się

urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

23 marca 2011 r. SN odmówił odpowiedzi na pytanie prawne sądu w sprawie detektywa – oskarżonego przez pewną kobietę o umieszczenie lokalizatora GPS w jej aucie – ale zarazem wypowiedział się co do istoty sprawy. Sąd pytał, czy takie zainstalowanie GPS dopuszcza ustawa o usługach detektywistycznych, czy też jest ono czynnością operacyjno-rozpoznawczą zastrzeżoną dla „upoważnionych organów". Sędzia SN A. Ryński mówił, że ustawa o usługach detektywistycznych nie ogranicza rodzaju informacji zdobywanych przez detektywów, ale ogranicza środki ich uzyskiwania. Detektyw może zatem zdobywać informacje wkraczające np. w kwestie relacji małżeńskich – uznano. Ale już środki techniczne niejawnego zdobywania informacji są zastrzeżone dla organów państwa. SN powołał się m.in. na wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu, który w 2010 r. uznał, że użycie lokalizatora GPS może prowadzić do naruszenia prawa do prywatności, także przez organy władzy. Ryński podkreślił, że w Niemczech zgodę na użycie GPS przez służby wydaje prokurator generalny. Jedyne szczególne uprawnienie nadane detektywowi – szersze niż wynikające z uprawnień obywatelskich – to prawo do przetwarzania danych osobowych zebranych w toku wykonywanej usługi bez zgody osób, których informacje dotyczą. Jednak ustawodawca zastrzegł, że nie może być to czynione dla innego podmiotu, a sam proces powinien być zgodny z przepisami ustawy o ochronie danych osobowych z wyłączeniem przepisów dotyczących konieczności uzyskania zgody. Można zatem powiedzieć, że profesja detektywa jest związana z dużym ryzykiem prawnym.

Andrzej Czop

M. Berent, W.J. Modrakowski, *Etyka zawodu detektywa w kontekście standardu minimalnego Internationale Kommission der Detektiv-Verbände*, „Krytyka Prawa" 2016, nr 1, t. 8; D. Brakoniecki, *Detektywistyka – prawne i funkcjonalne aspekty działalności detektywistycznej w Polsce i na świecie*, Di n, Warszawa 2016; G. Goz dór, *Usługi detektywistyczne. Komentarz*, Wydawnictwo C.H.Beck, Warszawa 2014; J. Konieczny, T. Aleksandrowicz, A. Konik, *Podstawy detektywistyki. Usługi detektywistyczne, prawo, taktyka, moralność*, Wydawnictwa Akademickie i Profesjonalne,

Warszawa 2008; K. Turaliński, *Wywiad Gospodarczy i Polityczny – podręcznik dla specjalistów ds. bezpieczeństwa, detektywów i doradców gospodarczych*, Wydawnictwo ARTEFAKT.edu.pl, Warszawa 2015; Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych, Dz. U. 2002, nr 12, poz. 110.

Dezercja – ucieczka, zbiegostwo → żołnierzy [t. 4] z armii, porzucenie pełnionej służby, samowolne oddalenie się z pola walki, samowolne opuszczenie wojska w czasie pokoju lub w czasie → wojny [t. 4] lub inne zachowanie cechujące się rezygnacją z czegoś z powodu braku odwagi, by stawić czoła trudnościom.

Pojęcie dezercji znane jest polskiemu prawu karnemu – przestępstwo to polega na opuszczeniu jednostki lub wyznaczonego miejsca przebywania lub pozostaniu w takim miejscu – może ono zostać popełnione zarówno przez działanie, jak i przez zaniechanie. Jest to przestępstwo indywidualne, czyli takie, które popełnić może wyłącznie osoba pełniąca czynną służbę wojskową, z wyjątkiem terytorialnej służby wojskowej pełnionej dyspozycyjnie. De nicja legalna żołnierza ujęta została w z art. 115 § 17 kk. Dalsze doprecyzowanie tego pojęcia zawiera ustawa o służbie wojskowej żołnierzy zawodowych (art. 3 ust. 1 i 1a oraz art. 124) oraz ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (art. 59).

Jednostką wojskową jest natomiast wyodrębniony administracyjnie i gospodarczo oddział lub instytucja wojskowa rozlokowana w wyraźnie wskazanym rejonie lub miejscu. Wyznaczone miejsce przebywania de niuje się jako znajdujący się poza jednostką wojskową rejon (np. szpital, warsztat, plac ćwiczeń, poligon, magazyn, areszt dyscyplinarny, sąd, żandarmeria czy → prokuratura [t. 3]), do którego żołnierz jest oddelegowany w celu wykonywania określonych zadań związanych ze służbą.

Od dezercji odróżnić należy samowolne opuszczenie przez żołnierza jednostki lub wyznaczonego miejsca przebywania albo samowolne poza nimi pozostawanie w wymiarze nieprzekraczającym jednorazowo 48 godzin, które stanowi odrębne przestępstwo zgodnie z art. 338 § 1 kk, jeżeli miało miejsce przynajmniej 2-krotnie w okresie 3 miesięcy. Sposób popełnienia przestępstwa w obu przypadkach jest zbliżony, różnią się one jednak zamiarem przyświecającym sprawcy. W obu przypadkach żołnierz świadomie łamie zasady → dyscypliny wojskowej, jednak

dla uznania jego absencji za dezercję konieczne jest nie tylko stwierdzenie, że trwała ona dłużej niż 48 godzin, ale też że jego celem było trwałe uchylanie się od służby wojskowej.

Typy kwalifikowane przestępstwa dezercji dotyczą sytuacji, gdy wystąpiła przynajmniej jedna z następujących okoliczności: dezerter działał wspólnie z innymi żołnierzami lub dokonał zaboru broni albo dezerter podjął ucieczkę za granicę bądź też uchylał się od powrotu do kraju z zagranicy. Każdy z tych przypadków zagrożony jest wyższą karą niż popełnienie przestępstwa w typie podstawowym.

Kodeks wprowadza karalność czynności przygotowawczych do wszystkich odmian przestępstwa dezercji, także do odmiany podstawowej.

Aktualnie obowiązujący kodeks karny z 1997 r. przyniósł złagodzenie podejścia ustawodawcy do przestępstwa dezercji. Warto zauważyć, że wszystkie typy przestępstwa dezercji stanowią występki, a nie zbrodnie. Odmiennie natomiast kwestia ta była uregulowana w poprzednio obowiązującym kodeksie karnym z 1969 r., w którym typy kwalifikowane dezercji, z uwagi na wymiar grożącej za nie kary, stanowiły zbrodnie. Zmiany zaszły także w sposobie ujęcia typów kwalifikowanych: kodeks z 1969 r. zawierał sformułowanie „dopuszcza się dezercji z zamiarem ucieczki za granicę lub urzeczywistnia taki zamiar w czasie trwania dezercji", co potencjalnie dawało szersze możliwości surowego ukarania poprzez relatywnie łatwą możliwość przypisania zamiaru ucieczki za granicę. Ponadto wydatnie złagodzono sankcje, różnicując równocześnie surowość ustawowego → zagrożenia [t. 4] w zależności od tego, czy chodzi o dezercję zbiorową lub dezercję łączącą się z zabraniem broni, czy też dezercję połączoną z ucieczką za granicę lub uchylaniem się od powrotu do kraju – wcześniej groziła za to jednakowa sankcja: kara pozbawienia wolności od lat 3 do 15. Kodeks Karny Wojska Polskiego z 1957 r. za dezercję w czasie wojny połączoną z zaborem broni oraz za dezercję zbiorową w czasie wojny przewidywał obok kary więzienia także karę śmierci. Dla porównania, wojskowy kodeks karny z 1932 r. za opuszczenie jednostki lub stanowiska służbowego wbrew obowiązkowi służbowemu groził więzieniem do lat 2, w czasie wojny do lat 3. W przypadku, gdy sprawca działał w zamiarze trwałego uchylenia się od obowiązku wojskowego bądź gdy nieobecność w jednostce trwała dłużej niż 6 miesięcy, czyn był zagrożony karą pozbawienia wolności do

lat 10, jego popełnienie w czasie wojny skutkowało podniesieniem dolnego pułapu kary od 1 roku pozbawienia wolności. Dopuszczenie się dezercji w obliczu nieprzyjaciela karane było śmiercią.

Problematyka dezercji nie jest szeroko ujmowana w prawie międzynarodowym. Przyjmuje się, że dezerterom przysługuje status jeńców wojennych.

Anna Pacholska

J. Majewski, *Art. 338*, [w:] *Kodeks Karny. Część szczególna. Tom III. Komentarz do art. 278–363*, A. Zoll (red.), Wolters Kluwer Polska, Warszawa 2016; A. Pacholska, *Dezercja*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; S.M. Pryjemski, M. Rogacka-Rzewnicka, *Przestępstwa przeciwko obowiązkowi pełnienia służby wojskowej i przeciwko zasadom pełnienia służby*, [w:] *System Prawa Karnego. Tom 11. Szczególne dziedziny prawa karnego. Prawo karne wojskowe, skarbowe i pozakodeksowe*, M. Bojarski (red.), Wydawnictwa C.H.Beck, Instytut Nauk Prawnych PAN, Warszawa 2018; Ustawa z dnia 6 czerwca 1997 r., Kodeks karny, Dz. U. 2019.1950 t.j.

Dezercja w armiach europejskich – zjawisko → dezercji jest znane od starożytności, zawsze stanowiły one jedno z najpoważniejszych → zagrożeń [t. 4] dla stabilnego funkcjonowania każdej armii. W kodeksach wojskowych dezercje traktowano jako poważne przestępstwo. Do XIX w. dezercje prawie zawsze były karane wyrokiem śmierci. Rozstrzelanie dezerterów orzekały sądy wojskowe, często sądy doraźne, a wykonywały specjalne plutony egzekucyjne. XIX w. przyniósł jednak zmiany w ocenie dezercji. Zaczęto rozróżniać długotrwałą ucieczkę z armii, czyli dezercję, i krótkotrwałe tzw. samowolne oddalenie się, po którym → żołnierze [t. 4] dobrowolnie powracali do macierzystych jednostek wojskowych. W wielu państwach zaczęto zupełnie odmiennie traktować zbiegostwo w czasie pokoju i w czasie walki. W większości kodeksów wojskowych dezercje z pola walki były znacznie bardziej surowo karane niż ucieczki w czasie pokoju, a nawet z miejsca bazowania pułku znacznie oddalonego od linii frontu. W porównaniu z dezercjami spowodowanymi tęsknotą za bliskimi czy też złym traktowaniem przez przełożonych większa odpowiedzialność karna czekała sprawców

tzw. zbiorowych ucieczek, dezerterów dopuszczających się szpiegostwa i zdrady na rzecz wroga lub obcego państwa w czasie pokoju. Poważnych konsekwencji karnych mogli spodziewać się także wszyscy dezerterzy, którzy dopuścili się przestępstw tak na szkodę wojska, jak i osób cywilnych. Kary dla zbiegłych z armii oficerów, żołnierzy szeregowych, a także kary za niestawiennictwo do służby wojskowej regulowały różnego rodzaju rozporządzenia, ustawy i kodeksy wojskowe. Do czasu wybuchu I wojny światowej w Europie był to m.in. francuski wojskowy kodeks karny z 1857 r., uproszczony przez Napoleona III w 1875 r., a także kolejne ustawy z 1893, 1899 i 1909 r., w carskiej Rosji ustawy z 1867 i 1874 r., w Austro-Węgrzech ustawy z 1889 i 1912 r., w Niemczech Niemiecki Kodeks Karny Wojskowy z 1872 r.

Liczba dezercji w wielu armiach europejskich wzrastała jeszcze przed I wojną światową. Przykładowo w 1911 r. w armii rosyjskiej za ucieczki ukarano 8027 żołnierzy, a w 1912 r. już 13358 dezerterów, w 1911 r. we Francji poszukiwano zaś 60 tys. dezerterów i ukrywających się przed służbą wojskową poborowych, co było znacznym wzrostem w stosunku do kilku wcześniejszych lat. Gigantyczną skalę dezercji ukazała dopiero I wojna światowa. Dezercje były jedną z przyczyn rozpadu armii austro-węgierskiej, w której wg węgierskich źródeł wojskowych we wrześniu osiągnęły 800 tys. żołnierzy. Wzrost dezercji notowano już w latach 1914–1915, które ukazały niechęć do służby w cesarsko-królewskiej (c.k.) armii żołnierzy narodowości słowiańskich. Jesienią 1914 r. prym w ucieczkach z pułków austro-węgierskich wiedli Czesi, Słowacy, Serbowie, Chorwaci i Słoweńcy. Pierwszej poważnej dezercji doświadczył 9 Korpus c.k. Armii, z którego tylko w listopadzie 1914 r. zbiegło 5500 żołnierzy, głównie Czechów, najchętniej uciekających na stronę Rosjan, których traktowali jak przyjaciół, wyzwolicieli spod jarzma Habsburgów. Symboliczny był tutaj 3 kwietnia 1915 r. i postawa praskiego 28 Pułku Piechoty, kiedy po kolejnym rosyjskim ataku z praskiego pułku na stronę rosyjską zdezerterowało tysiące oficerów i żołnierzy czeskich. Na stronę wroga nie przeszło jedynie 20 oficerów i 236 żołnierzy, którzy powrócili do zdekompletowanej jednostki. Największych rozmiarów dezercji w czasie I wojny światowej doświadczyła jednak armia rosyjska. Tylko w latach 1915–1916 rosyjska żandarmeria miała zatrzymać 420 tys. dezerterów, choć nie brak również

opinii, że w tym czasie zdezerterowało nawet 1,5 mln żołnierzy. Wzrost liczby dezercji w armii rosyjskiej wynikał z kilku przyczyn:

niejednolitego składu narodowościowego armii;

między żołnierzami szeregowymi a oficerami panowały feudalne relacje;

przedłużająca się → wojna [t. 4], a zwłaszcza kolejne klęski militarne działały zniechęcająco na armię, w której przewagę mieli niepiśmienni i zastraszeni chłopi;

rozkład armii przyspieszał obalenie caratu.

Dezercje w latach 1914–1918 były zjawiskiem nie tylko wstydliwym dla krajów, które przegrały wojnę, ale również dla państw zwycięskich. Po zakończeniu pierwszej wojny światowej w zwycięskiej Francji zwlekano z przedstawieniem faktycznej liczby zbiegłych żołnierzy. Dopiero w 1920 r. francuska → policja [t. 3] poinformowała społeczeństwo, że w latach 1914–1918 aresztowano 66 678 francuskich dezerterów. Współcześnie ocenia się, że liczba francuskich dezerterów w czasie Wielkiej Wojny wahała się od 80 do 90 tys. żołnierzy. Bardzo zbliżona liczba dezercji wydarzyła się w armii brytyjskiej. Wielu dezerterów z różnych armii, które walczyły na frontach I wojny światowej, szukało schronienia nie tylko w rodzinnych stronach. Celem ucieczek były neutralne w tej wojnie kraje, takie jak Hiszpania, Portugalia, Dania, Szwecja, a przede wszystkim Holandia i Szwajcaria. Tylko od połowy września 1918 r. do końca grudnia 1918 r. w samej Holandii zarejestrowano aż 4 tys. uciekinierów z armii niemieckiej. Wg jednego z raportów → wywiadu [t. 4] armii francuskiej w Genewie w styczniu 1918 r. przebywało 4800 dezerterów z francuskiej armii.

W Rosji na początku 1918 r. bolszewicy stworzyli własne siły zbrojne. 28 stycznia została utworzona Рабоче-крестьянская Красная армия (Rabocze-krest'janskaja Krasnaja armija), powszechnie znana jako Armia Czerwona. Armia bolszewików początkowo składała się z ochotników, ale 29 maja 1918 r. wprowadzono pobór. Dezercje, które były jednym z czynników rozkładu carskiej armii, dały tu o sobie znać niedługo po pierwszym poborze, kiedy z wysłanych przeciwko Korpusowi Czechosłowackiemu 50 tys. żołnierzy w rejonie koncentracji stawiło się jedynie 7 tys. żołnierzy. Większym problem militarno-politycznym dla bolszewików

było pojawienie się tzw. Zielonej Kadry (ZK), żołnierzy zbiegłych z Armii Czerwonej i organizującej własne oddziały. Rosyjskie ZK stworzyły *de facto* groźny, choć niewspółpracujący ze sobą ruch partyzancki, którego ideą była obrona chłopskiej, lokalnej rewolucji. Największe akcje rosyjskie ZK przeprowadzały w rejonie Woroneża, Saratowa, Riazania, Tuły, Niżnego Nowogrodu i Tweru. Zieloni walczyli również z oddziałami Białych, tj. oddziałami wojska opowiadającymi się za przedrewolucyjnym politycznym i ekonomicznym porządkiem, najczęściej jednak atakowały żołnierzy Armii Czerwonej. Kulminacja działań ZK przypadła na wiosnę 1919 r. W końcowej fazie istnienia Austro-Węgier, a także tuż po rozpadzie monarchii Habsburgów oddziały ZK pojawiły się również na terenach Chorwacji, Moraw, Słowacji oraz Galicji. W porównaniu z Chorwacją, a przede wszystkim Morawami Południowymi i Słowacją, działające na terenie Rosji oddziały Zielonych były nie tylko znacznie liczniejsze, ale i zdecydowanie bardziej wrogo nastawione do → komunizmu.

W międzywojniu żołnierze dezerterowali we wszystkich armiach na świecie. Szczególnie głośne były zagraniczne dezercje oficerów, którzy niejednokrotnie dostarczali wrogim krajom cennych → informacji. Dla państw takich jak Francja, która przed 1939 r. uchodziła za jedną z militarno-politycznych potęg, dezercja kpt. J. Sadoula wywoływała w latach 20. i 30. XX wieku nie mniejsze emocje niż słynna sprawa Dreyfusa. Kpt. Sadoul został wysłany wraz z francuską misją wojskową do ogarniętej rewolucją Rosji. We wrześniu 1917 r. przeszedł na stronę bolszewików, za co we Francji otrzymał zaoczną karę śmierci. Jego powrót do Francji w 1924 r. zbulwersował → opinię publiczną [t. 3]. Po procesie Sadoul został uniewinniony i z powodzeniem reprezentował sowieckie interesy we Francji. Duży wstrząs w Rumunii wywołała dezercja por. E. Bodnăraşa który w lutym 1932 r. zbiegł z 12 Pułku Artylerii w Czerniowcach. Już w 1936 r. przerzucono go do ojczyzny jako sowieckiego agenta. W 1942 r. Bodnăraş został na krótko aresztowany. Jego błyskotliwa kariera polityczna rozpoczęła się po objęciu władzy przez komunistów, był m.in. rumuńskim ministrem obrony narodowej. Znacznie bardziej szokowały w latach 30. dezercje oficerów, do których doszło w Niemczech i w Związku Sowieckim. Dla Hitlera z pewnością kłopotem było to, że do Szwajcarii w lipcu 1935 r. uciekło 15 oficerów Reichswehry, którzy pozostawali

do dyspozycji Wehrmachtu. O fakcie tym nie bez satysfakcji informowały francuskie i polskie gazety. Furię Stalina wywoływał fakt, że tylko w maju i czerwcu 1938 r. zbiegło do zajmowanej przez Japończyków Mandżurii 2 wysokich rangą o cerów. Byli to mjr Francewicz i gen. Gienrich Lusz kow. Do kilkudziesięciu tysięcy dezercji doszło także w latach 1936–1939, czyli w czasie → wojny domowej [t. 4] w Hiszpanii. Dezerterów nie brakowało tak wśród zwolenników gen. Franco, jak i Republiki.

Świadectwem pokaźnej liczby dezercji są fronty II wojny światowej. W czerwcu 1940 r. Niemcy pokonały jednego z najgroźniejszych politycznych i militarnych przeciwników, czyli Francję. Niebagatelny wpływ na pojawienie się wielu przypadków dezercji we Francji miała agitacja Francuskiej Partii Komunistycznej, która po podpisaniu paktu Ribbentrop–Mołotow wzywała francuskich żołnierzy do porzucenia szeregów armii. Największa skala dezercji nastąpiła w Armii Czerwonej, kiedy 22 czerwca 1941 r. Niemcy uderzyły na swojego niedawnego polityczno-wojskowego sojusznika – Związek Radziecki. Szacuje się, że w pierwszych tygodniach niemieckiej → inwazji na ZSRR zbiegło nawet 700 tys. czerwonoarmistów. Jedni z dezerterów poddawali się Niemcom, inni spieszyli w rodzinne strony. Wyłapywaniem i bardzo często niemal natychmiastowym rozstrzeliwaniem sowieckich dezerterów zajmowały się specjalnie powstałe tzw. oddziały zaporowe Armii Czerwonej, co w jakiś sposób powstrzymywało wzrost liczby dezercji. Na początku 1942 r. Niemcy z jeńców i dezerterów Armii Czerwonej rozpoczęli formowanie tzw. Legionów Wschodnich, w których znaleźli się Ormianie, Azerowie, Czeczeni, Gruzini, Tatarzy i Turkmeni. We wrześniu 1943 r. oddziały sformowane ze wspomnianych grup ludnościowych liczyły 500 tys. żołnierzy. Wiosną 1945 r. nastąpił natomiast gwałtowny wzrost liczby dezercji w Wehrmachcie. W kwietniu 1945 r. jedynie w oblężonym przez Armię Czerwoną Berlinie ukrywało się ok. 50 tys. dezerterów. W latach 1944–1945 niemieccy żołnierze najchętniej dezerterowali do Brytyjczyków i Amerykanów. Znacznie mniejsze dezercje charakteryzowały siły zbrojne aliantów, przykładowo w czasie II wojny światowej w armii brytyjskiej nie przekroczyły one 50 tys. przypadków.

Po 1945 r. do dezercji dochodziło we wszystkich wojskach świecie, włączywszy w to chyba najsilniejszą armię na świecie, czyli siły zbrojne

Stanów Zjednoczonych. Wg danych Pentagonu po wybuchu wojny koreańskiej z armii amerykańskiej zdezerterowało 46 tys. żołnierzy, z czego 35 tys. albo powróciło w szeregi wojska z własnej woli, albo zostało zatrzymanych na skutek działań żandarmerii. Dezercje w czasie wojny w Korei nie wywołały w amerykańskim dowództwie obaw, ponieważ w porównaniu z II wojną światową (ok. 100 tys. dezercji amerykańskich żołnierzy) były znacznie mniejsze. Więcej niepokoju wywoływała wojna w Wietnamie. W 1968 r. raportowano o podwojeniu się dezercji w siłach lądowych i lotniczych USA, nieco mniejszy wzrost tego zjawiska dotyczył jedynie → marynarki wojennej [t. 3]. W 1970 r. dowództwo armii amerykańskiej poinformowało o 65 643 dezerterach, jak podkreślono w meldunku, liczbie żołnierzy odpowiadających 4 amerykańskim dywizjom. Szacuje się, że po otrzymaniu rozkazu wyjazdu do Wietnamu ok. 7 tys. żołnierzy zbiegło ze Stanów Zjednoczonych do Kanady. W obawie przed przerzuceniem do Wietnamu żołnierze amerykańscy uciekali również z → baz wojskowych [t. 1] w Japonii i Niemczech. Z Japonii szukano azylu we wspomnianej Kanadzie, a z Niemiec w Szwecji. Do Kanady zbiegło również ok. 50 tys. młodych przedpoborowych, a także poborowych obawiających się wyjazdu do Wietnamu. Większość z nich deklarowała się jako obdżektorzy. Przyjęcie statusu obdżektora, tj. osoby, która ze względu na sprzeciw sumienia odmawia wojskowej powinności, stało się popularnym sposobem unikania służby wojskowej podczas I wojny w Zatoce Perskiej. W latach 1990–1991 liczba obdżektorów wśród żołnierzy amerykańskich gwałtownie wzrosła, warto przypomnieć, że ponad 2500 żołnierzy amerykańskich, którzy ogłosili się obdżektorami, zostało aresztowanych. Był to w historii USA największy wzrost liczby żołnierzy, którzy ogłosili, że ze względu na sprzeciw sumienia nie mogą dalej pełnić służby wojskowej. We wspomnianych latach ponad 1 tys. rezerwistów amerykańskiej armii powiadomiło władze wojskowe, że są obdżektorami. Wielu weteranów I wojny w Zatoce Perskiej, takich jak sierż. C. Mejia i K. Benderman, publicznie potępiło udział USA w tej wojnie. Trudno stwierdzić, czy takie wypowiedzi zdemotywowały wielu amerykańskich żołnierzy do udziału w II wojnie w Zatoce Perskiej. Z raportu armii amerykańskiej z maja 2005 r. wynikało, że w tym czasie liczba dezercji w wojsku amerykańskim sięgnęła blisko

6 tys. żołnierzy. W latach 1997–2004 w armii amerykańskiej odnotowano łącznie 21 187 dezercji.

