Nr 15 (8) 2016

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

CENTRALNY OŚRODEK SZKOLENIA
im. gen. dyw. Stefana Roweckiego „GROTA”

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 15 (8) 2016

INTERNAL SECURITY REVIEW

WARSAW 15 (8) 2016

ISSN 2080-1335

Wszystkie artykuły zamieszczone w czasopiśmie są recenzowane
All the articles published in the magazine are subject to reviews

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną
Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) znajduje się na liście czasopism naukowych Ministra Nauki i Szkolnictwa Wyższego z liczbą 5 punktów za umieszczone w nim publikacje. PBW można odnaleźć także w Index Copernicus Journal Master List z liczbą 44,99 punktów. Czasopismo jest również dostępne w bazach: Central European Journal of Social Science and Humanities i Polska Bibliografia Naukowa (PBN)

Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia
im. gen. dyw. Stefana Roweckiego „Grota" w Emowie
05-462 Wiązowna, ul. Nadwiślańczyków 2

Redakcja
tel. (+48) 22 58 58 613
fax. (+48) 22 58 58 645
e-mail: redakcja.pbw@abw.gov.pl
www.abw.gov.pl

Numer zamknięto i oddano do druku w listopadzie 2016 r.

Druk: Biuro Logistyki
Agencji Bezpieczeństwa Wewnętrznego
00-993 Warszawa, ul. Rakowiecka 2A
tel. (+48) 22 58 57 657

SPIS TREŚCI

CONTENTS

I
ANALIZY I ROZPRAWY

Tomasz R. Aleksandrowicz

Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego

Normatywne określenie bezpieczeństwa w cyberprzestrzeni jest bez wątpienia zadaniem niezwykle trudnym. Wynika to przede wszystkim z tego, że cyberprzestrzeń jest zjawiskiem stosunkowo nowym, trudnym do jednoznacznego zdefiniowania z uwagi na jej cechy charakterystyczne, stanowiące w wielu przypadkach swoiste novum.

Cyberprzestrzeń: próba definicji i cechy charakterystyczne

Termin cyberprzestrzeń (ang. *cyberspace*) stworzył i upowszechnił już w 1984 r. William Gibson, autor kultowej powieści cyberpunkowej *Neuromancer*. W swojej literackiej wizji określił on cyberprzestrzeń jako (…) *konsensualną halucynację, doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych* (…). *Graficzne odwzorowanie danych z banków wszystkich komputerów świata. Niewyobrażalna złożoność* (…)[1].

W literaturze przedmiotu cyberprzestrzeń określa się jako ogół powiązań o charakterze wirtualnym („nieprzestrzennym" w sensie fizycznym, niematerialnym) powstałych i istniejących dzięki ich fizycznym manifestacjom (komputery, infrastruktura telekomunikacyjna)[2]. Najogólniej można powiedzieć, że cyberprzestrzeń to (…) *całość powiązań ludzkiej działalności z udziałem ICT* (*Information and Communication Technology* – przyp. aut.)[3]. Innymi słowy (…) *mianem cyberprzestrzeni (cyberspace) określa się sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane, sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej i gazowej czy ochrony zdrowia*[4].

Cyberprzestrzeń została w Rzeczpospolitej Polskiej zdefiniowana ustawowo jako 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[5].

---

[1] W. Gibson, *Neuromancer*, Poznań 1999, s. 53.

[2] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, s. 28.

[3] A. Bógdoł-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 37.

[4] P. Tekielska, Ł. Czekaj, *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (red.), Warszawa 2014, s. 163.

[5] Art. 2 ust. 1b *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. z 2014 poz. 1815, ze zm.). Podobnie jest definiowana cyberprzestrzeń w *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy* [online],

Cyberprzestrzeń jako sfera ludzkiej działalności w zasadniczy sposób różni się od przestrzeni fizycznej. Po pierwsze należy wskazać na uniezależnienie się od miejsca zajmowanego w przestrzeni fizycznej (w sensie geograficznym). Jedynym wymaganiem jest techniczna możliwość włączenia się do sieci. Co więcej – poszczególne urządzenia podłączone w danej chwili do sieci mają szybki i równoprawny dostęp do pozostałych elementów układu, podobnie jak inni uczestnicy o tym samym statusie[6]. Po drugie należy wskazać na obniżający się koszt wejścia do sieci i podejmowania w niej różnych działań. Zmniejsza się także zasób wiedzy i umiejętności niezbędnych do podejmowania takich działań z uwagi na widoczną tendencję do maksymalnego upraszczania interfejsu. Po trzecie wreszcie sieć pozwala w znacznej mierze na zachowanie anonimowości uczestnika. Ślady, które użytkownik pozostawia za sobą w sieci, są tak naprawdę śladami komputera, z którego korzysta. Odrębnym problemem jest powiązanie tego komputera z konkretnym człowiekiem. Istnieje też możliwość pełnej anonimizacji[7].

Cyberprzestrzeń stała się – jak to określono w amerykańskiej *National Strategy to Secure Cyberspace* – „systemem nerwowym państwa": (…) *nasza gospodarka i bezpieczeństwo narodowe stały się w pełni zależne od technologii i infrastruktury informatycznej*[8]. Od sprawności i bezpieczeństwa cyberprzestrzeni zależy funkcjonowanie infrastruktury krytycznej[9].

W podsumowaniu tego wątku można stwierdzić, że cyberprzestrzeń charakteryzuje się następującymi cechami:

- niezależnością od miejsca,
- niezależnością od odległości,
- niezależnością od czasu,
- niezależnością od granic,
- względną anonimowością,
- możliwością ustalenia sprzętu, nie osoby.

Bezpieczeństwo w cyberprzestrzeni

Znaczenie cyberprzestrzeni dla współczesnego państwa i społeczeństwa powoduje, że coraz ważniejszy staje się problem jej bezpieczeństwa. Jak stwierdzają Bogusław Pacek i Romuald Hoffman, (…) *bezpieczeństwo cyberprzestrzeni* (…) *można określić jako brak ryzyka utraty danych informacyjnych w cyberprzestrzeni* (…) *Widać jasno, że zasobem, który chronimy, jest informacja*[10]. Przywołani autorzy wyraźnie sytuują kwestię bezpieczeństwa cyberprzestrzeni w kategoriach walki i wojny informacyjnej, co nakazuje przyjęcie za punkt wyjścia do dalszych rozważań bezpieczeństwa informacyjnego państwa jako integralnej części bezpieczeństwa narodowego, a następnie zagrożeń

April 2011: *Cyberspace is the interdependent network of information technology components that underpins many of our communications; the Internet is one component of cyberspace*, http://www.hsdl.org/?view&did=7010 [dostęp: 15 III 2012].

[6] Zob. T. Aleksandrowicz, *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 75 i nast.

[7] Na temat cech cyberprzestrzeni zob. M. Madej, *Rewolucja informatyczna*…, s. 29–31.

[8] *The National Strategy to Secure Cyberspace* [online], February 2003, http://www.hsdl.org/?view&did=1040 [dostęp: 15 III 2012].

[9] *International Strategy for Cyberspace. Prosperity, Secirity, and Openess in a Networked World* [online], May 2011, http://www.hsdl.org/?view&did=5665 [dostęp: 15 III 2012].

[10] B. Pacek, R. Hoffman, *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, s. 85.

informacyjnych[11]. W ramach takiego podejścia należy uwzględnić wiele uwarunkowań bezpieczeństwa informacyjnego, a przede wszystkim to, że:

- informacja stanowi zasób strategiczny państwa,
- informacja i wynikające z niej wiedza oraz technologie informatyczne stają się podstawowym czynnikiem wytwórczym,
- szeroko rozumiany sektor informacyjny wytwarza znaczną część dochodu narodowego[12],
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego są w znacznej mierze uzależnione od systemów przetwarzania i przesyłania informacji,
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych,
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej[13],
- technologie informatyczne stały się istotnym elementem funkcjonowania bezpieczeństwa państwa, w tym sił zbrojnych[14],
- media masowe mogą być wykorzystywane jako narzędzia skutecznego zakłócania informacyjnego, np. przez prowadzenie dezinformacji[15].

Eugeniusz Nowak i Maciej Nowak proponują bardzo szeroką definicję bezpieczeństwa informacyjnego, zgodnie z którą jest to stan warunków wewnętrznych i zewnętrznych pozwalający państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego. Zdaniem przywołanych autorów ten stan jest osiągnięty, gdy są spełnione następujące warunki:

- nie są zagrożone strategiczne zasoby państwa,
- organy władzy podejmują decyzje na podstawie wiarygodnych, istotnych, dokładnych i aktualnych informacji,
- przepływ informacji pomiędzy organami państwa jest niezakłócony,
- funkcjonowanie sieci teleinformatycznych tworzących teleinformatyczną infrastrukturę krytyczną państwa jest niezakłócone,
- państwo gwarantuje ochronę informacji niejawnych i danych osobowych obywateli,
- instytucje publiczne nie naruszają prawa obywateli do prywatności,
- obywatele, organizacje pozarządowe i przedstawiciele środków masowego przekazu mają dostęp do informacji publicznej[16].

Nie bez powodu zatem coraz większą popularnością – nie tylko wśród teoretyków – cieszy się pojęcie walki informacyjnej. Nie powinno też dziwić, że wywodzi się ono z nauk wojskowych. Jak podkreślają Piotr Sienkiewicz i Halina Świebo-

[11] P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [online], http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf, s. 373–374 [dostęp: 5 IV 2012].

[12] Technologie informatyczne i komunikacyjne stanowią silny czynnik wzrostu gospodarczego. W Unii Europejskiej ten sektor generuje 25% wzrostu PKB i 40% wzrostu produktywności. Takie dane podaje Komisja Europejska w dokumencie *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia* [online], Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Bruksela 1 VI 2005 COM(2005) 229 końcowy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PL:PDF [dostęp: 5 IV 2012].

[13] Zob. K. Liedel, *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, s. 57.

[14] B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 219.

[15] K. Liedel, *Bezpieczeństwo informacyjne…*, s. 57–58.

[16] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103.

da, nie istnieje jedna, uzgodniona definicja walki informacyjnej, jednak w większości proponowanych rozwinięć tego terminu występują wspólne treści. Wszystkie one sprowadzają się do postrzegania walki informacyjnej jako konfliktu, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią, a zarazem konflikt ten obejmuje fizyczne niszczenie infrastruktury wykorzystywanej przez przeciwnika do działań operacyjnych. *Obecnie słusznie uważa się, że ‚cyberwar', ‚infowar', walka informacyjna, cyberterroryzm, ‚netwar', informacyjni wojownicy, informacyjna dominacja, obrona w cyberprzestrzeni (‚cyberspace defence') czy informacyjny chaos to tylko neologizmy, dotyczące tego samego, ale bardzo szerokiego pojęcia wojny ery informacyjnej (information age warfare*)[17].

Powyższe wyjaśnienie wymaga doprecyzowania. Proponuje je zresztą sam P. Sienkiewicz, stosując do procesów informacyjnych na współczesnym polu walki zasady analizy systemowej. Jego zdaniem czynnikiem decydującym o rezultatach walki jest stosunek wiedzy stron walczących. Definiuje on w a l k ę i n f o r m a c y j n ą jako (…) *całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki informacyjnej jest 1. zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych, 2. zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych*[18]. Potencjał informacyjny jako czynnik potencjału militarnego tworzą zasoby informacyjne systemu obronnego państwa (dane, informacje, wiedza) oraz systemy informacyjne kształtujące infrastrukturę informacyjną państwa[19].

W świetle powyższego można zatem stwierdzić, że walka informacyjna to całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi nad przeciwnikiem i osiągnięcia zamierzonych celów. Istotą tej walki jest z jednej strony zniszczenie lub degradacja wartości zasobów informacyjnych przeciwnika (w tym także zasobów przestępcy) oraz stosowanych przez niego systemów informacyjnych, a z drugiej – zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych[20]. Elementami walki informacyjnej są destrukcja fizyczna, operacje bezpieczeństwa, operacje psychologiczne, sabotaż i walka elektroniczna[21]. Jako narzędzia wykorzystywane w tej walce można wskazać m.in.:

- dyplomację,
- propagandę,
- kampanie psychologiczne,
- działania wpływające na procesy polityczne lub kulturowe,
- dezinformację, manipulowanie lokalnymi mediami,
- infiltrację sieci komputerowych i baz danych[22].

[17] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, w: *Bezpieczeństwo teleinformatyczne państwa*…, s. 80 i nast. Autorzy zamieścili w cytowanym artykule przegląd definicji walki informacyjnej i działań informacyjnych. Zob. też: P. Sienkiewicz, *Wizje i modele wojny*…

[18] P. Sienkiewicz, *Wizje i modele wojny*…, s. 375.

[19] Tamże, s. 376.

[20] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako*…, s. 79–85.

[21] Tamże, s. 87.

[22] Zob. J. Arguilla, D. Ronfeldt, *Cyberwar is Coming!*, w: *In Athena's Camp: Preparing for Conflict in the Information Age,* Santa Monica 1993, s. 28; http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [dostęp: 6 IV 2012]. Por. też K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17, s. 22–23.

Informacja jest zatem w walce informacyjnej zarówno celem ataku, jak i bronią, tarczą i mieczem, zasobem, ale obejmuje także fizyczne niszczenie infrastruktury wykorzystywanej przez przeciwnika do działań operacyjnych, niszczenie (lub degradację wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych, zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych.

W cyberprzestrzeni walka informacyjna przybiera postać „konfliktu cybernetycznego", w którym sukces lub porażka są uzależnione od działań prowadzonych w sieciach komputerowych. Taki konflikt może przybrać postać **aktywizmu** (niedestrukcyjnej działalności informacyjno-propagandowej, np. na forach internetowych, czatach, portalach społecznościowych), **haktywizmu** (aktywizmu i działań zakłócających funkcjonowanie określonych systemów komputerowych, np. przez blokowanie dostępu do serwerów) lub **cyberterroryzmu** (politycznie motywowanych ataków na komputery, sieci lub systemy informatyczne w celu zniszczenia infrastruktury i wymuszenia na rządzie lub organizacji określonego działania lub zaniechania).

Cyberprzestrzeń należy zatem traktować jako nowe środowisko działania, w którym za pomocą zdigitalizowanej informacji jest prowadzona walka informacyjna w jej pełnym zakresie. Można tu mieć do czynienia ze szpiegostwem, przestępczością (ataki na konta bankowe, wyłudzenia, oszustwa itp.), terroryzmem (na szczęście – ciągle jeszcze teoretycznie) i działaniami nakazującymi traktować cyberprzestrzeń jako piąte – po lądzie, morzu, przestrzeni powietrznej i kosmicznej – środowisko walki.

Tak prowadzona walka informacyjna w cyberprzestrzeni wymaga specyficznych narzędzi (zwanych niekiedy potocznie „narzędziami hakerskimi"). W praktyce można wyróżnić 20 podstawowych narzędzi wykorzystywanych do przeprowadzania różnego rodzaju ataków na systemy informatyczne:

1) wirusy, robaki i bakterie (oprogramowanie złośliwe – *malware*) – programy rozprzestrzeniające się w systemie informatycznym i zmieniające sposób jego działania lub reprodukujące się i zajmujące pamięć procesora, przestrzeń dyskową i inne zasoby, a w rezultacie – blokujące dostęp do danych,
2) bomby logiczne – aktywizujące nowe funkcje elementów logicznych komputera i prowadzące do zniszczenia sprzętu i oprogramowania,
3) konie trojańskie – programy umożliwiające podejmowanie w systemie komputerowym działań bez wiedzy i zgody jego prawowitego użytkownika, np. usuwanie plików, formatowanie dysków, kopiowanie danych itp.,
4) próbkowanie – dostęp do komputera przez analizę jego charakterystyki,
5) uwierzytelnianie – podszywanie się pod osobę uprawnioną do dostępu do systemu,
6) ominięcie – ominięcie procesu zabezpieczającego system,
7) czytanie – nieuprawniony dostęp do informacji,
8) kopiowanie – nieuprawnione kopiowanie plików,
9) kradzież – przejęcie zasobów systemu przez osobę nieuprawnioną bez pozostawiania kopii,
10) modyfikacja – zmiana zawartości danych lub charakterystyki obiektu ataku,
11) usunięcie – zniszczenie obiektu ataku,
12) złośliwe podzespoły – umieszczanie w komputerach chipów zawierających programy umożliwiające nieuprawniony dostęp do systemu lub tworzące wady konstrukcyjne,

13) tylne drzwi – pozostawienie przez twórców oprogramowania „furtki" nieznanej użytkownikowi; za pomocą tylnych drzwi można uzyskać nieuprawniony dostęp do systemu,
14) maskarada – udawanie przez atakującego jednego z użytkowników systemu przez np. modyfikację pakietów w trakcie połączenia,
15) przechwycenie transmisji – uzyskanie dostępu do treści przesyłanych między komputerami,
16) podsłuchiwanie – śledzenie ruchu w sieci,
17) receptor van Ecka – oglądanie przez napastnika na oddzielnym monitorze repliki obrazów pojawiających się na monitorze użytkownika atakowanego komputera,
18) *DDoS* – zablokowanie dostępu do strony internetowej przez przesyłanie pod jej adresem olbrzymiego pakietu danych z różnych źródeł, co powoduje zawieszenie się serwera,
19) *e-mail bombing* – przesyłanie na skrzynkę pocztową atakowanego użytkownika wielkiej ilości danych, co powoduje jej przepełnienie,
20) *electromagnetic pulse* – emisja promieniowania elektromagnetycznego należącego do widma radiowego, które niszczy urządzenia elektroniczne i dane[23].

Normatywne ujęcie zagrożeń bezpieczeństwa w cyberprzestrzeni

Powyższe rozważania wskazują na trudności, jakie niosą za sobą próby stworzenia normatywnych definicji czynów wywołujących zagrożenia cyberprzestrzeni. W dziedzinie prawa międzynarodowego taką próbę podjęła po raz pierwszy Rada Europy, która w 2001 r. przyjęła w Budapeszcie konwencję o cyberprzestępczości (dalej: konwencja budapesztańska[24]). Definiując poszczególne pojęcia, konwencja budapesztańska stanowi w art. 1, że:

> a) „system informatyczny" oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych;
>
> b) „dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny;
>
> c) „dostawca usług" oznacza (i) dowolny podmiot prywatny lub publiczny, który umożliwia użytkownikom jego usług komunikowanie się za pomocą systemu informatycznego, oraz (ii) dowolny inny podmiot, który przetwarza lub przechowuje dane informatyczne w imieniu takich usług komunikacyjnych lub użytkowników takich usług,
>
> d) „dane dotyczące ruchu" oznaczają dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez sys-

[23] Wykaz na podstawie: E. Lichocki, *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP*, Wydział Bezpieczeństwa Narodowego Akademii Obrony Narodowej, Warszawa 2009, s. 62–63 (rozprawa doktorska).

[24] *Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.* (Dz.U. poz. 1514). Zob. na ten temat: D. Głowacka, *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji* [online], http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf [dostęp: 3 VII 2014]. Tekst konwencji: *Convention of Cybercrime* [online], Budapest, 23 XI 2001 r., European Treaty Series nr 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [dostęp: 3 VII 2014].

tem informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazujące swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę, rozmiar, czas trwania lub rodzaj danej usługi[25].

Konwencja budapesztańska zobowiązuje państwa członkowskie do uznania za przestępstwa wiele czynów popełnianych w cyberprzestrzeni. Dzieli je na cztery kategorie: przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów; przestępstwa komputerowe; przestępstwa ze względu na charakter zawartych informacji oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Do pierwszej kategorii wyżej wymieniona konwencja zalicza:

- nielegalny dostęp, rozumiany jako umyślny, bezprawny dostęp do całości lub części systemu informatycznego. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione przez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub z innym nieuczciwym zamiarem albo w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym (art. 2),
- nielegalne przechwytywanie danych, a więc umyślne, bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym (art. 3),
- naruszenie integralności danych rozumiane jako umyślne, bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych. Strona może zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie l musi skutkować poważną szkodą (art. 4),
- naruszenie integralności systemu, a więc umyślne, bezprawne, poważne zakłócanie funkcjonowania systemu informatycznego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych (art. 5),
- niewłaściwe wykorzystywanie urządzeń rozumiane jako umyślne i bezprawne działania polegające na produkcji, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:
  - urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim do popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2–5,
  - hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna (art. 6).

Drugą kategorię stanowią przestępstwa komputerowe, a więc fałszerstwo komputerowe (art. 7) i oszustwo komputerowe (art. 8). Fałszerstwem komputerowym jest umyślne, bezprawne wprowadzanie i dokonywanie zmian, wykasowywanie lub usuwanie danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem

[25] http://prawo.vagla.pl/node/1493 (przyp. red.).

jako autentyczne, bez względu na to, czy są one zrozumiałe i czy można je bezpośrednio odczytać. Strona może wprowadzić wymóg, że odpowiedzialność karna dotyczy działania w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze. Natomiast za oszustwo komputerowe konwencja budapeszteńska uznaje umyślne, bezprawne spowodowanie utraty majątku przez inną osobę przez: wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych bądź każdą ingerencję w funkcjonowanie systemu komputerowego z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.

Przestępstwa ze względu na charakter zawartych informacji (trzecia kategoria) dotyczą czynów związanych z bezprawnym i umyślnym produkowaniem, oferowaniem, udostępnianiem, pozyskiwaniem i posiadaniem pornografii dziecięcej za pomocą systemu informatycznego (art. 9). Czwarta kategoria dotyczy naruszania praw autorskich i pokrewnych z wykorzystaniem systemu informatycznego.

W podobny sposób czyny wymierzone w bezpieczeństwo cyberprzestrzeni definiuje prawo Unii Europejskiej, tzw. dyrektywa o atakach na systemy informatyczne[26]. Jej treść jest z punktu widzenia Rzeczpospolitej Polskiej szczególnie istotna, stanowi ona bowiem obowiązujący akt prawotwórczy. Dyrektywa 2013/40/UE obliguje państwa członkowskie Unii Europejskiej do podjęcia kroków umożliwiających karanie jako przestępstw następujących czynów:

- niezgodnego z prawem dostępu do systemów informatycznych, a zatem umyślnego i bezprawnego uzyskiwania dostępu do całości lub jakiejkolwiek części systemu informatycznego, gdy zostało ono popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 3),
- niezgodnej z prawem ingerencji w systemy, czyli umyślnego i bezprawnego uzyskiwania dostępu do całości lub jakiejkolwiek części systemu informatycznego, gdy to przestępstwo zostało popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 4),
- niezgodnej z prawem ingerencji w dane, rozumianej jako umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 5),
- niezgodnego z prawem przechwytywania, a więc umyślnego i bezprawnego przechwytywania za pomocą środków technicznych niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 6).

W art. 7 zatytułowanym *Narzędzia do popełniania przestępstw* stypizowano czyny polegające na umyślnym wytwarzaniu, sprzedaży, dostarczaniu w celu użycia oraz przywozu, rozpowszechnianiu lub udostępnianiu w inny sposób jednego z następujących narzędzi: programu komputerowego, zaprojektowanego lub przystosowanego głównie do popełnienia jednego z wymienionych przestępstw, hasła komputerowego, kodu dostępu lub podobnych danych umożliwiających dostęp do całości lub części systemu informa-

[26] *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiS* (Dz.Urz. UE L 218 z 14 VIII 2013 r. poz. 8).

tycznego. Podobnie jak w przypadku pozostałych czynów, warunkiem jest bezprawność i umyślność działania sprawcy oraz to, że czyn nie stanowi przypadku mniejszej wagi.

Należy zauważyć, że problematyka dotycząca czynów przeciwko bezpieczeństwu cyberprzestrzeni znalazła regulacje w polskim kodeksie karnym[27]. Ustawodawca słusznie potraktował te zagrożenia w kategoriach walki informacyjnej i pogrupował stosowne przepisy w rozdziale XXXIII – *Przestępstwa przeciwko ochronie informacji*. W grę wchodzą przepisy art. 267, 268, 268a, 269, 269a i 269b, które typizują przestępstwa przeciwko ochronie informacji w cyberprzestrzeni.

Za przestępstwa polski ustawodawca uznaje zatem następujące czyny:

Art. 267

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego.

Art. 268

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

[27] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137).

Art. 269

§ 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b

§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Wojna w cyberprzestrzeni

Cyberprzestrzeń stała się także środowiskiem walki i wojny. W tym kontekście trzeba podkreślić problem prawnomiędzynarodowej oceny środków walki informacyjnej prowadzonej w tej przestrzeni. Jej ranga i znaczenie – choćby w przypadku rozwoju technologicznego i coraz większego znaczenia informacji w formie cyfrowej – będzie w dającej się przewidzieć przyszłości wzrastać. Należy tu wskazać na kilka elementów. Po pierwsze nie ulega wątpliwości, że walka informacyjna w cyberprzestrzeni prowadzona w ramach toczącego się konfliktu zbrojnego jest immanentną częścią tego konfliktu. Po drugie coraz większego znaczenia nabiera walka informacyjna prowadzona w cyberprzestrzeni samoistnie, tj. w warunkach pokoju – bez prowadzenia działań zbrojnych. W takiej walce cele nie mają bezpośredniego znaczenia militarnego (jak np. w przypadku konfliktu zbrojnego cybernetyczne ataki na systemy dowodzenia i łączności przeciwnika), lecz należą do kategorii infrastruktury krytycznej państwa[28]. Tego typu ataki mogą wywołać zagrożenia

[28] W polskim ustawodawstwie infrastruktura krytyczna jest definiowana jako systemy i powiązane ze sobą funkcjonalnie obiekty wchodzące w ich skład, w tym obiekty budowlane, urządzenia, instalacje, usługi ważne dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Pojęcie infrastruktura krytycz-

bezpieczeństwa międzynarodowego (globalnego bezpieczeństwa informacyjnego), destabilizację infrastruktury krytycznej, zakłócenia w funkcjonowaniu administracji publicznej, straty gospodarcze (zahamowanie rozwoju firm i przedsiębiorstw) czy nawet straty osobiste obywateli[29]. Istotne znaczenie ma kwestia skali ataku i strat.

Po trzecie cyberprzestrzeń jest wykorzystywana przez przestępców działających jedynie z chęci zysku. Ten aspekt został omówiony powyżej.

Faktem pozostaje, że problem walki informacyjnej w cyberprzestrzeni prowadzonej samoistnie w ogóle nie znajduje odniesienia w obowiązującym prawie międzynarodowym. Podczas analizy hipotetycznych ataków cybernetycznych na infrastrukturę krytyczną państwa można wskazać na następujące sytuacje:

- napastnik jest znany, a państwo (ofiara) podejmuje przeciwko niemu działania zbrojne,
- w analogicznej sytuacji państwo (ofiara) odpowiada atakiem cybernetycznym na infrastrukturę agresora,
- napastnik nie jest znany, możliwe jest zidentyfikowanie tylko adresu IP, a zaatakowane państwo, posługując się narzędziami hakerskimi, dokonuje przejęcia kontroli nad twardym dyskiem i np. niszczy zapisane tam dane,
- napastnik w ogóle nie jest identyfikowany, co oznacza, że państwo (ofiara) nie wie, przez kogo zostało zaatakowane, i nie wie, przeciw komu wymierzyć działania odwetowe.

Reakcje zbrojne na ataki cybernetyczne są już przewidywane w strategiach państw. Na przykład Stany Zjednoczone zastrzegają sobie prawo do reakcji na tego typu zagrożenia wszelkimi koniecznymi i odpowiednimi środkami[30]. W polskim ustawodawstwie ataki z cyberprzestrzeni zostały potraktowane na równi ze zbrojną napaścią na terytorium Rzeczpospolitej Polskiej czy atakami terrorystycznymi jako zagrożenie zewnętrzne państwa uzasadniające wprowadzenie stanu wojennego[31].

Czy tego typu działania pozostają w zgodzie z prawem międzynarodowym? O ile kazus Polski jest poza sporem (wprowadzenie stanu wojennego nie oznacza podjęcia działań zbrojnych), o tyle możliwości podjęcia odwetu o charakterze stricte militarnym

---

na obejmuje następujące systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe; zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i telekomunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Zob. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (tekst jednolity: Dz.U. z 2013 r. poz. 1166).

[29] Zob. P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako…*, s. 90.

[30] *International Strategy for Cyberspace. Prosperity, Security and Openess in the Networked World* [online], May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [dostęp: 23 IV 2012].

[31] Art. 2 ust. 1 *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. z 2014 r. poz. 1815 dla ustawy: Dz.U. z 2002 r. Nr 156 poz. 1301). Ust. 1a przywołanej ustawy precyzuje, że przez zewnętrzne zagrożenie państwa, o którym mowa w ust. 1, rozumie się celowe działania godzące w niepodległość, niepodzielność terytorium, ważny interes gospodarczy Rzeczpospolitej Polskiej lub zmierzające do uniemożliwienia albo poważnego zakłócenia normalnego funkcjonowania państwa, podejmowane przez podmioty zewnętrzne w stosunku do niej. Analogiczne rozwiązanie znalazło się także w *Ustawie z dnia 21 czerwca 2001 r. o stanie wyjątkowym* (tekst jednolity: Dz.U. z 2014 r. poz. 1191); art. 2 ust. 1 tej ustawy stanowi, że w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte przez zastosowanie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu wniosku dotyczącego wprowadzenia stanu wyjątkowego do Prezydenta Rzeczpospolitej Polskiej.

czy jedynie cybernetycznym wywołują wątpliwości. Nie jest bowiem jasne (przynajmniej nie wynika to dobitnie z obowiązującego prawa międzynarodowego), czy atak cybernetyczny na infrastrukturę krytyczną można uznać za uzasadnienie do podjęcia działań w trybie art. 51 Karty Narodów Zjednoczonych (samoobrona), a zatem – działań zbrojnych w samoobronie. Bez wątpienia musiałby to być atak poważny, tj. nie incydent, lecz działanie pociągające za sobą znaczne straty w sferze materialnej i ofiary w ludziach (np. doprowadzenie do wybuchu elektrowni jądrowej[32]). Konsekwencją tego byłoby uznanie takiego ataku za napaść zbrojną, a co najmniej za zagrożenie międzynarodowego pokoju i bezpieczeństwa. W dzisiejszym stanie prawnym mogłaby to uczynić jedynie Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych, tak jak się to stało po zamachach z 11 września 2001 r. odnośnie do ataków terrorystycznych.

Reakcja zaatakowanego państwa polegająca na przeprowadzeniu odwetowego ataku cybernetycznego należałaby do tzw. kontrśrodków (*countermeasures*), zwanych niegdyś represaliami. Przy ich stosowaniu należy zachować zasadę proporcjonalności środka odwetowego do dokonanego naruszenia i zamierzonego celu, a przed ich uruchomieniem państwo pokrzywdzone powinno wystąpić z roszczeniem reparacji. W doktrynie prawa międzynarodowego podkreśla się, że represalia jako środki odwetowe polegają na tymczasowym zawieszeniu stosowania określonej normy prawa międzynarodowego przez państwo poszkodowane, podejmowanym w odpowiedzi na działania sprzeczne z prawem międzynarodowym innego państwa. W normalnej sytuacji środki użyte jako represalia pozostają w sprzeczności z prawem międzynarodowym, a jedynie uprzednie działanie innego państwa uzasadnia sięgnięcie po nie w odwecie. Zastosowane represalia nie mogą jednak naruszać zakazu groźby lub użycia siły, fundamentalnych praw człowieka, zobowiązań o charakterze humanitarnym i innych zobowiązań wynikających z norm peremptoryjnych (tj. norm typu *iuris cogentis*, bezwzględnie obowiązujących) powszechnego prawa międzynarodowego[33].

Trzeci przypadek hipotetycznego ataku niezwykle trudno klasyfikować na gruncie prawa międzynarodowego. Tego typu atak nosiłby raczej charakter przestępstwa konwencyjnego, a opisana reakcja państwa jest bardzo trudna do klasyfikacji prawnomiędzynarodowej.

Poruszone problemy wymagają pilnego rozwiązania. Trudno bowiem zgodzić się na dyktat ze strony sił nieuznających żadnych reguł prowadzenia konfliktu, w tym zbrojnego. Trudno też dopuszczać do sytuacji, w której państwa są zmuszone łamać obowiązujące prawo międzynarodowe. Stosowanie wspomnianej kilkakrotnie zasady „konieczność nie zna prawa" to prosta droga do degradacji roli prawa międzynarodowego i tym samym – anarchizacji stosunków międzynarodowych. Ta zasada może zostać uznana jedynie za wyjątek w sytuacjach nadzwyczajnych, wymagających szybkiego i zdecydowanego rozwiązania. Nigdy natomiast nie powinna znaleźć się w zbiorze podstawowych zasad prawa międzynarodowego.

---

[32] Taka próba została podjęta wobec irańskiej elektrowni jądrowej i polegała na przejęciu kontroli nad systemami sterowania za pomocą złośliwego programu (robaka) Stuxnet. Ostatecznie okazała się nieudana; nie wiadomo też, czy jej celem było wywołanie niekontrolowanej reakcji łańcuchowej i wybuchu, choć nie można takiej możliwości wykluczyć. Zob. K. Pielesiek, *Światowa cyberwojna – nie zobaczysz jej w telewizji*, Gazeta pl. Technologie [online], 19 IV 2012, http://technologie.gazeta.pl/internet/1,104530,11557651,Swiatowa_cyberwojna_nie_zobaczysz_jej_w_telewizji.html [dostęp: 19 IV 2012].

[33] Zob. J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2007, s. 10–13, 465–467; por.: W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2004, s. 661–664.

Pierwsze próby rozwiązania tego problemu zostały już podjęte. W 2009 r. NATO Cooperative Cyber Defence Center of Excellence (NATO CCD COE) zaprosiło grupę ekspertów prawa międzynarodowego do prac nad określeniem prawnych ram prowadzenia wojny w cyberprzestrzeni. Głównym zadaniem zespołu ekspertów było określenie sposobu zastosowania obowiązujących norm prawa międzynarodowego – zarówno w zakresie *ius ad bellum*, jak i *ius in bello* – do nowego środowiska walki, jakim stała się cyberprzestrzeń. Innymi słowy – dokonanie prawnomiędzynarodowej analizy cyberprzestrzeni i zjawisk w niej zachodzących. Autorzy pomysłu wzorowali się na projektach, których wynikami są *Manual on International Law Applicable to Armed Conflicts at Sea*[34] oraz *Manual on International Law Applicable to Air and Missile Warfare*[35].

Zadanie okazało się bardzo trudne, by nie powiedzieć – karkołomne. Oba opracowania powstały na przełomie stuleci, a więc w sytuacji, w której morskie i powietrzne środowiska walki były znane już od dziesiątków lat, gdy istniały już normy prawa międzynarodowego – zarówno umownego, jak i zwyczajowego – znajdujące do nich bezpośrednie zastosowanie oraz praktyka, orzecznictwo i bogata doktryna. W przypadku cyberprzestrzeni zachodzi diametralnie inna sytuacja. Ta przestrzeń jest stosunkowo nowym środowiskiem, nie tyle przez człowieka opanowywanym (jak w przypadku przestrzeni powietrznej i obszarów morskich), ile stworzonym, o zupełnie innych cechach – brakuje tu zarówno norm prawa międzynarodowego regulujących jej funkcjonowanie jako środowiska walki, jak i norm odnoszących się do środków i metod walki prowadzonej w jej ramach. Nie istnieje orzecznictwo, a doktryna dopiero zaczyna się tworzyć. Z punktu widzenia przedmiotu badań zespół poruszał się zatem w swoistej próżni prawnej[36].

Z rozwojem prawa międzynarodowego ma się do czynienia wówczas, gdy społeczność międzynarodowa zaczyna funkcjonować w nowych środowiskach lub też gdy napotyka na nowe wyzwania i zagrożenia. Konieczne stają się wtedy również nowe regulacje. Jako klasyczne przykłady takich sytuacji można uznać choćby powstanie i rozwój międzynarodowego prawa morza, międzynarodowego prawa lotniczego i kosmicznego oraz np. powstanie w ramach systemu ONZ wielu konwencji dotyczących zwalczania terroryzmu międzynarodowego. Można w tym zakresie wskazać dwa generalne sposoby: kodyfikację istniejących norm prawa zwyczajowego i ich rozwój lub tworzenie nowych norm konwencyjnych.

Zespół ekspercki NATO CCD COE poszedł inną drogą, a mianowicie dokonał interpretacji obowiązujących norm prawa międzynarodowego, dążąc do ustalenia: czy, które z nich i w jaki sposób można zastosować do sfery cyberprzestrzeni. Wynikiem tych prac stał się *Tallinn Manual on the International Law Applicable to Cyber Warfare*[37].

Twórcy *Tallinn Manual…* za punkt wyjścia przyjęli koncepcję suwerenności terytorialnej państwa. Rzecz jasna, trudno odnieść ją do cyberprzestrzeni jako takiej, znaj-

[34] http://www.icrc.org/ihl/385ec082b509e76c41256739003e636d/7694fe2016f347e1c125641f002d49ce [dostęp: 8 V 2013].

[35] http://www.ihlresearch.org/amw/manual/ [dostęp: 8 V 2013].

[36] Zob. na ten temat: T. Aleksandrowicz, *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, s. 39 i nast.

[37] *Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts by the Invitation of the NATO Cooperative Cyber Defence Center of Excellence*, M.N. Schnitt (general editor), Cambridge 2013. Tekst dostępny również na stronach internetowych NATO CCD COE – http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=window [dostęp: 8 V 2013].

duje ona jednak zastosowanie do infrastruktury (tj. serwerów, komputerów itp.) znajdujących się na terytorium państwa, które ponosi odpowiedzialność za ich bezpieczeństwo i wykorzystanie zgodne z prawem międzynarodowym. Stąd i jurysdykcja państwa – wobec sprawców przebywających na jego terytorium oraz wobec czynów dokonanych przeciwko infrastrukturze znajdującej się na jego terytorium – i tzw. jurysdykcja eksterytorialna, która jest ustanawiana w związku z narodowością sprawcy, narodowością ofiary, naruszeniem bezpieczeństwa narodowego i naruszeniem powszechnie obowiązujących norm prawa międzynarodowego (np. złamanie zakazu agresji czy dokonanie aktu terroryzmu międzynarodowego).

Przyjęcie takiego punktu wyjścia oznacza przyznanie państwu prawa kontroli nad własną cyberprzestrzenią (tj. istniejącą w ramach infrastruktury znajdującej się na jego terytorium), nie może ona bowiem być wykorzystywana do działań wrogich przeciwko innemu państwu. Państwo ponosi prawnomiędzynarodową odpowiedzialność za cyberoperacje naruszające prawo międzynarodowe, które mogą być mu przypisane. Sam fakt, że takie operacje zostały przeprowadzone z rządowej infrastruktury nie jest jednak traktowane jako wystarczający dowód do przypisania ich danemu państwu.

Drugim założeniem jest uznanie, że cyberoperacja może być traktowana jako użycie siły w rozumieniu Karty Narodów Zjednoczonych wówczas, gdy jej skutki są porównywalne z konwencjonalnym użyciem siły, a więc ze stratami fizycznymi (utrata życia lub zdrowia przez ludzi, straty materialne). Konsekwencją takiego stanowiska jest uznanie, że tzw. operacje niedestrukcyjne (np. propagandowe czy szpiegowskie) nie mieszczą się w kategoriach użycia siły. Jeśli przynoszą skutki fizyczne, to podlegają obowiązującemu prawu międzynarodowemu regulującemu kwestie *ius ad bellum*. Mają do nich zatem zastosowanie normy dotyczące agresji, zakazu użycia siły i samoobrony w trybie art. 51 Karty Narodów Zjednoczonych. Równocześnie, jeśli cyberoperacje spełniają kryterium użycia siły i są prowadzone w ramach konfliktu zbrojnego, podlegają międzynarodowemu prawu konfliktów zbrojnych, czyli *ius in bello*.

Konsekwencją przyjęcia takiego rozwiązania jest zastosowanie do aktów cyberwojny obowiązujących przepisów *ius in bello*, dotyczących np. udziału w działaniach zbrojnych, statusu kombatanta, ochrony ludności cywilnej i dóbr kultury. Analogicznie do *ius ad bellum*, także w *ius in bello* za kryterium przyjęto konsekwencje ataku. Tak więc za atak cybernetyczny uznaje się taką operację w cyberprzestrzeni, co do której można zasadnie przypuszczać, że spowoduje śmierć lub uszkodzenie ciała osób, szkody lub zniszczenie obiektów fizycznych (np. atak na systemy sterujące siecią energetyczną, których konsekwencją jest wybuch pożaru).

Wyniki pracy twórców *Tallinn Manual…* bez wątpienia zasługują na uznanie. Stanowią one doktrynalną wykładnię obowiązujących norm prawa międzynarodowego, pozwalającą na zastosowanie obowiązujących norm do nowej sytuacji i nowych zjawisk, jakie pojawiły się w związku z rozwojem współczesnych technologii informacyjnych. Trudno jednak uznać, że rozważania i propozycje zawarte w omawianym opracowaniu rozwiązują istniejący problem.

Po pierwsze mamy do czynienia z doktryną prawa międzynarodowego, a nie z jego źródłem. Przyjęcie prezentowanych powyżej interpretacji nie musi znaleźć odbicia ani w praktyce międzynarodowej państw, ani w orzecznictwie sądów międzynarodowych. Po drugie normy prawa międzynarodowego regulują m.in. kwestie odpowiedzialności państw i osób fizycznych za naruszenia prawa (np. agresję i zbrodnie wojenne). W takim przypadku nie jest możliwe uznanie odpowiedzialności przez ana-

logię, wymagana jest konkretna norma pozwalająca na wyegzekwowanie tej odpowiedzialności. Po trzecie cechy cyberprzestrzeni jako środowiska walki są na tyle specyficzne, że wymagają stworzenia norm prawa międzynarodowego uwzględniających tę specyfikę. Cyberprzestrzeń pozwala na przeprowadzenie np. ataku anonimowego, a przynajmniej takiego, który aby zidentyfikować napastnika, będzie wymagać określonego czasu. Jak w takim razie zastosować przepisy dotyczące kontrśrodków czy samoobrony? Należy też wskazać, że cyberprzestrzeń niejako zrównuje pozycję państwa z pozycją i możliwościami podmiotów niepaństwowych.

Chociaż z formalnego punktu widzenia *Tallinn Manual…* jest klasyczną formą rozważań *te lege lata*, to jednak – mając na uwadze rozwój prawa międzynarodowego, perspektywy rozwoju technologicznego oraz skalę i potencjalne konsekwencje cyberkonfliktów – wypada postulować traktowanie go jako uwag *de lege ferenda*, a zatem uznać za podstawę działań zmierzających do wykreowania nowych norm prawa międzynarodowego regulujących cybernetyczne aspekty *ius ad bellum* i *ius in bello*[38].

Podsumowanie

Powstanie i rozwój społeczeństwa informacyjnego przyniosły ze sobą – poza bezspornymi korzyściami – także wiele zagrożeń bezpieczeństwa państwa i jego obywateli. Większość z nich jest związana z rozwojem cyberprzestrzeni, a także z coraz większą i dziś już zasadniczą rolą informacji, rozumianą jako zasób strategiczny. Nic zatem dziwnego, że te zagrożenia sytuują się w kategorii walki informacyjnej.

Rodzi to nowe wyzwania dla służb odpowiedzialnych za bezpieczeństwo państwa. Podejmując walkę informacyjną w cyberprzestrzeni, muszą one mieć zdolności zarówno defensywne, jak i ofensywne, a zatem – innymi słowy – także zdolności do odstraszania potencjalnego napastnika, niezależnie od tego, czy mamy do czynienia z atakiem cybernetycznym ze strony państwa, podmiotu pozapaństwowego, czy stoimy wobec przestępstwa szpiegostwa w cyberprzestrzeni, czy też mamy do czynienia z przestępcą wykorzystującym nowoczesne technologie komunikacyjne.

Z punktu widzenia służb specjalnych stanowi to nie lada problem. Widać bowiem wyraźnie, że prawo z trudnością nadąża za przebiegającą dynamicznie rewolucją naukowo-techniczną. To poważny problem, gdyż służby specjalne demokratycznego państwa prawnego, jakim jest Rzeczpospolita Polska, muszą działać na podstawie i w granicach prawa. Zasadna wydaje się propozycja przeprowadzenia gruntownej analizy zmian warunków, w jakich przyszło działać polskim służbom specjalnym, aby na tej podstawie sformułować propozycje zmian w obowiązującym prawie uwzględniających realia współczesnego środowiska bezpieczeństwa.

Bibliografia:

Publikacje zwarte:

1. Aleksandrowicz T., *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, Difin.

[38] Zob. na ten temat: T. Aleksandrowicz, *Świat w sieci…*, s. 168 i nast.

2. Aleksandrowicz T., *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, Difin.
3. Arguilla J., Ronfeldt D., *Cyberwar is Coming!*, w: *In Athena's Camp:Preparing for Conflict in the Information Age,* Santa Monica 1993, RAND; http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [dostęp: 6 IV 2012].
4. Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, Scholar.
5. Barcik J., Srogosz T., *Prawo międzynarodowe publiczne*, Warszawa 2007, C.H. Beck.
6. Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, ASPRA-JR.
7. Czapliński W., Wyrozumska A., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2004, C.H. Beck.
8. Gibson W., *Neuromancer*, Poznań 1999, Książnica.
9. Głowacka D., *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji* [online], http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf [dostęp: 3 VII 2014].
10. Lichocki E., *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP*, Warszawa 2009, AON (rozprawa doktorska).
11. Liedel K., *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, Difin.
12. Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17, s. 15–28.
13. Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, PISM.
14. Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, Difin.
15. Pacek B., Hoffman R., *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, AON.
16. Pielesiek K., *Światowa cyberwojna – nie zobaczysz jej w telewizji*, Gazeta pl. Technologie [online], 19 IV 2012, http://technologie.gazeta.pl/internet/1,104530,11557651,Swiatowa_cyberwojna_nie_zobaczysz_jej_w_telewizji.html [dostęp: 19 IV 2012].
17. Sienkiewicz P., *Wizje i modele wojny informacyjnej* [online], s. 373–374, http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf [dostęp: 5 IV 2012].
18. Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, PISM.
19. Tekielska P., Czekaj Ł., *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (red.), Warszawa 2014, Difin.

Akty prawne:

1. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137).
2. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (tekst jednolity: Dz.U. z 2013 r. poz. 1166).

3. *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* (tekst jednolity: Dz.U. z 2014 r. poz. 1815 dla ustawy: Dz.U. z 2002 r. Nr 156 poz. 1301).
4. *Ustawa z dnia 21 czerwca 2001 r. o stanie wyjątkowym* (tekst jednolity: Dz.U. z 2014 r. poz. 1191).
5. *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* (tekst jednolity: Dz.U. z 2014 r. poz. 1815. ze zm.).
6. *Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r*. (Dz.U. z 2014 r. poz. 1514).
7. *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiS* (Dz.Urz. UE L 218 z 14 VIII 2013 r.).
8. *Convention of Cybercrime* [online], Budapest, 23 XI 2001 r., European Treaty Series nr 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [dostęp: 3 VII 2014].
9. *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy* [online], April 2011: *Cyberspace is the interdependent network of information technology components that underpins many of our communications; the Internet is one component of cyberspace,* http://www.hsdl.org/?view&did=7010 [dostęp: 15 III 2012].
10. *The National Strategy to Secure Cyberspace* [online], February 2003, http://www.hsdl.org/?view&did=1040 [dostęp: 15 III 2012].
11. *International Strategy for Cyberspace. Prosperity, Secirity, and Openess in a Networked World* [online], May 2011, http://www.hsdl.org/?view&did=5665 [dostęp: 15 III 2012].
12. *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia* [online], Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Bruksela 1 VI 2005, COM(2005) 229 końcowy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PL:PDF [dostęp: 5 IV 2012].
13. *Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts by the Invitation of the NATO Cooperative Cyber Defence Center of Excellence*, M.N. Schnitt (general editor), Cambridge 2013. Tekst dostępny również na stronach internetowych NATO CCD COE, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=window [dostęp: 8 V 2013].

Abstrakt

Artykuł jest poświęcony analizie zagrożeń w cyberprzestrzeni odnoszących się do bezpieczeństwa państwa. Autor bada ten problem z punktu widzenia prawa międzynarodowego publicznego oraz prawa Unii Europejskiej i polskiego prawa karnego.

Na podstawie przeprowadzonej analizy autor stwierdza, że walka informacyjna toczona w cyberprzestrzeni rodzi nowe wyzwania dla służb odpowiedzialnych za bezpieczeństwo państwa, które, operując w tej sferze, muszą mieć zdolności zarówno defensywne, jak i ofensywne. Jednocześnie trzeba zauważyć, że prawo z trudem nadąża za dynamicznie przebiegającą rewolucją naukowo-techniczną. To poważny problem, gdyż służby specjalne demokratycznego państwa prawnego, jakim jest Rzeczpospolita Polska, muszą działać na podstawie i w granicach prawa. Zasadna wydaje się propozycja przeprowadzenia gruntownej analizy zmian warunków, w jakich przyszło działać polskim służbom specjalnym, aby na tej podstawie sformułować propozycje zmian w obowiązującym prawie, które uwzględnia realia współczesnego środowiska bezpieczeństwa.

Słowa kluczowe: cyberprzestrzeń, prawo międzynarodowe, walka informacyjna.

Abstract

The paper treats cyberspace as a source of threats for national security. The Author analyses this issue from the point of view of international public law, European Union law and polish penal code. The Author states that information war in cyberspace creates new challenges for the institutions responsible for the national security. Those institutions should have both offensive and defensive capabilities. On the other hand the Author recommends changes in the contemporary law according to the changes in the security environment.

Keywords: cyberspace, international law, information warfare.

Sławomir Gładysz

Agencja Bezpieczeństwa Wewnętrznego w systemie ochrony obrotu strategicznego

Istotnymi elementami właściwości rzeczowej Agencji Bezpieczeństwa Wewnętrznego w zakresie operacyjno-procesowym są przeciwdziałanie szeroko rozumianej proliferacji broni masowego rażenia oraz analiza ryzyka dla Polski w zakresie obrotu strategicznego. Wskazują one na konieczność ścisłej współpracy ABW z różnymi podmiotami państwowymi, szczególnie z właściwymi jednostkami organizacyjnymi Ministerstwa Gospodarki, Ministerstwa Spraw Wewnętrznych, Służby Celnej i innych organów. Z uwagi na to, że tematyka dotycząca obrotu strategicznego obejmuje najczęściej transfer międzynarodowy, ta współpraca dotyczy również pozostałych służb specjalnych uprawnionych do prowadzenia czynności operacyjnych, tj. Służby Kontrwywiadu Wojskowego, Agencji Wywiadu i Służby Wywiadu Wojskowego.

Zadania Agencji Bezpieczeństwa Wewnętrznego w powyższym zakresie normuje art. 5 ust. 1 pkt 2 lit. d ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[1], który określa obszar rozpoznania, zapobiegania i wykrywania przestępstw (…) *w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa*. Systemowo ten przepis łączy się m.in. z ustawą z 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa[2] (dalej: ustawa o obrocie strategicznym) oraz z ustawą z 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym[3] (dalej: ustawa o obrocie specjalnym). Ustawy te są wkomponowane w system prawa unijnego, które określa ramy i główne kierunki, jakimi powinny się kierować kraje członkowskie UE w wewnętrznym procesie legislacyjnym.

Wskazane akty prawne regulują i reglamentują produkcję określonych towarów i technologii oraz obrót nimi, a także ustanawiają nad nimi rodzaj szczególnej kontroli i nadzoru państwowego w postaci konieczności uzyskania zezwoleń lub koncesji. Swoimi zapisami przydzielają także określone role centralnym organom administracji rządowej, tj. właściwym ministrom i szefom służb specjalnych. Ponadto wprowadzają odpowiedzialność karną za niezgodny z prawem obrót wyżej wymienionymi dobrami oraz za wykonywanie działalności gospodarczej.

I. Przepisy Unii Europejskiej

Podstawowymi aktami prawnymi ustanawiającymi ogólne reguły dotyczące obrotu o znaczeniu strategicznym dla bezpieczeństwa państw członkowskich UE są *Rozporządzenie Rady (WE) nr 428/2009 z dnia 5 maja 2009 r. ustanawiające wspólnotowy*

[1] Tekst jednolity: Dz.U. z 2015 r. poz. 1929, ze zm.
[2] Tekst jednolity: Dz.U. z 2013 r. poz. 195, ze zm.
[3] Tekst jednolity: Dz.U. z 2012 r. poz. 1017, ze zm.

system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania[4] oraz *Wspólne stanowisko Rady 2008/944/WPZiB z dnia 8 grudnia 2008 r. określające wspólne zasady kontroli wywozu technologii wojskowych i sprzętu wojskowego*[5]. Działania Rady opierają się m.in. na strategii UE przeciw rozprzestrzenianiu broni masowego rażenia przyjętej 12 grudnia 2003 r.[6] Jej założenia nakładają na Unię Europejską obowiązek wykorzystania wszelkich możliwych instrumentów w celu zapobiegania powstawaniu programów dotyczących proliferacji, odstraszania przed podejmowaniem takich inicjatyw, powstrzymywania niekontrolowanego przemieszczania produktów strategicznych i eliminowania zagrożeń oraz stwierdzonych bezprawnych zachowań. Oprócz ustawodawstwa unijnego kwestię wdrożenia właściwych systemów kontrolnych zawiązanych z zapobieganiem rozprzestrzenianiu się broni jądrowej, chemicznej i biologicznej oraz środków ich przenoszenia, podniosła także Organizacja Narodów Zjednoczonych w rezolucji Rady Bezpieczeństwa ONZ przejętej w 2004 r.[7]

1. *Rozporządzenie Rady (WE) nr 428/2009 z dnia 5 maja 2009 r. ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania*

Zasady przyjęte w *Rozporządzeniu Rady nr 428/2009* stanowią szkielet wspólnie utrwalonych rozwiązań, które winny być szczegółowo doprecyzowane przez ustawodawstwo krajowe. W tym celu Wspólnota zobowiązała państwa członkowskie do podjęcia kroków przyznających właściwym organom odpowiednie uprawnienia, które umożliwiają stosowanie przepisów *Rozporządzenia*. Ograniczeniami w polskiej legislacji są zasady polityki handlowej wynikające ze wspólnych reguł wywozu[8] przyjętych w UE oraz zasady celne zawarte we *Wspólnotowym Kodeksie Celnym*[9], szczególnie w zakresie definicji wywozu i powrotnego wywozu oraz uprawnień przyznanych mocą tego aktu.

Głównym postulatem Rady WE odnoszącym się do obrotu o znaczeniu strategicznym jest skuteczna kontrola podczas wywozu towarów o podwójnym zastosowaniu oraz uzbrojenia poza obszar celny Unii Europejskiej. Elementami tej kontroli są wspólne wykazy produktów podwójnego zastosowania oraz ich miejsc przeznaczenia. Na uwagę zasługuje tu doprecyzowanie umieszczone wśród zasad ogólnych, mówiące o tym, że przekazywanie oprogramowania i technologii za pomocą mediów elektronicznych, faksu lub telefonu do miejsc przeznaczenia poza UE również powinno być objęte kontrolą.

---

[4] Dz.U. UE L z 29 V 2009 r. Pierwotnym aktem prawnym było *Rozporządzenie Rady (WE) nr 1334/2000 z dnia 22 czerwca 2000 r. ustanawiające wspólnotowy system kontroli eksportu produktów i technologii podwójnego zastosowania*.

[5] Dz.U. UE L z 13 XII 2008 r. nr 335 poz. 99 – dalej: *Wspólne stanowisko Rady*.

[6] Dalej: strategia UE BMR. Zainicjowana w czerwcu 2003 r. w Salonikach, gdzie przyjęto plan działania przeciw rozprzestrzenianiu broni masowego rażenia. Zgodnie z zapisami planu państwa członkowskie miały przeprowadzić wzajemną ocenę kontroli wywozu towarów strategicznych. W dniu 13 XII 2003 r. Rada wydała oświadczenie, w którym przedstawiła zalecenia wynikające z wyżej wymienionej oceny i podkreśliła wagę problemu. Wykonanie tych zaleceń stało się priorytetem Grupy Roboczej ds. Towarów Podwójnego Zastosowania.

[7] Rezolucja Rady Bezpieczeństwa ONZ nr 1540 z 28 IV 2004 r.

[8] *Rozporządzenie Rady (WE) nr 1061/2009 ustanawiające wspólne reguły wywozu* (Dz.U. UE L z 2009 r. nr 291 poz. 1).

[9] *Rozporządzenie Rady (EWG) nr 2913/92 z dnia 12 października 1992 r. ustanawiające „Wspólnotowy Kodeks Celny"* (Dz.U. UE L z 1992 r. nr 302 poz. 1).

Wynika z tego chęć szerokiego potraktowania określenia produkty podwójnego zastosowania obejmująca zarówno towary oraz usługi, jak i procedury *know-how* umożliwiające ich wytwarzanie, modyfikację itp.[10]

O szerokim rozumieniu określenia obrót towarami podwójnego zastosowania świadczy również zobowiązanie państw członkowskich do objęcia szczególną uwagą kwestii powrotnego wywozu[11] i końcowego zastosowania przedmiotu kontrolowanej transakcji. Rozwinięciem powyższego jest także kontrola świadczenia usług pośrednictwa, szczególnie w sytuacji, gdy pośrednik został poinformowany przez organy krajowe lub jest świadomy, że pośrednictwo mogłoby skutkować produkcją lub dostarczeniem broni masowego rażenia w państwie trzecim.

W ramach takiego ujęcia obrotu towarami podwójnego zastosowania przyjęto zasadę wprowadzającą konieczność zabezpieczania się państw członkowskich przed niekontrolowanym tranzytem niewspólnotowych produktów podwójnego zastosowania przez wprowadzenie jego zakazu. Taki zakaz byłby możliwy w sytuacji, gdyby właściwe organy krajowe miały uzasadnione powody[12] do podejrzeń, że tego typu produkty mogą być w całości lub części przeznaczone do rozprzestrzeniania broni masowego rażenia lub środków jej przenoszenia.

W *Rozporządzeniu nr 428/2009*, w celu jednolitego i konsekwentnego stosowania kontroli w całej Unii Europejskiej, zalecono rozszerzenie zakresu konsultacji między państwami członkowskimi przed udzieleniem zezwolenia na wywóz. Te konsultacje umożliwiłyby realizację krajowej polityki bezpieczeństwa, uwzględniającej szczególnie specyfikę danego państwa, regionu oraz rodzaju towaru o podwójnym zastosowaniu.

Postulat jednolitego i konsekwentnego sposobu dokonywania kontroli jest realizowany także przez dążenie do zbieżności warunków przeprowadzania krajowej kontroli produktów podwójnego zastosowania oraz warunków udzielania i wykorzystywania różnych rodzajów zezwoleń. Do konieczności bieżącego uzupełniania prawa w zakresie poprawy skuteczności kontroli zalicza się także dążenie do bardziej precyzyjnego zdefiniowania niematerialnych transferów technologii, obejmujące również udostępnianie kontrolowanych technologii podmiotom zlokalizowanym poza obszarem celnym UE.

Narzędziem do egzekwowania zapisów *Rozporządzenia nr 428/2009* i uszczegóławiających je przepisów krajowych mają być skuteczne, proporcjonalne i odstraszające kary. Oznacza to penalizację zachowań sprzecznych z postanowieniami wymienionych aktów prawnych.

Konstrukcja części szczegółowej *Rozporządzenia...* składa się z rozdziału prezentującego definicje podstawowych pojęć[13] używanych w literaturze przedmiotu, zakres stosowania rozporządzenia, wyszczególnienie rodzajów zezwoleń na obrót towarami strategicznymi oraz zasady współpracy międzynarodowej, w tym konsultacji i bieżącej wymiany informacji pomiędzy państwami członkowskimi.

W załącznikach nr I[14] i IV wymieniono produkty podwójnego zastosowania podlegające kontroli przy wywozie poza obszar celny UE oraz w przypadku transferu wewnątrzunijnego. Ten wykaz nie jest zamknięty – przewidziano jego stałą aktualizację.

[10] Jak się wydaje, warunkiem powyższego jest niekontrolowany wypływ wyżej wymienionych informacji z terytorium WE do państw trzecich.

[11] Reeksport.

[12] Te podejrzenia winny się opierać na (…) *podstawie źródeł wywiadowczych lub innych*, co daje szerokie możliwości zweryfikowania danej informacji.

[13] Szczegółowo zostaną omówione w dalszej części, s. 7.

[14] Wykaz sporządzony z uwzględnieniem wymogów i zobowiązań przyjętych przez państwa członkowskie stosujące odpowiednie międzynarodowe systemy nierozprzestrzeniania broni. Zob. porozumienie z Wassenaar, Reżim Kontrolny Technologii Rakietowych, Grupa Dostawców Sprzętu Jądrowego, Grupa Australijska i inne.

Co więcej, dane państwo członkowskie może zabronić[15] wywozu towarów podwójnego zastosowania, które nie są wymienione w powyższych załącznikach, lub też wymagać zezwolenia na ich wywóz.

Pozostałe załączniki określają wzór formularza obowiązującego przy wydawaniu zezwoleń krajowych, globalnych i indywidualnych, w tym także na usługi pośrednictwa.

Rozporządzenie, o którym mowa, ustanawia wymóg posiadania zezwolenia na wszystkie produkty wymienione w załączniku nr I, a także na produkty niewymienione w wykazie, które mogą mieć zastosowanie w związku z bronią masowego rażenia lub bronią konwencjonalną, jeśli te rodzaje broni mają być wywiezione na obszar objęty embargiem na broń[16]. Przesłanką do objęcia danego produktu klauzulą ogólną jest jego częściowe lub całkowite końcowe zastosowanie w wojskowości[17].

Jak wskazano wcześniej, również pośredniczenie w obrocie produktami *dual use* jest objęte wymogiem posiadania zezwolenia. Podkreślenia wymaga nacisk położony na „świadomość pośrednika", że realizuje usługi dotyczące produktów podwójnego zastosowania.

Kolejnym rodzajem operacji handlowej wskazanym w zapisach *Rozporządzenia...* jest tranzyt niewspólnotowych produktów podwójnego zastosowania. Właściwe organy państwa mają prawo zakazać takiego tranzytu bądź wymagać na niego zezwolenia. Ten zakaz może być rozszerzony na produkty niewymienione w załączniku nr I oraz na produkty przeznaczone do zastosowania w wojskowości.

Rozporządzenie Rady nr 428/2009 wprowadza kilka rodzajów zezwoleń:

1. **Generalne unijne zezwolenie na wywóz, obowiązujące na terytorium całej Unii Europejskiej**. Jest ono skierowane do eksporterów wysyłających towary do sześciu grup następujących odbiorców:
   - Australia, Kanada, Japonia, Nowa Zelandia, Norwegia, Szwajcaria (wraz z Liechtensteinem), Stany Zjednoczone Ameryki[18];
   - Argentyna, Chorwacja, Islandia, Republika Południowej Afryki, Korea Południowa, Turcja[19];
   - Albania, Argentyna, Bośnia i Hercegowina, Brazylia, Chile, Chiny (wraz z Hongkongiem i Makao), Chorwacja, Republika Macedonii, francuskie terytoria zamorskie, Islandia, Indie, Kazachstan, Meksyk, Czarnogóra, Maroko, Rosja, Serbia, Singapur, Republika Południowej Afryki, Korea Południowa, Tunezja, Turcja, Ukraina, Zjednoczone Emiraty Arabskie[20];
   - Argentyna, Albania, Chorwacja, Bośnia i Hercegowina, Brazylia, Chile, Chiny (wraz z Hongkongiem i Makao), Republika Macedonii, francuskie terytoria zamorskie, Republika Korei, Islandia, Indie, Kazachstan, Meksyk, Czarnogóra, Maroko, Rosja, Serbia, Singapur, Republika Południowej Afryki, Tunezja, Turcja, Ukraina, Zjednoczone Emiraty Arabskie[21];

[15] Ze względów bezpieczeństwa publicznego lub praw człowieka.

[16] Tzw. klauzula ogólna.

[17] Oznacza to występowanie produktu w wykazie uzbrojenia danego państwa członkowskiego, a także wykorzystanie go do udoskonalania produkcji lub konserwacji produktów wojskowych i użycie produktu do wytwarzania produktów wojskowych.

[18] Wszystkie produkty wymienione w wykazie, z wyjątkiem (w najszerszym znaczeniu) materiałów rozszczepialnych, technologii jądrowej, ludzkich i zwierzęcych czynników chorobotwórczych oraz technologii rakietowej.

[19] Niektóre produkty podwójnego zastosowania.

[20] W sytuacji powrotnego wywozu, gdy odbywał się on na podstawie generalnego zezwolenia unijnego lub krajowego i gdy produkt został ponownie przywieziony w celu konserwacji, naprawy lub wymiany. Zakres zezwolenia wyłącza produkty wymienione enumeratywnie.

[21] W przypadku czasowego wywozu na wystawy lub targi oraz przy założeniu, że produkty ponownie

– Argentyna, Chiny (wraz z Hongkongiem i Makao), Chorwacja, Indie, Republika Korei, Rosja, Republika Południowej Afryki, Turcja, Ukraina[22];
– Argentyna, Chorwacja, Islandia, Republika Korei, Turcja, Ukraina[23].

Ten rodzaj zezwolenia obejmuje wyłącznie transakcje niskiego ryzyka.

2. **Zezwolenia krajowe: globalne, generalne i indywidualne**. Jeżeli chodzi o wywóz wszystkich innych produktów wymagających zezwolenia, to Rada pozostawiła ostateczną decyzję organom krajowym, które rozstrzygają o udzielaniu takich zezwoleń. Te dokumenty mogą być wykorzystywane przez wszystkich eksporterów mających siedzibę na terytorium państwa członkowskiego po spełnieniu stosownych warunków. Co do zasady nie obejmują one produktów związanych z materiałami rozszczepialnymi, technologią jądrową, ludzkimi i zwierzęcymi czynnikami chorobotwórczymi oraz technologią rakietową.
3. **Zezwolenia na pośrednictwo** – są wydawane na określoną liczbę wskazanych produktów, z zaznaczeniem ich umiejscowienia w państwie trzecim, a także ze wskazaniem użytkownika końcowego i jego lokalizacji.

Właściwe organy państwowe mogą nie przyznać zezwolenia na wywóz, a wydane unieważnić, zawiesić, zmodyfikować lub odwołać.

Powyższe działania nakładają na dane państwo obowiązek realizacji właściwej polityki informacyjnej polegającej na udzielaniu konsultacji i powiadamianiu pozostałych państw członkowskich oraz Komisji o przypadkach wydania odmownych decyzji w sprawie zezwoleń. Wymianę informacji umożliwia system bezpiecznego, szyfrowanego przekazu wiadomości, stworzony przez Komisję.

Szczególną uwagę należy zwrócić na procedurę celną w przypadku wywozu produktu podwójnego zastosowania. To eksporter ma obowiązek dostarczenia dowodu, że posiada właściwe zezwolenie. W razie potrzeby winien też przedstawić tłumaczenie przedłożonych dokumentów na język urzędowy państwa, w którym złożono deklarację eksportową. Istotnym obowiązkiem nałożonym na eksportera jest także konieczność przechowywania dokumentacji dotyczącej transakcji, w tym m.in. ewidencji i rejestrów, dokonanie opisu produktów podwójnego zastosowania, podanie nazwy i adresu przewoźnika oraz nazwy odbiorcy, a wreszcie – końcowego zastosowania produktu i danych użytkownika, jeżeli są one znane.

Na mocy *Rozporządzenia*... została powołana Grupa Koordynacyjna ds. Produktów Podwójnego Zastosowania. Każde z państw członkowskich ma w niej swojego przedstawiciela. Zadaniem Grupy jest badanie wszelkich kwestii związanych ze stosowaniem zapisów *Rozporządzenia*, w tym może ona zasięgać opinii zwłaszcza eksporterów, pośredników i innych zainteresowanych stron.

2. *Wspólne stanowisko Rady 2008/944/WPZiB z dnia 8 grudnia 2008 r. określające wspólne zasady kontroli wywozu technologii wojskowych i sprzętu wojskowego*

Przepisy Wspólnoty dotyczące wyznaczenia reguł związanych z obrotem bronią wyewoluowały do określenia wspólnych zasad kontroli wywozu technologii i sprzętu wojskowego. Tym samym państwa członkowskie uznały szczególną odpowiedzialność

wrócą na obszar celny WE w całości i w niezmienionej postaci w ciągu 120 dni po ich pierwotnym wywozie. Zezwolenie wyłącza produkty wymienione enumeratywnie.

[22] Niektóre produkty z dziedziny telekomunikacji i technologii.

[23] Związki chemiczne wskazane enumeratywnie.

eksporterów tego typu dóbr, a co za tym idzie – zostały zobowiązane do wdrożenia stosownych przepisów legislacyjnych ustanawiających minimalne standardy zarządzania transferem technologii wojskowych oraz działań zapobiegających niekontrolowanemu przepływowi broni.

Podstawą efektywności wdrażania wyżej wymienionych postulatów ma być wzmocnienie współpracy państw członkowskich na różnych płaszczyznach rynku zbrojeniowego. Ta współpraca ma dotyczyć z jednej strony harmonizacji wspólnej polityki zagranicznej i bezpieczeństwa Unii oraz wzmocnienia kontroli wywozu technologii wojskowych, a z drugiej – uczestnictwa w organizacjach międzynarodowych i realizacji zobowiązań oraz umów międzynarodowych wynikających ze współdziałania m.in. z Organizacją Narodów Zjednoczonych. Przyjęte rozwiązania respektują jednocześnie prawo państw do transferu środków obrony własnej, a także do posiadania i rozwoju przemysłu oraz potencjału obronnego.

Omawiany akt uprawnia państwa członkowskie do udzielania zezwoleń na obrót towarami[24] wymienionymi we *Wspólnym wykazie uzbrojenia Unii Europejskiej*[25]. Musi to być jednak poprzedzone postępowaniem prowadzonym według wspólnie przyjętych kryteriów wyznaczających kierunki polityki nadzoru i kontroli w handlu technologiami i sprzętem wojskowym. Te przesłanki zostały unormowane w art. 2 *Wspólnego stanowiska Rady* w postaci ośmiu najważniejszych kryteriów służących do oceny wniosków:

- kryterium 1: poszanowanie międzynarodowych zobowiązań państw członkowskich, szczególnie sankcji przyjętych przez Radę Bezpieczeństwa ONZ lub Unię Europejską, porozumień o nierozprzestrzenianiu broni masowego rażenia i w innych sprawach, jak również innych zobowiązań międzynarodowych;
- kryterium 2: poszanowanie praw człowieka w państwie końcowego przeznaczenia i poszanowanie przez to państwo międzynarodowego prawa humanitarnego;
- kryterium 3: sytuacja wewnętrzna w państwie końcowego przeznaczenia wynikająca z napięć lub konfliktów zbrojnych;
- kryterium 4: zachowanie pokoju, bezpieczeństwa i stabilności w regionie;
- kryterium 5: bezpieczeństwo narodowe państw członkowskich i terytoriów, za których stosunki zewnętrzne państwa członkowskie są odpowiedzialne, oraz bezpieczeństwo państw zaprzyjaźnionych i sprzymierzonych;
- kryterium 6: zachowanie się państwa kupującego wobec społeczności międzynarodowej, a zwłaszcza jego nastawienie do terroryzmu, charakter jego sojuszy i poszanowanie przez nie prawa międzynarodowego;
- kryterium 7: istnienie ryzyka, że nastąpi zmiana przeznaczenia technologii wojskowej lub sprzętu wojskowego w państwie kupującym lub że dojdzie do jego ponownego wywozu na niepożądanych warunkach;
- kryterium 8: zgodność wywożonych technologii wojskowych i sprzętu wojskowego z technicznymi i ekonomicznymi możliwościami państwa odbiorcy, przy uwzględnieniu, że jest pożądane, aby państwa zaspokajały swoje uzasadnione potrzeby bezpieczeństwa i obronności przy jak najmniejszym wykorzystaniu ludzi i zasobów gospodarczych na rzecz uzbrojenia.

Uwzględnianie powyższych kryteriów jest priorytetem państw członkowskich. Niespełnienie któregoś z nich skutkuje niewydaniem zezwolenia w trybie obligatoryj-

[24] Wywóz, pośrednictwo, tranzyt, przeładunek oraz niematerialne transfery oprogramowania i technologii.
[25] Dz.Urz. UE C z 2013 r. nr 90 poz. 1.

nym[26] lub fakultatywnym[27] bądź powoduje konieczność zachowania szczególnej ostrożności i czujności przy wydawaniu zezwoleń państwom oraz rozważenie ryzyka niezgodnego przeznaczenia technologii lub sprzętu[28]. W ramach powyższych działań państwa oceniają wpływ technologii wojskowych i sprzętu wojskowego przeznaczonych do wywozu na państwo – odbiorcę oraz biorą pod uwagę ryzyko, że taka technologia i taki sprzęt mogą zmienić przeznaczenie i trafić do niepożądanego użytkownika końcowego.

Co ciekawe, w ocenach wniosków o udzielenie zezwoleń na transfer technologii i sprzętu wojskowego są zawarte jedynie podstawowe zalecenia, z zaznaczeniem możliwości ustanowienia bardziej restrykcyjnej polityki krajowej[29].

Kolejne jednostki redakcyjne *Wspólnego Stanowiska Rady...* wyraźnie łączą się z *Rozporządzeniem Rady nr 428/2009*. Wynika to np. z zalecenia dotyczącego wykorzystania systemu certyfikacji użytkownika końcowego, co ma stanowić podstawę do uzyskania rzetelnej wiedzy na temat końcowego wykorzystania produktów podwójnego zastosowania w państwie końcowego przeznaczenia.

Warto tutaj podkreślić także zobowiązanie do szerokiego stosowania wymiany informacji pomiędzy państwami członkowskimi. Dotyczy to zarówno negatywnych decyzji dotyczących zezwoleń na obrót technologiami wojskowymi i sprzętem wojskowym, jak i sprawozdawczości z rocznego przepływu omawianych towarów. W tym też zakresie państwa, które działają w ramach wspólnej polityki zagranicznej i bezpieczeństwa, podejmują działania wzmacniające współpracę.

Zgodnie z art. 12 państwa członkowskie dbają o to, żeby ich przepisy krajowe umożliwiały kontrolę wywozu technologii i sprzętu wymienionego we *Wspólnym wykazie uzbrojenia UE*, który stanowi punkt odniesienia dla krajowych wykazów technologii i sprzętu w państwach członkowskich, choć bezpośrednio ich nie zastępuje[30].

II. Prawo krajowe

Państwo wymaga zapewniania mu szczególnej ochrony. To uzasadnia specjalne uprawnienia aparatu państwowego. Jednym z nich jest kontrolowanie obrotu towarami strategicznymi, tj. takimi, które we władaniu osób niepowołanych mogą być wykorzystane przeciwko państwu i jego obywatelom[31].

Na gruncie prawa polskiego aktami prawnymi ściśle powiązanymi z *Rozporządzeniem Rady nr 428/2009* oraz ze *Wspólnym stanowiskiem Rady nr 2008/944/WPZiB* z 8 grudnia 2008 r., określającymi wspólne zasady prowadzenia kontroli wywozu technologii wojskowych i sprzętu wojskowego, są: ustawa z 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpie-

[26] Kryterium 1, 3 i 4.

[27] Kryterium 2 (jeśli istnieje wyraźne ryzyko, że technologia wojskowa lub sprzęt wojskowy przeznaczone do wywozu mogłyby być wykorzystane do stosowania represji wewnętrznych oraz jeśli istnieje wyraźne ryzyko, że technologia wojskowa lub sprzęt wojskowy przeznaczone do wywozu mogłyby zostać wykorzystane do działań stanowiących poważne pogwałcenia międzynarodowego prawa humanitarnego).

[28] Kryteria 5–8.

[29] *Wspólne stanowisko Rady...*, art. 3.

[30] Tamże, art. 5.

[31] K. Majewski, *Nowelizacja ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa w świetle wypełniania zobowiązań międzynarodowych*, w: *Unia Europejska a obrót towarami strategicznymi. Nowe regulacje – nowe wyzwania*, J. Barcz, J. Bokszczanin (red.), Warszawa 2013, s. 37.

czeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa[32] oraz ustawa z 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym i obrocie nimi[33]. Regulują one zasady produkcji towarów o znaczeniu strategicznym, w tym broni, amunicji, materiałów wybuchowych, wyrobów i technologii wojskowych oraz policyjnych, a także obrotu nimi oraz ewidencji i kontroli tego obrotu. Jednocześnie wprowadzają odpowiedzialność administracyjno-porządkową i karną za nieprzestrzeganie tych zasad.

1. *Ustawa z dnia 29 listopada o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa oraz o zmianie niektórych ustaw*[34]

Ustawa o obrocie strategicznym wskazuje organy właściwe do realizacji jej zapisów. Najważniejszymi organami są tu minister właściwy do spraw gospodarki, jako organ kontroli obrotu, oraz szef Agencji Bezpieczeństwa Wewnętrznego, jako organ monitorujący, opiniujący i – jak się wydaje – właściwy[35] organ postępowania przygotowawczego. Dodatkowo ustawa wskazuje organy uprawnione do wydawania opinii, tj. pozostałe służby specjalne – centralne organy administracji rządowej: szefów SKW i SWW, szefa AW oraz – w zakresie materiałów i technologii jądrowych – prezesa Państwowej Agencji Atomistyki.

Aby przejść do szczegółowego omówienia norm ustawy, jej przedmiotu i rozwiązań prawnych, w pierwszej kolejności należy przytoczyć i precyzyjnie wyjaśnić pojęcia, jakimi posługuje się ustawodawca.

1.1. Definicje

Podstawowe pojęcia, jakie należy przyswoić, gdy omawia się ustawę o obrocie towarami o znaczeniu strategicznym, można skatalogować w pięć grup obejmujących przedmiot obrotu, podmioty w nim uczestniczące, operacje handlowe, rodzaje zezwoleń na obrót strategiczny i organy właściwe do spraw związanych z obrotem.

1.1.1. Pierwsza grupa pojęciowa obejmuje produkty podwójnego zastosowania, uzbrojenie oraz towary o znaczeniu strategicznym. Produkty podwójnego zastosowania[36] to produkty, włącznie z oprogramowaniem i technologią, stosowane zarówno do celów cywilnych, jak i wojskowych. Obejmują wszystkie towary, które mogą być wykorzystane i w celach niewybuchowych, i w każdym innym celu do wspomagania produkcji broni jądrowej lub urządzeń przeznaczonych do spowodowania wybuchu jądrowego. Uzbrojenie oznacza broń, amunicję, materiały wybuchowe oraz ich części i technologie wskazane w wykazie określonym przez ministra gospodarki[37]. Towary o znaczeniu strategicznym oznaczają towary będące produktami podwójnego zastosowania lub uzbrojeniem.

[32] Dz.U. z 2013 r. poz. 194.
[33] Dz.U. z 2012 r. poz. 1017.
[34] Dz.U. z 2000 r. Nr 119 poz. 1250.
[35] To jest -.właściwy rzeczowo.
[36] Delegacja ustawowa do art. 2 pkt 1 *Rozporządzenia Rady nr 428/2009*.
[37] Na podstawie art. 6a ust. 3 ustawy o obrocie towarami o znaczeniu strategicznym – rozporządzenie ministra gospodarki w sprawie wykazu uzbrojenia, na obrót którym jest wymagane zezwolenie.

Z powyższego jasno wynika, że ustawodawca określił dwie grupy produktów wymagających zezwolenia. Pierwszą z nich są towary podwójnego zastosowania określone zapisami załączników nr I i IV do *Rozporządzenia Rady nr 428/2009*, drugą – uzbrojenie wskazane w wykazie wprowadzonym przepisami krajowymi. Wynika to z konstrukcji przyjętych w rozdziale 2 ustawy, ustanawiających reżim posiadania zezwolenia na obrót uzbrojeniem w każdym przypadku (w tym także w przypadku operacji przeprowadzanych wewnątrz Unii)[38] oraz rezygnujących z tego obowiązku w razie przywozu lub transferu wewnątrzunijnego towarów podwójnego zastosowania do Polski. Podkreślenia wymaga tu ograniczenie obrotu towarami o znaczeniu strategicznym wynikające z art. 6b ustawy. Ceduje ono obowiązek wydania rozporządzenia zawierającego spis krajów, z którymi obrót określonymi towarami o znaczeniu strategicznym jest zakazany lub ograniczony, na Radę Ministrów. Jednocześnie zwraca uwagę na uwzględnienie bezpieczeństwa publicznego oraz praw człowieka, a w przypadku uzbrojenia – również potrzeb obronności lub bezpieczeństwa Rzeczpospolitej Polskiej i zobowiązań wynikających z umów i porozumień międzynarodowych oraz ze zobowiązań sojuszniczych[39]. Niemniej wywóz towarów o znaczeniu strategicznym jest każdorazowo objęty koniecznością posiadania stosownego zezwolenia.

1.1.2. W dalszej kolejności zdefiniowano operacje handlowe, takie jak wywóz, usługa pośrednictwa, przywóz, tranzyt oraz transfer wewnątrzunijny, które były objęte intencją niniejszej regulacji. Podobnie jak wcześniej, tak i tutaj polski ustawodawca posiłkuje się prawem unijnym.

Wywóz oznacza:

- wdrożenie procedury pozwalającej na wyprowadzenie towaru wspólnotowego poza obszar celny Wspólnoty[40];
- w odniesieniu do towarów niewspólnotowych – wdrożenie procedury umożliwiającej powrotne wywiezienie ich poza obszar celny Wspólnoty[41];
- przekazywanie oprogramowania lub technologii za pośrednictwem mediów elektronicznych, w tym faksu, telefonu, poczty elektronicznej lub wszelkich innych środków elektronicznych do miejsc przeznaczenia poza Wspólnotą Europejską;
- udostępnianie wspomnianego oprogramowania i technologii osobom prawnym i fizycznym oraz spółkom cywilnym poza terytorium Wspólnoty w formie elektronicznej. Wywóz obejmuje także ustne przekazywanie informacji o technologii, np. w przypadku, gdy jest ona opisywana przez telefon.

Usługa pośrednictwa oznacza negocjowanie albo organizowanie zakupu, sprzedaży lub dostawy produktów podwójnego zastosowania z państwa trzeciego do jakiegokolwiek innego państwa trzeciego oraz sprzedaż lub zakup produktów podwójnego

[38] Na zasadach respektowania wzajemnych zezwoleń.

[39] Zwłaszcza wynikających z międzynarodowych zobowiązań RP do wprowadzenia embarga na broń lub sankcji nałożonych przez Organizację Narodów Zjednoczonych, Unię Europejską oraz Organizację Bezpieczeństwa i Współpracy w Europie, wynikających z postanowień Grupy Australijskiej, Reżimu Kontroli Technologii Rakietowych, Komitetu Zanggera, Grupy Dostawców Jądrowych, Porozumienia z Wassenaar, *Haskiego kodeksu postępowania przeciwko proliferacji rakiet balistycznych*, *Układu o nierozprzestrzenianiu broni jądrowej, sporządzonego w Moskwie, Waszyngtonie i Londynie dnia 1 lipca 1968 r.*, konwencji o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu, sporządzonej w Moskwie, Londynie i Waszyngtonie 10 IV 1972 r. oraz konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej, a także zniszczeniu jej zapasów, sporządzonej w Paryżu 13 I 1993 r.

[40] *Wspólnotowy Kodeks Celny*, art. 161.

[41] Tamże, art. 182.

zastosowania znajdujących się w państwach trzecich w celu dokonania ich transferu do innego państwa trzeciego[42]. Przywóz zaś to wprowadzenie towaru o znaczeniu strategicznym na terytorium Rzeczpospolitej Polskiej z kraju trzeciego.

Transfer wewnątrzunijny oznacza przekazanie lub przemieszczenie towaru o znaczeniu strategicznym od podmiotu w jednym państwie członkowskim do podmiotu w innym państwie członkowskim, bez opuszczania obszaru celnego Unii Europejskiej. Tranzyt zaś – to transport niewspólnotowych produktów podwójnego zastosowania wprowadzanych na terytorium celne Wspólnoty i przechodzących przez to terytorium do miejsca przeznaczenia znajdującego się poza Wspólnotą lub – w przypadku uzbrojenia – przemieszczanie pomiędzy państwem członkowskim Unii Europejskiej (z wyłączeniem Rzeczpospolitej Polskiej) i krajem trzecim lub pomiędzy krajami trzecimi, przez terytorium Rzeczpospolitej Polskiej.

Na pierwszy plan wysuwa się tutaj intencja ustawodawcy dotycząca objęcia najszerszym zakresem pojęciowym operacji handlowych przeprowadzanych szczególnie w kierunku wywozowym poza Unię Europejską. W ten sposób przepisami jest objęty zarówno wywóz towarów wytworzonych na terytorium UE, jak i wywóz towarów podlegających reeksportowi. Charakterystyczne jest tu dodanie do kategorii „wywóz" przekazu oprogramowania lub technologii za pośrednictwem mediów elektronicznych lub ustnie[43]. W opisanym powyżej duchu jest zachowana definicja pośrednictwa, przez które rozumie się wszelkie działania okołotransakcyjne, charakterystyczne dla szeroko rozumianej działalności agencyjnej. Co ciekawe, regulacja obejmuje również pośrednictwo poza obszarem UE, np. pomiędzy kontrahentami z państw trzecich.

Kolejną operacją wymagającą sprecyzowania jest tranzyt. Chodzi tu o transport towarów spoza obszaru celnego Wspólnoty przez terytorium UE z końcowym miejscem przeznaczenia poza Wspólnotą. Polskie ustawodawstwo krajowe uszczegóławia tę definicję przez objęcie nią transportu uzbrojenia z państwa członkowskiego przez terytorium RP do państwa trzeciego lub pomiędzy państwami trzecimi[44].

Wskazane powyżej definicje potwierdzają determinację do objęcia kontrolą wszelkich możliwych sposobów wymiany handlowej towarów o znaczeniu strategicznym.

1.1.3. Trzecia grupa pojęć obejmuje uczestników obrotu towarami strategicznymi, tj. dostawcę, odbiorcę, eksportera, importera, pośrednika, użytkownika końcowego i przedsiębiorcę. Dostawca i odbiorca oznaczają podmioty uprawnione odpowiednio do przekazania i odbioru uzbrojenia. Eksporter – to każda osoba fizyczna lub prawna, w której imieniu jest składana deklaracja eksportowa i która jest uprawniona do decydowania o wysłaniu produktu poza obszar celny Wspólnoty. Jest to ponadto osoba, która podejmuje decyzję o przekazaniu lub udostępnieniu oprogramowania lub technologii za pośrednictwem faksu, telefonu, poczty elektronicznej albo innych środków elektronicznych do miejsca przeznaczenia znajdującego się poza Wspólnotą.