Remigiusz Kasprzycki

Armeen und ihre Deserteure. Vernachlässigte Kapitel einer Militärgeschichte der Neuzeit, U. Bröckling, M. Sikora (hg.), Vandenhoeck & Ruprecht, Göttingen 1998; Ch. Glass, *Dezerterzy. Ostatnia nieopowiedziana historia II wojny światowej* tłum. T. Fiedorek, Dom Wydawniczy Rebis, Poznań 2014; R. Fantina, *Desertion and American soldier 1776–2006*, Algora Publishing, New York 2006; C. Jahr, *Gewöhnliche Soldaten: Desertion und Deserteure im deutschen und britischen Heer 1914–1918*, Vandenhoeck & Ruprecht, Göttingen 1998; R. Kasprzycki, *Ucieczki do Polski żołnierzy z krajów sąsiednich w latach 1920–1939*, „Przegląd Nauk Historycznych" 2017, r. 16, nr 1; L. Milewski, *Dezercja cudzoziemca*, „Wojskowy Przegląd Prawniczy" 1936, r. IX, nr 2; A. Smoliński, *Dezercje z Robotniczo-Chłopskiej Armii Czerwonej w latach 1918– 1922. Wojna z Polską i wojna domowa w Rosji*, „Przegląd Wschodni" 2007, t. 10, z. 3 (39).

Dezercje w Wojsku Polskim w XX wieku – pierwsze → dezercje [t. 1] w Wojsku Polskim (WP) miały miejsce już w końcu 1918 r., ale dopiero w latach 1918–1921 ucieczki z wojska stały się dość poważnym problemem. Szacuje się, że w czasie wojny polsko-bolszewickiej (1919–1920) z polskiej armii zbiegło lub nie stawiło się w jej szeregi od 100 do 150 tys. dezerterów i poborowych. Dezerterzy porzucali szeregi frontu po zaciętych → bitwach [t. 1], opuszczali także bataliony zapasowe, które stacjonowały w głębi kraju. Przyczyny dezercji były bardzo różne, podobne do występujących w innych walczących armiach na całym świecie; powodowane strachem przed cierpieniem po odniesionych ranach, kalectwem i bezsensowną śmiercią. Były również sposobem zakończenia → przemocy [t. 3], której → żołnierze [t. 4] doświadczyli od przełożonych, niekiedy daleko od linii frontu. To ostatnie spotykało zwłaszcza rekrutów albo ideowo i patriotycznie nastawionych ochotników. Niestety, różne formy psychicznego oraz fizycznego znęcania się nad najmłodszymi stopniem i z najkrótszym stażem służby żołnierzami były smutnym dziedzictwem armii zaborczych, w największym stopniu pozostałością po armii carskiej. Takie problemy starali się wykorzystać komuniści, którzy z początku liczyli, że wywołają rewolucję w polskiej armii

i podporządkują sobie większość oddziałów. Okazało się to niewykonalne, więc wzywano do dezercji. W praktykach tych przodowała → propaganda [t. 3] bolszewicka. Oczekiwania bolszewików, że dezerterzy z WP masowo zasilą Armię Czerwoną, nie sprawdziły się, a nadzieja, że zbiegli polscy żołnierze stworzą silny „czerwony" pułk złożony z ochotników, również okazała się płonna. Ostatnią rzeczą, jakiej pragnęli ukrywający się przed poborem albo dezerterzy z WP, był udział w → wojnie [t. 4] po którejkolwiek ze stron. Najlepszym dowodem tego były tysiące poborowych i dezerterów, którzy w latach 1918–1921 w większości uciekali do Niemiec, a nie do Rosji bolszewickiej. Niestawiennictwo poborowych i dezercje charakteryzowały w tych latach zwłaszcza ludność pochodzącą z polskich wsi wchodzących w skład byłego zaboru rosyjskiego, a także narodowość żydowską. W czasie wojny polsko-bolszewickiej władze wojskowe starały się walczyć ze zjawiskiem dezercji w różny sposób. W miastach i na wyznaczonych obszarach stosowano niespodziewane obławy, a w garnizonach edukowano żołnierzy o negatywnych skutkach dezercji. Latem 1920 r. podjęto szeroką akcję propagandową skierowaną do → ludności cywilnej [t. 3], która miała zniechęcić do jakiejkolwiek pomocy dla dezerterów. Zaostrzający się kurs wobec dezerterów był widoczny w rozkazie Ministerstwa Spraw Wojskowych z 25 lipca 1920 r. Gen. br. K. Sosnkowski, wiceminister spraw wojskowych, od 9 sierpnia 1920 r. minister spraw wojskowych, wskazywał, że sądy doraźne rozpatrujące sprawy dezerterów miały funkcjonować energicznie i odpowiedzialnie. Orzeczenia miały być pozbawione zbędnej biurokracji, a wyroki wydawane niemal ekspresowo. Zalecał, aby prawo łaski było stosowane jedynie w wyjątkowych przypadkach. Surowe słowa gen. Sosnkowskiego nie oznaczały jeszcze, że wszyscy schwytani dezerterzy byli natychmiast rozstrzeliwani. O wiele ważniejsza była świadomość nieuchronności kary. W trakcie wojny polsko-bolszewickiej funkcjonowały wojskowe sądy doraźne, które decydowały o losach dezerterów. W czasie tej wojny liczba postawionych przed sądami polowymi dezerterów, którzy często popełniali różne kryminalne przestępstwa, sięgnęła w 1920 r. 11 tys., z czego 3 tys. skazano na karę śmierci; w zdecydowanej większości przypadków wykonanie kary śmierci zostało wstrzymane. W 1920 r. wojenne sądy doraźne orzekły 333 wyroki śmierci, spośród których dezerterami było

125 skazanych. W 1921 r. na mocy wyroków tych sądów wykonano jedynie 22 wyroki śmierci.

W latach 1921–1939 dezercje dalej stanowiły wciąż poważny problem WP. Wynikało to z kilku powodów:

Służba w polskiej armii była powszechna i obowiązkowa.

Warunki socjalno-bytowe codziennej służby (zwłaszcza w latach 20.) w wielu pułkach wymagały znacznej poprawy.

Działalność destrukcyjną przeciwko armii polskiej nieprzerwanie prowadzili nie tylko komuniści polscy (w latach 1918–1925 pod nazwą Komunistycznej Partii Robotniczej Polski, od 1925–1938 jako Komunistyczna Partia Polski), ale także komuniści białoruscy (Komunistyczna Partia Zachodniej Białorusi) i ukraińscy (Komunistyczna Partia Zachodniej Ukrainy).

WP miało charakter wielonarodowościowy, poza żołnierzami polskiej narodowości, którzy zawsze stanowili w armii polskiej zdecydowaną większość (w latach 1922–1939 zazwyczaj ponad 75% wcielonych rekrutów do armii polskiej było Polakami), w międzywojennych siłach zbrojnych II RP służyli również Żydzi, Białorusini, Ukraińcy, Litwini, Rosjanie, Niemcy i Czesi, a także przedstawiciele innych narodowości. Bardzo rozbieżne dane (choćby → policji [t. 3] i żandarmerii wojskowej) wskazują, że od 1921 do 1939 r. z WP zdezerterowało lub (w większości) dokonało krótkotrwałego samowolnego oddalenia się od 30 do 60 tys. żołnierzy.

Poza żołnierzami polskiej narodowości największą liczbę dezercji popełnili w latach 1923–1928 Ukraińcy (5–8 tys. dezercji) i Białorusini (4–6 tys. dezercji) oraz Żydzi (2–3 tys. dezercji). Dezerterzy, a także poborowi ukrywali się na terenie kraju, lecz również decydowali się na ucieczki za granicę. Nadal najbardziej popularnym kierunkiem ucieczek były Niemcy. Najzamożniejszy sąsiad II RP przyciągał nie tylko perspektywą poprawy materialnego bytu, ale i wizją przedostania się do innych krajów Europy Zachodniej, a także wyjazdu do USA. W 1923 r. tylko z województwa stanisławowskiego do odległych Niemiec zbiegło aż 150 poborowych, do Czechosłowacji 103, do ZSRR 98, a do Rumunii 50. Podobna tendencja „emigracyjna" utrzymała się w latach 30. W 1936 r. 81 dezerterów dotarło do Niemiec, 69 do ZSRR, 23 do Czechosłowacji,

23 na Litwę, 1 do Rumunii, a 1, jak ustalono, tra ł aż do Hiszpanii. W prze ważającej liczbie dezerterzy z WP, którzy znaleźli się za granicami kraju, doświadczyli poważnego rozczarowania. Po zatrzymaniu i dokładnych przesłuchaniach przez przedstawicieli obcych → w y w i a d ó w [t. 4] nie okazywali się „cennym źródłem" → i n f o r m a c j i. Ze względu na ni ski poziom wykształcenia, nierzadki analfabetyzm i półanalfabetyzm (przewaga żołnierzy służby zasadniczej z obszarów wiejskich) dezerterów z armii polskiej przeważnie nie przygotowywano do zadań szpiegowskich. W Niemczech i ZSRR uciekinierzy z WP stanowili zazwyczaj tanią siłę roboczą, jednak często rozczarowani powracali do Polski, gdzie osądzeni tra ali do więzień. Bardziej niebezpieczne były dezercje o cerów w mię dzywojennej Polsce, które były jednak nieliczne. Do najbardziej znanych należała ucieczka mjr. dypl. S. Kraussa, szefa wyszkolenia w Dowództwie Okręgu Korpusu Nr VI we Lwowie, który w połowie października 1930 r. nie powrócił z miesięcznego urlopu. Po przeprowadzonym śledztwie okazało się, że mjr Krauss nie tylko przywłaszczył od różnych o cerów i instytucji wojskowych 35 tys. złotych, ale i w swoim domu przechowywał kopię akt związanych z obronnością kraju. W latach 1932–1933 strona polska bezskutecznie starała się o ekstradycję Kraussa z Belgii i Francji. Francuzi informowali wręcz, że nic nie wiedzą o losie poszukiwanego. Nie przeszkodziło to jednak tamtejszemu wywiadowi zatrzymać wiosną 1934 r. Kraussa, który był niemieckim agentem działającym jako George Teworyt vel Sybert.

W latach 1921–1939 poważnym problemem były nie tylko dezercje, ale również niechęć do służby w WP. Największe zainteresowanie uniknięciem służby wojskowej wykazywali Żydzi, oceniani przez Samodzielne Referaty Informacji (SRI) WP jako najmniej „wartościowy materiał żołnierski" spośród wszystkich służących w polskiej armii mniejszości narodowych żołnierzy. Przykładowo wśród żołnierzy żydowskich notowano w trakcie służby największą liczbę symulowania różnego rodzaju chorób, a także wywrotowej komunistycznej agitacji. Dla porównania SRI wysoko ceniła kwali kacje żołnierskie Niemców, choć poważnie obawiała się lojalno ści tej narodowości. Nieufność polskiego → k o n t r w y w i a d u budzili także Litwini, a zwłaszcza Ukraińcy pozostający pod wpływem Organi zacji Ukraińskich Nacjonalistów (OUN), która przekonywała młodzież

ukraińską, że nie powinna dezerterować z WP, a czas służby w polskiej armii wykorzystać do zdobycia przydatnych umiejętności wojskowych. Władze WP znacznie mniej obawiały się postaw Białorusinów i Rosjan, wysoko natomiast ceniły lojalność nielicznie służących w polskiej armii Czechów.

W 1939 r. obawy władz wojskowych o postawę żołnierzy reprezentujących mniejszości narodowe częściowo okazały się uzasadnione. Sygnałem ostrzegawczym były masowe ucieczki niemieckich poborowych, które rozpoczęły się wiosną 1939 r. Prawdopodobnie do wybuchu wojny, tj. do września 1939 r., z II RP do III Rzeszy zbiegło ok. 10 tys. poborowych narodowości niemieckiej, w tym z samej Wielkopolski blisko 2500 niemieckiej młodzieży. Dezercje w szeregach WP miały miejsce od początku wybuchu II wojny światowej, ale dopiero 10 września 1939 r. niepokojące informacje zaczęły napływać z Małopolski Wschodniej, w której pojawiały się zbrojne grupy ukraińskich dezerterów z WP. Działania te inspirowała OUN. Wzrost dezercji w WP, w tym żołnierzy polskich, nastąpił dopiero w drugiej połowie września 1939 r., kiedy stało się jasne, że państwo i armia II RP zmierza ku klęsce. Zwrotnym momentem był 17 września 1939 r., zaatakowanie Polski przez ZSRR. W niektórych miejscach dezercje przybrały masowy charakter. Np. w nocy z 19 na 20 września 1939 r. z 3 Dywizjonu Taborów w Lidzie zdezerterowali wszyscy służący w nim Białorusini i Żydzi. Kategorycznie należy jednak zaprzeczyć, że wszyscy żołnierze białoruscy, niemieccy, ukraińscy i żydowscy, którzy służyli we wrześniu 1939 r., wykazali się nielojalnością wobec II RP. Znaczne męstwo charakteryzowało wielu Białorusinów, którzy dzielnie walczyli w oddziałach wchodzących w skład 20 Dywizji Piechoty (DP), która w dniach 1–4 września 1939 r. stoczyła ciężką bitwę pod Mławą. 10% obrońców Helu, który skapitulował dopiero 2 października 1939 r. stanowili Białorusini. We wrześniu 1939 r., walecznością wyróżnili się ukraińscy ułani służący w 2 i 7 Pułku Strzelców Konnych. Wielu z nich otrzymało za odwagę i poświęcenie na polu walki wysokie odznaczenia.

W sierpniu 1941 r. na mocy porozumień emigracyjnego rządu londyńskiego i rządu sowieckiego w ZSRR rozpoczęto formowanie Polskich Sił Zbrojnych (PSZ), potocznie nazywanych Armią Andersa. Od marca do listopada 1942 r. ze Związku Sowieckiego ewakuowano do Iranu ponad

78 tys. żołnierzy i 35 tys. cywilów. Ewakuacji odmówiła jednak pewna grupa oficerów współpracująca z sowieckimi władzami – byli to ppłk Z. Berling, ppłk L. Bukojemski i por. T. Wicherkiewicz – współtwórcy podporządkowanej Stalinowi i utworzonej przez komunistów w 1943 r. w ZSRR komunistycznej armii polskiej, którą w latach 60. i 70. w Polsce Ludowej nazywano Ludowym Wojskiem Polskim (LWP). W 1943 r. sąd wojenny przy 2 Korpusie WP uznał postępowanie Berlinga i wspomnianych oficerów za zdradę i dezercję. Innym problemem były dezercje żołnierzy narodowości żydowskiej, którzy ewakuowali się wraz z Armią Andersa. Do pierwszych ucieczek żołnierzy narodowości żydowskiej służących w PSZ doszło jeszcze w czasie pobytu w Iranie. W sierpniu i wrześniu 1942 r. zdezerterowało 193 żydowskich żołnierzy. Kolejne dezercje miały miejsce już w Palestynie, gdzie żydowscy dezerterzy z PSZ zasilali miejscowe podziemie zbrojne, walczące o niepodległość Izraela.

Najliczniejsze dezercje w wojsku polskim w ostatnich latach II wojny światowej wydarzyły się w LWP. Tuż przed końcem wojny, to jest w 1944 r., z 2 Armii LWP zdezerterował prawie cały 31 Pułk Piechoty (PP) – dokładnie 636 żołnierzy i 2 oficerów, którzy przyłączyli się do antykomunistycznej partyzantki. W marcu 1945 r. ze szkoły oficerskiej w Chełmie jednej nocy zbiegło ok. 300 podchorążych. Niemal wszystkie bataliony i kompanie drezdeńskiej 9 DP latem 1945 r. porzuciły koszary. Władze komunistyczne najpierw zreorganizowały, a następnie rozwiązały 3 Brygadę Korpusu Bezpieczeństwa Wewnętrznego. Powodem tej decyzji nie były straty poniesione w walce – całe bataliony tej jednostki znikały z bronią. Dezerterzy z LWP zasilali oddziały zbrojnego podziemia. Często w ten sposób tworzyły się także zalążki nowych oddziałów leśnych i siatek konspiracyjnych. W maju 1945 r. dotarła do 5 Wileńskiej Brygady AK 70-osobowa grupa dezerterów z 6 Zapasowego PP 2 Armii LWP z Torunia i poprosiła o wcielenie w szeregi formacji. Trzy dni później przybyło kolejnych 25 żołnierzy z Samodzielnego Batalionu Ochrony Lasów Państwowych z Hajnówki. W 1945 z LWP zdezerterowało 14 tys. żołnierzy, a w 1948 jeszcze więcej, bo 24 tys. Jednak tylko część z nich kierowała się do leśnych oddziałów „żołnierzy wyklętych" i tam docierała. W kolejnych latach przechodzenie żołnierzy LWP na stronę zbrojnego podziemia niepodległościowego wyraźnie zmalało. Miało to

ścisły związek z zewnętrzną i wewnętrzną sytuacją polityczno-militarną w Polsce i na świecie.

W latach 1944–1989 jednym z najważniejszych powodów dezercji z LWP był wzrost przemocy psychicznej i zycznej, którego doświadczali młodzi rekruci od starszych stażem kolegów. Różne formy znęcania się stosowali również podo cerowie, a nawet o cerowie, za co często nie ponosili żadnej odpowiedzialności karnej. W latach 1952–1955 doszło do 2954 pojedynczych i 278 zbiorowych przypadków dezercji z LWP. Wśród dezerterów Polski Ludowej dominowali młodzi żołnierze, którzy nie wytrzymywali trudów i prymitywnych rytuałów służby wojskowej – prze niesionych głównie z wzorów Armii Czerwonej, a wcześniej carskiej Rosji. W PRL kwestie samowolnych oddaleń z wojska i dezercji regulowały kolejne kodeksy karne, m.in. z 1944, 1957 i 1969 r., a także dekret o stanie wojennym z 13 grudnia 1981 r., który wprowadzał postępowanie doraźne przed sądami wojskowymi za przestępstwa powszechne i wojskowe. Za samowolne oddalenie się i dezercję dekret przewidywał 3 kary główne: karę śmierci, karę 25 lat pozbawienia wolności lub karę pozbawienia wolności na czas nie krótszy od 3 lat. 23 maja 1984 r. sąd wojskowy PRL skazał zaocznie płk. R. Kuklińskiego, który do czasu ucieczki w listopadzie 1981 r. pełnił obowiązki w Sztabie Generalnym WP. Kara została wymierzona za dezercję i zdradę państwa.

Po 1989 r. dezercje nie skończyły się, ale dzięki zniesieniu → c e n z u r y [t. 1] i wprowadzeniu jawności życia społecznego Polacy dowiadywali się znacznie więcej o problemach wojska. Wiele informacji mogło być jednak szokujących, np. jak ta związana z szer. pchor. J. Ochnikiem z Wyższej Szkoły O cerskiej Wojsk Łączności (WSOWŁ) w Zegrzu. W maju 1990 r. Ochnik zastrzelił dowódcę warty i 3 swoich kolegów, którzy znęcali się nad nim psychicznie. Dezerter z WSOWŁ kilkanaście dni ukrywał się w okolicznych lasach. W 1999 r. Naczelna Izba Kontroli (NIK) skontrolowała warunki pełnionej zasadniczej służby wojskowej. Z raportu NIK wynikało, że w kontrolowanych jednostkach wojskowych wymierzono łącznie 2715 kar dyscyplinarnych, z czego aż 1724 związanych było z nieobecnością żołnierzy na służbie lub z samowolnym oddaleniem się.

Remigiusz Kasprzycki

J. Grzybowski, *Białorusini w polskich regularnych formacjach wojskowych w latach 1918–1945*, Wydawnictwo ISP PAN, Warszawa 2006; D. Jarosz, G. Mierzejewski, *Pobór, wcielenie, „pruska dyscyplina", dezercje. Wstęp do badań nad historią społeczną służby wojskowej w stalinowskiej Polsce (1950–1955)*, „Polska 1944/45–1989. Studia i Materiały" 2018, nr 16; R. Kasprzycki, *Dezercje i unikanie służby w Wojsku Polskim w latach 1918–1939*, „Dzieje Najnowsze" 2016, r. 48, nr 3; tenże, *Miraże Czerwonego Raju. Losy dezerterów z Wojska Polskiego w Związku Radzieckim*, „Niepodległość i Pamięć" 2017, nr 1 (57); tenże, *Niespełnione marzenia naiwnych. Losy dezerterów z Wojska Polskiego w Niemczech w latach 1921–1939*, „Niepodległość i Pamięć" 2019, nr 1 (65); P. Stawecki, *Z badań nad dyscypliną i moralnością wojska Drugiej Rzeczypospolitej*, Wydawnictwo PAW, Warszawa 2000; T. Szczygieł, *Wojskowe postępowanie karne w II Rzeczypospolitej (1918–1939)*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2017.

Dezinformacja – metoda oddziaływania psychologicznego, która wprowadza w błąd osobę/grupę osób co do rzeczywistego stanu rzeczy, świadomie przekazuje nieprawdziwe → informacje w celu skuteczniejszego prowadzenia działań wojennych, sprawdzania wycieków informacji i kierunku ich wycieku, a także procesu manipulowania informacjami, wprowadzania w błąd przez podanie niepełnych lub kompletnych, ale już nie niezbędnych informacji, tworząc zniekształcony obraz rzeczywistości. Rozpowszechnianie zniekształconych, niepełnych lub świadomie fałszywych informacji do celów propagandowych, wojskowych (wprowadzających w błąd), handlowych lub innych.

Dezinformacja jest utożsamiana z procesem mylnego informowania, sytuacją, w której brakuje informacji rzetelnych, także z przekazem treści zamierzonych. Niektórzy uważają, że dezinformacja znajduje się między wprowadzaniem w błąd a wpływaniem. Strategiczna dezinformacja jest instrumentem rosyjskiej polityki zarówno w czasie → wojny [t. 4], jak i pokoju. Wyspecjalizowanymi organami realizującymi zadania z zakresu dezinformacji są organy → wojny psychologicznej [t. 4], taką rolę odgrywają również cywilne i wojskowe → służby specjalne [t. 4]. Dezinformacja obejmuje czynności podejmowane z zaangażowaniem poważnych środków, jest prowadzona w sposób systematyczny i fachowy, zawsze za pośrednictwem mass mediów i jest adresowana do → opinii publicznej [t. 3].

Wyróżnia się następujące poziomy manipulacji:

wzmocnienie istniejących w umysłach ludzi wartości, które są korzystne dla manipulatora (idee, postawy itp.);

częściowa zmiana poglądów na temat konkretnego wydarzenia lub okoliczności;

podejmowanie przez odbiorcę błędnych decyzji;

kardynalna zmiana postaw.

Rodzaje dezinformacji:

wprowadzanie w błąd konkretnej osoby lub grupy osób, czyli podawanie fałszywych informacji;

manipulowanie działaniami (jednej osoby lub grupy osób);

tworzenie opinii publicznej na temat problemu lub przedmiotu;

„półprawda" lub „fałszywe zaniedbanie". W szczególności totalitarne → reżimy [t. 3] polityczne pragną otrzymywać od władz niższego szczebla jedynie pozytywne informacje, ukrywając niepowodzenia i błędy. „Fałsz milczenia" przenika także do mediów, tworząc iluzję „udanego postępu", podczas gdy w rzeczywistości dochodzi do regresji. Ostatnio aktywnie wykorzystywana jest technologia dezinformacji znana jako „biały szum informacyjny". Oznacza to, że jeśli nie jest możliwe ukrycie „niewygodnej" informacji, jest ona zróżnicowana, tj. tworzy się pewien zestaw wersji, które są w równym stopniu potwierdzone, mocując je w masowej świadomości.

Rozwój internetu, → mediów społecznościowych [t. 3] oraz nowoczesnych technologii sprawił, że znacznie wrosło → zagrożenie [t. 4] dezinformacją. Obecnie fałszywe informacje rozprzestrzeniają się na nieosiągalną wcześniej skalę, a ich zasięg stał się na tyle duży, że może wpłynąć na funkcjonowanie całego kraju. Tym samym dezinformacja stała się dla państwa wyzwaniem. O dezinformacji możemy mówić, gdy rozpowszechniane informacje:

są całkowicie lub częściowo fałszywe, zmanipulowane lub wprowadzające w błąd;

dotyczą kwestii ważnych z punktu widzenia interesu publicznego;

mają wywołać niepewność lub wrogość, doprowadzić do polaryzacji albo zakłócenia procesów demokratycznych;

są rozpowszechniane lub wzmacniane za pomocą zautomatyzowanych i agresywnych technik, takich jak boty społeczne, → sztuczna inteligencja [t. 4] (AI), mikrotargeting lub trollowanie.