[42] Samo świadczenie usług pomocniczych jest wyłączone z niniejszej definicji. Usługami pomocniczymi są: usługi transportowe, finansowe, ubezpieczeniowe lub reasekuracyjne oraz prowadzenie ogólnej działalności reklamowej albo promocyjnej.

[43] W tej kategorii pole do działania mogą mieć służby specjalne – w zakresie uprawnień o charakterze wywiadowczym.

[44] Wydaje się, że ta definicja jest niepełna, nie określa bowiem, czy tranzyt to również przemieszczanie produktów podwójnego zastosowania sensu stricto z państwa członkowskiego przez terytorium RP do państwa trzeciego. Polskie prawo krajowe ograniczyło krąg towarów mieszczących się w definicji tranzytu jedynie do uzbrojenia.

Ustawa o obrocie towarami strategicznymi dodaje jeszcze definicje eksportera w zakresie uzbrojenia, importera, pośrednika, użytkownika końcowego i przedsiębiorcy. Według jej zapisów w tym kontekście eksporterem jest podmiot, który pozostaje w stosunku umownym z odbiorcą w kraju trzecim i jest uprawniony do wywozu uzbrojenia albo – w sytuacji gdy nie została zawarta umowa eksportowa lub formalna strona umowy nie działa we własnym imieniu – podmiot uprawniony do wywozu uzbrojenia i faktycznie go realizujący. Eksporterem w rozumieniu ustawy jest także podmiot – strona umowy – mająca siedzibę na terytorium Polski, w przypadku gdy prawo dysponowania uzbrojeniem przynależy podmiotowi z siedzibą poza RP na podstawie umowy, na której opiera się wywóz.

Importer to podmiot zamieszkujący albo mający siedzibę na terytorium Rzeczpospolitej Polskiej, który jest uprawniony do odbioru towaru o znaczeniu strategicznym z kraju trzeciego. Pośrednikiem jest każda osoba fizyczna lub prawna bądź spółka cywilna mająca miejsce pobytu lub siedzibę w państwie członkowskim Wspólnoty, świadcząca usługi w zakresie negocjowania lub organizowania transakcji zakupu, sprzedaży lub dostawy produktów podwójnego zastosowania z państwa trzeciego do jakiegokolwiek innego państwa trzeciego albo sprzedaży lub zakupu produktów podwójnego zastosowania znajdujących się w państwach trzecich w celu ich przetransferowania do innego państwa trzeciego.

Użytkownik końcowy to podmiot deklarujący wykorzystanie towaru o znaczeniu strategicznym do własnej działalności. Przedsiębiorcą zaś jest osoba fizyczna, osoba prawna i jednostka organizacyjna niebędąca osobą prawną, która na mocy przepisów nabyła zdolność prawną, wykonująca we własnym imieniu działalność gospodarczą. Za przedsiębiorców uznaje się także wspólników spółki cywilnej, w zakresie wykonywanej przez nich działalności gospodarczej[45].

Jak można zauważyć, trudno precyzyjnie określić, kto to jest eksporter, szczególnie jeśli chodzi o ustawę polską, która, posiłkując się przepisem unijnym, wprowadza własną kategorię w zakresie uzbrojenia. Generalnie eksporterem jest każda osoba fizyczna i prawna mająca stosowne uprawnienia i decydująca o faktycznym przemieszczeniu towaru.

Ustawa z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa przewiduje dwa rodzaje zezwoleń:

1. Zezwolenie indywidualne – jest to zezwolenie udzielone jednemu konkretnemu eksporterowi w odniesieniu do jednego użytkownika końcowego lub odbiorcy w państwie trzecim, obejmujące jeden lub więcej produktów podwójnego zastosowania albo uzbrojenia, a także inne formy obrotu produktami podwójnego zastosowania niż wywóz; zezwolenie udzielone jednemu podmiotowi w odniesieniu do jednego końcowego użytkownika, importera lub odbiorcy w innym państwie, dotyczące określonej ilości i wartości jednoznacznie określonych towarów o znaczeniu strategicznym.

2. Zezwolenie globalne – jest to zezwolenie udzielone jednemu określonemu eksporterowi w odniesieniu do typu lub kategorii produktu podwójnego zastosowania, które może być ważne, jeśli chodzi o wywóz do jednego lub więcej określonych użytkowników końcowych i (lub) w jednym lub więcej określonych państwach trzecich, a w przypadku uzbrojenia także w odniesieniu do innych niż wywóz form obrotu produktami podwójnego zastosowania; zezwolenie udzielone jednemu podmiotowi w od-

[45] Art. 4 ust. 1 i 2 *Ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej* (Dz.U. z 2013 r. poz. 672).

niesieniu do jednego lub większej liczby użytkowników końcowych, importerów lub odbiorców w innym państwie lub państwach, dotyczące określonych typów lub kategorii towarów o znaczeniu strategicznym.

Na mocy przepisów *Rozporządzenia...* w ustawie wskazano organy właściwe w zakresie obrotu towarami o znaczeniu strategicznym i przydzielono im określone zadania. W przypadku obrotu towarami strategicznymi uczestnikami ze strony państwa są:

- organ kontroli – minister właściwy do spraw gospodarki, który realizuje swoje uprawnienia przez wydawanie decyzji w sprawie zezwoleń, udzielanie wyjaśnień dotyczących konieczności uzyskania zezwolenia na obrót określonymi towarami, zasięganie opinii właściwych organów, wykonywanie obowiązków informacyjnych wynikających z przepisów UE, wydawanie zakazu tranzytu, występowanie do właściwych organów państwa członkowskiego Unii Europejskiej o nieudzielanie zezwolenia albo o jego unieważnienie; zawieszenie, modyfikację lub odwołanie, zasięganie opinii właściwych organów innego państwa członkowskiego Unii Europejskiej, wyznaczanie przedstawiciela Rzeczpospolitej Polskiej do Grupy Koordynacyjnej ds. Produktów Podwójnego Zastosowania[46];
- organ monitorujący – szef Agencji Bezpieczeństwa Wewnętrznego;
- organy opiniujące – minister właściwy do spraw zagranicznych, minister właściwy do spraw wewnętrznych, minister właściwy do spraw finansów publicznych, szefowie: Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, a w odniesieniu do materiałów jądrowych, technologii jądrowych oraz innych produktów podwójnego zastosowania – prezes Państwowej Agencji Atomistyki.

1.2. Organy właściwe w sprawach obrotu o znaczeniu strategicznym

Realizując wytyczne *Rozporządzenia Rady nr 428/2009*, Polska przyznała właściwym organom uprawnienia umożliwiające wdrożenie do krajowego systemu prawnego przepisów *Rozporządzenia...* oraz innych przepisów wynikających ze zobowiązań międzynarodowych. Uprawnienia te zostały przydzielone ministrowi gospodarki i szefowi Agencji Bezpieczeństwa Wewnętrznego oraz – w zakresie opiniowania – ministrowi spraw zagranicznych, ministrowi spraw wewnętrznych, ministrowi finansów, szefom: Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Agencji Wywiadu oraz prezesowi Państwowej Agencji Atomistyki.

1.2.1. Organ kontroli

Organem wykonawczym ustawy wyposażonym w stosowne uprawnienia dotyczące obrotu towarami o znaczeniu strategicznym jest minister gospodarki[47]. Odpowiada on za wykonanie zdecydowanej większości zadań związanych z problematyką przedmiotu, poczynając od realizacji uprawnień legislacyjnych, informacyjnych, formalnych, aż po uprawnienia kontrolne i uprawnienia o charakterze represyjnym.

Najistotniejszą płaszczyzną działania ministra gospodarki w zakresie obrotu strategicznego jest płaszczyzna legislacyjna[48]. Jest on także uprawniony do wydawania decyzji w sprawie udzielania zezwoleń na obrót towarami strategicznymi. Jak już wcześniej wspomniano, przez obrót należy rozumieć wywóz, transfer wewnątrzunijny, usługę

[46] Art. 17a ustawy o obrocie strategicznym.

[47] Departament Bezpieczeństwa Gospodarczego.

[48] Na podstawie delegacji wynikających z ustawy o obrocie strategicznym.

pośrednictwa, pomoc techniczną, przywóz i tranzyt. Tym samym wymienione czynności handlowo-techniczne są reglamentowane koniecznością aplikowania i następnie – w przypadku pozytywnego finału – uzyskania stosownego zezwolenia.

Przepisy regulujące kwestie zezwoleń dzielą je na dwie grupy. Pierwsza dotyczy towarów podwójnego zastosowania, gdzie na wywóz, transfer[49], pośrednictwo i pomoc techniczną wydaje się zezwolenie indywidualne lub globalne albo krajowe zezwolenie generalne[50]. Druga wprowadza obowiązek uzyskania zezwolenia indywidualnego lub generalnego na obrót uzbrojeniem. W zakresie transferu, pośrednictwa i pomocy technicznej może być również wydane zezwolenie globalne. Oczywiście w ramach powyższej działalności organ kontroli może odmówić wydania zezwolenia, cofnąć je lub zmienić jego warunki i zakres.

Ważnym zadaniem, jeśli chodzi o rolę ministra gospodarki w obrocie towarami strategicznymi, jest wydawanie wiążących wyjaśnień w sprawie konieczności uzyskania zezwolenia przedsiębiorcom i innym osobom zainteresowanym.

Oprócz zadań wymienionych powyżej organ kontroli realizuje obowiązki informacyjne wynikające z przepisów unijnych. Wynika z nich konieczność bieżącej współpracy z analogicznymi jednostkami państw członkowskich UE, choćby w ramach wzajemnych konsultacji i informowania się o negatywnych decyzjach w sprawach o zezwolenia czy w ramach Grupy Koordynacyjnej ds. Produktów Podwójnego Zastosowania.

Osobne uprawnienia umożliwiają wydanie certyfikatu importowego oraz potwierdzenia oświadczenia użytkownika końcowego. Te dokumenty są wydawane na wniosek zainteresowanego podmiotu w przypadku, gdy wymagają tego przepisy państwa eksportera. W analogiczne uprawnienie został wyposażony minister gospodarki.

Istotą regulacji dotyczących omawianej ustawy jest zorganizowanie całkowicie transparentnego dla organów państwowych obrotu strategicznego. W tym celu ministrowi gospodarki umożliwiono realizację czynności kontrolnych w zakresie przestrzegania zgodności obrotu towarami strategicznymi z zezwoleniem oraz weryfikowania transakcji, sprawdzania procedur kontrolnych w przedsiębiorstwach i wykonywania obowiązków ewidencyjnych. Ta kontrola może być prowadzona przez zespół złożony z funkcjonariuszy, żołnierzy i pracowników organów uczestniczących w opiniowaniu wniosków o udzielenie zezwoleń. Oprócz tego do prac zespołu można powołać biegłych i ekspertów.

Jednym z elementów budowania świadomości prawnej uczestników obrotu strategicznego oraz postaw najwyższej staranności przestrzegania przepisów prawa materialnego i proceduralnego jest możliwość orzekania kar pieniężnych[51]. Ustawodawca wyposażył w tym zakresie w stosowne narzędzia właśnie ministra gospodarki. Te kary, jak na warunki przepisów polskich, są dotkliwe, wynoszą bowiem od 50 000 do 200 000 zł, w zależności od stopnia stwierdzonych nieprawidłowości.

1.2.2. Organ monitorujący

Oprócz ministra właściwego do spraw gospodarki ustawodawca wyposażył w stosowne uprawnienia także szefa Agencji Bezpieczeństwa Wewnętrznego. Uprawnienia te można podzielić na trzy kategorie:

[49] Produktów wymienionych w załączniku nr IV do *Rozporządzenia Rady (WE) nr 428/2009*, szerzej zob. s. 6 i 13.

[50] Co do zasady przywóz lub transfer wewnątrzunijny na terytorium RP towarów podwójnego zastosowania nie wymaga uzyskania zezwolenia – art. 6c ustawy o obrocie strategicznym.

[51] Szerzej zob. s. 17.

1) uprawnienia dotyczące monitorowania przywozu i transferu wewnątrzunijnego produktów podwójnego zastosowania, wykorzystywanych w telekomunikacji lub do ochrony informacji,
2) uprawnienia dotyczące potwierdzania wiarygodności przedsiębiorców,
3) uczestniczenie w procesie opiniowania i w kontroli obrotu.

Przywóz do Polski towarów podwójnego zastosowania z kategorii „telekomunikacja i ochrona informacji" oraz ich transfer wewnątrzunijny podlegają monitorowaniu. Odbywa się to przez nałożenie obowiązków pisemnego informowania ABW o zamiarze realizacji tego typu czynności. W ramach zgłoszenia przedsiębiorca jest obowiązany zamieścić dane dotyczące odbiorcy, kontrahenta, przedmiotu operacji i sposobu jego wykorzystania, a także oświadczenie, że podmiot podejmie niezbędne działania, aby produkt, o którym mowa w zgłoszeniu, dotarł do użytkownika końcowego. Dodatkowo w sytuacjach związanych z obrotem urządzeniami lub technologiami związanymi z ochroną informacji niejawnych niezbędne jest dołączenie koncesji na wykonywanie działalności w zakresie obrotu towarami i technologiami przeznaczonymi dla wojska i policji.

Kolejnym elementem wpływającym na stabilność obrotu produktami podwójnego zastosowania jest możliwość uzyskania przez przedsiębiorcę świadectwa wiarygodności odbiorcy. Tego typu świadectwo jest potwierdzeniem przez administrację państwową spełniania wymogów regulacji o obrocie strategicznym. Dokument, o którym mowa, wydaje na wniosek zainteresowanego podmiotu szef Agencji Bezpieczeństwa Wewnętrznego – w trybie przepisów o postępowaniu administracyjnym. W trakcie procedowania nad wnioskiem o wydanie świadectwa wiarygodności szef ABW może zwrócić się do organów opiniujących w sprawie ewentualnych zastrzeżeń co do danego przedsiębiorcy. Na uwagę zasługuje wyposażenie szefa ABW w możliwość żądania, w zasadzie od wszystkich organów państwowych oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej, informacji niezbędnych do podjęcia decyzji dotyczącej wydania świadectwa wiarygodności.

1.2.3. Służba Celna

Zgodnie z art. 20 ust. 1 ustawy o obrocie strategicznym wywóz, przywóz lub tranzyt towarów o znaczeniu strategicznym jest realizowany w urzędach celnych wyznaczonych przez ministra finansów[52].

Służba Celna jest ważnym ogniwem systemu ochrony obrotu strategicznego. Jej zadania dotyczą szczególnie tej nielegalnej części obrotu, która jest wykrywana dopiero podczas weryfikacji zgłoszenia towaru do danej procedury celnej.

1.2.4. Organy opiniujące

W szeroko rozumiany proces kontroli obrotu strategicznego zostały zaangażowane również organy uprawnione do opiniowania procedur uregulowanych ustawą. Są to ministrowie spraw zagranicznych, spraw wewnętrznych i finansów, szefowie służb specjalnych oraz prezes Państwowej Agencji Atomistyki. Instytucje, których są reprezentantami, uczestniczą w wydawaniu zezwoleń generalnych, indywidualnych, świadectw wiarygodności odbiorcy i certyfikatów importowych[53] oraz mogą, na mocy art. 29 ust. 2 ustawy o obrocie strategicznym, delegować swoich funkcjonariuszy i żołnierzy do zespołu prowadzącego kontrolę obrotu.

[52] *Rozporządzenie Ministra Finansów z dnia 25 czerwca 2013 r. w sprawie urzędów celnych, w których może być dokonywany wywóz, przywóz i tranzyt towarów o znaczeniu strategicznym* (tekst jednolity: Dz.U. z 2015 r. poz. 136).

[53] Art. 12 ust. 2, art. 12a, art. 17, art. 21h ust. 2 oraz art. 22 ust. 2a ustawy o obrocie strategicznym.

1.3. Wykaz uzbrojenia i produkty podwójnego zastosowania

Najważniejsze znaczenie dla realizacji zapisów ustawy o obrocie strategicznym mają wykaz uzbrojenia, na obrót którym jest wymagane zezwolenie, oraz listy produktów podwójnego zastosowania wymienione w załącznikach do *Rozporządzenia Rady nr 428/2009*. W polskim prawie krajowym wykaz uzbrojenia został wydany na podstawie art. 6a ustawy o obrocie strategicznym, w formie rozporządzenia ministra gospodarki[54]. Ten wykaz podzielono na dwie części. Pierwsza z nich obejmuje wywóz uzbrojenia, jego transfer z terytorium RP i przez nie, pośrednictwo, pomoc techniczną oraz tranzyt. Druga dotyczy przywozu uzbrojenia i jego transferu wewnątrzunijnego przez terytorium RP.

1.3.1. Wykaz uzbrojenia, na obrót którym jest wymagane zezwolenie

Wykaz uzbrojenia, na obrót którym jest wymagane zezwolenie, zawiera 22 kategorie. Przypisano im konkretne numery listy uzbrojenia (LU). Zawiera on także cztery kategorie substancji chemicznych, na których przywóz również jest konieczne zezwolenie. W ten sposób utworzono grupy uzbrojenia i uwzględniono cechy charakterystyczne danego sprzętu. Opisy stosowane przez ustawodawcę są z jednej strony na tyle ogólne (nazwy grup), aby dokonać prawidłowej identyfikacji i kwalifikacji urządzenia, a z drugiej na tyle szczegółowe (dodatkowe uwagi opisowe, doprecyzowania), aby ta identyfikacja była precyzyjna i konkretna. Trzeba również zaznaczyć, że na potrzeby wykazu zostały przygotowane objaśnienia poszczególnych określeń specjalistycznych[55].

Poniżej wymieniono grupy sprzętu z listy uzbrojenia, na których wywóz, transfer z terytorium RP i przez nie, pośrednictwo, pomoc techniczną oraz tranzyt jest potrzebne zezwolenie:

- pozycja nr 1: broń gładkolufowa o kalibrze mniejszym niż 20 mm, inne uzbrojenie i broń automatyczna o kalibrze 12,7 mm (0,50 cala) lub mniejszym oraz wyposażenie i specjalnie zaprojektowane do nich elementy składowe;
- pozycja nr 2: broń gładkolufowa o kalibrze 20 mm lub większym, inna broń i uzbrojenie o kalibrze większym od 12,7 mm (0,50 cala), miotacze oraz wyposażenie i specjalnie zaprojektowane do nich elementy składowe;
- pozycja nr 3: amunicja i zapalniki oraz specjalnie zaprojektowane do nich elementy składowe;
- pozycja nr 4: bomby, torpedy, rakiety, pociski rakietowe, inne urządzenia i ładunki wybuchowe oraz związane z nimi wyposażenie i akcesoria oraz specjalnie zaprojektowane do nich elementy składowe;
- pozycja nr 5: sprzęt kierowania ogniem oraz związany z nim sprzęt ostrzegania i alarmowania, a także powiązane z nimi systemy oraz sprzęt do testowania, strojenia i zakłócania, specjalnie zaprojektowany do celów wojskowych oraz specjalnie zaprojektowane do nich elementy składowe i wyposażenie;
- pozycja nr 6: pojazdy naziemne i ich elementy składowe;
- pozycja nr 7: chemiczne lub biologiczne środki trujące, „środki rozpraszania tłumu", materiały radioaktywne oraz związany z nimi sprzęt, elementy składowe i materiały;
- pozycja nr 8: „materiały wysokoenergetyczne" oraz substancje pokrewne;
- pozycja nr 9: wojenne jednostki pływające (nawodne lub podwodne), specjalny sprzęt morski, wyposażenie, elementy składowe i inne nawodne jednostki pływające;

[54] *Rozporządzenie Ministra Gospodarki z dnia 8 maja 2014 r. w sprawie wykazu uzbrojenia, na obrót którym jest wymagane zezwolenie* (na bieżąco aktualizowane) – Dz.U. z 2014 r. poz. 627.

[55] Określenia niesprecyzowane w rozporządzeniu przyjmują swoje ogólnie przyjęte (słownikowe) znaczenie.

- pozycja nr 10: „statki powietrzne", „statki powietrzne lżejsze od powietrza", bezzałogowe statki powietrzne (UAV), silniki i wyposażenie „statków powietrznych", pokrewne wyposażenie i elementy składowe, specjalnie zaprojektowane lub zmodyfikowane do celów wojskowych;
- pozycja nr 11: sprzęt elektroniczny, „statki kosmiczne" i elementy składowe, niewymienione w innym miejscu wykazu uzbrojenia;
- pozycja nr 12: systemy broni opartej na energii kinetycznej dużych prędkości oraz sprzęt pokrewny i specjalnie zaprojektowane do nich elementy składowe;
- pozycja nr 13: sprzęt opancerzony lub ochronny, konstrukcje oraz ich elementy składowe;
- pozycja nr 14: „sprzęt specjalistyczny do szkolenia wojskowego" lub do symulacji gier wojennych, symulatory specjalnie zaprojektowane do szkolenia w posługiwaniu się jakąkolwiek bronią określoną w LU1 lub LU2 oraz specjalnie zaprojektowane do nich elementy składowe i akcesoria;
- pozycja nr 15: sprzęt do obrazowania lub przeciwdziałania, specjalnie zaprojektowany do celów wojskowych oraz specjalnie zaprojektowane do niego elementy składowe i akcesoria;
- pozycja nr 16: odkuwki, odlewy i inne półfabrykaty, które zostały specjalnie zaprojektowane do produktów określonych w pozycjach od 1 do 4, a także 6, 9, 10, 12 lub 19;
- pozycja nr 17: różnego rodzaju sprzęt, materiały i „biblioteki" oraz specjalnie zaprojektowane do nich elementy składowe;
- pozycja nr 18: sprzęt i elementy składowe do produkcji, takie jak: specjalnie zaprojektowany lub zmodyfikowany sprzęt do produkcji wyrobów określonych w niniejszym wykazie uzbrojenia oraz specjalnie zaprojektowane do niego elementy składowe, specjalnie zaprojektowane wyroby do prowadzenia badań środowiskowych oraz specjalnie zaprojektowane do nich wyposażenie wykorzystywane do certyfikacji, kwalifikacji lub badania produktów określonych w niniejszym wykazie uzbrojenia;
- pozycja nr 19: systemy broni o ukierunkowanej energii (ang. *Directed Energy Weapon* – DEW), sprzęt pokrewny lub sprzęt przeciwdziałania i modele badawcze (wymienione poniżej) oraz specjalnie zaprojektowane do nich elementy składowe;
- pozycja nr 20: sprzęt kriogeniczny lub „nadprzewodzący" oraz specjalnie zaprojektowane do niego elementy składowe i akcesoria;
- pozycja nr 21: „oprogramowanie";
- pozycja nr 22: „technologie".

Grupy substancji chemicznych, na których przywóz i transfer wewnątrzunijny na terytorium RP jest wymagane zezwolenie (rozwinięcie pozycji nr 7 listy uzbrojenia) to:

- bojowe środki trujące obejmujące środki paralityczno-drgawkowe i środki parzące,
- dwuskładnikowe oraz najważniejsze prekursory bojowych środków trujących,
- saksytoksyna,
- rycyna.

1.3.2. Załącznik nr I do *Rozporządzenia Rady nr 428/2009*

Załącznik nr I do *Rozporządzenia Rady nr 428/*2009 wprowadza[56] kontrolę produktów i technologii podwójnego zastosowania. *Rozporządzenie...* odsyła do ustawodawstwa krajowego[57] w przypadku towarów, które zostały zaprojektowane lub zmodyfikowane do celów wojskowych, i wprowadza 10 kategorii produktów podwójnego zastosowania oraz usług, tj.:

– kategoria 0: materiały, instalacje i urządzenia jądrowe,
– kategoria 1: materiały specjalne i związane z nimi urządzenia,
– kategoria 2: przetwarzanie materiałów,
– kategoria 3: elektronika,
– kategoria 4: komputery,
– kategoria 5: sprzęt telekomunikacyjny i ochrona,
– kategoria 6: czujniki i lasery,
– kategoria 7: nawigacja i awionika,
– kategoria 8: urządzenia okrętowe,
– kategoria 9: kosmonautyka, aeronautyka, napęd.

1.3.3. Załącznik nr IV do *Rozporządzenia Rady nr 428/2009*

Na wewnątrzwspólnotowy transfer produktów podwójnego zastosowania wymienionych w załączniku IV[58] również jest wymagane zezwolenie. Ten załącznik stanowi podzbiór załącznika nr I. Produkty wymienione w załączniku IV w części 2 nie są objęte zezwoleniem generalnym. Podzielono je na następujące grupy:

– produkty technologii zmniejszonej wykrywalności za pomocą odbitych fal radarowych (*stealth*),
– produkty objęte wspólnotową kontrolą strategiczną,
– produkty wspólnotowego sterowania strategicznego – kryptografia,
– produkty technologii MTCR[59].

Część druga załącznika wymienia produkty, które nie mogą zostać objęte zezwoleniem generalnym. Są to:

– produkty w ramach konwencji o zakazie broni chemicznej (CWC),
– produkty technologii NSG.

1.3.4. Zakazy i ograniczenia

Ustawodawca ograniczył obrót wskazanymi powyżej kategoriami oraz grupami produktów podwójnego zastosowania i uzbrojenia przez wprowadzenie obowiązku posiadania stosownego zezwolenia. Nie jest to jednak jedyna forma ingerencji w rynek towarów o znaczeniu strategicznym. Jedną z nich jest także delegacja ustawowa dla Rady Ministrów, wynikająca z art. 6b ustawy o obrocie strategicznym, która dotyczy ograniczenia lub zakazania obrotu z poszczególnymi krajami. Czynnikami mającymi wpływ na krąg „państw wykluczonych" są względy bezpieczeństwa publicznego i prawa człowieka, a w przypadku uzbrojenia – również potrzeby obronności lub bezpieczeństwa Polski, a także zobowiązania naszego kraju wynikające z umów i porozumień międzynarodowych oraz z zobowiązań sojuszniczych. Te ograniczenia są wymierzone w niektóre

[56] Na podstawie art. 3 *Rozporządzenia Rady...*
[57] Do wykazów uzbrojenia.
[58] Wprowadzony na podstawie art. 22 *Rozporządzenia Rady...*
[59] Reżim kontrolny technologii rakietowych.

instytucje i organizacje w krajach objętych częściowym lub całkowitym embargiem oraz w krajach prowadzących działania wojenne, które popierają i wspierają międzynarodowy terroryzm, a także w rozpoznane lub potencjalne organizacje terrorystyczne.

Kolejnym uprawnieniem jest prawo ministra gospodarki dotyczące zakazania tranzytu towarów strategicznych w sytuacji opisanej w art. 6 ust. 1 *Rozporządzenia Rady...*[60]

W przypadkach stwierdzonych nieprawidłowości w obrocie towarami o znaczeniu strategicznym prowadzonym na podstawie zezwolenia generalnego minister gospodarki w drodze decyzji administracyjnej zakazuje korzystania z zezwolenia.

1.4. Przepisy karne

Zgodnie z postulatem zawartym w preambule *Rozporządzenia Rady nr 428/2009* oraz jego normą zawartą w art. 24 każde państwo członkowskie ma obowiązek podjąć odpowiednie kroki, aby zapewnić właściwe egzekwowanie wszystkich przepisów w zakresie obrotu towarami o znaczeniu strategicznym. Powinno zwłaszcza ustanowić sankcje stosowne do naruszeń w ramach norm prawnych. Wytycznymi dla państw członkowskich przy tworzeniu przepisów karnych są wyznaczniki skuteczności, proporcjonalności i odstraszania.

Polska ustawa z 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa przewiduje różne rodzaje przepisów karnych i odpowiedzialności. Ten podział jest widoczny w zakresie stopnia naruszenia norm prawnych i konsekwencji takiego działania, a także w zakresie podmiotu łamiącego przepisy.

1.4.1. Przestępstwo

W art. 33 uregulowano odpowiedzialność karną za obrót towarami strategicznymi bez zezwolenia lub wbrew warunkom określonym w zezwoleniu. Ustęp 1 określa krąg adresatów, z którego wynika, że ta norma jest skierowana do wszystkich podmiotów dokonujących nielegalnego obrotu[61] towarami podwójnego zastosowania oraz uzbrojeniem, niezależnie od znamion strony podmiotowej tego czynu[62], który jest zagrożony karą pozbawienia wolności od roku do lat 10.

---

[60] Właściwe organy państwa, w którym następuje tranzyt, mogą zakazać tranzytu niewspólnotowych produktów podwójnego zastosowania wyszczególnionych w załączniku I, jeżeli te produkty są lub mogą być, w całości lub części, przeznaczone do zastosowania, o którym mowa w art. 4 ust. 1. Podejmując decyzję o takim zakazie, państwa członkowskie biorą pod uwagę swoje obowiązki i zobowiązania, które przyjęły na siebie jako strony traktatów międzynarodowych lub jako członkowie międzynarodowych systemów nieproliferacji.

[61] Należy tu przytoczyć także definicję obrotu, w tym ujęcie usług pośrednictwa. O b r ó t to wywóz, transfer wewnątrzunijny, usługa pośrednictwa, pomoc techniczna, przywóz i tranzyt. Można się posiłkować definicjami rozporządzenia Rady nr 428/2009 wskazującymi na to, że samo świadczenie usług pomocniczych, tj. zapewnianie transportu, usługi finansowe, ubezpieczeniowe itd., jest wyłączone z definicji usług pośrednictwa. Dotyczy to jednak produktów podwójnego zastosowania. W przypadku uzbrojenia definicja ustawodawstwa krajowego określa jako usługę pośrednictwa m.in. (…) *uczestnictwo, w jakiejkolwiek formie, w czynnościach związanych z wywozem, przywozem, tranzytem*.

[62] Z uwagi na liczne przykłady i charakterystykę tego typu przestępczości identyfikowanej w południowej części Polski można by w tym miejscu rozpocząć rozważania na temat ewentualnego błędu odnoszącego się do bezprawności czynu. Wynika to z dużej liczby obcokrajowców będących sprawcami wymienionych występków, którzy w toku prowadzonych śledztw zasłaniają się tym, że nie wiedzieli, co przewozili, i że (…) *na to potrzebne jest zezwolenie*. Zdaniem autora nie powinno się usprawiedliwiać tłumaczenia obcokrajowców wskazujących na nieświadomość wymogu posiadania zezwolenia na obrót np. kołami do czołgów, pojazdami opancerzonymi, mimo że zostały one wycofane z majątku wojska, czy silnikami lotniczymi itp. Powszechność

Ustawodawca przewidział złagodzenie odpowiedzialności dla osób, które posiadały zezwolenie i dokonywały obrotu. W związku jednak z działaniem nieumyślnym obrót odbywał się wbrew określonym w nim obwarowaniom. Warunkiem łagodniejszego potraktowania sprawcy jest działanie nieumyślne i przywrócenie w terminie jednego miesiąca stanu zgodnego z ustawą. Wówczas sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Możliwości uzależnienia wysokości kary od naprawienia skutków czynu (przywrócenia legalności działań post factum) nie przewidziano dla sprawców obrotu nieposiadających zezwolenia. Stosownie do zaleceń unijnych nie przewiduje się tolerancji dla nielegalnego obrotu towarami o znaczeniu strategicznym.

Surowe sankcje karne, analogicznie jak w przypadku nielegalnego obrotu, przewidziano za dopuszczenie do popełnienia przestępstw, o których mowa była wyżej. Tym samym jest widoczne dążenie do rozszerzenia kręgu osób odpowiedzialnych za czyn zabroniony z zakresu nielegalnego obrotu strategicznego, obejmujące nie tylko faktycznych, fizycznych sprawców obrotu, lecz także osoby zlecające takie działania i umożliwiające ich przeprowadzenie.

Przepisy prawnokarne odnoszą się także do samego aplikowania o zezwolenie. Mianowicie – została przewidziana odpowiedzialność karna za podanie nieprawdziwych lub niepełnych danych we wniosku.

W sytuacji skazania za powyższe przestępstwa sąd może orzec przepadek towarów o znaczeniu strategicznym. Odnosi się to również do innych przedmiotów służących lub przeznaczonych do ich popełnienia oraz przedmiotów pochodzących z przestępstwa, w tym do środków płatniczych i papierów wartościowych, chociażby nie stanowiły one własności sprawcy.

1.4.2. Wykroczenie

Osobną grupę przepisów karnych zawartych w ustawie o obrocie towarami o znaczeniu strategicznym stanowią art. 34, 35 i 35a. Dotyczą one braku realizacji obowiązku informacyjnego odnośnie do obrotu tymi towarami w danym roku, obowiązku informacyjnego szefa ABW odnośnie do zmiany danych podmiotu mającego siedzibę w RP oraz w sytuacji utrudniania kontroli obrotu. Za braki formalne w powyższym zakresie ustawodawca przewidział zagrożenie karą grzywny.

1.4.3. Kary pieniężne

Oprócz wyżej wymienionych sankcji ustawodawca wprowadza jeszcze jeden rodzaj reakcji państwa na nieprawidłowości przy obrocie towarami o znaczeniu strategicznym – kary pieniężne. Można je podzielić na sankcje skierowane wyłącznie do osób

regulacji, szczególnie w państwach europejskich, wskazuje na to, że w każdym kraju problematyka dotycząca obrotu towarami podwójnego zastosowania i uzbrojenia jest ujęta w porządku prawnym. Jest to wspierane zainteresowaniem i zaangażowaniem wielu organizacji międzynarodowych, m.in. ONZ, co, zdaniem autora, wpływa na brak możliwości zasłaniania się niewiedzą o ograniczonych możliwościach posiadania towarów o znaczeniu strategicznym, ich przewożenia, tranzytu, transefru itp. Jeśli chodzi o płaszczyznę prawnokarną, to jedną z podstawowych zasad procesu karnego jest zasada legalizmu, której konsekwencją jest m.in. konieczność wszczęcia postępowania i ukarania osoby winnej złamania właściwych przepisów karnych. Odejście od tej zasady może nastąpić wyjątkowo, lista towarów o podwójnym zastosowaniu i uzbrojenia jest bowiem wyjątkowo szczegółowa i kazuistyczna. W stosunku do podmiotu uczestniczącego w obrocie towarami o znaczeniu strategicznym trzeba jednak wymagać pełnego profesjonalizmu, a tym samym znajomości prawa i najwyższej staranności przy realizacji obrotu.

prawnych i jednostek organizacyjnych niemających osobowości prawnej[63] oraz na sankcje skierowane do wszystkich uczestników obrotu.

Konstrukcja pierwszego typu kar administracyjnych jest analogiczna jak w przypadku występków określonych w art. 33 i jest związana z nielegalnym obrotem towarami o znaczeniu strategicznym oraz obrotem wbrew warunkom określonym w zezwoleniu. Przewidziano tutaj także sankcje dla przedsiębiorstwa za podanie nieprawdziwych lub niepełnych danych we wniosku o wydanie zezwolenia oraz za brak rocznej informacji o obrocie. Te kary winny być orzeczone równolegle do odpowiedzialności karnej osób fizycznych, wynikającej z art. 33. Co charakterystyczne, w przypadku stwierdzenia naruszeń wskazanych w ustawie obligatoryjnie jest nakładana kara pieniężna, przy czym minister gospodarki ustala jedynie jej wysokość.

Kary pieniężne dotyczą zaniedbań formalnych. Nałożenie pierwszej z nich jest związane z obowiązkiem zgłoszenia zamiaru przywozu lub transferu wewnątrzunijnego szefowi ABW. Do drugiej grupy enumeratywnie wymienionych zaniedbań formalnych, za które przewidziano kary pieniężne, należą: niezłożenie oświadczenia o terminie rozpoczęcia obrotu, nieinformowanie kontrahentów o warunkach zezwolenia i o ograniczeniach w dysponowaniu towarami strategicznymi, brak i nieprowadzenie stosownej ewidencji obrotu oraz nieprzekazanie do ministra spraw zagranicznych rocznego raportu z faktycznego wywozu uzbrojenia.

Jak wynika z powyższego, ustawodawca, sporządzając przepisy karne, zwiększył krąg osób podlegających odpowiedzialności karnej i karom pieniężnym. Zasadniczo każdy – niezależnie od tego, czy jest to przedsiębiorca dokonujący obrotu, czy przewoźnik – kto w jakikolwiek sposób narusza zasady obrotu towarami o znaczeniu strategicznym, winien zostać ukarany. Zaznaczenia wymaga to, że penalizacji podlega zarówno obrót nielegalny, bez wymaganego zezwolenia, jak i obrót, w którego przypadku wprawdzie zezwolenie zostało wydane, ale który jest dokonywany wbrew warunkom w nim określonym. Co więcej, brak właściwej i terminowej realizacji obowiązków nałożonych na podmiot w zakresie legalnego obrotu będzie skutkował wymierzeniem dotkliwych, jak na warunki polskiego systemu prawnego, kar pieniężnych.

Intencją powyższego było wprowadzenie standardów bezwzględnego przestrzegania przepisów prawa przez uczestników obrotu towarami strategicznymi. W stosunku do podmiotów uczestniczących w tym obrocie winien bowiem obowiązywać miernik najwyższej staranności.

2. *Ustawa z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym*[64]

Nie sposób w niniejszym opracowaniu pominąć ustawy z 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym, która reguluje obrót technologiami i towarami koncesjonowanymi. Na wstępie wydaje się, że ta ustawa stanowi *lex specialis* do ustawy o obrocie strategicznym, ukierunkowane jednak na uzupełnienie i doprecyzowanie produkcji i obrotu

[63] O ile mają zdolność prawną.

[64] Tekst jednolity: Dz.U. z 2012 r. poz. 1017, ze zm.

konkretnymi wyrobami, tj. bronią i materiałami wybuchowymi oraz towarami i technologiami wojskowymi i policyjnymi.

Podstawowym wymogiem obowiązującym w produkcji materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym oraz w przypadku obrotu nimi jest wymóg uzyskania i posiadania koncesji. Jest to norma ogólna, od której ustawodawca przewidział wyjątki ściśle wskazane przepisami prawa. A zatem koncesji nie wymaga obrót:

- wyrobami pirotechnicznymi, o których mowa w art. 62c ust. 1 pkt 1 lit. a–c[65], pkt 2 lit. a[66] oraz pkt 3 lit. a[67] ustawy z 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego;
- bronią palną pozbawioną cech użytkowych zgodnie z przepisami ustawy z 21 maja 1999 r. o broni i amunicji;
- bronią inną niż broń palna oraz wyrobami o przeznaczeniu wojskowym lub policyjnym, pozbawionymi w sposób trwały i nieodwracalny bojowych cech użytkowych[68].

Organem koncesyjnym jest minister spraw wewnętrznych, który udziela koncesji, odmawia jej udzielenia, zmienia ją, cofa lub ogranicza jej zakres, po zasięgnięciu opinii ministra gospodarki, szefa Agencji Bezpieczeństwa Wewnętrznego, szefa Służby Kontrwywiadu Wojskowego i właściwego terytorialnie komendanta wojewódzkiego Policji.

Organ koncesyjny, w ramach omawianej regulacji, jest uprawniony do przeprowadzania kontroli, do której mogą być delegowani funkcjonariusze, żołnierze i pracownicy Ministerstwa Gospodarki, Ministerstwa Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego i Policji.

Zgodnie z art. 8 ustawy o obrocie specjalnym o koncesje mogą się ubiegać, po spełnieniu szczegółowo wskazanych warunków, osoby fizyczne[69] i prawne[70]. Te kryteria obejmują wiele cech, jakimi powinna wykazywać się osoba ubiegająca się o wydanie koncesji, od cenzusu wieku, wykształcenia i zdrowia[71], przez niekaralność, aż po konieczność wykazywania się wiedzą specjalistyczną. Z kolei przedsiębiorca, oprócz wyżej wymienionych warunków, winien legitymować się możliwościami technicznymi i organizacyjnymi do prawidłowej realizacji działalności objętej koncesją oraz brakiem wpisów do rejestru dłużników, prowadzonego przez Krajowy Rejestr Sądowy.

---

[65] Wyroby pirotechniczne widowiskowe.

[66] Wyroby pirotechniczne przeznaczone do wykorzystania w teatrze.

[67] Pozostałe wyroby pirotechniczne – wyroby, które charakteryzują się możliwością spowodowania zagrożenia życia i zdrowia ludzi oraz mienia i środowiska w stopniu niskim.

[68] Przez pozbawienie w sposób trwały broni oraz wyrobów o przeznaczeniu wojskowym lub policyjnym bojowych cech użytkowych należy rozumieć wyeliminowanie cech użytkowych przesądzających o przeznaczeniu wojskowym lub policyjnym.

[69] Obywatele polscy, obywatele państw UE oraz Szwajcarii lub państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA), obywatele innych państw, jeżeli otrzymali na terytorium Rzeczpospolitej Polskiej zezwolenie na pobyt stały lub zezwolenie na pobyt rezydenta długoterminowego Unii Europejskiej.

[70] Jeżeli co najmniej dwie osoby będące członkami organu zarządzającego przedsiębiorstwa albo członek organu zarządzającego przedsiębiorstwa i ustanowiony przez ten organ do kierowania działalnością określoną w koncesji prokurent lub pełnomocnik spełniają warunki określone w pkt 1, z tym że warunek, o którym mowa w pkt 1 lit. g i h, dotyczy także wspólników spółki, członków organu zarządzającego, prokurentów oraz udziałowców lub akcjonariuszy posiadających co najmniej 20% udziałów lub akcji.

[71] Są zobowiązane do przedstawienia raz na pięć lat aktualnego orzeczenia lekarskiego i psychologicznego stwierdzającego brak przeciwwskazań do wykonywania działalności gospodarczej lub kierowania nią.

2.1. Definicje

Definicje zawarte w ustawie o obrocie specjalnym są ograniczone stricte do regulowanej specyfiki i nieco różnią się od tych objętych ustawą o obrocie strategicznym. Jednak można je usystematyzować w grupy pojęciowe.

2.1.1. Pierwsza grupa obejmuje produkty będące przedmiotem koncesjonowanej działalności gospodarczej, tj.:

- materiały wybuchowe – substancje chemiczne stałe lub ciekłe albo mieszaniny substancji zdolne do reakcji chemicznej z wytwarzaniem gazu o takiej temperaturze i ciśnieniu oraz z taką szybkością, że mogą powodować zniszczenia w otaczającym środowisku, a także wyroby wypełnione materiałem wybuchowym, z wyłączeniem amunicji; materiały pirotechniczne – materiały lub mieszaniny materiałów przewidzianych do wytwarzania efektów cieplnych, świetlnych, dźwiękowych, gazu, dymu lub kombinacji tych efektów, w wyniku bezdetonacyjnej, samopodtrzymującej się reakcji chemicznej, oraz wyroby wypełnione materiałem pirotechnicznym; plastyczne materiały wybuchowe – materiały wybuchowe w giętkiej lub elastycznej prasowanej postaci;
- materiały niebezpieczne – substancje szkodliwe dla życia lub zdrowia ludzkiego, a zwłaszcza: materiały samozapalne, łatwopalne, trujące, żrące albo wytwarzające substancje o podobnym działaniu po zetknięciu się z wodą, powietrzem, wysoką temperaturą lub inną substancją, zakaźne oraz promieniotwórcze – w różnym stanie skupienia;
- materiał znakujący – tj. jedną z substancji wymienionych w konwencji dotyczącej znakowania plastycznych materiałów wybuchowych w celu ich wykrywania, podpisanej w Montrealu 1 marca 1991 r.[72];
- materiały wybuchowe przeznaczone do użytku cywilnego – materiały wybuchowe, o których mowa w art. 4 ustawy z 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego[73];
- broń i istotne części broni – broń i jej istotne części[74] w rozumieniu przepisów ustawy z 21 maja 1999 r. o broni i amunicji[75], a także inne urządzenia służące do niszczenia lub obezwładniania celów;
- amunicję – wyroby wypełnione materiałem wybuchowym, przeznaczone do miotania przy użyciu broni palnej, służące do niszczenia lub obezwładniania celów, a także do celów ćwiczebnych;
- istotne części amunicji – pociski wypełnione materiałami wybuchowymi, chemicznymi środkami obezwładniającymi lub zapalającymi albo innymi substancjami, których działanie zagraża życiu lub zdrowiu, spłonki inicjujące spalanie materiału miotającego i materiał miotający w postaci prochu strzelniczego;

[72] Dz.U. z 2007 r. Nr 135 poz. 948 – w części 2 załącznika technicznego: *Materiały znakujące*.

[73] Dz.U. Nr 117 poz. 1007, ze zm.: materiałami wybuchowymi przeznaczonymi do użytku cywilnego są substancje i wyroby, które w czasie procedury klasyfikacyjnej zostały zaliczone do 1 klasy materiałów niebezpiecznych; materiały wybuchowe w stanie niewybuchowym ujęte w klasie 4.1 materiałów niebezpiecznych, jeżeli przez wysuszenie lub przemycie mogą być im przywrócone właściwości wybuchowe; przedmioty ratownicze ujęte w klasie 9 materiałów niebezpiecznych i jeżeli zawierają materiały i przedmioty wybuchowe zaliczone do klasy 1 materiałów niebezpiecznych, jeżeli są przeznaczone do celów cywilnych.

[74] Broń palna, w tym broń bojowa, myśliwska, sportowa, gazowa, alarmowa i sygnałowa; broń pneumatyczna; miotacze gazu obezwładniającego; narzędzia i urządzenia, których używanie może zagrażać życiu lub zdrowiu, w tym broń biała, broń cięciwowa w postaci kusz oraz przedmioty przeznaczone do obezwładniania osób za pomocą energii elektrycznej.

[75] Dz.U. z 2012 r. poz. 576.

- wyroby i technologie o przeznaczeniu wojskowym lub policyjnym – wyroby zaprojektowane do celów wojskowych lub policyjnych oraz technologie związane z produkcją lub wykorzystywaniem tych wyrobów[76].

2.1.2. Druga grupa obejmuje operacje podlegające reglamentacji ustawy, tj.:

- wytwarzanie – oprócz działalności wytwórczej należy przez to rozumieć także odzysk w rozumieniu przepisów o odpadach oraz działalność rusznikarską polegającą na naprawianiu albo wytwarzaniu istotnych części broni niezbędnych do jej naprawy lub na przerabianiu broni przez ingerencję w jej istotne części;
- obrót – przez o b r ó t należy rozumieć działalność handlową dotyczącą materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, w tym pośrednictwo polegające na negocjowaniu, doradztwie handlowym, pomocy w zawieraniu umów oraz organizowaniu przemieszczania materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, z wyłączeniem spedytorów, wykonywaną na terytorium Rzeczpospolitej Polskiej;
- przemieszczanie broni palnej – jest to czynność w ramach wykonywania przez przedsiębiorcę działalności gospodarczej w zakresie, o którym mowa w art. 1. Polega ona na przemieszczeniu broni palnej: na terytorium Rzeczpospolitej Polskiej – jako państwa docelowego transakcji z państwa członkowskiego Unii Europejskiej lub państwa trzeciego traktowanego na równi z tymi państwami na podstawie umowy Rady Unii Europejskiej z państwami trzecimi w sprawie włączenia tych państw we wprowadzenie w życie, stosowanie i rozwój dorobku Schengen, zwanymi dalej „innym państwem członkowskim"; z terytorium Rzeczpospolitej Polskiej – jako państwa początkowego transakcji do innego państwa członkowskiego; przez terytorium Rzeczpospolitej Polskiej.

2.2. Wykaz wyrobów i technologii o przeznaczeniu wojskowym i policyjnym

Art. 6 ust. 3 zawiera delegację dla Rady Ministrów do ustanowienia wykazu rodzajów broni i amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub na obrót którymi jest wymagana koncesja. Uwzględnia się tu potrzeby obronności i bezpieczeństwa Rzeczpospolitej Polskiej, zagrożenie życia i zdrowia ludzkiego, mienia oraz środowiska naturalnego. Wykaz ten został wprowadzony aktem rangi rozporządzenia z 3 grudnia 2001 r. w sprawie rodzajów broni i amunicji oraz wykazu wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub na obrót którymi jest wymagana koncesja[77]. Rozporządzenie zawiera dwa załączniki: pierwszy – dotyczący rodzajów broni i amunicji, drugi – wyrobów i technologii o przeznaczeniu wojskowym i policyjnym.

[76] Orzecznictwo stoi w powyższym zakresie na stanowisku, że ustawodawca położył nacisk na cel, w jakim wyroby zostały zaprojektowane. Koncesjonowaniem na mocy omawianej ustawy jest objęta tylko ta działalność w zakresie wytwarzania i obrotu, która dotyczy wyrobów (technologii) specjalnie zaprojektowanych do celów wojskowych lub policyjnych i z tego powodu uznanych za wyroby przeznaczone do wykorzystania w wojskowości lub w pracy policji. Wyroby i technologie, które nie były projektowane do celów wojskowych lub policyjnych, z samego założenia nie są wyrobami o przeznaczeniu wojskowym lub policyjnym.

[77] Dz.U. z 2001 r. Nr 145 poz. 1625, ze zm.

2.2.1. Załącznik nr 1 – rodzaje broni i amunicji

Jako rodzaje broni i amunicji są wymienione: działa (haubice, armaty, moździerze i haubicoarmaty), broń przeciwpancerna, wyrzutnie pocisków, wojskowe miotacze ognia, zespół bojowy wyrzutni ładunków wydłużonych; broń palna: bojowa, myśliwska, sportowa, gazowa, alarmowa, sygnałowa (strzelby, karabiny, karabinki, rewolwery, pistolety, pistolety maszynowe, karabiny maszynowe, granatniki); broń pneumatyczna; miotacze gazu, miotacze wody, wyrzutnie siatek obezwładniających, wyrzutnie pocisków specjalnych (gumowych, z tworzyw sztucznych, ogłuszających, olśniewających, łzawiących, śrutowych, proszkowych), wyrzutnie granatów lub materiałów pirotechnicznych; istotne części broni palnej i pneumatycznej (szkielet broni, baskila, lufa, zamek, komora zamkowa oraz bęben nabojowy); urządzenia przeznaczone do strzelania amunicją ślepą; urządzenia do odstrzeliwania amunicji alarmowej, sygnałowej i gazowej; inne narzędzia i urządzenia służące do obezwładniania celu; amunicja do broni palnej; naboje sygnałowe, oświetlające i alarmowe; naboje do sondowania atmosfery; naboje zakłócające; naboje specjalne; pironaboje; granaty oraz zapalniki do granatów; amunicja artyleryjska, czołgowa, moździerzowa; amunicja agitacyjna i salutowa; amunicja do badań; rakiety i amunicja rakietowa; przeciwpancerne pociski kierowane; bomby lotnicze, głębinowe, w tym zapalniki do bomb; torpedy; głowice i zapalniki do broni i amunicji; środki minersko-zaporowe; środki pozoracji pola walki; szkolno-treningowe: rakiety, przeciwpancerne pociski kierowane, bomby, torpedy, granaty, środki minersko -zaporowe, amunicja; elementy: granatów, rakiet, przeciwpancernych pocisków kierowanych, bomb lotniczych i głębinowych, torped oraz środków pozoracji pola walki.

2.2.2. Załącznik nr 2 – wykaz wyrobów i technologii o przeznaczeniu wojskowym i policyjnym

W tym załączniku wyszczególniono w pkt od I do XIV sprzęt i technologie, którymi obrót i których wytwarzanie wymaga uzyskania koncesji. Punkty te zostały podzielone na konkretne grupy środków:

- środki toksykologiczne, „gazy łzawiące", sprzęt, składniki, materiały i technologie, tj. środki biologiczne i materiały radioaktywne przystosowane do powodowania ofiar w ludziach i zwierzętach, zniszczenia sprzętu lub plonów albo środowiska naturalnego oraz bojowe środki toksyczne (BST); określone środki paraliżujące, prekursory dwuskładnikowe i prekursory kluczowe, związki chemiczne zawierające atom fosforu, z którym jest związana jedna grupa metylowa, etylowa lub propylowa, gazy łzawiące oraz środki chemiczne przeznaczone do rozpraszania tłumu w czasie rozruchów, biopolimery wytworzone w celu wykrywania lub identyfikacji BST, biokatalizatory do dekontaminacji lub degradacji BST i ich systemów biologicznych, środki parzące, środki obezwładniające, defolianty;
- sprzęt kierowania ogniem, sprzęt ostrzegawczy i alarmujący, w tym jego komponenty lub wyposażenie, oraz systemy i sprzęt przeciwdziałania systemom kierowania ogniem i systemom ostrzegawczo-alarmującym;
- pojazdy naziemne, w tym ciągniki (z wyłączeniem cywilnych samochodów lub ciężarówek przeznaczonych do przewozu pieniędzy i kosztowności wyposażonych w osłony pancerne) i ich elementy;
- wojenne jednostki pływające i specjalny sprzęt morski oraz ich wyposażenie i składniki;

- załogowe i bezzałogowe statki powietrzne, lotnicze zespoły napędowe, sprzęt lotniczy i jego składniki;
- sprzęt elektroniczny nieujęty w pozycjach WT II–V oraz jego składniki;
- sprzęt specjalistyczny do szkolenia wojskowego oraz jego składniki i akcesoria;
- sprzęt do odwzorowywania ruchów przeciwnika lub zabezpieczania przed nimi (np. noktowizory, GPS-y) oraz jego specjalnie zaprojektowane składniki i akcesoria;
- systemy broni działającej z wykorzystaniem energii kierowanej (DEW), pokrewny sprzęt lub sprzęt do przeciwdziałania oraz modele testowe i ich składniki;
- sprzęt wykorzystujący zjawisko kriogeniczności lub nadprzewodnictwa oraz jego zaprojektowane składniki i akcesoria;
- wyroby i technologie związane z ochroną informacji niejawnych;
- sprzęt i konstrukcje opancerzone i ochronne oraz ich komponenty;
- sprzęt i „technologia" do „produkcji" wyrobów objętych niniejszym wykazem i ich specjalnie zaprojektowanych składników,
- wyroby nieujęte w WT I–XIII, przeznaczone do wykorzystania w wojskowości lub w pracy policji.

2.3. Wytwarzanie

Wytwarzanie materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym i policyjnym powinno się odbywać według ścisłych reguł określonych w rozdziale 3 ustawy o obrocie specjalnym. Ustawodawca wystosował trzy priorytetowe zasady dla producenta wyżej wymienionych produktów, opierające się na możliwie najmniejszym zagrożeniu życia, zdrowia, mienia i środowiska, na możliwości poddania nieodwracalnemu unieszkodliwieniu i wreszcie na obowiązku oznaczania wyrobów.

Przed przystąpieniem do wykonywania działalności wytwórczej w zakresie materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym i policyjnym przedsiębiorca jest zobowiązany do uzyskania oceny jednostki certyfikującej[78] pod względem przestrzegania podstawowych zasad produkcji.

Jak wynika z powyższego produkcja broni wiąże się także z możliwością jej unieszkodliwienia. Odbywa się to w trybie art. 19a przez działanie mające na celu eliminację cech użytkowych przesądzających o przeznaczeniu wojskowym lub policyjnym oraz w trybie art. 25 ustawy.

Ustawa nakłada na producenta wymienionych towarów wiele obowiązków formalnych wynikających ze szczególnego rodzaju wytwarzanych dóbr. Są to zwłaszcza: obowiązek prowadzenia systemu oceny jakości produkcji, w tym kontroli produktu końcowego, oraz prowadzenia ich ścisłej ewidencji.

2.4. Obrót

Zgodnie z ustawą obrotem jest prowadzenie działalności handlowej dotyczącej materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu

[78] To znaczy jednostki certyfikującej, która dysponuje personelem o odpowiedniej wiedzy technicznej i doświadczeniu w zakresie dokonywania oceny zgodności wyrobów przeznaczonych na potrzeby obronności i bezpieczeństwa państwa oraz sposobów przeprowadzania oceny zgodności. Jest ona niezależna od dostawców i dysponuje wyposażeniem technicznym niezbędnym do wykonania czynności związanych z oceną zgodności; ma system zarządzania jakością zgodny z wymaganiami określonymi w polskich normach oraz przestrzega przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

wojskowym lub policyjnym, polegające na negocjowaniu, doradztwie handlowym, pośrednictwie, pomocy w zawieraniu umów oraz organizowaniu przemieszczania materiałów wybuchowych, broni, amunicji, a także wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym. Podobnie jak przy produkcji ustawodawca określił podstawowe zasady obrotu wyrażone jako dopuszczenie do obrotu, zapewnienie maksymalnej niezawodności i bezpieczeństwa oraz oznakowanie umożliwiające precyzyjną identyfikację.

Kolejna ważna zasada dotyczy posiadania uprawnień do sprzedaży i nabycia towaru reglamentowanego[79]. Jej wzmocnieniem jest zakaz nabywania materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym i policyjnym od podmiotów nieposiadających koncesji, wyrażony w art. 31 ustawy o obrocie specjalnym.

III. Przepisy karne

Ustawa z 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym oraz obrotu nimi zawiera w rozdziale szóstym sankcje karne. Te przepisy, w zależności od stopnia naruszenia norm, przewidują odpowiedzialność za występek i wykroczenie.

Zgodnie z art. 36 ust. 1 ustawy o obrocie specjalnym (…) *kto wykonuje działalność gospodarczą w zakresie wytwarzania lub obrotu materiałami wybuchowymi, bronią, amunicją albo wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym bez koncesji lub wbrew warunkom określonym w koncesji, albo nie dopełnia obowiązku oznakowania broni palnej lub pojedynczego, podstawowego opakowania amunicji podlega karze pozbawienia wolności od roku do lat 10.* W tym miejscu należy zauważyć, że czynnością sprawczą tak opisanego przestępstwa jest wykonywanie działalności gospodarczej *w zakresie*. Pojęcie d z i a ł a l n o ś c i g o s p o d a r c z e j definiuje art. 2 ustawy z 2 lipca 2004 r. o swobodzie prowadzenia tego typu działalności[80], który mówi, że działalnością gospodarczą jest zarobkowa działalność wytwórcza, budowlana, handlowa, usługowa oraz poszukiwanie, rozpoznawanie i wydobywanie kopalin ze złóż, a także działalność zawodowa wykonywana w sposób zorganizowany i ciągły. Takie ujęcie przepisu karnego znacznie ogranicza krąg jego adresatów. Należy w tym miejscu zwrócić uwagę na treść art. 263 § 1 kk: (…) *kto bez wymaganego zezwolenia wyrabia broń palną albo amunicję lub nią handluje podlega karze pozbawienia wolności od roku do lat 10*.

Po konfrontacji tych dwóch przepisów wydaje się, że nie podlega przepisom ustawy o obrocie specjalnym działalność polegająca na incydentalnym, niemającym charakteru zarobkowego, zorganizowanego i ciągłego, wyrobie broni palnej lub amunicji albo handlu nimi.

Ustawodawca przewidział złagodzenie odpowiedzialności dla sprawcy działającego nieumyślnie.

Niemniej jednak w obydwu przypadkach przedmiot przestępstwa obligatoryjnie podlega przepadkowi na rzecz Skarbu Państwa. Dotyczy to również innych przedmiotów, które służyły lub były przeznaczone do popełnienia przestępstwa, albo pochodzących bezpośrednio lub pośrednio z przestępstwa, chociażby nie stanowiły własności sprawcy.

[79] Art. 30 ust. 1 ustawy o obrocie specjalnym.
[80] Tekst jednolity: Dz.U. z 2015 r. poz. 584.

Jak zaznaczono na wstępie niniejszego opracowania, zasadniczym elementem właściwości rzeczowej ABW w zakresie obrotu o znaczeniu strategicznym jest art. 5 ust. 1 pkt 2 lit. d ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, który określa obszar rozpoznania, zapobiegania i wykrywania przestępstw (…) *w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa* oraz ściganie ich sprawców. Wynikają z niego zadania ABW opierające się na zapobieganiu przestępstwom określonym przepisami karnymi ustawy dotyczącej obrotu towarami o znaczeniu strategicznym oraz obrotu specjalnego, rozpoznawaniu ich oraz ich wykrywaniu. Ta właściwość jest poparta rolą Agencji Bezpieczeństwa Wewnętrznego w procesach regulacji, kontroli wytwarzania i obrotu tymi dobrami.

Należy dodać, że w ramach ustawy o obrocie towarami o znaczeniu strategicznym uprawnienia ma także Służba Celna. Zgodnie z art. 2 ust. 1 pkt 4 ustawy z 27 sierpnia 2009 r. o Służbie Celnej[81] do jej zadań należy rozpoznawanie, wykrywanie i zwalczanie przestępstw oraz wykroczeń związanych z naruszaniem przepisów dotyczących wprowadzania na terytorium Rzeczpospolitej Polskiej oraz wyprowadzania z jej terytorium towarów objętych ograniczeniami lub zakazami obrotu ze względu na bezpieczeństwo i porządek publiczny lub bezpieczeństwo międzynarodowe, szczególnie takich, jak odpady, substancje chemiczne i ich mieszaniny, materiały jądrowe i promieniotwórcze, środki odurzające i substancje psychotropowe, broń, amunicja, materiały wybuchowe oraz towary i technologie o znaczeniu strategicznym[82].

1. Algorytm działania komórek operacyjno-śledczych ABW

Przedstawione powyżej zagadnienia natury formalnej stanowią punkt wyjścia do próby opracowania schematu działań Agencji Bezpieczeństwa Wewnętrznego w przypadku zgromadzenia lub uzyskania informacji o nieprawidłowościach w obrocie towarami o znaczeniu strategicznym. Ten schemat winien zawierać esencję dotychczasowych doświadczeń, które konstruktywnie przyczynią się do wskazania prawidłowych reakcji na dany problem. Taka praktyka, stosowana należycie i jednolicie, pozwoli na usprawnienie zarówno etapu przedprocesowo-wywiadowczego, jak i etapu następującego już po wszczęciu postępowania przygotowawczego. Niezbędne jest przy tym określenie podstawowych zadań funkcjonariuszy pionu kontrwywiadu ABW, a także określenie właściwego momentu skierowania sił pionu postępowań karnych do działań o charakterze procesowym. Prawidłowe decyzje w tym zakresie spowodują zwiększenie efektywności ABW i organów współpracujących.

Analiza spraw realizowanych dotychczas przez ABW pozwoliła na zaobserwowanie stałych punktów pojawiających się przy stwierdzeniu nieprawidłowości w obrocie towarami o znaczeniu strategicznym. Elementami niestałymi, charakterystycznymi dla danego, konkretnego rozpracowania są sposób inicjowania procedur o charakterze operacyjno-rozpoznawczym oraz moment wszczęcia postępowania przygotowawczego. Te elementy można pogrupować w następujące kategorie[83]:

[81] Tekst jednolity: Dz.U. z 2014 r. poz. 1404.

[82] Trzeba wspomnieć także o uprawnieniach Straży Granicznej, które mają charakter subsydiarny wobec wyżej wymienionych. Sa one uregulowane w art. 1 ust. 12 i 13 ustawy z 12 X 1990 r. o Straży Granicznej (Dz.U. z 2014 r. poz. 1402), w którym są zawarte zadania tej służby, takie jak zapobieganie transportowaniu – bez zezwolenia wymaganego w myśl odrębnych przepisów – przez granicę państwową odpadów, szkodliwych substancji chemicznych, materiałów jądrowych i promieniotwórczych, a także zanieczyszczaniu wód granicznych oraz przemieszczaniu środków odurzających, substancji psychotropowych, broni, amunicji i materiałów wybuchowych.

[83] Zawiera ono najczęstsze przypadki występujące w ostatnich pięciu latach. Konfiguracje opisane

1.1. Sprawy własne

Informacja – rozpracowanie – uzasadnienie podejrzenia – wszczęcie śledztwa – zabezpieczenie rzeczy i zabezpieczenie przechowywania dowodów – potwierdzenie właściwości rzeczy – ustalenie kręgu osób podejrzanych – kwalifikacja prawna czynu – merytoryczne zakończenie.

Wszelkie działania organów mających uprawnienia operacyjno-rozpoznawcze rozpoczynają się od uzyskania informacji. Informacja powinna zawierać elementy istotne do jej dalszego wykorzystania. Będą to przede wszystkim dane merytoryczne umożliwiające identyfikację nieprawidłowości, czasu ich wystąpienia, ewentualnie identyfikację sprawców danego czynu i pobudek, jakimi się kierowali przy popełnianiu czynu zabronionego. Oprócz powyższego muszą to być informacje przynajmniej wskazujące na właściwość rzeczową ABW do ich rozpoznania w ramach procedury określonej przez wewnętrzne przepisy. Pozyskiwanie informacji o takich właściwościach jest więc, a przynajmniej powinno być, priorytetem pionu operacyjno-rozpoznawczego.

W świetle dotychczasowych rozważań istotnymi elementami informacji z zakresu właściwości rzeczowej ABW będą elementy wskazujące na zagrożenia lub nieprawidłowości[84] przy produkcji i obrocie towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa. Będzie tutaj pożądana także informacja o ewentualnych osobach mających związek z tymi nieprawidłowościami. Zasadniczo przy uzyskiwaniu takich informacji należy dążyć do zebrania jak najbardziej szczegółowych danych, które będą stanowiły substraty dalszej pracy operacyjnej. Opracowaniem tych informacji będzie także wstępna analiza i identyfikacja ich poszczególnych elementów składowych, zwłaszcza wiadomość, czy zawierają one dane o charakterze zagrożenia lub nieprawidłowości, o rodzaju produktu reglamentowanego oraz o osobach uczestniczących w poszczególnych stadiach czynu.

Kolejnym etapem będzie decyzja o podjęciu czynności zmierzających do sprawdzenia uzyskanych informacji, a także do rozpracowania i zidentyfikowania ewentualnego przestępstwa i nieprawidłowości oraz wskazania osób, które mogą coś wiedzieć na ten temat, oraz tych, którzy mogą ponosić odpowiedzialność za naruszenie prawa. W ramach powyższych działań już na etapie operacyjnym jest niezbędna współpraca z Ministerstwem Gospodarki oraz z Ministerstwem Spraw Wewnętrznych. Tutaj bowiem można dokonać podstawowych sprawdzeń[85] dotyczących procedury operacyjnej albo następującego po niej procesu karnego, a mianowicie ustalenia, czy dany podmiot posiada stosowne zezwolenie lub koncesję oraz – w przypadku odpowiedzi pozytywnej – jakie warunki zostały określone w tej decyzji. Ten etap daje wiele możliwości operacyjnego zweryfikowania uzyskanych informacji, od przeglądu zasobów internetowych[86], przez pracę z aktywami osobowymi, aż do możliwości stosowania innych, zaawansowanych metod pracy operacyjnej[87]. Ważne jest także zainicjowanie współpracy ze służbami partnerskimi, która będzie miała wpływ na późniejszą formę i nierzadko zakres międzynarodowej pomocy prawnej w sprawie karnej.

w pkt a–c będzie można wykorzystać również w nieujętym w niniejszym opracowaniu stanie faktycznym.

[84] W ogólnym tego słowa znaczeniu.

[85] Być może jest to oczywiste, niemniej, jak pokazuje doświadczenie, o te informacje należy często uzupełniać stosowne procedury przed ich ewolucją do procesu karnego.

[86] Z niewiadomych przyczyn, często lekceważonych, a zawierających wiele istotnych informacji o podmiotach, ich kontaktach, osobach upoważnionych do kontaktowania się itd.

[87] Ważne jest jednak, aby skupić się na istocie sprawy, a ta winna być rozpatrywana według znamion czynu zabronionego wskazanych w ustawie o obrocie towarami o znaczeniu strategicznym.

Równolegle należy także dokonać sprawdzenia, czy na towar przeznaczony do obrotu są wymagane stosowne zezwolenie lub koncesja. Chodzi tutaj o wstępne przyporządkowanie przedmiotu produkcji lub obrotu do właściwego wykazu produktów reglamentowanych. Powinno się to opierać na określeniu tożsamości danego towaru, tj. czy jest on produktem podwójnego zastosowania, czy uzbrojeniem, w tym czy widnieje na wykazie rodzajów broni i amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym i policyjnym[88]. Tego typu informacje muszą być aktualne[89].

Oba omówione powyżej etapy operacyjnej weryfikacji uzyskanych wiadomości przy założeniu pozytywnym będą skutkować uzasadnieniem podejrzenia popełnienia przestępstwa. To uzasadnienie powinno być obiektywne i wielopłaszczyznowe, powinno też mieć potwierdzenie w różnych źródłach wiedzy. Tak rozpracowana sytuacja operacyjna i tym samym zweryfikowany materiał zawierający wskazanie miejsca, czasu i osób odpowiedzialnych za popełnienie czynów zabronionych będą stanowiły odpowiedni materiał do podjęcia przez prokuratora decyzji o wszczęciu postępowania karnego.

Finał rozpracowania operacyjnego i wszczęcie postępowania przygotowawczego to właściwy moment do zaangażowania pionu postępowań karnych ABW. *Jeżeli zachodzi uzasadnione podejrzenie popełnienia przestępstwa, wydaje się z urzędu lub na skutek zawiadomienia o przestępstwie postanowienie o wszczęciu śledztwa, w którym określa się czyn będący przedmiotem postępowania oraz jego kwalifikację prawną*[90]. Wówczas też wszelkie podejmowane czynności winny przybrać formę dwutorowego rozpoznania ujawnionego przestępstwa, z jednej strony – procesowej waloryzacji materiałów z etapu operacyjno-rozpoznawczego i gromadzenia dowodów, z drugiej – pozaprocesowej kontynuacji badania okoliczności sprawy i wspierania śledztwa.

Dotychczasowa praktyka pokazuje, że zasadniczo pierwszą czynnością śledztwa powinno być prawidłowe zabezpieczenie dowodów rzeczowych, tj. produktów podwójnego zastosowania lub wymienionych w wykazie uzbrojenia, na które jest wymagane stosowne zezwolenie. Jednak problemy mogą wyniknąć już na samym początku i mogą być związane z przechowywaniem dowodów wielkogabarytowych[91]. Jak pokazuje doświadczenie w tym zakresie, nieocenioną pomoc i współpracę niosą właściwe jednostki Służby Celnej, wojska i komend wojewódzkich Policji. To z nimi można uzgodnić właściwe przechowywanie zabezpieczonych rzeczy. Dobra i prawidłowa współpraca niesie za sobą kolejny pozytywny aspekt – redukuje koszty związane z organizacją depozytu. Warto tutaj, już na etapie zabezpieczenia przedmiotów, mieć na względzie to, że w sytuacji ewentualnego zakończenia sprawy skazaniem może być orzeczony przepadek zarówno towarów o znaczeniu strategicznym, jak i innych przedmiotów służących lub przeznaczonych do popełnienia przestępstwa. To samo dotyczy przedmiotów pochodzących bezpośrednio lub pośrednio z ujawnionego przestępstwa, chociażby nie stanowiły one własności sprawcy.

---

[88] Dla przykładu można się posłużyć informacją o mającym nastąpić eksporcie pojazdu opancerzonego bez zezwolenia. Mając informacje o pojeździe lądowym, dokonuje się sprawdzenia w wykazie uzbrojenia, w pozycji LU6, tj. dotyczącym pojazdów naziemnych i ich elementów składowych, takich jak pojazdy naziemne oraz ich elementy składowe specjalnie zaprojektowane lub zmodyfikowane do celów wojskowych oraz inne pojazdy naziemne i ich określone elementy składowe. Zaznaczenia wymaga tu dokładne czytanie uwag technicznych i wyłączających. Po spełnieniu warunków opisanych w pozycji LU6 wykazu uzbrojenia przystępuje się do dalszego działania.

[89] Wykazy są na bieżąco aktualizowane.

[90] Art. 303 kpk.

[91] Co często się zdarza w przypadku uzbrojenia i jego elementów.

Po wykonaniu wymienionych podstawowych czynności należy podjąć działania zmierzające do potwierdzenia właściwości zabezpieczonych rzeczy, lokujących je wśród produktów podwójnego zastosowania lub wśród pozycji listy uzbrojenia, na obrót którym jest wymagane zezwolenie. W realizacji powyższego celu pomocne, a w zasadzie niezbędne, są instytucje naukowe i specjalistyczne[92] oraz biegli i osoby z wiedzą specjalną. Z reguły czas oczekiwania na opinię jest stosunkowo długi, tak więc należy go przeznaczyć na realizację wszelkich czynności śledczych, w tym przede wszystkim wynikających z dotychczasowego urobku operacyjnego. To także korzystny moment do sformułowania wniosków dotyczących międzynarodowej pomocy prawnej[93].

Czynności procesowe realizowane w opisany powyżej sposób mają na celu wszechstronne wyjaśnienie okoliczności popełnienia czynu, w tym wykrycie sprawcy (sprawców) przestępstwa i pociągnięcie go (ich) do odpowiedzialności karnej. Priorytetem w tej fazie postępowania winno być ustalenie kręgu osób biorących udział w popełnieniu przestępstwa. Niezbędne przy tym jest precyzyjne wskazanie stopnia zaangażowania i roli poszczególnych osób. Od tego bowiem zależy właściwa kwalifikacja rozpoznawanych czynów przestępczych.

W toku wyjaśniania okoliczności popełnienia czynu oraz ustalania kręgu osób zaangażowanych w popełnienie przestępstwa nie można pominąć odpowiedzialności majątkowej sprawców czynu zabronionego. Dotyczy to także podmiotów gospodarczych realizujących obrót. W tym zakresie analiza przepisów ustawy o obrocie strategicznym wskazuje na konieczność zainicjowania stosownego postępowania administracyjnego. Winno to być poprzedzone, jak się wydaje, przekazaniem właściwych informacji ustalonych podczas śledztwa i wspierającej je procedury operacyjnej. Współpraca Agencji Bezpieczeństwa Wewnętrznego i Służby Celnej z Ministerstwem Gospodarki w tym zakresie jest niezbędna, ponieważ to organ kontroli, w drodze decyzji administracyjnej, nakłada karę pieniężną.

Czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze przeprowadzone w opisany wyżej sposób będą stanowiły podstawę do merytorycznego zakończenia postępowania. Ich prawidłowe wykonanie będzie gwarantowało zgromadzenie materiału dowodowego pozwalającego na obiektywną weryfikację zagadnień dotyczących znamion rozpoznawanego czynu i wszechstronnego wyjaśnienia okoliczności jego popełnienia.

1.2. Sprawy wynikające ze współpracy ze Służbą Celną

Informacja wynikająca ze współpracy z organami Służby Celnej – weryfikacja informacji – uzasadnienie podejrzenia popełnienia przestępstwa – wszczęcie śledztwa – zabezpieczenie rzeczy i zabezpieczenie ich przechowywania – potwierdzenie właściwości rzeczy – ustalenie kręgu osób podejrzanych – kwalifikacja prawna czynu – merytoryczne zakończenie.

Gros spraw dotyczących obrotu strategicznego wynika ze współpracy z organami Służby Celnej. Jest to oczywiste, zważywszy że każdy w zasadzie towar będący przedmiotem czynności handlowych z zagranicą prędzej czy później będzie przedmiotem postępowania właściwego organu Służby Celnej. To ten organ wreszcie, weryfikujący dokumenty zgłoszeń celnych, jest uprawniony do przeprowadzania kontroli celnych. Na tej płaszczyźnie warto wypracować dobre mechanizmy współpracy, które będą skutkowały prawidłową reakcją na stwierdzone nieprawidłowości bądź też na ich podejrzenie.

[92] Na przykład wyższe uczelnie, zakłady i instytuty wojskowe, chemiczne.

[93] Biorąc pod uwagę czas realizacji, w tym czas nadania przez wszystkie szczeble polskiej prokuratury, oraz czas przekazania do realizacji właściwym organom państwa, do którego zapytanie jest kierowane.

Służba Celna, z uwagi na wiele realizowanych zadań (m.in. dotyczących wykroczeń i przestępstw skarbowych) z reguły bez problemów przekazuje Agencji Bezpieczeństwa Wewnętrznego informacje o podejrzeniu nielegalnego obrotu towarami strategicznymi. Na tym etapie jednak należy ostrożnie podchodzić do tego typu informacji z uwagi na konieczność ich przedprocesowego zweryfikowania. Te działania są z reguły obarczone klauzulą pilności i niezwłocznego wykonania. Tutaj właśnie powinien się wykazać pion kontrwywiadu, szczególnie jeśli chodzi o uzyskiwanie danych uzasadniających ewentualne czynności o charakterze procesowym[94].

W pierwszej kolejności, podobnie jak w pkt 1.1., należy dokonać sprawdzenia informacji uzyskanych od Służby Celnej. W kręgu zainteresowań powinny się znaleźć powody, z jakich funkcjonariusze celni zakwestionowali towar. Należy też wskazać podstawy wysuwanych podejrzeń. Ta wstępna ocena będzie się wiązać z dalszymi czynnościami ustaleniowymi. Istotną, jeśli nie najistotniejszą, rolę w takich przypadkach odgrywają skutecznie zabezpieczone źródła informacji umożliwiające weryfikację wiadomości o charakterze specjalistycznym. Niezbędne jest tutaj potwierdzenie właściwości przedmiotu lub przynajmniej wskazanie właściwego kierunku jego identyfikacji[95]. Przeprowadzanie tych działań umożliwia planowo, perspektywicznie i celowo realizowana praca operacyjna.

Na uwagę zasługuje tu możliwość zyskania na czasie. Otóż w pierwszej kolejności, zanim jeszcze dany stan uzasadni podejrzenia dotyczące naruszeń przepisów o obrocie strategicznym, występuje uzasadnione podejrzenie dokonania oszustwa celnego[96]. Dochodzi do niego np. w przypadku stwierdzenia niezgodności towaru z deklaracją bądź też różnicy wartości towaru z wartością deklarowaną przez zgłaszającego itd. W takich sytuacjach, aby zyskać czas niezbędny do zgromadzenia informacji uzasadniających wszczęcie śledztwa z art. 33 ustawy o obrocie strategicznym, można zainicjować procedurę w opisanym wyżej trybie karno-skarbowym.

W podsumowaniu należy zaznaczyć, że włączenie się do działań pionu postępowań karnych warunkują sprawdzone dane operacyjne pochodzące od Służby Celnej. Przy założeniu, że wskazują one na uzasadnione podejrzenia, dalsze czynności procesowe, poczynając od ich wszczęcia do merytorycznego zakończenia, powinny być analogiczne jak w pkt 1.1.

1.3. Sprawy wynikające ze współpracy z organem kontroli

Informacja wynikająca ze współpracy z Ministerstwem Gospodarki – uzasadnienie podejrzenia popełnienia przestępstwa – wszczęcie śledztwa – zabezpieczenie rzeczy i zabezpieczenie jej przechowywania – potwierdzenie właściwości rzeczy – ustalenie kręgu osób podejrzanych – kwalifikacja prawna czynu – merytoryczne zakończenie postępowania przygotowawczego.

---

[94] Tu zawierają się również sprawy, w których są podejmowane czynności niecierpiące zwłoki, tj. w trybie art. 308 kpk. Tę kategorię spraw należy traktować jako zdarzenia skutkujące koniecznością podjęcia natychmiastowych czynności procesowych. Co do zasady tryb postępowania się nie zmienia, ale działania Agencji Bezpieczeństwa Wewnętrznego są jednak prowadzone pod presją czasu określonego na maksymalnie pięć dni od momentu przeprowadzenia pierwszej czynności. Pomocne w tym przypadku jest subsydiarne skorzystanie z wewnętrznych regulacji ABW, a mianowicie z zapisów *Decyzji nr 12 Szefa ABW z dnia 31 stycznia 2011 r. w sprawie sposobu reagowania w ABW w przypadku informacji o wystąpieniu zdarzenia o charakterze terrorystycznym ustanawiającego dyżury członków zespołów reagowania*.

[95] Na tym etapie weryfikacji.

[96] Art. 87 kks: *Kto przez wprowadzenie w błąd organu uprawnionego do kontroli celnej naraża należność celną na uszczuplenie* (…).

Jak wynika z przepisów karnych ustawy o obrocie strategicznym, nie tylko obrót towarami strategicznymi bez zezwolenia jest działaniem bezprawnym. Jest nim również obrót tymi towarami wbrew warunkom określonym w zezwoleniu. Ta kategoria spraw, jak się wydaje, powinna być obiektem działalności kontrolnej zwłaszcza Ministerstwa Gospodarki[97]. Minister gospodarki stoi na straży obrotu strategicznego i został w tym celu wyposażony w stosowne uprawnienia kontrolne. W wyniku przeprowadzenia wyżej wymienionych czynności dotyczących stwierdzonych błędów organ kontroli wzywa do przywrócenia stanu zgodnego z ustawą.

W przypadku gdy stwierdzi się złamanie warunków zezwolenia na obrót towarami strategicznymi oprócz wyżej wymienionego wezwania organ kontroli powinien wystosować zawiadomienie do właściwych organów o uzasadnionym podejrzeniu popełnienia przestępstwa. Ewentualna reakcja podmiotu na to wezwanie warunkuje skorzystanie z dobrodziejstwa przepisu przewidującego łagodniejsze potraktowanie nieumyślnego sprawcy wadliwego obrotu produktami strategicznymi, który naprawił swój błąd.

Działania operacyjne powinny być skoncentrowane na ścisłej i bieżącej współpracy z organem kontroli. Na szczególną uwagę zasługuje tu m.in. możliwość uczestniczenia funkcjonariuszy ABW w czynnościach kontrolnych, a także możliwość powołania zespołu złożonego z funkcjonariuszy i żołnierzy organów opiniujących oraz z ekspertów i biegłych. Tym samym można stworzyć naturalną sytuację operacyjną o potencjale informacyjnym porównywalnym z przeprowadzaniem oficjalnych czynności procesowych.

Podobnie jak wcześniej, algorytm dalszych czynności pozostaje niezmienny, zważywszy że przymiot uzasadnionego podejrzenia co do właściwości produktu i działania wbrew warunkom zezwolenia został potwierdzony podczas kontroli.

Bibliografia:

Publikacje zwarte:

1. *Unia Europejska a obrót towarami strategicznymi. Nowe regulacje – nowe wyzwania*, J. Barcz, J. Bokszczanin (red.), Warszawa 2013, Elipsa.
2. Wyrok Naczelnego Sądu Administracyjnego w Warszawie z 28 II 2013 r. nr II GSK 1617/11.
3. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 12 VII 2006 r. nr VI SA/Wa 997/06.

Akty prawne:

1. *Konwencja w sprawie znakowania plastycznych materiałów wybuchowych w celu ich wykrywania, podpisana w Montrealu dnia 1 marca 1991 r.* (Dz.U. z 2007 r. Nr 135 poz. 948).
2. Rezolucja Rady Bezpieczeństwa ONZ nr 1540 z 28 IV 2004 r.
3. *Rozporządzenie Ministra Finansów z dnia 25 czerwca 2013 r. w sprawie urzędów celnych, w których może być dokonywany wywóz, przywóz i tranzyt towarów o znaczeniu strategicznym* (Dz.U. z 2015 r. poz. 136).

[97] Nie można tu wykluczyć inicjatywy własnej jednostek operacyjno-rozpoznawczych.

4. *Rozporządzenie Ministra Gospodarki z dnia 19 maja 2014 r. w sprawie krajowego zezwolenia generalnego* (Dz.U. z 2014 r. poz. 702).
5. *Rozporządzenie Ministra Gospodarki z dnia 8 maja 2014 r. w sprawie wykazu uzbrojenia, na obrót którym jest wymagane zezwolenie* (Dz.U. z 2014 r. poz. 627).
6. *Rozporządzenie Ministra Gospodarki z dnia 13 marca 2015 r. w sprawie wykazu uzbrojenia, na obrót którym jest wymagane zezwolenie* (Dz.U. z 2015 r. poz. 387).
7. *Rozporządzenie Ministra Gospodarki z dnia 13 maja 2013 r. w sprawie zakresu informacji przekazywanych organowi kontroli obrotu przez podmiot dokonujący obrotu towarami o znaczeniu strategicznym w ramach zezwoleń generalnych* (Dz.U. z 2013 r. poz. 620).
8. *Rozporządzenie Parlamentu Europejskiego i Rady UE 2015/479 z dnia 11 marca 2015 r. w sprawie wspólnych reguł wywozu* (tekst jednolity: Dz.U. UE L z 27 III 2015 r. nr 83 poz. 34).
9. *Rozporządzenie Rady Ministrów z dnia 3 grudnia 2001 r. w sprawie rodzajów broni i amunicji oraz wykazu wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub obrót jest wymagana koncesja* (Dz.U. z 2001 r. Nr 145 poz. 1625, ze zm.).
10. *Rozporządzenie Rady (WE) nr 1061/2009 z dnia 13 października 2009 r. ustanawiające wspólne reguły wywozu* (Dz.U. UE L z 7 XI 2009 r. nr 291 poz. 1).
11. *Rozporządzenie Rady (EWG) nr 2913/92 z dnia 12 października 1992 r. ustanawiające Wspólnotowy Kodeks Celny* (Dz.U. UE L z 19 X 1992 r. nr 302 poz. 1).
12. *Rozporządzenie Rady (WE) nr 1334/2000 z dnia 22 czerwca 2000 r. ustanawiające wspólnotowy system kontroli eksportu produktów i technologii podwójnego zastosowania* (Dz.U. UE L z 30 VI 2000 r. nr 159 poz. 1).
13. *Rozporządzenie Rady (WE) nr 428/2009 z dnia 5 maja 2009 r. ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania* (Dz.U. UE L z 29 V 2009 r. nr 134 poz. 1).
14. *Rozporządzenie z dnia 3 grudnia 2001 r. w sprawie rodzajów broni i amunicji oraz wykazu wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub obrót jest wymagana koncesja* (Dz.U. z 2001 r. Nr 145 poz. 1625, ze zm.).
15. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (Dz.U. z 1997 r. Nr 88 poz. 553, ze zm.).
16. *Ustawa z dnia 10 września 1999 r. – Kodeks karny skarbowy* (tekst jednolity: Dz.U. z 2013 r. poz. 186, ze zm.).
17. *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (tekst jednolity: Dz.U. z 2016 r. poz. 23, ze zm.).
18. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (Dz.U. z 1997 r. Nr 89 poz. 555, ze zm.).
19. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (tekst jednolity: Dz.U. z 2015 r. poz. 1929, ze zm.).
20. *Ustawa z dnia 21 maja 1999 r. o broni i amunicji* (tekst jednolity: Dz.U. z 2012 r. poz. 576, ze zm.).
21. *Ustawa z dnia 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego* (tekst jednolity: Dz.U z 2015 r. poz. 1100, ze zm.).
22. *Ustawa z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzy-*

mania międzynarodowego pokoju i bezpieczeństwa (tekst jednolity: Dz.U. z 2013 r. poz. 195, ze zm.).
23. *Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej* (tekst jednolity: Dz.U. z 2015 r. poz. 990, ze zm.).
24. *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (tekst jednolity: Dz.U. z 2014 r. poz. 253, ze zm.).
25. *Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (tekst jednolity: Dz.U. z 2014 r. poz. 1402, ze zm.).
26. *Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej* (tekst jednolity: Dz.U. z 2015 r. poz. 584, ze zm.).
27. *Ustawa z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym* (tekst jednolity: Dz.U. z 2012 r. poz. 1017, ze zm.).
28. *Wspólne stanowisko Rady 2008/944/WPZiB z dnia 8 grudnia 2008 r. określające wspólne zasady kontroli wywozu technologii wojskowych i sprzętu wojskowego* (Dz.U. UE L z 13 XII 2008 r. nr 335 poz. 99).
29. *Wspólny wykaz uzbrojenia Unii Europejskiej przyjęty przez Radę w dniu 17 marca 2014 r., sprzęt objęty Wspólnym Stanowiskiem Rady 2008/944/WPZiB określającym wspólne zasady kontroli wywozu technologii wojskowych i sprzętu wojskowego (uaktualnia i zastępuje wspólny wykaz uzbrojenia Unii Europejskiej przyjęty przez Radę w dniu 11 marca 2013 r.)* – Dz.U.UE C z 27 III 2013 r. nr 90 poz. 1).

Abstrakt

Pierwotną intencją niniejszego artykułu była potrzeba wypracowania prawidłowych algorytmów działania Agencji Bezpieczeństwa Wewnętrznego na wypadek pojawienia się sytuacji i problemów dotyczących obrotu strategicznego. Poprawne określenie właściwych reakcji instytucji państwowych implikowało konieczność wskazania podstaw prawnych oraz faktycznych intencji ustawodawcy regulującego tak istotny obszar działania państwa.

Z uwagi na funkcjonowanie Rzeczpospolitej Polskiej w strukturach Unii Europejskiej, Organizacji Narodów Zjednoczonych itd. oraz na międzynarodowe zobowiązania naszego kraju zaprezentowane prawo krajowe należało umiejscowić w obowiązującym prawie międzynarodowym. Doprowadziło to do powstania kompilacji najistotniejszych przepisów prawnych regulujących omawianą problematykę, wspartych komentarzem praktyka z „linii działań".

Rozważania przedstawione w artykule nie zamykają tematu. Chociażby już po złożeniu niniejszego materiału w Redakcji PBW pojawiły się głosy dotyczące nieprecyzyjnej definicji ustawowej pojęcia t r a n z y t, które mogą stanowić punkt wyjścia do bieżących działań poszczególnych jednostek ABW i swego rodzaju bazę do dalszej, jeszcze bardziej szczegółowej dyskusji.

Słowa kluczowe: obrót strategiczny, podwójne zastosowanie, uzbrojenie, wywóz, transfer.

Abstract

The initial intention which triggered out the realization of this elaboration was the desire, or rather a necessary need of working out correct algorithms of action of the Internal Security Agency for situations and problems occurring within its assigned role in the system of a strategic trade procedure. This correct delimitation of necessary reactions of state institutions implied the necessity to point out legal basis and factual intentions of legislator regulating such an essential area of state actions.

Regarding the functioning of Republic of Poland within the European Union structures, United Nations Organizations etc., and considering international duties and commitment of Poland, the domestic law shown was to be placed in already existing international law.

This caused compilations of the most crucial legal regulations governing the matter considered, supported by the commentary of an "action line" practitioner.

The considerations presented of course, do not drain the topic, like after issuing this article, occurring divagations considering unprecise definition of statutory "transit", but they can constitute the starting point for current actions of individual departments of Internal Security Agency as well as a peculiar base for further, even more detailed discussion.

Keywords: strategic trade, dual use, weapon, export, transfer.

Marcin Piotrak

Rola i zadania szefa Agencji Bezpieczeństwa Wewnętrznego w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej

Sprawne zarządzanie sytuacjami kryzysowymi wymaga zaangażowania i współpracy wielu podmiotów reprezentujących zarówno organy administracji państwowej, samorządu terytorialnego, przedsiębiorców, jak i obywateli. Wymiana doświadczeń i informacji oraz wsparcie i pomoc w chwili próby jest nieodzownym elementem walki z zagrożeniami. Nie należy jednak zapominać o tym, że (…) *istotą zarządzania kryzysowego jest działalność mająca na celu w szczególności przeciwdziałanie powstawaniu sytuacjom kryzysowym i sprawne ich rozwiązywanie (reagowanie) już w momencie wystąpienia, w drodze zaplanowanych działań*[1]. Do szefa Agencji Bezpieczeństwa Wewnętrznego (ABW) jako centralnego organu administracji państwowej należy wykonywanie zadań i odgrywanie roli najważniejszego podmiotu w zakresie przeciwdziałania zagrożeniom terrorystycznym oraz zagrożeniom występującym w cyberprzestrzeni, które mogą doprowadzić do sytuacji kryzysowej w Rzeczpospolitej Polskiej.

Działania podejmowane przez ABW w zakresie zarządzania kryzysowego i ochrony infrastruktury krytycznej (IK) są realizowane w kilku obszarach: przeciwdziałania zagrożeniom terrorystycznym, cyberprzestrzeni, systemów telekomunikacyjnych oraz monitorowania tych zagrożeń; funkcjonowania ABW w sytuacji kryzysowej; udziału szefa ABW w pracach Rządowego Zespołu Zarządzania Kryzysowego (RZZK); współpracy szefa ABW z Rządowym Centrum Bezpieczeństwa (RCB) i administracją centralną; współpracy szefa ABW z terenowymi organami zarządzania kryzysowego oraz współpracy szefa ABW z posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej.

Rola i zadania szefa ABW w przeciwdziałaniu zagrożeniom terrorystycznym, zagrożeniom cyberprzestrzeni i systemów telekomunikacyjnych

Zadania i obowiązki uczestników systemu zarządzania kryzysowego w Polsce wynikają z wielu aktów prawnych. To powoduje, że wielokrotnie dochodzi do sytuacji, w której odpowiedzialność za przeciwdziałanie określonemu zagrożeniu leży w kompetencjach kilku podmiotów. W celu odzwierciedlenia rzeczywistego podziału kompetencyjnego stworzono Krajowy Plan Zarządzania Kryzysowego (KPZK) w formie siatki bezpieczeństwa (tab. 1). Dzięki temu, że wiedza w nim zawarta została przedstawiona w formie przekrojowej, istnieje możliwość zmiany, ulepszania oraz tworzenia nowych procedur i zależności systemowych. Agencja Bezpieczeństwa Wewnętrznego została wskazana w tym planie jako uczestnik zarządzania kryzysowego w trzech kategoriach zagrożeń: terrorystycznych, cyberprzestrzeni oraz systemów telekomunikacyjnych.

[1] G. Sobolewski, *Wprowadzenie*, w: *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, G. Sobolewski, D. Majchrzak (red.), Warszawa 2011, s. 11.

Tab. 1. Zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa.

ZARZĄDZANIE KRYZYSOWE	FAZA ZARZĄDZANIA KRYZYSOWEGO	Ministerstwo Spraw Wewnętrznych	Ministerstwo Administracji i Cyfryzacji	Ministerstwo Zdrowia	Ministerstwo Środowiska	Ministerstwo Infrastruktury i Rozwoju	Ministerstwo Obrony Narodowej	Ministerstwo Gospodarki	Ministerstwo Finansów	Ministerstwo Skarbu Państwa	Ministerstwo Edukacji Narodowej	Ministerstwo Nauki i Szkolnictwa Wyższego	Ministerstwo Spraw Zagranicznych	Agencja Bezpieczeństwa Wewnętrznego	Agencja Wywiadu	Rządowe Centrum Bezpieczeństwa	Prezydent RP	Rada Ministrów	Prezes Rady Ministrów	Wojewoda
Zagrożenia systemów telekomunikacyjnych	zapobieganie	Ws	W																	
	przygotowanie	Ws	W				Ws		Ws	Ws			Ws	Ws	Ws	Ws		Ws		Ws
	reagowanie	Ws	W																	
	odbudowa		W																	
Zagrożenia terrorystyczne	zapobieganie	Ws				Ws	Ws	Ws	Ws					W	Ws	Ws		Ws		Ws S
	przygotowanie	W	Ws	Ws		Ws	Ws							Ws		Ws		Ws		Ws
	reagowanie	W	Ws	Ws	Ws PAA	Ws	Ws	Ws					Ws	Ws		Ws	Ws	Ws		Ws
	odbudowa	W	Ws	Ws		Ws	Ws	Ws	Ws					Ws	Ws	Ws				Ws
Zagrożenia cyberprzestrzeni	zapobieganie	Ws	Ws				Ws			Ws	Ws	Ws		W	Ws	Ws		Ws	Ws	Ws
	przygotowanie	Ws	Ws				Ws			Ws				W		Ws		Ws		Ws
	reagowanie	Ws	Ws				Ws			Ws				W		Ws	Ws	Ws		Ws
	odbudowa	Ws					Ws			Ws				W	Ws	Ws				Ws

Legenda:
W – wiodący
Ws – wspomagający
PAA – Państwowa Agencja Atomistyki
S – zadania realizowane przez samorząd terytorialny

Źródło: Opracowanie własne na podstawie *Krajowego Planu Zarządzania Kryzysowego 2013–2015*, s. 46, 48.

Krajowy Plan Zarządzania Kryzysowego jest sporządzany przez RCB na podstawie art. 5 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[2] (i obejmuje wszystkie fazy zarządzania kryzysowego, tj. zapobieganie, przygotowanie, reagowanie i odbudowę). Plan składa się z trzech części: planu głównego, zespołu przedsięwzięć na wypadek sytuacji kryzysowej oraz załączników funkcjonalnych planu głównego. Układ strukturalny KPZK pozwala szybko się zorientować w rozłożeniu odpowiedzialności za wykonanie zadań na poszczególne organy, umożliwia ministerstwom zaplanowanie działań legislacyjnych w fazie zapobiegania zagrożeniom, wdrażanie przyjętych ustaw i planów wykonawczych w fazie przygotowania, a także sprawdzanie w formie ćwiczeń, czy przyjęte rozwiązania są adekwatne do zagrożeń i czy instytucje mają wystarczające kompetencje oraz środki do reagowania. Ponadto uwzględniono w nim system monitorowania zagrożeń oraz zawarto wykaz i rozmieszczenie sił i środków niezbędnych do planowania przyszłych działań[3]. Plan podlega systematycznej aktualizacji, a cykl planowania nie może być dłuższy niż dwa lata.

Zagrożenia terrorystyczne

Nadrzędna rola szefa ABW przy rozpoznawaniu zagrożeń terrorystycznych, zapobieganiu aktom terroru oraz wykrywaniu i ściganiu sprawców przestępstw o charakterze terrorystycznym, zawarta w art. 5 ust. 1 pkt 2 lit. a *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[4], znalazła początkowo swoją ciągłość i uzupełnienie w ustawie o zarządzaniu kryzysowym, a obecnie została potwierdzona w *Ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[5].

Ustawa o zarządzaniu kryzysowym określa działalność poszczególnych organów państwa w przypadku wystąpienia zdarzenia o znamionach kryzysu, a także przydziela zadania związane z ochroną infrastruktury krytycznej oraz zwalczaniem zagrożeń asymetrycznych, pozostające w ścisłym związku z przepisami ustawy o działaniach antyterrorystycznych określającymi zasady prowadzenia takich działań oraz współpracę między organami właściwymi w zakresie ich realizacji. Celem tych przedsięwzięć jest przeciwdziałanie sytuacjom kryzysowym będącym skutkiem zdarzenia o charakterze terrorystycznym.

Działania antyterrorystyczne, analogicznie do zarządzania kryzysowego, zostały podzielone na cztery fazy: zapobieganie zdarzeniom o charakterze terrorystycznym[6], przygotowanie do przejmowania nad nimi kontroli przez realizację zaplanowanych

[2] Dz.U. z 2013 r. poz. 1166, ze zm.

[3] http://rcb.gov.pl/wp-content/uploads/KPZK-2013-2015.tj_..pdf [dostęp: 15 XII 2015].

[4] Tekst jednolity: Dz.U. z 2015 r. poz. 1929.

[5] Dz.U. z 2016 r. poz. 904.

[6] Zdarzenie o charakterze terrorystycznym to sytuacja powstała na skutek czynu określonego w art. 115 § 20 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny* (Dz.U. Nr 88 poz. 553, ze zm.) lub zagrożenie zaistnienia takiego czynu, mogącego doprowadzić do sytuacji kryzysowej:

Art. 115 §20. Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

1) poważnego zastraszenia wielu osób,

2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,

3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej

– a także groźba popełnienia takiego czynu.

przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz usuwanie ich skutków, w tym odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia. Ustawa o działaniach antyterrorystycznych zakłada w art. 3 ust. 1, że głównym koordynatorem polityki antyterrorystycznej i osobą odpowiedzialną za zapobieganie zdarzeniom o charakterze terrorystycznym będzie szef ABW. Natomiast jako osobę odpowiedzialną za przygotowanie i odtwarzanie zasobów po zdarzeniach o charakterze terrorystycznym, a także za reagowanie na te zdarzenia wskazano w ustawie ministra właściwego do spraw wewnętrznych. Wszystkie organy administracji publicznej, właściciele i posiadacze obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej mają obowiązek współpracować z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego przy realizacji działań antyterrorystycznych.

W ramach współpracy organy i podmioty przekazują niezwłocznie szefowi ABW informacje dotyczące zagrożeń o charakterze terrorystycznym dla infrastruktury administracji publicznej[7] lub infrastruktury krytycznej (systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych), istotne z punktu widzenia bezpieczeństwa państwa. W przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze administracji publicznej lub infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku szef ABW może wydawać polecenia[8] organom i podmiotom zagrożonym tymi zdarzeniami, mające na celu przeciwdziałanie zagrożeniom, usunięcie ich albo zminimalizowanie, oraz przekazywać im informacje niezbędne do tego celu. Organy i podmioty zagrożone mają obowiązek poinformować szefa ABW o podjętych działaniach w tym zakresie. Równocześnie szef ABW powiadamia o wydanych poleceniach i przekazanych informacjach ministra koordynatora służb specjalnych[9].

Obowiązek zapobiegania zdarzeniom o charakterze terrorystycznym spoczywający na szefie ABW jest realizowany przez współpracę Agencji Bezpieczeństwa Wewnętrznego z innymi właściwymi służbami i instytucjami. Szef ABW na podstawie ustawy o działaniach antyterrorystycznych ma uprawnienia do:

- koordynowania czynności analityczno-informacyjnych realizowanych przez służby specjalne (ABW, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego i Centralne Biuro Antykorupcyjne) oraz wymiany informacji przekazywanych przez Policję, Straż Graniczną, Biuro Ochrony Rządu, Państwową Straż Pożarną, Służbę Celną, Generalnego Inspektora Informacji Finansowej, Generalnego Inspektora Kontroli Skarbowej (GIKS), Żandarmerię Wojskową i Rządowe Centrum Bezpieczeństwa dotyczących zagrożeń o charakterze terrorystycznym oraz danych o osobach, które mogą mieć związek ze zdarzeniami o charakterze terrorystycznym, przez ich gromadzenie, przetwarzanie i analizowanie (art. 5 ust. 1);
- prowadzenia wykazu informacji o:

[7] Infrastruktura administracji publicznej to systemy oraz obiekty niezbędne dla zapewnienia bezpiecznego i ciągłego funkcjonowania organów administracji publicznej.

[8] Do czasu wejścia w życie ustawy o działaniach antyterrorystycznych szef ABW informował o podjętych działaniach dyrektora Rządowego Centrum Bezpieczeństwa.

[9] O zarządzeniu szef ABW niezwłocznie zawiadamia ministra koordynatora służb specjalnych oraz Prokuratora Generalnego.

  - osobach podejmujących działalność na rzecz organizacji terrorystycznych lub organizacji związanych z działalnością terrorystyczną albo o członkach tych organizacji,
  - poszukiwanych osobach prowadzących działalność terrorystyczną lub osobach podejrzewanych o popełnienie przestępstw o charakterze terrorystycznym, wobec których w Rzeczpospolitej Polskiej zostało wydane zarządzenie o zatrzymaniu, poszukiwaniu lub postanowienie o poszukiwaniu listem gończym, a także poszukiwanych na podstawie europejskiego nakazu aresztowania,
  - osobach, wobec których istnieje uzasadnione podejrzenie, że mogą prowadzić działania zmierzające do popełnienia przestępstwa o charakterze terrorystycznym, w tym o osobach stanowiących zagrożenie bezpieczeństwa lotnictwa cywilnego,
  - osobach uczestniczących w szkoleniach terrorystycznych lub podejmujących podróż w celu popełnienia przestępstwa o charakterze terrorystycznym (art. 6);
- koordynowania czynności operacyjno-rozpoznawczych podejmowanych przez służby specjalne, Policję, SG, GIKS i ŻW oraz obserwacji i rejestrowania (przy użyciu środków technicznych) obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom, podejmowanych przez funkcjonariuszy celnych i dotyczących zdarzeń o charakterze terrorystycznym (art. 8 ust. 1);
- wydawania służbom specjalnym, Policji, SG, GIKS, ŻW i SC zaleceń mających na celu usunięcie bądź minimalizację zaistniałego zagrożenia terrorystycznego (art. 8 ust. 2);
- zarządzania niejawnego prowadzenia czynności operacyjno-rozpoznawczych wobec osoby niebędącej obywatelem RP, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej – na okres nie dłuższy niż trzy miesiące (art. 9);
- uzyskiwania nieodpłatnie dostępu do danych i informacji zgromadzonych w rejestrach publicznych i ewidencjach prowadzonych przez organy, służby i instytucje właściwe, a także obrazu zdarzeń rejestrowanego przez urządzenia rejestrujące obraz, umieszczone w obiektach użyteczności publicznej, przy drogach publicznych i innych miejscach publicznych, oraz otrzymywania nieodpłatnie kopii zarejestrowanego zapisu tego obrazu (art. 11);
- wydawania Policji, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, zaleceń dotyczących szczególnego zabezpieczania obiektów, uwzględniających rodzaj zagrożenia o charakterze terrorystycznym – w przypadku wprowadzenia drugiego lub wyższego stopnia alarmowego (art. 12 ust. 2);
- składania wniosku – do ministra właściwego do spraw wewnętrznych – o zarządzenie zakazu odbywania zgromadzeń publicznych lub imprez masowych na obszarze lub w obiekcie objętym stopniem alarmowym, na czas obowiązywania tego stopnia, jeżeli jest to konieczne dla ochrony życia i zdrowia ludzi lub bezpieczeństwa publicznego – w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowania (art. 21 ust. 1);
- składania wniosku – do ministra właściwego do spraw wewnętrznych – w sprawie wydania decyzji o wydaleniu z terytorium RP obywatela UE lub członka rodziny niebędącego obywatelem UE, co do których istnieje obawa, że mogą

prowadzić działalność terrorystyczną lub szpiegowską, albo podejrzewanych o popełnienie jednego z tych przestępstw (art. 48 pkt 2)[10];

- składania wniosku – do ministra właściwego do spraw wewnętrznych – w sprawie wydania decyzji o zobowiązaniu do powrotu cudzoziemca, co do którego istnieje obawa, że może prowadzić działalność terrorystyczną lub szpiegowską, albo podejrzewanego o popełnienie jednego z tych przestępstw (art. 57 pkt 2)[11].

Podmioty, czyli służby specjalne, Policja, SG, BOR, PSP, SC, GIIF, GIKS, ŻW i RCB, są zobowiązane do niezwłocznego przekazywania szefowi ABW informacji służących realizacji działań antyterrorystycznych, klasyfikowanych zgodnie z wykazem zdarzeń o charakterze terrorystycznym. W wykazie wyróżniono 14 kategorii tego typu zdarzeń[12]:

1) incydenty zagrażające bezpieczeństwu Rzeczpospolitej Polskiej,
2) incydenty związane z zagranicznymi przedstawicielstwami RP i obywatelami RP przebywającymi poza jej terytorium,
3) incydenty dotyczące zagrożeń występujących poza terytorium RP, w rejonach konfliktów i kryzysów międzynarodowych mających wpływ na jej bezpieczeństwo,
4) incydenty związane z nielegalnym wytwarzaniem i posiadaniem broni palnej, amunicji i materiałów lub urządzeń wybuchowych, a także broni masowej zagłady na terytorium RP oraz obrotem nimi,
5) incydenty z zakresu produkcji i obrotu towarami, technologiami i usługami podwójnego zastosowania,
6) incydenty dotyczące zagrożenia struktur wojskowych,
7) incydenty dotyczące przestępstw i wykroczeń związanych z naruszeniem przepisów celnych,
8) incydenty dotyczące kontroli ruchu granicznego,
9) incydenty związane z pobytem cudzoziemców w RP,
10) incydenty dotyczące aktywności terrorystycznej w mediach oraz w Internecie,
11) incydenty związane z wprowadzeniem do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł,
12) incydenty dotyczące zdarzeń o charakterze terrorystycznym związanych z uprowadzeniem i wzięciem zakładników,
13) incydenty dotyczące działalności środowisk związanych z ideologią odwołującą się do przemocy lub popierających ją,
14) incydenty związane z ochroną osób, obiektów i urządzeń ochranianych przez BOR lub ŻW oraz z działalnością polityczną.

Szef ABW, stosownie do potrzeb, przekazuje w ramach wzajemności właściwym służbom, instytucjom i innym organom administracji publicznej informacje służące realizacji działań antyterrorystycznych oraz dane zawarte w wykazie osób, które mogą mieć związek z terroryzmem, także w postaci bieżących analiz stanu zagrożenia zdarzeniami o charakterze terrorystycznym. Ponadto niezwłocznie przekazuje Prezydentowi RP, Prezesowi Rady Ministrów, ministrowi właściwemu do spraw wewnętrznych, mini-

[10] Art. 73c *Ustawy z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczpospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin* (tekst jednolty: Dz.U. z 2014 r. poz. 1525, ze zm.).

[11] Art. 329a *Ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach* (Dz.U. z 2013 r. poz. 1650, ze zm.).

[12] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym* (Dz.U. z 2016 r. poz. 1092).

strowi obrony narodowej, ministrowi właściwemu do spraw zagranicznych oraz ministrowi koordynatorowi służb specjalnych informacje mogące mieć istotne znaczenie dla zapobiegania zdarzeniom o charakterze terrorystycznym.

Kompetencje szefa ABW w zakresie koordynacji gromadzenia, przetwarzania, analizowania oraz udostępniania informacji dotyczących zdarzeń o charakterze terrorystycznym, w tym danych osobowych sprawców tych przestępstw, określone na poziomie ustawy, wzmacniają pozycję szefa ABW jako organu odpowiedzialnego za koordynację wymiany informacji pomiędzy uczestnikami systemu antyterrorystycznego RP. Ustawa umożliwia ponadto wdrożenie wspólnych procedur reagowania w przypadku zagrożenia o charakterze terrorystycznym. Jednocześnie na szefie ABW spoczywa obowiązek stałego, szybkiego i systematycznego informowania kierownictwa państwa o zagrożeniach o charakterze terrorystycznym oraz działaniach podjętych przez właściwe służby i instytucje w związku z nimi[13].

Koordynacja czynności analityczno-informacyjnych podejmowanych przez właściwe podmioty i służby specjalne umożliwia również szefowi ABW realizację zadania wynikającego z *Zarządzenia Nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego*[14]. Zgodnie z załącznikiem nr 1[15] do tego zarządzenia szef Agencji określa aktualny poziom zagrożenia terrorystycznego RP oraz podaje do publicznej wiadomości informację w tym zakresie, ostrzegając obywateli. Określenie poziomu zagrożenia terrorystycznego ma charakter informacyjny. Wyróżnia się cztery poziomy zagrożeń:

1) poziom niski, któremu nadaje się kolor zielony, oznacza brak informacji bezpośrednio wskazujących na zagrożenie o charakterze terrorystycznym,
2) poziom umiarkowany, któremu nadaje się kolor żółty, oznacza, że zdarzenie o charakterze terrorystycznym jest mało prawdopodobne, ale że pojawiły się informacje wskazujące na możliwość jego wystąpienia,
3) poziom wysoki, któremu nadaje się kolor pomarańczowy, oznacza, że zdarzenie o charakterze terrorystycznym jest prawdopodobne oraz że informacje o możliwości jego wystąpienia zostały potwierdzone,
4) poziom bardzo wysoki, któremu nadaje się kolor czerwony, oznacza, że zdarzenie o charakterze terrorystycznym wystąpiło lub że uzyskano informacje wskazujące na końcową fazę jego przygotowania.

W przypadku określenia poziomu zagrożenia terrorystycznego jako umiarkowanego, wysokiego lub bardzo wysokiego szef ABW informuje o tym organy uprawnione do wprowadzania stopnia alarmowego lub stopnia alarmowego CRP[16]. Określenie poziomu zagrożenia terrorystycznego jako jednego z wyżej wymienionych może stanowić

[13] Szerzej http://www.sejm.gov.pl/Druki8ka.nsf/0/9CCA65458151278AC1257FB50049D701/$File/516.pdf [dostęp: 11 VI 2016].

[14] http://rcb.gov.pl/wp-content/uploads/Zarzadzenie-nr-18.pdf [dostęp: 11 VI 2016].

[15] http://rcb.gov.pl/wp-content/uploads/Zalacznik-nr-1.pdf [dostęp: 11 VI 2016]. Załącznik nr 1 do *Zarządzenia Nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego* został częściowo zastąpiony przez *Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP* (Dz.U. z 2016 r. poz. 1101).

[16] Stopnie alarmowe są wprowadzane w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym albo w przypadku wystąpienia takiego zdarzenia. Stopnie alarmowe CRP są wprowadzane w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia.

przesłankę zalecenia przez szefa Agencji odnośnie do wprowadzenia przez uprawniony organ stopnia alarmowego lub stopnia alarmowego CRP.

Według ustawy o działaniach antyterrorystycznych w zależności od rodzaju zdarzenia o charakterze terrorystycznym stopnie alarmowe lub stopnie alarmowe CRP wprowadza, zmienia i odwołuje Prezes Rady Ministrów, po zasięgnięciu opinii ministra właściwego do spraw wewnętrznych i szefa ABW, a w przypadkach niecierpiących zwłoki – minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii szefa ABW, informując jednocześnie premiera.

W przypadku wprowadzenia stopnia alarmowego lub stopnia alarmowego CRP szef ABW powołuje sztab koordynacyjny, w którego skład wchodzą przedstawiciele służb specjalnych, Policji, SG, BOR, PSP, SC, GIIF, GIKS, ŻW i RCB, a także zaproszeni przedstawiciele Prokuratora Generalnego i innych organów administracji publicznej. Zadaniem sztabu koordynacyjnego jest rekomendowanie zmiany lub odwołania stopnia alarmowego oraz określenie form i zakresu współdziałania służb i organów wchodzących w skład sztabu lub biorących udział w jego pracach.

Rola szefa ABW wynikająca z ustawy o działaniach antyterrorystycznych oraz z zarządzenia nr 18 w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego nie została jeszcze zaktualizowana w Krajowym Planie Zarządzania Kryzysowego opracowanym w 2015 r.

Zadania z zakresu zapobiegania zagrożeniom terrorystycznym zostały w KPZK podzielone na działania samego szefa ABW oraz na czynności podejmowane przez podległą mu Agencję. Do zadań i obowiązków szefa ABW jako najważniejszego podmiotu w **fazie zapobiegania** zagrożeniom o charakterze terrorystycznym należą szczególnie[17]:

- koordynowanie czynności operacyjno-rozpoznawczych podejmowanych przez służby specjalne, które mogą mieć wpływ na bezpieczeństwo państwa,
- występowanie z wnioskiem do sądu okręgowego o zarządzenie kontroli operacyjnej przy wykonywaniu czynności operacyjno-rozpoznawczych podejmowanych przez ABW w celu rozpoznania i wykrycia przestępstw mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, w tym terroryzmu, oraz zapobiegania im,
- uzyskiwanie od organów administracji publicznej, posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej wszelkich informacji dotyczących zagrożeń o charakterze terrorystycznym, istotnych dla tej infrastruktury z punktu widzenia bezpieczeństwa państwa,
- współdziałanie z RCB w zakresie zapobiegania zdarzeniom o charakterze terrorystycznym,
- niezwłoczne przekazywanie Prezydentowi Rzeczpospolitej Polskiej i Prezesowi Rady Ministrów informacji, które mogą mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP,
- koordynacja przygotowania i aktualizacji *Raportu o zagrożeniach bezpieczeństwa narodowego* w części dotyczącej zagrożeń o charakterze terrorystycznym, które mogą doprowadzić do sytuacji kryzysowej,

[17] Podstawa prawna: ustawa o ABW oraz AW, ustawa o zarządzaniu kryzysowym, *Decyzja Rady 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, w szczególności w zwalczaniu terroryzmu i przestępczości transgranicznej* (Dz.Urz. UE L 210 z 6 VIII 2008 r. poz. 1), *Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 31 lipca 2012 r. w sprawie Krajowego Programu Ochrony Lotnictwa* (Dz.U. z 2012 r. poz. 912).

- możliwość udzielania przez szefa ABW zaleceń organom i podmiotom zagrożonym skutkami zdarzeń o charakterze terrorystycznym oraz przekazywania im niezbędnych informacji służących przeciwdziałaniu zagrożeniom.

Do zadań Agencji Bezpieczeństwa Wewnętrznego w fazie zapobiegania zagrożeniom o charakterze terrorystycznym należy:

- rozpoznawanie i wykrywanie przestępstw mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, a także zapobieganie im (wykonywanie czynności analityczno-informacyjnych, operacyjno-rozpoznawczych i dochodzeniowo-śledczych), w tym:
  - rozpoznawanie terroryzmu,
  - rozpoznawanie nielegalnego wytwarzania i posiadania broni, amunicji i materiałów wybuchowych oraz broni masowej zagłady w obrocie międzynarodowym, a także obrotu nimi,
  - rozpoznawanie przestępstw związanych z proliferacją broni masowego rażenia oraz środków jej przenoszenia do tzw. krajów ryzyka,
  - monitorowanie importu towarów i technologii podwójnego zastosowania;
- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego;
- prowadzenie współpracy z organami administracji publicznej oraz innymi podmiotami odpowiedzialnymi za ochronę bezpieczeństwa wewnętrznego państwa;
- prowadzenie współpracy międzynarodowej;
- informowanie społeczeństwa o aktualnych zagrożeniach terrorystycznych;
- podnoszenie świadomości społecznej w zakresie sposobu zachowania się w sytuacji zagrożenia terrorystycznego;
- realizowanie zadań krajowego punktu kontaktowego (Centrum Antyterrorystyczne ABW) odpowiadającego za wymianę danych dotyczących osób podejrzewanych o popełnienie przestępstw o charakterze terrorystycznym z punktami kontaktowymi innych państw członkowskich;
- dokonywanie corocznej oceny stopnia zagrożenia terrorystycznego w lotnictwie cywilnym na terytorium RP,
- dokonywanie oceny stopnia zagrożenia terrorystycznego dla danego lotniska w przypadku zwrócenia się przez ten podmiot do prezesa Urzędu Lotnictwa Cywilnego (ULC) o wprowadzenie alternatywnych środków ochrony,
- przekazywanie prezesowi ULC informacji o zagrożeniu aktami bezprawnej ingerencji w lotnictwie cywilnym oraz o wszelkich zagrożeniach, co do których istnieją przesłanki, że mogą one skutkować aktami bezprawnej ingerencji w lotnictwie cywilnym,
- obserwowanie pasażerów przylatujących i odlatujących statkami powietrznymi w celu wykrycia osób mogących stanowić zagrożenie bezpieczeństwa transportu lotniczego,
- współdziałanie z prezesem ULC, podmiotami zarządzającymi lotniskami oraz przewoźnikami lotniczymi w zakresie wprowadzenia do stosowania dodatkowych wymogów ochrony lotnictwa,
- uczestniczenie przedstawicieli Agencji Bezpieczeństwa Wewnętrznego w Zespołach Ochrony Lotniska działających w portach lotniczych.

W **fazie przygotowania** najważniejszą rolę odgrywa minister spraw wewnętrznych. Szef ABW staje się podmiotem wspomagającym, w którego zakresie obowiązków pozostaje[18]:

- uzyskiwanie, gromadzenie, analiza oraz weryfikacja informacji o potencjalnych zagrożeniach terrorystycznych,
- koordynowanie działań analityczno-informacyjnych służb i instytucji odpowiedzialnych za bezpieczeństwo państwa i porządek publiczny,
- planowanie działań mających na celu przeciwdziałanie aktom bezprawnej ingerencji w lotnictwie cywilnym,
- szkolenie podległych funkcjonariuszy w zakresie ochrony lotnictwa cywilnego przed aktami bezprawnej ingerencji w lotnictwie cywilnym,
- branie udziału przez przedstawicieli Agencji Bezpieczeństwa Wewnętrznego w Zespołach Ochrony Lotniska działających w portach lotniczych.

Do zadań Agencji Bezpieczeństwa Wewnętrznego natomiast należy:

- opracowywanie procedur reagowania w przypadku uzyskania informacji o zagrożeniu terrorystycznym,
- przeprowadzanie ćwiczeń antyterrorystycznych,
- wypracowanie systemów i metod rozpoznawania oraz monitorowania potencjalnych zagrożeń terrorystycznych,
- podejmowanie wspólnych inicjatyw, zwiększających skuteczność wykrywania zagrożeń terrorystycznych.

W **fazie reagowania** najważniejszą rolę odgrywa minister spraw wewnętrznych i administracji, szef ABW zaś jest podmiotem wspomagającym, do którego zadań należy[19]:

- w przypadku uzyskania informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku – udzielanie zaleceń organom i podmiotom zagrożonym tymi działaniami oraz przekazywanie im niezbędnych informacji służących przeciwdziałaniu zagrożeniom, a szczególnie:
  - wykonywanie czynności analityczno-informacyjnych,
  - wspomaganie działania służb i instytucji uczestniczących w ochronie antyterrorystycznej w zakresie analityczno-informacyjnym,
  - wspomaganie procesów decyzyjnych,
- informowanie dyrektora RCB o podjętych działaniach[20],
- ściganie sprawców przestępstw godzących w bezpieczeństwo państwa oraz jego porządek konstytucyjny, w tym terroryzmu, nielegalnego wytwarzania i posiadania broni, amunicji i materiałów wybuchowych, broni masowej zagłady w obrocie międzynarodowym oraz obrotu nimi,
- branie udziału w prowadzeniu negocjacji w przypadku wzięcia zakładników,
- przekazywanie informacji, na których podstawie Prezes Rady Ministrów, mini-

[18] Podstawa prawna: ustawa o ABW oraz AW, rozporządzenie MTBiGM w sprawie Krajowego Programu Ochrony Lotnictwa.

[19] Podstawa prawna: ustawa o zarządzaniu kryzysowym, *Ustawa z dnia 16 lipca 2004 r. prawo telekomunikacyjne* (tekst jednolity: Dz.U. z 2014 r. poz. 243, ze zm.), rozporządzenie MTBiGM w sprawie Krajowego Programu Ochrony Lotnictwa.

[20] Ustawa o działaniach antyterrorystycznych w art. 4 ust. 4 zobowiązuje szefa ABW do niezwłocznego poinformowania ministra koordynatora służb specjalnych. o poleceniach wydanych organom i podmiotom.

strowie i kierownicy urzędów centralnych oraz wojewodowie mogą wprowadzić, zmienić i odwołać stopień alarmowy[21],
- prowadzenie współpracy międzynarodowej,
- występowanie do prezesa Urzędu Komunikacji Elektronicznej z wnioskiem o wprowadzenie ograniczeń.

Krajowy Plan Zarządzania Kryzysowego przewiduje w **fazie odbudowy**, po zdarzeniu kryzysowym wynikającym z zagrożenia terrorystycznego, rolę nadrzędną dla ministra spraw wewnętrznych oraz zadania dla podmiotu wspomagającego podległego szefowi ABW, tj. Centrum Antyterrorystycznego ABW. Do tych zadań należy[22]:
- nowelizowanie procedur reagowania,
- podejmowanie wspólnych inicjatyw zwiększających skuteczność wykrywania zagrożeń terrorystycznych.

Zagrożenia cyberprzestrzeni

Ataki na cyberprzestrzeń są jednymi z najbardziej skutecznych i jednocześnie uciążliwych działań uderzających we współczesne społeczeństwa. Ustawa o ABW oraz AW jednoznacznie wskazuje ABW jako służbę właściwą w zakresie rozpoznawania i wykrywania zagrożeń godzących w bezpieczeństwo systemów teleinformatycznych organów administracji publicznej lub systemów sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej istotnych z punktu widzenia ciągłości funkcjonowania państwa[23]. W celu przeciwdziałania zagrożeniom cyberprzestrzeni ABW może:
- dokonywać oceny bezpieczeństwa systemów teleinformatycznych polegającej na przeprowadzaniu testów bezpieczeństwa. Badania mają zidentyfikować podatność i słabość zasobu lub zabezpieczenia, które mogą zostać wykorzystane przez zagrożenie wpływające na integralność, poufność, rozliczalność i dostępność do tego systemu. W tym celu ABW może wytwarzać lub pozyskiwać urządzenia lub programy komputerowe przystosowane do popełniania przestępstw (hakerskie) oraz używać ich, dążąc do określenia podatności ocenianego systemu na możliwość popełniania przestępstw. Uzyskiwanie dostępu do informacji będzie następowało przez przełamywanie lub omijanie elektronicznych, magnetycznych, informatycznych bądź innych zabezpieczeń, lub przez uzyskiwanie dostępu do całości lub części systemu teleinformatycznego,
- w przypadku uzyskania informacji o wystąpieniu zagrożenia o charakterze terrorystycznym dotyczącego systemów lub danych teleinformatycznych szef ABW może żądać od właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej informacji o budowie, działaniu oraz zasadach eksploatacji posiadanych systemów teleinformatycznych (w tym: haseł komputerowych, kodów dostępu i innych danych umożliwiających dostęp do systemu oraz ich używania) w celu zapobiegania zdarzeniom o charakterze terrorystycznym, dotyczącym systemów lub danych i reagowania na nie, a także ich wykrywania i ścigania ich sprawców,

[21] Ustawa o działaniach antyterrorystycznych w art. 16 ust. 1 umożliwia szefowi ABW wyrażanie opinii na temat wprowadzenia, zmiany i odwołania stopni alarmowych lub stopni alarmowych CRP przez Prezesa Rady Ministrów.

[22] Podstawa prawna: ustawa o ABW oraz AW.

[23] Art.5 ust. 1 pkt 2a ustawy o ABW oraz AW.

- szef ABW w celu zapobiegania przestępstwom o charakterze terrorystycznym, przeciwdziałania im, wykrywania ich oraz ścigania ich sprawców może złożyć wniosek do Sądu Okręgowego w Warszawie, po uzyskaniu zgody Prokuratora Generalnego, o zarządzenie zablokowania przez usługodawcę świadczącego usługi drogą elektroniczną, dostępności w systemie teleinformatycznym danych, które mają związek ze zdarzeniem o charakterze terrorystycznym lub usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym,
- szef ABW przeprowadza analizę zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych i wydaje podmiotom rekomendacje zmierzające do zapewnienia ich integralności, poufności, rozliczalności i dostępności.

Szef ABW prowadzi centralny rejestr zdarzeń o charakterze terrorystycznym naruszających bezpieczeństwo systemów teleinformatycznych o szczególnym znaczeniu dla bezpieczeństwa państwa, sieci teleinformatycznych albo systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej. Jednocześnie administratorzy tych systemów są obowiązani do przekazywania szefowi ABW danych dotyczących zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych.

Agencja Bezpieczeństwa Wewnętrznego została wskazana przez KPZK jako najważniejszy podmiot we wszystkich czterech fazach zarządzania kryzysowego związanego z zagrożeniem cyberprzestrzeni. W **fazie zapobiegania** zadania podejmowane pod nadzorem szefa ABW zostały podzielone między: ABW, Rządowy Zespół Reagowania na Incydenty Komputerowe działający w ramach ABW oraz Departament Bezpieczeństwa Teleinformatycznego ABW[24]. Do zadań ABW w tej fazie należy:

- rozpoznawanie i wykrywanie bezprawnego ujawnienia lub wykorzystania informacji niejawnych oraz zapobieganie tym przestępstwom,
- realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych,
- udzielanie akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej, zgodnie z właściwością określoną w art. 10 ust 3 *Ustawy z dnia 5 sierpnia o ochronie informacji niejawnych*[25],
- dokonywanie oceny bezpieczeństwa systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych,
- przeprowadzanie certyfikacji urządzeń lub narzędzi służących do realizacji zabezpieczenia teleinformatycznego w celu ochrony informacji niejawnych,
- zwiększanie świadomości pracowników administracji publicznej w zakresie zagrożeń cyberprzestrzeni oraz cykliczne podnoszenie ich wiedzy na temat metod przeciwdziałania zagrożeniom w tej sferze,
- sprawowanie funkcji Krajowego Punktu Centralnego (Focal Point) w ramach polityki ochrony cyberprzestrzeni NATO.

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL odpo-

[24] Podstawa prawna: *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r. Nr 182 poz. 1228, ze zm.), ustawa o ABW oraz AW oraz *Polityka Ochrony Cyberprzestrzeni RP* [online], http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html [dostęp: 15 XII 2015].

[25] Dz.U. z 2010 r. Nr 182 poz. 1228, ze zm.

wiada za koordynowanie procesu reagowania na incydenty komputerowe w obszarze administracji rządowej. Zadaniami CERT.GOV.PL w zakresie zarządzania kryzysowego w fazie zapobiegania są:

- rozwijanie zdolności jednostek organizacyjnych administracji rządowej Rzeczpospolitej Polskiej do ochrony przed cyberzagrożeniami,
- realizowanie zadań z zakresu II Poziomu Krajowego Systemu Reagowania na Incydenty Komputerowe w cyberprzestrzeni RP, o którym mowa w pkt. 4.2 *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[26], oraz jednocześnie głównego zespołu odpowiadającego za koordynowanie obsługi incydentów komputerowych w administracji rządowej,
- tworzenie wykazów zawierających specyfikację zagrożeń oraz możliwych podatności godzących w bezpieczeństwo cyberprzestrzeni,
- opracowywanie zaleceń oraz dobrych praktyk z zakresu bezpieczeństwa cyberprzestrzeni dla administracji rządowej,
- uruchomienie portalu do wymiany informacji o incydentach komputerowych pomiędzy zespołami reagowania na incydenty komputerowe powołanymi w administracji rządowej,
- współpraca z krajowymi instytucjami, organizacjami oraz podmiotami resortowymi w zakresie ochrony cyberprzestrzeni,
- reprezentowanie RP w kontaktach międzynarodowych,
- gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń krytycznej infrastruktury teleinformatycznej,
- przygotowywanie zaleceń dotyczących podniesienia poziomu ochrony systemów i sieci teleinformatycznych wykorzystywanych w administracji rządowej,
- przygotowywanie okresowych raportów dotyczących bezpieczeństwa teleinformatycznego państwa,
- analizowanie stron internetowych administracji państwowej we współpracy z organami państwowymi w zakresie weryfikacji wypełniania określonych zaleceń związanych z zapewnianiem dostępności, integralności oraz poufności witryn w domenie gov.pl.,
- prowadzenie szkoleń z zakresu bezpieczeństwa teleinformatycznego dla administratorów systemów podłączonych do sieci Internet w administracji rządowej oraz prowadzenie forum wymiany doświadczeń ze specjalistami ds. bezpieczeństwa teleinformatycznego (TI), pomocnikami ds. ochrony cyberprzestrzeni i administratorami systemów TI.

Zadaniem Departamentu Bezpieczeństwa Teleinformatycznego ABW w fazie zapobiegania zagrożeniom w cyberprzestrzeni jest akredytacja systemów do przetwarzania informacji niejawnych oraz prowadzenie badań i oceny bezpieczeństwa w ramach procesu certyfikacji dla środków ochrony elektromagnetycznej, kryptograficznej i narzędzi służących do realizacji zabezpieczeń teleinformatycznych.

[26] Szerzej: *Polityka Ochrony Cyberprzestrzeni RP*.
Rząd RP ustanawia trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w CRP:
(…) *2) Poziom II - reagowania na incydenty komputerowe:*
a) Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL - realizujący jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP,
b) Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizujące zadania w sferze militarnej.

W **fazie przygotowania** zadaniem szefa ABW jest wydawanie zaleceń dotyczących bezpieczeństwa teleinformatycznego. Rządowy Zespół Reagowania na Incydenty Komputerowe jest obowiązany do prowadzenia szkoleń z bezpieczeństwa teleinformatycznego dla administratorów systemów podłączonych do sieci Internet w administracji rządowej oraz prowadzenia forum wymiany doświadczeń ze specjalistami ds. bezpieczeństwa teleinformatycznego, pełnomocnikami ds. ochrony cyberprzestrzeni i administratorami systemów TI. Ponadto CERT.GOV.PL jest obowiązany do podnoszenia świadomości na temat zagrożeń komputerowych i przeprowadzania testów bezpieczeństwa. Natomiast rozbudowa systemu wczesnego ostrzegania przed zagrożeniami z sieci oraz wdrażanie i utrzymywanie rozwiązań prewencyjnych należą do zadań Departamentu Bezpieczeństwa Teleinformatycznego ABW[27].

W **fazie reagowania** KPZK przewiduje realizację zadań należących do podmiotu najważniejszego, którym jest szef ABW, za pośrednictwem Rządowego Zespołu Reagowania na Incydenty Komputerowe, działającego w strukturach ABW. Zadaniami CERT.GOV.PL jest[28]:

- realizowanie zadań głównego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w administracji rządowej,
- wykrywanie cyberzagrożeń, rozpoznawanie ich oraz przeciwdziałanie im,
- przekazywanie informacji administratorom w przypadku wykrycia błędów w zabezpieczeniach systemów TI,
- obsługiwanie zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV,
- publikowanie alertów i ostrzeżeń,
- przekazywanie informacji administratorom w przypadku wykrycia błędów w zabezpieczeniach systemów TI,
- prowadzenie analiz powłamaniowych,
- opracowywanie zaleceń mających na celu podniesienie bezpieczeństwa systemów teleinformatycznych w administracji rządowej.

W **fazie odbudowy** szef ABW, za pośrednictwem Rządowego Zespołu Reagowania na Incydenty Komputerowe, jest zobowiązany do prowadzenia analiz powłamaniowych[29].

Zagrożenia systemów telekomunikacyjnych

Na szefie ABW ciążą również zadania i obowiązki dotyczące zdarzeń kryzysowych powstających w wyniku zagrożeń systemów telekomunikacyjnych. Szef Agencji jest podmiotem wspomagającym w fazie przygotowania i jego działalność ogranicza się do uzgadniania – we właściwym sobie zakresie planów ogólnych – przedsięwzięć w sytuacjach szczególnych zagrożeń, opracowywanych przez przedsiębiorców telekomunikacyjnych[30].

W ramach obowiązku zapewnienia sprawności telekomunikacji, zwłaszcza z numerami alarmowymi, w związku z wydarzeniami, podczas których może wystąpić zdarzenie o charakterze terrorystycznym albo zagrożenie bezpieczeństwa i porządku publicznego, operator telekomunikacyjny jest obowiązany do zakładania tymczasowych

[27] Podstawa prawna: ustawa o ochronie informacji niejawnych oraz *Polityka Ochrony Cyberprzestrzeni RP*.

[28] Podstawa prawna: *Polityka Ochrony Cyberprzestrzeni RP*.

[29] Podstawa prawna: *Polityka Ochrony Cyberprzestrzeni RP*.

[30] Podstawa prawna: *Rozporządzenie Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń* (Dz.U. z 2010 r. Nr 15 poz. 77).

instalacji radiokomunikacyjnych wraz z antenami, szczególnie stacji bazowych ruchomej sieci telekomunikacyjnej. Z żądaniem do operatora może wystąpić minister właściwy do spraw informatyzacji lub organ odpowiedzialny za bezpieczeństwo i porządek publiczny.

Monitorowanie zagrożeń

Oprócz zadań i obowiązków uczestników zarządzania kryzysowego w Krajowym Planie Zarządzania Kryzysowego zawarto również zadania obejmujące monitorowanie zagrożeń, realizowane przez ministrów, kierowników urzędów centralnych i wojewodów. Obszar odpowiedzialności ustawowej szefa ABW w tym zakresie wynika z art. 5 ustawy o ABW oraz AW i obejmuje:

- rozpoznawanie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a szczególnie w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także w obronność państwa i zapobieganie im,
- rozpoznawanie i wykrywanie przestępstw:
  - szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa,
  - godzących w podstawy ekonomiczne państwa,
  - korupcji osób pełniących funkcje publiczne,
  - produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,
  - nielegalnego wytwarzania i posiadania broni, amunicji i materiałów wybuchowych, broni masowej zagłady oraz środków odurzających i substancji psychotropowych, a także obrotu nimi – w obrocie międzynarodowym –

  oraz zapobieganie im i ściganie ich sprawców,
- rozpoznawanie i wykrywanie zagrożeń godzących w bezpieczeństwo systemów teleinformatycznych organów administracji publicznej oraz systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 i 4 ustawy o zarządzaniu kryzysowym, istotnych z punktu widzenia ciągłości funkcjonowania państwa,
- realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych,
- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji, które mogą mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego,
- podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

W ramach powyższego obszaru odpowiedzialności na szefie ABW ciąży monitorowanie zagrożeń: terrorystycznych oraz występujących w sieciach teleinformatycznych organów administracji publicznej, a także udzielanie zaleceń organom i podmiotom zagrożonym skutkami zdarzeń o charakterze terrorystycznym oraz przekazywanie im niezbędnych informacji służących przeciwdziałaniu zagrożeniom. Zadaniem głównym

w warunkach sytuacji kryzysowej jest natomiast koordynowanie działań właściwych organów w przypadku zagrożenia terrorystycznego oraz cyberataku.

Jak wspomniano wyżej, szef ABW sprawuje nadzór nad monitorowaniem zagrożeń teleinformatycznych i terrorystycznych. Podmiotami odpowiedzialnymi za przeciwdziałanie zagrożeniom teleinformatycznym są dyrektor Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL[31]. Monitoringowi podlegają: incydenty w systemach teleinformatycznych jednostek organizacyjnych administracji publicznej RP oraz incydenty w systemach teleinformatycznych (w tym w Internecie) wymienione w art. 5 ustawy o ABW oraz AW. W tym celu są wykorzystywane metody (bazy) w postaci systemu wykrywania incydentów w systemach teleinformatycznych organów administracji publicznej (ARAKIS-GOV) i reagowania na nie. Informacje są zbierane na bieżąco i wykorzystywane w raportach kwartalnych publikowanych na stronie internetowej ABW.

Podmiotami odpowiedzialnymi za monitorowanie zagrożeń terrorystycznych są: dyrektor Departamentu Zwalczania Terroryzmu i Zagrożeń Strategicznych (DZTiZS), dyrektor Departamentu Kontrwywiadu ABW (DK ABW) oraz dyrektor Centrum Antyterrorystycznego ABW (CAT ABW). Departament Zwalczania Terroryzmu i Zagrożeń Strategicznych ABW monitoruje zagrożenia o charakterze terrorystycznym, wykorzystując możliwość prowadzenia czynności operacyjno-rozpoznawczych, a także korzystając z Centralnej Ewidencji Zainteresowań Operacyjnych oraz jawnych i niejawnych baz danych. Informacje są zbierane na bieżąco przez jednostki organizacyjne ABW w ramach prowadzonej pracy operacyjnej i wykorzystywane przez podmioty i jednostki prowadzące czynności dochodzeniowo-śledcze.

Centrum Antyterrorystyczne ABW monitoruje incydenty i zagrożenia o charakterze terrorystycznym mające wpływ na bezpieczeństwo RP i jej obywateli (ponad 100 incydentów podzielonych na 15 grup). Wykorzystywane metody i bazy to: czynności analityczno-informacyjne, jawne i niejawne bazy danych, system IT-CAT oraz CATEL, monitoring ogólnodostępnych źródeł informacji oraz współpraca międzynarodowa i krajowa. Ze zbieranych na bieżąco (całodobowo) danych są sporządzane opracowania miesięczne, półroczne i roczne. Źródłami informacji są: jednostki organizacyjne ABW, krajowe służby i instytucje współpracujące w ramach CAT ABW, służby zagraniczne oraz podmioty międzynarodowe: Counter Terrorist Group – CTG (Grupa ds. Przeciwdziałania Terroryzmowi), Middle Europe Conference – MEC (Konferencja Europy Środkowej), Working Party on Terrorism – WPT (Grupa Robocza UE ds. Terroryzmu), The Joint Situation Center – SinCen (Wspólne Centrum Sytuacyjne UE), a także źródła otwarte[32]. Uzyskane informacje są wykorzystywane w: raportach sytuacyjnych dla kierownictwa państwa dotyczących aktualnych zagrożeń o charakterze terrorystycznym, raportach operacyjnych, prognozach poziomu zagrożenia terroryzmem dla RP (comiesięczne – dla Międzyresortowego Zespołu do spraw Zagrożeń Terrorystycznych), długookresowych prognozach poziomu zagrożenia dla RP (roczne), cyklicznych raportach z monitoringu islamskich mediów radykalnych, informacjach sygnalnych, tworzeniu informacji na portalu antyterroryzm.gov.pl oraz do przygotowywania zaleceń dla organów i podmiotów

[31] Szerzej zob. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku* [online], CERT.GOV.PL., Warszawa 2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-brzpi/738,Raport-o-stanie-bezpieczeństwa-cyberprzestreni-RP-w-2014 roku.html [dostęp: 15 XII 2015].

[32] http://rcb.gov.pl/wp-content/uploads/KPZK-2013-2015.tj_..pdf [dostęp: 15 XII 2015].

zagrożonych możliwością wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym.

Funkcjonowanie Agencji Bezpieczeństwa Wewnętrznego w sytuacji kryzysowej

Na podstawie art. 12 ust. 2b ustawy o zarządzaniu kryzysowym ministrowie i kierownicy urzędów centralnych na potrzeby realizacji zadań z zakresu zarządzania kryzysowego tworzą zespoły zarządzania kryzysowego, w których skład wchodzą osoby kierujące właściwymi komórkami organizacyjnymi urzędu obsługującego ministra lub kierownika, a także inne osoby przez nich wskazane.

Zarządzeniem szefa ABW został powołany stały Zespół Zarządzania Kryzysowego (ZZK ABW), jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koordynowania podejmowanych działań, wspomagający szefa ABW w realizacji zadań z zakresu zarządzania kryzysowego[33]. Przedsięwzięcia podejmowane przez ZZK ABW polegają m.in. na:

- dokonywaniu okresowej oceny zagrożeń na potrzeby *Raportu o zagrożeniach bezpieczeństwa narodowego*;
- opiniowaniu projektów planów zarządzania kryzysowego uwzględniających szczególnie:
  - analizę i ocenę możliwości wystąpienia zagrożeń, w tym dotyczących infrastruktury krytycznej,
  - szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczenia i likwidacji ich skutków,
  - organizację monitoringu zagrożeń i realizację zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa,
  - organizację wykonywania zadań z zakresu ochrony infrastruktury krytycznej;
- opiniowaniu wykazu obiektów, instalacji i urządzeń wchodzących w skład infrastruktury krytycznej w ramach właściwości szefa ABW;
- wypracowaniu wniosków i pozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.

Przy wykonywaniu zadań ZZK ABW współpracuje przede wszystkim z Rządowym Zespołem Zarządzania Kryzysowego oraz zespołami zarządzania kryzysowego ministrów kierujących działaniami administracji rządowej oraz kierowników urzędów centralnych.

Zgodnie z art. 13 ust. 1[34] ustawy o zarządzaniu kryzysowym oraz w myśl *Rozporządzenia Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania*[35] szef ABW został zobowiązany do utworzenia centrum zarządzania kryzysowego. Do zadań powołanego Centrum Zarządzania Kryzysowego ABW (CZK ABW) należy m.in.:

- pełnienie całodobowego dyżuru w celu zapewniania przepływu informacji na potrzeby zarządzania kryzysowego,

[33] *Zarządzenie Nr 16 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 7 marca 2011 r. w sprawie organizacji, składu oraz miejsca i trybu pracy Zespołu Zarządzania Kryzysowego w Agencji Bezpieczeństwa Wewnętrznego* (Dz.Urz. ABW z 2011 r. Nr 1 poz. 9).

[34] *Art. 13 ust. 1. Ministrowie i centralne organy administracji rządowej, do których zakresu działania należą sprawy związane z zapewnieniem bezpieczeństwa narodowego, w tym ochrony ludności lub gospodarczych podstaw bezpieczeństwa państwa, tworzą centra zarządzania kryzysowego.*

[35] Dz.U. z 2009 r. Nr 226 poz. 1810.

- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej,
- nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,
- współpraca z podmiotami realizującymi monitoring środowiska,
- współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne,
- dokumentowanie działań podejmowanych przez Centrum,
- pełnienie stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa,
- współdziałanie na wszystkich szczeblach administracji rządowej w zakresie informowania i przekazywania poleceń do wykonania w systemie całodobowym dla jednostek ochrony zdrowia w przypadkach awaryjnych, losowych oraz zaburzeń funkcjonowania systemu.

Centrum Zarządzania Kryzysowego ABW zostało umieszczone w kompleksie wyodrębnionych pomieszczeń, w tym pomieszczeń operatorsko-dyspozytorskich (Główne Stanowisko Kierowania Szefa ABW), do których dostęp mają wyłącznie osoby upoważnione. Wyposażenie pomieszczeń umożliwia gromadzenie, przetwarzanie i wymianę niezbędnych informacji w zakresie zarządzania kryzysowego, prowadzenia analiz i ocen sytuacji kryzysowej, a także przekazywanie decyzji właściwych organów zarządzania kryzysowego. Centrum zarządzania kryzysowego realizuje swoje zadania na podstawie standardów określonych w *Ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczpospolitej Polskiej* (art. 6 ust. 2 pkt 2)[36] i *Rozporządzeniu Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym*[37] dla głównego stanowiska kierowania, z zachowaniem wymogów bezpieczeństwa systemów i sieci teleinformatycznych[38]. Centrum Zarządzania Kryzysowego ABW zapewnia obsługę Zespołu Zarządzania Kryzysowego ABW, koordynuje wymianę informacji z jednostkami organizacyjnymi ABW, sporządza oceny i analizy sytuacji kryzysowej na potrzeby ZZK ABW oraz sporządza meldunki o gotowości do realizacji zadań.

[36] Tekst jednolity: Dz.U. z 2016 r. poz. 1534.

[37] Dz.U. z 2004 r. Nr 98 poz. 978. System kierowania bezpieczeństwem narodowym został opracowany w 2004 r., przed wejściem w życie ustawy o zarządzaniu kryzysowym, na podstawie art. 6 ust. 2 pkt 2 ustawy o powszechnym obowiązku obrony Rzeczpospolitej Polskiej. Jego celem jest zapewnienie ciągłości podejmowania decyzji i działań dla utrzymania bezpieczeństwa narodowego, w tym:

- monitorowanie źródeł, rodzajów, kierunków i skali zagrożeń;
- zapobieganie powstawaniu zagrożeń bezpieczeństwa narodowego na terytorium RP oraz poza jej granicami;
- zapobieganie skutkom zagrożeń, a także ich usuwanie;
- kierowanie obroną państwa.

Przygotowanie systemu kierowania bezpieczeństwem narodowym obejmuje planowanie, organizowanie i realizowanie przedsięwzięć zapewniających organom administracji wykonywanie zadań związanych z kierowaniem bezpieczeństwem w czasie pokoju w razie wewnętrznego lub zewnętrznego zagrożenia, w tym w razie wystąpienia działań terrorystycznych i innych szczególnych zdarzeń, a także w czasie wojny. W ramach przygotowywania systemu kierowania szef ABW:

- zapewnia ochronę kontrwywiadowczą oraz rozpoznanie radioelektronicznego rejonów i obiektów stanowisk kierowania: Prezydenta RP, Prezesa Rady Ministrów, ministrów, centralnych organów administracji rządowej oraz wojewodów:
- zapewnia bezpieczeństwo systemów i sieci teleinformatycznych niezbędnych do wytwarzania, przetwarzania, przechowywania i przekazywania informacji niejawnych.

[38] Patrz: ustawa o ochronie informacji niejawnych.

W ramach swoich obowiązków CZK ABW współpracuje z RCB i innymi organami administracji publicznej, szczególnie w zakresie: wzajemnego informowania się (m.in. o potencjalnych zagrożeniach i możliwościach wystąpienia sytuacji kryzysowej, stratach i środkach niezbędnych do odtworzenia zasobów i infrastruktury krytycznej oraz o pomocy krajowej i międzynarodowej), analizowania i oceny sytuacji kryzysowej oraz zrealizowanych i planowanych działań. Przekazuje też raporty sytuacyjne do RCB – raz dziennie lub zgodnie z zapotrzebowaniem.

Centrum Zrządzania Kryzysowego ABW po otrzymaniu z RCB informacji o rozpoczęciu procedury uruchamiania środków reagowania kryzysowego systemu NATO NCRS (NATO Crisis Response System)[39] przekazuje ją do dyrektora jednostki organizacyjnej ABW będącego wykonawcą lub współwykonawcą zadania. Po dokonaniu analizy przez właściwego dyrektora Centrum melduje do RCB o gotowości do realizacji zadania albo przekazuje propozycje i sugestie dotyczące ograniczeń w realizacji środka reagowania kryzysowego[40].

Na podstawie art. 12 ust. 2 ustawy o zarządzaniu kryzysowym szef ABW opracowuje Plan Zarządzania Kryzysowego w ABW, który po uzgodnieniu z dyrektorem RCB jest zatwierdzany przez szefa i stanowi załącznik funkcjonalny do Krajowego Planu Zarządzania Kryzysowego. Plan działania ABW w sytuacji kryzysowej uwzględnia przede wszystkim:

- analizę i ocenę możliwości wystąpienia zagrożeń, w tym infrastruktury krytycznej uwzględnionej w wykazie,
- szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczania i likwidacji ich skutków,
- organizację monitoringu zagrożeń i realizację zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa,
- organizację wykonywania zadań z zakresu ochrony infrastruktury krytycznej.

Obowiązek podjęcia działań dotyczących zarządzania kryzysowego spoczywa na tym organie właściwym w sprawach zarządzania kryzysowego, który pierwszy otrzymał informacje o wystąpieniu zagrożenia. Taki organ niezwłocznie informuje o zaistniałym zdarzeniu organy odpowiednio wyższego i niższego szczebla i przedstawia jednocześnie swoją ocenę sytuacji oraz informacje o zamierzonych działaniach[41].

W myśl art. 4 ust. 1 i 2 ustawy o działaniach antyterrorystycznych przy realizacji działań antyterrorystycznych zadania z zakresu przeciwdziałania i zapobiegania skutkom zdarzeń o charakterze terrorystycznym i usuwania ich są realizowane przez organy administracji publicznej, właścicieli i posiadaczy obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej we współpracy z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego, szczególnie z szefem ABW. W związku z tym w Agencji została opracowana procedura reagowania w przypadku uzyskania informacji o wystąpieniu zdarzenia o charakterze terrorystycznym[42].

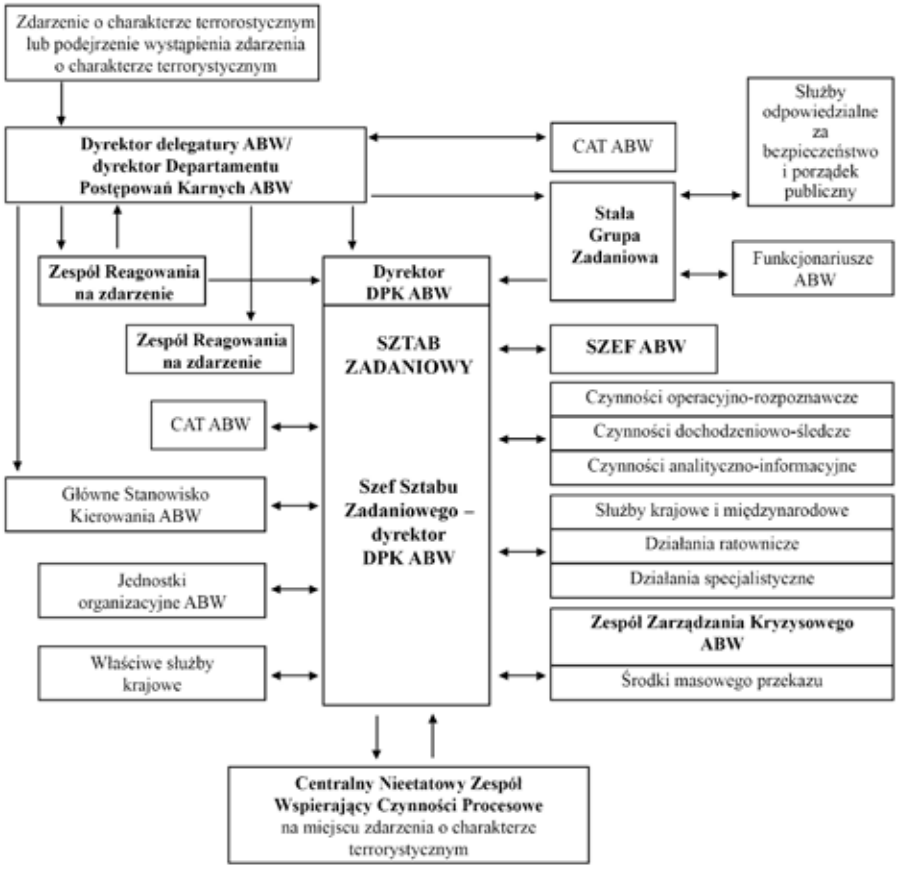
---

[39] Środki reagowania kryzysowego systemu NATO NCRS zostały określone w załączniku nr 2 do *Zarządzenia Nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego* (załącznik niepublikowany).

[40] Szerzej zob. *Zarządzenie Nr Z-20 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 9 kwietnia 2013 r. w sprawie realizacji przez Agencję Bezpieczeństwa Wewnętrznego zadań przewidzianych dla uruchomienia środków reagowania kryzysowego.*

[41] Art. 21 ustawy o zarządzaniu kryzysowym.

[42] *Decyzja Nr 164 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 15 grudnia 2015 r. w sprawie sposobu reagowania w Agencji Bezpieczeństwa Wewnętrznego w przypadku uzyskania informacji o wystąpieniu zdarzenia o charakterze terrorystycznym* (Dz.Urz. ABW z 31 XII 2015 r. poz. 32), www.abw.gov.pl/down-



Rys. 1. Sposób reagowania w ABW w przypadku uzyskania informacji o wystąpieniu zdarzenia o charakterze terrorystycznym.

Źródło: Opracowanie własne.

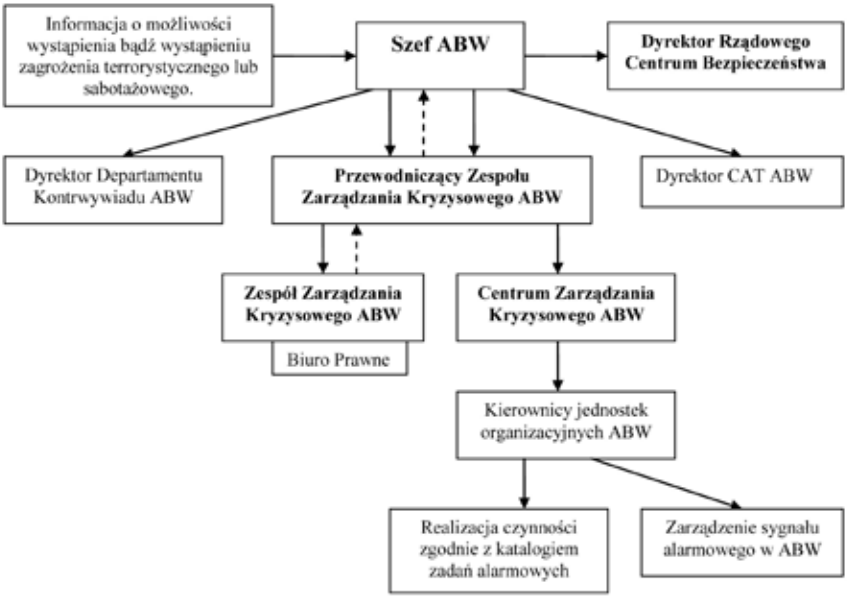
W przypadku uzyskania przez ABW informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym lub sabotażowym albo w przypadku wystąpienia zdarzenia o takim charakterze w ABW może zostać wprowadzony odpowiedni stopień alarmowania[43]. Szef ABW wprowadza, zmienia i odwołuje odpowiedni stopień alarmowania w przypadku wprowadzenia stopnia alarmowego przez Prezesa Rady Ministrów, a w przypadkach niecierpiących zwłoki – przez ministra właściwego do spraw wewnętrznych[44] na wniosek przewodniczącego Zespołu Zarządzania Kryzysowego ABW, w drodze zarządzenia. O wprowadzonym w ABW stopniu alarmowym szef ABW niezwłocznie informuje dyrektora Rządowego Centrum Bezpieczeństwa. W tym przypadku

load/8/2003/decyzja164z2015.pdf [dostęp: 10 I 2016].

[43] *Zarządzenie Nr 46 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 26 września 2012 r. w sprawie stopni alarmowych w Agencji Bezpieczeństwa Wewnętrznego* (D.Urz. ABW z 3 IX 2014 r. poz. 26), www.abw.gov.pl/download/8/1400/ZarzadzenieNr46z2012DOBRE.pdf [dostęp: 10 I 2016].

[44] Art. 16 ust. 1 ustawy o działaniach antyterrorystycznych.

ABW, niezależnie od zadań alarmowych, realizuje również czynności związane z zapewnieniem bezpieczeństwa i porządku konstytucyjnego, wynikające z zadań ustawowych.



Rys. 2. Wprowadzenie stopnia alarmowego w ABW.

Źródło: Opracowanie własne.

Zadania związane z wprowadzaniem stopni alarmowych są zadaniami porządkowo-ochronnymi podejmowanymi w celu przeciwdziałania lub minimalizacji skutków ataków terrorystycznych albo sabotażowych na obiekty ABW, wykonywanymi w miarę możliwości przy udziale innych służb, inspekcji i straży we współpracy z jednostką organizacyjną ABW odpowiedzialną za wykonanie tych zadań.

W przypadku możliwości wystąpienia lub wystąpienia zagrożeń o charakterze terrorystycznym albo sabotażowym dyrektor Departamentu Bezpieczeństwa Wewnętrznego i Audytu jako przewodniczący ZZK ABW, przy wsparciu dyrektora Centrum Antyterrorystycznego ABW, jest obowiązany do współdziałania i wymiany informacji z podmiotami właściwymi w sprawach zarządzania kryzysowego.

Tab. 2. Rodzaje stopni alarmowych oraz przesłanki ich wprowadzenia.

Stopień alarmowy	Przesłanki wprowadzenia
PIERWSZY STOPIEŃ ALARMOWY (CRP) STOPIEŃ ALFA (STOPIEŃ ALFA-CRP)	Można wprowadzić w przypadku: – uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego rodzaj i zakres są trudne do przewidzenia

DRUGI STOPIEŃ ALARMOWY (CRP) – STOPIEŃ BRAVO (STOPIEŃ BRAVO-CRP)	Można wprowadzić w przypadku: – zaistnienia zwiększonej i przewidywalnej możliwości wystąpienia zagrożenia o charakterze terrorystycznym, jednak gdy konkretny cel zdarzenia nie został zidentyfikowany
TRZECI STOPIEŃ ALARMOWY (CRP) – STOPIEŃ CHARLIE (STOPIEŃ CHARLIE--CRP)	Można wprowadzić w przypadku: – wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym, godzącego w: • bezpieczeństwo lub porządek publiczny, • bezpieczeństwo RP, • bezpieczeństwo innego państwa lub organizacji międzynarodowej oraz stwarzającego potencjalne zagrożenie dla RP; – uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym na terytorium RP; – uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym, którego skutki mogą dotyczyć obywateli RP lub instytucji polskich, lub polskiej infrastruktury – mieszczących się poza granicami RP
CZWARTY STOPIEŃ ALARMOWY (CRP) – STOPIEŃ DELTA (STOPIEŃ DELTA-CRP)	Można wprowadzić w przypadku: – wystąpienia zdarzenia o charakterze terrorystycznym, powodującego zagrożenie: • bezpieczeństwa lub porządku publicznego, • bezpieczeństwa RP, • bezpieczeństwa innego państwa lub organizacji międzynarodowej oraz stwarzającego zagrożenie RP; – uzyskania informacji wskazujących na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym na terytorium RP; – uzyskania informacji wskazujących na zaawansowaną fazę przygotowań do nieuchronnego zdarzenia o charakterze terrorystycznym, wymierzonego w obywateli RP lub w instytucje polskie, lub polską infrastrukturę mieszczącą się poza granicami RP

Źródło: Opracowanie własne na podstawie *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*.

Zadania funkcjonariuszy podległych szefowi ABW zostały określone w rozporządzeniu Prezesa Rady Ministrów w sprawie zakresu przedsięwzięć wykonywanych w czasie obowiązywania poszczególnych stopni alarmowych i stopni alarmowych CRP, w załączniku pod tytułem *Szczegółowy zakres przedsięwzięć wykonywanych w ramach kompetencji ustawowych przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego w poszczególnych stopniach alarmowych i stopniach alarmowych CRP*.

Udział szefa ABW w pracach Rządowego Zespołu Zarządzania Kryzysowego

Rządowy Zespół Zarządzania Kryzysowego (RZZK) został utworzony przy Radzie Ministrów jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koor-

dynowania działań podejmowanych w zakresie zarządzania kryzysowego. W jego skład wchodzą: Prezes Rady Ministrów, minister obrony narodowej, minister właściwy do spraw wewnętrznych, minister właściwy do spraw administracji publicznej, minister spraw zagranicznych oraz minister koordynator służb specjalnych[45]. W posiedzeniach RZZK bierze udział na prawach członka, w zależności od potrzeb, szef ABW. Do zadań Zespołu należy:

- przygotowywanie propozycji użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych,
- doradzanie w zakresie koordynowania działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych,
- opiniowanie sprawozdań końcowych z działań podejmowanych w związku z zarządzaniem kryzysowym,
- opiniowanie potrzeb w zakresie odtwarzania infrastruktury lub przywrócenia jej pierwotnego charakteru,
- opiniowanie i przedkładanie Radzie Ministrów Krajowego Planu Zarządzania Kryzysowego,
- opiniowanie projektu zarządzenia Prezesa Rady Ministrów w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego.

Szef ABW jest wyznaczany do udziału w posiedzeniach w przypadku, gdy przedmiotem obrad są zagrożenia o charakterze terrorystycznym lub zagrożenie cyberprzestrzeni.

Współpraca szefa ABW z Rządowym Centrum Bezpieczeństwa i administracją centralną

Rządowe Centrum Bezpieczeństwa zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, Rządowego Zespołu Zarządzania Kryzysowego i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełni funkcję krajowego centrum zarządzania kryzysowego. Zgodnie z art. 11 ustawy o zarządzaniu kryzysowym do zadań RCB należy m.in.: zapobieganie i przeciwdziałanie skutkom zdarzeń o charakterze terrorystycznym oraz ich usuwanie, a także współdziałanie z szefem ABW w tym zakresie.

W 2008 r. w ramach Agencji Bezpieczeństwa Wewnętrznego utworzono Centrum Antyterrorystyczne (CAT), które działa w systemie całodobowym przez siedem dni w tygodniu. Służbę w nim pełnią, oprócz funkcjonariuszy ABW, oddelegowani funkcjonariusze, żołnierze i pracownicy: Policji, SG, BOR, AW, SWW, SKW oraz SC. Ponadto z CAT ABW aktywnie współpracują inne służby i instytucje uczestniczące w systemie ochrony antyterrorystycznej RP, takie jak RCB, MSZ, PSP, GIIF, SG WP i ŻW. Przedstawiciele wszystkich wymienionych służb i instytucji realizują zadania w ramach swoich kompetencji[46].

Centrum Antyterrorystyczne ABW z założenia było pomyślane jako jeden z filarów informacyjnych RCB. Jego zadaniem jest wspieranie Centrum przez wspomaganie procesów decyzyjnych w przypadku realnego zagrożenia atakiem terrorystycznym, koordynowanie działań operacyjno-rozpoznawczych zmierzających do zweryfikowania informacji o potencjalnych zagrożeniach oraz prowadzenie szerokich działań analityczno-informacyjnych mających na celu poszerzanie wiedzy o zagrożeniach[47].

[45] http://rcb.gov.pl/?page_id=299 [dostęp: 15 XII 2015].

[46] A. Makarski, *Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 104.

[47] W. Skomra, *Zarządzanie kryzysowe – praktyczny komentarz po nowelizacji ustawy*, Warszawa 2010, s. 114.

Stała współpraca RCB z ABW wskazana w ustawie o zarządzaniu kryzysowym doprowadziła do podpisania w 2010 r. porozumienia pomiędzy dyrektorem Centrum a szefem Agencji[48]. Współdziałanie instytucji w sprawach zarządzania kryzysowego obejmuje m.in.:

- wymianę informacji, wzajemne udostępnianie materiałów, tworzenie wspólnych opracowań, uzgadnianie wspólnych stanowisk dotyczących:
  - koordynacji przygotowania *Raportu o zagrożeniach bezpieczeństwa narodowego*, w tym przekazanie przez szefa ABW dyrektorowi RCB ostatecznej jego wersji, w części dotyczącej zagrożeń o charakterze terrorystycznym, które mogą doprowadzić do sytuacji kryzysowej,
  - monitorowania potencjalnych zagrożeń, możliwości ich wystąpienia i rozwoju, w tym zagrożeń o charakterze terrorystycznym,
  - realizacji zadań w zakresie zapobiegania i przeciwdziałania zdarzeniom o charakterze terrorystycznym, reagowania na nie i usuwania ich skutków,
  - ochrony infrastruktury krytycznej,
  - opiniowania projektów dokumentów rządowych, w tym projektów aktów normatywnych i innych aktów prawnych,
  - opiniowania dokumentów innych niż wymienione w lit. e, związanych z realizacją ustawowych zadań stron porozumienia;
- współpracę dotyczącą ochrony informacji niejawnych;
- współpracę w organizowaniu, współorganizowaniu oraz opiniowaniu programów konferencji, szkoleń i narad poświęconych zarządzaniu kryzysowemu;
- wymianę doświadczeń dotyczących wykonywania ustawowych zadań każdej ze stron porozumienia.

Porozumienie usystematyzowało dziedziny współpracy instytucji oraz pozwoliło na ustalenie jej szczegółowego zakresu i sposobów. Umowa wskazuje, że ABW i RCB w przypadku zaistnienia zdarzeń o charakterze terrorystycznym chcą wspólnie tworzyć system zarządzania kryzysowego i ochrony infrastruktury krytycznej.

Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują, zgodnie z zakresem swojej właściwości, zadania dotyczące zarządzania kryzysowego. Opracowują również plany zarządzania kryzysowego, które stanowią załączniki funkcjonalne do Krajowego Planu Zarządzania Kryzysowego. Na potrzeby KPZK ministrowie, kierownicy urzędów centralnych oraz wojewodowie sporządzają tzw. raport cząstkowy do *Raportu o zagrożeniach bezpieczeństwa narodowego*. Koordynację przygotowania raportu cząstkowego w części dotyczącej zagrożeń o charakterze terrorystycznym, które mogą doprowadzić do sytuacji kryzysowej, zapewnia szef ABW. Kierunki działań wynikające z wniosków raportu cząstkowego stanowią element KPZK oraz są uwzględniane w planach zarządzania kryzysowego.

W przypadku wystąpienia zagrożeń o charakterze terrorystycznym mogących doprowadzić do sytuacji kryzysowej wykonawcy raportów cząstkowych przedkładają je dyrektorowi RCB oraz szefowi ABW. Szef ABW może w terminie jednego miesiąca wnieść zastrzeżenia i uwagi co do stopnia szczegółowości, zakresu i formy raportu cząstkowego lub jego części oraz wskazać na konieczność jego uzupełnienia o elementy wynikające z raportów cząstkowych sporządzonych przez innych wykonawców. Wy-

[48] *Porozumienie z dnia 19 sierpnia 2010 r. w sprawie ustalenia szczegółowego zakresu i sposobów współdziałania Rządowego Centrum Bezpieczeństwa i Agencji Bezpieczeństwa Wewnętrznego*, [online], http://mundurowi.info/index.php/abw/8-porozumienie-rcb-i-abw [dostęp: 15 XII 2015].

konawca jest zobowiązany rozpatrzeć zastrzeżenia i uwagi oraz, w razie konieczności, skorygować raport cząstkowy w terminie 30 dni, a następnie przesłać go ponownie do szefa ABW. W przypadku nieuwzględnienia uwag i zastrzeżeń wykonawca powiadamia o tym pisemnie szefa ABW i uzasadnia przyczynę odmowy. Wykonawca raportu cząstkowego dokonuje jego systematycznej aktualizacji, nie rzadziej niż raz na dwa lata oraz – w przypadku zagrożeń o charakterze terrorystycznym, które mogą doprowadzić do sytuacji kryzysowej – przedkłada go szefowi ABW. Możliwość wnoszenia uwag i zastrzeżeń oraz koordynacji prac wykonawców raportów cząstkowych przyznaje szefowi ABW główną rolę w opracowaniu *Raportu o zagrożeniach bezpieczeństwa narodowego* w części dotyczącej zagrożeń o charakterze terrorystycznym[49].

W ramach współpracy z administracją centralną ustawa o działaniach antyterrorystycznych nałożyła na szefa ABW obowiązek informowania ministra koordynatora służb specjalnych o poleceniach wydanych organom i podmiotom zagrożonym wystąpieniem sytuacji kryzysowej w postaci zdarzenia o charakterze terrorystycznym.

Współpraca szefa ABW z terenowymi organami zarządzania kryzysowego

System zarządzania kryzysowego w Polsce jest wieloszczeblowy i składa się z następujących elementów: organów zarządzania kryzysowego, organów opiniodawczo-doradczych właściwych w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego oraz centrów zarządzania kryzysowego utrzymujących 24-godzinną gotowość do podjęcia działań[50].

Rola szefa ABW w zakresie współpracy z terenowymi organami administracji rządowej i samorządowej właściwymi w sprawach zarządzania kryzysowego wynika z ustaw o zarządzaniu kryzysowym oraz o działaniach antyterrorystycznych. Do zadań wojewody (na terenie województwa), starosty (na terenie powiatu) oraz wójta, burmistrza i prezydenta miasta (na terenie gminy lub miasta), należy m.in.: zapobieganie i przeciwdziałanie skutkom zdarzeń o charakterze terrorystycznym[51] oraz ich usuwanie, a także współdziałanie z szefem ABW w tym zakresie[52]. Ustawowym zadaniem Agencji jest przede wszystkim niedopuszczanie do zaistnienia aktów terroryzmu, rolą terenowych organów zarządzania kryzysowego zaś – zajmowanie się skutkami zdarzeń o charakterze terrorystycznym.

Tab. 3. System zarządzania kryzysowego.

SYSTEM ZARZĄDZANIA KRYZYSOWEGO			
Szczebel administracyjny	**Organ zarządzania kryzysowego**	**Organ opiniodawczo-doradczy**	**Centrum Zarządzania Kryzysowego**
Krajowy	Rada Ministrów, Prezes Rady Ministrów	Rządowy Zespół Zarządzania Kryzysowego	Rządowe Centrum Bezpieczeństwa

[49] Według A. Podolskiego szef ABW wykonuje zadania podwykonawcze w stosunku do nadrzędnego zadania ciążącego na dyrektorze RCB. Szerzej zob. A. Podolski, *Miejsce Rządowego Centrum Bezpieczeństwa w systemie bezpieczeństwa antyterrorystycznego Rzeczpospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 104.

[50] http://rcb.gov.pl/?page_id=489 [dostęp: 15 V 2014].

[51] Art. 14 ust. 2 pkt 6, art. 17 ust. 2 pkt 5, art. 19 ust. 2 pkt 5 ustawy o zarządzaniu kryzysowym.

[52] Art. 14 ust. 2 pkt 6a, art. 17 ust. 2 pkt 5a, art. 19 ust. 2 pkt 5a ustawy o zarządzaniu kryzysowym.

Resortowy	minister kierujący działem administracji rządowej, kierownik organu centralnego	Zespół Zarządzania Kryzysowego (ministerstwa, urzędu centralnego)	Centrum Zarządzania Kryzysowego (ministerstwa, urzędu centralnego)
Wojewódzki	wojewoda	Wojewódzki Zespół Zarządzania Kryzysowego	Wojewódzkie Centrum Zarządzania Kryzysowego
Powiatowy	starosta powiatu	Powiatowy Zespół Zarządzania Kryzysowego	Powiatowe Centrum Zarządzania Kryzysowego
Gminny	wójt, burmistrz, prezydent miasta	Gminny Zespół Zarządzania Kryzysowego	mogą być tworzone (choć nie ma obowiązku utworzenia) gminne (miejskie) centra zarządzania kryzysowego

Źródło: Rządowe Centrum Bezpieczeństwa [online], http://rcb.gov.pl/?page_id=489 [dostęp: 15 V 2014].

Jednym z zadań organów administracji publicznej jest współpraca ze służbami właściwymi w sprawach bezpieczeństwa przy realizacji działań antyterrorystycznych. Współdziałanie z szefem ABW jest związane z przekazywaniem do Agencji informacji dotyczących zagrożeń o charakterze terrorystycznym wymierzonych w infrastrukturę administracji publicznej lub infrastrukturę krytyczną oraz uzyskiwaniem od ABW informacji, zaleceń, rekomendacji lub poleceń mających na celu przeciwdziałanie tego typu zagrożeniom. Następnie organy zarządzania kryzysowego informują szefa Agencji o podjętych działaniach.