Istnieją różne metody dezinformacji, z których każda ma swoje pozytywne i negatywne cechy. Konkretny wybór tej czy innej metody zależy bezpośrednio od sytuacji operacyjnej, która jest opracowana w określonym obszarze służby wywiadowczej, zadań, które są przed nią ustalane, itd. Metody dezinformacji:

tendencyjne opowiadanie faktów: to rodzaj dezinformacji, która obejmuje stronnicze przedstawianie pewnych faktów lub innych informacji o zdarzeniach przy użyciu specjalnie wybranych prawdziwych danych w określonych odstępach czasu – z reguły w tej metodzie informacja jest dozowana do stale rosnącego napięcia, a taki stan społeczeństwa/grupy jest utrzymywany przez ciągłe „podrzucanie" nowych części ściśle ograniczonych i mierzonych danych w środowisku de cytu informacji;

odwrotna dezinformacja: dzieje się to poprzez przekazywanie prawdziwych informacji w perwersyjny sposób lub w sytuacji, gdy cel postrzega je jako fałszywe – zastosowanie takich środków stwarza sytuację, w której odbiorca faktycznie zna prawdziwą informację o zamiarach lub konkretnych działaniach strony przeciwnej, ale postrzega ją w taki sposób, że nie jest gotowy do wytrzymania negatywnego wpływu;

terminologiczne „minowanie": jest wypaczeniem pierwotnej poprawnej istoty fundamentalnie ważnych, podstawowych terminów i interpretacji o ogólnym charakterze ideologicznym i operacyjnie stosowanym;

pochlebstwo: wykorzystanie przyjemnych interpelacji, czasami nieumiejętnie, w celu przekonania odbiorcy (np. „Jesteś bardzo inteligentny, powinieneś zgodzić się z tym, co mówię");

apel do autorytetu: cytuje się ważne postacie, aby poprzeć pomysł, argument lub linię postępowania, a nie inne opinie;

apel do strachu: przerażona publiczność znajduje się w sytuacji biernej otwartości i łatwiej ulega jakiejkolwiek indoktrynacji lub idei, którą chce się jej wpoić;

kozioł o arny: demonizując osobę lub grupę osób i oskarżając o bycie odpowiedzialnym za rzeczywisty lub rzekomy problem, propagandysta może uniknąć mówienia o prawdziwych sprawcach i pogłębić sam problem;
żądanie dezaprobaty lub wkładanie słów w usta: ma sugerować, że pomysł lub działanie jest przyjmowane przez grupę przeciwną, skłania to innych do zmiany zdania;
efekt skumulowany: próba przekonania publiczności do przyjęcia pomysłu sugerującego, że ruch masowy jest już zaangażowany w podtrzymywanie danej idei, chociaż jest to nieprawda – niestety, większość woli być zawsze po stronie zwycięzców, owa taktyka pozwala przygotować społeczeństwo do → propagandy [t. 3];
łatwiej jest gromadzić ludzi w grupach, aby wyeliminować indywidualne sprzeciwy i stosować większy przymus, przekonanie lub zasady marketingowe stosowane przez sprzedawców;
używanie haseł: krótkie frazy, łatwe do zapamiętania i rozpoznania, zdolne do pozostawienia śladu u wszystkich odbiorców, pozytywnie lub ironicznie (np. „Jan P. jest uczciwym człowiekiem");
stereotypowanie lub etykietowanie: ta technika wykorzystuje uprzedzenia i stereotypy odbiorców, aby coś odrzucić;
eufemizm lub semantyczny poślizg: zamiana jednego wyrażenia na inne, aby zmienić treść emocjonalną i znaczenie (np. „czystki etniczne" w przypadku umotywowanych rasizmem mordów, „solidarność" zamiast podatku);
celowa niedokładność: dotyczy powoływania się na statystyki lub odwoływania się do faktów je deformujących bez wskazywania źródeł lub wszystkich danych – zamiarem jest nadanie treści wypowiedzi pozorów charakteru naukowego i unieważnienie analizy jego przydatności bądź prawdziwości;
przyciemnienie: aby nie zgłaszać czegoś nieprzyjemnego dla władzy, treść zostaje przeformułowana (np. zamiast powiedzieć, że bezrobocie wzrosło do 4 mln, można powiedzieć, że stopa bezrobocia wzrosła w mniejszym stopniu niż w tym samym miesiącu ubiegłego roku);
poziom językowy oraz wygląd „zwykłego człowieka" dla zdobycia zaufania publiczności: z powodu psychologicznego mechanizmu

projekcji odbiorcy są bardziej skłonni zaakceptować przedstawione im pomysły, ponieważ ktoś, kto je przedstawia, jest podobny do samej publiczności;

rede nicja i rewizjonizm: polega na rede niowaniu słów lub fałszowaniu historii w sposób stronniczy, aby stworzyć iluzję spójności;

przesadne uproszczenie: ogólniki używane do kontekstualizacji złożonych problemów społecznych, politycznych, ekonomicznych lub wojskowych;

świadectwo: podawanie konkretnych przypadków zamiast ogólnych sytuacji, aby podtrzymać daną politykę (np. szanowana osobowość wchodzi do partii politycznej oskarżonej o → korupcję, aby wykorzystać swoją reputację i przeciwdziałać złemu wizerunkowi partii);

transfer: technika służąca projekcji pozytywnych lub negatywnych cech osoby, bytu, przedmiotu lub wartości (jednostki, grupy, organizacji, narodu, rasy, patriotyzmu) na coś, co uczyni to bardziej (lub mniej) akceptowalnym;

używanie ogólnych i prestiżowych słów, które mogą powodować intensywne emocje na widowni: miłość do kraju i pragnienie pokoju, wolności, chwały, sprawiedliwości, honoru i czystości itp. pozwalają zabić krytycznego ducha publiczności, ponieważ znaczenie tych słów różni się w zależności od interpretacji każdej osoby, ale ich ogólnie znaczenie jest pozytywne, w związku z czym wykorzystujące takie słowa koncepcje i programy propagandystów same będą postrzegane jako wielkie, dobre, pożądane i cnotliwe.

Dezinformacja jest integralną częścią → wojny informacyjnej [t. 4], która obejmuje:

→ operacje psychologiczne [t. 3] (wykorzystanie informacji do psychologicznego oddziaływania na → żołnierzy [t. 4] wroga);

wojnę elektroniczną (nie pozwala wrogowi na uzyskanie dokładnych informacji);

środki bezpieczeństwa (chęć uniknięcia wiedzy wroga o możliwościach i zamiarach strony przeciwnej);

bezpośrednie ataki informacyjne (zniekształcenie informacji bez widocznej zmiany jej istoty).

Aby skuteczniej manipulować opinią publiczną, dezinformacja może rozprzestrzeniać się jednocześnie za pośrednictwem mediów drukowanych i elektronicznych, telewizji, internetu, plotek, a także poprzez wykorzystanie ulotek w lokalnych konfliktach i wojnach.

W szerokim sensie wojna informacyjna jest jedną z metod konfrontacji między dwoma państwami, która ma miejsce głównie w czasie pokoju, gdzie przedmiotem wpływów wraz z siłami zbrojnymi i → ludnością cywilną [t. 3] jest społeczeństwo jako całość, jego państwowe systemy administracyjne, struktury zarządzania produkcją, nauka, kultura itp. W wąskim znaczeniu jest to jedna z metod operacji bojowych lub bezpośredniego przygotowania się do nich w celu uzyskania przewagi nad wrogiem w procesie przyjmowania, przetwarzania i wykorzystania informacji.

Do prowadzenia operacji informacyjnych i psychologicznych z wykorzystaniem dezinformacji aktywnie angażuje się telewizja, która we współczesnym świecie jest najważniejszym narzędziem masowego wpływu na społeczeństwo. Istnieje kilka metod manipulowania świadomością indywidualną i masową wykorzystywanych przez media:

→ przeciążenie informacyjne [t. 3] – odbiorca otrzymuje nadmierną ilość niepotrzebnych informacji (abstrakcyjne rozumowanie, niepotrzebne szczegóły itp.), co uniemożliwia mu zrozumienie prawdziwej istoty problemu;

dozowanie informacji – tylko część informacji jest przekazywana do odbiorcy, a reszta jest starannie ukryta, co prowadzi do zniekształcenia rzeczywistego obrazu w określonym kierunku;

wielkie kłamstwo – społeczeństwu podaje się możliwie poważnie najbardziej nieprawdopodobne kłamstwo, które wydaje się szczególnie przekonujące;

mieszanie faktów – fakty są mieszane ze wszelkiego rodzaju założeniami, hipotezami i plotkami; społeczeństwu niezwykle trudno jest odróżnić prawdę od fikcji;

opóźnienie czasu informacji – pod różnymi pretekstami opóźnia się podanie naprawdę ważnych informacji, aż do momentu, gdy będzie za późno, aby odbiorca coś zmienił;

ukryte uderzenie – kcyjna informacja jest przekazywana przez manipulatora do odbiorcy przez neutralnych, ale podstawionych ludzi;

rzeczywiste kłamstwo – społeczeństwu podaje się całkowicie fałszywą, ale niezwykle oczekiwaną w danej chwili informację (z czasem oszustwo zostaje ujawnione, ale dotkliwość sytuacji nie ustępuje lub pewien proces nabiera nieodwracalnego charakteru).

Celem działań dezinformacyjnych jest destabilizacja innych państw. Liberalne demokracje nie mają symetrycznej odpowiedzi na takie działania, które mogą być prowadzone jedynie przez agresywne, autorytarne państwa.

Podczas Warsaw Security Forum 8 listopada 2017 r. odbył się panel pt. „Polityka w erze post-prawdy: Zwalczanie dezinformacji i fake newsów w Europie Centralnej i Wschodniej", gdzie zaprezentowano raport *Rosyjska wojna dezinformacyjna przeciwko Polsce*Został wydany przez Fundację im. Kazimierza Pułaskiego we współpracy merytorycznej z → Centrum Analiz Propagandy i Dezinformacji [t. 1] oraz Studium Europy Wschodniej Uniwersytetu Warszawskiego.

W styczniu 2018 r. Komisja Europejska powołała grupę ekspertów wysokiego szczebla ds. nieprawdziwych informacji i dezinformacji w internecie (High-Level Expert Group on Fake News and Disinformation spread online, HLEG). Jej zadaniem jest doradzanie przy inicjatywach związanych z przeciwdziałaniem → fake newsom i dezinformacji w sieci. Efektem jej prac były sprawozdanie i raport, opublikowane 12 marca 2018 r., w których grupa analizuje problemy związane z dezinformacją w sieci, a w mniejszym stopniu fałszywych informacji, podkreślając, że dezinformacja może zagrażać demokratycznym procesom i wartościom. Grupa zaleciła m.in.: rozwój umiejętności korzystania z mediów w celu → przeciwdziałania dezinformacji [t. 3], opracowanie narzędzi, które pomogą użytkownikom i dziennikarzom zwalczać dezinformację, zachowanie różnorodności i stabilności europejskich mediów informacyjnych oraz dalsze badania wpływu dezinformacji na społeczeństwo w Europie.

Dezinformacja może destabilizować sytuację w państwie, wywierać destrukcyjny wpływ na jego struktury administracyjne i decyzyjne, a także

podważać podstawy społeczne, ekonomiczne oraz kulturowe. Wg raportu *Freedom on the Net 2017: Manipulating Social Media to Undermine Đe mocracy* coraz więcej krajów na świecie wykorzystuje media społecznościowe do działań dezinformacyjnych – zarówno do kształtowania swojej wewnętrznej polityki, jak i do wpływania na inne państwa. Przeciwdziała nie dezinformacji staje się wyzwaniem nie tylko dla pojedynczych państw, ale też instytucji i organizacji międzynarodowych.

Jak zaznaczają autorzy publikacji z września 2019 r. *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, konieczność przeciwdziałania kampaniom dezinformacyjnym w Europie podkreśliła po raz pierwszy Rada Europejska w marcu 2015 r. Od tego czasu w strukturach Europejskiej Służby Działań Zewnętrznych (European External Action Service) powstało kilka zespołów zajmujących się analizowaniem dezinformacji w Unii Europejskiej oraz krajach sąsiadujących ze wspólnotą. Wg Komórki UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych to dezinformacja ze strony Federacji Rosyjskiej miała stanowić największe zagrożenie przed przeprowadzonymi w maju 2019 r. wyborami do Parlamentu Europejskiego. Niepokojące doniesienia o skali i wpływie kampanii dezinformacyjnych sprawiły, że 2018 r. był w UE czasem wyjątkowo wytężonej pracy w tym zakresie. Opublikowano łącznie 4 istotne dokumenty, które podejmowały zagadnienie dezinformacji.

Olga Wasiuta

J. Darczewska, *Między jawną dezinformacją a niejawną praktyką gry rosyjskich służb*, Ośrodek Studiów Wschodnich im. Marka Karpia, Warszawa 2019; A. Janiuszko-Szakiel, *Dezinformacja jako narzędzie medialnej manipulacji świadomością* [w:] *Manipulacja pedagogiczno-społeczne aspekty. Część I. Interdyscyplinarne aspekty manipulacji*, J. Aksman (red.), Oficyna Wydawnicza AFM, Kraków 2010; T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2 (24); NASK Cyber Policy, *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, NASK Państwowy Instytut Badawczy, Warszawa 2019; P. Pogorzelski, *Zagrożenie rosyjską dezinformacją w Polsce i formy przeciwdziałania*, Kolegium Europy Wschodniej im. Jana Nowaka-Jeziorańskiego we Wrocławiu, Wrocław 2017; M. Świerczek, *„System matrioszek", czyli dezinformacja doskonała. Wstęp do zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19; V. Volko ,

Dezinformacja – oręż wojny, Delikon, Warszawa 1991; M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnych*, AON, Warszawa 2005.

Dezinformacja wojskowa – proces prowadzący do powstania → informacji fałszywej bądź też kłamliwej, mający na celu wprowadzenie odbiorcy w błąd i wytworzenie u przeciwnika fałszywego obrazu rzeczywistości. Rozwój → środowiska informacyjnego [t. 4] doprowadził do znaczącego poszerzenia pojęcia znaczenia od tradycyjnie rozumianej → propagandy [t. 3] o nową kategorię → fake newsów. W procesie → dezinformacji główny nacisk kładziony jest na cel przekazywania nieprawdziwej informacji, stosując ją jako narzędzie do osiągnięcia wymiernych korzyści. Podmiot dezinformujący oczekuje, że przekazanie nieprawdziwej informacji spowoduje podjęcie nieprawidłowych decyzji przez odbiorców, prowadząc tym samym do zamierzonego celu.

Dezinformacja to szereg działań konsekwentnie wprowadzany, skupiony na szerszej grupie społecznej, a nie tylko na pojedynczej jednostce. Dezinformacja może obejmować różne dziedziny, takie jak polityka, ekonomia, nauka, technika, wojskowość. Dezinformacja poza utrzymywaniem podmiotu dezinformowanego w niepewności i błędzie może pomóc w uzyskaniu efektów zaskoczenia niezwykle istotnych na płaszczyźnie operacyjno-strategicznej. Opiera się ona m.in. na blokowaniu kanałów wzajemnej komunikacji.

Środki dezinformacji wojskowej powinny być skoordynowane z → operacjami psychologicznymi [t. 3] gwarantującymi korzystne nastawienie → ludności cywilnej [t. 3] i kierownictwa wojskowego sił wielonarodowych. Zaniedbanie tej okoliczności może prowadzić do kompromisu w sprawie oszustwa. → Wywiad [t. 4] i → kontrwywiad również są niezwykle ważne dla organizacji dezinformacji wojskowej, szczególnie przy planowaniu, realizacji i zakończeniu każdej operacji.

Dezinformacja wojskowa to szczególny rodzaj dezinformacji skupiony na płaszczyźnie wojskowej. Podmiot dezinformujący wprowadza nieprawdziwe informacje dotyczące zamierzeń i planów, a także siły i proporcji o znaczeniu militarnym. Skutecznie zrealizowana dezinformacja wojskowa przynosi zwycięstwo. Proces ten jest przeprowadzany przez wyspecjalizowane jednostki posiadające odpowiednie zasoby, podstawą

których jest rozpoznanie podmiotu. Konieczne jest właściwe przygotowanie kanałów informacyjnych, pozbawiających podmiot dezinformowany możliwości wery kacji.

Dezinformacja wojskowa jest prowadzona nie tylko w trakcie → wojny [t. 4], lecz również w trakcie pokoju. Prowadzona jest na poziomach: strategicznym, operacyjnym i taktycznym, zarówno w formie działań ofensywnych, jak i defensywnych. Dezinformacja wykorzystuje różne kanały, m.in. polityczne, dyplomatyczne, ekonomiczne, naukowo-techniczne, wojskowe i specjalne.

M. Świerczek przytacza kilka zróżnicowanych określeń dezinformacji wojskowej, wskazując, że jest ona:

> wyjątkowo złożoną metodą pracy operacyjnej, będącą sposobem oddziaływania na aktualnego czy potencjalnego przeciwnika, wrogie → służby specjalne [t. 4] bądź określone grupy czy warstwy społeczne w innym, ale niekiedy też i własnym kraju. Termin wymyślony przez niemieckie służby specjalne w czasie I wojny światowej; przy sztabie armii niemieckiej do końca działań wojennych istniała komórka dezinformacyjna sterowana przez wojskową służbę wywiadowczą. Później służby specjalne innych państw wprowadziły tę formę działania jako metodologiczny sposób oddziaływania na przeciwnika, podejmowany z zamiarem wykreowania celowego, ukierunkowanego wpływu na kształtowanie opinii i bieg możliwych do przewidzenia zdarzeń;
>
> celowo fałszywą informacją, która ma wpłynąć na określoną grupę ludzi lub całą populację – jest to jedna z podstawowych metod pracy operacyjnej wywiadu, służąca wpłynięciu na postępowanie przeciwnika, by zachował się korzystnie dla służby wywiadowczej;
>
> tworzeniem i rozprzestrzenianiem mylącej lub fałszywej informacji w celu zniekształcenia obrazu przeciwnika;
>
> celowym przekazywaniem przeciwnikowi, za pomocą środków i metod pracy operacyjnej, nieprawdziwych informacji w celu wprowadzenia go w błąd i uzyskania zaplanowanych rezultatów;
>
> prowokacją, a nie kłamstwem państwa używającym swych wywiadów do malowania obrazu prowokującego przeciwnika do podejmowania błędnych ocen;

działaniem stawiającym sobie za cel realizację konsekwentnego programu zmierzającego do zastąpienia w świadomości, a przede wszystkim podświadomości, mas będących przedmiotem działań poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie;
systematycznymi wysiłkami zmierzającymi do rozprzestrzeniania nieprawdziwych informacji i do zafałszowania lub zablokowania informacji dotyczących rzeczywistej sytuacji i polityki.

Procesy dezinformacyjne muszą podlegać ciągłym zmianom, unikanie wcześniej używanych technik, różnorodność i nieszablonowość są charakterystyczne dla działań. Manipulacja jako jedna z form dezinformacji polega na przekazywaniu nieprawdziwych danych, pomijaniu ważnych danych a przekazywaniu mniej istotnych, zmniejszaniu rangi danych istotnych, przekazywaniu informacji wieloznacznych, co utrudnia ich właściwe zrozumienie, tworzeniu i przekazywaniu nadmiaru danych, prowadząc do powstania szumu informacyjnego. Dezinformacja jest niezwykle istotnym elementem prowadzenia walki informacyjnej, jej działania odbywają się m.in. poprzez paraliż procesu decyzyjnego, rozłam pomiędzy sojusznikami, wzbudzanie strachu, a także → trolling [t. 4], → dywersję ideologiczną czy też manipulowanie → mediami społecznościowymi [t. 3].

Zgodnie z terminologią przyjętą w rosyjskich siłach zbrojnych dezinformacja wojskowa jest elementem maskowania operacyjnego lub strategicznego. W ściśle tajnym słowniku KGB z 1972 r. zdefiniowano „dane dezinformacyjne" jako „specjalnie przygotowane dane, wykorzystywane do tworzenia w umyśle wroga niepoprawnych lub wyimaginowanych obrazów rzeczywistości, na podstawie których wróg podejmowałby korzystne decyzje" dla Związku Radzieckiego. Stosowanie dezinformacji wojskowej jako broni przez KGB, wcześniej GPU (Państwowy Zarząd Polityczny przy Ludowym Komisariacie Spraw Wewnętrznych Rosyjskiej Federacyjnej Socjalistycznej Republiki Radzieckiej) rozpoczęło się w 1923 r., kiedy I.S. Unszlicht, wiceprezes GPU, zaproponował utworzenie „specjalnego biura dezinformacji do prowadzenia aktywnych operacji wywiadowczych i wojskowych". Wg ostatniego tomu historii rosyjskiego wywiadu, opublikowanego w Rosji pod redakcją J. Primakowa, w różnych

okresach „radzieckie operacje dezinformacyjne przeciwko specjalnym służbom wroga miały kilka oznaczeń: «działania wpływowe», «dezinformacja operacyjna», «aktywne środki», «gry operacyjne» oraz «środki pomocy»". Pomimo różnic w kategoriach wszystkie były i są konkretnymi, ukierunkowanymi działaniami mającymi na celu dezinformowanie wojskowe faktycznego lub potencjalnego przeciwnika w stosunku do prawdziwych zamiarów lub możliwości oraz służącymi uzyskaniu korzystnej reakcji „celu działania", która byłaby praktycznie nieosiągalna za pomocą otwartych środków.

Wojskowe operacje dezinformacyjne stawiają sobie zwykle za cel doprowadzenie wroga do tego, by pozyskał informacje i uwierzył w to, że ofensywa lub atak planowane są w określonym czasie, przeciwnik posiada lub nie posiada określonego typu broni, mimo że jest dokładnie odwrotnie. Archetypem dezinformowania wojskowego może być przypadek wojny trojańskiej. O arowany Trojanom koń, w którym znajdowali się greccy wojownicy, został przekazany wrogom jako prezent sygnalizujący rezygnację z oblężenia miasta. Prezent został w Troi przyjęty z ulgą. Dezinformacja, wg mitów greckich przypisywania Odyseuszowi, udała się bezbłędnie, ponieważ zarówno Odyseusz, kreując treść dezinformującego komunikatu, w pełni osiągnął swój cel, jak i Trojanie całkowicie poddali się informacji dotyczącej otrzymania podarunku i wycofania się wojsk greckich.

Dezinformacja wojskowa była także stosowana w czasie → z i m n e j w o j n y [t. 4]. Na początku 1952 r. za sprawą działań Związku Radzieckiego prowadzono znaczącą kampanię dezinformacyjną, w której twierdzono, że USA wykorzystują broń biologiczną w Korei. Niedawno ujawnione dokumenty z radzieckich archiwów dowodzą, że KGB (wówczas pn. MGB – Ministerstwo Bezpieczeństwa Państwowego ZSRR) było głęboko zaangażowane w rozpowszechnianie fałszywej historii „w celu oskarżenia Amerykanów o użycie broni bakteriologicznej w Korei i Chinach". W. Burchett, australijski dziennikarz i członek Partii Komunistycznej, ściśle współpracował z chińskimi urzędnikami i był niezwykle aktywny w rozpowszechnianiu fałszywej opowieści wśród dziennikarzy na Dalekim Wschodzie. Później w 1957 r., gdy Burchett był w Moskwie, został agentem KGB. Dokument znaleziony w rosyjskich archiwach ujawnia, że w lipcu

1957 r. KGB poinformowało Komitet Centralny Partii Komunistycznej, że ich agent Burchett, który został wyznaczony „do penetracji amerykańskiej i zachodnioeuropejskiej prasy burżuazyjnej", został moskiewskim korespondentem prokomunistycznej amerykańskiej gazety „National Guardian".

Cel wojskowej operacji dezinformacyjnej jest postrzegany jako pożądany rezultat oszustwa, wyrażony jako to, co wróg powinien lub czego nie powinien robić w kluczowym czasie i/lub miejscu. Oznacza to, że w przypadku każdej operacji i potencjalnie na każdym jej etapie cele oszustwa będą różne, w zależności od konkretnych warunków bieżącej sytuacji.

Dezinformacja wojskowa jest przeprowadzana w celu wsparcia wspólnych operacji w celu wywarcia wpływu na dowództwo i kwaterę główną wroga, zmniejszając jego zdolność do zarządzania i kontroli.

W dzisiejszym środowisku postępującej informatyzacji, digitalizacji oraz rozwoju środowiska → b i g d a t a, w którym informacja podlega dynamicznym zmianom i każdy może być jej nadawcą, procesy związane z dezinformacją są ułatwione. Kreowanie wizji świata stało się jednym ze sposobów prowadzenia polityki, co prowadzi do wielu niebezpieczeństw zarówno dla jednostki, jak i dla całego społeczeństwa.