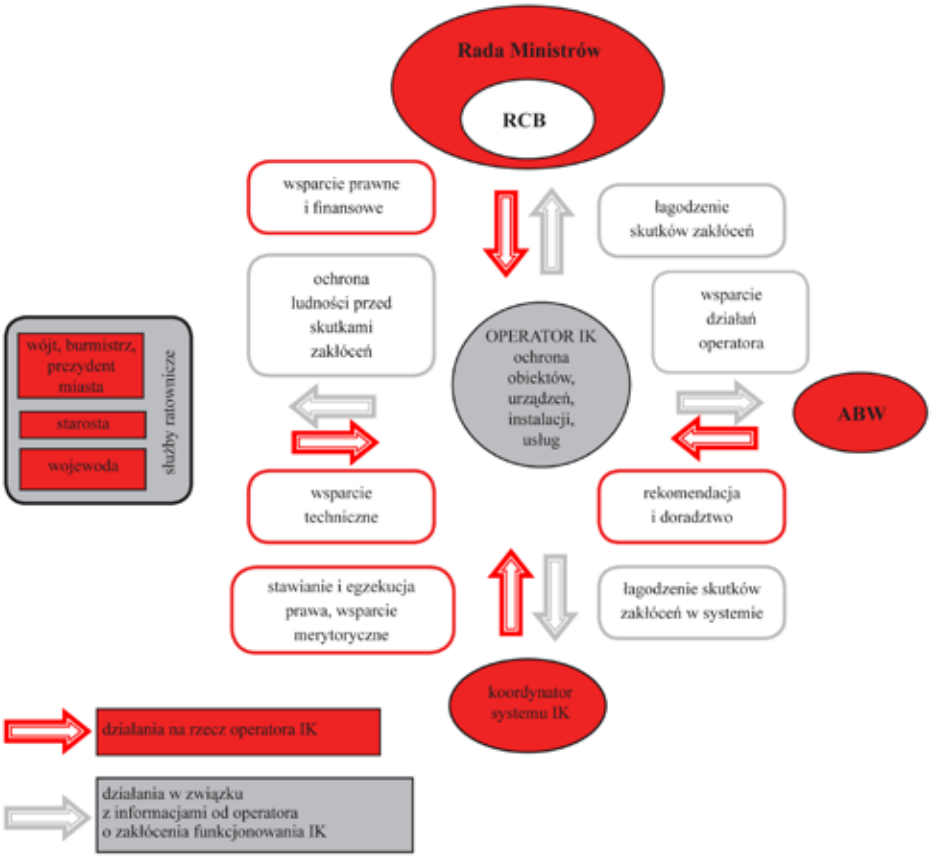
Prawidłowa współpraca szefa ABW z terenowymi organami administracji rządowej i samorządowej pozwala na wykorzystanie wiedzy i pomocy Agencji w celu właściwego zabezpieczenia infrastruktury krytycznej, osób i mienia oraz przećwiczenia wariantów zdarzeń kryzysowych i zapoznania się z dynamicznie zmieniającymi się sposobami, formami oraz metodami działania terrorystów. W fazie usuwania skutków zdarzeń o charakterze terrorystycznym oraz w odtwarzaniu zasobów wsparcie ABW pozwala na odpowiednio zhierarchizowane przywracanie stanu sprzed zdarzenia, z uwzględnieniem kolejnych działań, priorytetowych dla terrorystów[53].

Współpraca szefa ABW z posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej

Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, szczególnie przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bez-

[53] G. Pietrek, *Rola i zadania Agencji Bezpieczeństwa Wewnętrznego w systemie zarządzania kryzysowego,* w: *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, G. Sobolewski, D. Majchrzak (red.), Warszawa 2011, s. 176.

pieczeństwo i podtrzymujących działanie tej infrastruktury do czasu jej odtworzenia. Infrastruktura krytyczna to systemy oraz wchodzące w ich skład obiekty powiązane ze sobą funkcjonalnie, w tym obiekty budowlane, urządzenia, instalacje, usługi istotne dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię, surowce energetyczne i paliwa; łączności; sieci teleinformatycznych; finansowe; zaopatrzenia w żywność; zaopatrzenia w wodę; ochrony zdrowia; transportowe; ratownicze; zapewniające ciągłość działania administracji publicznej; produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.



Rys. 3. Główne podmioty uczestniczące w procesie ochrony IK i ich role.

Źródło: *Narodowy Program Ochrony Infrastruktury Krytycznej* [online], http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf, s. 26 [dostęp: 15 XII 2015].

Służby specjalne odgrywają szczególną rolę w ochronie infrastruktury krytycznej[54]. Dysponują rozwiniętymi siłami i środkami służącymi identyfikacji zagrożeń spowodowanych intencjonalną działalnością człowieka. Wymiana informacji o tych zagrożeniach z operatorami IK oraz innymi podmiotami właściwymi w sprawach ochrony tej infrastruktury w sposób i w zakresie określonym przepisami prawa i wewnętrznymi procedurami, jest bardzo ważna przy planowaniu jej ochrony[55].

Zadaniem posiadacza samoistnego i zależnego obiektów, instalacji lub urządzeń infrastruktury krytycznej jest niezwłoczne przekazanie szefowi ABW informacji wskazujących na zagrożenia o charakterze terrorystycznym wymierzone w infrastrukturę krytyczną. Dotyczy to niebezpieczeństw zagrażających funkcjonowaniu systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych, istotnych z punktu widzenia bezpieczeństwa państwa. Obowiązek przekazania informacji o wystąpieniu takich zagrożeń wiąże się z koniecznością prowadzenia przez posiadacza infrastruktury krytycznej stałej obserwacji zdarzeń i zjawisk, które mogą prowadzić do powstania zagrożenia życia lub zdrowia ludzi, mienia w znacznych rozmiarach, dziedzictwa narodowego lub środowiska. Przekazane informacje z jednej strony umożliwiają realizację ustawowych zadań ABW, tj. rozpoznawanie i wykrywanie przestępstw terroryzmu oraz zapobieganie im, a z drugiej strony ABW uzyskuje wiedzę na temat ewentualnych zamierzeń terrorystycznych z dodatkowego źródła[56].

W przypadku uzyskania informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze krytycznej szef ABW może wydawać polecenia organom i podmiotom zagrożonym tymi działaniami oraz przekazywać im niezbędne dane służące przeciwdziałaniu niebezpieczeństwom. Polecenia wydane przez szefa ABW powinny być wiążące dla właściciela lub posiadacza obiektów, instalacji lub urządzeń infrastruktury krytycznej, gdyż stanowią istotną pomoc dla podmiotów gospodarczych pozwalającą lepiej przygotować plany ochrony oraz stworzyć siatkę łączności i sygnałów o zagrożeniach[57]. Organy i podmioty mają obowiązek poinformowania szefa Agencji o podjętych działaniach.

Kierownik jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, jest obowiązany uzgodnić plan ochrony tych obszarów, obiektów i urządzeń w zakresie zagrożeń o charakterze terrorystycznym z właściwym terytorialnie dyrektorem delegatury ABW[58].

---

[54] Ochrona infrastruktury krytycznej to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzyku lub słabym punktom oraz ograniczenia i neutralizacji ich skutków, a także szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

[55] http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf [dostęp: 15 XII 2015].

[56] J. Derlacki, W. Kaczorowski, D. Lizakowski, *Zarządzanie kryzysowe*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1, s. 52.

[57] Według W. Skomry szef ABW na podstawie art. 12a ustawy o zarządzaniu kryzysowym mógł udzielać podmiotom niewiążących zaleceń; ustawa o działaniach antyterrorystycznych uprawnia szefa Agencji do wydawania poleceń, które powinny być wiążące, jednak w ustawie o działaniach antyterrorystycznych nie ma informacji dotyczących sankcji i trybu ponoszenia odpowiedzialności przez podmiot, który nie zastosuje się do polecenia, zob. W. Skomra, *Zarządzanie kryzysowe…*, s. 118.

[58] Art. 7 ust. 1 *Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* (Dz.U. z 2014 r. poz. 1099, ze zm.) zmieniony przez art. 33 ustawy o działaniach antyterrorystycznych.

Zakończenie

System zarządzania kryzysowego i ochrony infrastruktury krytycznej jest istotnym elementem zapewniania bezpieczeństwa państwa, polegającym na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli, a następnie reagowaniu w przypadku ich wystąpienia i usuwaniu ich skutków. Udział szefa Agencji Bezpieczeństwa Wewnętrznego w tych czterech fazach zarządzania kryzysowego został ograniczony do działań w przypadku wystąpienia zagrożeń w cyberprzestrzeni, zagrożeń o charakterze terrorystycznym oraz zagrożeń telekomunikacyjnych mogących doprowadzić do sytuacji kryzysowej. Tak wąskie określenie roli i zadań osoby kierującej największą służbą specjalną w RP może prowokować do myślenia o niewykorzystaniu w pełni potencjału ABW. Kompetencje szefa ABW przedstawione i omówione w artykule wskazują jednak na wiele czynności wykonywanych przez Agencję. Zlecenie działań w zakresie zapobiegania terroryzmowi jednej nadrzędnej instytucji i dzielenie się przez szefa ABW wiedzą z innymi podmiotami, włącznie z przedsiębiorcami, jest rozwiązaniem słusznym. Agencja Bezpieczeństwa Wewnętrznego, tak jak dotychczas, ma być instytucją odpowiedzialną za zapewnianie bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, szczególnie przez rozpoznawanie i wykrywanie przestępstw terroryzmu, zapobieganie im oraz ściganie ich sprawców.

Obecnie obowiązujący system prawny w zakresie zarządzania kryzysowego i ochrony infrastruktury krytycznej przed zagrożeniami o charakterze terrorystycznym i zagrożeniem cyberprzestrzeni, zbudowany na postawie ustawy o zarządzaniu kryzysowym i ustawy o ABW oraz AW, a następnie rozbudowany przez ustawę o działaniach antyterrorystycznych, jest systemem spójnym. Prace legislacyjne nad aktualizacją i dostosowaniem przepisów do zmieniających się zagrożeń są prowadzone na podstawie informacji otrzymywanych z monitoringu zagrożeń, doświadczeń międzynarodowych oraz wskazówek zdobywanych w czasie ćwiczeń.

Ustawa o działaniach antyterrorystycznych mająca na celu podniesienie efektywności polskiego systemu antyterrorystycznego została opracowana w ścisłym związku z przepisami ustawy o zarządzaniu kryzysowym. Równocześnie spowodowała, że kilka aktów prawnych, w tym zarządzenie nr 18 w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego, uzyskało status przepisów przejściowych. Wprowadzane obecnie rozporządzenia wykonawcze do ustawy o działaniach antyterrorystycznych powodujące zmiany w przedstawionych przepisach regulujących wewnętrzną działalność Agencji Bezpieczeństwa Wewnętrznego nie powinny wpłynąć na rolę szefa ABW w zakresie zarządzania kryzysowego i ochrony infrastruktury krytycznej oraz na zadania realizowane przez niego w tym zakresie.

Bezpieczeństwo nie jest stanem, który można osiągnąć raz na zawsze. Aby istniało poczucie bezpieczeństwa w państwie, cały czas trzeba prowadzić działania wyprzedzające potencjalne zagrożenia. Zgodnie z cyklem planowania należy w sposób ciągły zbierać informacje, analizować je, programować działania, opracowywać plany, wdrażać programy, testować je, a następnie uruchamiać systemy i – ponownie: zbierać informacje, analizować je...

Bibliografia:

Publikacje zwarte:

1. Derlacki J., Kaczorowski W., Lizakowski D., *Zarządzanie kryzysowe*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 1, s. 50–53.
2. Góralski D., *Artykuł 12a znowelizowanej ustawy o zarządzaniu kryzysowym – nowa odpowiedzialność ABW*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3, s. 80–90.
3. Makarski A., *Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 101–112.
4. Pietrek G., *Rola i zadania Agencji Bezpieczeństwa Wewnętrznego w systemie zarządzania kryzysowego*, w: *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, G. Sobolewski, D. Majchrzak (red.), Warszawa 2011, AON, s. 176.
5. Podolski A., *Miejsce Rządowego Centrum Bezpieczeństwa w systemie bezpieczeństwa antyterrorystycznego Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 141–148.
6. Skomra W., *Zarządzanie kryzysowe – praktyczny komentarz po nowelizacji ustawy*, Warszawa 2010, Presscom.
7. Sobolewski G., *Wprowadzenie*, w: *Zarządzanie kryzysowe w systemie bezpieczeństwa państwa*, G. Sobolewski, D. Majchrzak (red.), Warszawa 2011, AON.

Akty prawne:

1. *Decyzja Nr 164 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 15 grudnia 2015 r. w sprawie sposobu reagowania w Agencji Bezpieczeństwa Wewnętrznego w przypadku uzyskania informacji o wystąpieniu zdarzenia o charakterze terrorystycznym*, Dz.Urz. ABW z 2015 r. poz. 32, www.abw.gov.pl/download/8/2003/decyzja164z2015.pdf [dostęp: 10 I 2016].
2. *Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej*, Dz.Urz UE L 210 z 6 VIII 2008 r.
3. *Porozumienie z dnia 19 sierpnia 2010 r. w sprawie ustalenia szczegółowego zakresu i sposobów współdziałania Rządowego Centrum Bezpieczeństwa i Agencji Bezpieczeństwa Wewnętrznego* [online], http://mundurowi.info/index.php/abw/8-porozumienie-rcb-i-abw [dostęp: 15 XII 2015].
4. *Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 31 lipca 2012 r. w sprawie Krajowego Programu Ochrony Lotnictwa*, Dz.U. z 2012 r. poz. 912.
5. *Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*, tekst jednolity: Dz.U. z 2015 r. poz. 508.
6. *Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposoby ich funkcjonowania*, Dz.U. z 2009 r. Nr 226 poz. 1810.
7. *Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym*, Dz.U. z 2004 r. Nr 98 poz. 978.

8. *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*, Dz.U. z 2010 r. Nr 83 poz. 541.
9. *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej*, Dz.U. z 2010 r. Nr 83 poz. 542.
10. *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego*, Dz.U. z 2010 r. Nr 83 poz. 540.
11. *Rozporządzenie Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń*, Dz.U. z 2010 r. Nr 15 poz. 77.
12. *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych,* Dz.U. z 2016 r. poz. 904.
13. *Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach,* Dz.U. z 2013 poz. 1650, ze zm.
14. *Ustawa z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczpospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin,* Dz.U. z 2014 r. poz. 1525.
15. *Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*, tekst jednolity: Dz.U. z 2014 r. poz. 243, ze zm.
16. *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*, tekst jednolity: Dz.U. z 2016 r. poz. 1534.
17. *Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia,* Dz.U. z 2014 r. poz. 1099, ze zm.
18. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,* tekst jednolity: Dz.U. z 2015 r. poz. 1929.
19. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, tekst jednolity: Dz.U. z 2013 r. poz. 1166, ze zm.
20. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Dz.U. z 2010 r. Nr 182, poz. 1228, ze zm.
21. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*, Dz.U. Nr 88, poz. 553, ze zm.
22. *Zarządzenie Nr 16 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 7 marca 2011 r. w sprawie organizacji, składu oraz miejsca i trybu pracy Zespołu Zarządzania Kryzysowego w Agencji Bezpieczeństwa Wewnętrznego*, Dz.Urz. ABW z 2011 r. nr 1, poz. 9.
23. *Zarządzenie Nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego* [online] http://rcb.gov.pl/wp-content/uploads/Zarzadzenie-nr-18.pdf [dostęp: 11 VI 2016].
24. *Zarządzenie Nr 46 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 26 września 2012 r. w sprawie stopni alarmowych w Agencji Bezpieczeństwa Wewnętrznego*, Dz.Urz. ABW z 2014 r. poz. 26; www.abw.gov.pl/download/8/1400/ZarzadzenieNr46z2012DOBRE.pdf [dostęp: 10 I 2016].
25. *Zarządzenie Nr 78 Prezesa Rady Ministrów z dnia 11 października 2011 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego*, M.P. z 2011 r. Nr 93 poz. 955.
26. *Zarządzenie Nr Z-20 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 9 kwietnia 2013 r. w sprawie realizacji przez Agencję Bezpieczeństwa Wewnętrznego zadań przewidzianych dla uruchomienia środków reagowania kryzysowego.*

Źródła internetowe:

1. http://rcb.gov.pl/?page_id=299 [dostęp: 15 XII 2015].
2. http://rcb.gov.pl/?page_id=489 [dostęp: 15 V 2014].
3. http://rcb.gov.pl/wp-content/uploads/KPZK-2013-2015.tj_.pdf [dostęp: 15 XII 2015].
4. http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf [dostęp: 15 XII 2015].
5. http://rcb.gov.pl/wp-content/uploads/Zalacznik-nr-1.pdf [dostęp: 11 VI 2016].
6. http://rcb.gov.pl/wp-content/uploads/Zarzadzenie-nr-18.pdf [dostęp: 11 VI 2016].
7. http://www.sejm.gov.pl/Druki8ka.nsf/0/9CCA65458151278AC1257FB50049D701/$File/516.pdf [dostęp 11 VI 2016].
8. *Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej* [online], http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html [dostęp: 15 XII 2015].
9. Projekt Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie katalogu zdarzeń o charakterze terrorystycznym, http://www.sejm.gov.pl/Druki8ka.nsf/0/9CCA65458151278AC1257FB50049D701/$File/516.pdf [dostęp: 11 VI 2016].
10. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*, CERT.GOV.PL, Warszawa 2015 [online], http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html [dostęp: 15 XII 2015].

Abstrakt

Artykuł dotyczy niezwykle aktualnej problematyki – zarządzania kryzysowego i ochrony infrastruktury krytycznej ze szczególnym uwzględnieniem roli szefa Agencji Bezpieczeństwa Wewnętrznego jako głównego koordynatora polityki antyterrorystycznej i osoby odpowiedzialnej za zapobieganie zagrożeniom o charakterze terrorystycznym, w tym cyberzagrożeniom. Autor dokonał kompleksowego przeglądu aktualnego stanu prawnego, z uwzględnieniem *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* oraz wypracowanych podziałów kompetencyjnych i wskazał najistotniejsze zadania leżące we właściwości ABW. Przedstawił również system określania poziomu zagrożenia terrorystycznego na terenie Rzeczpospolitej Polskiej, wprowadzania stopni alarmowych oraz funkcjonowania instytucji w sytuacji kryzysowej.

W artykule opisano także relacje najważniejszej służby specjalnej w zakresie zarządzania kryzysowego i ochrony infrastruktury krytycznej z innymi uczestnikami zarządzania kryzysowego, w tym z Rządowym Zespołem Zarządzania Kryzysowego, ministrem koordynatorem służb specjalnych, Rządowym Centrum Bezpieczeństwa, administracją centralną i terenową oraz właścicielami i posiadaczami infrastruktury krytycznej.

Słowa kluczowe: zarządzanie kryzysowe, infrastruktura krytyczna, działania antyterrorystyczne, cyberprzestrzeń, monitorowanie zagrożeń.

Abstract

The article tackles a very current topic of crisis management and critical infrastructure protection, with special consideration of the Head of ABW as the key coordinator of antiterrorist policy and the person responsible for prevention of terrorist threats, including cyber-threats. The author has thoroughly studied the current legal status, including *the law on antiterrorist activities* and the existing division of competences, pointing to the most significant tasks from the area of ABW responsibility. The article also presents the system of determining terrorist threat levels in the territory of the Republic of Poland, introducing alarm degrees and functioning of state institutions in case of a crisis situation.

Furthermore, the article describes the relations between the leading special service and other participants of crisis management system, including Government Team for Crisis Management, Minister Coordinator for Special and Intelligence Services, Government Centre for Security, central and local administration and the owners of critical infrastructure.

Keywords: crisis management, critical infrastructure, antiterrorist activities, cyberspace, monitoring of the potential threats.

Rafał Wądołowski

Prawa i obowiązki strony postępowania sprawdzającego

Istotnym elementem systemu bezpieczeństwa państwa jest niewątpliwie ograniczanie dostępu do informacji niejawnych dla jego obywateli lub przedstawicieli innych państw, które są związane z Rzeczpospolitą Polską odpowiednimi umowami międzynarodowymi. Krajowym aktem prawnym o najszerszym zakresie regulacji tego zagadnienia jest *Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych*[1], zwana dalej „ustawą". Procedurę weryfikacji osoby, której mają być udostępnione informacje niejawne, określono w rozdziale 5 tej ustawy zatytułowanym *Bezpieczeństwo osobowe.*

Zgodnie z art. 21 ustawy o ochronie informacji niejawnych dostęp do informacji o klauzuli „poufne", „tajne" albo „ściśle tajne" może nastąpić po uzyskaniu przez daną osobę odpowiedniego poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony tego typu informacji. Należy zaznaczyć, że od tej ogólnej zasady istnieją jednak odstępstwa wynikające z regulacji zawartych w art. 34 ustawy, tj. wyrażenie zgody przez uprawnione podmioty na jednokrotny lub tymczasowy dostęp do informacji niejawnych. Ponadto ustawa zawiera wykaz wyłączeń podmiotowych; osoby zajmujące stanowiska, wymienione w tym wykazie, są zwolnione z obowiązku posiadania poświadczenia lub obowiązek ten jest ograniczony do określonych typów poświadczeń.

Wydanie wspomnianego poświadczenia bezpieczeństwa przez uprawniony organ[2] jest możliwe wyłącznie po przeprowadzeniu wobec określonej osoby postępowania sprawdzającego (stanowi o tym art. 29 ustawy). Ważne jest zatem ustalenie, czym jest postępowanie sprawdzające i w jakim celu się je prowadzi. Na podstawie ustawowo określonej procedury, obowiązków organu prowadzącego oraz praw strony można stwierdzić, że postępowanie sprawdzające jest uregulowanym ustawą, a także – w określonej części – administracyjnym prawem procesowym (kpa)[3], ciągiem czynności urzędowych podejmowanych przez uprawniony podmiot w celu ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy[4]. Ustawodawca w art. 24 ust. 6 ustawy określa, że postępowanie sprawdzające powinno być zakończone przed upływem trzech

[1] Tekst jednolity: Dz.U. z 2016 r. poz. 1167.

[2] Organami prowadzącymi zwykłe postępowania sprawdzające są pełnomocnicy kierowników jednostek organizacyjnych ds. ochrony informacji niejawnych, poszerzone postępowania sprawdzające prowadzą ABW i SKW, ponadto zgodnie z art. 23 ust 5: AW, CBA, Biuro Ochrony Rządu, Policja, Służba Więzienna, SWW, Straż Graniczna oraz Żandarmeria Wojskowa są uprawnione do prowadzenia zwykłych i poszerzonych postępowań sprawdzających.

[3] Art. 3 stanowi, że: „Do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w zakresie nieuregulowanym w ustawie, mają zastosowanie przepisy: art. 6–8, art. 12, art. 14–16, art. 24 § 1 pkt 1–6 i § 2–4, art. 26 § 1, art. 28, art. 29, art. 30 § 1–3, art. 35 § 1, art. 39, art. 41–47, art. 50, art. 55, art. 57–60, art. 61 § 3 i 4, art. 63 § 4, art. 64, art. 65, art. 72, art. 75 § 1, art. 77 § 1, art. 97 § 1 pkt 4 i § 2, art. 98, art. 101, art. 103, art. 104, art. 105 § 2, art. 107, art. 109 § 1, art. 112, art. 113 § 1, art. 125 § 1, art. 156–158 oraz art. 217 *Ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (Dz.U. z 2000 r. Nr 98 poz. 1071, ze zm.)".

[4] Definicja legalna: *rękojmią zachowania tajemnicy – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego* – art. 2 pkt 2 ustawy.

miesięcy od jego wszczęcia, a zatem ze względu na celowy charakter postępowania oraz instrukcyjny[5] termin prowadzenia jego tok powinien mieć charakter ciągły, tj. powinno być ono prowadzone bez przerwy od wszczęcia do rozstrzygnięcia decyzją administracyjną. Ponadto należy dodać, że ze względu na precyzyjne określenie w ustawie jego przebiegu, postępowanie sprawdzające jest postępowaniem autonomicznym z pewnym zakresem stosowania elementów postępowania jurysdykcyjnego określonego w kodeksie postępowania administracyjnego.

Należy zaznaczyć, że nie wszystkie jednostki organizacyjne (pracodawcy) są uprawnione do poddawania pracowników procedurze sprawdzeniowej. W odniesieniu do przepisów przywołanej ustawy można wskazać, że w art. 1 ust. 2 został zawarty częściowo zamknięty wykaz podmiotów „władzy publicznej" zobowiązanych do jej stosowania. Ustawodawca posłużył się ich przykładowym wyliczeniem. W pozostałym zakresie wykaz ma jednak charakter zamknięty. Tak więc podmioty, które nie zostały w nim wymienione i jednocześnie nie są organami władzy publicznej, nie mają obowiązku (a zwłaszcza prawa!) posługiwać się w klasyfikowaniu swoich informacji klauzulami niejawności ustanowionymi ustawą o ochronie informacji niejawnych. Tym bardziej nie mają legitymacji do prowadzenia lub występowania o przeprowadzenie wobec swoich pracowników postępowań sprawdzających (np. przedsiębiorcy niespełniający przesłanek określonych w art. 1 ust. 2 pkt 6)[6].

1. Strona i uczestnicy postępowania sprawdzającego

1.1. Uwagi ogólne

Dokonanie analizy uprawnień przysługujących stronie w toczącym się postępowaniu sprawdzającym wymaga na wstępie ustalenia, jakie podmioty mogą być jego stroną. Wyodrębnienie stron postępowania sprawdzającego napotyka na trudności wynikające ze sposobu ustawowego wprowadzenia do postępowań sprawdzających pojęcia s t r o n y w rozumieniu kodeksowym. Ustawodawca bowiem, przez odesłanie w art. 3 ustawy do art. 28 i 29 kpa[7] stwarza możliwość definiowania strony postępowania sprawdzającego przy zastosowaniu przesłanki *interesu prawnego* lub *obowiązku*. Przy uwzględnieniu orzecznictwa oraz poglądu utrwalonego w doktrynie należy stwierdzić, że wyprowadzenie pojęcia i n t e r e s p r a w n y i o b o w i ą z e k dającego przymiot bycia stroną jest możliwe wyłącznie z konkretnej normy prawa materialnego, która stanowi podstawę zdefiniowania i n t e r e s u i o b o w i ą z k u. *Mieć interes prawny w postępowaniu administracyjnym znaczy to samo, co ustalić przepis prawa materialnego, powszechnie obowiązującego, na którego podstawie można skutecznie żądać czynności organu z zamiarem zaspokojenia jakiejś potrzeby albo żądać zaniechania lub ograniczenia czynności organu sprzecznych z potrzebami danego podmiotu – strony postępowania*[8].

---

[5] Termin i n s t r u k c y j n y jest wyrażeniem języka prawniczego i oznacza, że czynności wykonane przez organ prowadzący dane postępowanie są ważne nawet po jego upłynięciu. Ten termin jest przeciwstawny do t e r m i n u p r e k l u z y j n e g o oznaczającego nieważność czynności wykonanej po tym terminie.

[6] Zob. J. Borowicz, *Przetwarzanie informacji niejawnych w stosunkach pracy,* „Praca i Zabezpieczenie Społeczne" 2011, nr 11, s. 24.

[7] Art. 28 kpa: *Stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes lub obowiązek*.

Art. 29 kpa: *Stronami mogą być osoby fizyczne i osoby prawne, a gdy chodzi o państwowe i samorządowe jednostki organizacyjne i organizacje społeczne – również jednostki nie posiadające osobowości prawnej*.

[8] Por. wyrok WSA w Warszawie z 8 lutego 2011 r. VII SA/Wa 2261/10 oraz wyrok WSA w Warszawie

1.2. Wnioskodawca

Przenosząc zasady ogólne na grunt postępowania sprawdzającego w celu określenia stron, *prima facie* można stwierdzić, że wnioskodawca w osobie kierownika jednostki organizacyjnej jest stroną postępowania sprawdzającego, ponieważ jest ono inicjowane na jego żądanie (wniosek lub polecenie). Ponadto należy zauważyć, że jest osobą działającą w ramach obowiązku, który nakłada na niego ustawodawca w art. 14 ust. 1 ustawy, zobowiązując go do ochrony informacji niejawnych przetwarzanych w podległej mu jednostce. Pozornie trafność tak wyłonionej strony potwierdzają:

- po pierwsze, *obowiązek* (w rozumieniu art. 28 kpa), ponieważ wnioskodawcą uprawnionym przez ustawę jest kierownik jednostki organizacyjnej lub osoba uprawniona do obsady stanowiska lub zlecenia prac (w ujęciu instytucjonalnym, co oznacza, że to uprawnienie jest związane z pełnioną funkcją lub zajmowanym stanowiskiem, nie zaś z konkretną osobą), które wnosząc (lub zlecając realizację zwykłego postępowania podległemu pełnomocnikowi ochrony) o przeprowadzenie postępowania sprawdzającego, dążą do zorganizowania systemu ochrony informacji niejawnych,
- po drugie, *interes prawny*, który przejawia się w uzyskaniu dostępu do informacji niejawnych przez danego pracownika tejże jednostki organizacyjnej, co zapewnia jej właściwe funkcjonowanie.

Należy jednak zauważyć, że pomimo niewątpliwej legitymacji procesowej do żądania przeprowadzenia postępowania, zainicjowane przez wnioskodawcę postępowanie nie rozstrzyga w formie decyzji administracyjnej o jego prawach, lecz wyłącznie odnosi się do osoby sprawdzanej. Ponadto istotnym elementem wskazującym na to, że wnoszący nie jest stroną, jest brak nadania wnioskodawcy uprawnień do odwołania się od decyzji organu pierwszej instancji oraz skargi na decyzję organu drugiej instancji. Powyższe jednoznacznie przesądza o tym, że pomimo niewątpliwych uprawnień, które zostaną omówione poniżej, wnioskodawca nie jest stroną postępowania sprawdzającego, a wyłącznie jego uczestnikiem.

1.3. Osoba sprawdzana

Osoba sprawdzana przez wyrażenie zgody na przeprowadzenie wobec niej postępowania sprawdzającego (w ankiecie bezpieczeństwa osobowego lub odrębnym oświadczeniu w przypadku trybu wynikającego z art. 32 ust. 4 ustawy) w sposób dorozumiany wskazuje, że jest zainteresowana uzyskaniem dostępu do informacji niejawnych, a posiadane uprawnienie podwyższy jej kwalifikacje i umożliwi zajmowanie stanowiska związanego z dostępem do tego rodzaju informacji. Należy przyjąć, że osoba sprawdzana występuje w charakterze strony postępowania od chwili jego wszczęcia przez organ powołany ustawą. Posiadanie statusu strony przez taką osobę wynika z celu prowadzonego wobec niej postępowania sprawdzającego kończącego się wydaniem decyzji administracyjnej konkretno-indywidualnej, która rozstrzyga o prawach osoby sprawdzanej w zakresie dostępu do informacji niejawnych. Jednocześnie należy nadmienić, że decyzja kończąca postępowanie sprawdzające nie rozstrzyga o prawach wnioskodawcy, chociaż pośrednio ma wpływ na

z 15 kwietnia 2011 r. I SA/Wa 2326/10.

jego funkcjonowanie jako jednostki organizacyjnej. Ponadto status osoby sprawdzanej znajduje swoje potwierdzenie w przyznaniu przez ustawodawcę wyłącznie takiej osobie środków zaskarżenia decyzji wydanej przez organ uprawniony do prowadzenia postępowania sprawdzającego (jak wspomniano wyżej wnioskodawca nie ma takich uprawnień).

1.4. Organ prowadzący postępowanie sprawdzające

Warto również zauważyć, że zgodnie z obowiązującym poglądem opartym na orzecznictwie sądowym organ powołany do wydania decyzji administracyjnej nie może być stroną prowadzonego postępowania administracyjnego (oznacza to między innymi, że nie ma legitymacji do wniesienia skargi na wydaną decyzję)[9].

2. Relacje zachodzące między podmiotami w postępowaniu sprawdzającym

Przy uwzględnieniu doktrynalnego ujęcia relacji zachodzących między podmiotami występującymi w postępowaniu sprawdzającym, należy stwierdzić, że najistotniejszym rodzajem zależności między stroną a organem prowadzącym postępowanie jest stosunek materialnoprawny. W literaturze jest on definiowany w następujący sposób:

> Stosunek materialnoprawny określa wzajemne prawa i obowiązki dwu lub więcej podmiotów, zawarte w normach prawa administracyjnego. Owe prawa i obowiązki mogą tworzyć prosty albo złożony układ zależności. W układzie prostym określone prawo odpowiada określonemu obowiązkowi i odwrotnie. (…) W prawie administracyjnym jednym z podmiotów tego stosunku jest zawsze organ administracji państwowej albo podmiot, któremu ustawa wprost lub za pośrednictwem tego organu powierza pełnienie administracji publicznej (funkcji z zakresu administracji publicznej)[10].

Przykładem takiego podmiotu jest pełnomocnik ds. ochrony informacji niejawnych, który nie jest ustawowo ustanowiony jako organ administracji publicznej (jak np. ABW lub SKW), jednak posiada ustawowe uprawnienie do wydawania decyzji w trybie administracyjnym.

Innym ważnym stosunkiem zachodzącym między uczestnikami postępowania sprawdzającego, o nieco szerszym charakterze, jest stosunek proceduralny. Łączy on podmiot prowadzący postępowanie, osobę sprawdzaną oraz wnioskodawcę, a także potencjalnie innych uczestników tego postępowania. Relacje zachodzące w tym stosunku są określone przepisami proceduralnymi ustawy o ochronie informacji niejawnych oraz mającymi zastosowanie przepisami kodeksu postępowania administracyjnego. Wymienione podmioty nabywają prawa, a także są zobowiązane do konkretnych zachowań, na podstawie przepisów stosowanych w toku prowadzonego postępowania w zależności od podejmowanych przez te podmioty aktywności oraz zdarzeń faktycznych mających znaczenie prawne (np. śmierć osoby sprawdzanej).

[9] Wyrok NSA z 19 stycznia 2012 r., II OSK 2585/11 oraz Postanowienie NSA z 29 kwietnia 1986 r., SA/Gd 43/86, za: B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2006, s. 228.

[10] M. Wierzbowski, J. Lang, *Prawo administracyjne*, Warszawa 2001, s. 25–26.

2.1. Pierwszeństwo stosowania przepisów

Hołdując fundamentalnej zasadzie prawa *Lex specialis derogat legi generali*, w odniesieniu do postępowania sprawdzającego, należy stwierdzić, że przepisy ustawy o ochronie informacji niejawnych są przepisami szczególnymi wobec kodeksowej procedury administracyjnej i z tego względu mają pierwszeństwo w stosowaniu (znajduje to potwierdzenie w treści art. 3 ustawy). Prawodawca w treści rozdziału 5 ustawy, w którym określono procedurę postępowania sprawdzającego, nie używa terminu strona postępowania i posługuje się wyłącznie pojęciami: osoba sprawdzana, wnioskodawca, kierownik jednostki organizacyjnej, osoba uprawniona do obsady stanowiska, a także osoba uprawniona do zlecenia prac. Takie wskazanie konkretnych uczestników postępowania sprawdzającego poważnie zawęża możliwość przystąpienia do niego innych osób w charakterze strony, nawet pomimo uzasadnienia interesu prawnego lub wykazania obowiązku. W przypadku wystąpienia takiej próby organ prowadzący powinien ustalić istnienie związku materialnoprawnego między sytuacją prawną podmiotu a postępowaniem sprawdzającym (np. żądanie kierownika jednostki organizacyjnej dotyczące podjęcia zawieszonego postępowania sprawdzającego wobec pracownika na podstawie art. 97 § 2 kpa). Jeżeli podmiot bezpośrednio zainteresowany wynikiem postępowania sprawdzającego nie może uzasadnić swego zainteresowania konkretnymi przepisami prawa, to nie może być uznany za stronę (np. w przypadku zmiany podmiotowej po stronie wnioskodawcy, tj. wystąpienia z żądaniem kontynuowania postępowania sprawdzającego przez kierownika jednostki organizacyjnej, w której osoba sprawdzana podjęła nowe zatrudnienie na stanowisku z dostępem do informacji niejawnych, pierwszeństwo zastosowania w zależności od sposobu rozwiązania stosunku pracy uzyskuje art. 31 ust. 1 pkt 1 lub pkt 2 ustawy, a zatem postępowanie należy umorzyć, a żądanie uznać za bezpodstawne).

Jak już wskazano, ustawa o ochronie informacji niejawnych w art. 3 odsyła do wybranych przepisów kodeksu postępowania administracyjnego, które należy stosować wyłącznie w zakresie nieuregulowanym w ustawie. Z treści wspomnianego przepisu odsyłającego wynika, że przepisy kpa należy stosować wprost, ponieważ ustawodawca nie zezwolił na ich *odpowiednie* stosowanie (przepis nie zawiera takiej dyspozycji). Brak możliwości *odpowiedniego* stosowania przepisów kpa utrudnia, a niekiedy uniemożliwia ich stosowanie na gruncie postępowania sprawdzającego. Wskazane jest zatem postulowanie zmiany, jak się wydaje, błędnej redakcji wspomnianego przepisu przez dodanie terminu odpowiednio.

3. Osoba sprawdzana jako strona postępowania sprawdzającego – uprawnienia i obowiązki

Najistotniejszym prawem osoby, wobec której uprawniony wnioskodawca zamierza wystąpić o przeprowadzenie postępowania sprawdzającego (polecić wszczęcie), jest prawo odmowy wyrażenia zgody na poddanie się procedurze sprawdzeniowej oraz cofnięcia zgody wyrażonej uprzednio. Zgoda osoby na przeprowadzenie wobec niej postępowania sprawdzającego jest warunkiem sine qua non wszczęcia i prowadzenia postępowania sprawdzającego przez uprawniony organ (stanowi o tym art. 24 ust. 8 ustawy). Pomijając legitymację podmiotu do prowadzenia postępowania wynikającą z ustawy, należy wskazać, że drugim filarem, na którym ta kompetencja się opiera, jest

zgoda osoby sprawdzanej. W przypadku cofnięcia udzielonej zgody organ traci uprawnienie do dalszego rozpoznawania osoby w trybie postępowania sprawdzającego (wymóg wyrażenia zgody obowiązuje przez cały tok postępowania). W związku z tym, że zgoda jest udzielana w formie przypisanej przez ustawę, tj. pisemnie (przez wypełnienie i podpisanie ankiety bezpieczeństwa osobowego), jej cofnięcie również powinno zostać wyrażone w takiej samej formie, co do zasady, przez złożenie pisemnego oświadczenia woli osoby sprawdzanej. Istnieje również możliwość przyjęcia od osoby sprawdzanej ustnego oświadczenia do protokołu w trakcie jej wysłuchania, o ile w toku postępowania przeprowadza się powyższą czynność. W przypadku braku zgody organ prowadzący postępowanie powinien je niezwłocznie zakończyć i wydać decyzję o umorzeniu z uwagi na jego bezprzedmiotowość (art. 31 ust. 1 pkt 4 ustawy). Szczególnym rodzajem postępowania jest kontrolne postępowanie sprawdzające, ponieważ zostaje ono wszczęte z urzędu, a zgoda osoby powtórnie sprawdzanej nie jest wymagana (art. 33 ust. 1 ustawy).

3.1. Gwarancje procesowe strony

W przypadku skutecznego złożenia wniosku o przeprowadzenie poszerzonego postępowania sprawdzającego przez wnioskodawcę lub wszczęcia postępowania przez pełnomocnika ochrony na polecenie przełożonego, osoba sprawdzana jako strona jest uprawniona do otrzymania zawiadomienia o jego wszczęciu. Kodeks nie określa formy zawiadomienia, ale ze względu na zasadę pisemności wyrażoną art. 14 kpa zawiadomienie powinno przybrać formę pisemną lub dokumentu elektronicznego (art. 61 § 4 kpa). Odrębną podstawą prawną do zawiadomienia osoby sprawdzanej o wszczęciu postępowania jest art. 33 ust. 6 ustawy, który ma zastosowanie wyłącznie w przypadku prowadzenia wobec osoby sprawdzanej kontrolnego postępowania sprawdzającego.

3.1.1. Zażalenie do organu II instancji

Jeżeli w toku postępowania organ prowadzący postanowi o jego zawieszeniu lub podjęciu, osoba sprawdzana na podstawie art. 27 ust. 3 ustawy jest uprawniona do otrzymania zawiadomienia o wydaniu wymienionych postanowień. Przywołany przepis, podobnie jak poprzedni, nie określa formy zawiadomienia, ale z uwagi na przysługujące stronie środki odwoławcze oraz zasadę pisemności zawiadomienie powinno przybrać formę pisemną. Warto zauważyć, że na podstawie art. 27 ust. 4 ustawy osobie sprawdzanej przysługuje zażalenie na postanowienie o zawieszeniu prowadzonego wobec niej postępowania (odpowiednio) w trybie przewidzianym dla procedury odwoławczej od decyzji I instancji. Determinuje to obowiązek doręczenia osobie sprawdzanej postanowienia wraz z jego uzasadnieniem. Niestety, przepisy ustawy nie stanowią o obowiązku uzasadnienia tego postanowienia. Jest to tym bardziej zaskakujące, że art. 125 § 3 kpa również nie ma zastosowania do postępowań sprawdzających. Brak nakazu uzasadnienia wskazanego postanowienia wynika z braku odpowiedniej regulacji w ustawie i może utrudniać wykorzystanie prawa do wniesienia zażalenia przez stronę. Luka prawna, o której mowa, powinna być zlikwidowana przez ustawodawcę przez odesłanie do art. 125 § 3 kpa. Ponadto kodeks postępowania administracyjnego uprawnia osobę sprawdzaną do żądania podjęcia postępowania na podstawie art. 97 § 2 kpa, jeżeli ustąpiły przyczyny uzasadniające jego zawieszenie. W razie negatywnego rozstrzygnięcia żądania strony i odmowy podjęcia zawieszonego postępowania przez organ, osobie

sprawdzanej przysługuje zażalenie na to postanowienie do organu II instancji na podstawie art. 101 § 3 kpa.

Ponadto *Stronie służy skarga na bezczynność, jeżeli organ nie wydaje postanowienia o podjęciu zawieszonego postępowania mimo ustania przyczyn jego zawieszenia po wyczerpaniu przewidzianego trybu lub gdy wniosek strony o podjęcie nie jest rozpoznany* (wyrok NSA z 7 maja 2003 r., I SAB 353/02, LexPolonica nr 394911; wyrok WSA w Warszawie z 15 marca 2006 r., II SA/Wa 137/06, Centralna Baza Orzeczeń Sądów Administracyjnych)[11].

Krytycznie należy ocenić brak możliwości zastosowania art. 98 § 1 kpa stanowiącego o uprawnieniu strony, na której wniosek wszczęto postępowanie, do wystąpienia o zawieszenie tego postępowania. Uprawnienie to nie może być wykorzystane, ponieważ osoba sprawdzana nie ma legitymacji do żądania wszczęcia wobec niej postępowania sprawdzającego (wniesienia wniosku). Z uwagi na powyższe, pomimo odesłania w art. 3 ustawy do art. 101 § 2 kpa, ten przepis nie może być skutecznie zastosowany.

3.1.2. Odwołanie do organu II instancji

Ustawodawca w art. 31 ust. 2 ustawy nakazuje zawiadomić osobę sprawdzaną o umorzeniu postępowania sprawdzającego. Przepis zredagowany w art. 31 ustawy wydaje się niezupełny, ponieważ umorzenie kończy postępowanie w danej instancji, a zatem powinno mieć formę decyzji administracyjnej, od której stronie służy odwołanie do organu II instancji. Przywołany przepis nakazuje jedynie zawiadomić osobę sprawdzaną o umorzeniu, bez określenia formy zawiadomienia oraz pouczenia strony o prawie wniesienia odwołania. Wskazówką dla organu i osoby sprawdzanej w tym zakresie jest treść art. 35 ust. 1 oraz art. 37 ust. 1 ustawy stanowiących, że od decyzji o umorzeniu postępowania osobie sprawdzanej przysługuje odwołanie. Wspomniany przepis powinien być zatem rozszerzony o wskazane powyżej elementy, tj. nakaz umorzenia postępowania decyzją z uzasadnieniem oraz obowiązek pouczenia strony o przysługującym prawie wniesienia odwołania.

Jednocześnie należy zasygnalizować, że również od decyzji o umorzeniu kontrolnego postępowania sprawdzającego na podstawie art. 33 ust. 11 pkt 3 stronie przysługuje odwołanie. Decyzja umarzająca postępowanie kontrolne nie zmienia jednak przyznanego stronie prawa dostępu do informacji niejawnych. Zatem jakie byłyby potencjalne przesłanki odwołania? Podstawą wydania tego typu decyzji nie jest rozstrzygnięcie merytoryczne o prawach strony, lecz upływ dwunastomiesięcznego terminu ustawowego oznaczonego do prowadzenia postępowania kontrolnego. Brak merytorycznego rozstrzygnięcia w przypadku postępowania wszczętego z urzędu pozostaje w sprzeczności z przyjętą w teorii prawa generalną regułą rozstrzygania decyzją administracyjną o prawach lub obowiązkach strony. Należy przyjąć, że ustawodawca, przyznając osobie sprawdzanej prawo do odwołania, kierował się zapewne zasadami ogólnymi w zakresie dwuinstancyjności organów. Na uwagę zasługuje odesłanie ustawowe do art. 105 § 2 kpa, który może być na tej podstawie stosowany w postępowaniu sprawdzającym. Wskazany przepis stanowi między innymi, że postępowanie może być umorzone na wniosek strony, na której żądanie zostało wszczęte. Powstają zatem trudności w jego stosowaniu, ponieważ strona (osoba sprawdzana) nie jest uprawniona do żądania wszczęcia

[11] S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010, s. 175.

postępowania sprawdzającego, wnioskodawca natomiast (najczęściej jest nim kierownik jednostki organizacyjnej) nie może żądać jego umorzenia w związku z tym, że nie jest stroną postępowania sprawdzającego. Wnioskodawca może spowodować umorzenie postępowania przez poinformowanie organu prowadzącego o okolicznościach stanowiących faktyczną podstawę umorzenia (art. 31 ustawy)[12].

Podmiot, który zakończył postępowanie sprawdzające z wynikiem pozytywnym na podstawie art. 29 ustawy jest zobowiązany przekazać osobie sprawdzonej poświadczenie bezpieczeństwa, podobnie jak w przypadku doręczenia decyzji o odmowie wydania albo cofnięciu poświadczenia bezpieczeństwa (art. 30 ust. 5 ustawy; przepis stosowany do kontrolnych postępowań sprawdzających w związku z odesłaniem do art. 33 ust. 8 ustawy).

Wyłącznie osoba, wobec której zakończono postępowanie sprawdzające w I instancji decyzją o cofnięciu albo odmową wydania poświadczenia bezpieczeństwa lub decyzją o umorzeniu postępowania sprawdzającego, a także o umorzeniu kontrolnego postępowania sprawdzającego, jest uprawniona do wniesienia odwołania do organu II instancji. W odniesieniu do zwykłego postępowania sprawdzającego prowadzonego przez podmioty inne niż wymienione w art. 23 ust. 5 ustawy strona wnosi odwołanie na podstawie art. 37 ustawy. Adresatem odwołania właściwym do jego rozpatrzenia jest szef ABW lub szef SKW. Osoba sprawdzona jest zobowiązana do wniesienia odwołania za pośrednictwem pełnomocnika ochrony (odwołanie nie wymaga uzasadnienia), który wydał zaskarżaną decyzję, w terminie 14 dni od dnia jej doręczenia. Pełnomocnik jest zobowiązany przesłać odwołanie wraz z aktami postępowania sprawdzającego odpowiednio szefowi ABW lub szefowi SKW (właściwość rzeczową wymienionych organów określono w art. 10 ust. 2 i 3 ustawy) w terminie 14 dni od dnia, w którym je otrzymał. Organ II instancji powinien rozpatrzyć odwołanie nie później niż w ciągu trzech miesięcy. Ponadto, jak stanowi art. 35 ust. 5 ustawy, wniesienie odwołania nie wstrzymuje wykonania decyzji. Zatem wnoszący odwołanie w toku postępowania kontrolnego traci dostęp do informacji niejawnych pomimo tego, że decyzja o cofnięciu poświadczenia bezpieczeństwa jest nieprawomocna albo nie uzyskuje uprawnienia w przypadku decyzji o odmowie jego wydania w ramach zwykłego postępowania.

Jeżeli strona wnosi odwołanie od decyzji wydanej w I instancji przez ABW, SKW oraz podmioty wymienione w art. 23 ust. 5, to kieruje je do Prezesa Rady Ministrów RP w terminie 14 dni od dnia jej otrzymania za pośrednictwem podmiotu, który wydał zaskarżaną decyzję, i nie wymaga ono uzasadnienia. Organ I instancji jest zobowiązany przesłać odwołanie wraz z aktami postępowania sprawdzającego Prezesowi Rady Ministrów RP w terminie 14 dni od dnia, w którym je otrzymał. Organ II instancji powinien rozpatrzyć odwołanie nie później niż w ciągu trzech miesięcy. Ponadto, podobnie jak w przypadku zwykłego postępowania sprawdzającego, wniesienie odwołania nie wstrzymuje wykonania decyzji.

3.1.3. Skarga do wojewódzkiego sądu administracyjnego

Na decyzję organu II instancji (odpowiednio szef ABW, szef SKW albo Prezes Rady Ministrów), jeżeli nie rozstrzyga ona odwołania według żądania strony, osobie sprawdzanej przysługuje skarga do wojewódzkiego sądu administracyjnego. Skargę należy wnieść w terminie 30 dni od dnia doręczenia decyzji organu odwoławczego. Do

[12] S. Hoc, *Ustawa o ochronie informacji niejawnych*..., s. 185.

postępowania przed sądem administracyjnym stosuje się odpowiednio przepisy *Ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi*[13]. Przepisami szczególnymi są regulacje wskazane w art. 38 ustawy, które stanowią, że skarga jest rozpatrywana na posiedzeniu niejawnym, odpis sentencji wyroku wraz z uzasadnieniem sąd doręcza tylko właściwemu organowi odwoławczemu i skarżącemu, natomiast osobie uprawnionej do obsady stanowiska doręcza tylko odpis wyroku.

Osoba wnosząca odwołanie, na podstawie art. 36 ust. 3 ustawy, jest uprawniona do żądania zlecenia przez Prezesa Rady Ministrów (odpowiednio w zwykłym postępowaniu przez szefa ABW albo szefa SKW) właściwemu podmiotowi (tj. organowi, który prowadził wobec osoby sprawdzanej postępowanie sprawdzające) przeprowadzenia dodatkowych czynności, w tym specjalistycznych badań, o których mowa w art. 26 ust. 6, w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym lub kontrolnym postępowaniu sprawdzającym. Należy dodać, że możliwość przeprowadzenia badań wskazanych w art. 26 ust. 6 istnieje wyłącznie w ramach poszerzonego postępowania sprawdzającego.

3.1.4. Wznowienie prawomocnie zakończonego postępowania sprawdzającego

Ustawa w art. 3 odsyła do art. 16 kpa, który w doktrynie jest uznawany za egzemplifikację zasady trwałości ostatecznych decyzji administracyjnych. Należy jednak wskazać, że ten przepis stanowi również o dopuszczalności wznowienia postępowania, ale wyłącznie w przypadkach przewidzianych w kodeksie lub ustawach. Wznowienie dotyczy ostatecznych decyzji, które okazały się prawnie wadliwe. Nie każda wada jednak uzasadnia eliminację decyzji lub przesłankę ponownego rozpatrzenia sprawy. Aby nie pozostawić organom stosującym prawo swobodnej oceny tego, które z wad mają taki charakter, ustawodawca określa te wady w postaci przesłanek wznawiających[14]. Przykładem ustawowego określenia przesłanki dopuszczalności wznowienia postępowania jest art. 39 ustawy o ochronie informacji niejawnych. Prawodawca uprawnia osobę sprawdzoną[15] do wystąpienia z wnioskiem o wznowienie postępowania sprawdzającego do podmiotu, który wydał decyzję o odmowie wydania albo cofnięciu poświadczenia bezpieczeństwa w I instancji, w terminie 30 dni od dowiedzenia się o zaistnieniu niżej wskazanych przesłanek. Pozytywnymi przesłankami umożliwiającymi wznowienie postępowania są:

1) wydanie wymienionych decyzji wyłącznie w związku z przedstawieniem osobie sprawdzanej zarzutu popełnienia przestępstwa, postawienie jej w stan oskarżenia albo skazanie za przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe,
2) postępowanie karne, w którego ramach wydano przytoczone orzeczenia (w pkt 1), i które zostało następnie umorzone lub zakończone uniewinnieniem osoby sprawdzanej.

Jeżeli organ uprawniony do wznowienia postępowania uzna wniosek za bezzasadny, to odmawia wznowienia postępowania w drodze decyzji, od której na podstawie

[13] Dz.U. z 2002 r. Nr 153 poz. 1270.

[14] E. Bojanowski, Z. Cieślak, J. Lang, *Postępowanie administracyjne i postępowanie przed sądami administracyjnymi*, Warszawa 2008, s. 65.

[15] W art. 39 ust. 2 ustawy błędnie zastosowano termin o s o b a s p r a w d z a n a, ponieważ z chwilą uprawomocnienia się decyzji kończącej postępowanie sprawdzające jest to osoba „sprawdzona".

art. 41 ustawy przysługuje osobie sprawdzonej odwołanie do organu II instancji. Wyjątek od tej zasady stanowią decyzje wydane przez Prezesa Rady Ministrów oraz szefów ABW i SKW, jeżeli te organy działały jako organ II instancji. Wówczas odwołanie nie przysługuje, osoba sprawdzana niezadowolona z decyzji może jednak zwrócić się z wnioskiem o ponowne rozpatrzenie sprawy.

3.2. Uprawnienia podmiotowe strony

3.2.1. Wysłuchanie

Nawiązaniem do zasady czynnego udziału strony w postępowaniu, ustanowionej w art. 10 kpa, który jednak nie ma zastosowania w postępowaniu sprawdzającym, jest instytucja wysłuchania. Osoba sprawdzana ma prawo do osobistego ustosunkowania się do informacji wywołujących wątpliwości niepozwalające na ustalenie, czy daje ona rękojmię zachowania tajemnicy (art. 25 ust. 6 ustawy). Podmiot prowadzący postępowanie jest zobowiązany do wysłuchania osoby sprawdzanej i sporządzenia z tej czynności protokołu. Ustawodawca uprawnia osobę sprawdzaną do stawienia się na wysłuchanie z pełnomocnikiem: *Osoba ta może stawić się na wysłuchanie ze swoim pełnomocnikiem*, nie definiuje jednak osoby pełnomocnika ani formy udzielonego pełnomocnictwa. Brak jednoznacznego określenia rodzaju pełnomocnictwa i ewentualnie kwalifikacji osoby przyjmującej pełnomocnictwo powoduje odmienne interpretacje w tym zakresie. Na przykład I. Stankowska w przytaczanym już komentarzu z roku 2011 stwierdza, że: *Należy zatem przyjąć, że osoba sprawdzana ma pełną swobodę decyzji w tym zakresie, to ona decyduje, kto wraz z nią będzie obecny podczas rozmowy z prowadzącym postępowanie* (…). Czy zatem osoba niemająca pełnej zdolności do czynności prawnych również? Nie można przyjąć takiego poglądu za trafny, ponieważ o sposobie ustanowienia pełnomocnika będzie przesądzał charakter czynności wysłuchania. Postępowanie sprawdzające jest rodzajem szczególnego postępowania w odniesieniu do postępowania administracyjnego, w jego toku jednak stosuje się bezpośrednio, a w części subsydiarnie, wiele przepisów kodeksowych. Pozwala to na stwierdzenie, że pełnomocnikiem osoby sprawdzanej może być pełnomocnik w rozumieniu kodeksu postępowania administracyjnego. Za takim pełnomocnictwem przemawia charakter wysłuchania. Artykuł 33 kpa może być zastosowany przez osobę sprawdzaną, ponieważ jest to przepis prawa powszechnie obowiązującego. Brak odesłania do tego przepisu w art. 3 ustawy nie wyłącza prawa strony do udzielenia pełnomocnictwa w tym właśnie trybie. Przy ewentualnej nowelizacji ustawy wskazane byłoby jednoznaczne określenie charakteru pełnomocnictwa przez odesłanie do art. 33 kpa.

3.2.2. Sprostowanie błędów pisarskich

Strona postępowania sprawdzającego może, na podstawie art. 113 § 1 kpa, żądać sprostowania błędów pisarskich i rachunkowych oraz innych oczywistych omyłek w decyzji o odmowie wydania albo cofnięciu poświadczenia bezpieczeństwa, decyzji o jego umorzeniu, a także w poświadczeniu bezpieczeństwa. Zakres zmian jest jednak ograniczony.

> Trafnie stwierdza się w literaturze, że nie będą podlegały sprostowaniu w omawianym trybie błędy i omyłki istotne, których dopuszczono się w stosowaniu prawa (…). Postanowienie o sprostowaniu błędów i omyłek w decyzji ma ten skutek, że po jego wydaniu decyzja musi być wykonywana stosownie do treści zgodnej ze sprostowaniem, a w przypadku zaskarżenia powinna być również wraz z nim oceniana. (…) Prawidłowo dokonane sprostowanie błędów i omyłek staje się bowiem integralną częścią treści decyzji[16].

Należy nadmienić, że w odniesieniu do postanowień wydanych w ramach postępowania sprawdzającego nie ma możliwości prawnych sprostowania omyłki w postanowieniach (o zawieszeniu i podjęciu postępowania) wydanych w toku postępowania sprawdzającego, art. 126 kpa nie ma bowiem zastosowania. Wyłączenie możliwości ingerencji (na wniosek lub z urzędu) w treść postanowień w trybie art. 113 kpa istotnie uchybia podstawowym prawom strony i zawęża możliwość autokontroli organowi wydającemu postanowienie. Powyższe zasługuje na zmianę przez prawodawcę.

3.2.3. Żądanie określenia terminu zakończenia postępowania

Jak już wspomniano, postępowanie sprawdzające powinno być zakończone przed upływem trzech miesięcy od dnia złożenia przez osobę zainteresowaną do pełnomocnika ochrony wypełnionej ankiety bezpieczeństwa osobowego lub wniosku (wraz z ankietą) o przeprowadzenie postępowania do ABW lub SKW przez uprawnionego wnioskodawcę. Należy również wskazać na termin sześciu miesięcy obowiązujący w przypadku prowadzenia kolejnego postępowania sprawdzającego na podstawie art. 32 ust. 2 ustawy. Na mocy art. 24 ust. 7 osoba sprawdzana jest uprawniona do wystąpienia z wnioskiem do organu prowadzącego postępowanie o informację na temat przewidywanego terminu zakończenia postępowania, o ile nastąpiło przekroczenie terminu ustawowego. Może również żądać podania powodów przedłużania się postępowania. Organ nie musi jednak ich przedstawić, powołując się na naruszenie zasad ochrony informacji niejawnych (oznacza to, że osoba sprawdzana nie może ich poznać w związku z tym, iż dotyczą one okoliczności, których ujawnienie zakłóciłoby gromadzenie materiału dowodowego lub jest determinowane brakiem posiadania odpowiedniego poświadczenia bezpieczeństwa przez osobę sprawdzaną).

3.2.4. Prawo do przejrzenia akt

Ważnym uprawnieniem strony zakończonego zwykłego postępowania sprawdzającego jest możliwość przejrzenia akt prowadzonego wobec niej postępowania sprawdzającego, wynikająca z art. 72 ust. 4 ustawy. Jednocześnie warto wskazać na mało precyzyjny sposób zredagowania tego przepisu. Ustawodawca bowiem wymienia akta zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających bez dookreślenia, czy odnośnie do akt postępowań kontrolnych chodzi wyłącznie o zwykłe, czy również o poszerzone postępowania sprawdzające. Za wskazówkę interpretacyjną może służyć zamknięty wykaz podmiotów uprawnionych do wglądu w akta zakończonych poszerzonych postępowań wymienionych w art. 72 ust. 1 ustawy. Ponadto przepis nie rozstrzyga o sposobie udostępnienia akt w przypadku, gdy zawierają one dokumenty niejawne,

[16] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2006, s. 541.

a osoba sprawdzona nie posiada poświadczenia bezpieczeństwa z powodu negatywnej decyzji kończącej postępowanie lub upływu jego ważności. Dodatkowo w zakresie udostępnienia akt nie mają zastosowania przepisy kodeksu, które rozstrzygają powyższą kwestię (art. 73 i 74 kpa), co komplikuje egzekwowanie ustawowego prawa przez stronę, a także wprowadza dowolność w realizacji obowiązku przez organ dysponujący aktami. Brak odpowiedniej szczegółowej regulacji powyższej kwestii zasługuje na krytykę ustawodawcy[17].

3.3. Obowiązki strony

Należy nadmienić, że osoba sprawdzana jako strona postępowania może występować w postępowaniu sprawdzającym prowadzonym w trybie ogólnym, tj. na wniosek (polecenie) uprawnionego podmiotu, z jednoczesnym wyrażeniem zgody na to postępowanie. Wówczas obowiązki osoby sprawdzanej wynikające z ustawy lub kodeksu są przez nią realizowane dobrowolnie. Odmiennie należy ocenić pozycję osoby sprawdzanej w kontrolnym postępowaniu sprawdzającym, ponieważ jest ono wszczynane z urzędu przez uprawniony organ, a zgoda osoby sprawdzanej nie jest wymagana do jego wszczęcia i prowadzenia. W toku postępowania kontrolnego organ, wzywając osobę sprawdzaną do wykonania określonej czynności, działa na podstawie władztwa administracyjnego i stosuje przymus określany w doktrynie jako funkcjonalny.

3.3.1. Poddanie się badaniom specjalistycznym

Organ prowadzący poszerzone postępowanie sprawdzające na podstawie art. 26 ust. 6 ustawy może zobowiązać osobę sprawdzaną do poddania się badaniom specjalistycznym oraz do udostępnienia wyników tych badań. Ustawodawca określa jedynie kategorie wątpliwości, które mogą powodować zobowiązanie osoby do poddania się badaniom, tj. chorobę psychiczną lub inne zakłócenia czynności psychicznych, a także uzależnienie od alkoholu, środków odurzających albo substancji psychotropowych. Przepis nie wskazuje specjalisty z zakresu nauk medycznych, który powinien przeprowadzić badanie określone w zobowiązaniu, ani konkretnej instytucji. Organ zobowiązujący powinien kierować się w tej mierze informacjami uzyskanymi od osoby sprawdzanej, a także ewentualnymi informacjami o przeprowadzonym leczeniu z placówek służby zdrowia i na tej podstawie wskazać odpowiedniego specjalistę. Z uwagi na brak szczegółowej regulacji tego zagadnienia w przepisach ustawy innym dopuszczalnym sposobem wyjaśnienia zaistniałych wątpliwości może być przedstawienie zaświadczenia o stanie zdrowia wystawionego przez odpowiedniego specjalistę wybranego przez samą osobę sprawdzaną, o ile organ nie wskazał konkretnej osoby lub podmiotu w zobowiązaniu. Należy w tym miejscu wskazać na ogólną zasadę zakazującą organom publicznym dokonywania interpretacji rozszerzającej stosowanych przepisów prawa[18]. Stosowanie takiej interpretacji nie może mieć na celu ograniczenia praw strony postępowania. Tego rodzaju wykładnia jest natomiast możliwa w odniesieniu do jej praw i wolności. W kontekście braku precyzji wspomnianych przepisów uzasadnionym postulatem kierowanym do prawodawcy wydaje się uszczegółowienie art. 26 ust. 6 ustawy, przede wszystkim

[17] Należy wskazać, że w komentarzu S. Hoca do ustawy o ochronie informacji niejawnych z 2010 r., jak również w komentarzu autorstwa I. Stankowskiej z 2011 r., nie dostrzeżono braku regulacji tej kwestii, zamieszczono jedynie powierzchowne omówienie przepisu, o którym mowa.

[18] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego*…, s. 60.

doprecyzowanie zakresu zobowiązania, jaki może zastosować organ, oraz sposobu wykonania obowiązku poddania się przez osobę sprawdzaną badaniom wskazanym przez organ. Jednocześnie regulacją ustawową należałoby objąć zasady pokrywania kosztów wynikłych z tego względu, z rozróżnieniem, gdy postępowanie toczy się na wniosek kierownika jednostki albo z urzędu (w przypadku kontrolnego postępowania sprawdzającego).

3.3.2. Stawienie się na wezwanie

Kolejnym potencjalnym obowiązkiem strony wynikającym z art. 50 § 1 kpa jest stawienie się na wezwanie organu prowadzącego postępowanie, np. w celu wzięcia udziału w protokołowanej czynności wysłuchania w trybie art. 25 ust. 6 ustawy. W przypadku błędnego wezwania strony (np. nieprzeprowadzenia czynności z winy organu) lub wezwania w toku kontrolnego postępowania sprawdzającego prowadzonego z urzędu, strona może dochodzić zwrotu kosztów podróży, których organ prowadzący postępowanie nie przyzna z powodu braku podstawy prawnej, art. 56 kpa nie ma bowiem zastosowania w toku postępowań sprawdzających. Należy również zauważyć, że ustawodawca nie zezwala też na nakładanie kary grzywny przez organ wzywający w przypadku niestawienia się strony, ponieważ zastosowanie art. 88 kpa jest wyłączone dyspozycją art. 86 kpa, który nie znalazł się w katalogu wymienionym w art. 3 ustawy i podobnie jak wskazany powyżej nie ma zastosowania w toku postępowań sprawdzających.

Brak możliwości wykorzystania w postępowaniu sprawdzającym art. 86 oraz art. 75 § 2 kpa poważnie ogranicza uzyskanie od osoby sprawdzanej wiarygodnych informacji, gdyż za fałszywe zeznania nie ponosi ona odpowiedzialności. Trzeba jednak nadmienić, że zatajenie istotnych danych lub świadome, niezgodne z prawdą przekazanie informacji mających znaczenie dla ochrony informacji niejawnych przez osobę sprawdzaną jest podstawą do odmowy wydania jej poświadczenia bezpieczeństwa (art. 24 ust. 2 pkt 4 w związku z art. 30 ust. 1 ustawy).

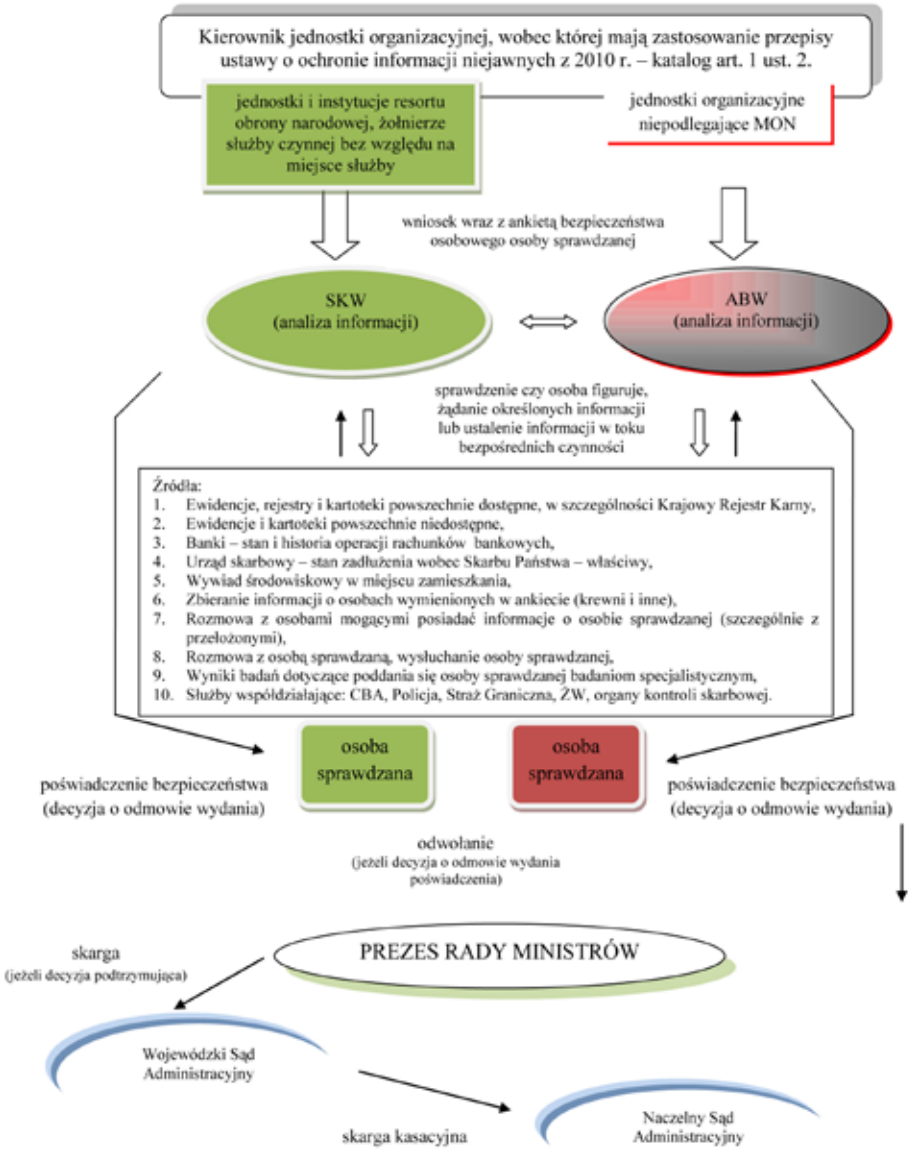
Jak wykazano powyżej, istnieje pewna niekonsekwencja ustawodawcy w odniesieniu do możliwości zastosowania art. 50 kpa przez podmioty prowadzące postępowania sprawdzające. Ponadto można sformułować pytanie, czym kierował się ustawodawca, uprawniając organ prowadzący postępowanie do korzystania z art. 50 kpa, jeżeli jednocześnie nie zobowiązał (w przepisach ustawy expressis verbis) osoby sprawdzanej do składania wyjaśnień, a jedynie uprawnił ją do ustosunkowania się do stwierdzonych przez organ wątpliwości. Jest to istotny brak regulacji, który powinien być uzupełniony w ewentualnej nowelizacji ustawy.

Uproszczony algorytm poszerzonego postępowania sprawdzającego z uwzględnieniem istotnych uprawnień jego uczestników przedstawia zamieszczony na końcu artykułu schemat.

4. Podsumowanie

W zakończeniu należy stwierdzić, że strona postępowania sprawdzającego prowadzonego na podstawie ustawy o ochronie informacji niejawnych ma ograniczone gwarancje procesowe w odniesieniu do gwarancji stanowionych kodeksem postępowania administracyjnego. Przyznane prawa pozwalają osobie sprawdzanej biernie śledzić przebieg prowadzonego wobec niej postępowania sprawdzającego, ponieważ nie ma ona inicjatywy dowodowej, a jedynie prawo do trybu odwoławczego i skargowego od wydanej decyzji rozstrzygającej. Ponadto, jak wykazano powyżej, niektóre

przepisy ustawy wymagają rozszerzenia lub uszczegółowienia, ponieważ nie są spójne z regulacjami kodeksowymi mającymi zastosowanie w toku postępowania sprawdzającego.



Schemat. Uproszczony model zakresu czynności realizowanych przez poszczególne podmioty partycypujące w postępowaniu sprawdzającym przed wydaniem poświadczenia bezpieczeństwa, stan prawny – 2016 r.

Źródło: Opracowanie własne.

Bibliografia:

Publikacje zwarte:

1. Adamiak B., Borkowski J., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2006, C.H. Beck.
2. Bojanowski E., Cieślak Z., Lang J., *Postępowanie administracyjne i postępowanie przed sądami administracyjnymi*, Warszawa 2008, LexisNexis.
3. Borowicz J., *Przetwarzanie informacji niejawnych w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne" 2011, nr 11.
4. Chrościelewski W., Tarno J.P., *Postępowanie administracyjne: kompendium dla urzędników i studentów administracji*, Zielona Góra 1999, Zachodnie Centrum Organizacji.
5. Hoc S., *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010, LexisNexis.
6. Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2011, LexisNexis.
7. Topolewski S., Żarkowski P., *Ochrona informacji niejawnych i danych osobowych*, Siedlce 2014, Uniwersytet Humanistyczno-Przyrodniczy w Siedlcach.
8. Wierzbowski M., Lang J., *Prawo Administracyjne*, Warszawa 2001, LexisNexis.

Akty prawne:

1. *Decyzja nr 119/MON Ministra Obrony Narodowej z dnia 23 kwietnia 2012 r. w sprawie szczegółowych zasad oraz trybu prowadzenia i dokumentowania postępowań sprawdzających w resorcie obrony narodowej* (Dz.Urz. MON z 2012 r. poz. 148).
2. *Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego* (Dz.U. z 2010 r. Nr 258 poz. 1750).
3. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (tekst jednolity: Dz.U. z 2016 r. poz. 1167).
4. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137).
5. *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (tekst jednolity: Dz.U. z 2016 r. poz. 23).

Abstrakt

Niniejszy artykuł koncentruje się na zagadnieniach związanych z ustawowymi prawami i obowiązkami osoby będącej podmiotem postępowania sprawdzającego prowadzonego na podstawie ustawy o ochronie informacji niejawnych. Autor dodatkowo omawia pierwszeństwo stosowania przepisów oraz kryteria wyłonienia strony postępowania w rozumieniu kodeksu postępowania administracyjnego. Istotnym elementem publika-

cji jest wskazanie niewłaściwej redakcji poszczególnych przepisów przywołanej ustawy i luk prawnych, które powodują trudności w jej odpowiednim stosowaniu w aspekcie praw i obowiązków strony postępowania.

Syntetyczne przedstawienie gwarancji procesowych oraz obowiązków strony może stanowić dla osób występujących w takim charakterze poradnik dotyczący korzystania z przysługujących im praw i adekwatnego wypełnienia obowiązków w toku postępowania sprawdzającego.

Słowa kluczowe: prawa i obowiązki, dostęp do informacji niejawnych, poświadczenie bezpieczeństwa, postępowanie sprawdzające, odwołanie.

Abstract

The article focuses on issues associated with legal rights and obligations of a person being a subject to a verifying procedure, conducted on the basis of the Law on protection of classified data. Additionally, the author discusses priority of application of provisions of law and criteria for identifying a party in the meaning of Code of Administrative Procedure. Another vital part of the publication is indication of improper wording of particular provisions of the said Law and legal loopholes, which are the source of difficulties as regards rights and obligations of a party in the procedure when it comes to application of the Law.

Synthetic presentation of parties procedural guarantees and obligations can be useful to people acting in such positions, and as a guide regarding exercising their rights and adequately fulfilling their obligations in the course of a verifying procedure.

Keywords: rights and obligations, access to classified information, security clearance certificate, security clearance procedure, appeal.

Mirosław Dela

Obowiązki ewidencyjne i informacyjne koncesjonariusza w zakresie obrotu bronią i amunicją

Wiek XXI nie uwolnił ludzkości od konfliktów zbrojnych. Ostatnie lata pokazały, że nawet na pozór stabilna i bezpieczna Europa może spłynąć krwią. Bezpieczeństwo najwyraźniej nie idzie w parze z postępem cywilizacyjnym, rozwojem nauki i techniki oraz poprawą poziomu życia społeczeństw. W niespokojnych czasach rośnie popyt na broń, a zapotrzebowanie na nią zgłasza nie tylko armia. Powstają nowe kluby strzeleckie i organizacje paramilitarne popularyzujące sporty obronne.

Rynek broni w Polsce jest jednak znacznie mniejszy, niż w innych krajach, głównie za sprawą reglamentacji dostępności obywateli do broni. Daleko mu do wielkości rynków USA, Szwajcarii, Serbii, Cypru czy Skandynawii[1]. Według danych Ministerstwa Spraw Wewnętrznych w Polsce w latach 2003–2015 udzielono ogółem 1290 koncesji na działalność w zakresie obrotu specjalnego[2].

Obrót bronią i amunicją jest zbyt często kojarzony z działalnością przestępczą, przez co ciągle wywołuje negatywne skojarzenia. Niewątpliwie do cześci transakcji dochodzi na czarnym rynku, ale istnieje także rynek legalny, którego działanie jest ściśle regulowane przepisami prawa. Handel bronią i amunicją sam w sobie nie niesie zagrożenia bezpieczeństwa i porządku publicznego, pod warunkiem, że odbywa się z poszanowaniem obowiązującego prawa i pod nadzorem powołanych do tego służb. Organy państwa dysponują narzędziami do kontroli podmiotów operujących na rynku broni i amunicji. Podstawowym narzędziem jest możliwość wglądu do ewidencji obrotu. Prawo nakłada na koncesjonariuszy także obowiązek przekazywania organom informacji o dokonanych transakcjach.

Uwagę zwraca natomiast brak publikacji prawniczych na temat obowiązków ewidencyjnych i informacyjnych koncesjonariuszy prowadzących działalność w zakresie tzw. obrotu specjalnego. Dzieje się tak zapewne dlatego, że ta tematyka pozostaje w kręgu zainteresowań wąskiej grupy osób.

Regulacja ustawowa

Podstawowym aktem prawnym regulującym obrót specjalny jest *Ustawa z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym*[3], nazywana potocznie ustawą o obrocie specjalnym (dalej: u.o.s.). Jak wynika z samej nazwy ustawy, ma ona szeroki zakres regulacji, stąd też – na potrzeby niniejszego artykułu – istnieje konieczność zawężenia omawianej tematyki. W artykule zostaną przedstawione tylko obowiązki koncesjonariuszy związane z obrotem bronią i amunicją, pominięte zaś zostaną obowiązki związane

[1] Zob. https://en.wikipedia.org/wiki/Number_of_guns_per_capita_by_country [dostęp: 14 VII 2015].

[2] Dane otrzymane z MSW, Wydział ds. Obrotu Specjalnego, Departament Zezwoleń i Koncesji – stan na 30 VI 2015 r.

[3] Tekst jednolity: Dz.U. z 2012 r. poz. 1017, ze zm.

z pozostałym zakresem przedmiotowym ustawy, tj. z wytwarzaniem broni i amunicji oraz wytwarzaniem materiałów wybuchowych i technologii o przeznaczeniu wojskowym i policyjnym, a także obrotem nimi.

Zgodnie z art. 6 ust. 1 pkt 1 u.o.s. wykonywanie działalności gospodarczej w zakresie obrotu bronią i amunicją wymaga uzyskania koncesji udzielanej w drodze decyzji przez organ koncesyjny, którym zgodnie z art. 7 ust. 1 u.o.s. jest minister właściwy do spraw wewnętrznych. Od tej zasady są jednak wyjątki. W art. 6 ust. 2 pkt 2 i 3 u.o.s. spod działalności koncesjonowanej wyłączono niektóre rodzaje broni. Należy jednak podkreślić, że działalnością koncesjonowaną jest także sprzedaż tych rodzajów broni, na których posiadanie nie wymaga się od nabywcy pozwolenia. Szczegółowy wykaz broni i amunicji, którymi obrót wymaga koncesji, określa *Rozporządzenie Rady Ministrów z dnia 3 grudnia 2001 r. w sprawie rodzajów broni i amunicji oraz wykazu wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub obrót jest wymagana koncesja*[4].

Definicje legalne

Przed omówieniem obowiązków ewidencyjnych i informacyjnych warto przyjrzeć się kilku definicjom legalnym zawartym w ustawowym słowniku, mającym istotne znaczenie z punktu widzenia omawianych zagadnień. Zgodnie z art. 3 ust. 1 pkt 2 u.o.s. pojęcie o b r o t u należy rozumieć szeroko, nie tylko jako działalność stricte handlową polegającą na sprzedaży i nabywaniu, lecz także jako pośrednictwo polegające na negocjowaniu, doradztwie handlowym, pomocy w zawieraniu umów oraz organizowaniu przemieszczania[5] broni i amunicji, jeśli ta działalność jest wykonywana na terytorium Rzeczpospolitej Polskiej. Widać więc wyraźnie, że zamiarem ustawodawcy było objęcie kontrolą nie tylko samego obrotu, lecz także czynności poprzedzających zawarcie umowy sprzedaży[6]. Ma to swoje uzasadnienie w znaczeniu obrotu specjalnego dla porządku i bezpieczeństwa państwa. Łatwiej jest reagować na nieprawidłowości *ex ante*, gdy transakcja jest dopiero przygotowywana, niż *ex post,* gdy już doszło do jej zrealizowania. Jednak – jak wykazano w szczegółowej analizie przepisów – organy powołane do kontroli otrzymują informacje wyłącznie po dokonaniu transakcji. Wyjątkiem jest obrót międzynarodowy, który wymaga uprzedniego poinformowania organu o zamierzonym przemieszczaniu broni pomiędzy krajami Unii Europejskiej[7]. Jest to swego rodzaju obowiązek informacyjny nałożony na koncesjonariusza, dzięki któremu organ państwa pozyskuje wiedzę o transakcji, zanim przesyłka trafi do rąk odbiorcy.

[4] Dz.U. z 2001 r. Nr 145 poz. 1625.

[5] Organizowanie przemieszczania nie dotyczy usług świadczonych przez spedytorów.

[6] Nie tylko handel, lecz także kojarzenie osób chcących zbyć lub nabyć broń czy amunicję i doradzanie im bez posiadania koncesji jest przestępstwem, ale tylko wówczas, gdy jest dokonywane w ramach prowadzonej działalności gospodarczej (art. 36 ust. 1 i 2 u.o.s.). Wysokie zagrożenie ustawowym wymiarem kary ma swoje uzasadnienie w dużej szkodliwości społecznej czynu.

[7] Zob. definicje pojęć z g o d a p r z e w o z o w a i u p r z e d n i a z g o d a p r z e w o z o w a w art. 3 ust. 2 pkt 6 i 8 u.o.s. Kwestie związane z obrotem bronią i amunicją w krajach UE zostały uregulowane w *Dyrektywie Rady 91/477/EWG z dnia 18 czerwca 1991 r. w sprawie kontroli nabywania i posiadania broni* (Dz.Urz. WE L 256 z 13 IX 1991 r. poz. 51) zmienionej *Dyrektywą Parlamentu Europejskiego i Rady 2008/51/WE z dnia 21 maja 2008 r. zmieniającą dyrektywę Rady 91/477/EWG w sprawie kontroli nabywania i posiadania broni* (Dz.Urz. UE L 179 z 8 VII 2008 r. poz. 5). Wdrożenie tej dyrektywy nastąpiło *Ustawą z dnia 23 czerwca 2006 r. o zmianie niektórych ustaw w związku z członkostwem Rzeczypospolitej Polskiej w Unii Europejskie*j (Dz.U. z 2006 r. Nr 133 poz. 935), która dodała do u.o.s. rozdział 5a. Ten rozdział reguluje przemieszczanie przez przedsiębiorców broni palnej na terenie UE.

Na uwagę zasługuje także szerokie zdefiniowanie broni i amunicji. Przepis art. 3 ust. 2 pkt 2 u.o.s. definiuje pojęcie broni i jej istotnych części przez odesłanie do przepisów *Ustawy z dnia 21 maja 1999 r. o broni i amunicji*[8] (dalej: u.b.a.), rozszerzając jednocześnie tę definicję o inne urządzenia służące do niszczenia lub obezwładniania celów[9].

Ustawa o obrocie specjalnym zawiera własną definicję amunicji i nie odsyła w tym zakresie do przepisów ustawy o broni i amunicji. W art. 3 ust. 2 pkt 3 u.o.s. zdefiniowano amunicję jako (…) *wyroby wypełnione materiałem wybuchowym, przeznaczone do miotania przy użyciu broni palnej, służące do niszczenia lub obezwładniania celów, a także dla celów ćwiczebnych*. Z kolei w art. 3 ust. 2 pkt 3a u.o.s. zdefiniowano pojęcie istotnych części amunicji rozumiane jako pociski wypełnione materiałami wybuchowymi, chemicznymi środkami obezwładniającymi lub zapalającymi albo innymi substancjami, których działanie zagraża życiu lub zdrowiu, a także spłonki inicjujące spalanie materiału miotającego i materiał miotający w postaci prochu strzelniczego.

Ustawowy obowiązek ewidencyjny i informacyjny

Ustawa o obrocie specjalnym w sposób bardzo ogólnikowy nakłada na koncesjonariuszy obowiązki w zakresie ewidencjonowania obrotu bronią i amunicją. W myśl przepisów ustawy ewidencjonowaniu podlegają broń, amunicja oraz istotne części broni i amunicji przeznaczone do obrotu (art. 29 ust. 1 u.o.s.). Przedsiębiorca będący stroną czynności prawnej mającej za przedmiot obrót bronią i amunicją jest obowiązany do prowadzenia ewidencji zawartych transakcji (art. 29 ust. 2 u.o.s.). Szczegółowych wytycznych na temat sposobu prowadzenia ewidencji należy poszukiwać w aktach wykonawczych.

Oprócz obowiązków ewidencyjnych ustawa równie ogólnikowo nakłada na przedsiębiorcę sprzedającego broń i amunicję obowiązek poinformowania organu, który wydał dokument uprawniający do zakupu, o każdej dokonanej transakcji (art. 30 ust. 3 u.o.s.). Ponadto zgodnie z art. 15 ust. 1 pkt 5 u.o.s. przedsiębiorca, który uzyskał koncesję na wykonywanie działalności gospodarczej w zakresie obrotu bronią i amunicją, jest obowiązany do przekazania prowadzonej ewidencji po zakończeniu działalności gospodarczej ministrowi właściwemu do spraw gospodarki, który ją przechowuje nie krócej niż 20 lat.

Realizacja obowiązków ewidencyjnych i informacyjnych niewątpliwie wymaga wiedzy dotyczącej aktualnych przepisów, którą przyszły koncesjonariusz powinien zdobyć podczas obligatoryjnego szkolenia specjalistycznego. Do przeprowadzania takich szkoleń jest upoważnionych zaledwie siedem instytucji w Polsce. Zgodnie z § 5 ust. 2 pkt 6 *Rozporządzenia Ministra Gospodarki z dnia 25 września 2002 r. w sprawie szkolenia potwierdzającego przygotowanie zawodowe do wykonywania lub kierowania działalnością gospodarczą w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją i wyrobami o przeznaczeniu wojskowym lub policyjnym oraz obrotu technologią o tym przeznaczeniu*[10] program szkolenia obejmuje m.in. zagadnienia związane z zasadami prowadzenia ewidencji oraz rodzajem dokumentacji ewidencyjnej i przepisami z tym związanymi. Przepis art. 8 ust. 1 pkt 1 lit. d u.o.s. zobowiązuje

[8] Tekst jednolity: Dz.U. z 2012 r. poz. 576, ze zm. Zob. definicje broni oraz istotnych części broni zawarte w art. 4 ust. 1 i art. 5 ust. 2 u.b.a.