Edyta Sadowska, Jakub Idzik

R. Brzeski, *Dezinformacja*, Warszawa 2011; L. Ciborowski, *Mechanizmy i przestrzenie walki informacyjnej*, [w:] *Informacja w walce zbrojnej*, G. Nowacki (red.), AON, Warszawa 2002; E. Sadowska, *Big data*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J. Janczak, *Zakłócenia informacyjne*, AON, Warszawa 2001; H. Lewandowski, *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, Wydawnictwo UOP, Warszawa 2000; S. Lewandowsky, W.G.K. Stritzke, A.M. Freund i in., *Misinformation, Disinformation, and Violent Con ict: From Iraq and the „War on Terror" to Future reats to Peace*, „American Psychologist" 2013, vol. 68 (7); NASK Cyber Policy, *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, NASK Państwowy Instytut Badawczy, Warszawa 2019; H. Romerstein, *Disinformation as a KGB Weapon in the Cold War*, „Journal of Intelligence History" 2001, vol. 1; M. Świerczek *„System matrioszek", czyli dezinformacja doskonała. Wstęp do zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19; V. Volko ,

Dezinformacja – oręż wojny, Wydawnictwo Delikon, Warszawa 1991; M. Wrzosek, *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2 (87); A. Żebrowski, *Ewolucja polskich służb specjalnych: wybrane obszary walki informacyjnej: wywiad i kontrwywiad w latach 1989–2003*, Wydawnictwo Arcana, Kraków 2005.

Dobra kultury – ochrona w warunkach konfliktu zbrojnego – pierwszymi dokumentami chroniącym dobra kultury były postanowienia konwencji haskich z lat 1899 i 1907. Później treści dotyczące ochrony dóbr kultury zawarto w traktacie wersalskim z 1919 r. W okresie międzywojennym rozwijało się prawo w tej dziedzinie, nie ochroniło ono jednak dóbr kultury przed zniszczeniami w trakcie II wojny światowej. Doświadczenia → wojny [t. 4] doprowadziły do prac nad całościową konwencją. Ukoronowaniem tych prac było przyjęcie w Hadze w 1954 r. Konwencji o ochronie dóbr kulturalnych w wypadku konfliktu zbrojnego (zob. → dobra kultury – ochrona w warunkach konfliktu zbrojnego).

Konwencja haska z 1954 w art. 1 podaje definicję dóbr kulturalnych, są to:

a) dobra ruchome lub nieruchome, które posiadają wielką wagę dla dziedzictwa kulturalnego narodu, na przykład zabytki architektury, sztuki lub historii, zarówno religijne, jak świeckie; stanowiska archeologiczne; zespoły budowlane posiadające jako takie znaczenie historyczne lub artystyczne; dzieła sztuki, rękopisy, książki i inne przedmioty o znaczeniu artystycznym, historycznym lub archeologicznym, jak również zbiory naukowe i zbiory książek, archiwaliów oraz reprodukcji wyżej określonych dóbr;
b) gmachy, których zasadniczym i stosowanym w praktyce przeznaczeniem jest przechowywanie lub wystawianie dóbr kulturalnych ruchomych, określonych pod lit. a), takie jak muzea, wielkie biblioteki, składnice archiwalne, jak również schrony mające na celu przechowywanie w razie konfliktu zbrojnego dóbr kulturalnych ruchomych, określonych pod lit. a);

c) ośrodki obejmujące znaczną ilość dóbr kulturalnych określonych powyżej, a zwanych w tekście Konwencji „ośrodkami zabytkowymi".

Elementem konwencji, który od początku budził istotne wątpliwości, była kwestia tzw. konieczności wojskowej, umożliwiającej uchylenie się od wymogu ochrony dóbr kulturalnych w wypadku zaistnienia kategorycznej konieczności wojskowej (art. 4.2 Konwencji).

Konwencja przewiduje możliwość przyznania niektórym dobrom kulturalnym tzw. ochrony specjalnej. Zgodnie z treścią art. 8 konwencji:

> Ochroną specjalną może być objęta ograniczona ilość schronów przeznaczonych do przechowywania dóbr kulturalnych ruchomych w razie konfliktu zbrojnego oraz ośrodków zabytkowych i innych dóbr kulturalnych nieruchomych o bardzo wielkim znaczeniu, pod warunkiem, że:
>
> a) znajdują się w dostatecznej odległości od wielkich ośrodków przemysłowych oraz od wszelkich ważnych obiektów wojskowych stanowiących punkty wrażliwe, jak na przykład lotnisk, radiowych stacji nadawczych, zakładów pracujących na rzecz obrony narodowej, portów lub dworców kolejowych o pewnym znaczeniu, jak również wielkich linii komunikacyjnych;
> b) nie są użytkowane do celów wojskowych.
>
> Schron dla dóbr kulturalnych ruchomych może być objęty ochroną specjalną bez względu na swoje położenie, jeżeli jest zbudowany w taki sposób, że według wszelkiego prawdopodobieństwa nie może ponieść szkody w bombardowaniu.
>
> Ośrodek zabytkowy uważa się za użytkowany do celów wojskowych, jeżeli służy do przemieszczania, chociażby tylko tranzytowego, osób wojskowych lub materiału wojskowego, jak również jeżeli jest terenem czynności bezpośrednio związanych z działaniami wojskowymi, z kwaterunkiem osób wojskowych lub z produkcją materiału wojennego.
>
> Natomiast nie jest uważane za użytkowanie do celów wojskowych strzeżenie dóbr kulturalnych wymienionych w ust. 1 przez uzbrojonych strażników specjalnie powołanych do tego zadania

> ani obecność w pobliżu dóbr kulturalnych sił policyjnych, do których stałego zakresu działania należy zapewnienie porządku publicznego.
>
> Dobro kulturalne, wymienione w ust. 1 niniejszego artykułu, położone w pobliżu ważnego obiektu wojskowego w rozumieniu tegoż ustępu, może być jednak objęte ochroną specjalną. Jeżeli Wysoka Umawiająca się Strona, która składa o to wniosek, zobowiąże się, że w razie konfliktu zbrojnego zaniecha wszelkiego użytkowania odnośnego obiektu, a w szczególności, gdy chodzi o port, dworzec kolejowy lub lotnisko – wyłączy go z wszelkiego ruchu komunikacyjnego. Wyłączenie takie powinno być przygotowane już w czasie pokoju.
>
> Ochrona specjalna zostaje przyznana dobru kulturalnemu przez wpisanie go do „Międzynarodowego Rejestru Dóbr Kulturalnych Objętych Ochroną Specjalną".

Co istotne z punktu widzenia → edukacji obywatelskiej i praw nej sił zbrojnych, konwencja zobowiązuje, by włączyć jej nauczanie

> do programów szkolenia wojskowego, a w miarę możliwości również cywilnego tak, aby […] zasady [konwencji – przyp. aut.] mogły być znane całej ludzkości, a zwłaszcza siłom zbrojnym i personelowi przydzielonemu do ochrony dóbr kulturalnych.

Konwencja została rozwinięta tekstem Protokołu drugiego do konwencji haskiej z 1954 r. o ochronie dóbr kulturalnych w razie konfliktu zbrojnego. Protokół podkreślił m.in. znaczenie prowadzenia specjalnych programów edukacyjnych i informacyjnych. Ponadto protokół w miejsce ochrony specjalnej wprowadził tzw. ochronę wzmocnioną (art. 10 i nast.). Zgodnie z postanowieniami Protokołu drugiego ochroną wzmocnioną może zostać objęte dobro kulturalne, pod warunkiem, że spełnia ono 3 następujące warunki:

a) jest dziedzictwem kulturalnym o największym znaczeniu dla ludzkości;

b) jest chronione na mocy odpowiednich krajowych środków prawnych i administracyjnych, uznających jego wyjątkową wartość kulturową i historyczną oraz zapewniającą ochronę w najwyższym stopniu;
c) nie jest wykorzystywane do celów wojskowych lub dla osłony miejsc wojskowych i Strona, która sprawuje władzę nad tym dobrem kulturalnym, złożyła deklarację potwierdzającą, że nie zostanie ono w ten sposób wykorzystane.

Regulacje Konwencji haskiej wraz z protokołami uzupełniają postanowienia norm → międzynarodowego prawa humanitarnego konfliktów zbrojnych [t. 3]. Również Statut → Międzynarodowego Trybunału Karnego [t. 3] chroni kulturę, penalizując działania skierowane przeciwko dobrom kulturalnym.

Piotr Łubiński

R. Abi-Saab, *Humanitarian Law and Internal Con icts: e Evolution of Legal Concern*, [w:] *Humanitarian Law of Armed Con ict: Challenges Ahead – Essays in Honour of Frits Kalshoven*, A.J.M. Delissen, G.J. Tanja (eds.), Nijho Publishers, Dodrecht–Boston–London 1991; Art. 8 Konwencji o ochronie dóbr kulturalnych w razie kon iktu zbrojnego wraz z regulaminem wykonawczym do tej konwencji oraz Protokół o ochronie dóbr kulturalnych w razie kon iktu zbrojnego, podpisane w Hadze dnia 14 maja 1954, Dz. U. 1957 nr 46, poz. 212; Art. 10 drugiego Protokołu do Konwencji o ochronie dóbr kulturalnych w razie kon iktu zbrojnego, podpisanej w Hadze dnia 14 maja 1954 r., sporządzony w Hadze dnia 26 marca 1999 r., Dz. U. 2012, poz. 248; R. Bierzanek, *Wojna a prawo międzynarodowe*, Wydawnictwo Ministerstwa Obrony Narodowej, Warszawa 1982; W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe publiczne*, Wydawnictwo C.H.Beck, Warszawa 2004.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej – dokument opracowany przez → Biuro Bezpieczeństwa Narodowego [t. 1] w konsultacji z organizacjami sektora publicznego (instytucji administracji, środowiska akademickiego) oraz prywatnego. Został zatwierdzony przez → Radę Bezpieczeństwa Narodowego [t. 3] 12 stycznia 2015 r. Ma charakter wykonawczy w stosunku do → Strategii Bezpieczeństwa Narodowego [t. 4].

Doktryna jest oficjalną podstawą koncepcyjną organów państwa Rzeczypospolitej Polskiej, mającą zapewnić strategiczny cel, którym jest → bezpieczeństwo [t. 1] funkcjonowania → cyberprzestrzeni [t. 1] w kontekście transsektorowym – w ujęciu praktycznym stanowi rekomendacje dla państwowych podmiotów odpowiedzialnych za teleinformatyczną → infrastrukturę krytyczną państwa oraz prywatnych podmiotów gospodarczych. Określa cele w dziedzinie → cyberbezpieczeństwa [t. 1], opisuje środowisko, wskazując na → zagrożenia [t. 4], ryzyka i szanse, a także wskazuje najważniejsze zadania, jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa.

Jego osiągnięciu ma służyć realizacja celów o charakterze operacyjnym i preparacyjnym. Do pierwszych zaliczono: ocenę warunków cyberbezpieczeństwa, w tym rozpoznanie zagrożeń, szacowanie ryzyka i identyfikowanie szans, zapobieganie zagrożeniom, redukowanie ryzyka i wykorzystanie szans, obronę i ochronę własnych systemów i ich zasobów, zwalczanie źródeł zagrożeń, odtwarzanie sprawności i funkcjonalności systemów cyberprzestrzeni po ewentualnym ataku. Warto zwrócić uwagę na wymienione zagadnienie „zwalczania źródeł zagrożeń", która precyzuje dopuszczalne odpowiedzi państwa w postaci działań ofensywnych i defensywnych, takich jak dezorganizacja, zakłócanie oraz niszczenie.

Cele preparacyjne sprowadzono do zbudowania, utrzymania i doskonalenia systemu cyberbezpieczeństwa obejmującego podsystemy kierowania (czyli organizowania skoordynowanych działań podmiotów państwowych i niepaństwowych), operacyjne i wsparcia (czyli posiadające rzeczywiste zdolności ofensywne i defensywne oraz możliwość wsparcia sojuszników). Dokument wskazuje Radę Ministrów jako organ, który ma być odpowiedzialny za koordynację działań w cyberprzestrzeni na poziomie strategicznym. Praktycznym posunięciem, które mogłoby przybliżyć realizację tego celu, jest pkt 38 doktryny rekomendujący tworzenie podporządkowanych właściwym ministrom odrębnych technicznych centrów kompetencyjnych.

Duże znaczenie ma umieszczony we wprowadzeniu wykaz pojęć, którymi posługuje się dokument, dotyczą one terminów w większości niezdefiniowanych w przepisach prawa polskiego, co w pewien sposób zawęża dalszą dyskusję i rozwiązuje dotychczasowe dylematy w naukach

społecznych i prawnych. Autorzy przybliżają m.in. definicję cyberbezpieczeństwa RP, bezpieczeństwa cyberprzestrzeni RP, → środowiska cyberbezpieczeństwa [t. 4], wyzwania cyberbezpieczeństwa, ryzyka cyberbezpieczeństwa, zagrożenia cyberbezpieczeństwa. Na uwagę zasługuje definiowanie pojęcia cyberprzestrzeni w sposób odmienny od definicji legalnej zawartej m.in. w ustawach o stanie wojennym i o stanie wyjątkowym.

Zwrócono uwagę na podnoszenie świadomości obywatelskiej w zakresie cyberbezpieczeństwa oraz cyberobrony i cyberochrony kraju. Wiele miejsca poświęcono współpracy sektora publicznego i prywatnego, wspieraniu podmiotów sektora prywatnego.

W drugim rozdziale dokumentu podjęto analizę środowiska cyberbezpieczeństwa, które definiowano jako ogół warunków funkcjonowania danego podmiotu w cyberprzestrzeni, scharakteryzowanego w doktrynie przez wskazanie wyzwań (szanse i ryzyka) oraz zagrożeń dla osiągania przyjętych celów, na 2 płaszczyznach – w wymiarze wewnętrznym i zewnętrznym.

Wśród najważniejszych wymienionych ryzyk wymiaru wewnętrznego są poruszone takie zagadnienia jak zakup infrastruktury technicznej systemowej z zagranicy oraz związany z tym brak dostępu do kodów źródłowych oprogramowania; problem dotyczący współpracy organów państwa z prywatnymi operatorami i dostawcami usług teleinformatycznych, których zarządy decyzyjne znajdują się poza granicami kraju; uwzględnienie ochrony → praw człowieka [t. 3] i obywatela w działaniach legislacyjnych i bezpośrednich, zwłaszcza z poszanowaniem prawa do wolności słowa oraz prywatności. W dokumencie zasugerowano rozwiązanie poprzez podniesienie wagi dialogu i znaczenia konsultacji społecznych, podniesienie stanu → edukacji obywatelskiej poprzez samokształcenie w zakresie cyberbezpieczeństwa – także poprzez wykorzystanie potencjału obywateli w społecznych inicjatywach wspierających cyberbezpieczeństwo RP w formie wolontariatu. Wsparcie dla tej inicjatywy miałoby powstać dzięki współpracy na linii obywatele – sektor prywatny – sektor publiczny.

Wśród poruszonych tematów związanych z szansami wymiaru wewnętrznego doktryna odwołuje się do rozwoju dziedziny nauk

informatycznych i podkreśla wyraźnie korelację między poziomem innowacyjności, posiadanej technologii, wiedzy i specjalistów a oddziaływaniem na → bezpieczeństwo narodowe [t. 1] państwa.

Doktryna zawiera zbiór zadań operacyjnych i preparacyjnych w dziedzinie cyberbezpieczeństwa państwa, które są skierowane do sektora publicznego w wymiarze krajowym i międzynarodowym, sektora prywatnego i obywatelskiego, wyznacza także zadania transsektorowe. Zadania operacyjne sektora publicznego w wymiarze krajowym obejmują m.in. rozpoznawanie źródeł zagrożeń, prowadzenie analiz ryzyka, działania w obszarze kryptografii i kryptoanalizy, bieżące monitorowanie zagrożeń z wykorzystaniem zespołów CERT (Computer Emergency Response Team), prowadzenie audytów cyberbezpieczeństwa. Podkreślono potrzebę przygotowania i wdrażania scenariuszy postępowania w warunkach → cyberataków [t. 1] i planów reagowania kryzysowego. Zaakcentowano konieczność prowadzenia aktywnej cyberobrony oraz utrzymania gotowości do → cyberwojny [t. 1], ochrony i obrony własnych systemów teleinformatycznych, przeciwdziałania i zwalczania → cyberprzestępczości [t. 1]. Do zadań sektora publicznego w wymiarze międzynarodowym zaliczono w szczególności współpracę w ramach systemów reagowania → NATO [t. 3] i UE. Zadania sektora prywatnego to współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom cybernetycznym, prowadzenie audytu środków i mechanizmów cyberbezpieczeństwa, współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni. Wśród zadań sektora obywatelskiego wymieniono na pierwszym miejscu dbałość o użytkowane systemy i urządzenia teleinformatyczne jako formę pomocy w zapewnieniu bezpieczeństwa państwa. Jedynym zadaniem transsektorowym jest koordynacja współpracy podmiotów sektora prywatnego i publicznego oraz tworzenie mechanizmów wymiany → informacji, a także standardów i dobrych praktyk w obszarze cyberbezpieczeństwa.

Najważniejszym zadaniem preparacyjnym jest wdrożenie i rozwój systemowego podejścia do cyberbezpieczeństwa w wymiarze prawnym, w tym przyjęcie nowych rozwiązań prawnych, organizacyjnych i technicznych. Rozwiązania przyjmowane w tym zakresie powinny być zgodne z dokumentami UE i NATO oraz innymi inicjatywami międzynarodowymi.

Twórcy doktryny zakładają wykorzystanie i rozszerzenie jej treści w pracach nad innymi dokumentami, takimi jak Polityczno-Strategiczna Dyrektywa Obronna, w planach → zarządzania kryzysowego [t. 4], programach rozwoju sił zbrojnych oraz programach pozamilitarnych przygotowań obronnych.

Wojciech Cendrowski

M. Adamczuk, K. Liedel, *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12; W. Cendrowski, *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2015; J. Kowalewski, M. Kowalewski, *Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017; Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz. U. 2002, nr 156, poz. 1301; Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz. U. 2002, nr 11, poz. 985.

Doktryna militarna (właśc. wojskowa) – oficjalnie przyjęty przez państwo system naukowo uzasadnionych poglądów dotyczących sposobu przygotowania obrony kraju w sytuacjach → zagrożenia [t. 4] zewnętrznego oraz prowadzenia działań wojennych z zastosowaniem metod i środków będących w dyspozycji państwa lub koalicji państw. Za sprawą powyższej definicji doktryna militarna często jest utożsamiana z doktryną wojenną, która jest pojęciem nieco szerszym i stanowi zbiór poglądów i idei związanych z przygotowaniem i prowadzeniem → wojny [t. 4] jako całości z uwzględnieniem takich czynników jak ustrój państwa, sytuacja polityczna (wewnętrzna i międzynarodowa), zasoby kraju, potencjał gospodarczy, poziom naukowo-techniczny, doświadczenie prowadzenia wojny, położenie geograficzne.

Doktryna militarna wywodzi się ze → sztuki wojennej [t. 4] będącej dziedziną wiedzy i umiejętności dotyczącą form i sposobów przygotowania oraz prowadzenia działań wojennych. Sztuka wojenna już w starożytności zaliczana była, podobnie jak większość dziedzin nauki,

do lozofii, a jako pierwszy opisał ją żyjący na przełomie VI i V w. p.n.e. chiński generał i filozof Sun Zi (Sun Tzu).

Polityka wojskowa jest integralną częścią działań każdego państwa, a jej głównym celem jest zagwarantowanie → bezpieczeństwa [t. 1] wojskowego kraju. Skoncentrowane rozumienie polityki wojskowej znajduje się w państwowej doktrynie wojskowej/militarnej, czyli deklaracji polityki państwa w dziedzinie bezpieczeństwa wojskowego (obronnego) określającej system oficjalnych poglądów i przepisów wyznaczających kierunki budowy wojsk, warunki przygotowania państwa i sił zbrojnych do wojny, środki i formy prowadzenia wojny. Podstawowe postanowienia doktryny militarnej są opracowywane i zmieniane w zależności od polityki i porządku społecznego, poziomu rozwoju sił produkcyjnych, nowych osiągnięć naukowych i charakteru spodziewanej wojny.

W rzeczywistości doktryna militarna stanowi ideologiczny rdzeń wszelkiej militarno-politycznej działalności państwa (polityki wojskowej) jako jeden z kierunków ogólnej polityki państwa, partii politycznych, organizacji pozarządowych i instytucji. Dotyczy interesów społeczeństwa i wszystkich struktur państwowych. W dokumentach tego rodzaju intencje państwa są głoszone otwarcie, więc doktryna wojskowa nie powinna zawierać żadnych zamkniętych rozdziałów, nie może jej opracowywać konkretna grupa osób, niezależnie od publicznych i wojskowych środowisk akademickich. Podstawowe elementy doktryny wojskowej mogą w zależności od formy rządu zostać określone przez odpowiednie władze państwowe na określony czas.

Doktryna militarna uwzględnia aspekty polityczne i wojskowo-techniczne. Podstawowe założenia doktryny są określane przez kierownictwo polityczne i wojskowe państwa w zależności od ustroju społeczno-politycznego i poziomu rozwoju gospodarczego, naukowego i technicznego oraz wyposażenia sił zbrojnych kraju. Doktryna militarna jest wyrazem tego, w jaki sposób siły wojskowe przyczyniają się do kampanii, dużych operacji, bitew i walk, jednocześnie oznacza zbiór zasad, którymi siły zbrojne kierują się w działaniach, prowadząc swoje operacje. Obejmuje elementy → obrony narodowej [t. 3] i sojuszniczej zarówno z perspektywy społeczno-politycznej, jak i wojskowo-technicznej.

W XX w. zasadniczo wykształciły się 3 typy doktryn wojennych, mające charakter defensywny (obronny), ofensywny i mieszany. Zasadnicza

różnica pomiędzy nimi polega na tym, że podstawowe założenia doktryny wojennej formułują najwyższe organy władzy państwowej (parlament, prezydent), a doktrynę militarną – naczelne dowództwo armii danego państwa albo sojuszu wojskowego.

Swoje doktryny w XX w. posiadał każdy rodzaj sił zbrojnych – wojska powietrzne, → wojska lądowe [t. 4], → marynarka wojenna [t. 3]. Wszystkie zawierały podstawowe normy postępowania i ogólne procedury pozwalające na maksymalne skoordynowanie działań tych formacji. Jest to przewodnik po działaniu, a nie twarde i skody kowane zasady postę powania. Doktryna zapewnia wspólne ramy odniesienia dla całej armii. Pomaga ustandaryzować operacje, ułatwiając gotowość, ustanawiając wspólne sposoby wykonywania zadań wojskowych. Doktryna łączy teorię, historię, eksperymenty i praktykę. Jej celem jest wspieranie inicjatywy i kreatywnego myślenia. Doktryna dostarcza armii zbiór oświadczeń na temat tego, jak siły wojskowe prowadzą operacje, i zapewnia wspólny leksykon do wykorzystania przez planistów i dowódców wojskowych.

W wielu krajach termin doktryna militarna traktuje się jako poli-tykę → bezpieczeństwa [t. 1], która reprezentuje system poglądów o cjalnie przyjętych i wiążących przez pewien czas w danym państwie (koalicji wojskowej), opisując charakter możliwych kon iktów zbrojnych oraz przygotowanie i wdrożenie zbrojnej zewnętrznej ochrony państwa. Dlatego doktryna militarna działa głównie jako dokument konstytutywny. Opracowanie szczegółów wdrożenia w wojskowej praktyce politycznej jest zwykle obowiązkiem kolejnych dokumentów lub kompetencji organów władzy państwowej.

Jednocześnie doktryna nie jest → strategią [t. 4], operacją ani tak tyką, służy jako ramy koncepcyjne łączące wszystkie 3 poziomy działań wojennych. Doktryna różni się również od teorii, ponieważ jest instytu-cjonalna, ma charakter poznawczy, ponieważ jest zarówno częścią, jak i wynikiem procesu zdobywania, oceny i rozpowszechniania wiedzy. Dok-tryna jest z natury subiektywna, ponieważ jej treść odzwierciedla system przekonań. Ale doktryna to coś więcej niż tylko zasady. Jest to re eksja nad tym, w jaki sposób siły armii zamierzają działać jako część wspólnych sił, oraz stwierdzenie, w jaki sposób armia zamierza walczyć. Ustana wia wspólne ramy odniesienia, w tym narzędzia intelektualne, których

przywódcy armii używają do rozwiązywania problemów wojskowych. Ma skupiać się na tym, „jak" myśleć, a nie na tym, „co" myśleć.

De nicja doktryny → NATO [t. 3], stosowana przez wiele państw członkowskich w niezmienionej formie, brzmi: „Podstawowe zasady, zgodnie z którymi siły zbrojne wykonują swoje zadania z zamiarem osiągnięcia określonych celów. Odgrywa ona rolę nadrzędną, ale wyma ga oceny zasadności wykorzystania jej w praktyce". Do niedawna więk szość doktryn NATO była odzwierciedlona przez równoważne, ale różne narodowe doktryny. Często powodowało to dylemat dla sił zbrojnych różnych państw zaangażowanych w operacje w ramach koalicji.

Współczesne doktryny amerykańskie opierają się na koncepcji ope racji pełnego spektrum, które łączą operacje ofensywne, defensywne i sta bilności lub wsparcia cywilnego, jednocześnie w ramach współzależnych lub połączonych sił w celu przejęcia, utrzymania i wykorzystania inicja tywy. Stosują zsynchronizowane działania – śmiercionośne i nieśmier cionośne – proporcjonalne do misji i oparte na dokładnym zrozumieniu wszystkich wymiarów środowiska operacyjnego. Operacje ofensywne pokonują i niszczą siły wroga oraz zajmują teren, zasoby i centra ludności, narzucają wrogowi wolę dowódcy. Operacje obronne pokonują atak wroga, zyskują czas, oszczędzają siły i rozwijają warunki sprzyjające operacjom ofensywnym lub stabilności. Operacje stabilności obejmują różne misje wojskowe, zadania i działania prowadzone za granicą w celu utrzymania lub przywrócenia bezpiecznego środowiska, odbudowy infrastruktury w → sytuacjach kryzysowych [t. 4] i pomocy humanitarnej. Opera cje wsparcia cywilnego to zadania i misje wspierające cywilów na wypadek sytuacji kryzysowych w kraju i innych działań dotyczących skutków klęsk żywiołowych lub katastrof spowodowanych przez człowieka.

Wojsko USA potrzebuje wspólnej doktryny, która poprowadzi wszystkie służby w kierunku skoordynowanego podejścia do operacji obejmujących wiele dziedzin i zapewni odpowiednie inwestycje w do wodzenie i kontrolę, tworzenie sieci i podejmowanie decyzji. Ostat nia wspólna doktryna (JP-1) została opublikowana w 2013 r. a zmieniona w 2017 r. Nawet wraz z aktualizacją nie odzwierciedla ona nowych wy zwań strategicznych stawianych przez wschodzące wielkie mocarstwa, takie jak Rosja i Chiny, ani wzmocnionych regionalnych przeciwników,

takich jak Iran i Korea Północna. Nie odnosi się także do podstawowych założeń nowych strategii → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1] lub obrony narodowej, nie odzwierciedla charakteru rywalizacji między mocarstwami, zasięgu i złożoności zagrożeń dla bezpieczeństwa USA i Zachodu, zmian technologicznych dotyczących sposobu prowadzenia operacji wojskowych.

Armia kanadyjska ma swoją de nicję doktryny militarnej:

> Doktryna militarna jest formalnym wyrazem wiedzy i myśli wojskowej, którą armia uznaje za istotne w danym czasie, która obejmuje charakter kon iktu, przygotowanie armii do kon iktu oraz metodę angażowania się w kon ikt, aby osiągnąć sukces […]. Ma charakter opisowy, a nie nakazowy, wymaga przemyślenia w zastosowaniu. Nie ustanawia dogmatów ani nie zapewnia listy kontrolnej procedur, ale jest nadrzędnym przewodnikiem opi - sującym to, jak wojsko myśli o walce, a nie jak powinno walczyć. Stara się być wystarczająco de nitywną, aby pokierować działa niami wojskowymi, a jednocześnie wystarczająco wszechstronną, aby uwzględnić wiele różnych sytuacji.

Przez ok. 280 lat armia brytyjska osiągała znaczące sukcesy bez for malnej doktryny wojskowej, chociaż powstało wiele publikacji dotyczą- cych taktyki, operacji i administracji. Jednak podczas pełnienia funkcji szefa sztabu generalnego (1985–1989) gen. N. Bagnall zlecił przygotowanie brytyjskiej doktryny wojskowej płk. (późniejszemu gen.) T. Granville'owi- -Chapmanowi (o cerowi → a r t y l e r i i [t. 1], który był jego asystentem wojskowym w 1. Korpusie Brytyjskim). Pierwsze wydanie *British Military Doctrine* (BMD) zostało opublikowane w 1988 r., a w 1996 r. stała się ona brytyjską doktryną obronną (*British Defence Doctrine*, BDD) obowią- zującą we wszystkich siłach zbrojnych. Czwarta edycja BDD została opublikowana w 2011 r., wykorzystując de nicję doktryny NATO.

Radzieckie znaczenie doktryny wojskowej bardzo różniło się od użycia tego terminu przez wojsko USA. A. Grieczko, minister obro- ny ZSRR, marszałek Związku Radzieckiego, naczelny dowódca Wojsk Lądowych Armii Radzieckiej, naczelny dowódca Zjednoczonych Sił

Zbrojnych Państw Stron Układu Warszawskiego, zde niował ją w 1975 r. jako „system poglądów na temat natury wojny i metod jej prowadzenia oraz na temat przygotowania kraju i armii do wojny, o cjalnie przyjętych w danym państwie i jego siłach zbrojnych". W czasach radzieckich teore tycy podkreślali zarówno polityczną, jak i wojskowo-techniczną stronę doktryny wojskowej, podczas gdy z punktu widzenia ZSRR ludzie Za chodu ignorowali stronę polityczną. Doktryna radziecka (i współczesna rosyjska) podkreśla rozpoczęcie działań wojennych w wybranym przez siebie czasie i miejscu, zgodnie z wyborem i obszernym przygotowaniem pola bitwy do operacji.

Doktryna wojskowa Federacji Rosyjskiej jest dokumentem plano wania strategicznego i stanowi system o cjalnie przyjętych poglądów na stan przygotowań do obrony zbrojnej Rosji. Najnowsza wersja dok tryny wojskowej została zatwierdzona w 2014 r. Liczne kolejne rewizje doktryny wojskowej były ogłaszane w listopadzie 1993 r. po wydarze niach w Naddniestrzu 1993 r.; w kwietniu 2000 r. po wojnie w Czecze nii w 1999 r.; w lutym 2010 r. po wojnie rosyjsko-gruzińskiej w 2008 r. oraz w grudniu 2014 r. po → a n e k s j i [t. 1] Krymu i początku wojny na wschodzie Ukrainy w 2014 r. Doktryna w ujęciu rosyjskim wykracza poza dyskusję o potencjalnych zagrożeniach. Chronologia wydarzeń, które ją poprzedzały, i odsłony doktryny FR w nowych wydaniach pokazują, jak rosyjscy przywódcy próbują za każdym razem zalegalizować swoje przestępcze działania, wybielić je, a co najważniejsze, dać na przyszłość podobnym przestępstwom podstawę prawną. Doktryna wojskowa Rosji wyraźnie stwierdza, że 3/4 doktryny to komponent informacyjny albo wpływ ekonomiczny i tylko 1/4 to wykorzystanie siły zycznej.

Doktryna militarna jest podstawową koncepcją bezpieczeństwa pań stwa, dąży również do sformułowania celów i zadań polityki wojskowej państwa oraz określenia priorytetowych interesów, a także do wyrażenia swojego stanowiska w kwestiach wojennych i zagadnieniach związanych z obszarami użytkowania sił zbrojnych oraz przygotowywaniem misji bojowych przydzielonych siłom państwa w czasie wojny lub pokoju. Jest również diagnozą charakteru faktycznych i potencjalnych → z a g r o ż e ń m i l i t a r n y c h [t. 4] wobec państwa, stara się określić charakter przy szłej wojny oraz metody, za pomocą których można odeprzeć wszelką

→ agresję [t. 1] środkami militarnymi i opracować nowe koncepcje strategii wojskowych oraz wytyczne dotyczące przygotowania państwa w celu obrony terytorium państwa i jego bezpieczeństwa.

Doktryna składa się z podstawowych zasad, taktyki, technik, procedur oraz terminów i symboli. Przede wszystkim doktryna zawiera podstawowe zasady. Odzwierciedlają one poglądy armii na temat działań wojennych na podstawie jej dawnych doświadczeń, porażek i sukcesów, określają zasady ognia, manewrów i wspólnych operacji sił zbrojnych. Co ważne, doktryna nie zawsze ma charakter nakazowy, ale jest nadrzędna i stanowi punkt wyjścia do rozwiązywania nowych problemów. Zasady powinny wspierać inicjatywę, by → żołnierze [t. 4] byli zdolni do adaptacji i kre atywni w rozwiązywaniu trudności, są podstawą wprowadzania nowych technologii i projektów organizacyjnych.

Taktyki, techniki i procedury wykorzystują wiedzę i doświadczenie armii, wspierają i wdrażają podstawowe zasady, obejmują różne metody i procesy. Taktyka polega na uporządkowanym rozmieszczeniu sił wzglę dem siebie. Techniki to nie nakazowe sposoby lub metody wykorzystywane do wykonywania misji, funkcji lub zadań, są one podstawowym sposobem przekazywania wyciągniętych wniosków, które jednostki zdobywają pod czas operacji. Procedury to standardowe metody postępowania, zwykle składają się z szeregu kroków w ustalonej kolejności. Procedury są naka zowe, niezależnie od okoliczności są one wykonywane w ten sam sposób. Wspólny zestaw procedur w wojsku obejmuje standardową procedurę operacyjną dla poszczególnych jednostek. Wreszcie doktryna zapewnia wspólny język komunikacji wojskowych. Jest to szczególnie ważne podczas kon iktu zbrojnego, gdy → informacje muszą być szybko i dokładnie przekazywane oraz powszechnie zrozumiałe.

Terminy i de nicje stanowią większą część wspólnego języka armii, zrozumiałego dla wszystkich jej jednostek tak, aby jasne były zadania, któ re należy wykonać. Symbole wojskowe są sposobem zapewnienia wspól nego gra cznego zrozumienia niezliczonej ilości informacji i zapewniają inny sposób szybkiego przesyłania informacji. Ustanawianie i używanie słów i symboli o wspólnych znaczeniach wojskowych usprawnia komu nikację i umożliwia wspólne rozumienie doktryny, szybką identy kację zaangażowanych jednostek, dokładną identy kację zadań do wykonania.

Znaczenie tego wspólnego języka jest nieprzecenione. Pozwala osobom z zupełnie różnych środowisk na szybką naukę uniwersalnego języka. Umożliwia armii szybkie komunikowanie się, nawet gdy istnieje bariera językowa.

Fryderyk II Wielki (Friedrich II von Hohenzollern) – król Prus w latach 1740–1786, pod rządami którego Prusy stały się jednym z najpotężniejszych państw europejskich, powiedział: „Wojna nie jest przypadkiem. Aby dobrze ją prowadzić, niezbędna jest ogromna wiedza, nauka i medytacja”.

Olga Wasiuta

AAP-06 Edition 2019. NATO glossary of terms and definitions (English and French) NATO Standardization Office, 2019; *AAP-6. Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO*, NATO Standardization Office, 2017; I.T. Brown, *A New Conception of War: John Boyd, the U.S. Marines, and Maneuver Warfare*, Marine Corps University Press, Quantico, Virginia 2018; Canada Department of National Defence, *Conduct Of Land Operations – Operational Level Doctrine For the Canadian Army (English)*, Department of National Defence, 1998; R.M. Cassidy, *Peacekeeping in the Abyss: British and American Peacekeeping Doctrine and Practice after the Cold War*, Praeger, London 2004; B. Chapman, *Military Doctrine: A Reference Handbook*, ABC-CLIO, Santa Barbara 2009; R. Frank, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907–1960*, Air University Press, 1989; A.P. Jackson, *The Roots of Military Doctrine: Change and Continuity in Understanding the Practice of Warfare. Combat Studies Institute Press*, Fort Leavenworth, KA 2013; E. Kier, *Imagining War: French and British Military Doctrine between the Wars*, Princeton University Press, Princeton 1998; A. Long, *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the US and UK*, Cornell University Press, London 2016; G. Sheffield, *Doctrine & Command in the British Army, A Historical Overview*, Army Doctrine Publication Land Operations, DGD&D, British Army, 2005; Ch.P. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations*, Cornell University Press, London 2010.

Doktryna ONZ „odpowiedzialność za ochronę” (ang. *Responsibility to Protect*, R2P, RtoP) – doktryna, która proponuje szereg kompleksowych rozwiązań – od prewencji, poprzez reakcję, do odbudowy – stosowanych w celu → ochrony ludności [t. 3] przed najdotkliwszymi

następstwami kon iktu. Doktryna ma ważną ogólną wartość teoretyczną, ponieważ dotyczy bezpośrednio podstawowych kategorii prawnych, w szczególności → praw człowieka [t. 3] i → suwerenności państwa [t. 4]. Jak podkreśla A.-M. Slaughter:

> doktryna odpowiedzialności za ochronę jest najważniejszą doktryną w koncepcji suwerenności państwa od czasu pokoju westfalskiego 1648 r. Zakłada ona fundament ładu międzynarodowego, który uznaje prawa i obowiązki jednostek i narodów.

Współczesne procesy transformacji stosunków międzynarodowych i myślenia geopolitycznego mają znaczący wpływ na kształtowanie nowego podejścia do → bezpieczeństwa narodowego [t. 1] jako jednego z głównych problemów geopolitycznych państwa. Znacznie zwiększa się rola czynników niemilitarnych bezpieczeństwa narodowego, jak stanu systemów informacyjnych, rozwoju strategicznie ważnych gałęzi nauki, ogólnego poziomu wykształcenia ludności itp.

Wydarzenia społeczne i polityczne ostatnich lat stały się trudnym sprawdzianem właściwości regulacyjnych i efektywności prawa międzynarodowego oraz zaktualizowały nowe problemy współczesnych badań. W tym samym czasie, gdy społeczeństwo staje w obliczu → zagrożenia [t. 4] → zbrodniami przeciwko ludzkości [t. 4], → ludobójstwem [t. 3], czystkami etnicznymi i innymi masowymi i rażącymi naruszeniami praw człowieka, a konkretne państwo najwyraźniej nie jest w stanie im przeciwdziałać, wtedy zobowiązania podtrzymania → bezpieczeństwa [t. 1] opierają się na społeczności międzynarodowej. Te idee zawiera doktryna „odpowiedzialność za ochronę”.

We wrześniu 2000 r. z inicjatywy Kanady powstała Międzynarodowa Komisja ds. Interwencji i Suwerenności Państwa przy Organizacji Narodów Zjednoczonych (International Commission on Intervention and State Sovereignty, ICISS). W jej skład weszli wybitni specjaliści w zakresie międzynarodowego prawa człowieka, na czele z byłym ministrem spraw zagranicznych Australii G. Evansem i specjalnym doradcą sekretarza generalnego ONZ M. Sakhnunem. W 2001 r. grupa przedstawiła sekretarzowi generalnemu i państwom członkowskim ONZ dobrze

znany w prawie międzynarodowym raport *e Responsibility to Protect* (R2P), w którym zaproponowano alternatywę dla tzw. prawa do humanitarnej interwencji, zastępując je „odpowiedzialnością za ochronę”. W doktrynie podkreślono transformację międzynarodowego rozumienia ochrony ludności i praw człowieka, przewidując międzynarodową interwencję w przypadku ludobójstwa czy innych masowych zbrodni i redefiniując pojęcie suwerenności. W raporcie komisji opublikowanym w grudniu 2001 r. bez odpowiedzi pozostało pytanie, czy i pod jakimi warunkami → interwencja humanitarna byłaby legalna w przypadku braku autoryzacji ze strony → Rady Bezpieczeństwa ONZ [t. 3] lub Zgromadzenia Ogólnego ONZ.

Odpowiedzialność za ochronę jest koncepcją prawa międzynarodowego, nową zasadą miękkiego prawa międzynarodowego, która została podtrzymana przez ONZ w 2005 r. Składa się ona z kilku reguł, opartych na idei suwerenności nie jako przywileju państwa, a jako przede wszystkim obowiązku, historycznie wynikających z idei pokoju westfalskiego i norm nieinterwencji. Ogólnie doktryna R2P stwierdza, że „suwerenne państwa mają obowiązek chronić swoich obywateli przed możliwością uniknięcia katastrofy”, a „społeczność międzynarodowa ma obowiązek promowania i wspierania państw w wypełnianiu tego obowiązku”.

Jej źródłem jest koncepcja interwencji humanitarnej, odrzucona przez społeczność międzynarodową po akcji → NATO [t. 3] przeciw Jugosławii, w związku z konfliktem w Kosowie. Nowa doktryna koncentruje się na zapobieganiu międzynarodowym zbrodniom ludobójstwa, → zbrodniom wojennym [t. 4], zbrodniom przeciwko ludzkości i czystkom etnicznym. Zastosowanie R2P w przypadku innych przestępstw lub katastrof humanitarnych jest wykluczone. Interwencja humanitarna sama w sobie jest konceptualną hybrydą znajdującą się na skrzyżowaniu praw człowieka, prawa międzynarodowego i stosunków międzynarodowych. Przede wszystkim istnieje wyraźna potrzeba normatywnego ujęcia zasad i ich politycznego egzekwowania.

W wyniku wydarzeń z lat 90. XX w. doszło do poważnej i bardzo nagłośnionej międzynarodowej debaty oraz rewizji zasady nieinterwencji, w wyniku czego społeczność międzynarodowa zaczęła dopuszczać interwencje zbrojne jako prawnie i moralnie uzasadnione

w wyjątkowych okolicznościach oraz po wyczerpaniu się możliwości zastosowania innych środków. Do przypadków takich zaliczono akty ludobójstwa, upadek państwa skutkujący przewlekłym → kryzysem wewnętrznym i anarchią, łamanie praw człowieka i zagrożenia dla pokoju międzynarodowego.

Zgodnie z koncepcją podstawowym obowiązkiem państwa jest ochrona ludności na terytorium własnego państwa. Zakłada ona, że każde państwo ma obowiązek chronić swoją ludność przed ludobójstwem, zbrodniami wojennymi, czystkami etnicznymi oraz zbrodniami przeciwko ludzkości. Kiedy państwa nie mogą lub nie chcą wypełniać tego obowiązku – czy to z powodu braku możliwości, czy z przyczyn związanych z wolą polityczną – odpowiedzialność za ochronę przenosi się na wspólnotę międzynarodową, nawet wbrew władzom danego państwa. Wspomniana idea stała się m.in. podstawą interwencji w Libii w 2011 r. Odpowiedzialność za ochronę jest przemyśleniem koncepcji interwencji humanitarnej, ale w odróżnieniu od niej wykorzystuje działania zbrojne jako obowiązek społeczności międzynarodowej, a nie jako prawo państwa lub grupy państw.

Jednak w końcowym dokumencie Światowego Szczytu ONZ z 2005 r., przyjętym przez Zgromadzenie Ogólne (rezolucja nr 60/1), wykluczono możliwość podejmowania działań przez poszczególne państwa na podstawie doktryny R2P bez zezwolenia Rady Bezpieczeństwa ONZ. Pierwszą rezolucją Rady autoryzującą użycie siły w odwołaniu do koncepcji R2P była rezolucja nr 1973, na podstawie której miała miejsce interwencja w Libii w 2011 r. (Rosja i Chiny wstrzymały się wtedy od głosu). Rosja poparła interwencję w Libii (pierwsze właściwe zastosowanie R2P), wstrzymując się od głosowania w Radzie Bezpieczeństwa ONZ, ale wniosła swój wkład w impas w Syrii, nie zgadzając się nawet na przyjęcie rezolucji potępiającej okrucieństwa → reżimu [t. 3] Assada. Potępiła natomiast wdrożenie decyzji Rady Bezpieczeństwa w sprawie Libii jako wykraczającej daleko poza zakres rezolucji. Decyzja o ochronie ludności cywilnej została zastąpiona zmianą reżimu. Interweniując w celu ochrony ludności cywilnej, siły NATO ukierunkowały swoje działania także na obalenie reżimu Kadda ego. Ta szeroka interpretacja mandatu Rady miała istotny wpływ na niechęć Rosji i Chin do wdrażania jakichkolwiek sankcji

przeciwko Syrii. Przypadek Libii pokazuje więc, jak istotne jest, aby R2P jako bardzo młoda doktryna, niemająca charakteru prawnie wiążącego, była stosowana rygorystycznie i w sposób neutralny.

Istnieją poglądy, że doktryna R2P może być wykorzystywana także w innych sytuacjach. Jest ona normą, nie prawem, choć wiąże się z prawem międzynarodowym. Przez długi czas ta doktryna była potężnym narzędziem oddziaływania zachodniej społeczności poprzez negocjacje, → sankcje [t. 4] ekonomiczne, przy wsparciu organizacji pozarządowych, państw i instytucji międzynarodowych. Innym przykładem może być, pomijając nawet wydarzenia z sierpnia 2008 r., kiedy sytuacja była nieco inna i Rosja rozpoczęła operację militarną przeciwko Gruzji, → aneksja [t. 1] Krymu i rozmieszczenie wojsk rosyjskich w Ukrainie, przez rosyjskich analityków uznawane za zgodne z zachodnimi koncepcjami „interwencji humanitarnej” i doktryny R2P.

R2P opiera się na 3 larach:

obowiązku każdego państwa do ochrony swojej ludności przed wymienionymi zbrodniami,

zobowiązaniu się społeczności międzynarodowej do pomocy państwom w wypełnianiu swoich obowiązków w tym zakresie,

gotowości państw do kolektywnego działania w ramach zasad Karty Narodów Zjednoczonych, kiedy państwo nie jest w stanie ochronić swojej ludności.

Różne ujęcia R2P odnoszą się do 5 kryteriów wspomagających ocenę legalności ewentualnej interwencji:

kryterium stopnia zagrożenia,

celu – przeciwdziałanie ludzkiemu cierpieniu,

ostateczności – inne możliwe i dostępne pokojowe rozwiązania zawiodły,

proporcjonalności środków – działania wojskowe powinny być ograniczone do minimum koniecznego do osiągnięcia celu,

bilansu skutków – korzyści z interwencji powinny przewyższać skutki zaniechania działania.

R2P jest ważną oraz zyskującą na znaczeniu zasadą, jednak podważa pkt. 7 art. 2 Karty Narodów Zjednoczonych (KNZ). Ów mówi o tym, że żadne postanowienie KNZ nie upoważnia ONZ do ingerencji w sprawy,

które ze swojej istoty należą do kompetencji wewnętrznych któregokolwiek państwa.

Chociaż R2P została przyjęta przez społeczność międzynarodową w 2005 r., wciąż jest słabo rozpoznawalna przez państwa członkowskie ONZ, jeśli chodzi o jej praktyczne zastosowanie. R2P nie jest jeszcze powszechnie akceptowaną zasadą, ale stała się ważną normą, dzięki której Zachód ma nadzieję na zbudowanie globalnej opieki nad naruszeniem praw człowieka. W kontekście prawa międzynarodowego R2P koncentruje się na ochronie ludności, a nie na interwencji w celu zmiany stylu rządzenia suwerennym państwem. Od kiedy norma została wprowadzona do społeczności międzynarodowej, narracja R2P była stosowana przez Radę Bezpieczeństwa ONZ w kilku rezolucjach. Jednak w przypadku interwencji w Libii i Republice Środkowoafrykańskiej R2P była wyraźnie cytowana tylko w odniesieniu do legalnej siły militarnej. R2P należy odróżniać od interwencji humanitarnej, ponieważ interwencja humanitarna jest tylko jedną z dostępnych odpowiedzi związanych z zasadą R2P.

Naukowcy twierdzą, że interwencja humanitarna jest uzasadniona, gdy:

system Rady Bezpieczeństwa ONZ nie działa, a rezolucja jest niedostępna,

trwa kryzys humanitarny związany ze zbrodniami wojennymi, zbrodniami przeciwko ludzkości, ludobójstwem, czystkami etnicznymi, występują dowody skrajnego nieszczęścia humanitarnego wymagającego natychmiastowej pomocy, kryzys humanitarny zakłóca porządek międzynarodowy (art. 51 KNZ – prawo państwa do samoobrony),

używanie siły powinno być dozwolone tylko po to, aby powstrzymać działania niezgodne z prawem i musi być konieczne, proporcjonalne i ukierunkowane na pomoc humanitarną, wyłącznie w celu położenia kresu zbrodniom i przywróceniu praw człowieka,

musi być jasne, że nie ma praktycznej alternatywy poza interwencją, a żadne pokojowe rozwiązanie nie jest możliwe,

żadne państwo nie powinno jednostronnie podejmować działań.

Te starannie przemyślane zasady zawiodły w przypadku → wojny domowej [t. 4] w Syrii. Chociaż w Radzie Bezpieczeństwa ONZ nie osiągnięto konsensusu co do tego, jakie działania należy podjąć, ale

większość zgadza się, że interwencja humanitarna jest uzasadniona faktem, że Baszar Al-Asad użył → broni chemicznej [t. 1] przeciwko swojej ludności. Po drugiej stronie medalu znajduje się Rosja, która dokonała aneksji Krymu, części terytorium innego państwa, twierdząc, że zrobiła to, ponieważ miała „obowiązek ochrony”:

> tych, którzy sprzeciwiają się → „puczowi wojskowemu” [t. 3] Euromajdanu, i tych, którzy byli „zagrożeni represjami”, a także ogólnie mniejszość rosyjskojęzyczną,
> przed nacjonalistami (zob. → nacjonalizm [t. 3]), neonazistami (zob. → neonazim [t. 3]), rusofobami i antysemitami, którzy dokonali nielegalnego i niekonstytucyjnego zamachu stanu i pozostają u władzy,
> ponadto Rosja legitymizowała użycie siły (→ inwazja i aneksja Krymu) za zgodą parlamentu, a prezydent Ukrainy W. Janukowycz i premier Krymu wezwali Rosję do użycia siły militarnej w celu „ochrony ich życia i praw”.