[9] Ta rozszerzona definicja wprowadza nieco zamieszania terminologicznego, przyjęło się bowiem, że bronią jest tylko to, o czym mowa w art. 4 ust. 1 u.b.a.

[10] Dz.U. z 2002 r. Nr 173 poz. 1415, ze zm.

przedsiębiorcę prowadzącego jednoosobową działalność gospodarczą, który ubiega się o koncesję, do odbycia takiego szkolenia. Od przedsiębiorcy innego niż osoba fizyczna, zgodnie z art. 8 ust. 1 pkt 2 u.o.s., wymaga się natomiast, aby przygotowanie zawodowe miały co najmniej dwie osoby będące członkami organu zarządzającego przedsiębiorstwem albo członek tego organu i prokurent lub pełnomocnik ustanowiony przez ten organ do kierowania działalnością określoną w koncesji. Takie zróżnicowanie świadczy o nierównym traktowaniu przedsiębiorców[11].

Trzeba wspomnieć także o innych obowiązkach informacyjnych ciążących na koncesjonariuszu. Jest on zobowiązany do zawiadomienia organu koncesyjnego o podjęciu działalności gospodarczej w terminie 14 dni od dnia jej podjęcia, a także o jej zaprzestaniu, przy czym w tym drugim przypadku ustawa nie określa terminu (art. 15 ust. 1 pkt 2 u.o.s.). Ponadto koncesjonariusz jest obowiązany do zawiadomienia organu koncesyjnego o zmianach stanu prawnego i faktycznego w zakresie danych zawartych we wniosku o wydanie koncesji i w dokumentach stanowiących załączniki do tego wniosku, jeśli takie zmiany powstały po wydaniu koncesji. Ten obowiązek powinien zostać wykonany w terminie 14 dni od powstania zmian (art. 15 ust. 1 pkt 3 u.o.s.). Za niedopełnienie tego typu obowiązków w art. 38 ust. 1 u.o.s. przewidziano grzywnę, karę ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Akty wykonawcze do ustawy

Na podstawie delegacji ustawowych zawartych w art. 15a, 29 ust. 3 i 30 ust. 5 u.o.s. wydano trzy rozporządzenia zawierające przepisy dotyczące ewidencjonowania obrotu bronią i amunicją oraz przekazywania informacji właściwym organom.

Wykonywanie obowiązków informacyjnych

Na podstawie art. 30 ust. 5 u.o.s. zostało wydane *Rozporządzenie Ministra Gospodarki i Ministra Spraw Wewnętrznych z dnia 6 marca 2013 r. w sprawie sprzedaży materiałów wybuchowych, broni, amunicji, wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym oraz kontroli przestrzegania warunków sprzedaży*[12] (dalej: rozp. sprz.). To rozporządzenie określa m.in. tryb, formę i zakres przekazywania przez przedsiębiorców informacji o dokonanej transakcji mającej za przedmiot broń lub amunicję[13], a także szczegółowe zasady i sposób dokumentowania odstrzelenia nabojów z broni wprowadzanej do obrotu.

Zgodnie z § 3 ust. 1 pkt 1–3 rozp. sprz. przedsiębiorca, który sprzedał broń lub istotne części broni[14], w terminie pięciu dni od dnia sprzedaży przekazuje informację

[11] Nie ma żadnego uzasadnienia, aby od spółek prawa handlowego wymagać zwiększonego stanu kadrowego i ponoszenia związanych z tym kosztów. Wątpliwe jest poszukiwanie uzasadnienia w skali prowadzonej działalności gospodarczej. Działalność jednoosobowa częstokroć jest prowadzona na porównywalną, a nawet większą skalę niż działalność spółek. *De lege ferenda* przepis ten jako przejaw dyskryminacji powinien ulec derogacji podczas najbliższej nowelizacji ustawy.

[12] Dz.U. z 2013 r. poz. 343.

[13] Dotyczy to także transakcji zawieranych za pośrednictwem sieci teleinformatycznej (art. 30 ust. 4 u.o.s.).

[14] Przepis nie dotyczy przedsiębiorcy, który sprzedał broń, o której mowa w art. 11 pkt 7–11 u.b.a., tj. przedmioty przeznaczone do obezwładniania osób za pomocą energii elektrycznej o średniej wartości prądu w obwodzie nieprzekraczającej 10 mA, ręczne miotacze gazu obezwładniającego, broń pneumatyczna, broń palna rozdzielnego ładowania wytworzona przed 1885 r. i repliki tej broni oraz broń palna alarmowa o kalibrze do 6 mm.

w formie pisemnej właściwemu organowi, który wydał zaświadczenie uprawniające go do nabycia broni lub jej istotnych części. Przepisy rozporządzenia dzielą nabywców na trzy grupy, a dla każdej grupy właściwy do przyjęcia informacji jest inny organ. Dla zobrazowania tej procedury w pewnym uproszczeniu można stwierdzić, że jeśli nabywcami są osoby fizyczne, przedsiębiorcy lub cudzoziemcy[15], organem właściwym do odbioru informacji jest Policja lub organ wojskowy, który wydał zaświadczenie uprawniające do nabycia określonego rodzaju oraz liczby egzemplarzy broni lub jej istotnych części. Jeśli nabywcą jest przedsiębiorca przedkładający koncesję[16], informacja powinna trafić do wystawcy wspomnianego dokumentu za pośrednictwem organu Policji właściwego ze względu na miejsce wykonywania działalności gospodarczej przez nabywcę. Jeśli zaś nabywcami są szeroko rozumiane służby mundurowe i agencje ochrony[17], przepis wskazuje tylko na to, że informację otrzymuje organ, który wydał dokument uprawniający do nabycia broni lub jej istotnych części. Stosownie do § 3 ust. 2 rozp. sprz. do wyżej wymienionych informacji dołącza się łuski odstrzelonych nabojów[18] wraz z protokołem ich odstrzału[19].

Zgodnie z § 3 ust. 5 rozp. sprz. w przypadku sprzedaży broni lub jej istotnych części nabywcom określonym w art. 30 ust. 2 pkt 2 lit. c i f u.o.s.[20] dopuszcza się możliwość przekazywania informacji za pośrednictwem środków komunikacji elektronicznej, po opatrzeniu jej bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem potwierdzonym profilem zaufanym ePUAP[21]. Widać, że możliwość składania informacji w formie elektronicznej została ograniczona do wąskiej grupy nabywców, tj. niektórych przedsiębiorców i wybranych formacji mundurowych. Należy postulować rozszerzenie stosowania tej formy przekazywania danych w odniesieniu do transakcji dokonywanych na rzecz wszystkich kategorii nabywców, a nie tylko niektórych.

---

[15] Ściślej: podmioty określone w art. 30 ust. 2 pkt 2 lit. a i b u.o.s., tj. osoby fizyczne, przedsiębiorcy oraz inne podmioty, które przedłożą zaświadczenie wydane odpowiednio przez właściwy organ Policji lub organ wojskowy, uprawniające do nabycia określonego rodzaju oraz liczby egzemplarzy broni, a także cudzoziemcy na warunkach określonych w ustawie o broni i amunicji.

[16] Ściślej: podmioty określone w art. 30 ust. 2 pkt 2 lit. c–e u.o.s., tj. przedsiębiorcy, którzy przedłożą koncesję na wykonywanie działalności gospodarczej w zakresie obrotu bronią, wytwarzania broni – zgodnie z zakresem koncesji – oraz wytwarzania amunicji, w celu przeprowadzania prób rodzajów amunicji wytwarzanej na podstawie koncesji.

[17] Ściślej: podmioty określone w art. 30 ust. 2 pkt 2 lit. f–i u.o.s., tj. Siły Zbrojne RP, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Policja, Agencja Wywiadu, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Służba Celna, Służba Więzienna, Biuro Ochrony Rządu, po okazaniu dokumentu uprawniającego do nabycia wystawionego przez właściwy organ, a także Państwowa Straż Łowiecka, Straż Ochrony Kolei, Straż Leśna, Państwowa Straż Rybacka, straż gminna i miejska, Straż Marszałkowska, Straż Parkowa, kontrola skarbowa, Inspekcja Transportu Drogowego, na podstawie dokumentu wydanego przez uprawniony organ Policji, specjalistyczne uzbrojone formacje ochronne – uprawnione do posiadania broni na podstawie świadectwa broni, na podstawie zaświadczenia właściwego organu Policji uprawniającego do nabycia określonego rodzaju oraz ilości egzemplarzy broni – oraz inne podmioty, których dostęp do broni regulują odrębne przepisy, na warunkach w nich określonych.

[18] Nie dotyczy podmiotów, o których mowa w art. 30 ust. 2 pkt 2 lit. c i f u.o.s. Te podmioty wraz z zakupioną bronią otrzymują do każdego egzemplarza broni łuski odstrzelonych nabojów łącznie z protokołem ich odstrzału.

[19] Na temat zawartości protokołu odstrzału zob. § 6 ust. 2 pkt 1–3 rozp. sprz.

[20] Dotyczy przedsiębiorców, którzy przedłożą koncesję na wykonywanie działalności gospodarczej w zakresie obrotu bronią, a także Sił Zbrojnych RP, SKW, SWW, Policji, AW, ABW, CBA, SG, SC, SW i BOR. Ta możliwość nie dotyczy sprzedaży pozostałym kategoriom nabywców.

[21] Elektroniczna Platforma Usług Administracji Publicznej, zob. *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (tekst jednolity: Dz.U. z 2014 r. poz. 1114).

Obowiązek przekazywania informacji o sprzedaży amunicji oparto na podobnych zasadach, jak w przypadku sprzedaży broni. Widoczne są jednak różnice chociażby w zakresie terminów realizacji tego obowiązku. Nabywców amunicji także podzielono na trzy kategorie. W dużym uproszczeniu można stwierdzić, że przedsiębiorca, który sprzedał amunicję osobom fizycznym, przedsiębiorcom lub cudzoziemcom[22], przekazuje co kwartał informację o jej sprzedaży – w formie pisemnej lub za pośrednictwem środków komunikacji elektronicznej – organowi Policji lub organowi wojskowemu, który wydał dokument uprawniający do nabycia amunicji (§ 4 ust. 1 pkt 1 rozp. sprz.). W przypadku gdy sprzedaż amunicji nastąpiła na rzecz przedsiębiorców posiadających koncesję[23], przedsiębiorca przekazuje co kwartał informację o jej sprzedaży – w formie pisemnej lub za pośrednictwem środków komunikacji elektronicznej – organowi, który wydał dokument uprawniający do nabycia amunicji, ale dokonuje tego za pośrednictwem organu Policji właściwego ze względu na miejsce wykonywania działalności gospodarczej przez tego przedsiębiorcę (§ 4 ust. 1 pkt 2 rozp. sprz.). Jeśli nabywcą są szeroko rozumiane służby mundurowe i agencje ochrony[24], to przedsiębiorca w terminie pięciu dni od dnia sprzedaży amunicji przekazuje informację o jej sprzedaży – w formie pisemnej lub za pośrednictwem środków komunikacji elektronicznej – organowi, który wydał dokument uprawniający do nabycia amunicji (§ 4 ust. 1 pkt 3 rozp. sprz.). Informacja przekazana za pośrednictwem środków komunikacji elektronicznej powinna być opatrzona bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu albo podpisem potwierdzonym profilem zaufanym ePUAP (§ 4 ust. 4 rozp. sprz.). Łatwo zauważyć, że w przypadku obrotu amunicją przekaz informacji może się odbywać w formie elektronicznej, bez względu na kategorię nabywcy. Tym bardziej może dziwić wspomniane wyżej ograniczenie dotyczące przekazywania informacji drogą elektroniczną w przypadku obrotu bronią.

Rozporządzenie nakłada także na przedsiębiorcę wprowadzającego broń palną do obrotu obowiązek odpowiedniego dokumentowania odstrzelenia nabojów[25]. Z tej czynności przedsiębiorca sporządza protokół zawierający oznaczenie daty i miejsca odstrzału, rodzaju, nazwy, marki, kalibru, serii, numeru i roku produkcji broni palnej, jej producenta oraz kraju lub miejsca jej wytworzenia. Protokół powinien zawierać również

[22] Ściślej: podmioty określone w art. 30 ust. 2 pkt 3 lit. a i b u.o.s., tj. osoby fizyczne, przedsiębiorcy oraz inne podmioty na podstawie legitymacji posiadacza broni lub świadectwa broni albo zaświadczenia wydanego odpowiednio przez właściwy organ Policji lub organ wojskowy, uprawniającego do nabycia określonego rodzaju oraz liczby egzemplarzy broni wraz z amunicją do tej broni, a także cudzoziemcy – na warunkach określonych w ustawie o broni i amunicji.

[23] Ściślej: podmioty określone w art. 30 ust. 2 pkt 3 lit. c i d u.o.s., tj. przedsiębiorcy, którzy przedłożą koncesję na wykonywanie działalności gospodarczej w zakresie obrotu amunicją, a także przedsiębiorcy, którzy przedłożą koncesję na wykonywanie działalności gospodarczej w zakresie obrotu bronią oraz dokument potwierdzający nabycie broni – w ilości niezbędnej do odstrzelenia trzech nabojów z każdej lufy egzemplarza broni palnej przeznaczonej do sprzedaży.

[24] Ściślej: podmioty określone w art. 30 ust. 2 pkt 3 lit. e–h u.o.s., tj. Siły Zbrojne RP, SKW, SWW, Policja, AW, ABW, CBA, SG, SC, SW i BOR, po okazaniu dokumentu uprawniającego do nabycia amunicji, wystawionego przez właściwy organ, a także Państwowa Straż Łowiecka, Straż Ochrony Kolei, Straż Leśna, Państwowa Straż Rybacka, straż gminna i miejska, Straż Marszałkowska, Straż Parkowa, kontrola skarbowa oraz Inspekcja Transportu Drogowego – na podstawie dokumentu wydanego przez uprawniony organ Policji, specjalistyczne uzbrojone formacje ochronne – na podstawie pisemnej zgody właściwego komendanta wojewódzkiego Policji, w celu szkolenia strzeleckiego, a także inne podmioty, których dostęp do amunicji regulują odrębne przepisy na warunkach w nich określonych.

[25] Ten obowiązek nie dotyczy broni, o której mowa w art. 11 pkt 10 i 11 u.b.a., tj. broni palnej rozdzielnego ładowania wytworzonej przed 1885 r. oraz jej replik, a także broni palnej alarmowej o kalibrze do 6 mm.

dodatkowe oznaczenia fabryczne stosowane przez producenta lub szczegółowy opis broni palnej, o ile są stosowane, a także podpisy przedsiębiorcy i funkcjonariusza Policji, w którego obecności dokonano odstrzelenia nabojów (§ 6 ust. 2 rozp. sprz.).

Zgodnie z § 9 ust. 1 rozp. sprz. przedsiębiorca, który sprzedał broń, o której mowa w art. 11 pkt 7–11 u.b.a.[26], przekazuje co kwartał w formie pisemnej lub za pośrednictwem środków komunikacji elektronicznej informację o ilości sprzedanej broni organowi Policji właściwemu ze względu na miejsce wykonywania działalności gospodarczej. Informacja przekazana za pośrednictwem środków komunikacji elektronicznej powinna być opatrzona bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu albo podpisem potwierdzonym profilem zaufanym ePUAP (§ 9 ust. 3 rozp. sprz.). W tym przypadku przepis rozporządzenia także nie wprowadza ograniczeń w stosowaniu elektronicznej drogi przekazu informacji.

Rozporządzenie zawiera też załączniki w postaci wzorów dokumentów, które przedsiębiorca powinien dostarczyć organowi. Załącznik nr 2 stanowi wzór informacji o sprzedaży broni lub jej istotnych części[27], załącznik nr 3 – wzór informacji o sprzedaży amunicji podmiotom, o których mowa w art. 30 ust. 2 pkt 3 lit. a i b u.o.s.[28], załącznik nr 4 – wzór informacji o sprzedaży amunicji podmiotom, o których mowa w art. 30 ust. 2 pkt 3 lit. c–h u.o.s.[29], w załączniku nr 6 natomiast określono wzór informacji o ilości sprzedanej broni, o której mowa w art. 11 pkt 7–11 u.b.a.[30]

Prowadzenie ewidencji

Spełnienie obowiązków informacyjnych nie byłoby możliwe bez prowadzenia ścisłej ewidencji obrotu. Aktem rangi podstawowej, wydanym na podstawie art. 29 ust. 3 u.o.s., regulującym zasady prowadzenia ewidencji w zakresie obrotu bronią i amunicją, jest *Rozporządzenie Ministra Gospodarki z dnia 22 sierpnia 2012 r. w sprawie sposobu ewi-*

[26] Zob. rodzaje broni wymienione w przypisie nr 14.

[27] Dotyczy wszystkich kategorii nabywców. Informacja zawiera następujące dane: miejscowość i datę sporządzenia, oznaczenie przedsiębiorcy, numer koncesji, adresata informacji, datę sprzedaży, oznaczenie nabywcy (w tym NIP albo PESEL, albo nazwę, serię i numer dokumentu tożsamości oraz adres), nazwę, numer i datę wydania dokumentu uprawniającego do zakupu broni i jego wystawcę oraz imię i nazwisko przedsiębiorcy dokonującego sprzedaży. W załączeniu powinien się znaleźć tabelaryczny wykaz sprzedanej broni lub jej istotnych części (oddzielnie dla każdego typu broni). Tabela zawiera nazwę wytwórcy, kraj lub miejsce wytworzenia, rodzaj broni lub jej istotnej części, markę, typ (model) broni, kaliber, numer seryjny i rok wytworzenia. Dołącza się również protokoły odstrzału i łuski.

[28] Dotyczy podmiotów wymienionych w przypisie nr 22. Informacja zawiera: miejscowość i datę sporządzenia, oznaczenie przedsiębiorcy, numer koncesji, adresata informacji, datę sprzedaży (kwartał i rok), miejsce sprzedaży oraz zestawienie tabelaryczne, a w nim rodzaj, nazwę, kaliber amunicji i jej ilość oraz imię i nazwisko przedsiębiorcy dokonującego sprzedaży.

[29] Dotyczy podmiotów wymienionych w przypisach nr 23 i 24. Informacja zawiera: miejscowość i datę sporządzenia, oznaczenie przedsiębiorcy, numer koncesji, adresata informacji, datę sprzedaży (kwartał i rok), miejsce sprzedaży oraz zestawienie tabelaryczne zawierające rodzaj, nazwę, kaliber amunicji, nazwę wytwórcy, numer partii amunicji i jej ilość, a ponadto oznaczenie nabywcy (w tym NIP albo PESEL, albo nazwę, serię i numer dokumentu tożsamości, adres), nazwę, numer i datę wydania dokumentu uprawniającego do zakupu amunicji i jego wystawcę oraz imię i nazwisko przedsiębiorcy dokonującego sprzedaży.

[30] Dotyczy wszystkich kategorii nabywców broni wymienionej w przypisie nr 14. Informacja zawiera: miejscowość i datę sporządzenia, oznaczenie przedsiębiorcy, numer koncesji, adresata informacji, a także wskazanie, za jaki okres jest sporządzona informacja, oraz imię i nazwisko osoby sporządzającej z podaniem jej stanowiska zajmowanego u przedsiębiorcy. Ponadto informacja zawiera w postaci tabeli: liczbę sprzedanej broni w sztukach i jej rodzaj z podziałem na poszczególne rodzaje wymienione w przypisie nr 14.

dencjonowania wprowadzonych do obrotu materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym[31] (dalej: rozp. ewid.). Na potrzeby tego rozporządzenia posłużono się ogólnym pojęciem m a t e r i a ł y, przez co rozumie się nie tylko – jak mogłoby się wydawać – materiały wybuchowe, lecz także broń i amunicję oraz istotne części broni i amunicji (§ 2 pkt 1 rozp. ewid.).

Zgodnie z § 3 ust. 1 rozp. ewid. zarówno ewidencję materiałów przeznaczonych do obrotu, jak i ewidencję zawartych transakcji prowadzi się w formie księgi ewidencyjnej zawierającej karty ponumerowane, przesznurowane i opieczętowane przez przedsiębiorcę, w sposób zapewniający bieżącą kontrolę stanu posiadania materiałów przeznaczonych do obrotu oraz pełną rejestrację transakcji zawartych przez przedsiębiorcę. Przepis § 3 ust. 2 rozp. ewid. dopuszcza, aby księga ewidencyjna była prowadzona z wykorzystaniem elektronicznych metod przetwarzania informacji, pod warunkiem zastosowania rozwiązań systemowych umożliwiających rejestrację i przechowywanie wszystkich operacji wraz z kopią zapasową oraz pozwalających na ich weryfikację na podstawie dokumentów przechowywanych przez przedsiębiorcę.

Przepis § 3 ust. 3 rozp. ewid. nakłada na koncesjonariusza obowiązek ochrony danych zawartych w księdze ewidencyjnej przed ich przypadkowym lub celowym uszkodzeniem lub zniszczeniem, kradzieżą, zmianą lub dostępem do nich osób nieuprawnionych, w tym również za pomocą złośliwego oprogramowania. Ewidencję broni przeznaczonej do obrotu, jej istotnych części oraz ewidencję zawartych transakcji dotyczących obrotu bronią prowadzi się odrębnie dla każdego rodzaju broni, w sposób pozwalający na jej identyfikację ze względu na nazwę, markę, kaliber, serię i numer fabryczny, rok produkcji, kraj producenta i nazwę wytwórcy (§ 4 ust. 2 rozp. ewid.). Z kolei ewidencję amunicji i jej istotnych części przeznaczonych do obrotu oraz ewidencję zawartych transakcji dotyczących obrotu amunicją prowadzi się odrębnie dla każdego rodzaju, marki i kalibru (§ 4 ust. 3 rozp. ewid.).

Przepis § 4 ust. 5 rozp. ewid. wskazuje, w jakich jednostkach miary należy ewidencjonować materiały przeznaczone do obrotu, w zależności od ich rodzaju oraz typu. W przypadku broni i amunicji tą jednostką będą sztuki. Transakcje ewidencjonuje się według ich przedmiotu (§ 4 ust. 6 rozp. ewid.).

Przepisy omawianego rozporządzenia zawierają dokładne wytyczne co do zawartości ewidencji. Dokumentacja związana z ewidencją materiałów przeznaczonych do obrotu składa się z księgi ewidencyjnej, dokumentu przychodu albo rozchodu, dokumentu przekazania materiału między komórkami organizacyjnymi przedsiębiorcy oraz dokumentu zużycia materiału, o ile jego zużycia wymaga wykonywana działalność gospodarcza (§ 5 ust. 1 rozp. ewid.). Dokumentację związaną z ewidencją zawartych transakcji stanowi księga ewidencyjna (§ 5 ust. 2 rozp. ewid.). Wpisu w księdze dokonuje sam przedsiębiorca albo osoby posiadające jego pisemne upoważnienie (§ 6 rozp. ewid.). Podstawą dokonania wpisu w księdze ewidencyjnej materiałów przeznaczonych do obrotu jest dokument przychodu albo rozchodu, dokument przekazania materiału między komórkami organizacyjnymi przedsiębiorcy oraz dokument zużycia materiału (§ 7 ust. 1 rozp. ewid.), podstawą zaś dokonania wpisu w księdze ewidencyjnej zawartych transakcji jest wyłącznie dokument przychodu albo rozchodu (§ 7 ust. 2 rozp. ewid.). Wpisu w księdze ewidencyjnej dokonuje się w sposób trwały i czytelny. Nie może być on wymazywany ani w inny

[31] Dz.U. z 2012 r. poz. 1008.

sposób usuwany. Zmian w księdze ewidencyjnej dokonuje się kolorem czerwonym, w sposób czytelny, z podaniem daty i podpisem osoby, która dokonuje tej zmiany (§ 7 ust. 4–6 rozp. ewid.).

Zgodnie z § 8 ust. 1 rozp. ewid. księga ewidencyjna materiałów przeznaczonych do obrotu[32] zawiera: numer i datę jej założenia, nazwę handlową, indeks, symbol oraz inne oznaczenia identyfikujące materiał, prawidłową nazwę przewozową, kod klasyfikacyjny i numer rozpoznawczy UN, jeśli są one wymagane odrębnymi przepisami[33], datę i kolejny numer wpisu do księgi ewidencyjnej operacji przychodu albo rozchodu materiału, jednostkę miary, numer i datę dokumentu przychodu, oznaczenie dostawcy ze wskazaniem dokumentu uprawniającego do obrotu, ilość przyjętego materiału lub (w przypadku obrotu jednostkowego wyrobami oznaczonymi numerem indywidualnym) zapis identyfikujący ten wyrób, numer i datę dokumentu rozchodu, dokumentu przekazania materiału między komórkami organizacyjnymi przedsiębiorcy lub dokumentu zużycia materiału, oznaczenie odbiorcy, oznaczenie dokumentu uprawniającego do zakupu, ilość wydanego materiału lub (w przypadku obrotu jednostkowego wyrobami oznaczonymi numerem indywidualnym) – zapis identyfikujący ten wyrób, stan magazynu po operacji przychodu lub rozchodu materiału, a także podpis osoby upoważnionej do prowadzenia ewidencji.

Zgodnie z § 9 rozp. ewid. dokument przychodu albo rozchodu powinien zawierać: numer i datę jego sporządzenia, oznaczenie przedsiębiorcy, który go sporządził, nazwę handlową, indeks, symbol oraz inne oznaczenia identyfikujące materiał, prawidłową nazwę przewozową, kod klasyfikacyjny i numer rozpoznawczy UN, jeśli są one wymagane odrębnymi przepisami[34], ilość przyjętego lub wydanego materiału i jednostkę miary, oznaczenie dostawcy lub nabywcy, numer i serię dowodu tożsamości osoby upoważnionej do odbioru materiału, datę przyjęcia lub wydania materiału, informację o posiadaniu koncesji na obrót materiałami przez przedsiębiorcę wystawiającego dokument rozchodu, a także nazwiska i podpisy osób: sporządzającej dokument, wydającej materiał i upoważnionej do odbioru materiału, przy czym np. sporządzający dokument może być jednocześnie wydającym materiał.

U przedsiębiorców prowadzących działalność na większą skalę często dokonuje się przekazania materiału między komórkami organizacyjnymi. Jak wynika z przepisów rozporządzenia, takie przekazanie także musi być udokumentowane. Zgodnie z § 10 rozp. ewid. dokument przekazania materiału między komórkami organizacyjnymi przedsiębiorcy powinien zawierać numer i datę jego sporządzenia, nazwę lub symbol komórki organizacyjnej przedsiębiorcy przekazującej i otrzymującej materiał, nazwę handlową, indeks, symbol oraz inne oznaczenia identyfikujące materiał, przekazaną ilość materiału i jednostkę miary oraz nazwiska i podpisy osób: sporządzającej dokument, wydającej materiał oraz upoważnionej do jego odbioru. Możliwe jest, aby we wszystkich trzech rolach występowała ta sama osoba, ponieważ przekazanie materiału odbywa się między komórkami organizacyjnymi u tego samego przedsiębiorcy[35].

---

[32] Nie dotyczy broni, o której mowa w art. 11 pkt 7, 8 i 11 ustawy o broni i amunicji, a więc przedmiotów przeznaczonych do obezwładniania osób za pomocą energii elektrycznej o średniej wartości prądu w obwodzie nieprzekraczającej 10 mA, ręcznych miotaczy gazu obezwładniającego oraz broni palnej alarmowej o kalibrze do 6 mm. Ewidencja tych materiałów jest prowadzona zgodnie z § 12 rozp. ewid.

[33] Zob. załącznik A do umowy europejskiej dotyczącej międzynarodowego przewozu drogowego towarów niebezpiecznych (*Oświadczenie Rządowe z dnia 23 marca 2011 r. w sprawie wejścia w życie zmian do załączników A i B „Umowy europejskiej dotyczącej międzynarodowego przewozu drogowego towarów niebezpiecznych (ADR), sporządzonej w Genewie dnia 30 września 1957 r.*", Dz.U. z 2011 r. Nr 110 poz. 641).

[34] Tamże.

[35] W praktyce trudno jednak wyobrazić sobie taką sytuację, gdyż dotyczy ona zazwyczaj przedsiębiorcy

Jak już wspomniano, przepisy przewidują możliwość zużycia materiału. Nie definiują jednak, czym jest z u ż y c i e. Wydaje się, że to pojęcie należy rozumieć bardzo szeroko, jako wszelkie zdarzenia zaistniałe w toku prowadzenia działalności, w wyniku których dochodzi do nieodwracalnego unicestwienia jednostki broni lub sztuki amunicji (np. zużycie amunicji w celu przeprowadzenia próby broni lub amunicji, niedająca się naprawić usterka, zniszczenie, kradzież i różne inne przypadki losowe). Zgodnie z § 11 rozp. ewid. dokument zużycia materiału zawiera: numer i datę jego sporządzenia, nazwę i symbol komórki organizacyjnej przedsiębiorcy, nazwę handlową, indeks, symbol oraz inne oznaczenia identyfikujące materiał, ilość zużytego materiału i jednostkę miary, cel zużycia, nazwiska i podpisy osób: sporządzającej dokument, dokonującej zużycia i potwierdzającej dokonanie zużycia materiału. Nic nie stoi na przeszkodzie, aby wszystkie trzy podpisy złożyła ta sama osoba (tak będzie zawsze u przedsiębiorcy jednoosobowego, który nie zatrudnia pracowników i samodzielnie wykonuje wszystkie trzy wyżej wymienione czynności).

Przepis § 12 ust. 1 rozp. ewid. stanowi, że ewidencję broni przeznaczonej do obrotu, o której mowa w art. 11 pkt 7, 8 i 11 u.b.a.[36], a także ewidencję zawartych transakcji dotyczących obrotu tą bronią prowadzi się w formie księgi ewidencyjnej zawierającej karty ponumerowane, przesznurowane i opieczętowane przez przedsiębiorcę[37]. Z kolei według § 12 ust. 2 rozp. ewid. taka księga zawiera: numer i datę jej założenia, rodzaj broni, liczbę egzemplarzy broni, datę i kolejny numer wpisu do księgi ewidencyjnej operacji przychodu albo rozchodu broni, informację o stanie magazynu po operacji przychodu albo rozchodu broni, a także podpis osoby upoważnionej do prowadzenia ewidencji.

Księga ewidencyjna zawartych transakcji dotyczących obrotu bronią i amunicją zawiera: numer i datę jej założenia, nazwę handlową, indeks, symbol oraz inne oznaczenia identyfikujące przedmiot transakcji, datę i kolejny numer wpisu, jednostkę miary i ilość przedmiotu transakcji, oznaczenie sprzedającego ze wskazaniem dokumentu uprawniającego do obrotu, oznaczenie kupującego ze wskazaniem dokumentu uprawniającego do zakupu, numer tego dokumentu oraz organ będący jego wystawcą (§ 13 rozp. ewid.).

Przedsiębiorca wykonujący działalność gospodarczą, zarówno w zakresie wytwarzania materiałów, jak i obrotu nimi, może prowadzić jedną dokumentację zawierającą wykaz materiałów wytworzonych i przeznaczonych do obrotu oraz ewidencję transakcji (§ 15 rozp. ewid.). Jest to wyraźne ułatwienie dla producentów będących jednocześnie sprzedawcami. Materiały wytworzone są zwykle materiałami przeznaczonymi do obrotu, przez co może dochodzić do zdublowania identycznych informacji.

Zgodnie z § 16 ust. 1 rozp. ewid. dokumentacja związana z ewidencją materiałów przeznaczonych do obrotu oraz ewidencją zawartych transakcji powinna być przechowywana w siedzibie przedsiębiorcy przez co najmniej 10 lat od daty dokonania ostatniego zapisu. Jednak w przypadku ewidencji przeznaczonej do obrotu broni palnej i jej istotnych części oraz w przypadku ewidencji zawartych transakcji dotyczących obrotu bronią palną okres przechowywania wynosi co najmniej 20 lat od daty ostatniego zapisu, o ile odrębne przepisy nie przewidują dłuższego okresu przechowywania. Ten przepis nie obowiązuje w razie zakończenia przez przedsiębiorcę działalności gospodarczej

działającego na większą skalę i posiadającego wydzielone komórki organizacyjne, a zatem zwykle zatrudniającego także personel do obsługi tych komórek.

[36] Zob. rodzaje broni wymienione w przypisie nr 32.

[37] Ten przepis stosuje się także do prowadzenia księgi ewidencyjnej przeznaczonej do obrotu amunicją do broni, o której mowa w art. 11 pkt 11 ustawy o broni i amunicji (tj. broni palnej alarmowej o kalibrze do 6 mm).

(§ 16 ust. 2 rozp. ewid.). Wówczas zastosowanie znajduje art. 15 ust. 1 pkt 5 u.o.s. zobowiązujący przedsiębiorcę do przekazania ewidencji ministrowi właściwemu do spraw gospodarki.

Przekazywanie ewidencji

Kolejnym aktem prawnym mającym związek z obowiązkami ewidencyjnymi koncesjonariusza jest *Rozporządzenie Ministra Gospodarki z dnia 18 lutego 2013 r. w sprawie trybu i szczegółowych warunków przekazywania ewidencji związanej z wykonywaniem działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym*[38] (dalej: rozp. przek.) wydane na podstawie art. 15a u.o.s. Precyzuje ono sposób wykonania obowiązku nałożonego w art. 15 ust. 1 pkt 5 u.o.s., szczególnie określając tryb i warunki przekazywania ewidencji przeznaczonej do obrotu bronią, amunicją oraz istotnymi częściami broni i amunicji, a także zawartych transakcji dotyczących obrotu bronią i amunicją (§ 1 pkt 2 i 3 rozp. przek.). Zgodnie z § 2 ust. 1 rozp. przek. ewidencję prowadzoną w formie księgi ewidencyjnej przekazuje się ministrowi właściwemu do spraw gospodarki przesyłką poleconą. Przesyłka składa się z ewidencji ułożonej w kolejności odpowiadającej liczbie porządkowej wskazanej w protokole przekazania ewidencji, który umieszcza się w przesyłce (§ 2 ust. 2 i 3 rozp. przek.). Przesyłkę oznakowuje się, umieszczając na niej nazwę i adres przedsiębiorcy, numer nadany przez przedsiębiorcę odpowiadający kolejności przekazywanych przesyłek (o ile przesyłek jest kilka), a także zabezpiecza się w sposób zapobiegający jej uszkodzeniu lub zniszczeniu (§ 2 ust. 4 pkt 1 i 2 rozp. przek.).

W przypadku stwierdzenia niezgodności protokołu przekazania ewidencji z zawartością przesyłki lub innych niezgodności z wymogami w zakresie trybu i szczegółowych warunków przekazywania ewidencji, przedsiębiorcę wzywa się w terminie siedmiu dni od dnia otrzymania przesyłki do niezwłocznego uzupełnienia ewidencji lub spełnienia pozostałych wymogów (§ 3 rozp. przek.).

Stosownie do § 4 ust. 1 rozp. przek. ewidencję prowadzoną z wykorzystaniem elektronicznych metod przetwarzania informacji przekazuje się w formie dokumentu elektronicznego przesyłką poleconą (z zastosowaniem przepisów § 2 i § 3 rozp. przek.) albo za pomocą środków komunikacji elektronicznej, na co pozwala § 4 ust. 3 rozp. przek. To drugie rozwiązanie wydaje się iść z duchem czasu. Ewidencję sporządzoną w obowiązującej formie (papierowej bądź elektronicznej) można przekazać także osobiście, składając ją w siedzibie ministerstwa obsługującego ministra właściwego do spraw gospodarki (§ 5 rozp. przek.). W tym przypadku także odpowiednio stosuje się omówione wyżej przepisy § 2 i 3 rozp. przek. dotyczące sposobu przekazania dokumentacji i przewidujące odpowiednią procedurę na wypadek stwierdzenia niezgodności.

Ewidencję uznaje się za przekazaną po przyjęciu jej przez ministra właściwego do spraw gospodarki, na podstawie protokołu przyjęcia ewidencji (§ 6 ust. 1 rozp. przek.). Protokół przyjęcia ewidencji sporządza się w dwóch jednobrzmiących egzemplarzach, z których jeden otrzymuje przedsiębiorca (§ 6 ust. 2 rozp. przek.). Ewidencję przekazuje się w terminie 30 dni od dnia zakończenia wykonywania działalności gospodarczej w zakresie obrotu bronią i amunicją (§ 7 ust. 1 rozp. przek.). Ten termin uważa się za za-

[38] Dz.U. z 2013 r. poz. 348.

chowany, jeżeli przesyłka została nadana przed jego upływem albo jeżeli w tym terminie została złożona osobiście w siedzibie ministerstwa obsługującego ministra właściwego do spraw gospodarki (§ 7 ust. 2 rozp. przek.).

Należy wspomnieć, że w przypadku uchybienia przez przedsiębiorcę terminu z przyczyn przez niego niezawinionych, przysługuje mu możliwość zwrócenia się z wnioskiem o przywrócenie terminu na podstawie art. 58 § 1 i 2 *Ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego*[39]. Ta możliwość dotyczy zresztą wszystkich terminów, o których mowa w analizowanych wyżej przepisach ustaw i rozporządzeń.

Omawiane rozporządzenie zawiera załączniki. Załącznik nr 1 zawiera wzór protokołu przekazania ewidencji przeznaczonych do obrotu bronią, amunicją, istotnymi częściami broni i amunicji, a także zawartych transakcji dotyczących obrotu bronią i amunicją[40]. Załącznik nr 2 zawiera wzór protokołu przyjęcia ewidencji przeznaczonych do obrotu bronią, amunicją, istotnymi częściami broni i amunicji, a także zawartych transakcji dotyczących obrotu bronią i amunicją[41].

Nieprzekazanie ewidencji ministrowi właściwemu do spraw gospodarki po zakończeniu działalności gospodarczej jest zagrożone grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat dwóch (art. 38 ust. 2 u.o.s.).

Zasygnalizowania wymaga jeszcze problem interpretacyjny. Termin na przekazanie dokumentacji jest liczony – jak wynika z § 7 ust. 1 rozp. przek. – od daty zakończenia wykonywania działalności w zakresie objętym koncesją. Trudno precyzyjnie określić, czy chodzi o faktyczne zaprzestanie prowadzenia działalności koncesjonowanej, czy o wykreślenie podmiotu z ewidencji działalności gospodarczej lub rejestru sądowego[42]. Działalność objęta koncesją może przecież być tylko fragmentem działalności gospodarczej danego przedsiębiorcy. Często jest tak, że zaprzestaje on prowadzenia działalności objętej koncesją, ale nadal wykonuje inne rodzaje działalności niekoncesjonowanej. Tym sposobem może on przez wiele lat figurować jako koncesjonariusz, nie wykonując faktycznie tej działalności, przez co baza danych organu koncesyjnego staje się nieaktualna. Gramatyczna wykładnia przepisu[43] uprawnia do stwierdzenia, że chodzi o zaprzestanie prowadzenia działalności polegającej na obrocie bronią i amunicją, nie zaś o zaprzestanie prowadzenia działalności w ogóle. Zaprzestanie to musi jednak mieć cha-

[39] Tekst jednolity: Dz.U. z 2016 r. poz. 23.

[40] Protokół zawiera: numer, nazwę przedsiębiorcy, miejscowość i datę sporządzenia, numer przesyłki (numer nadany przez przedsiębiorcę odpowiadający kolejności przekazywanych przesyłek), liczbę porządkową księgi zgodną z numerem będącym częścią obowiązkowego oznaczenia księgi ewidencyjnej, opis księgi ewidencyjnej i ewentualne uwagi oraz oświadczenie, że ewidencję prowadzoną z wykorzystaniem elektronicznych metod przetwarzania informacji przekazuje się na informatycznych nośnikach danych (z podaniem ilości nośników). Protokół obejmuje również zgodę wyrażoną na podstawie art. 39^1 § 1 pkt 2 kpa na doręczanie pism za pomocą środków komunikacji elektronicznej w rozumieniu przepisów *Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (tekst jednolity: Dz.U. z 2013 r. poz. 1422, ze zm.). Pod protokołem podpis składa przedsiębiorca.

[41] Protokół zawiera oznaczenie miejscowości i datę, nazwę i adres przedsiębiorcy przekazującego protokół oraz oświadczenie ministra o przyjęciu ewidencji wraz z protokołami przekazania ewidencji i podaniem ich liczby. Ewidencję prowadzoną z wykorzystaniem elektronicznych metod przetwarzania informacji przyjmuje się na informatycznych nośnikach danych z podaniem ich liczby. Pod protokołem podpis składa minister gospodarki. Protokół sporządza się w dwóch egzemplarzach, z czego egzemplarz nr 1 otrzymuje przedsiębiorca, a egzemplarz nr 2 składa się do akt ministra.

[42] Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG) i Krajowy Rejestr Sądowy (KRS).

[43] Wyjaśnienie pojęcia zob. www.tif.us.edu.pl/download/20150423183020Pojecie wykladni gramatycznej 1.0.doc (przyp. red.).

rakter trwały. Czasowa przerwa w prowadzeniu działalności koncesjonowanej wynikająca z przyczyn organizacyjnych, finansowych lub rynkowych (np. brak popytu) nie musi wcale oznaczać zaprzestania prowadzenia działalności w tym zakresie. Ma to szczególne znaczenie w warunkach polskiego, bardzo szczupłego, rynku broni i amunicji, na którym popyt jest znikomy.

Kontrola

Przedsiębiorca wykonujący działalność gospodarczą w zakresie obrotu bronią i amunicją podlega kontroli co do prawidłowości wykonywania obowiązków ewidencyjnych i informacyjnych. Kontrolę ewidencji sprawują minister właściwy do spraw gospodarki (art. 34 pkt 2 u.o.s.)[44] oraz komendanci wojewódzcy Policji (art. 34 pkt 4 u.o.s.). Wydaje się, że kompetencje organów kontrolnych powinny być wyraźnie rozdzielone. Tymczasem uprawnienia ministra i komendantów wojewódzkich Policji w znacznej mierze się pokrywają. Policja dysponuje nieporównywalnie większymi możliwościami technicznymi i organizacyjnymi, które pozwalają na prowadzenie skutecznej kontroli w terenie, niż organ naczelny. Może więc to policja powinna przejąć całość uprawnień kontrolnych nad obrotem specjalnym.

W § 12 rozp. sprz. przewidziano możliwość przeprowadzenia kontroli obejmującej m.in. prawidłowość prowadzenia dokumentacji sprzedaży oraz przestrzeganie terminów przekazywania bieżących informacji o dokonanej sprzedaży[45].

W praktyce kontrole nie odbywają się często, a raczej *a casu ad casum*, jednak ich wynik może mieć dla koncesjonariusza przykre konsekwencje. Nieprzestrzeganie obowiązków w zakresie ewidencjonowania i informowania może być uznane za rażące naruszenie warunków wykonywania koncesjonowanej działalności gospodarczej, skutkujące obligatoryjnym cofnięciem koncesji (art. 17 ust 2 pkt 2 u.o.s.). Inne nieprawidłowości w tym zakresie mogą spowodować fakultatywne cofnięcie koncesji (art. 17 ust 3 pkt 2 u.o.s.)[46], zwykle jednak przedsiębiorca zostaje uprzednio wezwany do usunięcia w wyznaczonym terminie stanu niezgodnego z przepisami regulującymi działalność gospodarczą objętą koncesją (art. 17 ust. 2 pkt 1 u.o.s.).

Ustawa o obrocie specjalnym zawiera przepisy karne. Jednak *de lege lata* żaden z nich nie penalizuje dobitnie czynu polegającego na niewykonywaniu lub nienależytym wykonywaniu bieżących obowiązków ewidencyjnych i informacyjnych[47]. Należy

[44] Może dziwić to, że ministrowi przyznano kompetencję do prowadzenia kontroli w zakresie obrotu amunicją, lecz nie przyznano kompetencji w zakresie obrotu bronią. Stąd też nie jest jasne, czy ten przepis upoważnia ministra do kontroli ewidencji obrotu bronią, czy tyko amunicją.

[45] Dotyczy informacji, o których mowa w § 3 ust. 1, § 4 ust. 1 oraz § 9 ust. 1 rozp. sprz. Zgodnie z § 13 ust. 1 rozp. sprz. taką kontrolę przeprowadza się w godzinach pracy kontrolowanego przedsiębiorcy, a w sytuacjach szczególnie uzasadnionych – o każdej porze. Kontrola może być przeprowadzona w siedzibie kontrolowanego przedsiębiorcy, innych miejscach związanych z wykonywaną przez niego działalnością gospodarczą lub w siedzibie organu kontrolującego (§ 13 ust. 2 rozp. sprz.). Z przeprowadzonej kontroli sporządza się protokół kontroli (§ 14 ust. 1 rozp. sprz).

[46] Oba przepisy zawierają wykazy otwarte przesłanek cofnięcia koncesji.

[47] Art. 38 ust. 1 i 2 u.o.s. wprowadził wyraźne sankcje wyłącznie za czyny określone w art. 15 ust. 1 pkt 2, 3 i 5 u.o.s. W przypadku innych nieprawidłowości przy wykonywaniu obowiązków ewidencyjnych i informacyjnych brakuje precyzyjnego przepisu karnego. Znamiona opisywanego zachowania nie pokrywają się ze znamionami ustawowymi określonymi w art. 36 ust. 1 u.o.s., który dotyczy tylko wykonywania działalności gospodarczej bez koncesji lub wbrew określonym w niej warunkom. Obowiązki ewidencyjne i informacyjne wynikają z ustawy i przepisów wykonawczych, a nie z treści koncesji. Koncesja może zawierać szczególne warunki, o których mowa w art. 14 ust. 2 u.o.s., nie dotyczą one jednak wymogów ewidencyjnych i informa-

jednak dodać, ze przypadki nieprzestrzegania przepisów dotyczących tych obowiązków należą do rzadkości. Koncesjonariusze mają świadomość znaczenia obrotu specjalnego dla bezpieczeństwa państwa i porządku publicznego i z reguły dopełniają wymogów z należytą starannością. Nie oznacza to jednak, że w ewidencji nie mogą pojawić się nieprawidłowości. Dlatego należy oczekiwać, że ustawodawca *de lege ferenda* dokona precyzyjnej typizacji tego czynu[48].

Podsumowanie

Zarówno przepisy ustawy o obrocie specjalnym, jak i aktów rangi podustawowej wydają się jasne i spójne, a ich poprawne stosowanie daje organom państwa możliwość szczegółowej kontroli podmiotów zajmujących się obrotem bronią i amunicją. W praktyce jednak mogą pojawić się trudności, zwłaszcza z uwagi na konieczność prowadzenia kilku rodzajów ewidencji i wysoki stopień ich szczegółowości, który sprzyja popełnianiu omyłek. Ważne jest, aby organy kontrolne potrafiły właściwie odróżnić błędy nieumyślne od świadomego działania na szkodę porządku publicznego i bezpieczeństwa państwa.

Czynności podejmowane przez państwo wobec koncesjonariuszy nie powinny polegać wyłącznie na kontroli, ale także na oferowaniu im merytorycznego wsparcia w realizacji nałożonych obowiązków. Wydaje się, że relacje pomiędzy przedsiębiorcami a organami kontrolnymi są obecnie oparte na dobrze pojętej współpracy. Sprzyja temu znikoma liczba podmiotów prowadzących działalność w zakresie obrotu specjalnego oraz to, że przedsiębiorcami w tej branży są często osoby wcześniej związane z formacjami mundurowymi.

Mimo możliwości przekazywania informacji organom z wykorzystaniem środków komunikacji elektronicznej, sposób prowadzenia ewidencji i przekazywania informacji może jednak wydawać się nieco archaiczny. W dobie tzw. administracji elektronicznej ewidencję można byłoby znacznie usprawnić przez stworzenie witryny internetowej zawierającej interfejs użytkownika. Przedsiębiorca po zalogowaniu do indywidualnego konta wprowadzałby potrzebne dane za pomocą formularza elektronicznego bezpośrednio do systemu, dzięki czemu obieg informacji byłby przyspieszony. Ponadto organ kontroli miałby bezpośredni wgląd w ewentualnie dokonywane korekty w dokumentacji. Przedsiębiorca nie przechowywałby ewidencji w swojej siedzibie, dzięki czemu nie byłaby ona narażona na przypadkowe lub celowe uszkodzenie, zniszczenie czy kradzież. Dokumentacja przechowywana w profesjonalnie administrowanym systemie informatycznym byłaby lepiej zabezpieczona przed dostępem osób nieuprawnionych, w tym przed atakami złośliwego oprogramowania. Prowadzenie ewidencji w takiej formie uczyniłoby omawiany obowiązek przekazywania informacji bezprzedmiotowym, gdyż organ dysponowałby wszystkimi informacjami od momentu ich wprowadzenia do ewidencji internetowej.

---

cyjnych. Treść koncesji nie może powielać treści przepisów ustawy czy rozporządzenia. Wątpliwe byłoby też uznanie braku ewidencji lub jej wad za utrudnienie prowadzenia kontroli, spenalizowane w art. 39 ust. 1 u.o.s. Opisywany czyn nie jest także naruszeniem warunków udzielenia koncesji, gdyż te są określone w art. 8 u.o.s., a obowiązki ewidencyjne i informacyjne powstają dopiero po rozpoczęciu wykonywania koncesjonowanej działalności gospodarczej.

[48] Ten czyn jest związany tylko z treścią ustawy o obrocie specjalnym i nie kwalifikuje się jako naruszenie przepisów innych ustaw. Dlatego stosownie do § 28 załącznika do *Rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (Dz.U. z 2002 r. Nr 100 poz. 908) sankcje karne za jego popełnienie powinny być kompleksowo uregulowane w omawianej ustawie.

Od pewnego czasu są prowadzone prace nad wdrożeniem elektronicznej platformy o nazwie „e-koncesje", która ma pełnić funkcję bazy udzielonych koncesji w zakresie wytwarzania materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, a także obrotu nimi. Może warto w ramach takiej platformy wprowadzić możliwość zdalnego prowadzenia ewidencji obrotu specjalnego. Każde usprawnienie wykonywania obowiązków ewidencyjnych i informacyjnych w obrocie bronią i amunicją, skutkujące dokładniejszym i szybszym przepływem informacji, ma korzystny wpływ na poprawę stanu bezpieczeństwa i porządku publicznego. Te zaś wartości powinny stanowić priorytet nie tylko dla organów kontroli, lecz także dla koncesjonariuszy.

Bibliografia:

Akty prawne:

1. *Dyrektywa Parlamentu Europejskiego i Rady 2008/51/WE z dnia 21 maja 2008 r. zmieniająca dyrektywę Rady 91/477/EWG w sprawie kontroli nabywania i posiadania broni* (Dz.Urz. UE L 179 z 8 VII 2008 r. poz. 5).
2. *Dyrektywa Rady 91/477/EWG z dnia 18 czerwca 1991 r. w sprawie kontroli nabywania i posiadania broni* (Dz.Urz. WE L 256 z 13 IX 1991 r. poz. 51).
3. *Oświadczenie Rządowe z dnia 23 marca 2011 r. w sprawie wejścia w życie zmian do załączników A i B „Umowy europejskiej dotyczącej międzynarodowego przewozu drogowego towarów niebezpiecznych (ADR), sporządzonej w Genewie dnia 30 września 1957 r."* (Dz.U. z 2011 r. Nr 110 poz. 641).
4. *Rozporządzenie Ministra Gospodarki z dnia 18 lutego 2013 r. w sprawie trybu i szczegółowych warunków przekazywania ewidencji związanej z wykonywaniem działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym* (Dz.U. z 2013 r. poz. 3480).
5. *Rozporządzenie Ministra Gospodarki z dnia 22 sierpnia 2012 r. w sprawie sposobu ewidencjonowania wprowadzonych do obrotu materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym* (Dz.U. z 2012 r. poz. 1008).
6. *Rozporządzenia Ministra Gospodarki z dnia 25 września 2002 r. w sprawie szkolenia potwierdzającego przygotowanie zawodowe do wykonywania lub kierowania działalnością gospodarczą w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją i wyrobami o przeznaczeniu wojskowym lub policyjnym oraz obrotu technologią o tym przeznaczeniu* (Dz.U. z 2002 r. Nr 173 poz. 1415, ze zm.).
7. *Rozporządzenie Ministra Gospodarki i Ministra Spraw Wewnętrznych z dnia 6 marca 2013 r. w sprawie sprzedaży materiałów wybuchowych, broni, amunicji, wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym oraz kontroli przestrzegania warunków sprzedaży* (Dz.U. z 2013 r. poz. 343).
8. *Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (Dz.U. z 2002 r. Nr 100 poz. 908).
9. *Rozporządzenie Rady Ministrów z dnia 3 grudnia 2001 r. w sprawie rodzajów broni i amunicji oraz wykazu wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub obrót jest wymagana koncesja* (Dz.U. z 2001 r. Nr 145 poz. 1625).

10. *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (tekst jednolity: Dz.U. z 2016 r. poz. 23).
11. *Ustawa z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym* (tekst jednolity: Dz.U. z 2012 r. poz. 1017, ze zm.).
12. *Ustawa z dnia 23 czerwca 2006 r. o zmianie niektórych ustaw w związku z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej* (Dz.U. z 2006 r. Nr 133 poz. 935).
13. *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (tekst jednolity: Dz.U. z 2013 r. poz. 1422, ze zm.).
14. *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (tekst jednolity: Dz.U. z 2014 r. poz. 1114).
15. *Ustawa z dnia 21 maja 1999 r. o broni i amunicji* (tekst jednolity: Dz.U. z 2012 r. poz. 576, ze zm).

Źródła internetowe:

https://en.wikipedia.org/wiki/Number_of_guns_per_capita_by_country [dostęp: 14 VII 2015].

Abstrakt

Handel bronią i amunicją zazwyczaj jest kojarzony bądź z działalnością państwa (sił zbrojnych), bądź organizacji przestępczych. Na rynku broni i amunicji funkcjonują jednak także legalnie działające prywatne podmioty gospodarcze ściśle kontrolowane przez organy państwa. Kontrolę tych podmiotów umożliwiają przepisy zawarte zarówno w akcie rangi ustawowej, jak i w kilku aktach wykonawczych. Nakładają one na przedsiębiorców nie tylko obowiązek uzyskania koncesji, lecz także prowadzenia szczegółowej ewidencji obrotu i przekazywania ściśle określonych informacji wyznaczonym organom państwa. Dzięki sprawnemu obiegowi informacji państwo dysponuje możliwością wglądu w działalność sprzedawców i nabywców, ograniczając tym samym możliwość niekontrolowanego przepływu broni i amunicji oraz jej dostępność na czarnym rynku. Autor dokonuje szczegółowego przeglądu przepisów dotyczących sposobu ewidencjonowania obrotu bronią i amunicją oraz przekazywania informacji właściwym organom. Omawia także konsekwencje, jakie mogą ponieść przedsiębiorcy nieprzestrzegający obowiązków ewidencyjnych i informacyjnych. Autor proponuje również rozwiązania, które nie tylko mogą ułatwić wykonywanie omawianych obowiązków, lecz także usprawnić kontrolę działalności koncesjonowanej.

Słowa kluczowe: broń, amunicja, obrót, handel, ewidencja.

Abstract

Arms and ammunition trade is usually associated either with activities of the State (armed forces) or criminal organizations. However, on the market of arms and ammunition there are also legally functioning, private business entities, which are strictly controlled by the authorities of the state. This control is enabled by a number of provisions

contained in both - the act of statutory rank, as well as in several implementing acts. They impose on entrepreneurs, not only the obligation to obtain a license, but also keep detailed records of trade and transfer of specific information to designated authorities of the state. Through efficient cycle of information, the state has the power to inspect activities of sellers and buyers, thereby limiting the possibility of uncontrolled movement of arms and ammunition as well as its availability on the black market. The author provides a thorough review of the provisions concerning methods of registering arms and ammunition trade as well as providing information to competent authorities. Also discussed are consequences to be suffered by entrepreneurs not complying with registration and information obligations. The author also proposes solutions that not only facilitate exercising discussed obligations, but also improve the control of licensed activities.

Keywords: arms, ammunition, trade, commerce, registration.

Karol Falandys

Odzyskiwanie personelu (Personnel Recovery – PR) jako forma reakcji na bezprawną izolację osób

Polityków można podzielić na przyzwoitych i rozważnych oraz na mężnych. Pierwsi miłujący pokój, stają się z czasem niezdolni do walki i popadają w uzależnienie od wrogów. Drudzy natomiast – na skutek wszczynanych konfliktów sprowadzają na siebie i swój lud gniew wrogów. Warunkiem ładu jest łączenie ze sobą obydwu postaw (rozwagi i waleczności).

Platon (429–347 przed Chr.)

Posiadanie środków do odzyskiwania personelu nie gwarantuje, że wygrasz wojnę, ale ich brak z pewnością doprowadzi do przegranej.

gen. Lance Smith, były Głównodowodzący
Połączonego Dowództwa Sił Amerykańskich

Uprowadzenia i bezprawna izolacja osób nie są zjawiskami nowymi czy wynikającymi z procesów globalizacji. Powszechność ruchu osobowego w wymiarze globalnym spowodowała jednak zarówno nasilenie się tego zjawiska, jak i objęcie nim szerszej grupy osób. W kontekście historycznym działania mające na celu odnalezienie osób wynikały przede wszystkim z ich zaginięcia, rzadziej porwania lub bezprawnego przetrzymywania. Typowymi przykładami akcji poszukiwawczych były te dotyczące doktora Davida Livingstone'a[1] i kapitana Scotta[2], chociaż w ówczesnej rzeczywistości podobne przedsięwzięcia były rzadkością. Generalnie uznawano, że zaginiony uległ wypadkowi i nie podejmowano dalszych działań. W ten sam sposób postępowano w przypadku żołnierzy zaginionych podczas operacji militarnych. Ich zaginięcie czy ujęcie przez stronę przeciwną było traktowane jako konsekwencja prowadzonych działań. Inaczej zaczęto postrzegać ten problem dopiero w czasie II wojny światowej. Za nestorów nowego podejścia do kwestii zaginionych żołnierzy uznaje się Brytyjczyków, którzy zdecydowali się na prowadzenie działań poszukiwawczo-ratowniczych w odniesieniu do pilotów Royal Air Force (RAF). W tym przypadku jednak odzyskiwanie załóg lotniczych nie

[1] W połowie XIX w. toczono debatę dotyczącą źródła Nilu. Niektórzy szukali jego początków w jeziorze Wiktorii, inni umiejscawiali je dalej na południu. W styczniu 1866 r. doctor David Livingstone wyruszył na wyprawę, aby zbadać ten problem. Podróż rozpoczął w pobliżu ujścia rzeki Ruvuma. Niedługo potem asystenci doktora opuścili go, informując władze o jego rzekomej śmierci. W tym samym czasie Livingstone kontynuował wyprawę. Gdy skończyły mu się zapasy żywności i lekarstwa, zachorował na kilka chorób tropikalnych. Na sześć lat Livingstone niemal całkowicie stracił kontakt ze światem zewnętrznym, a przez cztery ostatnie lata swojego życia – chorował. Z 44 wysłanych depesz tylko jedna dotarła do Zanzibaru. Henry Morton Stanley, który w 1869 r. został wysłany przez gazetę „New York Herald" do Afryki, 27 października 1871 r. odnalazł doktora Livingstone'a na brzegu jeziora Tanganika.

[2] Kapitan Scott jako pierwszy na świecie usiłował zdobyć biegun południowy, ale po 33 dniach zrezygnował. Wraz ze swoją ekipą zaginął w drodze powrotnej. Ich ciała odnaleziono osiem miesięcy później.

było działaniem stricte humanitarnym, ale wynikało z przesłanek operacyjnych. Stanowiło bowiem jedną z form utrzymania gotowości bojowej RAF i efektywności działań zbrojnych, gdyż podczas II wojny światowej największym problemem brytyjskiej armii był brak wyszkolonych pilotów[3].

Współcześnie problematyka poszukiwania osób zaginionych stała się istotnym elementem polityki państw demokratycznych. Podobnie jak pilot wojskowy w okresie II wojny światowej, tak i obecnie żołnierz (funkcjonariusz) stał się wymierną wartością z operacyjnego (z uwagi na poziom wyszkolenia i efektywność jego działań) oraz ekonomicznego (z uwagi na koszty szkolenia oraz wykorzystywanego przez niego sprzętu) punktu widzenia. Ważną rolę odegrały też media, które, odpowiednio budując przekaz medialny (np. odnośnie do toczącej się wojny), mogą dowolnie kreować jej odbiór społeczny. Doskonałym tego przykładem może być casus Wietnamu bądź tzw. efekt CNN osiągnięty podczas pierwszej operacji irackiej w 1991 r., który polegał na transmitowaniu na żywo reportaży z obszaru działań wojennych. W wyniku tak prowadzonych relacji dziennikarskich media natychmiast pokazywały przetrzymywanych żołnierzy koalicji, mimo że z formalnego punktu widzenia było to złamanie zapisów artykułu 13 III konwencji genewskiej, która uznaje publiczne pokazywanie jeńców wojennych, niezależnie od środków przekazu (TV lub zdjęcia), za łamanie międzynarodowego prawa humanitarnego, co w skrajnych przypadkach może być sądzone jako zbrodnia wojenna. Pierwszymi jeńcami pokazanymi w mass mediach byli kpt. Maurizio Cocciolone oraz por. Peters i por. Nichol[4].

To, w jaki sposób pokazanie pojmanego jeńca może wpływać na decyzje o zaangażowaniu militarnym państwa, obrazują zdarzenia, do jakich doszło podczas misji pokojowej Unified Task Force (UNITAF) w Somalii oraz w czasie operacji ONZ/NATO w Bośni i Hercegowinie. W światowych mediach ukazały się relacje z bezczeszczenia zwłok amerykańskiego żołnierza na ulicach Mogadiszu[5] oraz wykorzystywania pojmanego personelu ONZ jako „żywych tarcz" chroniących ważne obiekty wojskowe. W pierwszym z omawianych przypadków reakcja opinii publicznej doprowadziła do podjęcia przez prezydenta Billa Clintona decyzji o zaprzestaniu przez Amerykanów wszelkich czynności bojowych na tym obszarze, a następnie do całkowitego wycofania się z terytorium tego państwa. W drugim przypadku siły NATO odstąpiły od atakowania strategicznych obiektów, w których umieszczono pracowników ONZ[6].

Zaprezentowane przykłady wyraźnie wskazują, że zagrożenie bezprawną izolacją lub samo pojmanie personelu cywilnego może stanowić formę działań jednej ze stron sporu lub konfliktu. Ofiarami tych działań są pracownicy instytucji międzynarodowych, organizacji pozarządowych, doradcy, mediatorzy, obserwatorzy i dziennikarze. Decydując się na taki krok, strona konfliktu może dążyć do uzyskania przewagi politycznej lub wojskowej, co pokazały przypadki porwań Terriego Waite'a[7] i Giuliany Sgreny[8]. In-

[3] K. Falandys, *Uwarunkowania prawne determinujące kształt Narodowego Systemu Odzyskiwania Obywateli Rzeczypospolitej Polskiej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2015, nr 2, s. 134.

[4] Tamże.

[5] Ofiarą był pilot amerykańskiego śmigłowca, który 3 X 1993 r. został zestrzelony nad Somalią. Był to jedyny członek załogi, który przeżył upadek śmigłowca, ale został zamordowany przez miejscowe zbrojne bandy.

[6] K. Falandys, *Uwarunkowania prawne*..., s. 134–135.

[7] Brytyjczyk porwany 20 stycznia 1987 r. w Bejrucie. Został zakładnikiem i był przetrzymywany w niewoli przez 1763 dni, które spędził w całkowitym odosobnieniu. Został uwolniony po czterech latach, 18 XI 1991 r., http://news.bbc.co.uk/onthisday/hi/witness/november/18/newsid_2903000/2903953.stm [dostęp: 10 XI 2015].

[8] Ta włoska komunistyczna dziennikarka, pracująca dla włoskiej gazety komunistycznej „Il Manifesto" i niemieckiego tygodnika „Die Zeit", podczas pracy w Iraku została 4 II 2005 r. porwana przez powstańców. Uwolniono ją tego samego dnia, ale podczas uwalniania od ostrzału sił amerykańskich zginął oficer włoskiego wywiadu

nym celem może być dążenie do skutecznego zastraszenia wspólnoty międzynarodowej. W tym przypadku poza pracownikami organizacji ponadnarodowych czy NGOs (ang. Non-Governmental Organisations – 'organizacje pozarządowe') ofiarami mogą być zwyczajni cywile, czasowo przebywający w danym rejonie, np. turyści, pracownicy firm czy biznesmeni[9].

> Powszechność stosowania porwania i bezprawnej izolacji staje się więc poważnym problemem natury politycznej. Medialność tych zdarzeń powoduje zaś to, że władze państw są zmuszone do podejmowania działań zmierzających do uwolnienia przetrzymywanych obywateli. Niekiedy nie jest to możliwe na drodze negocjacji lub w ramach planowej ewakuacji i wówczas niezbędne jest podjęcie działań siłowych. Podstawową formą reagowania w takiej sytuacji są procedury określane właśnie jako odzyskiwanie personelu, czyli Personnel Recovery[10].

Istota przedsięwzięć określanych jako „odzyskiwanie personelu"

Odzyskiwanie personelu jako forma aktywności państwa obejmuje wiele przedsięwzięć o charakterze dyplomatycznym, militarnym (operacyjnym) i administracyjnym, których celem jest uwolnienie i reintegracja osoby bezprawnie izolowanej[11]. Znaczne koszty wyszkolenia i wyposażenia żołnierza współczesnego pola walki powodują, że procedury odzyskiwania personelu mają zastosowanie w odniesieniu do czterech głównych grup:

1) żołnierzy prowadzących działania operacyjne w chwili ich zaginięcia lub przejęcia przez wroga,
2) przedstawicieli państwa, zwłaszcza dysponujących informacjami niejawnymi ważnymi dla jego bezpieczeństwa,
3) obywateli; w tym przypadku są traktowane jako forma podnoszenia zaufania do własnego państwa,
4) sprzętu wojskowego o dużym znaczeniu operacyjnym[12].

Przedstawiona kolejność nie jest przypadkowa – odzwierciedla hierarchię celów działania państwa w przypadku konieczności stosowania procedur Personnel Recovery. Tym samym należy wskazać, że odzyskiwanie personelu nie jest zadaniem ograniczanym do odbijania osób przetrzymywanych – najczęściej przez grupy przestępcze i ugrupowania terrorystyczne[13] – ale kompleksowym działaniem państwa i jego sił zbrojnych. Należy sobie bowiem uzmysłowić, że równie ważne, co uratowanie życia przetrzymywanej osobie, jest odzyskanie sprzętu, zwłaszcza jeśli jest on wytworzony w nowej technologii i jeśli jego przejęcie przez niepowołane osoby lub ugrupowania mogłoby

wojskowego, a inny został ranny. Zdarzenie wywołało oburzenie opinii międzynarodowej. Zob. http://www.nytimes.com/2005/03/05/world/middleeast/italian-hostage-returns-homeafter-2nd-brush-with-death.html [dostęp: 2 VII 2016].

[9] Zob. K. Falandys, *Zjawisko izolacji (bezprawnego przetrzymywania) – jego skala i regionalizacja,* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 178–194.

[10] K. Falandys, *Uwarunkowania prawne*..., s. 135.

[11] *Koncepcja i ogólne zasady funkcjonowania Narodowego Systemu Odzyskiwania Personelu Wojskowego,* Warszawa 2008, s. 8.

[12] Tamże, s. 10.

[13] Próby ograniczenia zakresu Personnel Recovery do problemu izolacji osób porwanych przez terrorystów miały miejsce i w Polsce. Taki pogląd wysuwają eksperci zajmujący się tymi sprawami w Ministerstwie Spraw Wewnętrznych.

przynieść poważne straty finansowe bądź technologiczne[14]. Dlatego niezwykle istotne jest wprowadzenie jednoznacznych pojęć pozwalających określić nie tylko status osoby izolowanej, lecz także formę podejmowanych wobec niej działań.

Przyjmując za punkt wyjścia do stworzenia kategorii pojęć powszechnie stosowaną i przywołaną powyżej definicję PR (ang. Personnel Recovery – 'odzyskiwanie personelu'), należy uznać, że osobami, które mogą otrzymać status IP (ang. Isolated Personnel – 'personel izolowany') będą żołnierze, funkcjonariusze, pracownicy cywilni oraz osoby, które zostały odseparowane od macierzystej jednostki lub organizacji i zmuszone do stosowania technik przeżycia, ukrywania się, przeciwdziałania wykorzystaniu lub przygotowania ucieczki. Równie ważne, zwłaszcza w kontekście charakteru podejmowanych działań w celu odzyskania porwanych osób oraz stosowanych sposobów izolacji, jest określenie zdarzenia, które doprowadziło do ich izolacji. Może do tego dojść w wyniku prowadzonych działań bojowych, wypadku lub zwykłego zagubienia się w terenie, klasycznego zatrzymania przez siły przeciwnika oraz uprowadzenia przez bojowników, organizacje przestępcze lub terrorystyczne[15].

Istotnym zagadnieniem jest także uznanie zasadności podejmowania działań z zakresu Personnel Recovery. Akcje bojowe będą praktycznie niemożliwe do przeprowadzenia w przypadku zatrzymania osób przez siły rządowe, wojskowe lub policyjne władz lokalnych[16]. Możliwe jest natomiast prowadzenie takich działań w czasie pokoju lub w przypadku braku działań wrogich.

Tab. 1. Klasyfikacja przyczyn bezprawnej izolacji i grupy osób podatne na dane zdarzenie.

Rodzaj zdarzenia	Potencjalne ofiary (cele bezprawnej izolacji)	Powód bezprawnej izolacji
Prowadzenie działań bojowych (ang. isolated)	żołnierze i funkcjonariusze służb państwowych biorący udział w działaniach bojowych	prowadzenie konkretnej operacji lub akcji bojowej na obszarach opanowanych przez przeciwnika
Zagubienie (zaginięcie), brak orientacji w terenie lub wypadek (ang. missing)	żołnierze, funkcjonariusze biorący udział w działaniach bojowych oraz osoby cywilne przebywające w danym rejonie geograficznym	zdarzenie losowe w postaci awarii samolotu, awaria lub zatonięcie okrętu, odłączenie się od zespołu prowadzącego działania, zagubienia; na skutek prowadzenia wrogich działań w stosunku do obywateli, m.in. zestrzelenie samolotu, zatopienie okrętu, rozproszenie zespołu prowadzącego określone działania w niesprzyjającym środowisku

[14] *Cheney do Obamy: jak mogłeś dopuścić do tego?* [online], http://www.polskieradio.pl/5/3/Artykul/499145,Cheney-do-Obamy-jak-mogles-dopuscic-do-tego [dostęp: 20 VII 2013].

[15] K. Falandys, *Uwarunkowania prawne*..., s. 136.

[16] *Koncepcja i ogólne zasady*..., s. 14 i 15.

Zatrzymanie przez siły rządowe lub władze lokalne (ang. detained)	pracownicy misji dyplomatycznych, turyści łamiący lokalne prawo	działania wymierzone w przedstawiciela państwa lub jego obywatela w celu uzyskania korzyści
Uprowadzenie przez bojowników lub ugrupowania przestępcze i terrorystyczne (ang. captured)	wszystkie wymienione grupy osób	pozyskanie środków finansowych, możliwość uzyskania określonych profitów politycznych, np. uwolnienie zatrzymanych terrorystów oraz uzyskanie elementu zastraszenia

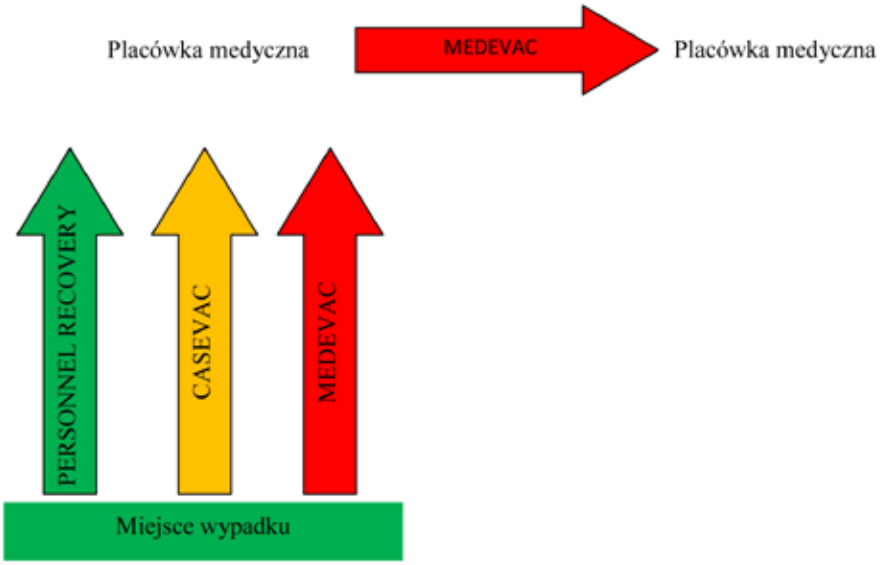
Źródło: Opracowanie własne na podstawie K. Falandys, *Uwarunkowania prawne…*, s. 136.

Najczęściej będzie to dotyczyć sytuacji, które pozwolą zaliczyć zdarzenie do zaprezentowanej w powyższej tabeli kategorii *missing*. W takim przypadku ważnym wyróżnikiem są także cechy środowiska, w którym doszło do zagubienia.

Innymi działaniami, niekiedy błędnie uznawanymi za działania prowadzone w ramach procesu Personnel Recovery, są przedsięwzięcia typu **ewakuacja medyczna** (ang. Medical Evacuation – MEDEVAC**)** oraz **ewakuacja ofiar** (ang. Casualty Evacuation – CASEVAC). Są one elementem Personnel Recovery lub występują równocześnie z tymi działaniami, w związku z czym niekiedy trudno je rozróżnić. MEDEVAC to transport osób, które odniosły obrażenia, zostały ranne lub zachorowały, do miejsc wykonywania zabiegów medycznych i (lub) pomiędzy tymi miejscami, prowadzony pod kontrolą medyczną. Dlatego procedura MEDEVAC jest stosowana w ramach działań Personnel Recovery lub jako ich osobny element w przypadku, gdy odzyskiwana osoba jest ranna bądź gdy jej stan zdrowia wymaga jej przewiezienia pod kontrolą medyczną. Równocześnie może zajść sytuacja odwrotna – gdy procedura MEDEVAC zostaje wzmocniona działaniami Personnel Recovery. Dochodzi do tego szczególnie wtedy, gdy miejsce odbioru pacjenta lub docelowy punkt jego transportu nie są w pełni zabezpieczone. W opinii autora niniejszej publikacji MEDEVAC jest raczej przedsięwzięciem logistycznym i – nieco upraszczając – transportem pod nadzorem medycznym do placówek medycznych.

W podobny sposób należy ocenić drugą ze wskazanych procedur, czyli CASEVAC. Definiuje się ją jako taktyczną ewakuację ofiar placówek na obszarze działań wojennych. Najczęściej te działania oznaczają transport osób wymagających opieki medycznej w sytuacji, gdy jej zapewnienie w danej jednostce leczniczej nie jest możliwe zarówno z powodu braku sprzętu, jak i wystąpienia zagrożeń niemedycznych. W dodatku, co należy jednoznacznie podkreślić, takie działania nie będą prowadzone w odniesieniu do personelu, który nie wymaga opieki medycznej, a które to ograniczenie nie występuje w przypadku procedur Personnel Recovery[17]. Z tego względu zarówno MEDEVAC, jak i CASEVAC należy zaliczyć do czynności logistycznych polegających na przetransportowaniu ofiar z terenu względnie bezpiecznego do placówek medycznych. Personnel Recovery natomiast stanowią procedury działań, których celem jest odzyskanie personelu izolowanego, w tym z terenu niebezpiecznego, wraz z udzieleniem mu stosowej pomocy medycznej podczas transportu do placówki medycznej.

[17] *Personnel Recovery,* JAPCC, 2011, s. 26.



Schemat 1. Wzajemne zależności między procedurami Personel Recovery, MEDEVAC i CASEVAC.

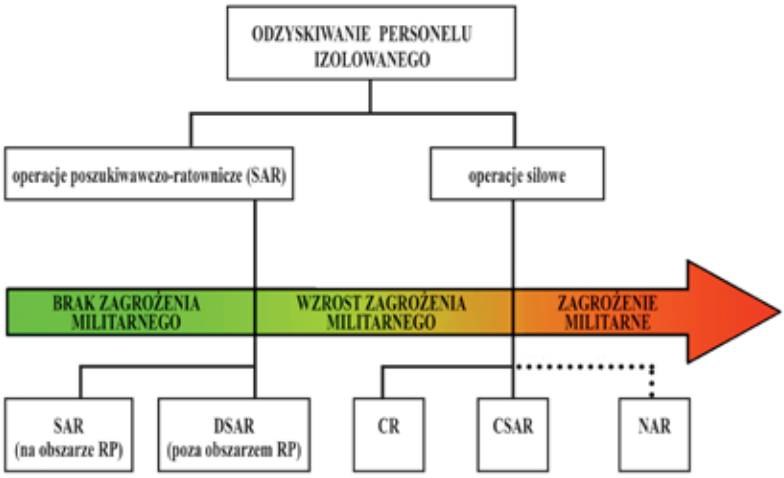
Źródło: Opracowanie własne na podstawie *Personnel Recovery,* JAPCC, 2011, s. 27.

Metody odzyskiwania personelu i sprzętu w przypadku zdarzeń o charakterze niemilitarnym

Odzyskiwanie personelu izolowanego (bezprawnie przetrzymywanego) jest, jak już wcześniej wspomniano, procesem obejmującym ściśle skorelowane działania dyplomatyczne i wojskowe, prowadzonym przez różne instytucje państwowe, organizacje ponadnarodowe i pozarządowe. Niekiedy istotną rolę odgrywają tu osoby zaufania społecznego. Działania mające na celu odzyskanie personelu powinny być prowadzone wielotorowo i wielowątkowo przez powołane do tego celu instytucje państwowe. Najważniejszą rolę należy przyznać ministerstwom: spraw zagranicznych, obrony i spraw wewnętrznych. Pierwsze z nich, poza nawiązaniem kontaktów międzynarodowych, powinno prowadzić działania dyplomatyczne ukierunkowane na prowadzenie negocjacji i ewentualne zawarcie ugody, skierowane bezpośrednio do organizacji (osób) stosujących bezprawną izolację. Rolą resortu spraw wewnętrznych jest poszukiwanie i ewentualna lokalizacja osób przetrzymywanych oraz uzyskanie informacji o sprawcach tego przestępstwa. Ewentualne działania wojskowe kierowane przez ministerstwo obrony powinny obejmować przygotowanie i przeprowadzenie operacji odzyskania przetrzymywanego personelu.

Jeżeli do zdarzenia doszło w środowisku (na terytorium) definiowanym jako przyjazne i nie występuje wobec poszukiwanych zagrożenie ze strony osób trzecich, to działania określa się jako **akcje poszukiwawczo-ratownicze** (ang. Search and Rescue – SAR) lub **ekspedycyjne akcje poszukiwawczo-ratownicze** (ang. Deployable Search and Rescue – DSAR). Zakres SAR doskonale zdefiniowano w instrukcji ATP-10

(SAR). Sprowadzają się one do użycia samolotów, pojazdów naziemnych, podwodnych, wyszkolonych ekip ratunkowych i wyspecjalizowanego sprzętu w celu odzyskania personelu znajdującego się w sytuacji zagrożenia na ziemi lub na morzu. Tym samym ich zasadniczym wyróżnikiem jest przynależność terytorialna obszaru, na którym są prowadzone działania (czynności na terytorium państwa lub wymagające dyslokacji sprzętu i sił poza obszar kraju). Akcje SAR i DSAR mają wiele cech wspólnych, zwłaszcza to, że w ich czasie nie występuje zagrożenie ze strony osób trzecich. Ponadto rozróżnia się instrukcje dotyczące odzyskiwania ludzi i odzyskiwania sprzętu. Występuje też podział ze względu na poziom ryzyka, wyszkolenie personelu izolowanego i jego wyposażenie[18].



Schemat 2. Metody odzyskiwania personelu izolowanego.

Źródło: Opracowanie własne na podstawie materiałów szkoleniowych otrzymantych podczas kursu instruktorskiego SERE. K. Falandys, *Uwarunkowania prawne*..., s. 138.

Podstawowe metody odzyskiwania personelu w sytuacji zagrożenia militarnego

Sposób prowadzonych działań z zakresu Personnel Recovery jest uzależniony od wielu czynników, ale istotną rolę odgrywa tu status osób izolowanych. Najczęściej za personel izolowany uznaje się, przypomnijmy, funkcjonariuszy i urzędników państwowych, którzy zostali odseparowani od swoich organizacji i są zmuszeni do stosowania technik przeżycia, ukrywania się, przeciwdziałania wykorzystaniu lub przygotowania ucieczki. W zależności od ich pozycji zawodowej należy wyróżnić dwie kategorie osób zagrożonych izolacją: **personel wysokiego ryzyka** (ang. High Risk of Isolation – HRI) oraz **personel średniego ryzyka** (ang. Medium Risk of Isolation – MRI)[19].

Pierwszą grupę stanowią osoby, które z racji pełnionej funkcji lub realizowanych zadań są szczególnie narażone na ryzyko izolacji, a następnie wykorzystania przez przeciwnika w celu pozyskania istotnych informacji. Do tej grupy należy zaliczyć wysokich rangą przedstawicieli dyplomatycznych, osoby o statusie VIP, załogi statków powietrz-

[18] K. Falandys, *Uwarunkowania prawne*..., s. 137.
[19] *Odzyskiwanie izolowanego personelu (DD/3.3.9)*, Warszawa 2010, s. 7.

nych, funkcjonariuszy i pracowników służb specjalnych, personel zespołów szkoleniowo-treningowych, żołnierzy: rozpoznania osobowego (ang. Human Intelligence – HUMINT), współpracy cywilno-wojskowej (ang. Civil-Military Co-operation – CIMIC), operacji psychologicznych (ang. Psychological Operations – PSYOPS) oraz żołnierzy jednostek specjalnych i dalekiego rozpoznania działających w odosobnieniu.

Drugą grupę stanowi personel, który może być przydzielony do bezpośredniego udziału jako element zabezpieczenia działań w rejonie niebezpiecznym. Do tej grupy należy zatem personel przedstawicielstw dyplomatycznych średniej i niższej rangi, pracownicy firm prywatnych wykonujący zadania służbowe w krajach podwyższonego ryzyka, żołnierze pełniący służbę na etatach logistyczno-sztabowych oraz inne osoby przebywające w rejonach szczególnie narażonych na uprowadzenie w celach terrorystycznych[20].

Niezbędne jest wydzielenie zasadniczych form działania, które mają doprowadzić do odzyskania personelu. Najważniejszymi przedsięwzięciami są **bojowe akcje poszukiwawczo-ratownicze** (ang. Combat Search and Rescue – CSAR) oraz **bojowe odzyskiwanie** (ang. Combat Recovery – CR). Są to działania realizowane w warunkach występowania zagrożenia ze strony przeciwnika, z reguły prowadzone na terytorium państwa obcego. Elementami różnicującymi te kategorie są poziom przygotowania i zakres współpracy personelu izolowanego. W pierwszym przypadku jest on odpowiednio przeszkolony i posiada wyposażenie umożliwiające współpracę w celu przeprowadzenia udanej operacji odzyskiwania, w drugim zaś – nie jest przeszkolony do prowadzenia takich działań i nie posiada stosownego wyposażenia[21].

Innymi rodzajami działań są tak zwane **niekonwencjonalne odzyskiwanie personelu** (ang. Non-conventional Assisted Recovery – NAR) i **uwalnianie zakładników** (ang. Hostage Rescue – HR). Przeprowadza się je na terytorium obcego państwa w warunkach dużego zagrożenia ze strony przeciwnika i przy braku innych możliwości odzyskania izolowanych. Do ich uwolnienia najczęściej angażuje się siły specjalne lub korzysta się z pomocy miejscowych przeciwników organizacji uprowadzającej[22].

Inaczej traktuje się odzyskanie tak zwanego **personelu pozostałego** (ang. Other Personnel). W ten sposób określa się wszystkie osoby znajdujące się na terenie operacyjnym i jednocześnie nieposiadające statusu urzędnika państwowego (instytucji ponadnarodowej). Dotyczy to zwłaszcza członków organizacji pozarządowych, reporterów itp. Nie są oni zaliczani do kategorii personelu izolowanego i nie są tym samym celem działań ukierunkowanych na odzyskiwanie personelu. Chyba że w rozkazie operacyjnym uwzględniono konieczność objęcia ich procedurami odzyskiwania personelu. Wobec takich osób stosuje się działania określane jako **akcja ewakuacyjna** (ang. Non-combatant Evacuation Operation – NEO)[23].

Odzyskiwanie personelu wojskowego i cywilnego *(case studies)*

Do odzyskiwania personelu wojskowego w trakcie działań zbrojnych dochodziło podczas wielu konfliktów, zarówno w czasie wojen globalnych, jak i lokalnych. Pierwszym konfliktem po zakończeniu II wojny światowej, w którym podjęto takie działania,

[20] K. Falandys, *Uwarunkowania prawne*..., s. 138–139.

[21] Tamże, s. 137.

[22] Tamże, s. 136. Istnieje również takie pojęcie, jak odzyskiwanie sprzętu. W przypadku działań o charakterze militarnym niekiedy może wystąpić sytuacja, w której **odzyskanie ekwipunku** (ang. Recovering Equipment) może być postrzegane jako bardziej priorytetowe niż odzyskiwanie personelu.