Takie argumenty nie mogły być podstawą ani jednostronnej → secesji [t. 4], ani jednostronnej interwencji humanitarnej. W tym czasie etniczni Rosjanie nie byli zabijani ani prześladowani. Represje, o których mówił W. Putin, nie uzasadniają interwencji Rosji, a interwencja oparta na zainteresowaniach jest współczesną wersją imperializmu.

Putin posunął się za daleko – aneksja, → agresja [t. 1] i interwencja, gdy nie ma kryzysu humanitarnego, są tak samo szkodliwe dla koncepcji R2P, jak brak działania, gdy kryzys humanitarny jest jawnie oczywisty. Jakkolwiek trudna jest równowaga pomiędzy pomocą humanitarną a interesami państwa, ważne jest, aby ludzie nie cierpieli, nie zważając na wszystkie inne czynniki. Wola polityczna (pod wpływem interesów państwa) niestety zwycięża nad względami humanitarnymi i widzimy groteskowe tego przykłady w Ukrainie i Syrii. W Ukrainie rosyjska wola polityczna doprowadziła do interwencji bez legitymizacji, a w Syrii warunki zostały spełnione, lecz nie było woli politycznej (ze strony Rosji i Chin) do działania w obliczu kryzysu. Dlatego dobrze byłoby wziąć pod uwagę – lub przynajmniej nie całkowicie odrzucić – wolę polityczną i interesy państwa w rozważaniu stosowania zasady R2P. Zasadą jest, aby ta doktryna działała niezależnie od interesów państwowych, ale niestety

jest ona i tak napędzana wolą polityczną, która musi być uwzględniana przy każdej ocenie zastosowania tej doktryny, inaczej niezbędna byłaby zmiana praktycznie całej koncepcji. Ukraina i Syria to bardzo dobre przykłady konsekwencji działania i bezczynności.

Rosja była przekonana, że każda interwencja mająca na celu powstrzymanie cierpienia i → przemocy [t. 3] w Syrii musi zostać zatwierdzona przez Radę Bezpieczeństwa. Natomiast w 2014 r., w odpowiedzi na nieznane i niejasne groźby dla ukraińskich Rosjan, Kreml był chętny do jednostronnego odrzucenia suwerenności Ukrainy. Nie było zrozumiałe, w obliczu jakiego zagrożenia znajdowali się Rosjanie z Ukrainy: na Krymie nie było bezpośredniego zagrożenia ludobójstwem, zbrodniami przeciwko ludzkości ani czystkami etnicznymi, których dziś doświadcza naród tatarski. Używanie przez Rosję koncepcji R2P jest tym bardziej niepewne, że większość zagrożeń dla Ukraińców płynie z samej Rosji. Doktryna kategorycznie wyklucza możliwość jej wykorzystania przez jedno państwo przeciwko innemu państwu pod hasłem „ochrony obywateli” przed rzekomymi zagrożeniami, a w celu aneksji obcych terytoriów.

Inwazja na Ukrainę nie dotyczy koncepcji R2P, ponieważ jedynym prawowitym organem, który decyduje o zatwierdzeniu interwencji, jest Rada Bezpieczeństwa ONZ. Interwencja w imię odpowiedzialności za ochronę nie może być jednostronna. Poprzez sprzeniewierzenie i nadużywanie koncepcji R2P w celu usprawiedliwienia interwencji Rosja osłabia samą koncepcję R2P.

Gdy R2P została przywołana przez Radę Bezpieczeństwa ONZ w celu przerwania rozlewu krwi – i uzasadnienia interwencji NATO – w Libii, po upadku reżimu Muhammara al-Kadda ego wspólnota międzynarodowa wykazała, że doktryna jest czymś więcej niż tylko retoryką. R2P powinna być narzędziem, do którego kraje mogą sięgać w tych przypadkach, kiedy trwa prawdziwy kryzys humanitarny, a ONZ lub inna międzynarodowa pomoc humanitarna zawodzi. Koncepcja R2P może pomóc w zapobieganiu → wojnom [t. 4] czy klęskom żywiołowym. Aby chronić integralność tej zasady, państwa muszą przeciwstawić się tym, którzy ją naruszają, jednak należy również uznać, że z samej swej natury R2P jest bardziej narzędziem politycznym.

Wojna rosyjsko-ukraińska udowodniła, jak kruchy jest współczesny pokój i jak szybko może rozpocząć się międzynarodowy kon ikt zbrojny.

A. Eban, słynny izraelski minister spraw zagranicznych, powiedział kiedyś, że „prawo międzynarodowe – to prawo, którego przestępcy nie wykonują, a sprawiedliwi nie zmuszają ich go wykonywać”. Niezaprzeczalne dowody zbrodni masowych w Syrii i agresja Rosji wobec Ukrainy wzmacniają przekonanie, że zbrodniarze nadal ignorują normy prawa międzynarodowego.

Olga Wasiuta, Sergiusz Wasiuta

G.J. Bass, *Freedom's Battle: The Origins of Humanitarian Intervention*, Alfred A. Knopf, New York 2008; A. Domagała, *Interwencja humanitarna w stosunkach międzynarodowych*, Wydawnictwo Branta, Bydgoszcz–Wrocław 2008; G. Evans, *The Responsibility to Protect: Ending Mass Atrocity Crimes Once and For All*, Brookings Institution Press, 2009; F. Francioni, Ch. Bakker, *Responsibility to Protect, Humanitarian Intervention and Human Rights: Lessons from Libya to Mali. The Transatlantic Relationship and the Future Global Governance*, „Working paper” 2013, no. 15; S.F. Gagro, *The Responsibility to Protect (R2P) Doctrine*, „International Journal of Social Sciences” 2014, no. 3 (1); S. De Geest, *Russian Intervention in Ukraine: R2P Limits and reclaiming the Concept and Narrative*, 11.04.2015, HSCentre.org (dostęp 19.02.2019); A. Hehir, *The Responsibility to Protect: Rhetoric, Reality and the Future of Humanitarian Intervention*, Palgrave Macmillan, Basingstoke 2012; Human Rights Watch, *Statement: Possible Intervention Syria, Human Rights Watch*, 28.08.2013, HRW.org (dostęp 15.02.2019); International Commission on Intervention and State Sovereignty *The Responsibility to Protect*, International Development Research Centre (Canada), Ottawa 2001; M. Kersten, *Does Russia have a „Responsibility to Protect” Ukraine? Don't buy it*, 4.03.2014, eGlobe-AndMail.com (dostęp 19.02.2019); A.S. Kolb, *The UN Security Council Members' Responsibility to Protect: A Legal Analysis*, Springer, New York 2017; D. Kuwali, *The Responsibility to Protect: Implementation of Article 4(h). Intervention*, Martinus Nijho Publishers, Leiden–Boston 2011; D. Kuwali, F. Viljoen, *Africa and the Responsibility to Protect: Article 4(h) of the African Union Constitutive Act*, Routledge, New York 2013; M. Martin, M. Kaldor, *The European Union and Human Security: External Interventions and Missions*, Routledge, London 2010; J. Pattison, *Humanitarian Intervention and Responsibility to Protect. Who Should Intervene?* Oxford University Press, Oxford 2012; *Responsibility to Protect: The Global Moral Compact for the 21st Century*, R.H. Cooper, J.V. Kohler (eds.), Palgrave Macmillan, London 2008; Rezolucja RB ONZ nr 1970 z 26 lutego 1970 roku; Rezolucja RB ONZ nr 2127 z 5 grudnia 2013 roku; N. Tsagourias, *Russia, Georgia and the Responsibility to Protect*, „Amsterdam Law Forum” 2019, vol. 1; C.B. Walling, *All the Necessary Measures: The United Nations and Humanitarian Intervention*, University

of Pennsylvania Press, Philadelphia 2013; O. Wasiuta, *Doktryna odpowiedzialności za ochronę*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Doktryna „Responsibility to protect" w praktyce politycznej Rosji*, „Przegląd Geopolityczny" 2019, nr 29; J. Welsh, *Implementing the „Responsibility To Protect"*, „Policy Brief" 2009, no. 1; I. Wrońska, *Zasada odpowiedzialności za ochronę w stosunkach międzynarodowych a działania NATO: uwagi na tle współczesnej koncepcji ochrony praw człowieka*, „Ante Portas. Studia nad Bezpieczeństwem" 2014, nr 1 (3).

Doktryny (koncepcje) operacyjne – zespół poglądów dotyczących przygotowania poszczególnych rodzajów sił zbrojnych do konfrontacji militarnej z potencjalnym przeciwnikiem na określonym obszarze geograficznym. Pojęcie doktryn operacyjnych jest pojęciem węższym niż → doktryna wojskowa i doktryna wojenna. Jak podkreślił J. Solarz w książce *Doktryny militarne w XX wieku*, doktryną militarną będzie sposób przygotowania obrony kraju w sytuacji → zagrożenia [t. 4] zewnętrznego oraz prowadzenie działań wojennych z zastosowaniem metod i środków będących w dyspozycji państwa lub koalicji państw. Doktryną wojenną będzie z kolei zbiór poglądów i idei związanych z przygotowaniem i prowadzeniem → wojny [t. 4] jako całości, z uwzględnieniem takich czynników jak ustrój państwa, sytuacja polityczna (wewnętrzna i międzynarodowa), zasoby kraju, potencjał gospodarczy, poziom naukowo-techniczny, doświadczenia prowadzenia wojny i położenie geograficzne. Doktryny operacyjne zostają opracowane w praktyce przez wyspecjalizowane organy wojska lub organizacje pozarządowe (think tanki zajmujące się naukami strategicznymi lub → naukami o bezpieczeństwie [t. 3]), a następnie, po akceptacji na najwyższych szczeblach dowódczych sił zbrojnych, zostają przedstawione w oficjalnych dokumentach strategicznych lub podręcznikach polowych jako obowiązujące. Przykładem doktryn operacyjnych były 4 koncepcje, jakie pojawiły się w ciągu ostatnich kilkudziesięciu lat w siłach zbrojnych USA:

- koncepcja bitwy powietrzno-lądowej (AirLand Battle, ALB);
- koncepcja bitwy powietrzno-morskiej (AirSea Battle, ASB);
- koncepcja bitwy wielodomenowej (Multi-Domain Battle, MDB);
- koncepcja operacji wieloobszarowej (Multi-Domain Operation, MDO).

Doktryna bitwy powietrzno-lądowej została opracowana w latach 70. XX w. na potrzeby ewentualnej konfrontacji wojsk → NATO [t. 3] z wojskami Układu Warszawskiego na nizinach Europy Środkowej. Pierwszym dokumentem, w którym przedstawione zostały zasady ALB, była broszurka zatytułowana *The AirLand Battle and Corps 86, TRADOC Pamphlet 525-5* z 1981 r. W 1982 r. doktryna ta została opisana w podręczniku polowym *Field Mannual (FM) 100-5 Operations*. Przed pojawieniem się koncepcji bitwy powietrzno-lądowej, w 1976 r., w armii USA została opracowana doktryna aktywnej obrony. Była ona jedną z pierwszych propozycji zmiany doktryny militarnej po tzw. traumie wietnamskiej. Opierała się na doświadczeniach izraelskich wojny Jom Kippur w 1973 r. Zakładała ona „pogłębienie" pola walki, uderzenie na pierwszy rzut armii przeciwnika oraz niszczenie jego kolejnych rzutów za pomocą najnowocześniejszej broni. Jako przykład prowadzenia → bitwy [t. 1] z użyciem metod aktywnej obrony podawane było starcie izraelskich i syryjskich wojsk pod Al-Kunajtirą (Quneitra) w czasie wojny Jom Kippur. 6 października 1973 r. izraelska 7 Brygada Pancerna wyposażona w 100 czołgów stawiła czoło przeważającym siłom wroga i utraciła w ciągu 4 dni większość własnego sprzętu wojskowego. Pomimo strat → żołnierze [t. 4] 7 Brygady, wykorzystując kilkanaście naprawionych czołgów, przypuścili kontratak na pozycje syryjskie, zmuszając syryjskie wojska do odwrotu. Heroiczna postawa żołnierzy 7 Brygady umożliwiła wzmocnienie izraelskich sił na południu i przeprowadzenie przez dywizje gen. Lanera i Peleda 2 głębokich manewrów oskrzydlających. Był to kluczowy moment wojny Jom Kippur na odcinku syryjskim, który uświadomił obserwatorom, jak skuteczne mogą być działania opóźniające oraz niszczące, głęboko w regionie działań przeciwnika, prowadzone za pomocą → wojsk lądowych [t. 4] i sił powietrznych.

Sama koncepcja ALB została opisana w książce *Wojna i antywojna* autorstwa A. i H. To erów. Zdaniem autorów, zgodnie z teorią 3 fal rozwoju cywilizacyjnego (agrarną, przemysłową i informacyjną), jest ona krokiem w kierunku transformacji sił zbrojnych USA z instytucji typu drugiej fali (masowej, zbiurokratyzowanej, hierarchicznego porządku) w kierunku instytucji trzeciej fali (nasyconej nowymi technologiami, elastycznej, sieciowej). Koncepcja ALB zakładała prowadzenie „głębokiej

bitwy", „rozszerzonego pola walki", „izolację pola walki" tak, aby zapobiec posuwaniu się wojska przeciwnika naprzód, zapewnić dostawy zaopatrzenia, dopływ → informacji oraz umożliwić uderzenia oskrzydlające na przeciwnika i walkę na jego tyłach.

Za opracowaniem nowej koncepcji operacyjnej przemawiał również potencjał sił zbrojnych państw Układu Warszawskiego. Dowództwo armii USA zdawało sobie sprawę, iż NATO nie posiada przewagi ilościowej w jednostkach sprzętu wojskowego i ilości dywizji. Ponadto w latach 50. XX w. w Armii Radzieckiej pojawiły się nowe koncepcje operacyjne, przygotowujące tę armię do starcia konwencjonalnego z wojskami NATO w Europie. Jedną z nich była koncepcja Operacyjnych Grup Manewrowych (OGM), tj. jednostek składających się z 2 dywizji czołgów i 4 dywizji zmechanizowanych, przygotowanych do prowadzenia głębokich operacji na terytorium przeciwnika. Prowadzenie przez NATO walki przeciwko przeważającym siłom przeciwnika nie byłoby możliwe bez nowoczesnego uzbrojenia. Dlatego równolegle do zmian w obszarze teorii i doktryn militarnych na przełomie lat 70. i 80. XX w. pojawił się w armii USA szereg jednostek nowego sprzętu wojskowego, określanych jako tzw. wielka piątka – czołgi M1 Abrams, śmigłowce Apache, wozy bojowe Bradley, wieloprowadnicowe wyrzutnie pocisków rakietowych MRLS i samochody HMMWV (wielozadaniowe pojazdy kołowe).

Mimo że doktryna bitwy powietrzno-lądowej została opracowana na przełomie lat 70. i 80. XX wieku na potrzeby ewentualnej konfrontacji wojsk NATO z wojskami Układu Warszawskiego, jej założenia można nadal obserwować we współczesnych konflikach zbrojnych. Jak zauważył M. Gawęda na łamach Defence24.pl, połączone operacje powietrzno-lądowe w duchu ALB prowadziła Rosja w Syrii w 2015 i 2016 r. Polegały one m.in. na współpracy niewielkich oddziałów komandosów z lotnictwem w celu naprowadzenia samolotów na cel, oceny skali zniszczenia, odparcia ataku sił przeciwnika, rażenia przeciwnika na całej głębokości (linia frontu, bliskie zaplecze, dalekie tyły). Przez lata armia rosyjska z powodu „luki technologicznej" w stosunku do państw zachodnich nie była w stanie prowadzić tego typu operacji. Wyposażenie wojska w systemy transmisji danych KRUS Strielec oraz pojawienie się w arsenale rosyjskiej armii bezzałogowych statków latających znacznie zwiększyło

jej możliwości. Skalę i efekty prowadzenia operacji bazującej na zasadach bitwy powietrzno-lądowej przedstawił pod koniec 2017 r. były dowódca wojsk rosyjskich w Syrii gen. S. Surowikin. Jego zdaniem w ciągu 227 dni zlikwidowano ponad 32 tys. terrorystów, zniszczono 394 czołgi oraz wyzwolono spod władzy → Państwa Islamskiego [t. 3] 67 tys. km² powierzchni Syrii.

Kolejna doktryna operacyjna, koncepcja bitwy powietrzno-morskiej, powstała w 2010 r. Wpływowy amerykański think tank Center for Strategic and Budgetary Assessments opublikował wówczas 2 raporty: *Why Air-Sea Battle?* oraz *Air-Sea Battle, a Point of Departure Operational Concept*. W 2012 r. z kolei ukazał się dokument Pentagonu *Joint Operational Access Concept* (JOAC), w którym opisane zostały założenia systemu Anti Access/Area Denial (A2/AD) i koncepcja bitwy powietrzno-morskiej. Obserwując rosnące zdolności Chin w izolowaniu pola walki na zachodnim Pacyfiku, pracownicy Center for Strategic and Budgetary Assessments zaproponowali przyjęcie przez Departament Obrony USA nowej koncepcji operacyjnej, przygotowującej amerykańskie siły zbrojne do konfrontacji militarnej z Chińską Armią Ludowo-Wyzwoleńczą (PLA). O ile w przypadku koncepcji bitwy powietrzno-lądowej miejscem konfrontacji miały być niziny Europy Środkowej, w przypadku koncepcji bitwy powietrzno-morskiej miałby to być zachodni Pacyfik. Głównymi obszarami konfrontacji byłyby morza, powietrze, ale także kosmos i → cyberprzestrzeń [t. 1]. Koncepcja zakłada konieczność obrony amerykańskich sojuszników – Japonii i Korei Południowej – oraz utrzymanie kontroli nad szlakami handlowymi, takimi jak Cieśnina Malakka. Zdaniem autorów dokumentów jednym z pierwszych posunięć strony chińskiej w czasie konfrontacji będzie użycie broni antysatelitarnej i cybernetycznej. W przypadku użycia broni cybernetycznej celem ataku będą amerykańskie systemy C2, radary znajdujące się na zachodnim Pacyfiku, jak również wszystkie naziemne i powietrzne obiekty tworzące obraz świadomości sytuacyjnej. Inną formą ataku będą rakiety mające na celu zniszczenie tzw. sanktuariów, czyli stałych lub rotacyjnych baz amerykańskich na zachodnim Pacyfiku. Do niedawna szereg baz amerykańskich znajdował się poza zasięgiem chińskich samolotów i pocisków balistycznych, jednak obecnie nawet jedna z największych baz amerykańskich na wyspie

Guam nie jest bezpieczna, jako że pociski typu DF-11, DF-15, DF-21 czy DF-4 osiągają dystans od kilkuset do 2500 mil morskich. Szczególnym zagrożeniem dla strony amerykańskiej jest rakieta balistyczna DF-21D, nazywana „zabójcą lotniskowców". DF-21D znacząco zmienia potencjał militarny obu stron w tym obszarze geograficznym, ponieważ naraża na zniszczenie lotniskowce już w pierwszej fazie konfliktu. Atutem po stronie USA jest z kolei dominacja w ilości okrętów podwodnych. Poza tym, jak podkreślają autorzy koncepcji, armia USA w pierwszych dniach bitwy powietrzno-morskiej skupi się na „oślepieniu" dowództw chińskiej armii w ramach „nowoczesnej bitwy zwiadowczej", niszcząc satelity oraz radary przeciwnika. Następnie, po zwycięskim starciu lotniczym nad Japonią, skupi się na eliminacji potencjału chińskiej floty, aby później przystąpić do blokady morskiej Państwa Środka.

W 2017 r. została przedstawiona kolejna koncepcja – → bitwa wieloobszarowa [t. 1] (Multi-Domain Battle). Jej założenia zostały opisane w dokumencie *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040* wydanym przez U.S. Army Training and Doctrine Command (TRADOC). Jak podkreślił były dowódca TRADOC gen. D. Perkins, konieczność opracowania doktryny bitwy wielodomenowej wynikała z kilku przyczyn. Po pierwsze, w przeciwieństwie do czasów → zimnej wojny [t. 4] i obowiązującej wówczas koncepcji bitwy powietrzno-lądowej, armia USA musi być przygotowana do konfrontacji nie z jednym, ale z kilkoma rodzajami przeciwników: mocarstwami międzynarodowymi, państwami upadłymi, ugrupowaniami terrorystycznymi itp. Po drugie, w latach 90. XX w. żaden z przeciwników nie był w stanie zagrozić USA w ani jednym obszarze (domenie) prowadzenia działań zbrojnych – na lądzie, w powietrzu, na morzu, w przestrzeni kosmicznej czy cyberprzestrzeni. USA posiadały wówczas niekwestionowaną przewagę w siłach powietrznych i → marynarce wojennej [t. 3]. Jedynym kwestionowanym obszarem dominacji Ameryki był ląd, gdzie za pomocą asymetrycznych metod prowadzenia walki nawet słabszy przeciwnik mógł zadać wojskom konwencjonalnym duże straty. Obecnie, biorąc pod uwagę zdolności chińskie na zachodnim Pacyfiku oraz możliwości armii rosyjskiej w wojnie na Ukrainie i wojnie w Syrii, należy się spodziewać, iż w przyszłych konfliktach zbrojnych dominacja amerykańska będzie

kwestionowana na wszystkich obszarach (domenach). Po trzecie, Stany Zjednoczone, aby wciąż posiadać status globalnego mocarstwa, muszą utrzymywać siły zbrojne w różnych odległych od siebie miejscach świata, narażając je tym samym w czasie ewentualnego konfliktu na odcięcie linii zaopatrzeniowych. Skutkuje to koniecznością przygotowania sił do operowania w warunkach dużej samodzielności, wystarczalności i zdolności prowadzenia operacji na wszystkich obszarach (domenach). Bitwa wielodomenowa zakłada tym samym powstanie nowych oddziałów, nazywanych oddziałami ICEW (ang. *intelligence, cyberwarfare and electronic warfare*), zdolnych prowadzić operacje w kilku obszarach jednocześnie. Na większą samodzielność wojska będą miały wpływ również nowe technologie medyczne, umożliwiające pomoc rannym na polu walki czy zastosowanie nowych części zamiennych do sprzętu wojskowego.

Najnowszą doktryną operacyjną rozwijaną w siłach zbrojnych USA jest koncepcja operacji wieloobszarowej. Jak podkreślił gen. E. Wesley, dyrektor U.S. Army Capabilities Integration Center (ARCIC), koncepcja operacji wieloobszarowej jest rozbudowaną wersją MDB. Zawiera o wiele więcej szczegółów opisujących to, jak powinny być prowadzone operacje w wielu domenach, weryfikowana jest ona także w cyklicznych ćwiczeniach wojskowych odbywających się w różnych miejscach na świecie, takich jak Joint Warfighting Assessment 18 w Niemczech czy Joint Warfighting Assessment19 na Pacyfiku. TRADOC definiuje MDO jako metodę, za pomocą której siły zbrojne USA, będące częścią sił sojuszniczych, mogą powstrzymać i pokonać przeciwnika posiadającego zdolności kwestionujące dominację amerykańską we wszystkich obszarach (domenach) prowadzenia walki zbrojnej. Podobnie jak MBD, MDO wskazuje jako potencjalnego przeciwnika siły zbrojne Federacji Rosyjskiej i Chińskiej Republiki Ludowej oraz innych państw rozwijających zdolności antydostępowe (→ antydostępowe zdolności [t. 1]) (Iran, Korea Północna). Szczegóły koncepcji operacji wieloobszarowej przedstawione zostały w dokumencie TRADOC *The U.S. Army in Multi-Domain Operations 2028*, który ukazał się w 2018 r. Zdaniem autorów w przyszłości wojny prowadzone będą przez niewielkie siły zbrojne na dużych przestrzeniach. Ponadto, biorąc pod uwagę postępujące procesy urbanizacyjne, walka będzie się odbywać w terenie miejskim, gdzie przeciwnicy USA będą starali

się wykorzystać otoczenie do zminimalizowania przewagi amerykańskiej. Koncepcja dzieli aktywność wojskową na okres rywalizacji, okres walki zbrojnej oraz powrót do rywalizacji po zakończeniu konfliktu. W okresie rywalizacji podejmowane są działania dyplomatyczne i ekonomiczne, prowadzona jest → wojna informacyjna [t. 4] i działania nieregularne. Bardzo trudno jest określić, kiedy rywalizacja przechodzi w okres wojny, ponieważ → agresja [t. 1] ma charakter podprogowy (poniżej progu wojny). Walka zbrojna charakteryzuje się prowadzeniem operacji we wszystkich 5 domenach (lądowej, powietrznej, morskiej, kosmicznej i cyberprzestrzeni) na 7 obszarach:

- na strategicznym obszarze wsparcia położonym powyżej 5 tys. km poza miejscem prowadzonych walk,
- na operacyjnym obszarze wsparcia położonym powyżej 1,5 tys. km od miejsca prowadzonych walk,
- na taktycznym obszarze wsparcia położonym powyżej 500 km od miejsca prowadzonych walk,
- na bliskim obszarze i głębokim obszarze manewru położonym do 200 km od miejsca prowadzonych walk, zarówno w kierunku terytorium sojusznika, jak i wroga,
- na operacyjnym głębokim obszarze prowadzenia walk,
- na strategicznym głębokim obszarze prowadzenia walk położonych powyżej 500 km i 1 tys. km na terenie przeciwnika.

Zadaniem sił zbrojnych jest przełamanie zdolności antydostępowych wroga, uzyskanie swobody manewru, pokonanie jego sił zbrojnych, a następnie powrót do okresu rywalizacji.

Tomasz Wójtowicz

J. Bartosiak, *Pacyfik i Euroazja. O wojnie*, Jacek Bartosiak, Warszawa 2016; M. Gawęda, *Bitwa powietrzno-lądowa po rosyjsku. Przykład Syrii*, 11.02.2018, Defence24.pl (dostęp 22.12.2019); J. Judson, *From Multi-Domain Battle to Multi-Domain Operations: Army evolves its guiding concept*, 9.10.2018, DefenseNews.com (dostęp 20.12.2019); Ł. Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009; A.F. Krepinevich, *Why Air-Sea Battle?*, Center for Strategic and Budgetary Assessments, Washington 2010; A.H. Toffler, *Wojna*

i antywojna. Jak przetrwać na progu XXI wieku, Wydawnictwo Kurpisz S.A., Poznań 2006; J. van Tol, M. Gunzinger, A. Krepinevich, J. omas, *AirSea Battle. A Point-of-Departure Operational Concept*, Center for Strategic and Budgetary Assessments, Washington 2010; United States Army Training and Doctrine Command, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040*, United States Army Training and Doctrine Command, 2017; ciż, *e U.S. Army in Multi-Domain Operations 2028*, United States Army Training and Doctrine Command, 2018; U.S. Army Training and Doctrine Command's Joint Modernization Command, *Joint War ghting Assessment 18*, 24.04.2018, Army.mil (dostęp 22.12.2019); K. Weinberger, *Russian Anti-Access and Area Denial*, 29.08.2016, UnderstandingWar.org (dostęp 22.12.2019); T. Wójtowicz, *Doktryny operacyjne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

Doktryny obronne RP – zbiór poglądów na → zagrożenie militarne [t. 4] kraju oraz zasad i wytycznych dotyczących przygotowania państwa, sił zbrojnych i społeczeństwa do prowadzenia → wojny [t. 4], wyrażających się w konkretnych przedsięwzięciach o charakterze militarnym i pozamilitarnym, realizowanych w czasie pokoju i ewentualnej wojny. Analizując doktryny obronne, należy jasno zaznaczyć, iż termin ten w polskich realiach zadomowił się na dobre po 1989 r., wcześniej, w czasach PRL, wydawano (głównie przez Sztab Generalny Wojska Polskiego, SGWP) dokumenty doktrynalne odnoszące się do powyższych zagadnień, lecz określano je częściej mianem doktryn wojennych. Owe doktryny we wspomnianym okresie były pod względem polityczno-ideologicznym tożsame z doktryną Układu Warszawskiego. Od 1967 r. wiele elementów doktryny wojennej można było odczytać z ustawy o powszechnym obowiązku obrony Polskiej Rzeczypospolitej Ludowej, będącej swoistą konstytucją obronności. W latach 60. XX w. ukształtowała się koncepcja organizacji systemu obronnego państwa na podstawie 3 układów:

- militarny (WP),
- funkcjonalny (resorty cywilne pogrupowane w szereg działów, np. polityczny, planowania i ekonomiki, → ochrony ludności [t. 3], komunikacji itp.),
- terytorialny (odpowiedniki działów układu funkcjonalnego na szczeblu województwa i powiatu).

Taka doktryna obronna (wojenna) z pewnymi modyfikacjami przetrwała aż do 1990 r. Zmiany polityczno-społeczne, które dokonały się w Polsce po 1989 r., niejako wymusiły nowe podejście do obronności państwa. Głównym wyzwaniem w pierwszej fazie było zerwanie z mentalnością „operatora", czyli wykonawcy zadań strategicznych przychodzących z zewnątrz, i zainicjowanie kreatywnej narodowej → kultury strategicznej, opartej na identyfikacji i uwzględnianiu własnych → interesów narodowych. Tak zrodziła się pierwsza doktryna obronna RP z 1990 r. Jak przyjęto w uchwale Komitetu Obrony Kraju (KOK), doktryna wytyczała generalne kierunki polityki obronnej obowiązujące organy państwowe, podmioty gospodarcze, organizacje społeczne i zawodowe oraz każdego obywatela. W myśl przedmiotowej doktryny polityka obronna została zdefiniowana jako podejmowanie działań na rzecz zapewnienia → bezpieczeństwa militarnego [t. 1] przy użyciu wszelkich dostępnych środków. System obrony państwa obejmował dziedzinę polityczno-społeczną, administracyjno-gospodarczą, militarną, ochrony państwa oraz → obronę cywilną [t. 3]. Treść doktryny utożsamiała → bezpieczeństwo narodowe [t. 1] z dziedziną obronną, a wspomniany i użyty w zapisach doktryny system obrony państwa stanowił główne narzędzie zapewnienia bezpieczeństwa narodowego. Nie należy się dziwić takiemu podejściu, biorąc pod uwagę istnienie jeszcze w tamtym okresie Układu Warszawskiego, RWPG, ZSRR i stacjonowania w Polsce Armii Radzieckiej. Kolejny dokument tego rodzaju pod nazwą Polityki Bezpieczeństwa i Strategii Obronnej RP został przyjęty w 1992 r. Co do podstawowych założeń nie różnił on się zbytnio od przyjętego 2 lata wcześniej. Nadal dominującą rolę w → systemie bezpieczeństwa narodowego [t. 4] odgrywał system obrony państwa, do tego stopnia, iż nawet kwestie ochrony ludności przed → katastrofami naturalnymi czy przemysłowymi przypisano podmiotom określonym jako pozamilitarne ogniwa obronne. Na kolejne tego typu opracowanie czekano 8 lat. W 2000 r. w ślad za przyjętą Strategią Bezpieczeństwa RP utworzono Strategię Obronności RP. Dokument ten nie okazał się rewolucyjny czy przełomowy. Warto jednak podkreślić, że dostrzeżono w nim → zagrożenia [t. 4] pozamilitarne, w reagowaniu na które państwo byłoby zmuszone zaangażować swój potencjał obronny. Kolejny tego typu dokument

ujrzał światło dzienne w 2009 r., czyli 2 lata po ukazaniu się → strategii bezpieczeństwa narodowego [t. 4]. Strategia Obronności RP, bo taki tytuł otrzymało to opracowanie, była niczym innym jak → strategią [t. 4] sektorową do tej pierwszej. W dokumencie obronność zdefiniowano jako dziedzinę bezpieczeństwa narodowego, stanowiącą sumę wszystkich cywilnych i wojskowych przedsięwzięć, mających na celu zapobieganie i przeciwstawianie się wszelkim potencjalnym → zagrożeniom bezpieczeństwa [t. 4] państwa, zarówno militarnym, jak i pozamilitarnym, mogącym doprowadzić do → kryzysu polityczno-militarnego. Innymi słowy, aby zapewnić zdolność do obrony, powinno się wykorzystywać wszystkie możliwe środki i podporządkować jej działania polityczne, gospodarcze, dyplomatyczne i wojskowe.

Z dokumentów doktrynalnych, a zwłaszcza tych z XXI w., wyłania się obraz → obrony narodowej [t. 3] jako jednego z podstawowych, elementarnych ogniw bezpieczeństwa narodowego, którą należy rozpatrywać o wiele szerzej aniżeli w aspekcie czysto militarnym.

Łukasz Szewczyk

W. Kitler, *Bezpieczeństwo Narodowe. Podstawowe kategorie. Uwarunkowania. System*, AON, Warszawa 2011; *Strategia Obronna RP*, MON, Warszawa 2000; *Strategia Obronności Rzeczypospolitej Polskiej*, Warszawa 2009; Uchwała Komitetu Obrony Kraju z dnia 21 lutego 1990 r. w sprawie doktryny obronnej Rzeczypospolitej Polskiej, M.P. 1990 nr 9, poz. 66; J. Wojnarowski, *System obronności państwa*, AON, Warszawa 2005; Z. Wilk-Woś, P. Kornacki, *Bezpieczeństwo i zarządzanie kryzysowe – bezpieczeństwo i obronność państwa*, Wydawnictwo Społecznej Akademii Nauk, Warszawa–Łódź 2016.

Dokument z Montreux (dokument z Montreux w sprawie istotnych międzynarodowych zobowiązań prawnych i dobrych praktyk państw związanych z operacjami prywatnych firm wojskowych i ochroniarskich w trakcie konfliktu zbrojnego z dnia 17 września 2008 r.) – pierwszy dokument o znaczeniu międzynarodowym, który określa, w jaki sposób prawo międzynarodowe stosuje się do działalności prywatnych firm wojskowych i ochroniarskich (ang. *private military and security companies*, PMSC), gdy działają one w strefie konfliktu zbrojnego. Przepisy zawarte w dokumencie

określają również obowiązki prawne spoczywające na samych prywatnych rmach ochroniarskich.

Dokument z Montreux jest wynikiem inicjatywy podjętej wspólnie przez Szwajcarię i Międzynarodowy Komitet Czerwonego Krzyża przy udziale ekspertów rządowych m.in. z Afganistanu, Angoli, Australii, Austrii, Kanady, Chin, Francji, Niemiec, Iraku, Polski, Szwajcarii, Wielkiej Brytanii, Ukrainy i USA. Prace prowadzone w latach 2006–2007 zaowocowały sformułowaniem treści tzw. dokumentu z Montreux. Opracowano go na podstawie wyników 4 spotkań międzyrządowych:

Federalny Departament Spraw Zagranicznych – departament odpowiadający za prowadzenie polityki zagranicznej Szwajcarii – zorganizował pierwsze spotkanie rozpoznawcze w Zurychu w dniach 16–17 stycznia 2006 r., na którym zgromadzili się eksperci rządowi oraz przedstawiciele branż związanych z sektorem → bezpieczeństwa [t. 1], a także przedstawiciele organizacji działających na rzecz → społeczeństwa obywatelskiego [t. 4];

drugie spotkanie o podobnej tematyce odbyło się w Montreux w dniach 13–14 listopada 2006 r. i zostało poświęcone omówieniu dobrych praktyk, które powinny być stosowane przez państwa: zawierające umowy z PMSC, na których terytorium działają PMSC oraz których obywatele działają w PMSC;

trzecie spotkanie w dniach 14–16 kwietnia 2008 r. posłużyło konsolidacji opinii szerszego kręgu ekspertów rządowych, przedstawicieli organizacji działających na rzecz → praw człowieka [t. 3] i przedstawicieli branży na temat pierwszego projektu. Na podstawie tych dyskusji projekt został zmieniony i przekazany uczestniczącym w spotkaniach rządom do ostatecznych konsultacji;

na czwartym (i końcowym) spotkaniu w sprawie inicjatywy w dniach 15–17 września 2008 r. prace nad dokumentem zostały s nalizowane, a rządy uczestniczące przyjęły go w drodze konsensusu.

W październiku 2008 r. Stały Przedstawiciel Szwajcarii przy Organizacji Narodów Zjednoczonych przedstawił dokument Montreux Zgromadzeniu Ogólnemu i Radzie Bezpieczeństwa ONZ. Dokument

i towarzyszący mu list zostały przetłumaczone na 6 oficjalnych języków ONZ: angielski, arabski, chiński, francuski, hiszpański i rosyjski.

Dokument z Montreux określa obowiązki 3 głównych typów państw: 1. państw, które zatrudniają PMSC; 2. państw, na terytorium których działają PMSC, oraz 3. państw, w których zlokalizowane są siedziby PMSC. Chociaż dokument jest skierowany przede wszystkim do państw, dobre praktyki mogą być przydatne dla innych podmiotów, takich jak organizacje międzynarodowe, organizacje społeczne, firmy, które zawierają umowy z PMSC i same PMSC.

Przed przyjęciem dokumentu z Montreux panowało błędne przekonanie, że PMSC działają w próżni prawnej, albowiem nie można stosować względem nich reguł prawa międzynarodowego. Dokument ma praktyczne, realne znaczenie dla promowania poszanowania międzynarodowego prawa humanitarnego (MPH) i międzynarodowego prawa dotyczącego praw człowieka, a także zapewnia rządom plan skutecznego regulowania funkcjonowania PMSC. Zawiera on listę rekomendacji oraz dobrych praktyk, które państwa ratyfikujące dokument powinny implementować do swojego porządku prawnego. Do najważniejszych można zaliczyć następujące zasady:

> ugruntowane zasady prawa międzynarodowego mają zastosowanie do państw w ich relacjach z prywatnymi firmami wojskowymi i ochroniarskimi (PMSC);
>
> dokument zawiera katalog dobrych praktyk w zakresie promowania zgodności z MPH i prawami człowieka podczas konfliktu zbrojnego, które powinny być stosowane przez wszystkie państwa;
>
> dokument nie jest prawnie wiążącym instrumentem i nie wpływa na istniejące zobowiązania państw wynikające ze zwyczajowego prawa międzynarodowego lub umów międzynarodowych, których są stronami, w szczególności ich zobowiązania wynikające z Karty Narodów Zjednoczonych.

Dokument akcentuje obowiązki państw wynikające z prawa międzynarodowego, w szczególności MPH i międzynarodowego prawa dotyczącego praw człowieka, odnoszące się do działalności prywatnych firm wojskowych i ochroniarskich (PMSC) w sytuacjach konfliktu zbrojnego. Katalog dobrych praktyk i opcji regulacyjnych ma stanowić zbiór

praktycznych narzędzi, gotowych do zastosowania przez poszczególne państwa. Sprecyzowanie zagadnień dotychczas nieuregulowanych posłuży promowaniu poszanowania międzynarodowego prawa humanitarnego przez PMSC. Do chwili obecnej 54 państwa i 3 organizacje międzynarodowe poparły dokument z Montreux. Dokument zawiera 27 „oświadczeń" – fragmentów poświęconych różnym tematom, stanowiących przypomnienie głównych międzynarodowych zobowiązań prawnych państw w odniesieniu do operacji PMSC podczas kon iktów zbrojnych. Każde oświadczenie jest potwierdzeniem ogólnej zasady MPH, prawa międzynarodowego dotyczącego praw człowieka lub odpowiedzialności państwa, sformułowanym w sposób wyjaśniający ich zastosowanie w operacjach PMSC. Chociaż dokument został opracowany z myślą o tym, że PMSC działają w sytuacjach kon iktu zbrojnego, będzie mieć również znaczenie w sytuacjach pokon iktowych i innych porównywalnych z kon iktem zbrojnym.

Dokument został podzielony na 2 części: 1. istotne międzynarodowe zobowiązania prawne dotyczące PMSC i 2. dobre praktyki dotyczące PMSC.

W pierwszej części przedstawiono obowiązki różnych podmiotów wynikające z międzynarodowego prawa humanitarnego i prawa międzynarodowego dotyczącego praw człowieka, przypomniane zostały również istotne zobowiązania prawne państw dotyczące PMSC. Obowiązki PMSC i ich personelu oraz odpowiedzialność przełożonych są również omówione w części pierwszej.

W drugiej części przedstawiono ok. 70 „najlepszych praktyk", które mają na celu zapewnienie wskazówek i pomocy państwom w regulowaniu działalności PMSC. Dobre praktyki służą ustaleniu, jakie usługi mogą być zlecane PMSC, a które wymagają odpowiedniego szkolenia, ustalania warunków udzielania licencji oraz przyjmowania środków w celu poprawy nadzoru, przejrzystości i rozliczalności PMSC.

We współczesnych kon iktach zbrojnych udział prywatnych rm wojskowych stał się coraz powszechniejszy. Początków nowożytnego najemnictwa należy szukać w okresie po II wojnie światowej. Wówczas setki byłych → ż o ł n i e r z y [t. 4] próbowały szczęścia, walcząc w różnych wojnach w Afryce. W późniejszym czasie, obok klasycznych najemników,

zaczęły działać coraz liczniejsze prywatne firmy ochroniarskie, których status w świetle prawa międzynarodowego był niejasny. Przełomowym wydarzeniem dla rozwoju tego rodzaju przedsięwzięć był konflikt w Iraku. Amerykańscy przywódcy liczyli na to, że uda im się przeprowadzić wojnę nowego typu, posługując się w tym celu znaczną liczbą prywatnych firm, które miały przejąć klasyczne zadania wojskowe takie jak → wywiad [t. 4] czy logistyka. Najbardziej znanym podmiotem prywatnym spośród działających w Iraku była Blackwater USA, występująca także pod nazwami Blackwater Worldwide, Xe Services LLC, obecnie Academi. Choć brak oficjalnych danych, szacuje się, że w samym Iraku działały tysiące najemników i rynek ich usług jest wyceniany w miliardach dolarów. Jednak rozwój rynku usług tego rodzaju, choć postrzegany pozytywnie przez państwa, rządy i samych przedsiębiorców, przyniósł szereg ważnych pytań dotyczących odpowiedzialności za działania w ramach konfliktu zbrojnego podmiotów niebędących państwami, których sytuacja nie została wprost uregulowana w aktach prawa międzynarodowego. Wątpliwości te stawały się obiektem zainteresowania → opinii publicznej [t. 3] po każdym nagłośnionym przez media incydencie, a tylko sam konflikt iracki przyniósł ich wiele, by wymienić np. zabicie przez najemników 17 Irakijczyków w Bagdadzie, we wrześniu 2007 r. Wydarzenia te unaoczniły społeczności międzynarodowej, jak wielkie → zagrożenie [t. 4] może wynikać z działania PMSC poza prawem lub na granicy prawa, i doprowadziły do szeregu inicjatyw mających na celu uregulowanie ich działalności.

Dokument z Montreux stanowi uzupełnienie projektu konwencji ONZ ws. PMSC (Draft International Convention On the Regulation, Oversight And Monitoring Of Private Military And Security Companies). Projekt konwencji proponuje wprowadzenie zakazu delegowania określonych uprawnień państw na podmioty prywatne, co ma dotyczyć w szczególności monopolu państwa na możliwość użycia siły w stosunkach międzynarodowych, którą należy rozumieć jako:

bezpośredni udział w działaniach zbrojnych,
prowadzenie wojny i operacji obejmujących walkę,
branie jeńców,
wywiad,
transfer → informacji wywiadowczych,

użycie i działania powiązane z użyciem → broni masowego rażenia,
działania o charakterze policyjnym, w tym aresztowanie, przetrzymywanie i przesłuchiwanie zatrzymanych (art. 2 ppkt. i) projektu konwencji).

Konwencja zakłada także, że każde państwo ponosi odpowiedzialność z tytułu działalności firm zarejestrowanych na terytorium danego państwa niezależnie od tego, czy dana firma działa na rzecz interesów tego państwa. Ponadto konwencja zakłada, że każde państwo powinno podjąć wszelkie konieczne kroki prawne w celu doprowadzenia do odpowiedzialności personelu takich firm z tytułu naruszenia prawa międzynarodowego lub krajowego.

W grudniu 2014 r. zostało utworzone Forum Dokumentu z Montreux (Montreux Document Forum) jako platforma, za pomocą której sygnatariusze i uczestnicy mogą dzielić się wskazówkami dot. dobrych praktyk w postępowaniu wobec PMSC i omawiać wyzwania dotyczące regulacji prywatnych firm wojskowych. Opracowano także uzupełniający globalny kodeks postępowania dla branży bezpieczeństwa.

Piotr Łubiński, Olga Wasiuta

S. Borelli, *Casting Light on the Legal Black Hole: International Law and Detentions Abroad in the War on Terror*, „International Review of the Red Cross" 2005, vol. 87; J. Cockayne, *Regulating Private Military and Security Companies: The Content, Negotiation, Weaknesses and Promise of the Montreux Document*, „Journal of Conflict and Security Law" 2008, vol. 13, iss. 3; P. Łubiński, *Status kombatanta, ochrona i uprawnienia jeńców wojennych i innych osób zatrzymanych*, [w:] *Międzynarodowe prawo humanitarne konfliktów zbrojnych. Materiał szkoleniowy dla oficerów* Z. Falkowski (red.), Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014; M. Maxwell, M. Watts, *Unlawful Enemy Combatant: Status, Theory of Culpability, or Neither*?, „Journal of International Criminal Justice" 2007, vol. 5; D. Moeckli, *The US Supreme Court's 'enemy combatant' decisions: a 'major victory for the rule of law'?*, „Journal of Conflict and Security Law" 2005, vol. 10, iss. 1; *Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict: Montreux 17 September 2008*, „Journal of Conflict and Security Law" 2008, vol. 13, iss. 3; Report of the Working Group on the use of mercenaries

as a means of violating human rights and impeding the exercise of the right of peoples to self-determination (A/HRC/15/25), 2.07.2010; *e Montreux Document: On pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed con ict*, International Committee of the Red Cross, 2009.

Doubleswitch – nowa forma przejęcia kontroli nad kontami w por - talach społecznościowych, wykorzystywana bardzo często w odniesieniu do kont w serwisie Twitter, ale możliwa do zastosowania także do kont na Facebooku i Instagramie. Jej specy ka polega na tym, że atak czyni stan dardowe mechanizmy odzyskiwania konta bezużytecznymi, co pozwala napastnikowi utrzymać kontrolę nad kontem o ary przez dłuższy czas. Nowa forma ataku uwypukla nieprzewidziane luki w zasadach działania i funkcjach kont na Twitterze i w innych → m e d i a c h s p o ł e c z n o ś c i o w y c h [t. 3], powinna stanowić ostrzeżenie dla osób korzystających z tych platform. Użytkownicy zagrożeni takimi atakami powinni stosować uwierzytelnianie wieloetapowe, aby w pierwszej kolejności zapobiec przejęciu kontroli nad kontem przez osoby niepowołane, zaś sam Twitter i platformy mediów społecznościowych z podobnymi funkcjami konta, takie jak Facebook i Instagram, powinny aktualizować swoje zabezpie czenia pod kątem ataków typu Doubleswitch.

Atak Doubleswitch polega na przejęciu konta w portalu społecznościowym w kilku krokach. Najbardziej narażeni na niego są użytkownicy, którzy nie włączyli dla swoich kont opcji uwierzytelniania wieloetapowego. Osoba atakująca może nakłonić użytkownika do ujawnienia hasła za pomocą → p h i s h i n g u [t. 3]. Brak uwierzytelnienia wieloetapowego sprawia, że niewymagane jest kolejne działanie, by przejąć konto. Następnie możliwe staje się wysyłanie wiadomości, ale także subtelne zmienianie → i n f o r m a c j i o koncie, w tym nazwy użytkownika. Oryginalna nazwa użytkownika dla tego konta staje się wówczas dostępna, co pozwala zainteresowanemu zarejestrować konto przy użyciu oryginalnej nazwy użytkownika, dysponując jednocześnie innymi danymi do logowania. Jeśli wówczas o ara spróbuje odzyskać oryginalne konto poprzez zre setowanie hasła, wiadomość e-mail związana z tą procedurą zostanie wysłana bezpośrednio do atakującego. Taka forma przejmowania kont

ma poważne konsekwencje zwłaszcza w przypadku działaczy na rzecz → praw człowieka [t. 3], dziennikarzy lub osób, dla których ważna jest możliwość komunikowania się ze swoimi zwolennikami. Atakujący może wykorzystywać konto i wpływy swojej o ary, a także niszczyć jej reputację. Niektóre o ary ataku mogą nigdy nie odzyskać swojego konta, a nawet kiedy jest to możliwe, muszą poświęcić na to sporo czasu i wysiłku.