[23] *Personnel Recovery,* JAPCC, 2011, s. 2.

była wojna wietnamska. Najgłośniejszą akcją odzyskiwania personelu było poszukiwanie dowódcy zestrzelonego amerykańskiego samolotu EB-66 płk. Hambletona. Do zdarzenia doszło 2 kwietnia 1972 r. Siły wietnamskie ostrzelały dwa amerykańskie samoloty wykonujące lot patrolowy, które zbierały informacje pozwalające na przygotowanie uderzenia bombowców strategicznych dalekiego zasięgu B-52 w prowincji Quang Tri. W wyniku wietnamskiego ostrzału ocalał tylko jeden pilot, któremu udało się wyskoczyć z samolotu i wylądować na terenie kontrolowanym przez wrogie siły. Natychmiast po zestrzeleniu samolotu i stwierdzeniu faktu uratowania się pilota cztery amerykańskie śmigłowce podjęły działania poszukiwawczo-ratownicze. Dwie maszyny zostały jednak zestrzelone, a jeden członek załogi dostał się do niewoli. Dzień później ponowiono akcję poszukiwawczą – wysłano trzy śmigłowce i samolot patrolowy (OV-10A). Również w tym przypadku dwa śmigłowce zostały ostrzelane i zmuszone do powrotu do bazy, trzeci zaś i samolot – zestrzelono. Załoga zestrzelonego śmigłowca (cztery osoby) została uznana za zaginioną w akcji, a z dwójki pilotów samolotu jeden dostał się do niewoli, a drugi ukrywał się przez 14 dni na terytorium wroga.

W ciągu kilku następnych dni, ze względu na warunki pogodowe i dużą koncentrację sił wietnamskich, wykonano kilkanaście ataków na pozycje wroga, wykorzystując między innymi informacje radiowe od ukrywających się amerykańskich żołnierzy. W niedługim czasie jednak jeden z czterech śmigłowców kolejnego zespołu także został zestrzelony, a załoga zginęła. Dzień później został zestrzelony następny samolot patrolowy, czego konsekwencją było przyjęcie innego wariantu przeprowadzenia akcji. Pilotom polecono przebić się w inny rejon, gdzie zostali przejęci przez oddział Navy Seals[24].

Jak wynika z powyższego opisu, dla uratowania jednego pilota Amerykanie poświęcili osiem statków powietrznych i co najmniej 24 żołnierzy. W sumie podczas wojny w Wietnamie w latach 1964–1973 amerykańskie jednostki poszukiwawczo-ratownicze uratowały 3883 osoby. W czasie tych działań zginęło 71 ratowników i stracono 45 śmigłowców. Ten bilans pokazuje, że wysiłek został okupiony dość dużymi stratami, ale w tym kontekście równie ważnym powodem podejmowania akcji poszukiwawczo-ratowniczych były względy polityczno-propagandowe i próba podniesienia morale żołnierzy.

Podobną akcję poszukiwawczo-ratowniczą, jak wyżej opisana w Wietnamie, siły amerykańskie przeprowadziły podczas operacji Deny Flight. Jej celem była kontrola respektowania zakazu lotów nad terytorium Bośni i Hercegowiny, wprowadzonego przez ONZ w czasie wojny w Jugosławii. Znaczenie tej operacji podnosi stosowanie przez ofiarę zasad SERE. Zestrzelony pilot (kpt. Scott O'Grady) zdołał przetrwać na terytorium kontrolowanym przez Serbów sześć dni i 8 czerwca 1995 r. został ewakuowany przez zespół ratowniczy[25].

Przykładem skutecznej, natychmiastowej ewakuacji z miejsca zdarzenia jest zaś operacja odzyskania pilota, do której doszło 27 marca 1999 r. koło miejscowości Budanovci w Serbii. Pilotowi udało się katapultować z zestrzelonego samolotu i zaledwie sześć godzin później został bezpiecznie ewakuowany przez komandosów z bazy sił specjalnych NATO w Tuzli[26].

[24] Obydwaj piloci otrzymali zaszyfrowany rozkaz dotarcia nad rzekę Cam Lo. Był on szyfrowany w postaci szarad dotyczących historii i kultury USA oraz zasad gry w golfa. Piloci zostali przejęci przez oddział Neavy Seals 12 i 13 kwietnia około 2 km od obszarów kontrolowanych przez siły amerykańskie. Zob. https://en.wikipedia.org/wiki/Rescue_of_Bat_21_Bravo oraz http://www.dtic.mil/dtic/tr/fulltext/u2/a220660.pdf [dostęp: 2 VII 2016].

[25] http://www.stosunkimiedzynarodowe.info/kalendarz_historyczny_na_dzien_2_czerwiec [dostęp: 23 VII 2013].

[26] https://pl.wikipedia.org/wiki/Zestrzelenie_F-117 [dostęp: 2 VII 2016].

Innym ważnym przykładem ze względu na sposób odzyskania personelu wojskowego jest uwolnienie załogi śmigłowca MH-60A Black Hawk dowodzonej przez Michaela Duranta. Śmigłowiec uczestniczył w operacji Gothic Serpent w Somalii i 3 października 1993 r. został trafiony granatnikiem przeciwpancernym. Rozbił się około 2 km na południowy wschód od celu operacyjnego w centrum Mogadiszu. Trójka członków załogi przeżyła wypadek, ale w jego wyniku wszyscy zostali ciężko ranni. Po zestrzeleniu śmigłowca dwóch żołnierzy służb specjalnych (Delta Force) próbowało chronić załogę przed atakiem band Somalijczyków, ale musieli się poddać, gdyż zabrakło im amunicji. Wraz z dwójką pilotów zostali zastrzeleni na miejscu zdarzenia. Trzeci ranny – dowódca załogi Michael Durant – został pojmany i był przetrzymywany przez 11 dni. W wyniku działań dyplomatycznych, najprawdopodobniej dzięki wpłaconemu okupowi, został uwolniony wraz z innym przetrzymywanym żołnierzem (Nigeryjczykiem) i przekazany Międzynarodowej Komisji Czerwonego Krzyża[27].

Kolejnym istotnym przypadkiem była bezprawna izolacja starszego szeregowego Jessiki Lynch. Została ona ujęta przez siły irackie 23 marca 2003 r. w trakcie ataku na konwój sił amerykańskich. W wyniku ataku zginęło 11 żołnierzy, a sześcioro (w tym Jessica Lynch) zostało wziętych do niewoli. Irakijczycy przekazali nagrania wideo z jeńcami wojennymi telewizji Al-Dżazira, co nadało sprawie wymiar polityczny. Szczegółowe informacje o miejscu przetrzymywania Lynch (szpital w Nasiriyah) wywiad amerykański uzyskał od lokalnych agentów. Ważna dla planowanych działań okazała się wiadomość o możliwości poddania kobiety torturom. Odbicie szeregowej Lynch przewidywało dokonanie ataku dywersyjnego, którego celem było odciągnięcie sił irackich od okolic szpitala. W konsekwencji pozwoliło to na przeprowadzenie desantu powietrznego na obiekty szpitalne, co z kolei umożliwiło odbicie rannej oraz przejęcie ciał ośmiu pozostałych żołnierzy[28].

Przedstawione *case studies* jednoznacznie wskazują na znaczenie odzyskania izolowanego personelu wojskowego. Wynika to przede wszystkim z wagi, jaką Amerykanie przywiązują do żołnierzy – specjalistów, ale równie ważny jest tu kontekst polityczny i medialny, rozumiany jako przekaz zarówno do własnego społeczeństwa, jak i do własnych sił zbrojnych[29]. Podobnie, chociaż z mniejszym ryzykiem i przy uwzględnieniu skali ewentualnych strat, są prowadzone działania ukierunkowane na odzyskiwanie osób przebywających w miejscu konfliktu lub działań operacyjnych.

W rejonach konfliktów oraz w rejonach objętych działaniami humanitarnymi na niebezpieczeństwo są najczęściej narażeni dziennikarze i pracownicy organizacji pomocowych. Porywaczami bywają przedstawiciele walczących stron lub zwykłe organizacje przestępcze. Najczęściej domagają się oni okupu, rzadziej wysuwają żądania o charakterze politycznym, np. dotyczące przerwania danej działalności lub uwolnienia przetrzymywanych członków swojej organizacji. Jednym ze sposobów reakcji jest podjęcie próby siłowego uwolnienia przetrzymywanych, ale ważne jest, aby informacje odnośnie do takiego rozwiązania zbyt wcześnie nie zostały udostępnione opinii publicznej. Do takiej sytuacji, niestety, doszło w przypadku obywatela Niemiec – pracownika firmy Bilfinger Berger – porwanego w styczniu 2012 r. w nigeryjskim

[27] http://mikedurant.com/ [dostęp: 23 VII 2013].

[28] *Jessica Lynch uwolniona przez siły specjalne USA*, [online], http://wiadomosci.wp.pl/kat,1356,title,-Jessica-Lynch-uwolniona-przez-sily-specjalne-USA,wid, 770022,wiadomosc.html [dostęp: 23 VII 2013].

[29] Informacja uzyskana przez autora niniejszego artykułu podczas różnego rodzaju szkoleń i spotkań służbowych z żołnierzami, funkcjonariuszami i pracownikami MON, MSW i MSZ.

Kano. Po zdobyciu informacji o planowanej próbie siłowego odzyskania zakładnika porywacze zamordowali przetrzymywanego[30].

Przykładem udanych działań ukierunkowanych na siłowe uwolnienie bezprawnie izolowanych osób cywilnych była operacja odbicia czwórki aktywistów szwajcarskiej pozarządowej organizacji charytatywnej Madair w Afganistanie (22 maja 2012 r.)[31]. Uwolnienia dokonali brytyjscy komandosi, którzy przeprowadzili pieszy rajd na terenie kontrolowanym przez porywaczy. Wszyscy członkowie grupy przestępczej zostali zabici[32].

Odzyskiwanie personelu może dotyczyć także osób nieprzebywających w strefie działań zbrojnych. Najczęściej są to akcje prowadzone w celu ewakuowania osób z miejsc potencjalnego zagrożenia i tym samym mające charakter prewencyjny. Równie często dotyczą one osób cywilnych, które stały się ofiarami działań grup przestępczych. Przykładem mogą być ewakuacje pracowników zatrudnionych przy eksploatacji pola naftowego w czasie konfliktu wewnętrznego w Libii, które przeprowadziły niemieckie, a następnie brytyjskie siły specjalne z wykorzystaniem samolotów transportowych[33].

Jako przykład działań zmierzających do uwolnienia personelu izolowanego i jednocześnie odzyskania mienia zagarniętego przez grupy przestępcze można uznać wszystkie formy zwalczania piractwa morskiego. Procedura odbicia jeńców jest generalnie taka sama: polega na wejściu sił specjalnych na pokład porwanej jednostki, aresztowaniu wszystkich osób przebywających na niej, a później – ich podziale na ofiary i członków grupy przestępczej. Wejście na pokład może nastąpić z wody – z wykorzystaniem łodzi półsztywnych – lub z powietrza – z wykorzystaniem śmigłowca – albo też w ramach działań kombinowanych. Jedyną zasadniczą różnicą jest sposób potraktowania piratów. Wynika to jednak z interpretacji zapisów prawa morza przez poszczególne państwa[34].

Najbardziej radykalnym przykładem operacji ukierunkowanej na odzyskanie personelu izolowanego i mienia zajętego przez piratów, właśnie w kontekście działań podjętych wobec sprawców, było, w ocenie autora, uwolnienie członków załogi rosyjskiego statku „Moskowskij Uniwiersitiet" (6 maja 2010 r.). Po zajęciu jednostki rosyjscy komandosi zgodnie z zapisami prawa morza powinni byli przekazać piratów władzom państwa, z którego tamci pochodzili. Nie mogąc jednak ustalić ich narodowości, Rosjanie uwolnili piratów na pełnym morzu, ale łódź, którą przestępcy mogli odpłynąć, pozbawili wyposażenia nawigacyjnego[35].

Jednym z najbardziej dobitnych przykładów tego, jak istotna dla rządzących i opinii publicznej jest sprawa odzyskiwania personelu izolowanego, jest przypadek izra-

[30] http://www.rp.pl/artykul/884766-Porywacze-zabili-uprowadzonego-Niemca.html [dostęp: 2 VII 2016].

[31] Operacja miała miejsce w zalesionym okręgu Szahr-e-Bozorgd, w pobliżu granicy afgańsko-tadżyckiej, w północno-wschodniej prowincji Badachszan. Porywacze zażądali okupu w wysokości 11 mln dolarów oraz całkowitego wycofania się pracowników zagranicznych organizacji pomocowych z tej prowincji.

[32] I. Krawczyk, *Komandosi SAS odbili w Afganistanie czworo zakładników* [online], http://www.rp.pl/artykul/886084.html [dostęp: 23 VII 2013].

[33] *Samoloty wojskowe ewakuowały 150 osób z libijskiej pustyni* [online], http://www.polskieradio.pl/5/3/Artykul/320039,Samoloty-wojskowe-ewakuowaly-150-osob-z-libijskiej-pustyni [dostęp: 23 VII 2013].

[34] http://www.tvn24.pl/wiadomosci-ze-swiata,2/rosjanie-wypuscili-piratow-ci-utoneli,133624.html [dostęp: 2 VII 2016].

[35] *Bułgarski ambasador uciekł przed porywaczami* [online], http://www.polskieradio.pl/5/3/Artykul/603179,Bulgarski-ambasador-uciekl-przed-porywaczami [dostęp: 23 VII 2013]. Ten przykład jest radykalnym rozwiązaniem, gdyż najczęściej piraci są w stanie dotrzeć do lądu, a na przykład niemieckie instrukcje nakazują ich odstawienie na ląd.

elskiego żołnierza Gilada Szalita. Został on porwany 25 czerwca 2006 r. po tym, jak terroryści z Hamasu zaatakowali posterunek armii izraelskiej w pobliżu Kerem Szalom, niedaleko granicy ze Strefą Gazy. Po około pięciu i pół roku przetrzymywania 18 października 2011 r. Szalit został wymieniony aż za 1027 palestyńskich więźniów[36]!

Przedstawione przykłady są charakterystyczne dla podstawowych form zagrożenia bezprawną izolacją. Zasadne jest jednak przywołanie kontekstu polskiego przez ukazanie sytuacji, w których uprowadzano naszych rodaków. Na potrzeby niniejszego opracowania za cezurę, od której będą wymienione wybrane przypadki, przyjęto lata 90. XX w.

Pierwszy nagłośniony przypadek uprowadzenia obywateli RP miał miejsce 30 listopada 1994 r., kiedy w Angoli porwano trzech Polaków, pracowników włosko-anglosaskiej spółki zajmującej się wyrębem lasów. Zostali oni schwytani przez partyzantów Frontu Wyzwolenia Enklawy Kabinda. Dzięki mediacji biskupa Paolino Madeli doszło jednak do ich uwolnienia.

Do kolejnego przypadku doszło 1 czerwca następnego roku w Jugosławii. Serbowie porwali dwóch polskich żołnierzy: płk. Janusza Kalbarczyka i ppłk. Wiesława Wojtasiaka. Zostali oni uwolnieni po 19 dniach przetrzymywania w charakterze żywych tarcz.

W 1996 r. miały miejsca trzy różne uprowadzenia polskich obywateli. Do pierwszego doszło 23 września. Uprowadzono wówczas dwójkę polskich alpinistów – Magdalenę Głowacką i Tomasza Nałęcz-Mrozowskiego. Porwania dokonali w Turcji partyzanci Partii Pracujących Kurdystanu. Polaków uwolniono po trzech dniach, ale niedługo potem zostali oni aresztowani przez tureckie władze i przez kilka tygodni byli przetrzymywani w więzieniu. Zarzucano im udzielanie pomocy kurdyjskim separatystom. Z powodu braku dowodów winy zostali jednak wypuszczeni. W dniu 17 grudnia polski ambasador w Peru Wojciech Tomaszewski został uwięziony przez partyzantów Rewolucyjnego Ruchu Tupaka Amaru w Limie. Wypuszczono go po pięciu dniach. Ostatni przypadek miał miejsce 25 grudnia, kiedy to porwano pięcioro polskich turystów w Jemenie. Dzięki mediacji jemeńskich władz zostali oni jednak po kilku dniach uwolnieni.

Do jednego z głośniejszych przypadków schwytania polskich obywateli doszło w dniach 17 grudnia 1997 r. – 10 lutego 1998 r. Uprowadzono wtedy pięciu Polaków: Marka Kurzyńca, Pawła Chojnackiego, Krzysztofa Galińskiego, Dominika Piaskowskiego i Marcina Thiela, którzy przebywali z pomocą humanitarną w Czeczenii. Osoby te zostały odnalezione i odbite przez czeczeńskie siły specjalne.

Również kolejnego uprowadzenia polskich obywateli dokonali czeczeńscy bojownicy. W dniu 9 sierpnia 1999 r. prof. Zofia Fiszer-Malanowska i doc. Ewa Marchwińska-Wyrwał zostały porwane w Dagestanie. Porywacze uwolnili kobiety po 208 dniach.

Dnia 1 marca 2000 r. w stolicy Jemenu – Sanie – został porwany polski ambasador Krzysztof Suprowicz. Do jego oswobodzenia doszło dzięki mediacji jemeńskich władz i głodówce, którą Suprowicz rozpoczął w niewoli.

Podczas wojny w Iraku miały miejsce co najmniej trzy przypadki izolacji polskich obywateli. W dniu 7 kwietnia 2003 r. dwaj polscy dziennikarze – Marcin Firlej i Jacek Kaczmarek – zostali zatrzymani przez Irakijczyków. Dzięki pomocy jednego z porywaczy następnego dnia udało im się uciec[37]. Z kolei 1 czerwca 2004 r. uprowadzono Jerzego Kosa.

[36] *Gilad Szalit wolny. Jest już w Izraelu* [online], http://www.jewish.org.pl/index.php/ru/izrael-mainmenu-61/4480-gilad-szalit-wolny-jest-ju-w-izraelu.html [dostęp: 20 V 2014].

[37] *Porwania Polaków* [online], http://www.dziennikpolski24.pl/pl/aktualnosci/swiat/404910-porwania-polaklw.html [dostęp: 22 VII 2013].

Odzyskał wolność po tygodniu przebywania w izolacji. Pod koniec tegoż roku, 28 października, została porwana Teresa Borcz. Również ona została uwolniona dzięki współpracy służb specjalnych[38].

W dniu 27 czerwca 2006 r. czwórka Polaków została uprowadzona przez maoistyczną partyzantkę w Nepalu w związku z odmową zapłacenia podatku[39], a 26 października 2007 r. porwano sześciu robotników naftowych, w tym dwóch naszych rodaków – pracowników włoskiego koncernu ENI. Po kilku dniach przetrzymywania nigeryjscy porywacze uwolnili zakładników[40].

Dnia 28 września 2008 r. na północy Pakistanu talibowie uprowadzili polskiego inżyniera Piotra Stańczaka. Pomimo starań podjętych przez polski rząd, 7 lutego 2009 r. P. Stańczak został zabity[41].

Od 26 marca do 10 kwietnia 2009 r. miało miejsce przetrzymywanie porwanego norweskiego chemikaliowca „Bow Asir", na którego pokładzie przebywało m.in. pięciu Polaków. W następnym roku doszło do dwóch uprowadzeń statków z Polakami na pokładzie: jednego – na brytyjskim chemikaliowcu „St. James Park", drugiego – na kutrze rybackim „Sakoba". Obu polskim marynarzom udało się odzyskać wolność – w pierwszym przypadku po sześciu, a w drugim – po pięciu miesiącach od porwania[42].

Dnia 10 sierpnia 2009 r. w walce z talibami w Usman Khel w Afganistanie zginął kpt. Daniel Ambroziński. Talibowie ukryli ciało kapitana i dopiero kilka godzin później udało się je odzyskać[43].

W dniu 31 sierpnia 2010 r. dwóch polskich turystów porwano w Libanie. Polacy zostali wciągnięci przez dwóch mężczyzn do samochodu w pobliżu miasta Baalbek w dolinie Bekaa i uprowadzeni. Gdy porywacze nie zatrzymali się w punkcie kontrolnym, libańscy żołnierze otworzyli ogień do pojazdu. Jeden z porywaczy zginął na miejscu, drugiemu udało się uciec. Porwanym Polakom nic się nie stało[44].

W tym samym roku doszło jeszcze do izolacji ośmiu obywateli RP po trzęsieniu ziemi na Haiti, zaginięcia 200 obywateli Polski w Chile, izolacji pięciu Polaków w Machu Picchu (Peru) – na skutek zejścia lawiny[45], oraz izolacji kilkunastu naszych rodaków spowodowanej przez siły natury w indyjskich Himalajach[46].

---

[38] G. Starzak, *Polacy coraz częściej stają się ofiarami porwań za granicą* [online], http://www.dziennikpolski24.pl/pl/aktualnosci/kraj/903679-polacy-coraz-czesciej-staja-sie-ofiarami-porwan-za-granica.html [dostęp: 22 VII 2013].

[39] *Nepal: uprowadzeni Polacy są bezpieczni* [online], http://www.rmf24.pl/fakty/swiat/news-nepal-uprowadzeni-polacy-sa-bezpieczni,nId,229631 [dostęp: 22 VII 2013].

[40] *MSZ: wśród porwanych w Nigerii jest dwóch Polaków* [online], http://www.rmf24.pl/fakty/swiat/news-msz-wsrod-porwanych-w-nigerii-jest-dwoch-polakow,nId, 188646 [dostęp: 22 VII 2013].

[41] *Porwany w Pakistanie krośnianin nie żyje* [online], http://www.krosno24.pl/informacje.php3?id=3108 [dostęp: 22 VII 2013]. Ciekawa analiza związana z uprowadzeniem i śmiercią Piotra Stańczaka ukazała się na stronach Biura Bezpieczeństwa Narodowego w maju 2009 r. Zob. *Analiza w sprawie oceny rzetelności działań podejmowanych przez urzędy państwowe w związku z uprowadzeniem i śmiercią Piotra Stańczaka* [online], https://www.bbn.gov.pl/download/1/2108/AnalizadotPStanczaka.pdf [dostęp: 12 IX 2016].

[42] *Raport Polskiej Służby Konsularnej za rok 2010*, Ministerstwo Spraw Zagranicznych, Warszawa 2011, s. 49.

[43] *Śmierć kapitana. Wojsko ujawnia przebieg bitwy* [online], http://news.money.pl/artykul/smierc;kapitana;wojsko;ujawnia;przebieg;bitwy,17,0,519697.html [dostęp: 22 VII 2013].

[44] *Liban: Polscy turyści porwani i uwolnieni* [online], http://swiat.newsweek.pl/liban-polscy-turysci-porwani-i-uwolnieni,63873,1,1.html [dostęp: 22 VII 2013].

[45] *Raport Polskiej Służby Konsularnej za rok 2010*, s. 44 i 45.

[46] Tamże, s. 51.

Wyzwaniem okazały się również wydarzenia z 2011 r., powszechnie znane jako „arabska wiosna", w związku z którymi nastąpiła konieczność ewakuacji znacznej liczby polskich obywateli z Libii, Tunezji, Egiptu i Syrii[47].

W roku 2012 znacznie wzrosła liczba ostrzeżeń o zdarzeniach mających wpływ na poziom bezpieczeństwa w określonych regionach świata, włącznie z zaleceniami dotyczącymi powstrzymania się od wyjazdów we wskazane miejsca. Ogółem Ministerstwo Spraw Zagranicznych wydało ich 107 (w 2011 r. opublikowano 44 ostrzeżenia)[48].

W dniu 24 lipca 2013 r. w Syrii miało miejsce uprowadzenie fotoreportera Marcina Sudera. Jak wynika z doniesień medialnych, tylko dzięki niebywałemu szczęściu udało mu się pod koniec października 2013 r. uciec, po czym został przewieziony do Polski[49].

Dnia 25 kwietnia 2014 r. w Słowiańsku na Ukrainie zostali uprowadzeni członkowie misji obserwacyjnej OBWE, w tym Polak mjr Krzysztof Kobielski. Został on uwolniony 3 maja 2014 r.[50]

W nocy z 12 na 13 października z misji w Baboua w Republice Środkowoafrykańskiej, położonej ok. 50 km od granicy z Kamerunem, został uprowadzony polski ksiądz Mateusz Dziedzic. Uwolniono go 26 listopada 2014 r. w następstwie prowadzonych negocjacji[51].

W dniu 24 grudnia 2015 r. zostali uwolnieni dwaj Polacy: operator Tomasz Głowacki i dziennikarz Marcin Mamoń, porwani 15 listopada 2015 r. Zostali oni uprowadzeni w Syrii przez syryjską Al-Kaidę[52].

Powyższe pobieżne zestawienie przykładów izolacji polskich obywateli wskazuje na wzrost zagrożenia uprowadzeniami. Potwierdza to również analiza wykonana przez szefa Zakładu Studiów Strategicznych Uniwersytetu Adama Mickiewicza w Poznaniu prof. Sebastiana Wojciechowskiego na zlecenie Ministerstwa Spraw Wewnętrznych i Administracji RP, stwierdzająca, że Polacy są coraz bardziej narażeni na porwania[53].

---

[47] *Raport Polskiej Służby Konsularnej za rok 2011*, Ministerstwo Spraw Zagranicznych, Warszawa 2012, s. 10 i 11.

[48] *Raport Polskiej Służby Konsularnej za rok 2012*, Ministerstwo Spraw Zagranicznych, Warszawa 2013, s. 9. Ważnym składnikiem mechanizmu reagowania służby konsularnej na sytuacje kryzysowe były działania informacyjne prowadzone przez MSZ i polskie placówki. Najważniejszym medium wykorzystywanym do tych potrzeb był Internet. Wzorem lat ubiegłych, urzędy konsularne na bieżąco monitorowały sytuację pod względem bezpieczeństwa w poszczególnych państwach i regionach świata. Na podstawie ich informacji, w zależności od rozwoju sytuacji, były podejmowane konkretne działania o charakterze prewencyjnym. Należały do nich ostrzeżenia dla podróżujących. Tamże, s. 9.

[49] E. Bieńczak, *Porwany w Syrii fotoreporter jest już w kraju! „Uciekł z niewoli"* [online], http://www.rmf24.pl/raport-konfliktwsyrii/fakty/news-porwany-w-syrii-fotoreporter-jest-juz-w-kraju-uciekl-z-niewo,nId,1050951 [dostęp: 15 XII 2013].

[50] *Uwolniony obserwator OBWE już w kraju; „Czuliśmy zagrożenie"* [online], http://www.tvp.info/15054762/uwolniony-obserwator-obwe-wiele-razy-czulismy-zagrozenie [dostęp: 10 XI 2015].

[51] *Polski misjonarz Ks. Mateusz Dziedzic uprowadzony w Afryce Środkowej został uwolniony* [online], http://wyborcza.pl/1,75477,17031625,Polski_misjonarz_Ks__Mateusz_Dziedzic_uprowadzony.html?disableRedirects=true [dostęp: 10 XI 2015].

[52] *Islamiści porwali dwóch Polaków. Są już wolni – akcja owiana tajemnicą* [online], http://niezalezna.pl/74320-islamisci-porwali-dwoch-polakow-sa-juz-wolni-akcja-owiana-tajemnica [dostęp: 29 XII 2015]; *Polak porwany przez Al-Kaidę o kulisach uwolnienia. „Służby działały profesjonalnie"* [online], http://niezalezna.pl/74354-polak-porwany-przez-al-kaide-o-kulisach-uwolnienia-sluzby-dzialaly-profesjonalnie [dostęp: 29 XII 2015].

[53] G. Starzak, *Polacy coraz częściej stają się ofiarami porwań za granicą* [online], http://www.dziennikpolski24.pl/pl/aktualnosci/kraj/903679-polacy-coraz-czesciej-staja-sie-ofiarami-porwan-za-granica.html [dostęp: 22 VII 2013].

Szkolenie SERE[54] jako element przygotowania personelu narażonego na ryzyko bezprawnej izolacji

Na bezprawną izolację są narażeni zarówno żołnierze prowadzący działania w rejonach konfliktów lub miejscach prowadzenia działań stabilizacyjnych czy humanitarnych, jak i osoby cywilne, które mogą paść ofiarą grup politycznych albo przestępczych pragnących uzyskać okup lub osiągnąć cele społeczne, polityczne bądź ekonomiczne. Zjawisko porwań dla okupu jest we współczesnym świecie jedną z najszybciej rozwijających się form działalności przestępczej. Jego skala wymusiła na państwach cywilizacji zachodniej podejmowanie skutecznych działań mających na celu odzyskanie personelu izolowanego. Jak wynika z wyżej wymienionych przykładów izolacji, w zdecydowanej większości dzięki systemom obowiązującym w danych państwach i działającym strukturom odzyskiwania personelu można uratować wielu obywateli swojego kraju i krajów sojuszniczych.

Tylko w jednym przytoczonym wyżej przypadku uprowadzony obywatel Niemiec poniósł śmierć, co było spowodowane tym, że terroryści dowiedzieli się o planowanej operacji uwolnienia zakładnika (w przypadku Piotra Stańczaka tego typu operacja nie była planowana). Na tym przykładzie widać, jak ważne jest zachowanie tajemnicy o przygotowywaniu operacji PR. Tak samo ważny jest czas. Im dłużej zwleka się z rozpoczęciem odzyskiwania personelu, tym trudniej jest ją skutecznie przeprowadzić, gdyż porwana osoba jest stale przewożona w bardziej niedostępne rejony kraju, w którym była porwana, lub poza jego granice. Potwierdza to przypadek izraelskiego żołnierza Gilada Szalita, który praktycznie każdego dnia był przewożony z jednego miejsca w inne. Ta metoda skutecznie uniemożliwiła namierzenie go przez izraelskie służby specjalne i zmusiła rząd tego kraju do negocjacji.

Skala zagrożenia bezprawną izolacją zarówno funkcjonariuszy państwa, jak i obywateli cywilnych powoduje, że niezbędne staje się upowszechnienie wśród potencjalnie zagrożonych osób procedur postępowania w sytuacji ich bezprawnej izolacji. Ze względu na możliwość wykorzystania sił państw trzecich do uwolnienia przetrzymywanych potrzebna jest uniwersalizacja takich procedur. Stąd pogląd, że zasady postępowania w przypadku bezprawnej izolacji powinny opierać się na międzynarodowych rozwiązaniach, a te w pełni gwarantują szkolenia SERE. Obecnie takie szkolenia powinny odbywać się we wszystkich służbach, instytucjach i firmach prowadzących aktywność polityczną, społeczną i gospodarczą, w regionach uznawanych za obszary ryzyka. Takie szkolenia uczą, jak postępować w sytuacji zaginięcia, bezprawnej izolacji oraz ewentualnej samodzielnej ucieczki z miejsca przetrzymywania. Zakres szkoleń obejmuje: problematykę walki ze stresem, klasyczny survival (m.in. sposoby rozpalania ognia, budowy schronienia), metody unikania schwytania, stosowania oporu po ewentualnym ujęciu, metody przygotowania ucieczki z miejsca izolacji i zasady postępowania w czasie próby odzyskania personelu przez zespół ratunkowy[55].

[54] Kursy SERE są prowadzone w siłach zbrojnych większości państw członkowskich Paktu Północnoatlantyckiego z osobami narażonymi na ryzyko zaginięcia. Pierwszymi szkolonymi byli piloci wojskowi. Nazwa SERE jest skrótem utworzonym od pierwszych liter angielskich słów *survival* – przetrwanie (bytowanie), *evasion* – unikanie, *resistance* – opór (przeciwdziałanie wykorzystaniu), *escape* (*extraction*) – ucieczka (odzyskanie).

[55] K. Falandys, *Uwarunkowania prawne*..., s. 139.

Zakres szkolenia SERE dla personelu wojskowego

Szkoleniu SERE podlega zwłaszcza personel wojskowy uczestniczący w misjach stabilizacyjnych i humanitarnych oraz w działaniach zbrojnych poza granicami kraju. W Polsce takie szkolenie przechodzą żołnierze Wojsk Specjalnych[56] (od niedawna również pozostali żołnierze), ale w odniesieniu do żołnierzy uczestniczących w misjach wojskowych należy uznać, że mają oni ograniczoną wiedzę oraz umiejętności umożliwiające przeżycie i przetrwanie w izolacji. Jak zaznaczono powyżej, zasadna jest uniwersalność takiego szkolenia w warstwie merytorycznej. W państwach Paktu Północnoatlantyckiego ma ono zostać oparte na przygotowanym dokumencie *Polityka NATO w zakresie odzyskiwania personelu.* Jego zapisy nakładają na państwa członkowskie obowiązek prowadzenia takiego szkolenia przed wysłaniem personelu na misję[57]. Jak można się przekonać po zapoznaniu się z poniższym schematem, szkolenie SERE – co szczegółowo opisuje poniższy rysunek – dzieli się na trzy poziomy, tj. A, B, C, oraz na dwa poziomy instruktorskie.

Schemat 3. Szkolenia SERE.

Źródło: *Personnel Recovery,* JAPCC, 2011, s. 22.

SERE poziom A to przede wszystkim szkolenie teoretyczne, traktowane jako szkolenie wstępne. Tego typu kurs przechodzi personel przed pierwszym skierowaniem do udziału w misji lub operacji, a jego celem jest zapoznanie uczestników ze zbiorem podstawowych taktyk, technik, procedur i działań SERE. Poziom B to średnio zaawansowany pakiet szkolenia przeznaczony dla personelu wojskowego i cywilnego objętego średnim poziomem ryzyka zajścia zdarzenia. Określa się je jako średnie zagrożenie izolacją (ang. Medium Risk of Isolation – MRI). Szkolenie SERE poziom C natomiast obejmuje zaawansowany pakiet szkolenia praktycznego i jest prowadzone dla personelu wojskowego oraz cywilnego objętego wysokim poziomem ryzyka zajścia zdarzenia izolacji

[56] Informacja uzyskana przez autora artykułu podczas szkoleń i spotkań służbowych z żołnierzami, funkcjonariuszami i pracownikami MON, MSW i MSZ.

[57] Dokument ma klauzulę tajności i jego treść nie może być przywołana w niniejszym opracowaniu. Powyższe założenie zostało jednak ogłoszone jako podstawa do podjęcia prac nad jego przygotowaniem.

(ang. High Risk of Isolation – HRI). Ten poziom obejmuje również szkolenie w zakresie praktycznego przeciwdziałania wykorzystaniu w przypadku schwytania[58].

Immamentnym zagadnieniem poruszanym na szkoleniach SERE wszystkich trzech poziomów jest umiejętność stworzenia dokumentu EPA[59] zawierającego informacje pomocne dla sił odzyskujących, takie jak np.: informacje dotyczące sposobów komunikowania się z siłami odzyskującymi, informacje umożliwiające potwierdzenie naszej tożsamości, dotyczące sposobów podawania kierunku przemieszczania się itp. W tym dokumencie powinno się również nanieść mapkę terenu, na którym zamierzamy przebywać wraz ze wskazaniem ewentualnego kierunku przemieszczania się w przypadku izolacji. Rozróżniamy podział EPA na EPA GROUND (stosowany w przypadku osób poruszających się po ziemi) i EPA AIR (stosowany w przypadku osób przemieszczających się z wykorzystaniem statków latających)[60].

Podsumowanie

Jak wykazano w niniejszym opracowaniu, zagrożenie wystąpieniem izolacji z powodu uprowadzenia dla okupu lub zamachu terrorystycznego prowadzącego do sytuacji zakładniczej jest zjawiskiem, które w ostatnich czasach przybrało na sile. Do izolacji dochodzi m.in. w celu zbierania funduszy na działalność terrorystyczną[61]. Wcześniej izolacja w zdecydowanej większości dotyczyła żołnierzy biorących udział w konfliktach zbrojnych. W okresie II wojny światowej odnosiła się szczególnie do żołnierzy japońskich oraz amerykańskich i była związana z ogromnym teatrem działań wojsk, dużą liczbą wysp oraz trudno dostępnym, nieodkrytym terenem, na którym toczyły się walki, a także tempem przemieszczania się wojsk. Również w okresie wojny wietnamskiej na rozległych zalesionych terenach Półwyspu Indochińskiego zaginęło wielu żołnierzy armii amerykańskiej, którzy do dziś są poszukiwani przez amerykański rząd.

Wzmagający się w ostatnich czasach konflikt o podłożu religijno-politycznym i kampania antyterrorystyczna prowadzona przez państwa należące do NATO i UE przeciwko wybranym państwom Bliskiego i Dalekiego Wschodu, a także niektórym krajom Afryki i Ameryki Południowej spowodowała, że obywatele państw zachodnich stali się częstym celem porwań i zamachów terrorystycznych. W związku z powszechną globalizacją światowe koncerny wysyłają swoich (notabene nieuzbrojonych) pracowników w zagrożone rejony świata, gdzie tamci padają ofiarami różnego rodzaju konfliktów. Również porwania załóg statków pływających są dziś częstym zjawiskiem w niektórych krajach Afryki.

Powyższe okoliczności wymusiły na państwach cywilizacji zachodniej podjęcie skutecznych działań mających na celu odzyskiwanie personelu izolowanego. Aby zwiększyć szanse na odzyskiwanie takiego personelu niezbędne jest wdrożenie szkoleń SERE

[58] K. Falandys, *Uwarunkowania prawne*..., s. 139.

[59] EPA (ang. *Evasion Plan of Action*) – plan unikania i ewakuacji na podstawie zaplanowanego korytarza unikania. Plan unikania i ewakuacji powinien opracować personel, każdorazowo na czas działania w przydzielonym rejonie. W razie konieczności jest on przekazywany siłom odzyskującym. Po zakończeniu działań „Plany Unikania Przeciwnika – EPA", ze względu na poufny charakter zawartych w nich danych, muszą być natychmiast zniszczone.

[60] K. Falandys, *Uwarunkowania prawne*..., s. 140.

[61] Międzynarodowym aktem prawnym poświęconym uprowadzeniom jest konwencja z 18 XII 1979 r. przeciwko braniu zakładników uchwalona w ramach ONZ, która została ratyfikowana przez Polskę 13 III 2000 r. i w stosunku do Polski weszła w życie 24 VI 2000 r. Oprócz naszego kraju do konwencji przystąpiło 87 państw. W celu uniknięcia problemów z ekstradycją przestępców dokonujących uprowadzeń podpisano *Europejską konwencję o zwalczaniu terroryzmu sporządzoną w Strasburgu dnia 27 stycznia 1977 r.* (Dz.U. z 1996 r. Nr 117 poz. 5570, w której umawiające się państwa przyjęły, że dla celów ekstradycyjnych nie uważa się uprowadzeń ani przestępstw polegających na wzięciu zakładników za przestępstwa polityczne lub pozostające w związku z przestępstwem politycznym.

we wszystkich służbach, instytucjach i firmach realizujących zadania poza granicami państwa. Szkolenia SERE należy zaliczyć do działań wyprzedzających, podejmowanych równolegle z przedsięwzięciami natury dyplomatycznej, polegającymi na zacieśnianiu współpracy z miejscowymi wywiadami i siłami bezpieczeństwa.

Ponadto ważne jest, aby szkolenia z zakresu SERE były prowadzone zarówno dla żołnierzy, jak i osób cywilnych, i miały zunifikowane programy. Różnica powinna dotyczyć tylko obszaru specyficznych umiejętności wybranych grup, np. żołnierzy jednostek specjalnych, funkcjonariuszy służb specjalnych, dyplomatów oraz przewidywanego terenu działania. Jednolite powinny być natomiast procedury zachowania w przypadku przebywania w izolacji oraz w czasie operacji odzyskiwania. Jeśli te działania pozwolą uniknąć choć jednego przypadku izolacji lub w razie jego wystąpienia pomogą przetrwać osobie nią dotkniętej, to będzie to świadczyło o sukcesie całego przedsięwzięcia. Zasadą powinno być także uznanie każdego indywidualnego przypadku bezprawnej izolacji za zdarzenie ważne dla funkcjonowania państwa. Jego zadaniem powinno być podjęcie działań niezbędnych dla ratowania swoich obywateli i zapewnienie ich uwolnienia.

Bibliografia:

Publikacje zwarte i artykuły prasowe:

1. *Analiza w sprawie oceny rzetelności działań podejmowanych przez urzędy państwowe w związku z uprowadzeniem i śmiercią Piotra Stańczaka,* Warszawa 2009, BBN.
2. Falandys K., *Uwarunkowania prawne determinujące kształt Narodowego Systemu Odzyskiwania Obywateli Rzeczypospolitej Polskiej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2015, nr 2, Wrocław 2015.
3. Falandys K., *Zjawisko izolacji (bezprawnego przetrzymywania) – jego skala i regionalizacja,* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 178–195.
4. *Koncepcja i ogólne zasady funkcjonowania Narodowego Systemu Odzyskiwania Personelu Wojskowego*, Warszawa 2008, Ministerstwo Obrony Narodowej, Sztab Generalny WP.
5. *Odzyskiwanie izolowanego personelu (DD/3.3.9)*, Warszawa 2010, Ministerstwo Obrony Narodowej, Sztab Generalny WP.
6. *Personnel Recovery*, b.m.w. 2011, Joint Air Power Competence Centre.
7. Poray A., *Jugosławia 1999, cz. II*, „Skrzydlata Polska" 2011, nr 6.
8. *Raport Polskiej Służby Konsularnej za rok 2010*, Warszawa 2011, Ministerstwo Spraw Zagranicznych.
9. *Raport Polskiej Służby Konsularnej za rok 2011*, Warszawa 2012, Ministerstwo Spraw Zagranicznych.
10. *Raport Polskiej Służby Konsularnej za rok 2012*, Warszawa 2013, Ministerstwo Spraw Zagranicznych.

Akty prawne:

1. *Europejska konwencja o zwalczaniu terroryzmu, sporządzona w Strasburgu dnia 27 stycznia 1977 r.* (Dz.U. z 1996 r. Nr 117 poz. 557).
2. *Konwencja o traktowaniu jeńców wojennych (III konwencja genewska)*, Genewa, 12 VIII 1949 r. (Dz.U. z 1956 r. Nr 38 poz. 175, załączniki).
3. *Międzynarodowa konwencja przeciwko braniu zakładników*, Nowy Jork, 10 XII 1979 r., (Dz.U. z 2000 r. Nr 106 poz. 1123).

Źródła internetowe:

1. http://www.bbn.gov.pl/.
2. http://www.dziennikpolski24.pl/.
3. http://www.jewish.org.pl/.
4. http://www.krosno24.pl/.
5. http://mikedurant.com/.
6. http://news.bbc.co.uk/.
7. http://money.pl/.
8. http://newsweek.pl/.
9. http://niezalezna.pl/.
10. http://nytimes.com/.
11. http://www.polskieradio.pl/.
12. http://www.rmf24.pl/.
13. http://www.rp.pl/.
14. http://www.stosunkimiedzynarodowe.info/.
15. http://www.tvn24.pl/.
16. http://tvp.info/.
17. http://wp.pl/.
18. http://wyborcza.pl/.

Abstrakt

W niniejszym artykule skupiono się na zaprezentowaniu możliwości odzyskiwania personelu (Personnel Recovery – PR) jako formy przeciwdziałania bezprawnej izolacji osób. W tym celu wyjaśniono istotę przedsięwzięć określanych jako „odzyskiwanie personelu" oraz metody odzyskiwania personelu i sprzętu w przypadku zdarzeń o charakterze niemilitarnym i militarnym. Znaczną część artykułu poświęcono analizie operacji odzyskiwania personelu wojskowego i cywilnego (*case study*). Omówiono również poszczególne poziomy szkolenia SERE będącego elementem szkolenia personelu narażonego na ryzyko bezprawnej izolacji oraz zaprezentowano zakres tego szkolenia, realizowanego przez personel wojskowy.

Słowa kluczowe: odzyskiwanie personelu, personel izolowany, bezprawna izolacja, operacje poszukiwawczo-ratunkowe, SERE.

Abstract

In the article the author focused on presenting the possibility of personnel recovery (PR) as a form of unlawful people isolation. For this purpose the author explained personnel recovery essence, methods of personnel and equipment recovery in case of non-military and military events. The important issue in the article is the analysis of the military and civilian personnel recovery operations (case study). The author also discussed the basics of SERE training, which is part of the training of personnel exposed to the risk of unlawful isolation. He also presented the scope of the SERE training conducted by military personnel.

Keywords: personnel recovery, isolated personnel, unlawful isolation, operations search and rescue, SERE.

Janusz Wasilewski

Przestępczość w cyberprzestrzeni – zagadnienia definicyjne

Choć takie wyrażenia, jak przestępczość komputerowa czy cyberprzestępczość nie należą w obowiązującym stanie prawnym do polskich wyrażeń ustawowych, nie sposób nie zgodzić się z twierdzeniem, że odnoszą się do jednego z największych zjawisk przestępnych dzisiejszych czasów. Zgodnie z aktualnymi szacunkami łączna wartość globalnych strat ponoszonych na skutek popełniania cyberprzestępstw już od kilku lat jest porównywalna do wartości całego rynku narkotykowego i plasuje się na poziomie 388 mld dolarów rocznie[1]. Jak wynika z przeprowadzonych badań, ofiarami wszelkich form nielegalnej działalności w Internecie (w tym także związanej z rozsiewaniem wirusów komputerowych oraz innych typów złośliwego oprogramowania) pada rocznie pół miliarda ludzi, co w skali światowej daje średnią około 14 ofiar tego typu bezprawnej aktywności na sekundę! W Polsce w 2010 r., według oficjalnych danych Policji[2], zgłoszono prawie osiem tysięcy przestępstw popełnionych w sieci, z czego ponad sześć tysięcy – oszustw. W 2012 r. ogólna liczba przestępstw komputerowych oscylowała już na poziomie 19 tys. (około 3/4 przypadków oszustw), aby w 2015 r. przekroczyć 20 tys. Należy zaznaczyć, że ogromna liczba przestępstw komputerowych, które potęgują zagrożenie, pozostaje ukryta w szarej strefie i wymyka się wszelkim statystykom[3]. Specyfika przestępstw popełnianych w cyberprzestrzeni powoduje bowiem, że wiele tego typu czynów pozostaje niewykrytych lub nie jest poprawnie identyfikowanych jako przestępstwo. Powodem takiego stanu rzeczy jest z jednej strony nierzadko sam użytkownik komputera lub innego urządzenia, który nie zdaje sobie sprawy z tego, że padł ofiarą przestępstwa (brak „technicznej" świadomości), z drugiej zaś zdarzenia, które są wykrywane i poprawnie kwalifikowane jako przestępne, nie zawsze zostają zgłoszone do ścigania. W przypadku dużych firm zachowanie w tajemnicy informacji o tym, że uległy one skutecznemu atakowi hackerskiemu, w którym przełamano zbyt słabe zabezpieczenia infrastruktury teleinformatycznej przedsiębiorstwa, może nie tylko być próbą ochrony swojego wizerunku, lecz także sposobem na uniknięcie ewentualnych konsekwencji odszkodowawczych (np. informacja o cyberataku na bank, w którego wyniku mogło dojść do wycieku poufnych danych jego klientów).

W świetle przytoczonych informacji suma zysków potencjalnie generowanych przez cyberprzestępczość czyni ten rodzaj działalności jedną z najbardziej lukratywnych gałęzi przestępczości w ogóle i przyciąga nie tylko drobnych złodziei czy oszustów, lecz także cybergangi specjalizujące się w nowoczesnych technologiach lub „konwencjonalne", zorganizowane grupy przestępcze, które chcą rozszerzyć swój dotychczasowy

[1] Pierwotne dane z raportu *Norton Cybercrime Report 2011*, dostępnego w wersji elektronicznej na stronie internetowej pod adresem: http://pl.norton.com/cybercrimereport/ [dostęp: 20 VI 2016].

[2] Dane pochodzą z oficjalnej strony internetowej Policji, dostępnej pod adresem: http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html oraz http://statystyka.policja.pl/st/informacje/85606,Przestepstwa-w-sieci.html [dostęp: 20 VI 2016].

[3] M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1; opracowanie dostępne również na stronie internetowej pod adresem: http://prawo.vagla.pl/node/905.

obszar aktywności. W każdym z tych przypadków cyberprzestępczość pozostaje działalnością tanią, stwarzającą przestępcom ogromne możliwości (także np. terrorystyczne), a przy tym wciąż uważaną za zapewniającą większe bezpieczeństwo niż inne, tradycyjne formy działalności przestępnej, i to zarówno przed wymiarem sprawiedliwości, jak i działaniami innych, rywalizujących przestępców[4]. Można powiedzieć, że wszelkie słabości cyberprzestrzeni stają się automatycznie siłą napędową nowoczesnych przestępców.

Mimo że określenie cyberprzestępczość[5] – oraz inne wyrażenia stosowane do opisu poruszanego tu zjawiska – wciąż nie stanowi kategorii prawnej, to z uwagi na prezentowane w literaturze przedmiotu jego zakres[6], specyfikę oraz konieczność tworzenia i poprawnego stosowania prawa należy uznać, że zapewnienie skutecznego zwalczania zagrożeń w cyberprzestrzeni uzasadnia, a wręcz wymaga, prowadzenia szerokiej analizy całej gałęzi związanej z tą dziedziną działalności przestępnej i pojęć odnoszących się do czynów wchodzących w jej skład.

Artykuł jest próbą uporządkowania stosowanych terminów oraz udzielenia odpowiedzi na podstawowe pytania o to, czym jest cyberprzestępstwo, jakie są jego rodzaje oraz co je odróżnia od innych kategorii przestępstw[7]. Tak wskazana problematyka pozostaje w ścisłym związku z określeniem, jakie (jak ujęte?) dobra prawnie chronione są przedmiotem zamachu tego rodzaju działalności przestępnej. Podobnie jak w przypadku określania cyberprzestrzeni, także i te rozważania nie mogą ograniczać się wyłącznie do płaszczyzny prawnej, która bez kontekstu technologicznego pozostaje zawieszona w próżni. Definicja cyberprzestępczości jest prezentowana oraz rekonstruowana na podstawie wielu rozwiązań przyjętych na gruncie piśmiennictwa, aktów okołoprawnych oraz powszechnie obowiązujących przepisów, zarówno krajowych, w tym także polskich, jak i powstałych w ramach inicjatyw międzynarodowych. Do rozważań wprowadzono także dodatkowe pojęcia wspomagające opis cyberprzestępczości – cyberincydent oraz cyberatak.

Analiza stosowanych pojęć

Brak jednolitych rozwiązań prawnych nakierowanych na zapobieganie oraz zwalczanie nowoczesnych form przestępczości komputerowej, wynikający w dużej mierze

[4] Zob. *Fighting Cybercrime: Technical, Juridical and Ethical Challenges*. Opracowanie dostępne na stronie internetowej pod adresem: http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.

[5] Termin powstał jeszcze na początku lat 90. XX w. Oficjalnie został użyty przez tzw. Grupę z Lyon, działającą w ramach grupy G8, której zadaniem było prowadzenie prac analitycznych nad nowymi formami przestępczości, za: S. Perrin, *Cybercrime*, w: A. Ambrosi, V. Peugeot, D. Pimienta, *Word Matters: multicultural perspectives on information societies*, Caen 2005. Opracowanie dostępne także w wersji elektronicznej na stronie internetowej pod adresem: http://media.mcgill.ca/en/word_matters. A. Adamski zwraca uwagę na zastosowanie omawianego terminu w 1996 r. przez L.E. Quarantiellego, w: tenże, *Cyber Crime: How to protect yourself from computer criminals*, Wisconsin 1996; A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 30 i nast.

[6] Niektórzy autorzy podają wręcz w wątpliwość, czy czyny określane pojęciami odnoszącymi się do cyberprzestępczości zachowują w rzeczywistości homogeniczność. Zob. np. U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, nr 3, s. 6, za: A. Kania, *Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni*, e-biuletyn CBKE 1/2009, Wrocław 2009, s. 8. Tekst opracowania jest dostępny również na stronie internetowej pod adresem: http://bibliotekacyfrowa.pl/Content/34350/Oszustwo_komputerowe.pdf.

[7] Stosowanie klasycznego dorobku prawa karnego wobec cyberprzestępczości zaznacza K. Dobrzeniecki w: tenże, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 61 i nast.

z niechęci (lub niezdolności) państw do wypracowywania wspólnych stanowisk oraz spóźnionego podjęcia odpowiednich inicjatyw legislacyjnych, spowodował wytworzenie wyjątkowo niespójnej oraz niejednorodnej siatki pojęciowej z obszaru cyberprzestępczości. Nieco ironicznie zauważa się już od dawna w piśmiennictwie, że pojęcia stosowane w tym zakresie mają często charakter bardziej publicystyczny niż naukowy[8]. Ten pogląd należy, niestety, podzielić. Tym samym wyrażeniom często są nadawane różne, krzyżujące się zakresowo znaczenia. Definicje często są tworzone ad hoc, przy okazji tworzenia nowego dokumentu lub opracowania. Na domiar złego ustawiczne zmiany spowodowane rozwojem nowoczesnych technologii, stanowiące przecież fundament cyberprzestrzeni oraz nowoczesnych usług świadczonych za pośrednictwem sieci komputerowych, również nie sprzyjają jednoznaczności oraz trwałości budowanych definicji[9]. Zasadne jest zatem, aby podjąć próbę uporządkowania istniejącego stanu rzeczy.

Pojęcie nadużycia komputerowego

W ujęciu historycznym proces formułowania nowych, specyficznych pojęć odnoszących się do przestępczości komputerowej rozpoczął się jeszcze w połowie lat 70. XX w. Był to okres pierwszych głośnych, medialnych doniesień o atakach hackerskich, które uświadomiły nie tylko szerszej opinii publicznej, lecz także przedstawicielom władz rządowych pojawienie się nowych cyberzagrożeń. Warto dodać – zagrożeń, które mogą powodować jak najbardziej realne straty finansowe. W latach 70. spopularyzowało się także określenie hacker, które negatywnie zaczęło się kojarzyć dopiero w połowie następnego dziesięciolecia[10].

Jednym z pierwszych, szeroko rozpoznawanych opracowań poświęconych zwalczaniu nowoczesnych form przestępczości stała się książka autorstwa Donna Parkera zatytułowana *Crime by Computer* (*Przestępstwo z wykorzystaniem komputera*) wydana w 1976 r.[11] Wbrew tytułowi autor skupił się w niej wokół pojęcia nadużycie komputerowe[12], które rozumiał jako (…) *każdy incydent polegający na zamierzonym zachowaniu, którego ofiara poniosła lub mogła ponieść szkodę, zaś sprawca odniósł lub mógł odnieść zysk, wiążący się z komputerami*[13]. Wskazał także cztery rodzaje przeznaczenia komputera lub zgromadzonych w nim danych w tak określonym nadużyciu:

1) jako przedmiot ataku,
2) jako narzędzie wytwarzające specyficzne środowisko lub nowe formy dóbr prawnych podlegających ochronie,
3) jako środek lub narzędzie służące do popełnienia nadużycia,
4) jako symbol użyty w celu zastraszenia lub dokonania oszustwa[14].

---

[8] Zob. np. A. Adamski, *Prawo karne komputerowe*…, s. 30.

[9] Trudnościom w budowaniu odnośnych definicji była poświęcona nawet odrębna część *Zalecenia Nr R(89)9 Komitetu Ministrów Rady Europy z 1989 r. w sprawie przestępczości komputerowej*.

[10] Słowo „*hacker*" oznaczało pierwotnie (znaczenie pozytywne) osobę o wysokich kwalifikacjach komputerowych, potrafiącą w szerokim zakresie wykorzystywać możliwości nowych technologii informatycznych.

[11] D.B. Parker, *Crime by Computer*, Nowy Jork 1976 (tłumaczenie tytułu – własne).

[12] W oryginale: *computer abuse.*

[13] W oryginale: *any incident involving an intentional act where a victim suffered or could have suffered a loss, and a perpetrator made or could have made a gain and is associated with computers*. Cyt. za: A. Reyes, *Cyber Crime Investigations*, bmw, [USA] 2007, s. 25 (tłumaczenie własne).

[14] Tamże, s. 25.

Choć wymienione rodzaje przeznaczenia komputera i zgromadzonych w nim danych częściowo przeplatały się zakresowo, każdy z nich odnosił się do różnych form dokonywania nadużyć. Pierwszy nawiązywał do ochrony samych systemów teleinformatycznych oraz przechowywanych w nich danych w postaci elektronicznej, które mogą stać się celem działania przestępnego. Drugi, zdecydowanie wyprzedzający swoje czasy, nawiązywał do nowego sposobu postrzegania dóbr prawnie chronionych, które wraz z rozwojem cyberprzestrzeni mogą wyrażać się w zupełnie nowych, nieznanych dotychczas formach, wykraczając poza postać typowych praw, ruchomości, nieruchomości oraz dóbr osobistych. Trzeci rodzaj przeznaczenia można odnieść do kategorii nadużyć komputerowych sensu stricto, w których komputer staje się niezbędnym narzędziem do popełnienia przestępstwa (które może być skierowane także przeciwko dobrom prawnym mającym wyłącznie swój cyfrowy wymiar), czwarty zaś odwoływał się do tych czynów, dla których komputer staje się wyłącznie środkiem komunikacyjnym, samo zaś zachowanie można kwalifikować jako przejaw klasycznych form czynów bezprawnych (jak np. oszustwo czy zniesławienie). Pomimo tak szerokiego ujęcia, żaden z wymienionych rodzajów przeznaczenia nie odnosił się jednak bezpośrednio do wykorzystywania komputerów jako samodzielnych źródeł dowodowych, które mogą dostarczać dowodów także w sprawach niezaliczających się ściśle do kategorii nadużyć komputerowych. Z uwagi na czasy, w których definicja była budowana (przed powstaniem Internetu), żadne z ujęć nie odwoływało się także do wykorzystania komputera w celu przeprowadzania ataków za pośrednictwem sieci.

W przytoczonej definicji proponuje się, aby dwiema głównymi cechami nadużycia komputerowego były jego umyślność oraz jednoczesna strata bądź korzyść majątkowa, powstające na skutek przestępstwa. Innymi słowy – n a d u ż y c i e m k o m p u t e r o w y m nie mógł stać się ani czyn niezamierzony, jak np. nieumyślne uszkodzenie zasobów chronionych, ani taki, który w ogóle nie zakładał możliwości odniesienia korzyści przez jego sprawcę, jak akt wandalizmu polegający na skasowaniu lub podmianie plików strony internetowej. Oba wskazane wymogi, stanowiące przejaw utożsamiania nadużyć komputerowych z przestępczością nastawioną na określone korzyści majątkowe, należy wiązać z dawnym rozumieniem przestępczości komputerowej jako przestępczości wysokospecjalistycznej, wymagającej świadomego podejmowania skomplikowanych operacji.

Pojęcie n a d u ż y c i e k o m p u t e r o w e znalazło się w wydanym w 1986 r. raporcie Organizacji Współpracy Gospodarczej i Rozwoju *(*OECD) zatytułowanym *Computer -related Crime: Analysis of Legal Policy* (*Przestępstwa związane z komputerem: analiza polityki legislacyjnej*)[15]. Czyn n a d u ż y c i a k o m p u t e r o w e g o został roboczo określony w raporcie jako *Każde zachowanie niezgodne z prawem, nieetyczne lub nieuprawnione, odnoszące się do automatycznego przetwarzania oraz przekazywania danych*[16].

Oprócz przytoczonej wyżej definicji nadużycia komputerowego w raporcie OECD wymieniono także enumeratywnie i określono pięć kategorii nadużyć komputerowych, które powinny być penalizowane we wszystkich porządkach prawnych. Zaliczono do nich: oszustwo komputerowe (nastawione na uzyskiwanie korzyści majątkowych), fałszerstwo komputerowe, zakłócenie poprawnego funkcjonowania systemu (sabotaż), nielegalne kopiowanie programów komputerowych oraz nielegalny dostęp do systemu

[15] *Computer-related Crime: Analysis of Legal Policy*, OECD, Paris 1986 (tłumaczenie tytułu – własne).

[16] Tłumaczenie własne. W oryginale: *Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data*.

komputerowego uzyskany przez naruszenie zabezpieczeń lub w celu wyrządzenia szkody[17]. Wykaz typowych nadużyć komputerowych został zatem przedstawiony wyłącznie w kontekście czynów, które powinny podlegać kwalifikacji karnej, w odróżnieniu od podejścia, które zaprezentowano w ramach budowy definicji nadużycia komputerowego. Jednocześnie łączył kategorie ściśle karnistyczne (fałszerstwo, włamanie) z ochroną praw autorskich, nazywając nadużyciem komputerowym także kopiowanie programów (dziś zwane potocznie piractwem komputerowym), które może być dokonywane z całkowitym pominięciem komputerów. Na marginesie warto zaznaczyć, że oprócz omawianego tu pojęcia w raporcie OECD posługiwano się również kategorią przestępstwa związanego z komputerem, które, choć odgrywało drugorzędną rolę, pojawiało się z niewyjaśnionych przyczyn w samym tytule dokumentu.

Równolegle do pojawienia się pojęcia nadużycie komputerowe w raporcie OECD w 1986 r. to pojęcie pojawiło się w obszernej amerykańskiej kodyfikacji prawa nastawionej na kompleksowe zwalczanie zagrożeń komputerowych. Przybrała ona formę ustawy zatytułowanej *Computer Fraud and Abuse Act*[18], której przepisy stały się podstawowym narzędziem amerykańskiego wymiaru sprawiedliwości w walce z przestępstwami popełnianymi z wykorzystaniem komputera. Co istotne, pomimo historycznej już daty wprowadzenia tej ustawy, pozostaje ona aktem wciąż obowiązującym, co nadaje prowadzonym rozważaniom waloru aktualności. Od chwili wejścia w życie ustawa była wielokrotnie nowelizowana, m.in. w latach 1989, 1994, 1996, 2001 (ustawą *PATRIOT Act*[19] wydaną po zamachu na WTC) oraz 2008 (ustawą *Identity Theft Enforcement and Restitution Act*[20])[21]. Przepisy wprowadzone ustawą z 1986 r. uzupełniły także sekcję 1030 (stworzoną w 1984 r.) 47. rozdziału 18. tytułu amerykańskiego *United States Code*[22]. W tej sekcji pierwotnie była uregulowana penalizacja szczególnych przypadków uzyskania bezprawnego dostępu do informacji rządowych, przede wszystkim informacji niejawnych oraz informacji finansowych, w sytuacji gdy te informacje były przetwarzane w komputerach należących do agend rządowych[23]. Sama sekcja 1030 została zatytułowana *Oszustwo oraz podobna działalność w powiązaniu z komputerami*[24].

Ustawą *Computer Fraud and Abuse Act* wprowadzono penalizację wielu czynów stypizowanych, które, zgodnie z samą nazwą aktu normatywnego, zostały określone jako „nadużycia oraz oszustwa komputerowe". W odniesieniu do zastosowanej

[17] A. Adamski, *Prawo karne komputerowe*…, s. 6.

[18] W tłumaczeniu własnym: *Ustawa o komputerowym oszustwie oraz nadużyciu*. Tekst ustawy dostępny na stronie internetowej pod adresem: http://www.law.cornell.edu/uscode/text/18/1030.

[19] Nazwa ustawy „*PATRIOT Act*" pisana wielkimi literami stanowi skrót od wyrazów: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*. W tłumaczeniu własnym: *Jednocząc oraz wzmacniając Amerykę poprzez dostarczenie stosownych narzędzi wymaganych do wykrywania oraz zapobiegania terroryzmowi*.

[20] W tłumaczeniu własnym: *Ustawa o ściganiu przestępstwa kradzieży tożsamości oraz jej restytucji*.

[21] C. Doyle, *Cybercrime*: *An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, Congressional Research Service, s. 1. Tekst pełnego opracowania dostępny na stronie internetowej pod adresem: http://www.fas.org/sgp/crs/misc/97-1025.pdf.

[22] *United States Code* (U.S.C.) jest swoistym odpowiednikiem Dziennika Ustaw, który obejmuje skodyfikowane prawo federalne USA. Więcej na temat U.S.C. na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/United_States_Code.

[23] H.M. Jarrett, M.W. Bailie, E. Hagen, S. Eltringham, *Prosecuting Computer Crimes*, Washington DC 2010, s. 1. Opracowanie dostępne na stronie internetowej pod adresem: http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

[24] Tłumaczenie własne. W oryginale: *Fraud and related activity in connection with computers*.

tu nazwy zbiorczej uwagę zwraca wyraźne wydzielenie oszustwa komputerowego z pozostałych nadużyć komputerowych, co z jednej strony może podkreślać szczególny charakter tego czynu (obejmujący połączenie działań komputerowych z elementami socjotechniki oraz nastawienie na uzyskanie korzyści majątkowej), z drugiej zaś czyni zasadnym pytanie, czy w tej sytuacji oszustwo komputerowe należy, na gruncie omawianego aktu, zaliczać do ogólnej kategorii nadużyć komputerowych. Wyraźne usytuowanie „oszustw" obok „nadużyć" mogłoby sugerować intencjonalne oddzielenie obu kategorii, przesądzające, że „oszustwo" nie należy do zbioru nadużyć komputerowych, choć brakuje możliwości potwierdzenia takiej tezy na gruncie samych przepisów. Z uwagi na pozostawienie w treści ustawy omawianych wyrażeń bez jakichkolwiek definicji, także określenie ich znaczenia jest możliwe wyłącznie przez prezentację typologii przestępstw ujętych w przepisach aktu. Z uwagi na normatywny charakter omawianego dokumentu forma, w jakiej zostały określone kolejne przestępstwa, jest typowo kodeksowa (np.: *Kto uzyskuje bezprawny dostęp*...). W rezultacie w przepisach zostały pominięte jakiekolwiek dodatkowe określenia, które miałyby się stać nazwami dla poszczególnych przestępstw. Nazwy rodzajowe stosowane w dalszej części artykułu nie pochodzą zatem z samej ustawy, a z oficjalnego opracowania Kongresu USA i tym samym przynależą do sfery języka prawniczego, to jest języka II stopnia.

Amerykańska ustawa o nadużyciach oraz oszustwach komputerowych określiła siedem kategorii czynów zabronionych:

1) świadome uzyskanie dostępu do komputera bez uprawnienia lub z przekroczeniem posiadanych uprawnień oraz zdobycie w ten sposób informacji prawnie chronionych, w tym informacji obronnych lub dotyczących stosunków międzynarodowych, w sytuacji gdy z okoliczności wynika, że te informacje mogłyby zostać użyte na szkodę USA, a także nastąpiłoby przekazywanie takich informacji na korzyść jakiegokolwiek obcego państwa,
2) umyślne uzyskanie nieuprawnionego dostępu do komputera bez uprawnienia lub z przekroczeniem posiadanych uprawnień oraz zdobycie informacji bankowych lub finansowych, informacji przetwarzanych przez organy administracji publicznej lub informacji pochodzących z chronionych komputerów,
3) umyślne uzyskanie nieuprawnionego dostępu do niedostępnego publicznie komputera administracji, który jest przeznaczony do użytku wyłącznie na rzecz rządu USA lub jest używany przez rząd USA, działanie sprawcy zaś wpływa na ten użytek,
4) świadome oraz z zamiarem dokonania oszustwa uzyskanie dostępu do chronionego komputera bez uprawnienia lub z przekroczeniem uprawnień oraz osiągnięcie w ten sposób jakiejkolwiek korzyści majątkowej, chyba że przedmiotem oszustwa oraz jedyną korzyścią jest samo użycie komputera, a wartość tego użycia nie przekracza 5 tys. dolarów w ciągu roku,
5) umyślne spowodowanie szkód w chronionym komputerze przez świadome spowodowanie transmisji programu, informacji, kodu lub polecenia, a także uzyskanie dostępu bez uprawnienia,
6) świadoma oraz z zamiarem dokonania oszustwa nielegalna sprzedaż haseł lub podobnych informacji mogących służyć uzyskaniu dostępu do komputera bez uprawnień, pod warunkiem, że takie działanie może wpłynąć na obrót międzystanowy lub zagraniczny albo że dany komputer jest wykorzystywany przez rząd USA lub na jego rzecz,

7) transmitowanie, w ramach obrotu międzystanowego lub zagranicznego, jakichkolwiek komunikatów zawierających groźby spowodowania uszkodzeń chronionego komputera, groźby nieuprawnionego zdobycia informacji pochodzących z chronionego komputera lub ich uszkodzenia, a także żądania pieniędzy lub innych korzyści majątkowych w związku z uszkodzeniem chronionego komputera – w celu bezprawnego osiągnięcia korzyści majątkowych od jakiejkolwiek osoby[25].

Pojęcie przestępstwa związanego z komputerem

Trzy lata po napisaniu przez D. Parkera pierwszego, obszernego opracowania naukowego traktującego o fenomenie przestępczości komputerowej, a więc jeszcze pod koniec lat 70. XX w., problematyka zwalczania cyberzagrożeń została wprowadzona na grunt dokumentów rządowych. Pierwszym na świecie quasi-normatywnym aktem dotyczącym zwalczania tego typu działalności przestępnej stał się wydany w 1979 r. podręcznik dla pracowników amerykańskiego wymiaru sprawiedliwości zatytułowany *Computer Crime: Criminal Justice Resource Manual*[26]. Rządowy podręcznik, mający stać się ogólną instrukcją postępowania śledczych w sprawach przestępczości dotyczącej nowoczesnych technologii, został przygotowany na zamówienie Ministerstwa Sprawiedliwości USA (Department of Justice) we współpracy z Instytutem Naukowym Stanforda (Stanford Reserch Institute – SRI). Z uwagi na zaangażowanie w tę tematykę udział w pracach brał także sam D. Parker.

Pomimo wcześniejszego dorobku doktryny amerykańskiej, wyrażeniem stosowanym jako podstawowe na gruncie omawianego podręcznika stało się pojęcie przestępstwa związanego z komputerem[27] (w oryginale: *computer-related crime*). Warto zaznaczyć, że w samym tytule dokumentu zupełnie niekonsekwentnie posłużono się innym – niezdefiniowanym w podręczniku i stosowanym wówczas głównie w kontekście publicystycznym – wyrażeniem przestępczość komputerowa (w oryginale: *computer crime*[28]), w tekście opracowania zaś pojawiały się także inne, również niezdefiniowane w nim, pojęcia, m.in. nadużycie komputerowe[29]. Podstawowym określeniem omawianego opracowania pozostawało jednak przestępstwo związane z komputerem, które zostało wyjaśnione w treści tego dokumentu jako *Każde nielegalne działanie, które dla skutecznego ścigania wymaga wiedzy w zakresie technologii komputerowej*[30].

Na gruncie przytoczonej definicji przestępstwem związanym z komputerem mógł tym samym stać się każdy czyn zabroniony – niezależnie od dobra prawnie chronionego będącego przedmiotem ataku, modus operandi sprawcy czy jakichkolwiek innych cech przestępstwa – jeśli tylko jego ściganie wymagało od śledczych określonych umiejętności.

---

[25] Ustawa federalna *Computer fraud and abuse act* (18 U.S.C. 1030), lit. a, pkt 1–7. Tłumaczenie własne.

[26] *Computer Crime*: *Criminal Justice Resource Manual* [online], SRI International, National Criminal Justice Information and Statistics Service, California, 1979; Washington DC 1989, https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf.

[27] S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*. Opracowanie jest dostępne w postaci elektronicznej na stronie internetowej pod adresem: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

[28] Zob. przypis nr 14.

[29] W oryginale: *computer abuse*.

[30] Tłumaczenie własne. W oryginale: *Any illegal act for which knowledge of computer technology is essential for a successful prosecution*, za: *Computer Crime: Criminal Justice Resource Manual*…, s. XXVI.

W rezultacie zastosowania wskazanej konstrukcji zakres semantyczny definicji stał się jednak zbyt szeroki i objął także takie kategorie czynów niedozwolonych, które w żadnym razie nie dotyczyły nowoczesnych technologii teleinformatycznych. Dla zaktualizowania wymagań „wiedzy komputerowej" od śledczych wystarczające było, aby w trakcie ścigania dowolnego czynu posłużyli się oni nowoczesnymi bazami danych, w których są przechowywane elektroniczne wersje kartotek. Obecnie takie działanie jest standardowym elementem pracy dochodzeniowo-śledczej.

Przestępstwem związanym z komputerem mógł być także każdy czyn, dla którego źródłem materiału dowodowego były dane zapisane na komputerze, na którym np. prowadzono listę nielegalnych transakcji, niekoniecznie wykonywanych za pośrednictwem sieci. Można także stwierdzić nieco ironicznie, że tak zdefiniowanym przestępstwem komputerowym mogła być nawet kradzież sprzętu komputerowego ze sklepu.

Przytoczona definicja pomijała jednak nowe, specyficzne formy przestępstw, które pojawiły się dopiero z chwilą rozwinięcia sieci oraz świadczonych za ich pośrednictwem usług, jak choćby ataki typu *dos*, *ddos*, *man-in-the-middle*, *cache poisoning* czy *pharming*, stanowiące różne formy zakłócania pracy systemów, podszywania się pod użytkowników lub dokonywania włamań komputerowych. Tak sformułowany zakres semantyczny definicji (pojęć) stanowił zatem rozwiązanie zupełnie nieefektywne, które nie tylko obejmowało zbyt wiele czynów, lecz także nie pozwalało na wyróżnienie jakichkolwiek cech szczególnych przestępczości związanej z komputerem. Pomimo przedstawionych wad przyjętej konstrukcji, analogiczne rozwiązanie zostało wprowadzone także do kolejnego, wydanego w 1989 r., opracowania Ministerstwa Sprawiedliwości USA[31].

Powtórna implementacja oryginalnego zapisu stworzonego jeszcze w połowie lat 70. XX w. spotkała się jednak z gruntowną krytyką[32]. Ostatecznie należy zauważyć, że w dobie postępującej informatyzacji coraz mniej czynności wykonuje się z wykluczeniem udziału systemów teleinformatycznych, co jednak nie powinno oznaczać logicznego przeniesienia całej przestępczości do sfery cyberprzestrzeni. Definicja odwołująca się do „obszaru przestępczości komputerowej" powinna przy tym umożliwiać precyzyjne wydzielenie tego typu działalności z innych form przestępczości. W innym przypadku tworzenie nowych, szczególnych regulacji prawnych, zarówno materialnych, jak i procesowych, nastawionych na walkę z nowoczesnymi zagrożeniami, stałoby się niemożliwe.

Wyrażenie przestępstwo związane z komputerem było wykorzystywane w kolejnych latach także w licznych aktach międzynarodowych, które proponowały swoje definicje tego pojęcia. Przykładowo: na potrzeby zalecenia Nr R (89) 9[33] w sprawie przestępczości związanej z komputerami wydanego przez Komitet Ministrów Rady Europy w 1989 r. grupa ekspertów, która przygotowywała dokument, postanowiła określić znaczenie analizowanego pojęcia przez stworzenie jego typologii, a zatem przez zbudowanie wykazu czynów, a nie określenie ich cech rodzajowych. Jako uzasadnienie odstąpienia od budowy klasycznej definicji pojęcia wskazano

[31] *Computer Crime: Criminal Justice Resource Manual*, b.m.w. 1989, U.S. Department of Justice, National Institute of Justice.

[32] Np. M. Goodman, *Making Computer Crime Count*, „FBI Law Enforcement Biulettin", 2001, t. 70, s. 12. Biuletyn dostępny na stronie internetowej pod adresem: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2001-pdfs/aug01leb.pdf. Także: R.W. Aldrich, *Cyberterrorism and Computer Crimes*: *Issues Surrounding the Establishment of an International Legal Regime*. Materiał dostępny na stronie internetowej pod adresem: http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf.

[33] Council of Europe, *Computer-Related Crime: Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems*, Strasbourg 1989.

trudności w wypracowaniu wspólnego, jednolitego sposobu postrzegania tego typu przestępczości. Spowodowało to wymienienie we wspomnianym zaleceniu tych kategorii czynów, które powinny być penalizowane właśnie jako przestępstwa związane z komputerem. Do czynów obligatoryjnie kwalifikowanych w ten sposób (znajdujących się na tzw. liście minimalnej – obligatoryjnej) zaliczono wówczas: oszustwo związane z komputerem, fałszerstwo komputerowe, uszkodzenie danych lub programów, sabotaż komputerowy, nieuprawniony dostęp do zasobów, nieuprawniony podsłuch, bezprawne powielanie chronionych programów komputerowych oraz bezprawne powielanie topografii półprzewodników. Dodatkowo wskazano cztery kolejne kategorie przestępstw, co do których nie osiągnięto pełnego konsensusu w ich zakwalifikowaniu przy tworzeniu tzw. listy opcjonalnej do grupy przestępstw związanych z komputerem. Znalazły się na niej: nieuprawniona modyfikacja danych lub oprogramowania, szpiegostwo komputerowe, wykorzystywanie komputera bez zezwolenia oraz nieuprawione używanie programu komputerowego[34]. Z wyjątkiem bezprawnego kopiowania topografii półprzewodników wszystkie wymienione kategorie działań odnosiły się bezpośrednio do szeroko rozumianego przetwarzania danych i łączyły, w sposób charakterystyczny dla dawniejszych dokumentów, sferę stricte karną z ochroną praw autorskich. W typologii nie wyodrębniono także specjalistycznych ataków komputerowych jako osobnej kategorii, starając się uzyskać bardziej definicyjny, ogólny charakter. Warto zaznaczyć, że pomimo oparcia przywołanego dokumentu Rady Europy na ustaleniach wcześniejszego, pochodzącego z połowy lat 80. XX w., raportu OECD zatytułowanego *Przestępstwa związane z komputerem: analiza polityki legislacyjnej*[35], wcześniejsze opracowanie międzynarodowe – co zostało już zaznaczone – zawierało określenie nadużycie komputerowe, a nie przestępstwo związane z komputerem.

Pojęcie przestępstwa związanego z komputerem było wymieniane także w regulacjach ONZ, m.in. w *Rezolucji VIII Kongresu ONZ w sprawie zapobiegania przestępczości i postępowania z przestępcami* (1990), w której tytule się pojawiło (*computer-related crime*)[36]. Ta rezolucja jednak nie tylko nie oferowała żadnej definicji tego pojęcia, lecz także wprowadzała inne, nieznane dotychczas, również niezdefiniowane wyrażenia: nadużycia komputerów[37] (w przeciwieństwie do nadużycia komputerowego) oraz nadużycia związanego z komputerem[38].

Jednocześnie te pojęcia były traktowane synonimicznie. Pomimo niespójności oraz nieokreśloności przyjętej siatki pojęciowej, rezolucja jest często wskazywana jako wyraz zaangażowania ONZ w problematykę przeciwdziałania nowoczesnym formom przestępczości. Podkreśla się jej ponadeuropejski zasięg stawiający poruszany temat na arenie światowej oraz kierunki działań proponowane w treści rezolucji, m.in. koniecz-

[34] Tamże, s. 36 i nast.

[35] *Computer-related crime: Analysis*…

[36] Rezolucja opublikowana w: *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Havana, 27 August – 7 September 1990: report prepared by the Secretariat, United Nations publication, Sales No. E.91.IV.2), sekcja C, rezolucja nr 9, s. 140 i nast. Pełny tekst raportu dostępny na stronie internetowej pod adresem: http://www.asc41.com/UN_Congress/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/026%20ACONF.144.28.Rev.1%20Eighth%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf.

[37] Tłumaczenie własne. W oryginale *abuse of computers*.

[38] Tłumaczenie własne. W oryginale *computer-related abuse*.

ność uzupełnienia prawodawstwa o nowe rodzaje czynów bezprawnych[39]. Chaotyczność terminologii zastosowanej na gruncie rezolucji należy uznać za istotną wadę opracowania, które, stawiając sobie za jeden z głównych celów identyfikację niedostatków obowiązującego prawa, nie określało jednoznacznie samego przedmiotu prowadzonej analizy. Wyrażenie przestępstwo związane z komputerem zostało wykorzystane przez ONZ także w wydanym w 1994 r. podręczniku, który był kolejnym opracowaniem tej organizacji.

Pojęcie bezprawnego użycia komputera

Pojęcie bezprawnego użycia komputera pochodzi z wydanej w 1990 r. brytyjskiej ustawy *Computer Misuse Act*[40], będącej pierwszą na Wyspach i nadal obowiązującą kodyfikacją prawa nakierowaną na zwalczanie przestępstw popełnianych z użyciem komputera. Ta ustawa wprowadziła do zasobu słownictwa prawniczego języka angielskiego nowe, nieznane dotychczas w doktrynie określenie: bezprawne użycie komputera (w oryginale: *computer misuse*), które znaczeniowo miało zastępować inne, rozpoznawane już na arenie międzynarodowej wyrażenia: nadużycie komputerowe i przestępczość związana z komputerem. Z uwagi na niuanse językowe, niezbędne staje się poczynienie uwagi o charakterze technicznym: anglojęzyczne wyrazy *misuse* oraz *abuse* (wykorzystywane odpowiednio w dwóch różnych wyrażeniach: *computer misuse* oraz *computer abuse*) można tłumaczyć synonimicznie jako „nadużycie”[41]. Tym samym, na gruncie językowym, polskojęzyczna kategoria „nadużycie komputerowe” mogłaby obejmować łącznie pojęcia: *computer abuse* (omówione wcześniej) oraz *computer misuse*, choć z punktu widzenia prawnego błędnie stawiałoby to znak równości między zwrotami zachowującymi w oryginale różne brzmienia. Aby uniknąć takiej sytuacji, zwrot *computer misuse* należy tłumaczyć jako „bezprawne użycie komputera”, mając na uwadze brytyjskie rozumienie prawniczego zwrotu *misuse* oraz przypadki jego występowania na gruncie angielskiego ustawodawstwa[42].

Z uwagi na brak ustawowej definicji omawianego pojęcia znaczenie „bezprawnego użycia komputera” musi być rekonstruowane na podstawie typologii czynów zabronionych charakteryzowanych w ustawie. Podobnie jak w przypadku amerykańskiej ustawy karnej z 1986 r., także ustawa brytyjska została skonstruowana w sposób typowo kodeksowy (np. *kto uzyskuje*...), a typizowane w niej czyny nie zostały nazwane żadnymi określeniami rodzajowymi (np. *hacking*). Tak samo kodeks karny nie posługuje się terminami zabójstwo i morderstwo. W brytyjskiej ustawie można zatem znaleźć wyłącznie opisy poszczególnych typów przestępstw zawarte w hipotezach przepisów. W oryginalnym kształcie ta ustawa przewidywała penalizację trzech następujących kategorii czynów:

[39] Na te cechy wskazuje m.in. A. Adamski w: tenże, *Prawo karne komputerowe*…, s. 9–10.

[40] *Computer Misuse Act 1990*. W tłumaczeniu własnym: *Ustawa o bezprawnym użyciu komputera z 1990 r.* Pełny oryginalny tekst aktu dostępny na stronie internetowej parlamentu brytyjskiego pod adresem: http://www.legislation.gov.uk/ukpga/1990/18/enacted.

[41] Zob. np. internetowy słownik Mirriam-Webster dostępny na stronie internetowej pod adresem: http://www.merriam-webster.com/dictionary/misuse.

[42] Wyraz *misuse* jest wykorzystywany m.in. przez brytyjską ustawę antynarkotykową *Drugs Misuse Act 1986*. Ta ustawa porusza problem nie tylko samego używania środków odurzających, lecz także ich produkcji czy sprzedaży, wykraczając tym samym poza zakres rozumienia polskiego wyrażenia nadużywanie narkotyków.

1) nieuprawnionego, umyślnego dostępu do zasobów komputera polegającego na użyciu jakiejkolwiek funkcji komputera z zamiarem zapewnienia dostępu do jakiegokolwiek programu lub danych przechowywanych na jakimkolwiek komputerze,
2) nieuprawnionego dostępu, o którym mowa w pkt 1, z zamiarem popełnienia dalszych przestępstw lub ułatwienia ich popełnienia dowolnej osobie, w dowolnym czasie,
3) nieuprawnionej modyfikacji zasobu komputerowego dokonywanej w celu zakłócenia poprawnego funkcjonowania jakiegokolwiek komputera, uniemożliwienia lub utrudnienia dostępu do programu, a także zakłócenia działania programu lub naruszenia wiarygodności danych[43].

Pojęcie przestępstwa komputerowego

Już od drugiej połowy lat 70. XX w. w piśmiennictwie oprócz wyrażenia nadużycie komputerowe było popularyzowane także inne określenie nowego zjawiska przestępnego – przestępczość komputerowa. Tym pojęciem posłużyli się m.in. Ulrich Sieber, uważany za jednego z ojców „prawa informatycznego", oraz August Bequai, którzy wprowadzili je do tytułów swoich opracowań wydanych odpowiednio: w 1977[44] oraz 1978[45] r. Ogólne rozumienie pojęcia prezentowane w tych opracowaniach nie odbiegało jednak od sposobu charakteryzowania wcześniej zdefiniowanego wyrażenia nadużycie komputerowe. W następnych latach wyrażenie przestępstwo komputerowe pojawiało się wielokrotnie także w opracowaniach amerykańskich (m.in. w amerykańskiej prasie), jednak bez stworzenia definicji tego pojęcia, która stałaby się szeroko rozpoznawana w literaturze przedmiotu.

Cztery lata po uchwaleniu przez VIII Kongres ONZ rezolucji w sprawie przestępstw związanych z komputerem (opisanej już przy omawianiu tego pojęcia) Organizacja Narodów Zjednoczonych podjęła kolejną inicjatywę odnoszącą się do problematyki zwalczania nowoczesnych form przestępczości. Wyrazem tego stało się wydanie w 1994 r. *Podręcznika w sprawie zapobiegania oraz kontroli przestępstw związanych z komputerem*[46]. Dostrzegając dotychczasowe trudności w ustaleniu spójnej siatki pojęciowej (odczuwalne już globalnie), a także chcąc nadać podręcznikowi możliwie uniwersalny charakter, ponownie odstąpiono od budowy ogólnej definicji na rzecz ujęcia funkcjonalnego (zastosowano zatem rozwiązanie analogiczne do rozwiązania zawartego w opracowaniu wydanym w 1989 r. przez Komitet Ministrów Rady Europy). Zamiast klasycznej definicji zaproponowano wykaz zdarzeń, które miały być określane – co wymaga zaznaczenia – zamiennie, mianem przestępstwa związanego z komputerem lub przestępstwa komputerowego[47]. Na gruncie omawianego podręcznika ONZ oba wyrażenia stały się więc tak naprawdę synonimami i nie tylko postawiły pod znakiem zapytania jakąkolwiek zasadność ich różnicowania, lecz także uczyniły to wbrew przyjętym zasadom tworzenia oraz interpretacji przepisów, które jednoznacznie nakazują, aby dwóm różnym pojęciom nadawać zawsze dwa różne znaczenia, jednemu zaś – zawsze jedno i to samo.

[43] *Computer Misuse Act 1990*, art. 1–3.

[44] U. Sieber, *Computercriminalität und Strafrecht*, Köln 1977.

[45] A. Bequai, *Computer Crime*, Heath (Massachusetts) 1978.

[46] *United Nations Manual on the prevention and control of computer-related crime*. Tekst dostępny na stronie internetowej pod adresem: http://www.uncjin.org/Documents/EighthCongress.html.