Znaczenie przejmowania kont społecznościowych przy wykorzystaniu techniki Doubleswitch wynika z faktu, że działacze polityczni, biznesmeni, dziennikarze i aktywiści na całym świecie wykorzystują platformy mediów społecznościowych, aby komunikować się z otoczeniem. Rządzący w re presyjnych → reżimach [t. 3] politycznych czy zwykli przeciwnicy lub konkurenci czynią konta społecznościowe takich osób celami ataku. Zdobywając kontrolę nad kontami społecznościowymi, mogą uniemożliwić lub utrudnić o erze komunikację, zawstydzić jej zwolenników, a także wywołać niepewność i szerzyć → dezinformację. Efekty takich działań można złagodzić za pomocą zautomatyzowanych procesów odzyskiwania kont opracowywanych przez samą platformę mediów społecznościowych, przy użyciu takich narzędzi jak formularze online do zgłaszania nieprawidłowości. Ataki typu Doubleswitch ewoluują i są coraz trudniejsze do zastosowania. Są szczególnie popularne w Wenezueli, Bahrajnie i Mjanmie. Aktywiści działający na rzecz demokracji i praw człowieka, którzy próbują odzyskać swoje konta w mediach społecznościowych za pomocą standardowych procesów odzyskiwania kont, często przez wiele miesięcy pozostają zablokowani. Za sprawą omawianej formy przejęcia konta o ary nie tylko tracą kontrolę nad kontami w mediach społecznościowych, ale także trudniej im je odzyskać, a w wielu przypadkach nigdy ich już nie odzyskują.

Infolinia Digital Security przedsiębiorstwa Access Now, która pomaga osobom prywatnym i rmom na całym świecie w zakresie → bezpieczeństwa w sieci [t. 1], zidenty kowała tę nową formę ataku poprzez pracę wspierającą aktywistów w Wenezueli, gdy kraj przechodził okres głębokich niepokojów politycznych. W tym okresie obowiązywał dekret prezydenta zezwalający na nadzór i → cenzurę [t. 1] online. 9 stycznia 2017 r. infolinia Digital Security otrzymała prośbę o pomoc od znanej dziennikarki M. Socorro, która poinformowała, że jej konto na Twitterze zostało przejęte. Miesiąc później zgłoszony został drugi wniosek o pomoc

od M. Pizarro, obrońcy praw człowieka i członka parlamentu Wenezueli. Wówczas pracownicy Access Now – firmy, która regularnie zajmuje się odzyskiwaniem kont mediów społecznościowych dla swoich klientów działających na rzecz → społeczeństwa obywatelskiego [t. 4] – zorientowali się, że nowe ataki były inne. W każdym przypadku atakujący uzyskiwali dostęp do konta na Twitterze ofiary, przy czym nie jest jasne, w jaki sposób. Następnie atakujący aktualizowali informacje o koncie, zmieniając hasło i powiązany adres e-mail, w efekcie blokując dostęp legalnego użytkownika do konta. W pierwszym przypadku porywacze zmienili nazwę użytkownika kont z @MilagrosSocorro na @DESAMORTOOT, a konto @Miguel_Pizarro na @PizarroPSUV, a następnie na @BuscoAsao. Po uzyskaniu pełnej kontroli nad zaatakowanym kontem wykorzystano funkcję, która pozwala Twitterowi nadawać po raz kolejny nieużywane nazwy użytkowników. Po zmianach atakujący zarejestrowali konta na Twitterze przy użyciu oryginalnych nazw użytkowników, które były teraz swobodnie dostępne, i podłączali konta do nowego adresu e-mail. Byli wtedy w stanie podszyć się pod Socorro i Pizarro. Gdy ofiary próbowały odzyskać swoje konta, wiadomości e-mail z potwierdzeniem na Twitterze trafiły do atakujących, którzy udawali, że problem został rozwiązany. Następnie atakujący usunęli jedno z oryginalnych kont, co jeszcze bardziej utrudniło ofierze jego odzyskanie. Pracownicy Twittera ściśle współpracowali z ofiarami, aby pomóc w przywróceniu kont, i ostatecznie udało się odnieść sukces. Niestety, atakujący zdążyli już rozpowszechnić fałszywe informacje przy użyciu przejętych kont, a także usuwać prawdziwe tweety.

Doubleswitch jest działaniem, którego sprawca może trwale zablokować lub wydłużyć okres, w którym kontroluje konto w serwisie społecznościowym, zmieniając nazwę użytkownika, a następnie usuwając oryginalne konto. Atak Doubleswitch myli potencjalnych obserwujących (followersów) i sprawia, że standardowe mechanizmy odzyskiwania są nieskuteczne. Platformy mediów społecznościowych zazwyczaj nie powiadamiają użytkowników o zmianach w nazwach użytkowników. Metodę można stosować także w innych serwisach społecznościowych, w tym na Facebooku i Instagramie.

Jakub Idzik, Rafał Klepka

A new social media attack called „Doubleswitch", 10.06.2017, LatestHackingNews.com (dostęp 20.01.2020); A.J. Dellinger, *DoubleSwitch Twitter Hack: New Attack Targets Activists On Twitter*, 6.09.2017, IBITimes.com (dostęp 20.01.2020); J. Idzik, R. Klepka, *Doubleswitch*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; G. Masters, *„Doubleswitch" targeting activists via social media, Access Now report* 20.06.2017, SCMagazine.com (dostęp 20.01.2020); *e „Doubleswitch" social media attack: a threat to advocates in Venezuela and worldwide*, 9.06.2017, AccessNow.org (dostęp 20.01.2020); Q. Wong, *Twitter hack: Activists and journalists targeted in 'Doubleswitch' social media attack*, 9.06.2017, SiliconBeat.com (dostęp 30.04.2019).

Dowództwo Europejskie Stanów Zjednoczonych (United States European Command, USEUCOM) – jest jednym z 11 połączonych dowództw Departamentu Obrony USA stacjonujących w Stuttgarcie (Niemcy), który odgrywa również rolę dowództwa operacyjnego → NATO [t. 3].

Prezydent H.S. Truman 14 grudnia 1946 r. zatwierdził pierwszy ujednolicony plan dowodzenia dla sił amerykańskich. Zunifikowana struktura dowodzenia zrodziła się w 1949 r. Pojawiły się pytania dotyczące zaangażowania USA w obronę Europy Zachodniej przed ZSRR. Zapewnienie wspólnej obrony było ważnym problemem, zwłaszcza po kryzysie berlińskim w latach 1948–1949, kiedy ZSRR zablokował dostęp do podzielonego miasta, w rezultacie czego w 1949 r. sojusznicy utworzyli Organizację Traktatu Północnoatlantyckiego (NATO).

USEUCOM zostało utworzone jako następca Sił Zbrojnych Stanów Zjednoczonych w Europie, które powstało po II wojnie światowej z siedzibą we Frankfurcie nad Menem. Przed 1 sierpnia 1952 r. Siły Powietrzne, Marynarka Wojenna i Armia Stanów Zjednoczonych w Europie prowadziły odrębne dowództwa, które podlegały bezpośrednio Połączonym Szefom Sztabów (Joint Chiefs of Staff). Taka sytuacja zaistniała na skutek stanowiska generała armii D.D. Eisenhowera, który nie chciał pełnić podwójnej funkcji dowódcy wszystkich sił amerykańskich w Europie oraz Naczelnego Dowódcy Sił Sojuszniczych Europy NATO. Jednak 19 maja 1952 r. poinformował Połączonych Szefów Sztabów, że obejmie bezpośrednie dowództwo sił amerykańskich w Europie i utworzy osobny sztab, który będzie prowadził wspólne sprawy wojskowe USA.

Pierwsze ujednolicone dowództwo na obszarze europejskim zostało ustanowione przez Połączonych Szefów Sztabów 1 sierpnia 1952 r. w celu zapewnienia „jednolitego dowództwa i władzy" nad wszystkimi siłami USA w Europie. W 1952 r. obszar odpowiedzialności USEUCOM obejmował Europę kontynentalną, Wielką Brytanię, Afrykę Północną i Turcję, następnie został rozszerzony na Azję Południowo-Zachodnią po Iran i na południu do Arabii Saudyjskiej.

W 1954 r. kwatera główna USEUCOM została przeniesiona do Camp-de-Loges na obrzeżach Paryża, aby być w pobliżu Naczelnego Dowództwa Sił Sojuszniczych Europy. Na początku lat 60. w NATO pojawiły się ostre spory polityczne, a w 1966 r. prezydent Francji Ch. de Gaulle zażądał usunięcia wszystkich kwater i sił zbrojnych USA i NATO z francuskiego terytorium. Od 14 marca 1967 r. siedziba znajduje się w Patch Barracks w Stuttgarcie-Vaihingen.

Dowództwo USEUCOM wykonuje pełen zakres operacji wielodomenowych we współpracy z sojusznikami i partnerami, aby „wspierać NATO, odstraszać Rosję, pomagać w obronie Izraela, umożliwiać operacje globalne i przeciwdziałać zagrożeniom transnarodowym, wzmacniać bezpieczeństwo euroatlantyckie".

Wraz z końcem → z i m n e j w o j n y [t. 4] Stany Zjednoczone zaczęły wycofywanie swoich wojsk z Europy. W 2004 r. prezydent G.W. Bush ogłosił nową doktrynę stacjonowania sił zamorskich, tzw. Global Posture Review. Była to najpoważniejsza zmiana od czasów zakończenia II wojny światowej. Bush nazwał nowy typ baz mianem *lily pad* (z ang. liść lilii wodnej). Zamiast stałych, gigantycznych baz miały powstawać w wielu regionach świata małe jednostki składające się najczęściej z lotniska, niewielkiej załogi, składów amunicji i paliw. Dzięki nim siły Stanów Zjednoczonych w razie potrzeby mogą w krótkim czasie uderzyć w każdym zakątku globu. Jeszcze w 2004 r. tylko amerykańskie siły lądowe liczyły w Europie 62 tys. wojskowych korzystających z 240 obiektów i zorganizowanych m.in. w ramach 2 dywizji (1 Dywizja Piechoty i 1 Dywizja Pancerna) oraz brygady powietrznodesantowej. W kolejnych latach kontynuowano proces konsolidacji jednostek, rozwiązywania zbędnych czy powrotu części z nich do Stanów Zjednoczonych (powrót dotyczył przede wszystkim obu wspomnianych dywizji). W 2006 r. U.S. Army utrzymywała w Europie

55 tys. → żołnierzy [t. 4], chociaż istotnie zmieniła się struktura organizacyjna jednostek, w których służyli.

W 2007 r. pod dowództwem USEUCOM znajdowało się ok. 72 tys. żołnierzy. W 2010 r. Stany Zjednoczone obsługiwały ok. 737 amerykańskich baz rozsianych w blisko 150 krajach świata, w których na stałe stacjonowało prawie 400 tys. żołnierzy, 38 tys. spośród nich w miejscach o strategicznym znaczeniu dla lotnictwa i marynarki wojennej USA. Około 500 amerykańskich baz było w Europie, z czego nieco ponad 200 to lotniska wojskowe i powiązane obiekty. W 1990 r. w samej tylko Republice Federalnej Niemiec było 47 większych baz USA, w tym 10 baz sił powietrznych.

W połowie pierwszej kadencji B. Obamy rozpoczął on istotną redukcję amerykańskiego potencjału wojskowego w Europie. Decyzja ta miała wymiar strategiczny, USA dokonywały bowiem zmiany środka ciężkości swej globalnej obecności militarnej ze sfery atlantyckiej na Pacyfik. Dotyczyło to jednostek → marynarki wojennej [t. 3], ale i w podobnym stopniu sił powietrznych, a nawet wojsk lądowych. Gdy USEUCOM pozostała w Europie z dwoma związkami taktycznymi o potencjale brygady, Rosjanie – inspirowani zmianami politycznymi w Ukrainie – w 2014 r. dokonali błyskawicznej → aneksji [t. 1] Krymu i rozpoczęli ograniczony konflikt w Donbasie. W odpowiedzi amerykańskie siły zbrojne zwiększyły swą aktywność na wschodniej flance NATO.

Największe amerykańskie bazy zostały ulokowane wzdłuż gigantycznego półksiężyca niestabilności ciągnącego się od Karaibów poprzez Hawaje, Japonię, Koreę Południową, Guam aż po Zatokę Perską i kraje Europy Zachodniej. Tradycyjnie bazy USA mają spełnić 3 cele:

- powstrzymanie powiększania się wpływów największych rywali Stanów Zjednoczonych: Chin i Rosji;
- zapewnienie kontroli nad strategicznymi składami surowców, przede wszystkim ropy w Zatoce Perskiej;
- powstrzymanie gróźb islamskiego fundamentalizmu (zob. → fundamentalizm religijny).

Obecnie w Europie stacjonuje ok. 60 tys. żołnierzy z 5 typów sił zbrojnych, natomiast w rekordowych pod tym względem latach 60. było ich 400 tys. Dowódcy sił amerykańskich w Europie podlegają gen. C. Scaparrottiemu, który jednocześnie pełni funkcję najwyższego dowódcy

wojskowego NATO. Generał w maju 2020 r. apelował do Kongresu, aby zwiększyć liczbę amerykańskich żołnierzy w Europie, bo tylko to zapewni skuteczne odstraszanie Moskwy. Kwatera główna sił USA w regionie znajduje się w Stuttgarcie. W Neapolu z kolei mieści się dowództwo VI Floty, która operuje na wschodnim Atlantyku i zachodniej części Oceanu Indyjskiego. Amerykanie mają w Europie również bomby atomowe pod postacią zwykłych, zrzucanych z bombowców ładunków. Szacuje się, że 150–200 sztuk takiego uzbrojenia znajduje się na wyposażeniu baz wojskowych w Holandii, Niemczech, Turcji i Wielkiej Brytanii. Amerykanie stacjonują w niemieckim Ramstein, włoskim Aviano, na japońskiej wyspie Okinawa, w tureckim İncirlik czy południowokoreańskim Kunsan – bazy tworzą zamknięte miasta, do których na kilka lat przyjeżdża wraz z rodzinami po kilkadziesiąt tysięcy amerykańskich żołnierzy i gdzie znajduje się najnowocześniejszy sprzęt wojskowy: we Włoszech stacjonuje 401 eskadra myśliwców F-16, w Niemczech czołgi M1A2 Abrams wyposażone w ultraprecyzyjne systemy naprowadzania, a w bazie Kleine Brogel w Belgii (80 km od Brukseli) Amerykanie mają pociski typu B-61 z głowicami atomowymi. Większość żołnierzy USEUCOM to 7 Armia Stanów Zjednoczonych, 6 Flota Stanów Zjednoczonych oraz 3 i 16 Brygada Sił Powietrznych.

Europejska inicjatywa odstraszania, ogłoszona w 2014 r., umożliwia Stanom Zjednoczonym wzmocnić odstraszającą postawę USA, zwiększyć gotowość i szybkość reakcji sił amerykańskich w Europie, wspierać obronę zbiorową oraz → bezpieczeństwo [t. 1] sojuszników NATO, a także wzmacniać bezpieczeństwo i potencjał sojuszników i partnerów USA.

W 2014 r. w związku z wydarzeniami w Ukrainie (aneksja Krymu przez Federację Rosyjską i konflikt zbrojny na wschodzie Ukrainy) USA rozpoczęły ćwiczenia militarno-polityczne w ramach operacji Atlantic Resolve. Zaczęto regularnie przeprowadzać rotację wojsk amerykańskich ze Stanów Zjednoczonych do Europy Wschodniej (do udziału w ćwiczeniach i wspólnym szkoleniu bojowym z siłami zbrojnymi państw tego regionu), po raz pierwszy w Polsce i krajach bałtyckich pojawiły się czołgi amerykańskie. Wielkość amerykańskich sił zbrojnych w Europie według „The Military Balance" w latach 2013–2016 zmniejszyła się z 70,1 do 67,1 tys. osób. Nie uwzględnia to jednak sił rotacyjnych, które

stacjonują w Europie przez określony czas. Ich średnioroczną liczbę można szacować na ok. 8 tys. osób. Od 2017 r. w Europie było więc ok. 75 tys. żołnierzy amerykańskich.

USA rozpoczęły w lutym 2017 r. wzmacnianie swych sił lądowych w Europie w ramach ciągłego rotacyjnego przenoszenia brygad pancernych, co zwiększyło obecność armii USA w Europie do 3 brygad. Według komunikatu dowództwa USEUCOM armia i przede wszystkim wojska lądowe USA rozpoczęły składowanie uzbrojenia w swych wysuniętych magazynach armijnych (Army Prepositioned Stocks, APS) na terenie Europy na potrzeby ewentualnych działań doraźnych. Chodzi o nieprzerwane rozmieszczenie w Europie Wschodniej brygady pancernej, bowiem rotacje wojsk będą przebiegały bez przerwy, co oznacza ciągłą obecność wojsk pancernych w tej części Europy. Ten plan rozmieszczenia armii jest kolejnym przejawem zdecydowanego i zrównoważonego podejścia do kwestii gwarancji dla sojuszników w obliczu agresywnej polityki Rosji w Europie Wschodniej. Według zapowiedzi USEUCOM uczestniczące w dziewięciomiesięcznych misjach rotacyjnych brygady zabiorą ze sobą z USA własne nowoczesne wyposażenie. Będzie to najnowocześniejsze wyposażenie, jakie armia ma do dyspozycji. Natomiast używane obecnie przez siły rotacyjne wyposażenie pozostanie w Europie, by po naprawach i unowocześnieniu stać się podstawowym elementem APS, które będą rozmieszczone w Belgii, Holandii i Niemczech. W razie potrzeby zmagazynowany w APS materiał zapewni wojskom dodatkowy potencjał bojowy.

Od końca 2017 r. w Europie znajdują się 3 w pełni wyposażone brygady armii USA – jedna pancerna (stacjonuje w Niemczech), jedna powietrznodesantowa (stacjonująca we Włoszech) i jedna typu Stryker – zmechanizowana brygada pancerna. Amerykańskie plany zakładają możliwość przerzucenia na wschodnie obrzeża NATO 4 brygad: 2 stacjonujących w Europie Zachodniej, kolejnej brygady ćwiczącej rotacyjnie w regionie, czwarta byłaby przerzucana z USA lub innej pozaeuropejskiej amerykańskiej bazy, sprzęt dla niej ma być składowany w Europie.

Pięć elementów europejskiego planu dowództwa USA dotyczącego wdrożenia EDI (ang. *Electronic Data Interchange*) składa się na opracowaną technikę wymiany danych wykorzystującą zasady działania poczty

elektronicznej, której cechą charakterystyczną jest niezależność od właściwości stosowanego sprzętu i oprogramowania (5910,6 mln USD na rok budżetowy 2020):

Zwiększona obecność (2051 mln USD): Stany Zjednoczone będą nadal wspierać zwiększoną rotacyjną obecność wojskową USA w całej Europie, która jest w stanie odstraszać i – w razie potrzeby – reagować na regionalne → zagrożenia [t. 4].

Ćwiczenia i szkolenie (609 mln USD): wzrost tempa szkolenia, które poprawia ogólną gotowość i interoperacyjność sojuszników NATO i partnerów, a także może służyć jako środek odstraszający wobec agresywnych podmiotów regionalnych.

Lepsze pozycjonowanie wstępne (2359 mln USD): zwiększenie nowoczesnego sprzętu w całej Europie, który umożliwia jednocześnie szybkie rozmieszczenie sił zbrojnych według zapotrzebowania.

Modernizacja infrastruktury (517 mln USD): kluczowe usprawnienia infrastruktury w całej Europie będą wspierać operacje wojskowe USA.

Budowanie potencjału partnerstwa (374 mln USD): rozszerzone zaangażowanie i ćwiczenia wzmacniają zdolność sojuszników i partnerów do obrony i utrzymania → bezpieczeństwa europejskiego [t. 1].

USEUCOM utrzymuje operacyjne siły zbrojne do prowadzenia pełnych operacji samodzielnie lub we współpracy z partnerami koalicyjnymi i stawia przed sobą następujące zadania:

zwiększenie bezpieczeństwa transatlantyckiego dzięki wsparciu NATO;

zapewnienie stabilności regionalnej;

powstrzymanie konfliktów, wojna z → terroryzmem [t. 4];

przeciwdziałanie zagrożeniom transnarodowym w celu ochrony i obrony Stanów Zjednoczonych;

reprezentacja interesów USA w regionie.

Aktualne obszary zainteresowania USA obejmują również:

przegląd pozycji europejskich sił strategicznych;

aktualizację problemów związanych z koronawirusem;

międzynarodowe ćwiczenia sił morskich Northern.

Celem USEUCOM jest budowa bardziej efektywnych sił i utrzymanie współpracy z sojusznikami USA w Europie. Ma towarzyszyć temu optymalizacja amerykańskiej obecności militarnej na świecie, tj. lepsze ulokowanie sił i środków, zwiększenie ich efektywności w zmieniającym się współczesnym świecie.

Generalnie, zdaniem Szefa Pentagonu, przed USEUCOM stoi 5 kluczowych wyzwań:

→ strategia [t. 4] → odstraszania [t. 3] Rosji;
wzmocnienie NATO;
zagwarantowanie pewności sojusznikom;
poprawa strategicznej elastyczności Stanów Zjednoczonych i operacyjnej elastyczności USEUCOM;
zadbanie o wojskowych i ich rodziny.

W 2020 r. ok. 5,6 tys. wojskowych zostało przeniesionych z Niemiec do innych państw Sojuszu, ok. 6,4 tys. osób wraca do USA. Znaczna część żołnierzy jest zaangażowana w rotacyjną obecność w Europie. Amerykańskie dowództwa w Europie mają być przesunięte bliżej struktur dowodzenia NATO w Belgii oraz we Włoszech. Przesunięcia w systemie dowodzenia mogą objąć grupę nawet 2 tys. amerykańskich wojskowych.

Zgodnie z planami ogłoszonymi w lipcu 2020 r. przez Pentagon ze Stuttgartu w Niemczech do Mons w Belgii zostało przeniesione Dowództwo Europejskie Stanów Zjednoczonych oraz towarzyszące mu dowództwo amerykańskich sił operacji specjalnych w Europie. Z Niemiec – do jeszcze nieustalonej lokalizacji – przenieść mają się także dowództwa odpowiedzialne za amerykańskie siły zbrojne w Afryce oraz siły specjalne USA na tym kontynencie. Część mniejszych amerykańskich jednostek wojskowych ma zostać przesunięta z Niemiec do Belgii i Włoch.

Naczelny Dowódca Sił Sojuszniczych w Europie generał T.D. Wolters, udzielając wywiadu przedstawicielom NATO w październiku 2019 r. podkreślił, że:

> pierwszym priorytetem działalności EUCOM […] jest wspieranie NATO. Drugim priorytetem jest zwalczanie złośliwych wpływów Rosji. […] Trzecim dużym priorytetem są relacje i zaangażowanie […] dla wspierania gotowości naszych sił, aby były one

jak najbardziej responsywne, odporne i zabójcze, dotrzymując i promując te wartości demokratyczne, które są tak ważne dla NATO i USA.

Warto wskazać kilka ostatnich działań, które zostały przyjęte z perspektywy USEUCOM oraz z perspektywy SACEUR (Supreme Allied Commander Europe) – naczelnego dowódcy sojuszniczego w Europie, głównodowodzącego połączonych sił zbrojnych NATO w Europie, stojącego na czele Sojuszniczego Dowództwa Operacji (Allied Command Operations):

adaptacja nowej strategii wojskowej NATO, która de niuje 2 podstawowe zagrożenia – jedno pochodzi z Rosji, a drugie dotyczy międzynarodowego terroryzmu;

wstępna koncepcja odstraszania i obrony obszaru euroatlantyckiego NATO, którą muszą przyjąć wszystkie spośród 29 zaangażowanych krajów, żeby poprawić zdolność odstraszania w XXI w. i obrony w taki sposób, aby nigdy nie dochodziło do sytuacji, w której wyniknie kon ikt kinetyczny i trzeba będzie się bronić;

adaptacja struktury dowodzenia NATO – umieszczanie sił zbrojnych tam, gdzie muszą być, żeby były najlepiej dopasowane, we właściwym miejscu i czasie, żeby najskuteczniej odstraszać, tak aby niefortunny potencjał kon iktu nigdy się nie pojawił.

Od zakończenia II wojny światowej europejscy sojusznicy i partnerzy współpracują ze Stanami Zjednoczonymi, żeby osiągnąć bezpieczeństwo i stabilność, a Europa nadal ma kluczowe znaczenie dla → bezpieczeństwa narodowego [t. 1] USA. Obecnie Europejskie Dowództwo Stanów Zjednoczonych mierzy się z najgłębszymi negatywnymi zmianami w europejskim środowisku bezpieczeństwa od zakończenia zimnej wojny. Masowa migracja, terroryści, → wojna informacyjna [t. 4] i hybrydowa, → cyberataki [t. 1], utrzymujące się skutki światowego kryzysu nansowego i niedo nansowane budżety obronne państw sojuszników zagrażają bezpieczeństwu europejskiemu, USA oraz światowemu bezpieczeństwu i stabilności.

Szereg krajów Europy Wschodniej należy do regionów na obszarze EUCOM, w których pomimo ogólnej redukcji ma nastąpić wzrost