[47] Tłumaczenie własne. W oryginale odpowiednio: *computer-related crime* oraz *computer crime*.

Pomimo deklarowanej równości pojęć, w dokumencie wyraźnie częściej posługiwano się określeniem przestępstwa komputerowego, które zostało użyte także przy próbie nazwania zjawiska. W celu przybliżenia zakresu semantycznego tak określonej kategorii czynów, w punkcie 22 opracowania została wprowadzona quasi-definicja, zgodnie z którą *Przestępstwo komputerowe może polegać na podejmowaniu tradycyjnych w swojej naturze działań przestępnych, takich jak kradzież, oszustwo, fałszerstwo oraz wyrządzanie szkód, które zasadniczo wszędzie podlegają sankcji karnej. Komputery wytworzyły jednak także wiele nowych, potencjalnych działań bezprawnych lub możliwości nadużyć, które mogą lub powinny być uważane za przestępstwa*[48].

W przytoczonym zapisie w sposób czytelny zwrócono uwagę na rozróżnienie dwóch głównych kategorii czynów, które mogą być określone jako przestępczość komputerowa. Z jednej strony są to „tradycyjne z natury" działania przestępne, dla których komputer staje się nowym narzędziem przestępstwa (w tym tworzy nowe, specyficzne środowisko do ich popełniania), z drugiej zaś – zupełnie nowe typy czynów bezprawnych, niepoddające się subsumpcji. W podręczniku podkreślano też, że komputer może stać się nie tylko narzędziem, lecz także przedmiotem, czyli innymi słowy – celem tak określonego czynu. Zaprezentowane rozróżnienie na kategorie typowych oraz nowych form przestępstw stało się w kolejnych latach cechą charakterystyczną omawianego tu pojęcia przestępstwa komputerowego.

Poza przytoczoną definicją w podręczniku ONZ prezentowano także wykaz typowych przestępstw komputerowych, w którym zostały zawarte następujące kategorie czynów: oszustwo przez komputerową manipulację (odnoszące się do zaburzenia poprawnego funkcjonowania urządzenia), fałszerstwo komputerowe, uszkodzenie lub modyfikacja przetwarzanych danych lub oprogramowania, nieuprawniony dostęp do systemu komputerowego lub usługi oraz nieuprawnione powielanie chronionego prawem programu komputerowego. Pomimo przyjęcia nieco innego nazewnictwa, przedstawiony wykaz pozostawał w istocie zbieżny z listą przestępstw stworzoną osiem lat wcześniej przez ekspertów OECD na potrzeby wydanej przez tę organizację analizy polityki legislacyjnej. Zważywszy na niezwykle szybkie tempo rozwoju technologicznego oraz podążający za nim rozwój form i metod nowoczesnej przestępczości, brak nowych, precyzyjnych zapisów spełniających standardy prawa karnego należy uznać za przejaw nienadążania regulacji prawnych za wymaganiami, jakie stawia otaczająca nas rzeczywistość. Korzystanie z już przyjętych rozwiązań świadczy o tym, jak trudnym zadaniem jest wypracowywanie na arenie międzynarodowej kompromisów w odniesieniu do tworzenia nowych, wspólnych regulacji karnych.

Pojęciem przestępstwa komputerowego w Polsce posłużył się także Andrzej Adamski, zawierając je w swoim opracowaniu zatytułowanym *Prawo karne komputerowe*[49]. Książka, wydana w 2000 r., jest uznawana za kanon polskich rozważań prawniczych dotyczących charakteryzowania zjawiska przestępczości komputerowej. A. Adamski zwrócił uwagę na istotne wady siatki pojęciowej stosowanej w prawie karnym komputerowym i zaprezentował własną, poszerzoną charakterystykę przestępstwa komputerowego, wprowadzając podział definicyjny przestępczości komputerowej na

[48] Tłumaczenie własne. W oryginale: *Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may, or should, be criminal as well*.

[49] A. Adamski, *Prawo karne komputerowe*…, s. 30 i nast.

dwa odrębne ujęcia: materialno-prawne oraz procesowe. W ramach ujęcia materialno-prawnego, stosując kryterium roli, w jakiej mogą występować komputery w działaniu przestępnym, wyróżnił dwie subkategorie przestępczości komputerowej – w rozumieniu wąskim (tzw. przestępstwa stricte komputerowe) oraz szerokim:

1) przestępstwami stricte komputerowymi A. Adamski nazwał te czyny bezprawne, które są skierowane przeciwko systemom, danym lub programom, czyli czyny, w których nowoczesne technologie informatyczne stanowią bądź to sam przedmiot zamachu, bądź też środowisko do jego przeprowadzenia. Jak zauważa autor, w tym przypadku następuje swoiste genetyczne powiązanie nowoczesnych form przestępczości z technologią komputerową. Przestępstwa należące do tej kategorii trzeba odnieść do czynów naruszających tzw. atrybuty bezpieczeństwa danych, szczególnie ich poufność, integralność oraz dostępność. Te cechy oznaczają odpowiednio, że dane przetwarzane w systemach teleinformatycznych nie zostały ujawnione osobom nieuprawnionym (zdarzenie nazywane także kompromitacją danych); nie zostały one w sposób nieuprawniony zmodyfikowane ani uszkodzone oraz są dostępne dla uprawnionych użytkowników, zgodnie z zasadami panującymi w danym systemie (np. nie dokonano przeciążenia łączy, co uniemożliwiałoby odwołanie się do danego zasobu),
2) przestępstwami komputerowymi w ujęciu szerokim zostały nazwane wszystkie czyny, których ustawowa regulacja wprowadza expressis verbis wykorzystanie komputera do ich popełnienia, np. przestępstwa z art. 130 § 3, art. 267–269, art. 278 § 2, art. 285 i art. 287 *Kodeksu karnego*[50]. Jak zauważa A. Adamski są to przestępstwa komputerowe (…) *nie ze względu na przedmiot zamachu, lecz ustawowo określony sposób działania sprawcy*[51]. Dobrem prawnie chronionym nie jest tutaj samo funkcjonowanie systemu, lecz różne inne dobra. Przestępstwa należące do tej grupy A. Adamski sugeruje nazywać „przestępstwami komputerowymi" z dodaniem określenia przedmiotu ochrony, np. „przestępstwo komputerowe przeciwko wiarygodności dokumentów".

Istotnym uzupełnieniem zaprezentowanego podziału jest także sposób uwzględnienia pozostałych czynów (nienależących do żadnej z kategorii przestępstw komputerowych), w których komputer może jednak wystąpić w roli narzędzia do popełnienia „klasycznego" przestępstwa, np. przestępstwa zniewagi, zniesławienia, groźby karalnej, propagacji treści prawnie zabronionych lub oszustwa. Dla tej kategorii zdarzeń A. Adamski przyjmuje nazwę „przestępstwa popełniane z użyciem (wykorzystaniem) komputera". Tym mianem są określane te czyny, których ustawowa regulacja nie zakłada użycia komputera jako przesłanki konstytuującej czyn, lecz możliwe jest ich popełnienie także z zastosowaniem systemów teleinformatycznych (szczególny, lecz niewymagany przepisem rodzaj modus operandi sprawcy).

W ujęciu procesowym przestępstwami komputerowymi, na gruncie opracowania A. Adamskiego, określono (…) *wszelkie czyny zabronione przez prawo karne, których ściganie wymaga od organów wymiaru sprawiedliwości uzyskania dostępu do informacji przetwarzanej w systemach komputerowych lub teleinformatycznych. Pojęcie przestępstw komputerowych w aspekcie procesowym obejmuje zatem zarówno przypadki, w których system komputerowy stanowi przedmiot, jak i narzędzie zamachu*[52].

[50] *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 5 lipca 2016 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137) – przyp. red.

[51] A. Adamski, *Prawo karne komputerowe*…, s. 31–32.

[52] Tamże, s. 34.

Pojęcie przestępstwa powiązanego z technologią informacyjną

Pojęcie przestępstwa powiązanego z technologią informacyjną, przyjmujące w oryginale brzmienie: *Offence Connected with Information Technology*[53], zostało zdefiniowane w związku z pracami prowadzonymi nad *Zaleceniem Komitetu Ministrów Rady Europy Nr R (95)13 z dnia 11 września 1995 r. w sprawie „Problemów karnoprocesowych związanych z technologią przetwarzania informacji"*[54].

Powyższy dokument stał się pierwszym istotnym wyrazem międzynarodowego zainteresowania problematyką podejmowania czynności procesowych ze szczególnym uwzględnieniem ich roli dowodowej w zwalczaniu nowoczesnych form przestępczości[55]. Analiza definicji zawartej w dokumencie pozwoli zaprezentować podejście, które zostało stworzone specjalnie z myślą o zagadnieniach karnoprocesowych. Zgodnie z memorandum wyjaśniającym (*explanatory memorandum*), stanowiącym funkcjonalne uzupełnienie treści samego *Zalecenia...*, przestępstwem powiązanym z technologią informacyjną jest *Każde przestępstwo, w którego procesie śledczym właściwe organy wymiaru sprawiedliwości muszą uzyskać dostęp do informacji przetwarzanych lub przekazywanych w systemach komputerowych lub* (...) *systemach przetwarzania danych występujących w postaci elektronicznej*[56].

Na potrzeby *Zalecenia...* pojęcia systemy komputerowe oraz systemy przetwarzania danych zostały ujęte możliwie szeroko i objęły w zasadzie wszelkie przykłady technologii informacyjnych, w tym zarówno pojedyncze (odseparowane od środowiska cyfrowego) komputery, jak i całe sieci. Jak można przeczytać we wprowadzeniu do definicji, systemy w tak określonym przestępstwie mogą być wykorzystane jako:

1) narzędzia do popełnienia przestępstwa,
2) przedmiot (cel) przestępstwa,
3) środowisko popełnienia przestępstwa,
4) środowisko, w którym mogą się pojawić dowody przestępstwa; w tym przypadku sam system nie musi stanowić żadnego elementu w procesie popełniania przestępstwa.

Pojęcie cyberprzestępstwa

Pojęcie cyberprzestępstwo (w oryginale: *cybercrime*) jest obecnie jednym z najszerzej rozpoznawanych pojęć używanych do określenia nowoczesnych form przestępczości komputerowej. Swoją rangę zawdzięcza wprowadzeniu go do konwencji Rady Europy o cyberprzestępczości[57] (dalej: konwencji), zwanej też czasami konwen-

[53] W skrócie też *IT offence* – 'przestępstwo dotyczące IT'.

[54] *Problems of Criminal Procedural Law Connected with Information Technology. Recommendation No. R(95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995 and explanatory memorandum*, Council of Europe Publishing, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 [dostęp: 20 VI 2016].

[55] A. Adamski, *Prawo karne komputerowe*…, s. XVII.

[56] Tłumaczenie własne. W oryginale: *Any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems, or, as they are referred to above, electronic data processing systems*.

[57] *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.* (Dz.U. z 2015 r. poz. 728) – przyp. red. Tytuł oryginalny: *Convention on Cybercrime*, CETS Nr: 185. Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.

cją z Budapesztu lub konwencją budapesztańską[58], będącej wynikiem jednej z najistotniejszych inicjatyw na arenie międzynarodowej odnoszących się do regulacji zwalczania przestępczości komputerowej. Konwencja została otwarta do podpisu 23 listopada 2001 r., w życie zaś weszła 1 lipca 2004 r., po uzyskaniu ratyfikacji pięciu państw (wymogiem było, aby przynajmniej trzy z nich należały do Rady Europy). Łącznie podpisało ją 47 państw, w tym Polska, która stała się sygnatariuszem dokumentu już w dniu jego otwarcia do podpisu[59]. Wśród ważnych sygnatariuszy należy wskazać Wielką Brytanię, Niemcy, Francję, Szwecję, Rosję, a także Stany Zjednoczone i Japonię[60]. W dniu 28 stycznia 2003 r. w Strasburgu został otwarty do podpisu także *Protokół dodatkowy do Konwencji w sprawie kryminalizacji aktów natury rasistowskiej oraz ksenofobicznej popełnianych za pośrednictwem systemów komputerowych*[61]. Protokół wszedł w życie 1 marca 2006 r. (po uzyskaniu pięciu ratyfikacji). Polska podpisała go 21 lipca 2003 r.[62]

Choć nasz kraj oficjalnie nie ratyfikował konwencji, o której mowa, aż do 2015 r. (ustawa ratyfikacyjna – 27 maja 2015 r.[63]), to krajowe ustawodawstwo karne zostało dostosowane do jej zapisów znacznie wcześniej, szczególnie na mocy *Ustawy z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń*[64].

Omawiając szczegółowe zapisy konwencji z Budapesztu, należy zauważyć, że nie wprowadzono w niej definicji pojęcia cyberprzestępstwo. Nakazano tym samym rekonstrukcję jego znaczenia na podstawie opisanych w akcie rodzajów czynów zabronionych. Podobnie jak w przypadku wielu innych dokumentów, także i tu zastosowano tzw. ujęcie funkcjonalne, skupiające się na opisach hipotez czynów, które powinny być penalizowane w systemach prawnych państw stron umowy, oraz tworzeniu katalogów takich czynów. Sam termin cyberprzestępstwo lub cyberprzestępczość (w oryginale: *cybercrime*), stosowane wymiennie, jest użyte w konwencji dziewięciokrotnie, przy czym tylko raz w samej treści postanowień aktu (w odniesieniu do współpracy międzynarodowej), a pozostałe osiem razy w preambule niestanowiącej materiału normatywnego. Uwzględniając kryterium „dobra prawnie chronionego" będącego przedmiotem ataku, czyny stypizowane w konwencji zostały podzielone na cztery kategorie (wskazane w tytułach 1–4 rozdziału II konwencji): przestępstwa przeciwko poufności, integralności i dostępności danych informatycz-

int/Treaty/EN/Treaties/Html/185.htm.

[58] Zob. np. na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Convention_on_Cybercrime.

[59] Aktualne informacje dotyczące sygnatariuszy można znaleźć na oficjalnej stronie internetowej konwencji, dostępnej pod adresem: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.

[60] Konwencję podpisały cztery państwa niebędące członkami Rady Europy, choć z tej grupy ratyfikowało ją wyłącznie USA (29 września 2006 r.); w USA konwencja weszła w życie 1 stycznia 2007 r.

[61] Tytuł oryginalny: *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, CETS Nr: 189. Pełny tekst protokołu jest dostępny na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm. Polska wersja: *Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu dnia 28 stycznia 2003 r*. (Dz.U. z 2015 r. poz. 730).

[62] Aktualne informacje dotyczące sygnatariuszy protokołu można znaleźć na oficjalnej stronie internetowej konwencji, dostępnej pod adresem: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG.

[63] *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r*. (Dz.U. z 2001 r. poz. 728) – przyp. red.

[64] Dz.U. z 2004 r. Nr 69 poz. 626.

nych i systemów[65]; przestępstwa komputerowe[66]; przestępstwa ze względu na charakter zawartych informacji[67] oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[68]. Klasyfikację poszczególnych czynów zaprezentowano poniżej:

I. Przestępstwa przeciwko poufności, integralności oraz dostępności danych oraz systemów komputerowych:
   - nielegalny dostęp – rozumiany jako dostęp do całości lub części systemu bez posiadania uprawnień do takiego działania,
   - nielegalne przechwytywanie danych – rozumiane jako przechwytywanie wszelkich transmisji danych komputerowych nieposiadających charakteru publicznego, w tym przechwytywanie ulotu elektromagnetycznego,
   - naruszenie integralności danych – rozumiane jako niszczenie, wykasowywanie, uszkadzanie i usuwanie danych informatycznych oraz dokonywanie ich zmian,
   - naruszenie integralności systemu – rozumiane jako poważne zakłócenie funkcjonowania systemu komputerowego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie i dokonywanie zmian lub usuwanie danych informatycznych,
   - niewłaściwe wykorzystanie urządzeń – rozumiane jako posiadanie, wytwarzanie lub inne formy udostępniania urządzeń lub programów zaprojektowanych albo przystosowanych do popełniania wymienionych wyżej czynów albo kodów dostępowych lub innych danych pozwalających na uzyskanie dostępu do całości lub części systemu komputerowego oraz handel nimi.

II. Przestępstwa komputerowe:
   - fałszerstwo komputerowe – rozumiane jako bezprawne wprowadzenie, dokonywanie zmian, wykasowywanie lub ukrywanie danych informatycznych, skutkujące ich nieautentycznością, z zamiarem wykorzystania tak przekształconych danych jako autentyczne,
   - oszustwo komputerowe – rozumiane jako powodowanie strat majątkowych z zamiarem bezprawnego uzyskania dla siebie lub osoby trzeciej korzyści majątkowych przez wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych lub też ingerencję w funkcjonowanie systemu komputerowego.

III. Przestępstwa ze względu na charakter informacji:
   - przestępstwa związane z pornografią dziecięcą – polegające na wytwarzaniu, udostępnianiu, posiadaniu lub pozyskiwaniu materiałów pornograficznych z udziałem małoletniego (domyślnie konwencja ustala granicę 18 lat, zezwalając jednak państwom na obniżenie cezury wieku do lat 16).

IV. Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych – rozumiane jako działania kierowane przeciwko prawom autorskim lub prawom pokrewnym na skalę komercyjną, przy zastosowaniu systemu komputerowego.

[65] W oryginale: *Offences against the confidentiality, integrity and availability of computer data and systems*.

[66] W oryginale: *Computer-related offences*. Wydaje się, że poprawne tłumaczenie powinno brzmieć: *przestępstwa związane z komputerami*.

[67] W oryginale: *Content-related offences*.

[68] W oryginale: *Offences related to infringements of copyright and related rights.*

Zgodnie z definicjami przyjętymi na gruncie konwencji:

- system informatyczny to każde urządzenie lub grupa połączonych lub wiązanych urządzeń, z których przynajmniej jedno przetwarza dane w zautomatyzowany, zaprogramowany sposób,
- dane informatyczne to wszelkie przedstawienie faktów, informacji lub pojęć w formie odpowiedniej do przetwarzania w systemie, w tym także oprogramowanie zdolne do wykonywania określonych funkcji.

Przytoczony wykaz czynów zabronionych uzupełniają zapisy wspomnianego *Protokołu dodatkowego do Konwencji...* (art. 3–7). Ten dokument wprowadza szczególną penalizację czynów dokonywanych za pośrednictwem systemów komputerowych, które polegają na:

- publicznym udostępnianiu rasistowskich oraz ksenofobicznych materiałów w systemach komputerowych,
- kierowaniu gróźb karalnych o podłożu rasowym lub ksenofobicznym, przekazywanych przez systemy komputerowe,
- publicznym znieważaniu osób na tle rasistowskim lub ksenofobicznym, dokonywanym przy użyciu systemów komputerowych,
- publicznym udostępnianiu przez systemy komputerowe materiałów odmawiających ludziom praw lub im umniejszających na tle rasistowskim lub ksenofobicznym, a także pochwalających lub usprawiedliwiających zbrodnie ludobójstwa lub inne zbrodnie przeciwko ludzkości, zdefiniowane na mocy odpowiednich przepisów międzynarodowych,
- udzielaniu pomocy w popełnieniu lub ułatwianiu popełnienia któregokolwiek z powyższych czynów zabronionych.

Przy omawianiu powyższego wykazu czynów bezprawnych, określanych łącznie – zgodnie z tytułem konwencji – mianem „cyberprzestępstw", należy podkreślić jego szeroki zakres przedmiotowy oraz złożoność. Obejmuje on wiele zróżnicowanych czynów, które są kierowane przeciw różnym dobrom prawnie chronionym. Z uwagi na szeroki zakres opisów poszczególnych czynów, ich szczegółowy modus operandi może przybierać rozliczne formy i treści. Ponadto zawiera on zarówno te czyny, których popełnienie jest możliwe wyłącznie w cyberprzestrzeni, jak i te, w których systemy teleinformatyczne są wyłącznie narzędziami, to jest czyny, których popełnienie nie narusza samej pracy systemów czy bezpieczeństwa przetwarzanych w nich danych. Przestępstwa związane z propagowaniem pornografii dziecięcej, nielegalnym kopiowaniem materiałów chronionych prawem autorskim czy udostępnianiem materiałów rasistowskich także stają się cyberprzestępstwami, jeśli są popełnione z wykorzystaniem komputera.

Jako ciekawostkę warto także zauważyć, że w *Raporcie wyjaśniającym*[69] do konwencji o cyberprzestępczości pojęcie *cybercrime* pojawia się tylko raz w tytule samej konwencji. Raport wprowadza natomiast inne, nieznane na gruncie konwencji budapesztańskiej, pojęcia: czyny bezprawne cyberprzestrzeni oraz przestępstwa cyberprzestrzeni[70], odwołujące się zarówno do czynów skierowanych przeciw integralności, dostępności i poufności systemów komputerowych oraz sieci telekomunikacyjnych, jak i czynów zawierających element wykorzystania takich sieci oraz oferowanych przez nie usług do popełnienia tradycyjnych przestępstw[71].

[69] *Explanatory Report* [online], http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm [dostęp: 20 VI 2016].
[70] Tłumaczenie własne. W oryginale: *cyber-space offences*.
[71] *Explanatory Report*…, cz. 2, pkt 8.

W dokumentach krajowych pojęcie cyberprzestępstwo było wykorzystywane po przyjęciu konwencji o cyberprzestępczości w wielu rządowych programach ochrony cyberprzestrzeni. Zostało wprowadzone w pierwszej kolejności do programu USA (2003 r.), a następnie programów Polski (2009 r.), Anglii (2009 r. i 2011 r.), Niemiec (2011 r.), Francji (2011 r.) oraz Holandii (2011 r.). Pojawia się także w *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[72], nazywanej na wcześniejszych etapach prac legislacyjnych *Rządowym Programem Ochrony Cyberprzestrzeni na lata 2011–2016*. Ten dokument to kontynuacja wcześniejszego *Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011*. Pomimo występowania omawianego pojęcia na szeroką skalę, jedynie dwa ze wskazanych wyżej rządowych programów wprowadzają jego definicję – są nimi strategia francuska oraz *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*.

Pochodzący z 2011 r. rządowy program Francji, zatytułowany *Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji*[73], definiuje cyberprzestępstwo jako *Czyny naruszające postanowienia umów międzynarodowych lub regulacji krajowych, wykorzystujące sieci lub systemy informacyjne jako narzędzia do popełnienia deliktu lub przestępstwa, lub jako cel bezprawnego zamachu*[74]. Wymieniony system informacyjny to zorganizowany zbiór zasobów sprzętowych, programowych, osobowych oraz organizacyjnych (proceduralnych), służący do przetwarzania oraz przesyłania informacji[75].

Inaczej niż w przypadku zapisów zawartych w konwencji o cyberprzestępczości, przytoczona definicja nie buduje zamkniętego wykazu czynów bezprawnych, wskazując w zastępstwie dwie przesłanki, których łączne spełnienie jest niezbędne, aby dany czyn uznać za cyberprzestępstwo:

1) czyn musi być penalizowany na mocy przepisów odrębnych – krajowych bądź międzynarodowych,
2) sieci lub systemy teleinformatyczne muszą występować w takim czynie przynajmniej w jednej z dwóch ról – jako narzędzie popełnienia przestępstwa lub jako przedmiot zamachu.

Z punktu widzenia analizy pojęciowej ciekawe określenie cyberprzestępstwa prezentuje *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* przyjęta 25 czerwca 2013 r. uchwałą Rady Ministrów RP, wprowadzająca jedną z najkrótszych, choć jednocześnie najnowocześniejszych charakterystyk omawianego pojęcia. Cyberprzestępstwo jest tu określane jako *Czyn zabroniony popełniony w obszarze cyberprzestrzeni*. Charakterystyczną cechą przytoczonego określenia jest jego wyraźne odwoływanie się do pojęcia cyberprzestrzeń. Inaczej niż w przypadku omawianych wcześniej definicji zagranicznych, definicja krajowa nie określa ani wykazów czynów zabronionych, które powinny być penalizowane jako cyberprzestępstwa, ani szczegóło-

[72] Pełny tekst dokumentu jest dostępny na stronie internetowej pod adresem: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html. Należy zaznaczyć, że dokument jest kontynuacją wydanego w 2009 r. *Rządowego programu ochrony cyberprzestrzeni RP na lata 2009–2011. Założenia*.

[73] Tłumaczenie własne. W oryginale: *Défense et sécurité des systèmes d'information. Stratégie de la France*. Dokument dostępny na stronie internetowej pod adresem: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011 [dostęp: 20 VI 2016].

[74] Tłumaczenie własne. W oryginale: *Cybercriminalité Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible*; cyt. za: tamże, s. 21 [dostęp: 20 VI 2016].

[75] Tłumaczenie własne. W oryginale: *Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information*, tamże, s. 22.

wych metod działania cyberprzestępców, zastępując wskazane elementy odwołaniem do obszaru cyberprzestrzeni stanowiącej cyfrową domenę przetwarzania danych. Pomimo pozornego uproszczenia semantycznego, zastosowane w niej odwołanie nie tylko zapewnia szeroki kontekst znaczeniowy charakteryzowanego pojęcia, lecz także pozwala na wprowadzenie nieco mniej konwencjonalnego spojrzenia na opis zjawiska nowoczesnej przestępczości komputerowej oraz jego form.

Stosując wcześniej zaproponowany sposób analizy przywoływanych definicji, należy wskazać, że na gruncie *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* cyberprzestępstwem jest każdy czyn spełniający łącznie dwie następujące przesłanki:

1) jest czynem zabronionym w rozumieniu dowolnego przepisu prawnego,
2) szczególnym miejscem popełnienia czynu musi być cyberprzestrzeń rozumiana nie jako kategoria geograficzna, ale nowa, logiczna domena ludzkiej działalności, podbudowywana przez szeroko rozumianą infrastrukturę teleinformatyczną, lecz z nią nieutożsamiana (cyberprzestrzeń jako środowisko wirtualne, oderwane od substratu fizycznego).

Po przeanalizowaniu wymienionych przesłanek jako główne kryterium zaliczania poszczególnych czynów do kategorii cyberprzestępstw przyjęto ocenę możliwości wystąpienia danego czynu w cyberprzestrzeni. Pojawiające się w innych definicjach oceny charakteru dóbr prawnie chronionych będących przedmiotem zamachu, roli systemów teleinformatycznych w przestępstwie czy też opisu szczególnego rodzaju modus operandi sprawcy, w omawianym przypadku straciły w rezultacie swoje znaczenie na rzecz ujednoliconego odwołania do pojęcia cyberprzestrzeń. Na jego tle uzasadnione staje się zadanie następującego pytania: Czy do stwierdzenia zaistnienia tak charakteryzowanego cyberprzestępstwa konieczne jest, aby dany czyn w całości „zamykał się" w cyberprzestrzeni (w tym także ze swoimi skutkami), czy też jest wystarczające, aby w cyberprzestrzeni wystąpiły jedynie niektóre z elementów opisujących dane przestępstwo[76]? Czy wprowadzenie kogoś w błąd w rozmowie telefonicznej przez fałszywe podanie się za osobę pracującą np. w dziale obsługi technicznej banku, skutkujące wykonaniem przez osobę oszukaną niekorzystnej operacji za pośrednictwem sieci Internet (m.in. przesłanie hasła, autoryzowanie przelewu online) powinno być oceniane jako cyberprzestępstwo czy też jako przestępstwo „klasyczne"? Podczas analizy przedstawionego problemu niezbędne wydaje się odwołanie do przepisu art. 6 § 2 kodeksu karnego, zgodnie z którym miejscem popełnienia czynu jest miejsce działania lub zaniechania sprawcy, a także miejsce, w którym nastąpił lub jedynie miał nastąpić skutek stanowiący znamię przestępstwa. Tym samym należy stwierdzić, że na gruncie omawianej definicji, w celu ukonstytuowania cyberprzestępstwa jako przestępstwa popełnianego w cyberprzestrzeni, wystarczające jest stwierdzenie wystąpienia w obszarze domeny cyfrowej choćby jednego ze wskazanych elementów, tj. przestępnego działania, zaniechania lub skutku. W rezultacie przyjętej konstrukcji zakres pojęciowy omawianego wyrażenia ulega wydatnemu rozszerzeniu i obejmuje nie tylko typowe, bezsporne przykłady cyberprzestępstw, jak *hacking*, podmiana treści stron czy zakłócanie poprawnego funkcjonowania systemów, lecz także przypadki działań występujących tak naprawdę w całości poza cyberprzestrzenią. Przykładem może być zaniechanie sprawdzenia poprawnego funkcjonowania systemów teleinformatycznych, które może sprowadzić niebezpieczeństwo dla ludzi, np. kierowanie ruchem pojazdów. Ten czyn, choć intuicyjnie nie zalicza

[76] Zob. B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, s. 25 i nast.

się do zjawiska cyberprzestępczości z powodu braku działania w systemach teleinformatycznych, w świetle postanowień definicji będzie właśnie cyberprzestępstwem.

Odwołanie do cyberprzestrzeni przyjęte w omawianej definicji z uwagi na brak wprowadzenia jakichkolwiek ograniczeń powoduje także swoistą konkurencyjność kwalifikacji miejsca popełnienia czynu zabronionego między przestrzenią fizyczną a cyberprzestrzenią, umożliwiając przyjmowanie podwójnej kwalifikacji dla jednego czynu (np. gdy działanie przestępne następuje w świecie fizycznym, skutek zaś pojawia się w cyberprzestrzeni). Takie rozwiązanie, choć nie ułatwia kwalifikowania przestępczości w cyberprzestrzeni, wydatnie zwraca uwagę na ścisłą zależność współczesnych społeczeństw od nowoczesnych technologii, w tym technologii cyberprzestrzeni.

Przy ocenie definicji cyberprzestępstwa proponowanej w krajowej *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, należy stwierdzić, że pomimo jej szerokiego zakresu przedmiotowego, wyznacza ona nowoczesny kierunek utożsamiania cyberprzestępczości z przestępczością popełnianą w cyberprzestrzeni, niezależnie od jej form oraz szczegółowych metod działania sprawcy. Przyjęte założenie pozwala uniknąć tworzenia specyficznych katalogów cyberprzestępstw i stawia swoisty znak równości między przestępczością „klasyczną" a cyberprzestępczością, z jednoczesnym wprowadzeniem kryterium miejsca popełnienia przestępstwa jako determinującym istotę cyberprzestępczości.

Po przeanalizowaniu literatury prawniczej można zauważyć, że pojęcie cyberprzestępstwa coraz częściej występuje w nowych opracowaniach przedmiotu, szczególnie w opracowaniach amerykańskich[77]. Posługuje się nim także Federalne Biuro Śledcze USA – używa go w swoich biuletynach informacyjnych publikowanych na oficjalnej stronie internetowej agencji. W kontekście konwencji o cyberprzestępczości jest ono wykorzystywane także w piśmiennictwie europejskim i zdobywa coraz większą popularność wśród autorów, w tym też autorów polskich. W opracowaniach krajowych tym pojęciem posłużył się przede wszystkim A. Adamski w swoim artykule zatytułowanym *Cyberprzestępczość – aspekty prawne i kryminologiczne* (tekst ukazał się w 2005 r.[78]). Zachowując przekrojowy charakter artykułu, A. Adamski zaprezentował w nim systematykę cyberprzestępczości będącą swoistym rozwinięciem koncepcji przedstawionych wcześniej w innej jego książce pt. *Prawo karne komputerowe* (2000 r.). Na potrzeby analizy omawianego zjawiska A. Adamski podzielił roboczo cyberprzestępczość na cztery kategorie:

1) przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych (np. nieuprawniony dostęp do systemu, podsłuchiwanie transmisji danych lub zakłócanie funkcjonowania systemów),
2) przestępstwa przeciwko dostępowi warunkowemu do usług informacyjnych (np. nieuprawniony dostęp do płatnej, kodowanej telewizji),
3) przestępstwa związane z wykorzystywaniem komputerów (np. oszustwo komputerowe, fałszerstwo komputerowe),
4) przestępstwa związane z rozpowszechnianiem lub przesyłaniem określonych rodzajów informacji (np. propagowanie treści rasistowskich, pornografii dziecięcej czy choćby rozsyłanie niezamówionych informacji handlowych, tzw. spamów).

Przy odwoływaniu się do systematyki przyjętej w *Prawie karnym kompute-*

[77] Na przykład M. Cross, D.L. Shinder, *Scene of the Cybercrime*, b.m.w. [USA] 2008 oraz A. Reyes, *Cyber Crime*… to jedne z najczęściej cytowanych pozycji.

[78] A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4, s. 51 i nast.

rowym, pierwszą kategorię przestępstw można przyrównać do przestępstw stricte komputerowych, podczas gdy kategorie trzecia i czwarta obejmują swoim zakresem zarówno przestępstwa z wykorzystaniem komputera (przestępstwa klasyczne), jak i przestępstwa komputerowe w ujęciu szerokim (przestępstwa, co do których przepis karny przewiduje szczególny modus operandi sprawcy zakładający obligatoryjne wykorzystanie komputera lub sieci). Kategoria druga zawęża analizę wyłącznie do obszaru cyberprzestrzeni i wydaje się być szczególną podgrupą przestępstw kierowanych przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych (zawartych w pierwszej kategorii), i w ten sposób zalicza się ponownie do przestępstw stricte komputerowych.

Wnioski

Poniżej przedstawiono w postaci tabelarycznej wykaz omawianych dokumentów wraz ze wskazaniem, które z definiowanych pojęć było stosowane na gruncie danego dokumentu.

Tabela. Występowanie pojęć związanych z przestępczością w cyberprzestrzeni w dokumentach i literaturze przedmiotu (w ujęciu chronologicznym).

Lp.	Rok wydania	Rodzaj oraz oryginalny tytuł dokumentu źródłowego	Pojęcie stosowane jako centralne	
			w oryginale	w tłumaczeniu
1.	1976	**Opracowanie naukowe**: D.B. Parker, *Crime by Computer*	***computer abuse***	**nadużycie komputerowe**
2.	1979	**Rządowy podręcznik USA**: *Computer Crime: Criminal Justice Resource Manual*	***computer-related crime***	**przestępstwo związane z komputerem**
3.	1986	**Raport OECD**: *Computer-related crime: Analysis of legal policy*	***computer abuse***	**nadużycie komputerowe**
4.	1986	**Ustawa USA:** *Computer Fraud and Abuse Act*	***computer abuse***	**nadużycie komputerowe**
5.	1989	**Zalecenie Komitetu Ministrów Rady Europy**: *Recommendation No. R (89) 9 of the Committee Of Ministers to Member States on Computer-Related Crime*	***computer-related crime***	**przestępstwo związane z komputerem**
6.	1990	**Ustawa Wielkiej Brytanii**: *Computer Misuse Act 1990*	***computer misuse***	**bezprawne użycie komputera**

7.	1990	**Rezolucja ONZ:** *Prevention of Crime and the Treatment of Offenders*	***computer-related crime***	**przestępstwo związane z komputerem**
8.	1994	**Podręcznik ONZ**: *United Nations Manual on the prevention and control of computer-related crime*	***computer crime*** = ***computer-related crime***	**przestępstwo komputerowe** = **przestępstwo związane z komputerem**
9.	1995	**Zalecenie Komitetu Ministrów Rady Europy:** *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with information technology*	***offence connected with Information Technology***	**przestępstwo powiązane z technologią informacyjną**
10.	2000	**Opracowanie naukowe:** A. Adamski, *Prawo karne komputerowe*	**przestępstwo komputerowe**	–
11.	2001	**Konwencja Rady Europy**: *Convention on Cybercrime*	***cybercrime***	**cyberprzestępstwo**
12.	2003	**Rządowy program USA:** *The National Strategy to Secure Cyberspace*	***cybercrime***	**cyberprzestępstwo**
13.	2009	**Rządowy program Polski:** *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011*	**cyberprzestępstwo**	–
14.	2009	**Rządowy program Wielkiej Brytanii:** *Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space*	***cyber crime***	**cyberprzestępstwo**
15.	2011	**Rządowy program Wielkiej Brytanii:** *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*	***cyber crime***	**cyberprzestępstwo**

16.	2011	**Rządowy program Niemiec:** *Cyber Security Strategy for Germany*	***cybercrime***	**cyberprzestępstwo**
17.	2011	**Rządowy program Francji:** *Défense et sécurité des systèmes d'information. Stratégie de la France*	***cybercriminalité***	**cyberprzestępstwo**
18.	2011	**Rządowy program Holandii:** *The National Cyber Security Strategy (NCSS). Success through cooperation*	***cybercrime***	**cyberprzestępstwo**
19.	2013	**Rządowa polityka Polski:** *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*	**cyberprzestępstwo**	***cybercrime*** **(oficjalna wersja ang.)**

Źródło: Opracowanie własne.

Po podsumowaniu najistotniejszych elementów występujących w definicjach analizowanych pojęć można wskazać następujące cechy charakteryzujące fenomen nowoczesnej przestępczości:

- systemy teleinformatyczne oraz sieci mogą służyć zarówno do popełniania tradycyjnych przestępstw (np. oszustwo, zniewaga), jak i przestępstw, które pojawiły się dopiero wraz z pojawieniem się cyberprzestrzeni (np. włamywanie się do zasobów komputerów, przechwytywanie transmisji danych),
- przestępstwa popełniane w cyberprzestrzeni nie ograniczają się metodologicznie wyłącznie do dokonywania określonych czynności technicznych, mających na celu np. przełamanie zastosowanych na serwerze zabezpieczeń, ale mogą polegać także na wykorzystywaniu metod socjotechnicznych, które wprowadzają użytkownika w błąd (np. podanie swojego hasła do skrzynki pocztowej w przekonaniu, że aktywuje nowe, darmowe usługi),
- regulacja karna penalizująca poszczególne cyberprzestępstwa nie musi odnosić określonego czynu wprost do systemów teleinformatycznych. Zakwalifikowanie popełnionego czynu do cyberprzestępczości powinno się odbywać na podstawie kryteriów materialnych, odwołujących się do sposobu oraz miejsca popełnienia danego czynu, nie zaś formalnych,
- systemy oraz sieci mogą być wykorzystywane w zjawiskach przestępnych jako narzędzie oraz jako cel. W przypadku przestępstw zamykających się w całości w cyberprzestrzeni te dwa rodzaje przeznaczenia występują równolegle,
- pojawienie się cyberprzestrzeni wykreowało nowe środowisko dla działań bezprawnych, co spowodowało nie tylko to, że miejscem popełniania nowoczesnych przestępstw jest logiczny obszar domeny cyfrowej, lecz także zmieniło sposób rozumienia dobra prawnie chronionego stanowiącego przedmiot zamachu. Cyberprze-

stępczość często jest kierowana zarówno przeciw samemu bezpieczeństwu systemów teleinformatycznych, jak i bezpieczeństwu danych przetwarzanych w tych systemach w postaci elektronicznej. W zależności od rodzaju danych możliwe jest też dalsze kwalifikowanie czynu np. jako kradzież (w przypadku przesuwania aktywów finansowych między kontami w atakowanej usłudze bankowości elektronicznej),

- przestępczość w cyberprzestrzeni może być popełniana przez bezpośrednie działanie sprawcy bądź przez zautomatyzowane działania odpowiednio przygotowanego systemu lub oprogramowania. Przykładem jest umieszczenie wirusa komputerowego, który może wykraść dane oraz wysyłać je do osoby, która go stworzyła, nawet po kilku latach od umieszczenia go w sieci,
- z uwagi na sposób popełniania cyberprzestępstw ściganie ich sprawców wymaga podejmowania wielu czynności technicznych pozwalających na odnajdywanie elektronicznych dowodów przestępstwa. Pozyskiwanie takich dowodów wymaga przede wszystkim zabezpieczania fizycznych nośników danych oraz tzw. logów wskazujących na historię ruchu sieciowego,
- pośród najczęściej wymienianych cyberprzestępstw można wymienić: bezprawny dostęp do danych lub do systemu (dostęp do systemu nie musi wiązać się z dostępem do chronionych danych, może ograniczać się jedynie do części konfiguracyjnej), uszkadzanie danych, zakłócanie poprawnego funkcjonowania systemu, udostępnianie narzędzi służących do popełniania przestępstw w cyberprzestrzeni (na przykład tzw. exploitów będących gotowymi programami przystosowanymi do wykorzystania określonej podatności systemu), propagowanie w sieciach treści zabronionych czy nielegalne powielanie materiałów chronionych prawami autorskimi lub naruszanie takich praw w inny sposób. Należy dodać, że każde z cyberprzestępstw może być popełnione na wiele sposobów technicznych – nazywanych także atakami – odnoszących się do modus operandi sprawcy.

Pełne ujęcie zjawiska cyberprzestępczości wymaga, w ocenie autora, łącznego objęcia wszystkich wskazanych powyżej cech, wynikających z definicji różnych pojęć.

Bibliografia:

1. Adamski A., *Prawo karne komputerowe*, Warszawa 2000, C.H. Beck.
2. Aldrich R.W., *Cyberterrorism and Computer Crimes*: *Issues Surrounding the Establishment of an International Legal Regime* [online], http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf.
3. Bequai A., *Computer Crime*, Heath 1978, Lexington Books.
4. Cross M., Shinder D.L., *Scene of the Cybercrime*, Burlington 2008, Syngress.
5. Doyle C., *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* [online], Congressional Research Service, http://www.fas.org/sgp/crs/misc/97-1025.pdf.
6. Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, Zakamycze.
7. Fortinet G.L., *Fighting Cybercrime: Technical, Juridical and Ethical Challenges* [online], http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.
8. Goodman M., *Making Computer Crime Count*, „FBI Law Enforcement Biulettin" 2001, t. 70, s. 10–17.

9. Jarrett H.M. i in., *Prosecuting Computer Crimes*, Washington DC 2010, Office of Legal Education, Executive Office for United States Attorneys, Department of Justice.
10. Kliś M., *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.
11. Parker D.B., C*rime by Computer*, New York 1976, Scribner.
12. Reyes A., *Cyber Crime Investigations*, Burlington 2007, Syngress.
13. Schjolberg S., *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva* [online], http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.
14. Sieber U., *Computercriminalitat und Strafrecht*, Köln 1977, Heymann.

Abstrakt

Artykuł stanowi próbę uporządkowania siatki pojęciowej stosowanej w prawie do określenia gałęzi przestępczości zwanej popularnie „komputerową". W tekście zostają przytoczone definicje pojęć: nadużycie komputerowe, przestępstwo związane z komputerem, bezprawne użycie komputera, przestępstwo komputerowe oraz cyberprzestępstwo, używane w rozlicznych dokumentach prawnych, zarówno krajowych, jak i międzynarodowych. Rozważania definicyjne wskazują na swoistą ewolucję rozumienia tego, czym charakteryzuje się omawiana dziedzina czynów bezprawnych. We wnioskach dokonano syntetycznego zestawienia najważniejszych cech definicyjnych wymienionych pojęć oraz wskazano ich najistotniejsze elementy wspólne.

Słowa kluczowe: definicje prawne, cyberprzestępstwo, przestępstwo komputerowe, bezprawne użycie komputera, przestępstwo związane z komputerem.

Abstract

The article is an attempt to regulate terminology that is used in law to define the kind of crime referred to as "computer crime". It contains such definitions as: computer abuse, computer-related crime, unlawful use of computer, computer crime or cybercrime, used in numerous national and international documents. Considerations that have been carried out point out to a kind of evolution in the understanding of what the unlawful activities discussed herein refer to. Conclusions contain a synthetic specification of key definition characteristics of the listed terms, as well as their common elements.

Keywords: legal definitions, cybercrime, computer crime, unlawful use of computer, computer-related crime.

Elżbieta Posłuszna

Terroryzm w czasach globalizacji. Przyczynek do rozważań nad wojnami czwartej generacji

Przekonanie, że wojny wygrywają silni aktorzy, było przez wiele wieków uznawane za dogmat. Rzeczywistość zdawała się ten dogmat potwierdzać. W drugiej połowie XX w. coś się jednak zmieniło. Jak ukazuje to w swej analizie Ivan Arrequin-Toft, przewagę zaczęli zyskiwać słabi – skazani, jak by się wydawało, na pewną porażkę. Jeśli rzeczywista siła (to jest taka, która przekłada się na realne zwycięstwo w konfliktach) coraz częściej jest po stronie potencjalnie słabszej, to należy postawić pytanie: Co sprzyja takiemu stanowi rzeczy? Czy ta tendencja będzie się pogłębiać? Przy podjęciu próby udzielenia odpowiedzi na te pytania, należy zwrócić uwagę na dwa czynniki, które mogą ją dodatkowo wzmocnić: odrzucenie przez słabych aktorów hierarchicznych i centralnie zarządzanych struktur organizacyjnych oraz zaadaptowanie przez nich nowej taktyki opartej na atakach pulsacyjnych.

Siła słabych

Przez wieki uważano (poniekąd słusznie), że podstawą militarnego sukcesu jest przewaga materiałowa, wyrażająca się zazwyczaj w liczbie zbrojnych, posiadanej broni, sprawności logistycznego zaplecza oraz wydolności ekonomicznej państwa. Krótko mówiąc, silny przeciwnik z uwagi na przewagę potencjału powinien zawsze wygrywać. I rzeczywiście, jak pokazuje to Ivan Arrequin-Toft, w większości asymetrycznych konfliktów[1], to jest takich, w których różnica potencjałów wynosi 1:10, silny przeciwnik[2] zwykle wygrywał – w 70,8 proc. konfliktów. Nie wygrywał natomiast w 29,2 proc. konfliktów, a więc nie był w stanie zrealizować zakładanych wcześniej celów (wykres 1).

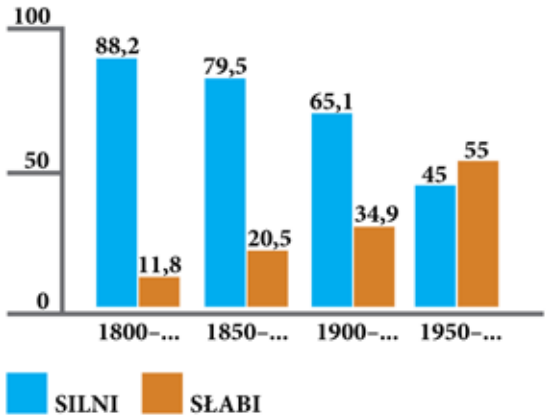
Wykres 1. Procentowy wskaźnik zwycięstw w wojnach asymetrycznych w zależności od typu aktora, lata 1800–1998.

Źródło: I. Arrequin-Toft, *How the Week Win Wars. A Theory of Asymmetric Conflict,* „International Security" 2001, nr 1, s. 93–128. Wykonanie: Kaja Popoff-Szczepańska.

[1] Podstawą rozważań I. Arrequina-Tofta była analiza 197 konfliktów zbrojnych, toczonych w latach 1800–1998.

[2] Silny przeciwnik to według I. Arrequina-Tofta taki aktor, którego potencjał materiałowy przewyższa potencjał adwersarza lub adwersarzy co najmniej dziesięciokrotnie. Konflikt zaś jest definiowany jako wojna, w której przeciętna liczba zabitych wynosi co najmniej 1000 osób.

Jak wynika z analizy wykresu 2, słabi jednak coraz częściej wygrywają konflikty zbrojne. W latach 1950–1998 wygrali aż 55 proc. wojen.



Wykres 2. Procentowy wskaźnik zwycięstw w wojnach asymetrycznych w zależności od typu aktora w poszczególnych latach.

Źródło: I. Arrequin-Toft, *How the Week Win Wars…*, s. 93–128. Wykonanie: Kaja Popoff-Szczepańska.

Dlaczego tak się dzieje? Dlaczego słabi aktorzy często wygrywają, mimo że potencjał militarny, jakim dysponują, skazuje ich na pewną przegraną? Próbę wyjaśnienia tego faktu podejmuje Andrew Mack w artykule *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*[3]. Według niego aktorzy uczestniczący w asymetrycznej walce, w której istnieje duża dysproporcja sił, mają różną polityczną wrażliwość (odporność na wewnętrzną krytykę). Silnych aktorów cechuje niska determinacja i wysoka wrażliwość polityczna. Słabych aktorów zaś charakteryzuje wysoka determinacja oraz niska wrażliwość polityczna. Wysoka wrażliwość polityczna oznacza, że w sytuacji porażek czy przedłużających się działań wojennych oraz opóźnień w realizacji zakładanych celów społeczeństwo dźwigające na sobie ciężar wojny będzie wymuszać na organach władzy i dowodzenia zakończenie konfliktu (casus wojny w Wietnamie). Innymi słowy, asymetria siły determinuje asymetrię zaangażowania – im mniejsza siła, tym większe zaangażowanie i odwrotnie. Wysokie zaangażowanie do pewnego stopnia rekompensuje niewielką siłę. Koncepcja Macka jest dość intuicyjna, jednak niewiele tłumaczy, nie wyjaśnia m.in. dlaczego na przestrzeni wieków słabi coraz częściej wygrywają wojny.

O wiele bardziej interesująca jest koncepcja Ivana Arrequina-Tofta, której dał wyraz w artykule *How the Week Win Wars. A Theory of Asymmetric Conflict*. Toft wyróżnia dwa typy idealne strategicznego podejścia: bezpośrednie i pośrednie. Podejście bezpośrednie (BP) jest wymierzone w siły militarne adwersarza (celem jest fizyczne zniszczenie przeciwnika). Charakterystyczne dla niego są: klasyczny atak (użycie wojska w celu eliminacji sił militarnych przeciwnika, aby zdobyć kontrolę nad jego wartościami, tj. terytorium, ludnością, zasobami materialnymi i niematerialnymi –

[3] A.J.R. Mack, *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*, „World Politics" 1975, nr 2.

np. systemami przekonań i systemami aksjologicznymi) oraz klasyczna obrona (użycie zbrojnej siły wymierzonej w wojsko adwersarza w celu udaremnienia zniszczenia wyżej wymienionych wartości). Podejście pośrednie (PP) jest wymierzone w wolę walki przeciwnika. Należą do niego barbaryzm, definiowany jako pogwałcenie prawa wojennego (tortury, zastraszanie ludności, morderstwa), oraz guerrilla, definiowana jako walka małych oddziałów unikających bezpośredniej konfrontacji z wrogiem. Silny aktor zwykle stosował dwa strategiczne podejścia: bezpośredni atak (BP) oraz barbaryzm (PP), podczas gdy słaby aktor stosował bezpośrednią obronę (BP) oraz guerrillę (PP).

Na podstawie przeanalizowania 197 konfliktów toczonych w latach 1800–1998 Toft stwierdza, że kluczem do wyjaśnienia tego, że słabi wygrywają wojny, jest wybór opozycyjnego podejścia strategicznego. Interakcja podobnego podejścia (bezpośrednie–bezpośrednie oraz pośrednie–pośrednie) implikuje porażkę słabych aktorów. I odwrotnie, opozycyjne podejście w interakcji (bezpośrednie–pośrednie oraz pośrednie–bezpośrednie) implikuje zwycięstwo słabego aktora (walka jest zwykle długa, a czas sprzyja słabym). Innymi słowy silni aktorzy wygrywają, gdy mają to samo strategiczne podejście, co przeciwnicy, a przegrywają, gdy mają inne. W rezultacie w konfliktach toczonych w latach 1800–1998 silni zwyciężali w 76 proc. konfliktów o tym samym strategicznym nastawieniu, słabi zaś – w 63 proc. konfliktów o przeciwnym strategicznym nastawieniu.

Analizy Tofta wspierają hipotezę o istnieniu dużego prawdopodobieństwa, że silni przegrają wojny, gdy zaistnieje opozycyjne nastawienie. Ponieważ ta hipoteza jest oparta na analizie faktów, ma niewątpliwie swoją moc perswazyjną. Nie wyjaśnia jednak wszystkiego. A mianowicie: dlaczego coraz częściej słabi sięgają po podejście opozycyjne, które zwykle przyjmuje formę działania pośredniego – działań nieregularnych (podczas gdy silny aktor stosuje działanie bezpośrednie – wymierzone w siły militarne przeciwnika)? Dlaczego to podejście (działania nieregularne) jest coraz bardziej skuteczną formą walki? Czy będzie tak również w przyszłości? I bardziej ogólnie: skoro rzeczywista siła (to jest taka, która przekłada się na realne zwycięstwo w konfliktach) coraz częściej jest po stronie potencjalnie słabszych, to co sprzyja takiemu stanowi rzeczy? Co sprzyja sile słabych? I czy można się tej sile przeciwstawić?

Ewolucja działań wojennych – zmiana paradygmatów

Przekonanie wielu pacyfistów, że człowiek jest z natury dobry i pokojowo nastawiony do innych, nie znajduje potwierdzenia w rzeczywistości. Działania o charakterze wojennym są wpisane w historię zorganizowanych społeczeństw. Zwykle celem działań agresora było opanowanie określonego terytorium, podporządkowanie sobie miejscowej ludności i wyciągnięcie korzyści ekonomicznych. Strona atakowana miała odwrotny cel – obronę własnego terytorium przed agresorem. Wojna, wyjąwszy przypadek wojny domowej, była zwykle prowadzona przy współpracy trzech stron: armii, narodu i rządu[4]. Ta Clausewitzowska triada przez wieki funkcjonowała właściwie bezbłędnie. Rząd wypowiadał wojnę i wyznaczał jej polityczne ramy, armia realizowała wojenne cele, naród zaś dostarczał żołnierzy oraz dóbr koniecznych do jej prowadzenia. Przeobrażenia w zakresie polityki, ekonomii i technologii zmieniły ten stan rzeczy. Historyk wojskowości William S. Lind w artykule

[4] Tę kwestię rozwija R. Brzeski w artykule *Wojna czwartej generacji* [online], http://niepoprawni.pl/blog/6063/wojna-czwartej-generacji [dostęp: 20 III 2016].

z 1989 r. pt. *The Changing Face of War: into the Fourth Generation* zamieszczonym w „Marine Corps Gazette" (nr 10) opisał zmieniające się oblicze wojen, wyróżniając ich cztery generacje.

Wojny pierwszej generacji zaczęły wybuchać w XVII wieku wraz z wykrystalizowaniem się świadomości narodowej (wcześniej były postrzegane jako „sport królów" i zwykle nie wzbudzały specjalnego entuzjazmu ludu), swoją kulminację zaś znalazły w okresie wojen napoleońskich. Charakteryzowały się wykorzystywaniem wielkich mas ludzkich (zwykle poborowych) sformowanych w linie i kolumny, ścierających się na polu bitwy. Były one wystawiane przez królestwa bądź państwa narodowe. Podstawą działań bitewnych była musztra, bo tylko ona umożliwiała synchronizację w oddawaniu ognia. Głównym celem wojennym było nie tyle zajęcie określonego terytorium, co zniszczenie armii przeciwnika. Teoretykiem wojen pierwszej generacji był Carl Philipp Gottlieb von Clausewitz.

Wojny drugiej generacji zrodziły się na początku I wojny światowej. Ich charakter określała zmasowana siła ognia (broń maszynowa), która z jednej strony wymuszała rozproszenie oddziałów (niektóre z nich operowały samodzielnie), z drugiej skłaniała do działania w okopach i atakowania tyralierą. Ta wojna oznaczała przewagę obrony nad atakiem. Taktycznym celem działań było opanowanie lub zniszczenie ośrodków przemysłowych bądź dużych ośrodków miejskich. Pole bitwy (tak jak w wojnach pierwszej generacji) miało charakter linearny, jednak było szersze ze względu na zasięg artylerii. Próby ataków zwykle kończyły się dużymi stratami w ludziach i siłą rzeczy prowadziły do impasu. Teoretykiem tego rodzaju wojny był feldmarszałek Helmuth von Moltke.

Początek wojen trzeciej generacji wyznaczała wojna polsko-bolszewicka, szczytową formą był blitzkrieg, zamknięciem zaś wojna o Kuwejt. W wojnach trzeciej generacji najistotniejsza stała się zdolność manewrowa, uzyskana w dużej mierze dzięki czołgom. Faworyzowanie tych możliwości było rezultatem refleksji wyciągniętej z I wojny światowej, zgodnie z którą wysyłanie żołnierzy do frontalnego ataku na karabiny maszynowe umieszczone w okopach nie miało sensu. Wojna manewrowa bazowała na czołgach, mobilnej piechocie, artylerii, siłach powietrznych oraz łączności. Doktryna wojny manewrowej zalecała omijanie silnie bronionych punktów oraz otaczanie wrogich sił. Duże znaczenie w tej wojnie miała inicjatywa własna dowódców pojedynczych jednostek. Teoretykiem wojen trzeciej generacji był Sir Basil Liddell Hart.

Jak słusznie zauważa Rafał Brzeski, te trzy typy wojen mieściły się jeszcze w ramach paradygmatu Carla von Clausewitza, w którego myśl państwo sprawuje pieczę nad działaniem armii narodowej, wspieranej z własnej woli bądź przez większość społeczeństwa[5]. Pod koniec XX w. coś się jednak zmieniło i Clausewitzowski model powoli przestał być aktualny. Stało się tak za sprawą przemian, do jakich doszło niemal we wszystkich zakątkach świata. Objęły one swym zasięgiem także charakter działań wojennych. Najważniejszą z tych przemian była globalizacja[6].

Choć **globalizacja** jest zjawiskiem zarówno gospodarczym, politycznym, jak i kulturowym, to w opracowaniach na jej temat zwykle przeważają rozważania o charakterze ekonomicznym[7]. To zjawisko jest w nich ujęte jako związane z odśrodkowymi

[5] Tamże.

[6] Więcej na temat globalizacji w: E. Posłuszna, *Ekstremizm ekologiczny – źródła, przejawy, perspektywy*, Warszawa 2012.

[7] Dzieje się tak nadal, mimo że coraz częściej wskazuje się także na inne wymiary globalizacji, np. wymiar ekologiczny, militarny czy społeczno-kulturowy. Zob. J.S. Nye, R. Keohane, *Globalization. What's*

przekształceniami w obrębie kapitalizmu, które zmierzają w kierunku sieciowej międzynarodowej produkcji, coraz bardziej wymykającej się kontroli narodowej czy etnicznej. Źródłem tych odśrodkowych przemian jest pojawienie się po II wojnie światowej instrumentów i instytucji odpowiedzialnych za swobodny przepływ towarów, usług i ludzi ponad granicami państw narodowych[8], takich jak np. Międzynarodowy Fundusz Walutowy, Bank Światowy lub Światowa Organizacja Handlu. Wymienione instytucje nie są oczywiście jedynymi, które działają na rzecz zniesienia ograniczeń w swobodnym przepływie kapitału i usług, ale ich wpływ na rozwój globalizacji z rozmaitych względów jest postrzegany jako najbardziej znaczący. Jedną z politycznych konsekwencji liberalizacji światowej gospodarki (w perspektywie badań nad przyszłością terroryzmu najbardziej nas tu interesujących) jest powolna utrata przez państwa narodowe możliwości kontroli nad działaniami gospodarczymi[9]. Oczywiście państwa narodowe nadal jeszcze podejmują decyzje (z formalnoprawnego punktu widzenia mają charakter suwerenny), są jednak coraz bardziej ograniczone przez międzynarodowe uwarunkowania ekonomiczne i polityczne (instytucje gospodarcze, korporacje transnarodowe, organizacje międzynarodowe czy zwykłe układy). W tych warunkach państwa stają się coraz mniej podobne do scentralizowanych, częściowo autonomicznych struktur, zdolnych sprawować suwerenną władzę w obrębie granic swojego terytorium. Uzależnione od międzynarodowych instytucji, zaczynają działać bardziej na zasadzie „pasów transmisyjnych" ułatwiających przepływ dóbr i kapitału w obszarach podlegających ich coraz bardziej wątpliwej jurysdykcji[10]. Wiele wskazuje na to, że nawet ta ich skromna funkcja może w przyszłości zostać podana w wątpliwość. Proces funkcjonowania gospodarek poza kontekstami narodowymi (ta ich swoista „deterytorializacja") wpływa szczególnie silnie na sferę polityki i kultury. Zmiany w nich zachodzące są czasem opisywane w kategoriach zaniku narodowej suwerenności politycznej oraz kultury określanej jako „narodowa". W rezultacie tych zmian państwo przestaje kontrolować przypływ informacji, ludzie zaś (oraz samo państwo) stają się coraz bardziej wrażliwi na globalne zdarzenia[11]. Ten proces postępuje, rzecz jasna, stopniowo, niemniej jednak jest trwałym trendem, w istotny sposób wpływającym na bezpieczeństwo, w tym na możliwość wzrostu zagrożeń asymetrycznych.

Globalizacja, zaplanowana i wykreowana przez sieci bogactwa i władzy, całkowicie zmienia nasz świat. Abstrakcyjność władzy zaowocowała rozpadem dotychczasowych mechanizmów kontroli społecznej i reprezentacji politycznej, czego rezultatem jest poczucie utraty panowania przez obywateli nad swoim życiem, pracą, gospodarka-

new? What's not? (and so what?), w: *Power in the Global Information Age. From Realism to Globalization*, J.S. Nye (red.), London–New York 2004, s. 192–193.

[8] Określenie początków globalizacji zależy bez wątpienia od sposobu jej definiowania. Najczęściej początki procesów globalizacyjnych są sytuowane po II wojnie światowej, niektórzy badacze jednak są skłonni umiejscawiać je znacznie wcześniej, np. w okresie wielkich odkryć geograficznych, kolonializmu czy w XIX wieku. Sam termin g l o b a l i z a c j a pojawił się w literaturze naukowej w latach 60. XX w. Patrz m.in. R. Kuźniar, *Globalizacja, polityka i porządek międzynarodowy*, w: *Globalizacja a stosunki międzynarodowe,* E. Haliżak, R. Kuźniar, J. Symonides (red.), Bydgoszcz–Warszawa 2003.

[9] Odrębną sprawą jest istnienie tzw. państw upadłych, które w wyniku konfliktów domowych oraz procesów globalizacyjnych utraciły możliwość kontrolowania swojego terytorium. Te państwa w naturalny sposób stają się bazą grup terrorystycznych, które bez obaw mogą tam prowadzić obozy szkoleniowe lub werbować aktywistów.

[10] Por. R. Cox, *Production, Power and World Order: Social Forces in the Making of History*, New York 1987.

[11] T. Blyth, *Terrorism as Technology: a Discussion of the Theoretical Underpinnings*, w: *Technology and Terrorism*, D. Clarke (red.), New Brunswick–London 2004, s. 44.

mi, rządem i środowiskiem naturalnym. Również państwo narodowe (dawniej źródło wartości i sensu egzystencji), omijane przez globalne sieci bogactwa, straciło możliwość reprezentowania swych terytorialnie zakorzenionych społeczności, stając się „pustą skorupą", coraz mniej zdolną do bycia punktem odniesienia. W ten sposób świat staje się dla większości ludzi obcy, gdyż źródła mocy jawią się jako będące poza zasięgiem.

Taki stan rzeczy niesie za sobą poważne konsekwencje, jeśli chodzi o możliwość tworzenia i utrzymywania społecznych tożsamości[12]. Potrzeba odczuwania przez zbiorowość sensu współistnienia bowiem nie zanika. Wprost przeciwnie – wobec braku zinstytucjonalizowanego jego dostarczyciela (państwa), potrzeba ta staje się silniejsza i bardziej roszczeniowa, czego rezultatem jest pojawienie się ekspresji zbiorowych tożsamości, rzucających wyzwanie globalizacji w imię kulturowej wyjątkowości oraz przejęcia przez ludzi kontroli nad własnym życiem. Te nowe tożsamości buntują się przeciw dominacji legalnych, a także globalnych struktur oraz przeciw bezsilności, której doświadczają, określając nowe źródła sensu i wartości. Globalizacja anihiluje granice kulturowe; w rezultacie dochodzi do dezintegracji przestrzeni społecznej, co owocuje fragmentaryzacją tej przestrzeni – wyodrębnieniem się silnych „kulturowych enklaw" usilnie broniących swoich tożsamości i niechcących mieć nic wspólnego z innymi tego typu enklawami czy globalnym nurtem masowej kultury. Globalizacja nie tworzy jedności, raczej erupcję zbiorowych i indywidualnych tożsamości. Te tożsamości kwestionują to, co do niedawna wydawało się trudne do zakwestionowania (przynajmniej na gruncie kultury zachodniej), a mianowicie demokrację opartą na historycznej konstrukcji państwa obywatelskiego, które jako źródło legitymizacji także zostaje zakwestionowane. Rzucają także wyzwanie logice nowego porządku globalnego, który przez wielu jest odczuwany jako nieporządek. To wyzwanie nie jest manifestacją bezsilnego oporu słabych, lecz realną siłą, która się może stać źródłem zmiany w świecie, także w zakresie identyfikacji wroga. Wrogiem nie jest już inne państwo narodowe, lecz wszyscy, którzy ograniczają subiektywnie postrzeganą wolność – inne grupy, jednostki, instytucje. W ten właśnie sposób obok globalizacji pojawia się zjawisko odwrotne – fragmentaryzacja.

Fragmentaryzacja wyraża się na dwa sposoby: jako wieloetniczne społeczeństwo istniejące w ramach jednego państwa (np. emigranckie wspólnoty w USA) oraz jako społeczności sieciowe – transgraniczne grupy interesów, które łączą wspólne emocje i interesy (np. obrońcy środowiska, grupy anarchistyczne lub prawicowe). Jedni i drudzy mają na celu „kulturowy apartheit", czego skutkiem jest kontestacja dawnych struktur lojalności, usankcjonowanych przez wieki tradycji. Nowe struktury lojalności stają się silniejsze, nie są to bowiem struktury zastane, do których przynależność była odgórnie przypisana (decydowało o tym zwykle urodzenie – w danej gminie, wspólnocie, państwie), lecz coś, co się „emocjonalnie wybrało" i do czego miało się co najmniej aksjologiczną skłonność. Opozycyjność nowych struktur lojalności (nowych tożsamości) oraz brak takich, które by je odgórnie mocno spajały, skazuje je na walkę w imię jednej jedynej prawdy, która jest ich udziałem. Nie jest to, co prawda, Hobbesowska „walka każdego z każdym", angażuje jednak dużą liczbę aktorów i jest intensywna.

Charakter i przebieg wojen czwartej generacji trudno jest jeszcze opisać. Istnieje jednak wiele przesłanek, aby pokusić się o stworzenie ich zarysu, czego dokonało w ostatnich latach wielu autorów. Wśród podstawowych cech tych wojen wymienia się najczęściej: długotrwałość, dominację działań nieregularnych, stosowanie metod ter-

[12] Por. M. Castells, *Siła tożsamości*, Warszawa 2008, s. 22.

rorystycznych, transnarodową i ponadnarodową podstawę konfliktu, brak centralizacji zarządzania, wykorzystanie mediów, manewrowość, niemożność wyznaczenia granicy między wojną a pokojem, skoncentrowanie działań na cywilach oraz ich zapleczu (wojna pośród ludzi), oparcie tych wojen na ideach (walka informacyjna i propagandowa) oraz to, że działania wojenne składają się z wielu krótkich potyczek (rojenie).

W 1991 r. Martin von Creveld w swojej książce *Transformation of War* stwierdził, że wojny prowadzone w Clausewitzowskim paradygmacie (ściśle powiązanych z sobą: rządu, armii i narodu) będą powoli zanikać[13]. Zastępować je będą konflikty rozproszone, o niskiej intensywności (toczone pomiędzy rozmaitymi grupami: etnicznymi, religijnymi, ideologicznie zorientowanymi oraz samymi państwami), w których będą się zacierać różnice pomiędzy żołnierzami a cywilami, frontem a tyłami. Wojny te, twierdzi Creveld, mimo zaangażowania w nie wielu mniejszych aktorów, będą krwawe i okropne. Thomas X. Hammer, emerytowany pułkownik US Marine Corps, w swoim studium pt. *The Sling and the Stone: On War in the 21st Century* opisywał wojnę czwartej generacji jako rozwiniętą formę aktywności powstańczej, w której dąży się do zastosowania wszystkich dostępnych sieciowych powiązań po to, aby nie tyle pokonać militarnie wroga, co przekonać jego decydentów, że cele, do których zmierzają, są niewarte ponoszonych kosztów[14]. Wspomniane przez Hammesa powiązania sieciowe to wszelkie hierarchiczne i niehierarchiczne relacje – polityczne, społeczne, ekonomiczne, militarne, które za sprawą pojawiających się technologii komunikacyjnych tworzą nową morfologię społeczną, negującą dawną konfigurację interesów, to znaczy taką, która biegnie niezależnie od tradycyjnych konfiguracji społecznych.

Walka sieciowa i opór bez przywództwa

Mimo wpisanej w społeczeństwo sieci negacji dawnych powiązań społecznych, które zwykle były hierarchiczne i wykluczające, bycie w sieci nie oznacza równości. W strukturę sieci jest wpisana także nierówność wynikająca z różnej ważności jej poszczególnych węzłów oraz charakteru poszczególnych sieci (sieci finansowe, społeczne, towarowe, kulturowe). Niektóre węzły są „silne" – sprawują nad innymi kontrolę i dają początek przepływom (korporacje, wielkie firmy działające na skalę światową), inne są tylko odbiorcami przepływów (konsumenci)[15]. Silne węzły kontrolują dostęp do światowej sieci przepływów informacji i dóbr, skazując tych, którzy dostępu do niego nie mają lub dla których jest on ograniczony, na mniejsze lub większe wykluczenie. Wykluczeni (jednostki, klasy czy narody) tworzą „czwarty świat" złożony z „czarnych dziur informacyjnego kapitalizmu"[16] – obszarów zamieszkałych przez tych, którzy w porównaniu z uczestnikami sieci przepływów niewiele znaczą (z uwagi na ich znikomy wkład w konsumpcję, pracę, życie społeczne), tj. bezdomnych, mieszkańców ubogich dzielnic i krajów. W ten sposób globalizacja, uobecniona w sieci przepływów, tworzy świat biedy i wykluczenia. Świat, który zaczyna wrzeć i przygotowuje się do podjęcia walki określanej przez wielu autorów jako „walka sieciowa".

[13] Patrz: M. von Creveld, *Transformation of War,* New York 1991, s. 198.

[14] W wojnach czwartej generacji dąży się zatem do zniszczenia woli politycznej przeciwnika. Patrz: T.X. Hammes, *The Sling and the Stone: On War in the 21st Century*, St. Paul, MN, 2004; G. Michael, *Lone Wolf Terror and the Rise of Leaderless Resistance*, Nashville 2012, s. 15.

[15] Por. D. Barney, *Społeczeństwo sieci*, Warszawa 2008, s. 42.

[16] M. Castells, *End of Millenium*, Oxford 1998, s. 166–170.

Koncepcję walki sieciowej (zwanej także „wojną sieciową") opracowali analitycy RAND Corporation, m.in. John Arquilla, David Ronfeldt i Michele Zanini w pracach pt. *The Advent of Netwar, Countering the New Terrorism* oraz *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Twórcy terminu w a l k a s i e c i o w a, Arquilla i Ronfeldt, w pracy *The Advent of Netwar* wyjaśniają to pojęcie w następujący sposób:

> Termin „wojna sieciowa" odnosi się do wyłaniającej się formy konfliktu (i przestępczości) na poziomie społecznym, w której wykorzystywane są środki mniej intensywne niż wojenne, jak również sieciowe formy organizacyjne, doktrynalne, strategiczne i komunikacyjne. Strony uczestniczące w takich konfliktach składają się zazwyczaj z rozproszonych, często małych grup oraz odpowiadających im komunikacji, koordynacji i działań sieciowych, często bez określonego scentralizowanego przywództwa oraz ośrodków dowodzenia. Podejmowanie decyzji może być rozmyślnie zdecentralizowane i rozproszone. (...) Podmioty objęte spektrum konfliktów społecznych i przestępczych ewoluują w stronę wojny sieciowej. Dotyczy to podmiotów, które modyfikują swoje struktury i strategie w celu czerpania korzyści płynących z rozwoju modeli sieciowych, jak np. międzynarodowe grupy terrorystyczne, czarnorynkowi handlarze broni masowego rażenia, narkotyków i inne syndykaty przestępcze, ruchy fundamentalistyczne i nacjonalistyczne, złodzieje własności intelektualnej oraz przemytnicy uciekinierów i emigrantów. Niektóre wielkomiejskie gangi, wiejskie organizacje milicyjne, walczące grupy jednej sprawy (...) także rozwijają swój potencjał sieciowy. Ale to nie wszystko. W spektrum wojny sieciowej coraz częściej znajdować się będzie nowa generacja rewolucjonistów i aktywistów wyznających postindustrialne ideologie ery informacyjnej, które właśnie dziś się kształtują. W niektórych przypadkach, tożsamości i uczucia lojalności mogą przesunąć się z poziomu narodowego na ponadnarodowy poziom „globalnego społeczeństwa obywatelskiego". W wojnie sieciowej wziąć udział mogą też nowego typu podmioty – np. członkowie anarchistycznych i nihilistycznych sprzysiężeń wykwalifikowanych informatycznie cyber-sabotażystów[17].

Walkę sieciową z uwagi na wykorzystywanie niemilitarnych środków (m.in. informacji i narzędzi cybernetycznych) oraz zaangażowanie niescentralizowanych jednostek i grup niebędących reprezentantami ugrupowań, partii lub organizacji nazywa się „konfliktem o stosunkowo niedużej intensywności". Takie określenie może być nieco mylące. W tym konflikcie bowiem występuje silna społeczna mobilizacja biorąca się z możliwości pozyskiwania „dla sprawy" szerokiego, globalnego wręcz audytorium. Znaczenia nabierają też niescentralizowane formy organizacyjne – nowe modele sieciowe, bardziej bezpieczne (pod względem odporności na inwigilację) i efektywne (pod względem zdolności zadawania wysokich strat przy udziale minimum zaangażowanych środków) niż dotychczasowe struktury hierarchiczne. W walce sieciowej wykorzystuje się rozmaite formy powiązań, np. **powiązania łańcuchowe** (*chain network*, *line network*). W takim przypadku komunikacja między poszczególnymi ogniwami (wymiana dóbr i informacji) przebiega wzdłuż linii ogniw połączonych jedynie ośrodkami sąsiadującymi. Ten typ struktury sieciowej najczęściej można spotkać w przypadku gangów przemytniczych.

Innym typem powiązań jest **sieć węzłowa** (*star network*, *hub network*, *wheel network*). Tu komunikacja między ośrodkami i koordynacja działań jest uzależniona od ośrod-

[17] J. Arquilla, D. Ronfeldt, *The Advent of Netwar*, Santa Monica 1996, s. 5–6.

ka centralnego, swoistego węzła pośredniczącego, który pełni funkcję przekaźnika informacji i dóbr. Nie jest to jednak komunikacja zorganizowana hierarchicznie. Bywa i tak, że poszczególne ośrodki nic nie wiedzą o sobie wzajemnie. Ten typ najczęściej można spotkać zarówno w kartelach czy franczyzach, jak i w przypadku ugrupowań terrorystycznych.

Kolejnym rodzajem powiązań jest **sieć wszechkanałowa** (*all-channel network*, *full-matrix network*). W przypadku tej sieci wszystkie ośrodki są powiązane ze sobą – każdy z każdym. Nie ma tu jakichkolwiek wyróżnionych węzłów, a komunikacja między wybranymi punktami sieci może się dokonywać niezależnie od wszelkich pozostałych powiązań. Najczęściej ten typ powiązań odnajduje się wśród ugrupowań wojowniczych (szczególnie wśród tzw. ugrupowań jednej sprawy[18]), które są w wysokim stopniu zdecentralizowane i zinformatyzowane. Wśród tych niescentralizowanych form wykorzystywanych w walce sieciowej ważne miejsce zajmuje opór bez przywództwa[19].

Za twórcę koncepcji oporu bez przywództwa uchodzi pułkownik Ulius Louis Amoss, oficer CIA, który w 1953 r. twierdził, że walka z komunizmem (w wypadku agresji ZSRR na USA) powinna być oparta na niescentralizowanych formach organizacyjnych, czyli takich, w których elementem jednoczącym jest nie przywódca, lecz wspólna (podzielana przez wszystkich bojowników) myśl[20]. W podobnym duchu wypowiadał się w 1983 r. radykalny działacz amerykańskiej prawicy Louis Beam, który w swoim słynnym eseju zatytułowanym *Leaderless resistance* stwierdził, że pora już odejść od piramidalnych form organizacyjnych i (…) *rozważyć inne metody organizacji, które najlepiej byłoby określić jako organizacje bez organizacji*[21]. Podobne idee pojawiły się też w innych publikacjach. W 1972 r. w podręczniku ekologicznego sabotażu pt. *Ecotage!* można przeczytać: *Siła ruchu polega na tym, że nie posiada on formalnej struktury i nie może być powstrzymany przez eliminację kluczowych przywódców. I chociaż nie opiera się na sztywnych regułach, jest on jednak zunifikowany dzięki swej filozofii szacunku dla życia*[22]. O p ó r b e z p r z y w ó d z t w a to innymi słowy strategia (a zarazem nowa forma organizacji), która zakłada rezygnację z wszelkich hierarchicznych struktur, które zostają zastąpione luźną konfiguracją niewielkich, autonomicznych komórek, jednostek bądź małych grup, którymi nie kieruje żaden ośrodek decyzyjny. Elementem jednoczącym jest w takim przypadku ideologia, z której członkowie ruchu czerpią wiedzę na temat skutecznych form walki.

Powyższy opis oporu bez przywództwa to oczywiście opis typu idealnego. W rzeczywistości w twierdzeniu o braku przywództwa chodzi o formalny wymiar tego przywództwa – o brak rozkazotwórczej siły zdolnej wymuszać posłuch wśród podporządkowanych jej aktywistów. W oporze bez przywództwa istnieje jednak przywództwo duchowe. Jego źródłem są konkretni ludzie, którzy za pośrednictwem nowych technologii komunikacyjnych – przede wszystkim Internetu – tworzą i rozpowszechniają idee, pod których szyldem jest prowadzona walka (czasem też ukierunkowują aktywność sympatyków tych idei). Nie robią tego jednak bezpośrednio – nie wydają rozkazów, nie kontrolują poczynań

[18] Tym mianem określa się zwykle radykalne ugrupowania prozwierzęce (np. Animal Liberation Front), prośrodowiskowe (np. Earth First!) oraz antyaborcyjne (np. Armia Boga).

[19] Więcej na ten temat autorka pisze w: E. Posłuszna, *Ekstremizm ekologiczny – źródła, przejawy, perspektywy*, Warszawa 2012.

[20] Patrz: http://www.publiceye.org/liberty/terrorism/insurgency/amoss.html [dostęp: 20 III 2016].

[21] L.R. Beam, *Leaderless Resistance* [online], „The Seditionist" 1992, nr 12, http://www.louisbeam.com/leaderless.htm. [dostęp: 20 III 2016].

[22] *Ecotage!*, S. Love, D. Obst (red.), New York 1972; cyt. za: R. Arnold, *Eco-Terror. The Violent Agenda to Save Nature. The World of the Unabomber*, Bellevue–Washington 1997, s. 125.

aktywistów ani nie spotykają się z nimi. Opór bez przywództwa w swym idealnym kształcie jest zjawiskiem nader rzadkim. Zwykle organizacje, które chętnie go wykorzystują, przyjmują formy hybrydowe – są połączeniem hierarchii, rozmaitych form sieciowych i oporu bez przywództwa. Złożone struktury organizacyjne mogą być zróżnicowane na poszczególnych poziomach funkcjonowania, np. na poziomie najwyższym mogą funkcjonować zgodnie z którąś z sieciowych form organizacji, hierarchizując jednocześnie organizację poszczególnych ośrodków sieci. Hierarchiczne struktury organizacyjne mogą też posługiwać się sieciowymi formami organizacji któregoś ze swoich elementów. Mogą to robić stale lub doraźnie w celu np. wykonania jakiegoś zadania, którego nie mógłby sprawnie wykonać organ mający strukturę hierarchiczną. Cała zaś organizacja może być oparta na funkcjonowaniu według modelu oporu bez przywództwa, tzn. zachęcać potencjalnych aktywistów do takiego właśnie uczestnictwa w organizacji.

Zalety strategii oporu bez przywództwa są oczywiste. W strukturze tradycyjnej, a więc hierarchiczno-piramidalnej, policyjny agent, jeśli tylko zdoła przeniknąć na określony szczebel przestępczej hierarchicznej piramidy, bez trudu zniszczy wszystkie szczeble znajdujące się poniżej jego własnego poziomu zaczepienia oraz zagrozi szczeblom znajdującym się powyżej. Niebezpieczeństwo infiltracji jest o wiele mniejsze w przypadku „organizacji", w których pojedyncze indywidua lub niewielkie grupy nie tylko nie mają organizacyjnego centrum, lecz także działają bez jakiegokolwiek strukturalnego powiązania pomiędzy sobą. W organizacjach tego typu podstawowym elementem jednoczącym staje się ideologia – rozpowszechniana zwykle za pośrednictwem Internetu, z którego członkowie ruchu czerpią też wiedzę na temat właściwych (tj. skutecznych i moralnie, w ich mniemaniu, słusznych) metod walki[23]. Nie jest to jedyna zaleta oporu bez przywództwa. Daje on także możliwość odcięcia się od działań niepożądanych pod pretekstem, że nie spełniają one kryteriów ideowych – nie mogą zatem być przypisane danej organizacji. Ponadto pozwala uznać za własne te akcje, które pasują do przyjętego wzorca działań bezpośrednich (choć w istocie mogły one zostać dokonane przez kogoś innego i z całkiem innych powodów). Inaczej rzecz ujmując, to rodzaj akcji przesądza o tym, czy dane działanie zostanie wpisane w działalność organizacyjną. Oczywiście, opór bez przywództwa ma także i wady. Brak hierarchii oraz rozmycie organizacyjne nie pozwalają na realizowanie tymetycznych[24] ambicji, które zwykle leżą u podstaw ruchów społecznych (są ich siłą napędową). Ponadto brak centralnego zarządzania oznacza, że nikt tak naprawdę nie ma większej kontroli nad poczynaniami potencjalnych aktywistów, uważających się za członków organizacji. W przypadku gdy „nieprawowiernych" członków będzie wielu, może to doprowadzić do trwałego „organizacyjnego rozmycia" bądź kompromitacji całej organizacji. Aby do tego nie doszło, idee muszą być silne, a drogi „jedynie słusznej" aktywności jasno wytyczone. Dlatego tak ważne są źródła idei, w imię których jest prowadzona walka. Tworzą je jednostki najbardziej zaangażowane, zdolne zrezygnować z formalnych atrybutów władzy, które daje przynależność do tradycyjnej, hierarchicznej organizacji, na rzecz władzy realnej – w niczym niezapośredniczonego przywództwa duchowego.

W oporze bez przywództwa zalety przeważają nad wadami. Nie bez powodu w drugiej połowie lat 80. XX w. wiele organizacji zaczęło powoli odchodzić od centralistycznych i hierarchicznych struktur ku strukturom luźniejszym, bardziej elastycznym

[23] Szerzej zob. J. Posłuszny, *http://www.nowyterroryzm.org*, w: *U progu wielkiej zmiany? Media w kulturze XXI wieku. Nurty, kategorie, idee*, M. Sokołowski (red.), Olsztyn 2005, s. 529–531.

[24] Nawiązanie do Francisa Fukuyamy, który twierdził, że przyczyn konfliktów społecznych należy szukać nie w dążeniu do zdobycia zasobów materialnych, lecz w zaspokojeniu potrzeby uznania (*thymos*).

i mniej podatnym na dekompozycję, choć zarazem bardziej zagrożonym rozpadem. Wiele z nich zdecydowało się uczynić opór bez przywództwa podstawą swojej egzystencji. Uczyniły tak najpierw organizacje ekstremistyczne jednej sprawy, w ślad za nimi poszły organizacje prawicowe i rasistowskie, a w latach 90. dołączyła do nich część ugrupowań anarchistycznych. Na początku XXI wieku opór bez przywództwa został przyjęty przez większość organizacji o zasięgu globalnym. Nic nie wskazuje na to, aby popularność tego modelu miała się zmniejszyć. Opór bez przywództwa to nie tylko organizacja, to także pewien sposób taktycznego funkcjonowania, określany jako *swarming* (rojenie). J. Arquilla i D. Ronfeld definiują *swarming* w następujący sposób:

> Swarming to pozornie amorficzny, lecz w gruncie rzeczy ustrukturyzowany i skoordynowany strategiczny sposób uderzenia ze wszystkich stron na szczególny punkt bądź punkty, za pomocą trwałego pulsowania siły i/lub ognia, zarówno z wewnętrznych, jak i zewnętrznych pozycji. Pojęcie „siły i/lub ognia" można tu rozumieć literalnie, gdy mowa o działaniu jednostek policji czy wojska, jak i metaforycznie, w przypadku aktywistów NGO, którzy mogą np. blokować skrzyżowania czy wysyłać serie maili czy faksów. Swarming działa najlepiej, gdy jest utworzony z rozlokowanych niezliczonych, małych, rozproszonych, sieciowo manewrujących jednostek. Swarming pojawia się, gdy rozproszone jednostki sieci małych sił zbiegają się nad celem z różnych kierunków. Głównym celem jest ciągłe pulsowanie. Mrowiące sieci muszą być w stanie połączyć się nagle i ukradkiem nad celem, następnie rozdzielić się, ponownie się rozpraszać, by nagle być gotowym do ponownego pulsowania[25].

Sam mechanizm ataku swarmingowego jest prosty. Informacje o celach (zawierające ich nazwę, lokalizacje oraz sposób, w jaki powinno się je nękać) są podawane na najważniejszych portalach odgrywających rolę „ideologicznego źródła" danego ruchu. Te informacje są następnie powielane na innych, „bratnich" portalach, silniej lub słabiej powiązanych ze „źródłem". Po rozpowszechnieniu informacji o „celach i metodach" rozpoczyna się właściwy proces nękania (pulsowania), trwający wiele dni, tygodni, a nawet miesięcy, aż do osiągnięcia pożądanego rezultatu. Bez wątpienia swarming w wykonaniu współczesnych ugrupowań znacznie różni się od swarmingu tradycyjnego, opisywanego przez teoretyków wojskowości. Różnic jest co najmniej kilka, choć najważniejsze niewątpliwie dotyczą: właściwości atakowanego celu, charakteru powiązań jednostek uczestniczących w swarmingu oraz sposobu koordynowania przez nie działań. I tak na przykład w klasycznej postaci swarmingu cel ataku był zwykle militarny – miał świadomość zagrożenia, uczestniczył w walce, i co najważniejsze – mógł bezpośrednio zareagować na atak. Atak nowych swarmingowych jednostek jest skierowany na cele cywilne – z tego też względu atakowany nie tylko nie jest w stanie przeprowadzić „na własną rękę" kontrataku, lecz także zapewnić sobie we własnym zakresie obrony. Z uwagi na praktycznie nieograniczoną liczbę możliwych celów ataki swarmingowe nowego typu są w nieporównanie wyższym stopniu bezpieczniejsze dla strony atakującej niż te znane z przeszłości, w których obydwie strony miały charakter wybitnie militarny i były nastawione na wzajemne zniszczenie. Poziom bezpieczeństwa jeszcze wzrasta, gdy ataki odbywają się za pośrednictwem sieci internetowej i przy użyciu botnetu[26].

[25] J. Arquilla, D. Ronfeld, *Networks and Netwar* [online], http://radio-weblogs.com/0107127/stories/2002/09/10/networksAndNetwar.html [dostęp: 19 II 2011].

[26] Botnet to grupa komputerów zombie zainfekowanych złośliwym oprogramowaniem (botem), które są zdalnie kierowane – oczywiście bez wiedzy ich użytkowników.

Ponadto w klasycznym swarmingu grupy przeprowadzające atak były powiązane zarówno formalnie, jak i taktycznie. Stosunkowo nieliczne, zorganizowane wokół zastanej struktury rozkazów, wykonywały z góry narzucone zadania i na bieżąco koordynowały pomiędzy sobą przebieg akcji, a także, mimo dość znacznej autonomii, porozumiewały się (przynajmniej okresowo) z „centrum". Współczesne jednostki swarmingowe, zorganizowane według modelu oporu bez przywództwa, rezygnują zarówno z nadrzędnej struktury rozkazów, jak i z wymogu koordynacji. Dzięki takiej rezygnacji zyskują nieosiągalną w zasadzie dla uczestników klasycznego swarmingu właściwość, a mianowicie masowość. Ta cecha sprawia, że dla przeciwnika jednostki swarmingowe są, przynajmniej przed rozpoczęciem akcji, niewidoczne (taką jednostką może być każdy człowiek). Ich mobilizacja zależy jedynie od siły ideologicznego impulsu, którego źródłem jest sieć internetowa, niezwykle trudna do skontrolowania. Walka może sie toczyć właściwie nieustannie i nic poza konkurencyjnym ideologicznym impulsem nie będzie w stanie jej zatrzymać.

Zakończenie

Wiele wskazuje na to, że jeśli słabi w umiejętny sposób zastosują opór bez przywództwa, to silni znajdą się w niemałych tarapatach. Jeśli dodatkowo słabi na większą skalę wzbogacą go o taktykę swarmingu, to możliwość obrony przed takimi atakami stanie się więcej niż wątpliwa. Trzeba przyznać, że na razie po taktykę swarmingu (zarówno w rzeczywistości fizycznej, jak i wirtualnej) sięgają głównie ugrupowania zaliczane do terroryzmu wewnętrznego (przede wszystkim anarchiści, obrońcy zwierząt oraz prośrodowiskowcy), jednak powoli zaczynają się nią interesować także i inne ugrupowania (np. radykalne ugrupowania islamskie). Jeśli będzie to postępowało, to walka z sieciowymi organizacjami działającymi na podstawie modelu oporu bez przywództwa może być przegrana. Zwłaszcza jeśli będzie ona oparta jedynie na hierarchii i odgórnym zarządzaniu. W takim przypadku bowiem nikt nie będzie w stanie ogarnąć całego spektrum zdarzeń konstytuujących współczesne pole walki ani też wystarczająco elastycznie na nie reagować. Ten problem zauważyli w latach 90. XX w. J. Arquilla i D. Ronfeld, którzy pisali, że (…) *strukturom hierarchicznym będzie bardzo trudno walczyć z sieciami*[27]. W podobnym tonie wypowiada się Toby Blyth, twierdząc, że (…) *użycie hierarchicznej siły przeciwko quasi-terrorystycznym sieciom może nie być szczególnie efektywne*[28]. Czy jednak rządzący, którzy chcą sprostać wyzwaniom współczesnego pola walki, będą w stanie przejąć organizacyjny model i strategię swoich przeciwników? Może to być bardzo trudne. Ale przecież „zaadaptowanie struktur przeciwnika" nie musi się odbywać przez transformację hierarchii w sieci. Skuteczna może okazać się struktura hybrydowa, np. połączenie sieci i hierarchii. W praktyce oznaczałoby to umiejętne inicjowanie i motywowanie inicjatyw oddolnych, a w razie potrzeby – ich kontrolę i „pacyfikację". Ważną zaletą tej struktury jest niewątpliwie to, że można ją zaadaptować także do walki z innymi strukturami hierarchicznymi, tj. z innymi państwami. W tym kierunku zdaje się zmierzać koncepcja szefa Sztabu Generalnego Federacji Rosyjskiej generała armii Walerija Gierasimowa, który 25 stycznia 2013 r. na konferencji w Akademii Nauk Wojskowych w Moskwie stwierdził, że klasyczny sposób prowadzenia wojny, oparty na pokonywaniu

[27] J. Arquilla, D. Ronfeld, *The Advent of Netwar: Analytic Background*, „Studies in Conflict & Terrorism" 1999, nr 22, s. 199–200.

[28] T. Blyth, *Terrorism as Technology: a Discussion ...,* s. 45.

sił zbrojnych przeciwnika i zajęciu jego terytorium, już się przeżył i winien zostać zastąpiony strategią pośrednią, której istotą jest użycie środków niemilitarnych (działań ekonomicznych, informatycznych, politycznych). Szczególnie duże znaczenie generał przypisał działaniom asymetrycznym, do których zaliczył wykorzystanie „potencjału protestu" w kraju potencjalnego przeciwnika[29]. Wykorzystanie „potencjału protestu" odbywa się przez zaktywizowanie warstw niezadowolonych za pośrednictwem środków informacyjno-psychologicznych, zbudowanie z nich oddolnego ruchu i posłużenie się nim do realizacji określonych celów. Wzmocnieniem dla tych działań miałaby być walka informacyjna, w której za pomocą środków propagandowych podważałoby się wartości i idee przeciwnika. Takie działania miały już oczywiście miejsce w historii, nigdy jednak nie postrzegano ich jako priorytetowych. Czy są to kroki w kierunku wojen czwartej generacji? Tego nie wiemy. Jednak niebezpiecznie się one wpisują w schemat nakreślony przez ich teoretyków.

Bibliografia:

1. Arnold R., *Eco-Terror. The Violent Agenda to Save Nature. The World of the Unabomber*, Bellevue–Washington 1997, Free Enterprise Press.
2. Arquilla J., Ronfeld D., *Networks and Netwar* [online], http://radio-weblogs.com/0107127/stories/2002/09/10/networksAndNetwar.html [dostęp: 19 III 2011].
3. Arquilla J., Ronfeld D., *The Advent of Netwar: Analytic Background*, „Studies in Conflict & Terrorism" 1999, nr 22.
4. Arquilla J., Ronfeldt D., *The Advent of Netwar*, Santa Monica 1996, RAND.
5. Arrequin-Toft I., *How the Week Win Wars. A Theory of Asymmetric Conflict,* „International Security" 2001, nr 1.
6. Barney D., *Społeczeństwo sieci*, Warszawa 2008, Wydawnictwo Sic!
7. Beam L.R., *Leaderless Resistance* [online], „The Seditionist" 1992, nr 12, http://www.louisbeam.com/leaderless.htm. [dostęp: 20 III 2016].
8. Blyth T., *Terrorism as Technology: a Discussion of the Theoretical Underpinnings*, w: *Technology and Terrorism*, D. Clarke (red.), New Brunswick–London 2004, Transaction Publishers.
9. Brzeski R., *Wojna czwartej generacji* [online], http://niepoprawni.pl/blog/6063/wojna-czwartej-generacji [dostęp: 20 III 2016].
10. Castells M., *End of Millenium*, Oxford 1998, Blackwell.
11. Castells M., *Siła tożsamości*, Warszawa 2008, PWN.
12. Cox R., *Production, Power and World Order: Social Forces in the Making of History*, New York 1987, Columbia University Press.
13. Creveld M. von, *Transformation of War*, New York 1991, The Free Press.
14. *Ecotage!*, S. Love, D. Obst (red.), New York 1972, Pocket Books.
15. Hammes T.X., *The Sling and the Stone: On War in the 21st Century*, St. Paul, MN, 2004, Zenith Press.
16. Kuźniar R., *Globalizacja, polityka i porządek międzynarodowy*, w: *Globalizacja a stosunki międzynarodowe,* E. Haliżak, R. Kuźniar, J. Symonides (red.), Bydgoszcz–Warszawa 2003, BRANTA.
17. Mack A.J.R., *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*, „World Politics" 1975, nr 2.

[29] Zob. M. Wojnowski, *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 13–39.

18. Michael G., *Lone Wolf Terror and the Rise of Leaderless Resistance,* Nashville 2012, Vanderbilt University Press.
19. Nye J.S., Keohane R., *Globalization. What's new? What's not? (and so what?)*, w: *Power in the Global Information Age. From Realism to Globalization*, J.S. Nye (red.), London–New York 2004, Routledge.
20. Posłuszna E., *Ekstremizm ekologiczny – źródła, przejawy, perspektywy*, Warszawa 2012, Scholar.
21. Posłuszny J., *http://www.nowyterroryzm.org*, w: *U progu wielkiej zmiany? Media w kulturze XXI wieku. Nurty, kategorie, idee*, M. Sokołowski (red.), Olsztyn 2005, Kastalia.
22. Wojnowski M., *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 13–39.

Abstrakt

Punktem wyjścia do rozważań zaprezentowanych w niniejszym artykule jest pytanie, dlaczego coraz częściej w różnych typach konfliktów (lokalnych czy państwowych) przewagę zyskują słabi aktorzy. Autorka artykułu wskazuje najważniejsze czynniki, które przyczyniają się do takiego stanu rzeczy. Jej zdaniem próba odpowiedzi na pytanie postawione na początku artykułu musi z konieczności zawierać analizę przekształceń wpisujących się w paradygmat wojen czwartej generacji, do których doszło w obrębie struktur organizacyjnych ugrupowań ekstremistycznych i terrorystycznych pod wpływem rozwoju procesów globalizacyjnych i nowych technik komunikacyjnych. Istotą tych przekształceń jest decentralizacja, a jedną z jej konsekwencji jest współczesna taktyka swarmingu. Ta analiza stanowi treść niniejszego artykułu.

Słowa kluczowe: wojna czwartej generacji, walka sieciowa, opór bez przywództwa, rojenie, konflikt asymetryczny.

Abstract

The question why in various types of conflicts (local and national) the advantage is gained by the weak actors is the basis for the deliberations presented in this article. The author shows the most important factors responsible for the occurrence of such state of affairs. In her opinion, the attempt to answer that question must necessarily contain the analysis of the characteristic for the fourth-generation warfare paradigm transformations that took place in organizational structures of the extremist and terrorist groups due to the development of globalisation processes and new communication technologies. Decentralisation is the essence of these transformations, and one of its consequences is the modern tactic of swarming. These analyses are the subject of this article.

Keywords: fourth-generation warfare, netwar, leaderless resistance, swarming, asymmetric conflict.

Anatolij I. Maruschak

Modern information policy of Ukraine and civil rights

Modern information policy in the developed countries is a complex of directions and means of the competent state bodies control, regulation and planning in the sphere of obtaining, storage, processing, usage and circulation of the information. Thus, the European Union (EU) is nowadays actively working on the single EU information policy making.

However, the state information policy of Ukraine at the present stage should actualize the question of Ukrainian national traditions and respect for the nation. The consciousness of the population of state built on the ethnic grounds implies the awareness of national unity within the specified territory (not the class or the whole world), identification of its members with the specific language, culture, traditions. Prevalence of the TV programs of foreign production or of foreign sample provided conditions for the spread of values and lifestyle unusual for the Ukrainian culture as well as cult of violence and cruelty, disrespect for human and national dignity, unwillingness for self-identification.

Article 5 of *the Law of Ukraine "On Information"* (as in force in 1992) states that the state information policy is a complex of major directions and means of the state activity in the sphere of obtaining, usage, processing and storage of the information[1].

State policy directions should be based on the national interests of Ukraine and consider the existing threats in the information sphere, though nowadays all the conceptual documents concerning information security policy are still in the process of development. Thus, according to the decision of the National Security and Defense Council (NSDC) of Ukraine from April 28, 2014 *On measures on the improvement of the formation and realization of state information security policy* put in force by the presidential decree № 449/2014 from May 1, 2014 *the Information Security Doctrine of Ukraine № 514/2009* from July 8, 2009 was canceled and a number of legal acts were supposed to be elaborated. Among them: *the Strategy for the Development of the Information Space of Ukraine*, *Strategy for the Cyber Security of Ukraine*, *draft Law of Ukraine "On The Cyber Security of Ukraine"*. However, so far only *the Strategy for the Cyber Security of Ukraine* has been adopted.

In Ukraine various aspects of the state information policy formation are in the competence of a number of state bodies and authorities among them – National Council of Television and Radio Broadcasting of Ukraine, Ministry of Foreign Affairs of Ukraine, Ministry of Culture of Ukraine, Ministry of Justice of Ukraine, State Security Service of Ukraine, Foreign Intelligence Service of Ukraine, Ministry of Internal Affairs of Ukraine and so on, whose activities are often duplicated and are not coordinated. The above mentioned problem has not been solved even after the creation of the Ministry of Information Policy of Ukraine. The analysis of its tasks shows that the functions it performs narrow the notion of "state information policy of Ukraine" and do not cover all the directions of the information policy, defined in the national legislation.

[1] *The Law of Ukraine "On Information"*, "Vidomosti Verkhovnoi Rady Ukrainy" 1992, № 48, p. 351.

At the NSDC also operates the Interdepartmental Commission on Information Policy and Information Security. Its primary tasks, in particular, include the analysis of the state and potential threats to the national security of Ukraine in the information sphere and assimilation of the best world practice in the sphere of information policy formation and realization[2]. It could be quite useful under the condition of information aggression against Ukraine to enlarge the powers of the above mentioned state authority and to include coordination of the operation activity of other state bodies, civil society institutions.

At the present time in the legal science as well as in the legislation of Ukraine two approaches to the interpretation of the right to information were formed. Within the narrow approach the right to information is defined only as the right to receive (access to) information, that is a relative right. Broadside approach assigns all kinds of legal rights focused on the information or performing some actions with it[3].

Thus what is meant here is the public right to information. In author's foregoing scientific researches it was grounded that the right to information means state-guaranteed capability of citizens to satisfy their need for obtaining, usage, circulation, protection and security of the volume of information that is necessary for daily living[4].

The right to information which includes the right to freely collect, store, use and disseminate the information orally, in a written form or in any other way of your choice, is defined as the basis of the public right to information. The key part of the right to information is a public right to access to (obtain) information, and freedom of convictions and opinion, freedom of information exchange[5] are included into the notion of right to information.

Revolution of dignity has brought the opportunity for Ukraine to build a new system of relations between citizens, society and state on the basis of freedom and democracy. However, due to the Russian occupation of the Ukrainian territories – Autonomous Republic of Crimea – and military aggression in the East of Ukraine, the country was faced with additional tasks, in particular those connected with the issues of maintaining information security: countermeasures to information operations against Ukraine, public mind control and circulation of corrupted information, creation and development of the institutes responsible for the information and psychological security[6].

Under the specified conditions the legal regulation of the public right to information is closely connected with the consolidation of public right to information security, specifically in terms of protection of citizens from incomplete, untimely and unreliable information and from negative information impact. That is why the question of state "reaction" to the circulation of unreliable information for maintaining public and state information security is of primary importance. Thus, the Constitution of Ukraine states that maintaining information security is one of the key functions of state, concern of every Ukrainian citizen[7], and information security is classically defined as

[2] *The Statute on the Interdepartmental Commission On Information Policy and Information Security* at the National Security and Defense Council of Ukraine was adopted by the presidential decree on January 22, 2002, №63/2002 [electronic recourse], http://zakon.rada.gov.ua/laws/show/63/2002.

[3] A.I. Maruschak, *Information law: access to information: Study guide*, K.: KHT 2007, 532 p.

[4] A.I. Maruschak, *Definition of the notion "public right to information"*, "Informaciya i pravo" 2011, № 2, p. 21–26.

[5] Article 2 of *the Law of Ukraine* "*On making amendments to the Law of Ukraine "On Information"* from January 13, 2011, "Oficiyniy visnyk Ukrainy" 2011, № 10.

[6] Decree of the President of Ukraine from May 26, 2015 № 287/2015 "On the decision of National Security Council and Defense of Ukraine, from May 6, 2015 "About National Security Strategy of Ukraine", Oficiyniy Visnyk Ukrainy 2015, № 43, P. 1353, p. 4.11.

[7] *The Constitution of Ukraine* from June 28, 1996, "Vidomosti Verkhovnoi Rady Ukrainy" 1996, № 30,

(...) *state of security for vital interests of a human, society and state which ensures prevention of possible harm caused through incomplete, untimely and unreliable circulation of information, violation of integrity and availability of information* [8].

In this direction, the state changes legal regulation of public relations in the sphere of direct execution of defense functions by the Ukrainian citizens. For example, (...) *storage and usage procedures for personal photo cameras, tape recorders, radio receivers, cellular phones and other means of mobile communications and data transfer, computer and other domestic radioelectronic equipment for the military personnel on duty is regulated by the unit commanding officer* [9]. While formally abridging the information right of the military personnel, this provision of law is aimed at maintaining their security during the military operations to preserve the territorial integrity of Ukraine.

Of practical importance becomes also the question of professional activity of the journalists from TV and radio companies, printed and internet media in Ukraine. They are formally not engaged in the realization of the state information policy.

Nevertheless, numerous facts of discrediting the state authorities of Ukraine, violation of classified or "sensitive" information, (according to NATO categories), public information concerning location, composition, plans and equipment of the Ukrainian Armed Forces and so on actualize the problem of regulation of mass media activity during the special period and under martial law.

Nowadays there is in fact the special period for Ukraine that consists in (...) *functioning of national economy, state authorities, other state bodies, local government bodies, Military Forces of Ukraine, other military units, civil defense forces, enterprises, institutions and organizations and performing the constitutional duty to defend homeland, independence and territorial integrity of Ukraine by its citizens* that started when the decision on mobilization was announced[10].

The working legislation of Ukraine about the special period and martial law allows state authorities to influence the mass media. Thus, in Ukraine mobilization preparation consists in (...) *preparation of the editorial staff of printed media and TV and radio companies to the special period and martial law operation mode*[11].

Military command together with military administrations (in case of their creation) can: (...) *regulate the work of* (...) *publishing companies, TV and radio companies, TV and radio centers* (...) *mass media*[12].

It is necessary to lay foundations for the public discussions of making amendments to the legislation in the sphere of printed mass media (press) in Ukraine and TV and radio broadcasting concerning the introduction of provisions on the review of reports and materials that appear in mass media and are "sensitive" for the national security during the special period and martial law.

P. 141, p. 17.

[8] Paragraph 13 chapter III of *the Main foundations of the development of information society in Ukraine for 2007–2015*, enacted by the Law of Ukraine from January 9, 2007, "Vidomosti Verkhovnoi Rady Ukrainy" 2007, № 12, P. 102.

[9] *The Law of Ukraine "On making amendments to Article 143 of the Statute of the Internal Service of the Ukrainian Armed Forces"* from July 1, 2015, "Vidomosti Verkhovnoi Rady Ukrainy" 2015, № 33, P. 326.

[10] *The Law of Ukraine "On mobilization preparation and mobilization"* from October 21, 1993, "Vidomosti Verkhovnoi Rady Ukrainy" 1993, № 44, P. 416.

[11] Paragraph 3, Article 3 of *The Law of Ukraine "On mobilization preparation and mobilization"* from October 21, 1993, "Vidomosti Verkhovnoi Rady Ukrainy" 1993, № 44, P. 416.

[12] Article 8 of *the Law of Ukraine "On the Legal Regime of Martial Law"*, "Vidomosti Verkhovnoi Rady Ukrainy" 2015, № 28, P. 250.

It is obvious that we are not talking about the creation of state censor body similar to totalitarian Golovlit (Main Administration for Safeguarding State Secrets in the Press). The best solution would be to join efforts of state, society and mass media to establish the working mechanism of the countermeasures against the information aggression, in particular: information operations against Ukraine, manipulation of public consciousness and circulation of unreliable information, development of the institutions responsible for information and psychological security of citizens.

The EU countries already have such experience of the information policy development by means of introducing strategic communications. Besides there is also the experience of teaching journalists the principles of state information policy and the indicators of negative information impacts against the state. Ukraine is acquiring its own experience in this sphere, taking into account the best practices of the foreign countries. That is why we consider the proceeding of the discussion on the realization of state information policy at the period of military operation on its territory to be useful for Ukraine and for other countries as well.

Vitalij Hrebenuk

European security – new threats and demands

The latest events in Ukraine show that European project became the object for hybrid warfare – coordinated, flexible and dynamic influence in artificially created instability on the key elements of "victims`" national security systems on their territories, beyond them and on the international level. It is realized by the network of various groups, operated from a single strategic centre. This influence is possible owing to European countries` contradictions, because of strenthening of antieuropean positions.

Unfortunately Europeans in this context underestimate state, tendencies and foreseen consequences of Russian-European confrontation. As a result of absence of unity within EU, hesitation between American and Russian development vectors, sometimes absolutely national (not European) direction, chaotic forming of EU geostrategic line, there appears the possibility of arising of complicated mixture of threats for European security in general.

After 1991 the concept of EU foreign policy in the postsoviet spaces was based on the idea of cooperation with Russian Federation, which seemed to control these areas, to follow the way of democratic reforms and to lead other former Soviet republics on this way. EU and RF didn't exclude mutual integration. Decisive step act in realization of these aspirations became the *Treaty on European Union 1992*[1]. Russia formulated its own symmetric document – *Russia strategy on EU till 2010 p.*, aimed at building united Europe without dividing lines, interconnected and balanced strengthening of Russia and EU in international community[2].

Simultaneously Russia hoped to exclude or at least postpone European eastward expansion, first of all on the Baltic territory, limiting Russian geopolitical impact in Eastern Europe. Bilateral agreements on partnership and cooperation between European Union and former Soviet republics were considered alarming.

Almost all these documents anticipated EU eastern neighbour's adaptation to the system of European values and priorities. Officially, such a relationship with Ukraine was framed in 1994 by signing *The Agreement on Partnership and Cooperation between the European Community and Ukraine*.

A qualitatively new stage of europolicy on the former Soviet spaces began with the speech of the European Commission President R. Prodi in 2002[3] and New Neighbours Initiative, oriented on Moldova, Belarus and Ukraine[4]. Ukraine received special neighbour status and in 2004 – immediate border with the new EU members – Poland

[1] S.U. Kashkin, *The law of the European Union*, The State Law Moscow Academy, M.: Prospect 2011, p. 30.

[2] *Russian Federation and European Union relations Strategy in the medium term (2000–2010)*, MSIIR University, http://www.mgimo.ru/files2/y11_2013/243404/4.4.strategy_russia_relations_eu.htm.

[3] R.A. Prodi, *Wider Europe – a Proximity Policy as the key to stability: Speech at the Sixth ECSA World Conference. Brussels 5–6 December 2002*, http://www.europa.eu/ jnt/comm/commissioneres/prodi/speeches/index_en.htm.

[4] Follow-up to the European Council in Brussels (24–25 October 2002), Brussels, November 18, 2002, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/gena/73248.pdf, p. 13.

and the Baltic countries. New members started to form special geopolitic space, proclaimed their mission of assisting eastern neighbours in reforming, democratization and distancing from Russia[5].

The climax of this was the failure of "Wide Europe" concept, Russia adaptation to EU standards according to the results of Petersburg Summit 2003 and European Parliament resolution on relations between the EU and Russia[6]. Russian-European relations entered the rivalry stage, able to cause confrontation.

In 2007–2008 formal negotiations on the new quality of relations between Ukraine and the European Commission, signing *Association Agreement and Deep and Comprehensive Free Trade Area* (DCFTA), started[7]. At the initiative of the Minister of Foreign Affairs R. Sikorsky the program *Eastern Partnership* (EP) was launched (main partners – Poland and Lithuania). It was aimed at convergence, political association and economic integration with Armenia, Azerbaijan, Georgia, Moldova, Belarus and Ukraine.

EP officially assumes such inter-regional dialogue platforms, democracy, good governance and stability, economic integration and convergence with EU policies, energy security, contacts between people[8].

However, firstly, despite the fact that about half of all project assets was designed to its main participant – Ukraine, the EU relations with Ukraine remain functional part of its relations with Russia. The exception is Poland, where development of relations with Ukraine is considered the part of their europolicy. Its initiative in 2011 resulted in the EuroNest and the Polish-Ukrainian forum. It meant actual EP output beyond the program according to the Polish scenario.

Secondly, against the background of the present geopolitical reality these platforms seemed to be minor. Their range unjustifiably excludes cooperation in the military sphere and challenges to European security.

In our opinion, it identifies the main problem of EP for today and points to the need of forming new platforms of inter-regional dialogue.

Many European researchers realize that Ukraine is forced to restore its cultural space as well as the European civilizational space by the cost of human lives.

Simultaneously our country faced the challenges to European security, the danger of which Europeans do not fully understand. In its turn, Russian political establishment considers EP as well as NATO to be a threat to Russia's interests, an attempt of post-soviet disintegration.

In the view of the acute security challenges in the European geopolitical interests' sphere, developed by Russia by exploiting current crisis, disintegration, discrediting European integration, military and intelligence-subversive activities, for the purpose of the effective counteraction it would be logical to create an additional EP platform – "European Security".

It should be based on the issue of strengthening solidarity of EU Member States and participants of the Eastern Partnership in the sphere of geopolitical threats counter-

[5] *European Neighbourhood Policy Strategy Paper*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0373&f rom=EN.

[6] Communication from the Commission to the Council and the European Parliament on relations with Russia: EU Commission document COM(2004) 106, Brussels, February 9, 2004, p. 3.

[7] *EU–Ukraine Deep and Comprehensive Free Trade Area*, http://trade.ec.europa.eu/doclib/docs/2013/april/tradoc_150981.pdf, 9 p.

[8] *Eastern Partnership*, http://www.kmu.gov.ua/kmu/control/uk/publish/article?art_id=248068721&cat_id=223345569.

action, national defense and security systems development, as well as integration into the European space, harmonizing policies in the field of national and common security. This platform`s flagship initiatives could be formulated as "Comprehensive Analysis of Potential Threats", "The Development and Implementation of Preventive Measures".

As a whole, Ukraine is moving closer to the EU and away from Russia economically and politically against the background of a deep economic and political crisis. Hybrid warfare sharpened the crisis, social tensions, intensified the need for foreign financial support in order to save the economic and the political system from collapse.

Russian-Euroatlantic geopolitical rivalry resulted in Maidan bloody confrontation, anti-terrorist operation in eastern Ukraine, implementing scenarios of controlled chaos. It was the price for signing "economic section" of the *Agreement about Association* in 2014. But even after the tragic events on Ukrainian way to Europe it didn't mean European unanimity and unity.

Europe has not served as a subject of international relations yet. In fact, the prevailing trend is replacing "defense" with "politics" and general philosophy of EU interest[9]. Ch. Patten, Commissioner for External Relations of the EU, aptly noted: (...) *EU occasionally publishes conscript declarations, usually a few weeks after important international events,* (…) *acting as a commentator, not a functioning entity*[10]. All this gives rise to ideological differences of the EU members' elites in understanding security problems, their ambiguous perceptions of European issues. The reason for this is not only a variety of geopolitical thoughts, but legal specific features of Europe construction.

Under Article 17 of *the Treaty of Nice*, the common security policy has no right to bring damage to foreign policy of individual countries and their commitment concerning participation in NATO and other organizations. The commonly adopted policy cannot affect the exclusive interests of the foreign policies of individual states[11]. According to the American experts, EU foreign policy resembles normal interstate coordination[12].

In fact, the EU has no unifying foreign policy and geostrategy. Each country creates its geospace, guided by the principles of national egoism. Under such conditions of the EU geopolitical unity, the reforms of the existing organizational structure of the European security sphere are needed.

[9] J. Dobbins, *Friends again?* in: *Friends again? EU-US relations after the crisis*, M. Zaborowski (ed.), Paris 2006, p. 26–27.

[10] Ch. Patten, *The European Union and the World*, in: *Europe in the New Century. Visions of an Emerging Superpower*, R. Guttman (ed.), London 2001, p. 79.

[11] *Treaty of Nice*. Amending the *Treaty on the European Union, the Treaties Establishing the European Communities and Certain Related Acts* (2001/C 80/01), "Official Journal of the European Communities", March 10, 2001.

[12] B. White, *Understanding European Foreign Policy*, Hampshire–N.Y. 2001, p. 100.

II
RECENZJE

Mirosław Sikora

Andrew Hussey, *The French Intifada. The Long War between France and its Arabs*[1]

Autor i paradygmat

Książek poświęconych współczesnemu terroryzmowi dziś nie brakuje. Na ogół jednak czytelnicy są zapoznawani z analizą rezultatów działalności terrorystycznej, tj. z kulisami aktów terrorystycznych oraz ich konsekwencjami, a także z metodami działania zamachowców. Rzadziej dostają do wglądu pogłębioną analizę obejmującą dłuższy okres (np. kilkudziesięcioletni) i rozległy obszar geograficzny (np. cały region Bliskiego Wschodu), pomagającą tym samym zrozumieć postawy zamachowców przez odwołanie się do procesów determinujących egzystencję nie jednego, ale wielu pokoleń. Aby wniknąć w złożone uwarunkowania i motywy pchające ludzi w szeregi organizacji ekstremistycznych, dobrze jest zgłębić wiedzę z zakresu różnych nauk humanistycznych (społecznych). W tym miejscu można by było odwołać się do postulatów metodologicznych francuskiej szkoły historycznej Annales, które stanowią jej credo, zwłaszcza do ukazywania zagadnień w perspektywie długofalowej. Nie chodzi zatem o krótki okres, ale o tzw. długie trwanie i ewolucję obserwowanych zjawisk na przestrzeni dziesiątków, a nawet setek lat.

The French Intifada… wychodzi naprzeciw tym, którzy są zainteresowani nie tyle szczegółami funkcjonowania zakonspirowanych komórek i sieci terrorystycznych czy detalami związanymi z ich tropieniem i neutralizacją, ile raczej genezą problemów o podłożu etniczno-religijno-ekonomicznym (a w rzeczywistości – polityczno-społecznym), z jakimi boryka się współczesna Europa, szczególnie jej postimperialna zachodnia flanka.

Andrew Hussey (ur. w 1963 r.) to brytyjski kulturoznawca specjalizujący się w historii kultury nowożytnej Francji. Jest absolwentem University of Manchester oraz Université Lyon III im. Jeana Moulina. Szczególną uwagę w swoich badaniach i publikacjach poświęca francuskiemu kolonializmowi w Afryce Północnej oraz epoce postkolonialnej w tym regionie. Od lat 90. ubiegłego stulecia wykłada na brytyjskich uniwersytetach, a w 2014 r. został dyrektorem Centre for Post-Colonial Studies University of London's School of Advanced Study. W trakcie swojej kariery zajmował się również działalnością dziennikarską – współpracował z BBC.

Autor wprawdzie nie jest ekspertem w sprawach dotyczących terroryzmu czy ogólnie „świata islamu", ale książce to nie szkodzi, gdyż ma ona charakter raczej popularno-naukowy. Dostrzegalne są literackie skłonności Husseya, który często odsyła do Alberta Camusa i innych twórców – myślicieli XX w. związanych z jednej strony z krajami Maghrebu, a z drugiej – z Francją (Michel Houellebecq, Jean Paul Sartre), a także do przedstawicieli lokalnej (Maghreb) bohemy.

Hussey porusza się w obrębie paradygmatu, zgodnie z którym obecne zmagania rządów (zwłaszcza państw europejskich i bliskowschodnich) z aktami terrorystycznymi to poniekąd czwarta wojna światowa (przy założeniu, że trzecią była tzw. zimna wojna).

[1] London 2015, Granta Books, 437 s.

Autor prezentuje perspektywę historyczną – sięga do czasów kolonialnych. Z powodzeniem stara się – i to jest chyba największy atut książki – osadzić czytelników w realiach, w których aktualnie znaleźli się mieszkańcy Afryki Północnej. W tym celu prezentuje znacznie bardziej zróżnicowane informacje na temat Huntingtonowskiego konfliktu Północy z Południem niż te przedstawiane w zbanalizowanych przekazach medialnych. Prawdopodobnie jego zamierzeniem nie było tłumaczenie współczesnych procesów politycznych zachodzących na południowym wybrzeżu Morza Śródziemnego (mających swe korzenie w tzw. arabskiej wiośnie) przeszłością kolonialną tego regionu. Chodziło raczej o posłużenie się narracją historyczną, w której „arabska wiosna" stanowi kolejne stadium zmagania się społeczeństw Maghrebu już nie tyle z kolonialnym, ile z postkolonialnym dziedzictwem Algierii, Maroka i Tunezji.

W podsumowaniu (s. 403) autor ujawnia intencje, które mu przyświecały podczas badań: *What I have aimed to present here is an accessible analysis of current tensions on both sides of Mediterranean, informed by an account of the historical circumstances which have brought us to where we are*.

Struktura

Husseya interesują trzy kraje: Algieria, Maroko i Tunezja. Każdemu z nich poświęca jeden rozdział. W sumie rozdziałów jest pięć, z czego ostatni (pt. *Więźniowie wojny*) stanowi zakończenie. W rozdziale pierwszym Hussey zapoznaje czytelników z problemami współczesnej Francji, wynikającymi z koegzystencji w jej granicach mniejszości etnicznych i religijnych. Kolejne dwa rozdziały stanowią próbę znalezienia odpowiedzi na pytanie o przyczynę buntowania się francuskich przedmieść (franc. *banlieue*) w minionych latach.

Retrospekcja przeprowadzona przy tej okazji obejmuje nie tylko klasyczne, tj. polityczne, ujęcie problemu, lecz także historię kultury i obyczajów społeczeństw zamieszkujących południowe wybrzeże Morza Śródziemnego w czasach francuskiej ekspansji zamorskiej w XIX i początkach XX w. oraz zmniejszanie się wpływów IV i V Republiki. Autor stara się usystematyzować relacje trzech wyżej wymienionych krajów z Centrum. Umieszcza je na osi, począwszy od najbardziej skonfliktowanej Algierii, przez bardziej ugodową Tunezję, po najbardziej zwesternizowane Maroko, którego stosunkowo późną kolonizację określa mianem „pokojowej penetracji".

Akcja opisywanych wydarzeń rozgrywa się to w Paryżu, Tuluzie i Marsylii, to w Marrakeszu, Tangerze, Algierze, Tunisie i innych miastach regionu, gdzie przez ostatnie półtora wieku wpływy francuskie ścierały się z berberyjskimi i muzułmańskimi kontrakcjami.

Algieria w centrum uwagi

W najbardziej rozbudowanym rozdziale poświęconym Algierii Hussey śledzi proces zdobywania praw obywatelskich przez mieszkańców tego najbardziej znanego francuskiego dominium. Ukazuje tarcia wewnątrz społeczności muzułmańskiej, towarzyszące temu procesowi zwłaszcza w okresie międzywojennym. Elity tej społeczności były faworyzowane przez Paryż, zainteresowany antagonizowaniem algierskiego społeczeństwa w myśl maksymy *divide et impera*.

W książce nie mogło zabraknąć komentarza do końcowego stadium algierskich dążeń niepodległościowych, realizowanych pod znakiem Frontu Wyzwolenia Narodowego

(Front de Libération Nationale – FLN) w latach 50. i 60. XX w., a także odniesienia do ikon francuskiego ruchu oporu z tamtych czasów, tj. do organizacji OAS i generała Raoula Salana.

Interesującym elementem algierskiej epopei stanowiącym moralne wyzwanie dla współczesnej Francji jest także smutna historia tzw. harkis, czyli muzułmańskich najemników rekrutowanych przez francuski rząd, którzy do 1962 r. wspierali siły interwencyjne Francji. Gdy Algieria uzyskała niepodległość, zostali oni pozostawieni przez Paryż na pastwę nacjonalistów, represjonujących ich jako zdrajców i kolaborantów.

Innym ważnym etapem zmian w relacjach dawnych kolonii z dawnym Centrum była arabizacja algierskiego społeczeństwa, zainicjowana w latach 60. XX w. Hussey ukazuje ten proces na różnych przykładach, szczególnie jednak na przykładzie tego typu zmian zachodzących w sferze kultury i sztuki oraz wobec instytucji rodziny i szeroko pojętego stylu życia (wzorców). Zwraca przy tym uwagę na lansowane, zwłaszcza w radykalnych kręgach muzułmańskich, kontestowanie postępującej westernizacji świata arabskiego. Czytelnik jest tu konfrontowany z pojęciem wahabizmu i ruchem Bractwa Muzułmańskiego, które szerszym kręgom polskiego społeczeństwa są znane właściwie dopiero od „arabskiej wiosny" 2011 r. (i to raczej w kontekście Egiptu). Autor analizuje też programy innych radykalnych organizacji wyznaniowych działających w Algierii, w tym osławionego Islamskiego Frontu Ocalenia (fr. Front Islamique du Salut), współodpowiedzialnego za wojnę domową w latach 90. ubiegłego wieku.

Niezależnie od kwestii dotyczących odleglejszej, nawet XIX-wiecznej, historii regionu w książce nie brakuje odniesień do wydarzeń współczesnych, np. do tajemniczej śmierci imama Abdelbaki Sahraouiego, zamachów na paryską stację metra Saint Michel w czerwcu 1995 r. czy licznych zamieszek w Paryżu i dzielnicach podmiejskich, których autor był naocznym świadkiem. Zanalizowany jest też m.in. głośny przypadek Mohameda Meraha, odpowiedzialnego za zabicie trójki żydowskich dzieci na przedmieściach Tuluzy w 2012 r.

Autor nie omieszkał skomentować także konfliktogennych momentów w relacjach dwóch pozostałych krajów Maghrebu (Maroka i Tunezji) z Francją. Poznajemy chociażby epizody związane z działaniem profrancuskiej organizacji terrorystycznej La Main Rouge w Casablance w latach 50. XX w. Hussey wnika także w wewnętrzne rozgrywki na szczytach władzy w Maroku, jak na przykład w konflikt króla Hassana II z socjalistą Mehdim Ben Barką, oraz szkicuje genezę pierwszych organizacji islamistycznych formujących się na terenie tego państwa (Chabiba Islamiya i Al Adl Wal Ihsane) na początku lat 70. XX w. Podkreśla przy tym szczególny przypadek władz Maroka, które pozwoliły na bezprecedensową ingerencję zachodnioeuropejskich trendów kulturowych w świat arabski i tym samym doprowadziły w latach 90. ubiegłego wieku m.in. do wykształcenia się wśród marokańskiej młodzieży tzw. generacji M6. Innym przykładem są ekskluzywne kurorty turystyczne oraz rozwinięta sieć kasyn. Westernizacja monarchii skutkowała w latach 80. i 90. dyfuzją ruchów odwołujących się do wahabizmu i salafizmu (m.in. organizacja Salafi Jihadi).

Wyjaśniając kulisy zamachów na pociągi w Madrycie, dokonanych m.in. przez marokańskich ekstremistów w marcu 2004 r., Hussey wykracza w swojej opowieści także poza główne kraje jego zainteresowania – odnosi się do hiszpańskich terytoriów autonomicznych Ceuta i Mililla.

Nieprzypadkowo chyba klamrą zamykającą książkę jest rozdział dotyczący Tunezji, która przez osobę Mohammeda Bouaziziego staje się symbolicznym induktorem „arabskiej wiosny" 2011 r.

Dzięki retrospektywnemu podejściu Husseya do realiów obecnie panujących we Francji czytelnik styka się z korzeniami francuskiego ruchu nacjonalistycznego, działającego od lat 70. XX w. pod przywództwem kontrowersyjnego lidera Jeana-Marie Le Pena, a następnie jego córki.

Opinia

Recenzowana publikacja jest napisana przystępnie i ciekawie. Intryguje zwłaszcza przez wzgląd na wieloaspektowe – polityczne, społeczne i kulturowe – ujęcie problemów. Odnajdujemy tu wiele odniesień do architektury, muzyki i języka. Książka jest utrzymana w konwencji publicystyki dziennikarskiej. Tezy w niej zawarte sprawiają wrażenie rzeczowych i logicznych.

Słabością publikacji jest natomiast marginalne potraktowanie ekonomicznego aspektu francuskiego kolonializmu i zignorowanie problemów gospodarczych w relacjach państw Maghrebu z francuskimi władzami. W książce są zamieszczone przypisy, ale jest ich stosunkowo niewiele i odsyłają one wyłącznie do źródeł publikowanych. Brakuje map (poza dwoma wyjątkami) i materiału ikonograficznego, choć nie utrudnia to odbioru treści. Do każdego z rozdziałów autor dołączył wykaz literatury przedmiotu.

Publikacja zawiera indeks nazwisk, nazw geograficznych i rzeczowy. Jej mankamentem może być ograniczenie literatury (w tym nielicznych wspomnień i relacji – w przypadku Tunezji autorstwa Leïly Ben Ali oraz Habiba Burgiby) oraz czasopism do wydań anglo- i francuskojęzycznych („Le Monde", „Le Parisien", „Le Figaro") i jednoczesne zignorowanie piśmiennictwa arabskojęzycznego (chyba że doczekało się ono przekładów na języki europejskie).

The French Intifada… pełni funkcję edukacyjno-popularyzatorską. Pod względem gatunku literackiego jest zbliżona do reportażu. Autor w udany sposób próbuje poszerzyć wiedzę czytelników poszukujących głębszych korzeni niepokojów na tle etnicznym, religijnym, społecznym i politycznym w dzisiejszej Francji, poza związanymi ze zradykalizowaniem się imamów i propagandą ISIS. Pomaga zrozumieć frustrację, upokorzenie, i często nieuzasadnione pretensje muzułmańskich obywateli V Republiki, drzemiące na francuskich przedmieściach. Oczywiście chodzi tu jedynie o wybrane grupy etniczne. Hussey nie komentuje bowiem nastrojów Francuzów wywodzących się z krajów Sahelu i dawnych kolonii Afryki Subsaharyjskiej.

III
PRZEGLĄD
PRAC KONKURSOWYCH

V edycja ogólnopolskiego konkursu szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa

Edycja 2014/2015 – wyniki konkursu

Na ogłoszony przez szefa Agencji Bezpieczeństwa Wewnętrznego konkurs dla absolwentów studiów I i II stopnia wpłynęło 21 prac obronionych w roku akademickim 2014/2015.

Komitet konkursowy, po dokonaniu oceny nadesłanych prac, zdecydował przyznać następujące nagrody:

I nagroda:

– p. Kamil Baraniuk (Uniwersytet Wrocławski, Wydział Nauk Społecznych) – *Działalność służb wywiadowczych Federacji Rosyjskiej w świetle raportów służb specjalnych wybranych państw Unii Europejskiej.*

II nagroda:

– p. Sandra Kochanowicz (Uniwersytet Szczeciński, Wydział Humanistyczny) – *Powstanie, organizacja i działalność Urzędu Ochrony Państwa (1990–2002).*

III nagroda:

– p. Konrad Graczyk (Uniwersytet Śląski, Wydział Prawa i Administracji) – *Sprawa majora Jerzego Sosnowskiego w świetle niemieckich i polskich akt procesowych.*

– p. Jakub Dej (Uniwersytet Warszawski, Wydział Dziennikarstwa i Nauk Politycznych) – *Przeciwdziałanie finansowaniu terroryzmu w świetle obowiązującego prawa.*

VI edycja ogólnopolskiego konkursu szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa.

Edycja 2015/2016 – ogłoszenie konkursu

Celem konkursu jest promocja i upowszechnianie problematyki bezpieczeństwa wewnętrznego państwa wśród młodzieży i kadry akademickiej, zwiększenie świadomości społecznej w tym zakresie oraz profilaktyka i edukacja na rzecz bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Obszary tematyczne konkursu:

1. Służby specjalne II RP.
2. Rola służb specjalnych w demokratycznym państwie prawa i w państwach autorytarnych.
3. Konstytucyjne prawa obywateli a uprawnienia służb specjalnych.
4. Bezpieczeństwo Polski w XXI wieku – zagrożenia i wyzwania przez pryzmat ustawowych zadań służb specjalnych.
5. Służby specjalne państw NATO, UE i krajów sąsiedzkich RP – współdziałanie i historia.
6. Obraz służb specjalnych w mediach – stereotypy i uprzedzenia.
7. Służby specjalne w literaturze, sztuce i w filmie.

Uczestnicy mogą zgłosić do konkursu własną pracę licencjacką lub magisterską napisaną w języku polskim i obronioną na oceną bardzo dobrą w roku akademickim 2015/2016. Prace powinny być przesłane w wersji papierowej i elektronicznej wraz z wypełnionym formularzem zgłoszenia (plik do pobrania). Do pracy powinny być dołączone opinie promotora (lub recenzentów) i ich pisemna zgoda na wykorzystanie opinii (lub recenzji) w celach konkursowych.

Prace powinny być przesłane na adres:

Gabinet Szefa ABW
00-993 Warszawa
ul. Rakowiecka 2a

z dopiskiem „KONKURS" na kopercie

e-mail: redakcja.pbw@abw.gov.pl

Prace należy przesłać do **30 września 2016 r.** (decyduje data stempla pocztowego).

Nadesłane prace będzie oceniać Komitet Konkursowy wyłoniony przez szefa ABW. Komitet wyłoni laureatów konkursu: I, II, III miejsce oraz wyróżnienia, w terminie do **30 listopada 2016 r**.

Wyniki konkursu zostaną opublikowane na stronie internetowej www.abw.gov.pl w ciągu 14 dni od wyłonienia laureatów. Laureaci i ich macierzyste uczelnie otrzymają pisemne powiadomienia o wyniku konkursu.

Nagrody:

1. Pierwsza nagroda – nagroda finansowa – 3000 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego".
2. Druga nagroda – nagroda finansowa – 2500 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego".
3. Trzecia nagroda – nagroda finansowa – 2000 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego".

Wyróżnienia:

nagroda rzeczowa oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego".

Osoby biorące udział w konkursie szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa muszą oświadczyć, że wyrażają zgodę na upowszechnienie treści zawartych w ich pracy w celu promowania tematyki bezpieczeństwa państwa oraz w celach służbowych ABW. Muszą również wyrazić zgodę na przetwarzanie swoich danych osobowych. Jednocześnie mają prawo dostępu do swoich danych i ich poprawiania zgodnie z przepisami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922).

Konrad Graczyk

Sprawa majora Jerzego Sosnowskiego w świetle niemieckich i polskich akt procesowych[1]

(…) Niemiecki kontrwywiad prowadził postępowanie sprawdzające Jerzego Sosnowskiego na przełomie 1927 i 1928 r. Zastosowano wobec niego obserwację, kontrolę korespondencji oraz podsłuch telefoniczny[2]. Ze względu na udział w czynnościach Günthera Rudloffa – agenta Sosnowskiego, postępowanie nie wykazało, aby polski oficer prowadził w Berlinie działalność szpiegowską. Rudloff zaproponował bowiem swojemu przełożonemu – majorowi Niedenführowi[3] nawiązanie bliższej znajomości z Sosnowskim, co ten zaaprobował[4]. Było to sprytne posunięcie pozwalające skutecznie maskować współpracę.

W 1928 r. Rudloff został dyscyplinarnie zwolniony z Abwehry. Nie mógł już informować Sosnowskiego o działaniach kontrwywiadu ani na nie wpływać, w związku z czym przestał być współpracownikiem polskiego wywiadu[5]. Wydaje się, że wraz z odejściem Rudloffa Sosnowski przestał otrzymywać informacje z wnętrza Abwehry[6].

Gdy przyjmuje się narrację chronologiczną, na podstawie literatury można sądzić, że mniej więcej w 1932 r. niemiecki kontrwywiad rozpoczął czynności, których podmiotem był Jerzy Sosnowski, a przedmiotem – rozpoznanie jego kontaktów[7]. Ponieważ prym w otoczeniu polskiego oficera wiodły kobiety, Abwehra[8] usiłowała pozyskać je do współpracy. Oficerowie niemieckiego kontrwywiadu nie przypuszczali jednak, że poinformują one o tym Sosnowskiego. Uczyniła tak baronowa von Ronhay, która w porozumieniu z Sosnowskim przekazała Abwehrze listę obejmującą ponad 60 nazwisk[9] osób, z którymi utrzymywał on kontakty. Zaletą tego rodzaju działania było to, że rozpracowywana osoba – w tym przypadku Sosnowski – była świadoma stanu wiedzy niemieckiej

[1] Fragment pracy magisterskiej pt. *Sprawa majora Jerzego Sosnowskiego w świetle niemieckich i polskich akt procesowych*, która zajęła trzecie miejsce w konkursie szefa ABW na najlepszą pracę magisterską/licencjacką z dziedziny bezpieczeństwa wewnętrznego (V edycja). Redakcja dokonała niezbędnych poprawek oraz zmian numeracji przypisów (przyp. red.).

[2] H. Ćwięk, *Rotmistrz Sosnowski*. *As wywiadu Drugiej Rzeczypospolitej*, Kraków 2010, s. 99 i 101.

[3] W dotychczasowych pracach występowało nazwisko „Niederführ", jednak materiał archiwalny przywołany w poprzednim rozdziale nie pozostawia wątpliwości.

[4] W. Kurpis, *Berlińska misja*, Warszawa 1983, s. 73–75.

[5] H. Ćwięk, *Rotmistrz Sosnowski*..., s. 108 i 147.

[6] Najprawdopodobniej jedynie M. Zacharski, odnosząc się do tej sprawy, podaje, że utratę Rudloffa zrekompensował kontakt z niejaką Elizabeth, żoną wysokiego rangą pracownika Abwehry. Autor jednak w żaden sposób tego nie udokumentował. Zob. M. Zacharski, *Operacja Reichswehra*. *Kulisy wywiadu II RP*, Poznań 2013, s. 557, 558, 568, 575 i 583; tenże, *Rotmistrz*, Poznań 2011, s. 295.

[7] W. Kurpis, *Berlińska misja*…, s. 108–116; H. Ćwięk, *Rotmistrz Sosnowski*..., s. 115–117; tenże, *W tajnej służbie II Rzeczypospolitej*. *Wywiad Polski wobec Niemiec w latach 1918–1939*, Częstochowa 2009, s. 202. O. Reile podaje, że tajna policja (*Geheime Staatspolizei – Gestapo*) i Abwehra w 1933 r. rozpoczęły ustalenia, które doprowadziły do aresztowania Sosnowskiego w lutym 1934 r. Zob. O. Reile, *Geheime Ostfront. Die deutsche Abwehr im Osten 1921–1945*, München 1963, s. 129.

[8] S. Lewicki w swojej pracy podał, że w celu „przypadkowego" nawiązania znajomości z Sosnowskim grupa złożona z piętnastu młodych dziewczyn, agentek Abwehry, miała polecenie przebywania w tych kabaretach i restauracjach, w których bywał Polak. Nie przyniosło to jednak rezultatu, Sosnowski bowiem unikał przygodnych kontaktów w nocnych lokalach i bawił się w kręgu sprawdzonych przyjaciół. Zob. S. Lewicki, *Szpiedzy Kajzera i Hitlera*, Warszawa 1987, s. 124–126.

[9] H. Ćwięk, *Rotmistrz Sosnowski*…, s. 115–116.

służby na swój temat, a co ważniejsze – stymulowała jej dalsze działania. Można przypuszczać, że Abwehra zajęła się sprawdzaniem wskazanych osób. Zważając jednak na ich liczbę, była to praca żmudna i czasochłonna.

Na polecenie Abwehry bliższy kontakt z Sosnowskim nawiązała Xenia von Bockelmann. Jej zadaniem było m.in. przeglądanie notatek oraz listów polskiego oficera. Również ona poinformowała Sosnowskiego o swoich kontaktach z niemieckim kontrwywiadem[10].

Najprawdopodobniej identyczną rolę powierzono poznanej przez Sosnowskiego Xeni von Engelhardt. Kolejną kochanką polskiego oficera, której Abwehra zleciła gromadzenie informacji o nim, była Maria de Camp. Także ona ostrzegła go przed niemieckim kontrwywiadem oraz przed współpracownikami Abwehry: Xenią Heuer i porucznikiem von Flotowem[11].

Ponieważ w dotychczasowej literaturze przedmiotu brakowało informacji na temat Xeni Heuer i porucznika von Flotowa[12], w pracy zostaną poczynione starania, aby zapełnić tę lukę na podstawie przeglądu niemieckich archiwaliów. Będzie to okazją do poznania taktyki i metod niemieckiego kontrwywiadu, zastosowanych przeciwko Sosnowskiemu i placówce „In-3".

Sprawa Xeni Heuer

Jeśli chodzi o sprawę Xeni Heuer, to został zachowany akt oskarżenia z 22 listopada 1934 r. w sprawie o sygnaturze 7/11 J 145/34[13]. Czytamy w nim, że oskarżona Xenia Heuer, z domu von Engelhardt, zamieszkała w Berlinie przy ulicy Duisburgerstrasse 16, urodziła się 6 lipca 1910 r. w Wilnie i była urzędniczką handlową (*kaufmännische Angestellte*). Miała niemieckie obywatelstwo, była niekarana i rozwiedziona. Od 17 maja 1934 r. była tymczasowo aresztowana w więzieniu śledczym (*Untersuchungsgefängnis*) w Berlinie-Moabicie[14].

Z powyższego dokumentu można też się dowiedzieć, kiedy Xenia Heuer została tymczasowo aresztowana. Okres pomiędzy zatrzymaniem Sosnowskiego (27 lutego 1934 r.) i jego aresztowaniem a aresztowaniem Heuer (17 maja 1934 r.) pozwala sądzić, że nie uważano jej za osobę działającą wspólnie z polskim oficerem na szkodę Rzeszy. W innym przypadku zostałaby ujęta razem z nim, a w razie nieobecności – przy najbliższej okazji. Do jej zatrzymania musiało dojść krótko przed osadzeniem w więzieniu śledczym, skoro przepisy niemieckiej procedury karnej mówiły o bezzwłocznym doprowadzeniu zatrzymanej osoby przed oblicze sędziego sądu pierwszej instancji w okręgu, w którym nastąpiło zatrzymanie (§ 128 ust. 1 StPO). Sędzia przesłuchiwał zatrzymanego najpóźniej następnego dnia po doprowadzeniu (§ 128 ust. 2 StPO). Jeżeli uważał zatrzymanie za nieusprawiedliwione albo jego przesłanki za wyeliminowane, to zarządzał zwolnienie. W przeciwnym razie wydawał nakaz aresztowania (§ 128 ust. 2 StPO).

Xenia Heuer została oskarżona o to, że w 1933 r. w Berlinie umyślnie przesłała (*gelangen lassen*) osobie działającej w interesie zagranicznego rządu informację, której utrzymanie w tajemnicy było niezbędne do ochrony i obrony interesów narodowych, przez co zagroziła bezpieczeństwu Rzeszy. Oskarżono ją więc o zbrodnię (*Verbrechen*) przeciwko

[10] Tamże, s. 116–117.
[11] Tamże, s. 119–121. Zachowane archiwalia wskazują, że Xenia von Engelhardt i Xenia Heuer to ta sama osoba.
[12] Tamże, s. 121.
[13] Bundesarchiv (BArch), R 3017/14987, t. 1, z. 2, *Anklageschrift gegen Xenia Heuer*.
[14] Tamże, s. 1.

§ 1 ust. 2 ustawy przeciwko zdradzie tajemnic wojskowych z 3 czerwca 1914 r. w związku z § 88, § 89 StGB w wersji ustawy z 24 kwietnia 1934 r., § 1 pkt 2 rozporządzenia prezydenta Rzeszy przeciwko zdradzie narodu niemieckiego i zdradzieckim knowaniom z 28 lutego 1933 r. i § 2 ust. 2 StGB[15].

O życiu osobistym oskarżonej Heuer wiadomo, że po ukończeniu liceum przez dwa i pół roku pracowała w wydawnictwie Ullstein w Berlinie. W styczniu 1931 r. wyszła za mąż za Wernera Heuera, ale rozwiodła się z nim już po roku. Od tego momentu utrzymywała się z alimentów od byłego męża oraz dotacji jednego z przyjaciół[16].

Autor aktu oskarżenia podaje, że Xenia Heuer poznała polskiego oficera wywiadu Jerzego Sosnowskiego 6 lipca 1932 r. dzięki jednej z jego kochanek – Marii de Camp. Po około 5–6 tygodniach znajomości stosunki pomiędzy obojgiem zaczęły być coraz bliższe. Na początku sierpnia 1932 r. wspólnie wybrali się samochodem na kilkudniową wycieczkę do Pragi. Później Heuer pozostawała w gronie znajomych Sosnowskiego, poznała m.in. panią von Berg (tj. Benitę von Falkenhayn, która wtedy nosiła nazwisko męża – Josefa von Berga – przyp. aut.), jego rodziców oraz brata[17].

Informacja o tym, że Heuer poznała rodziców Sosnowskiego oraz jego brata, jest zaskakująca. Po pierwsze nie pojawiła się do tej pory w literaturze. Po drugie trudno wskazać sytuację, w której takie spotkanie miałoby się odbyć. Mogło mieć miejsce w Berlinie lub w Polsce. Jest jednak mało prawdopodobne, że się odbyło, ponieważ rodzice Sosnowskiego przyjechali do Berlina na początku 1932 r., a więc przynajmniej pół roku przed poznaniem Heuer przez Sosnowskiego. Nawet jeśli przyjąć, że przyjazd rodziców Sosnowskiego do Berlina nastąpił później, to w żadnym z przekazów nie ma informacji o tym, że zabrali ze sobą brata Jerzego – Janusza. Nikt też nie wspominał o osobnej wizycie brata[18]. Ponowne odwiedziny rodziców wydają się wątpliwe, zwłaszcza ze względu na ostrożność wymuszoną publikacją artykułu w „Berliner Tribüne", który powstał w wyniku podejrzeń niezamierzenie wywołanych przez matkę Sosnowskiego, opowiadającą o sytuacji majątkowej rodziny. O ile wiadomo, żaden z autorów nie wspomina, aby podczas którejkolwiek z podróży do Polski Xenia Heuer towarzyszyła Sosnowskiemu.

Rodzi się więc pytanie, skąd autor aktu oskarżenia zaczerpnął tę informację? Pod uwagę bierze się tutaj dwie hipotezy: z wyjaśnień podejrzanej lub obserwacji kontrwywiadu (ewentualnie policji). Wydaje się, że ten problem można rozstrzygnąć, opierając się na odesłaniu akapitowym umieszczonym na marginesie aktu oskarżenia, które brzmiało: *Sbd. H Bl. 5*. Oznaczało ono, że informacje zawarte w danym akapicie pochodzą z tomu specjalnego (*Sonderband – Sbd.*)[19]. Litera „H" była inicjałem nazwiska oskarżonej, skrót Bl. (*Blatt*) wskazywał kartę akt. Świadczyłoby to o tym, że o poznaniu rodziców Sosnowskiego i jego brata Xenia Heuer opowiedziała podczas przesłuchania. Wydaje się, że nie miała powodu kłamać lub zatajać prawdy. Fakt poznania przez nią

[15] Przepisy prawa przywołane w akcie oskarżenia, poza § 2 ust. 2 StGB, zostały scharakteryzowane w rozdziale I, w podrozdziale poświęconym ustawodawstwu Niemiec. Przepis § 2 ust. 2 StGB w wersji obowiązującej od 1 stycznia 1872 r. do 1 września 1935 r. stanowił, że w razie różnicy w ustawie między czasem popełnienia czynu a czasem jego osądzenia należy stosować ustawę łagodniejszą.

[16] Bundesarchiv (BArch), R 3017/14987, t. 1, z. 2, *Anklageschrift gegen Xenia Heuer*, s. 2.

[17] Tamże.

[18] Wiarygodny dowód na tę okoliczność prezentuje w swojej książce jedynie S. Strumph-Wojtkiewicz. Mowa tu o zdjęciu, wedle opisu wykonanym w berlińskim parku Tiergarten. Ma ono przedstawiać Sosnowskiego, jego brata Janusza oraz Benitę von Falkenhayn. Zob. S. Strumph-Wojtkiewicz, *Gra wojenna*, Warszawa 1969, s. 112.

[19] Metodyka postępowania determinowała, aby w tomie głównym (*Hauptband – Hptbd.*) znalazły się ogóły sprawy (*Allgemeines*), w podtomie (*Unterband – Ubd.*) – rezultaty ustaleń policyjnych (*polizeiliche Ermittlungen*), a w tomie specjalnym – rezultaty śledztwa wstępnego (*Vorgänge der Voruntersuchung*).

rodziców i brata Sosnowskiego był prawnie irrelewantny, tj. nieistotny dla odpowiedzialności karnej z przywołanych w akcie oskarżenia przepisów prawa.

W części aktu oskarżenia poświęconej stanowi faktycznemu można przeczytać, że w kwietniu 1933 r. skontaktował się z oskarżoną porucznik w stanie spoczynku (*Oberleutnant außer Dienst – Oberleutnant a.D.*) Andreas von Flotow, działający na zlecenie Abwehry. Jego celem było poznanie Jerzego Sosnowskiego i Benity von Berg. W dniu 18 kwietnia 1933 r., po wcześniejszym kontakcie telefonicznym, Flotow złożył krótką wizytę w mieszkaniu Heuer. Poinformował ją, jak sama przyznała, pod najsurowszym nakazem milczenia, że Sosnowski jest podejrzewany o szpiegostwo na rzecz Polski. O sobie powiedział, że pracuje dla RWM (*Reichswehrministerium* – Ministerstwo Reichswehry) i dlatego chce zostać przedstawiony Sosnowskiemu i pani von Berg. Ze względu na nieobecność Sosnowskiego (wyjechał za granicę) Heuer postanowiła najpierw poznać Flotowa z Benitą von Berg. Uknuła więc spisek. Powiedziała von Berg, że niedawno poznała ziemianina z Meklemburgii, niejakiego von Flotowa, za którego chce wyjść za mąż. Chciałaby jednak w kwestii zamążpójścia poradzić się kobiety bardziej od siebie doświadczonej. Von Berg, która uchodziła za taką właśnie osobę, zgodziła się jej pomóc. Zaproponowała, że zaprosi narzeczonych na wieczorek do swego domu. Zaproszenie nadeszło w końcu kwietnia 1933 r. Heuer, zgodnie z umową, przekazała je Flotowowi. Ten miał przed sobą pilną podróż, ale obiecał, że do dnia przyjęcia na pewno wróci do Berlina. Tak się jednak nie stało. Flotow nie zjawił się na spotkaniu. W dniu 1 maja 1933 r. Heuer przeczytała w gazecie, że poszukiwany listem gończym (*steckbrieflich*) von Flotow został zastrzelony podczas ucieczki[20].

We wspomnianym fragmencie aktu oskarżenia została opisana jedna z wielu nieudanych prób „podejścia" Abwehry do Jerzego Sosnowskiego. W tym przypadku w misji kontrwywiadu działał Andreas von Flotow, a osobą, która miała go wprowadzić w krąg towarzyski polskiego oficera, była jedna z jego kobiet – Xenia Heuer. Wyraźnie również wskazano, że w kwietniu 1933 r. Sosnowski był podejrzewany o szpiegostwo na rzecz Polski.

Dalej autor aktu oskarżenia podaje, że jesienią 1933 r. Heuer powróciła do kręgu towarzyskiego Sosnowskiego i wzięła udział w wielkim przyjęciu w jego domu. Najprawdopodobniej wówczas zdradziła polskiemu oficerowi misję von Flotowa. Prokurator oparł swoje podejrzenie na wiarygodnym zeznaniu tancerki Lei Kruse. Sosnowski zwierzył się jej w grudniu 1933 r. lub w styczniu 1934 r., że Heuer poinformowała go, iż za wynagrodzeniem 50 marek otrzymała zadanie obserwowania go z powodu podejrzewania go o szpiegostwo. Z sympatii do niego obiecała mu jednak, że go nie zdradzi. Prokurator podkreślił, że Kruse składała to zeznanie nie tylko w fazie śledztwa wstępnego (*Voruntersuchung*), lecz także przed wdrożeniem postępowania przygotowawczego (*Vorverfahren*) w obecności funkcjonariusza kontrwywiadu. Treść oskarżenia wzmocnił wskazaniem, że swego czasu von Flotow zażądał od Abwehry 50 marek tytułem zwrotu kwoty, którą zapłacił Heuer, żeby „pójść dalej" w sprawie Sosnowskiego[21]. O postawie oskarżonej czytamy, że po początkowych zaprzeczeniach 19 kwietnia 1934 r., po przeprowadzeniu przez radcę kryminalnego (*Kriminalrat*) Kubitzkiego konfrontacji z Leą Kruse w urzędzie tajnej policji państwowej w Berlinie (*Geheime Staatspolizeiamt*), przyznała się do winy. Wyjaśniła wówczas, że podczas wieczorku zorganizowanego przez Sosnowskiego w jego mieszkaniu pod koniec jesieni 1933 r. rozmawiała z nim o krążą-

[20] BArch, R 3017/14987, t. 1, z. 2, *Anklageschrift gegen Xenia Heuer*, s. 2–3.
[21] Tamże, s. 3–4.

cych w publicznym obiegu podejrzeniach dotyczących jego osoby. Mówiła mu o misji von Flotowa i o swojej w niej roli. Z tego opowiadania Sosnowski mógł wywnioskować, że Abwehra jest blisko Heuer. Oskarżona powiedziała mu także, że nie chce być dla niego zła. Zaprzeczyła natomiast, jakoby powiedziała, że otrzymała od Flotowa na wykonanie zadania 50 marek. Chciała, aby Sosnowski był na wolności. Twierdzenie Flotowa, że na zlecenie RWM ma on obserwować polskiego oficera w związku z podejrzewaniem go o szpiegostwo, uważała za nieprawdziwe. Ponadto dodała, że powiedziała Sosnowskiemu o swoich obawach, tj. o tym, że przez jego kontakty może znaleźć się w niebezpieczeństwie i że z jego powodu może zostać przewieziona do Oranienburga (do ówczesnej siedziby SS; od lipca 1936 r. znajdował się w tym mieście obóz koncentracyjny Sachsenhausen – dop. aut.). Początkowe zaprzeczenia tłumaczyła obawą przed kłopotami[22].

Powyższy fragment świadczy o przeprowadzeniu przez prowadzącego sprawę policjanta z tajnej policji państwowej (Gestapo) właściwej czynności procesowej we właściwym momencie. Norma kompetencyjna była zawarta w § 58 ust. 2 niemieckiego kodeksu postępowania karnego z 1 lutego 1877 r. (*Strafprozessordnung* – StPO)[23]. Ten przepis stanowił, że konfrontacja (*Gegenüberstellung*) ze świadkiem lub podejrzanym była dozwolona w postępowaniu przygotowawczym, jeżeli było to uzasadnione dla dalszego postępowania. Jak wynika z przepisu, przesłanka dotycząca uzasadnienia podjęcia czynności była niewystarczająca i ocenna. Wydaje się, że w praktyce nie stanowiła bariery dla przeprowadzania konfrontacji w postępowaniu przygotowawczym.

Istotą konfrontacji jest postawienie sobie do oczu przesłuchiwanych osób składających sprzeczne lub zupełnie odmienne od siebie oświadczenia w celu wyjaśnienia różnic[24]. Konfrontację określa się jako szczególną formę przesłuchania dwóch osób, która to forma charakteryzuje się jednością czasu, miejsca, przedmiotu i dokumentacji przesłuchania[25]. W analizowanej sprawie przyniosła ona skutek w postaci przyznania się podejrzanej, a następnie oskarżonej Xeni Heuer. Z tego wynika, że czynność procesowa została przeprowadzona prawidłowo.

Autor aktu oskarżenia podaje, że w fazie śledztwa wstępnego *(Voruntersuchung*) oskarżona twierdziła, iż podczas przesłuchania 19 kwietnia 1934 r. nie złożyła oświadczeń, które znalazły się w protokole przesłuchania. Przed sędzią śledczym (*Untersuchungsrichter*) zaś przedstawiła sprawę inaczej. Wyjaśniła, że krótko przed wspomnianym przyjęciem w prasie ukazał się artykuł[26], w którym napisano o podejrzeniach wobec Sosnowskiego (szpiegostwo na szkodę Niemiec). Tego rodzaju plotki krążyły między gośćmi polskiego oficera. Sosnowski zwierzył się, że był nawet przez swoich znajomych pozdrawiany słowami: *Dzień dobry, panie szpiegu*[27]. Heuer dedukowała przy tym, że jeżeli Sosnowski naprawdę przebywałby w Niemczech z tajną misją, to byłby dość przebiegły, aby tak zorganizować swoją działalność, żeby przez nikogo nie została roz-

[22] Tamże, s. 4–5.

[23] Reichsgesetzblatt (RGBl.) 1877, s. 253. Ten przepis w czasie przeprowadzania czynności procesowej miał taką samą treść jak dzisiaj.

[24] S. Waltoś, *Proces karny*. *Zarys systemu*, Warszawa 2009, s. 407.

[25] P. Łobacz, *Konfrontacja*. *Studium karnoprawne i kryminalistyczne*, Warszawa 2013, s. 62. Ekspresywnie o konfrontacji wypowiedział się prawnik i filozof Jeremy Bentham. Pisał on: (…) *gdy natrafi na zeznania sprzeczne z sobą, zarządza konfrontację i daje stronom możność wzajemnego natarcia na siebie, a z tego zderzenia wykrzesza się prawda*. Zob. J. Bentham, *Traktat o dowodach sądowych,* Gniezno 1935, s. 20.

[26] Najprawdopodobniej chodzi o inną publikację niż artykuł z 10 maja 1932 r. z „Berliner Tribüne". Wątpliwe jest bowiem, aby Heuer okres pomiędzy 10 maja 1932 r. a jesienią 1933 r., tj. gdy odbyło się przyjęcie u Sosnowskiego, uważała za krótki.

[27] W oryginale: *Guten Tag, Herr Spion*.

poznana[28]. Ponadto wskazała, że na jej uwagi, iż kontakty z nim wywołują podejrzenia, Sosnowski odpowiedział, że grono jego gości jest doborowe i zagrożenie, o jakim ona mówi, nie istnieje. Heuer odparła Sosnowskiemu, że była u niej osoba, która ostrzegała ją przed kontaktami z nim i przed nieprzyjemnościami, jakie z tego mogą wyniknąć. Prokurator wskazał, że to oświadczenie odnosiło się do podejrzenia o szpiegostwo przytoczonego przez samego Sosnowskiego. Oskarżona jednak nie powiedziała, że swego czasu zwrócono jej na to uwagę. Nie wspomniała o von Flotowie, przyjęciu pieniędzy ani o niemieckim kontrwywiadzie. Ponadto twierdziła, iż nie myślała, że ścigany listem gończym Flotow (czytała o tym w gazecie), zbliżając się do niej, działał na rzecz Abwehry. Nie mogła więc sądzić, że taki człowiek może służyć w RWM. Przed sędzią śledczym dodała, że Sosnowski – jak to często miał w zwyczaju – żartował, opowiadając Kruse o tym, jakoby dowiedział się od Heuer, że za swoje zadanie otrzymała ona 50 marek[29].

Prokurator wskazał, że Sosnowski dowiedział się od pani de Camp, iż za jej pośrednictwem niejaki von Flotow lub Flotwell skontaktował się z oskarżoną Heuer i zaangażował ją do swojego zadania. Polski oficer zaprzeczył jednak, jakoby Heuer kiedykolwiek powiedziała mu o zwerbowaniu jej przez Abwehrę w celu obserwowania go i że otrzymała za to 50 marek. Wyłącznie Kruse powiedział, gdy ta z uznaniem wypowiadała się o Heuer, że nie należy jej za bardzo ufać, ponieważ wiedział, jakie Heuer ma polecenie. Stanowisko zajęte przez świadka Kruse Sosnowski wyjaśnił w ten sposób, że być może oskarżona Heuer sama się jej zwierzyła. Wątek zeznań polskiego oficera prokurator podsumował tym, że zasłaniał się on niepamięcią. Przypomniał sobie tylko tyle, że Heuer raz wspomniała mu, że została ostrzeżona przed nim przez jakiegoś mężczyznę[30].

Prokurator przedstawił postawę oskarżonej oraz rezultaty śledztwa wstępnego przed rozprawą główną. Oskarżona zmieniła złożone wyjaśnienia. Przypomnijmy, że początkowo zaprzeczyła formułowanym zarzutom, po czym przyznała się do nich po przeprowadzeniu konfrontacji, a następnie znów wycofała zeznania. Ostatni z zabiegów, polegający na wyparciu się wyjaśnień (zaprotokołowanych 19 kwietnia 1934 r. i przez nią podpisanych), wydaje się obraną przez nią linią obrony. W tym miejscu warto nadmienić, że składane wyjaśnienia, nawet następnie zmienione, podlegały w całości ocenie sądu, który powinien był kierować się zasadą swobodnej oceny dowodów, tj. jednym oświadczeniom mógł dać wiarę, a innym nie.

Znajdujemy wreszcie fragment aktu oskarżenia oparty na zeznaniach Jerzego Sosnowskiego jako świadka. Jakkolwiek nie są one obszerne, pozwalają potwierdzić wniosek dotyczący jego postawy w czasie przesłuchań, formułowany już przez innych autorów[31]. Odpowiedzi udzielane przez polskiego oficera pozwalają sądzić, że starał się on umniejszyć winę oskarżonej Heuer. Wskazał bowiem, że o powiązaniach von Flotowa i Heuer z niemieckim kontrwywiadem dowiedział się od Marii de Camp. Obciążył tym samym osobę zmarłą, której żadna odpowiedzialność ze strony niemieckiego państwa już nie groziła. Taktycznym, aczkolwiek skutecznym zabiegiem zastosowanym przez polskiego oficera było zasłanianie się niepamięcią. Zeznania Sosnowskiego nie wydawały się wspierać aktu oskarżenia.

Trzecia część aktu oskarżenia została poświęcona prawnej ocenie stanu faktycznego. Czytamy w niej, że na podstawie wyjaśnień (prawidłowość ich zaprotokołowania

[28] W oryginale: (…) *wenn er aber wirklich in geheimer Mission in Deutschland wäre, würde er gewiss schlau genug sein, seine Tätigkeit so einzurichten, dass sie von niemandem erkannt werden würde*.

[29] BArch, R 3017/14987, t. 1, z. 2, *Anklageschrift gegen Xenia Heuer*, s. 5–6.

[30] Tamże, s. 6–7.

[31] Zob. H. Ćwięk, *Rotmistrz Sosnowski*..., s. 127, W. Kurpis, *Berlińska misja*..., s. 150.

nie budzi wątpliwości) oskarżonej Heuer oraz wyników dochodzeń (szczególnie zeznań Kruse) złożonych przed policją należy uważać za udowodnione, że oskarżona Heuer poinformowała polskiego oficera wywiadu Sosnowskiego o zleconej jej przez wydział Abwehry RWM misji, i przez to go ostrzegła. Misję tę – jak wiedziała na podstawie nałożonego na nią przez Flotowa nakazu milczenia – ze względu na dobro państwa należało zachować w tajemnicy. Kiedy oskarżona Heuer (mimo iż nie miała podstaw do wątpienia w prawdziwość zleconego jej przez von Flotowa zadania) posłała wiadomość Sosnowskiemu, zostało zagrożone bezpieczeństwo Rzeszy. Tego faktu nie zmienia twierdzenie polskiego oficera, że o zadaniu oskarżonej dowiedział się wcześniej od pani de Camp. Nawet jeśli dano by wiarę stanowisku Sosnowskiego, to informacje uzyskane od oskarżonej potwierdzało oświadczenie pani de Camp, na którego podstawie polski oficer był w stanie podjąć działania przeciwko kontrwywiadowi. Uczynił to, wprowadzając do akcji Kruse[32].

Prokurator skonstatował, że oskarżona Heuer przekazała osobie działającej w interesie zagranicznego rządu informację, której utrzymanie w tajemnicy było niezbędne dla ochrony i obrony interesów narodowych, i przez to zagroziła bezpieczeństwu Rzeszy[33].

W trzeciej części aktu oskarżenia prokurator przedstawił swój punkt widzenia. Zwrócił uwagę na materiał dowodowy uzasadniający wniesienie skargi publicznej. Dezawuował zaś okoliczności korzystne dla oskarżonej. Choć jako oskarżyciel publiczny powinien zachować obiektywizm w ocenie materiału dowodowego, nie mogła dziwić taka redakcja aktu oskarżenia. Prokurator dążył bowiem do skazania Heuer.

Jako materiały dowodowe (*Beweismittel*) zostały przedstawione wyjaśnienia oskarżonej oraz zeznania świadków: radcy kryminalnego Kubitzkiego z tajnej policji państwowej; jednego z funkcjonariuszy Abwehry (miał zostać wskazany później), przed którym zeznania składała Kruse przed wdrożeniem postępowania przygotowawczego; tancerki Lei Kruse osadzonej w więzieniu śledczym Berlin-Moabit oraz biegłego (*Sachverständiger*) do przedstawienia opinii RWM[34].

Prokurator Werner[35], który podpisał akt oskarżenia, wnosił o:

a) przeprowadzenie rozprawy głównej przed trzecim wydziałem Trybunału Ludowego (*Senat des Volksgerichtshofs*), stosownie do art. 3 § 3 ust. 1 ustawy o zmianie przepisów prawa karnego i postępowania karnego z 24 kwietnia 1934 r.,
b) orzeczenie dalszego aresztowania oskarżonej Heuer,
c) wyznaczenie obrońcy oskarżonej Heuer.

[32] BArch, R 3017/14987, t. 1, z. 2, *Anklageschrift gegen Xenia Heuer*, s. 7.

[33] Tamże, s. 8.

[34] Tamże.

[35] Tamże, s. 9. Karl August Werner był wówczas naczelnym prokuratorem. Najprawdopodobniej postępowanie prowadził i akt oskarżenia sporządził inny prokurator – Rudolf Kempter, ponieważ to on brał udział w rozprawie sądowej. Werner natomiast podpisał akt oskarżenia jako szef najwyższej jednostki organizacyjnej prokuratury, odpowiadającej za popieranie aktu oskarżenia przed Trybunałem Ludowym. Doktor Karl Werner urodził się 14 marca 1876 r. w Mülhausen. Studiował prawo na uniwersytetach w Strassburgu, Berlinie i Monachium. Walczył w pierwszej wojnie światowej jako kapitan (*Hauptmann*). Karierę prawniczą rozpoczął od zdania egzaminu referendarskiego w Colmar na początku grudnia 1897 r., po czym pracował jako referendarz. Państwowy egzamin prawniczy zdał 30 listopada 1903 r. na ocenę dobrą, a 14 grudnia tego roku został mianowany asesorem sądowym. Na początku 1907 r. został sędzią sądu rejonowego w Mülhausen. Następnie przeszedł do prokuratury i 10 maja 1908 r. został mianowany prokuratorem przy Wyższym Sądzie Krajowym w Colmar (*Staatsanwalt beim Oberlandesgericht Colmar*). W połowie 1919 r. został przeniesiony do Ministerstwa Sprawiedliwości Rzeszy (*Reichsjustizministerium*) na stanowisko pomocnicze, a już 1 kwietnia 1920 r. został radcą tego ministerstwa. W dniu 1 września 1926 r. został mianowany naczelnym prokuratorem przy Sądzie Rzeszy (*Reichsgericht*). Zmarł 12 października 1936 r. Zob. BArch, R 3002/PA/1050, k. 4, 31.

Powyżej zaprezentowano materiał dowodowy dotyczący Xeni Heuer i oparty na nim akt oskarżenia. Ważniejsze jest jednak to, co uczynił z nim sąd. Trybunał Ludowy po posiedzeniu w dniu 11 lutego 1935 r. w sprawie o sygnaturze 3 L 30/34 wydał wyrok uniewinniający oskarżoną Xenię Heuer[36]. W posiedzeniu, jako sędziowie, brali udział: prezydent wydziału dr Springmann – jako przewodniczący, dyrektor sądu krajowego dr Merten, sekretarz stanu Hofmann, podpułkownik Reinecke, radca rządowy dr Herzlieb – jako sędzia wotant (*Beisitzer*), pilot dowódca (*Fliegerkommandant*) Stutzer – jako sędzia zastępczy (*Ersatzrichter*)[37], prokurator Kempter – jako przedstawiciel prokuratury oraz sekretarz Schmidt – jako sądowy pracownik administracyjny[38].

Uzasadnienie wyroku trybunał rozpoczął od wskazania, że proces karny dotyczył wycinka z działalności szpiegowskiej polskiego rotmistrza Jerzego Sosnowskiego, który 16 lutego 1935 r.[39] został skazany przez ten sam wydział w tym samym składzie na karę dożywotniego ciężkiego więzienia (*lebenslänglichen Zuchthaus*). Dlatego w razie potrzeby sąd odesłał do wydanego wyroku oraz stanu faktycznego w sprawie o sygnaturze 11 J 145/34; 3 L 29/34[40].

Trybunał uzupełnił opis sytuacji osobistej Xeni Heuer. Wskazał, że była ona córką rosyjskiego oficera, który przeniósł się do Niemiec i służył w wywiadzie. Dnia 12 lutego 1931 r. poślubiła handlowca Wernera Heuera. Wyrokiem z 5 marca 1932 r. sąd krajowy w Berlinie w sprawie o sygnaturze 1. R. 74/32 orzekł rozwód z wyłącznej winy jej męża. Późniejszy sposób prowadzenia się Xeni Heuer trybunał ustalił, opierając się na rezultatach przeszukania przeprowadzonego w jej mieszkaniu 28 lutego 1934 r. W jej toaletce znaleziono cztery pudełka środków antykoncepcyjnych oraz dużo wizytówek i notatek adresowych z jej rozległych znajomości z mężczyznami. W notatkach przewijało się kilka znanych niemieckich nazwisk oraz nazwiska obcokrajowców, np. von Sosnowskiego.

W opisie czytamy również, że Xenia Heuer poznała Jerzego Sosnowskiego 6 lipca 1932 r. (dzięki pani de Camp, w restauracji Kempiński). Rychło doszło do intymnych stosunków między obojgiem. W dniu 4 sierpnia 1932 r. Heuer i Sosnowski pojechali samochodem do Pragi i w hotelu Shrubek wynajęli pokój na dwa dni. Kiedy podczas podróży oskarżona zapytała Sosnowskiego, w jakim celu tam jadą, ten jej odparł, że ma w Polsce grunty o wartości tych znajdujących się w Grunewaldzie[41], które zamierza sprzedać. W Pradze ma spotkać osobę, z którą ma zawrzeć transakcję kupna-sprzedaży. Drugiego dnia wycieczki Sosnowski wrócił zadowolony do hotelu i powiedział Heuer, że interes się udał i znów ma dużo pieniędzy. Wieczorem odwiedzili kilka restauracji;

[36] BArch, R 3017/14987, t. 2, *Urteil in der Strafsache gegen Xenia Heuer.*

[37] Instytucja sędziego zastępczego (dodatkowego) jest uniwersalna, fakultatywna i polega na wyznaczeniu do składu sądzącego dodatkowej osoby, która bierze udział w rozprawie lub posiedzeniu, a w naradzie i głosowaniu nad wyrokiem tylko w razie niemożności uczestniczenia przez jednego z pozostałych sędziów. Ma to na celu zapobieganie ujemnym następstwom związanym z niemożnością uczestniczenia w procesie sędziego wyznaczonego do składu orzekającego. Przykładowo w razie śmierci jednego z sędziów i braku sędziego dodatkowego proces należałoby prowadzić od nowa. Sędzia dodatkowy nie mógł brać udziału w rozstrzyganiu spraw incydentalnych w procesie, chyba że zastępował członka składu orzekającego. Mógł natomiast zadawać pytania oraz miał obowiązek brania udziału w rozprawie.

[38] BArch, R 3017/14987, t. 2, *Urteil in der Strafsache gegen Xenia Heuer*, s. 1.

[39] Mimo że wyrok w sprawie Xeni Heuer został wydany 11 lutego 1935 r., w uzasadnieniu sąd zwrócił uwagę na skazanego 16 lutego 1935 r. Jerzego Sosnowskiego. Sąd mógł tak uczynić, ponieważ uzasadnienie było sporządzane później.

[40] Z numeru sygnatury akt sądowych sprawy Sosnowskiego (3 L 29/34) wynika, że wpłynęła ona do Trybunału Ludowego bezpośrednio przed sprawą Xeni Heuer (3 L 30/34). Zob. BArch, R 3017/14987, t. 2, *Urteil in der Strafsache gegen Xenia Heuer*, s. 2.

[41] Dzielnica Berlina.

następnego dnia wrócili do Berlina. Pod koniec 1932 r. oskarżona zorientowała się, że Sosnowski utrzymuje bliskie relacje także z innymi kobietami, dlatego wycofała się ze znajomości z nim. Miała jednak świadomość, że polski oficer nadal interesował się kręgiem jej znajomych, a przy okazji rozmów telefonicznych dowiadywał się o nazwiska osób, z którymi utrzymywała kontakty. W styczniu 1933 r. na balu u Reimanna (*Reimann-Ball*) Heuer ponownie spotkała Sosnowskiego. Ponieważ negatywnie wyraził się o jej kostiumie, poczuła się urażona i przez kilka miesięcy nie kontaktowała się z nim.

Następnie trybunał przywołał treść oskarżenia postawionego Xeni Heuer[42].

W toku rozprawy głównej ujawniono, że porucznik w stanie spoczynku Flotow narzucał się Abwehrze twierdząc, że był dowódcą jednej z grup SA w Monachium (twierdził, że został co prawda z niej usunięty, ale wkrótce miał być zrehabilitowany) i został wyznaczony do spraw kontrwywiadowczych. W kwietniu 1933 r. Flotow nawiązał – w misji wydziału Abwehry RWM – kontakt z oskarżoną Heuer, aby dzięki niej zbliżyć się do Sosnowskiego i pani von Falkenhayn. Następnie sąd powtórzył ustalenia oskarżyciela dotyczące spotkania Heuer z Flotowem, fortelu z nim jako kandydatem na męża, pobrania przez niego 50 marek z ministerstwa i rozmowy z Benitą von Falkenhayn. Sąd dodał, że w ramach pilnego wyjazdu Flotow udał się do Rostocku (jego brat był ostro skonflikowany z pewnym ziemianinem). Następnie został przytoczony fragment artykułu prasowego, o którym mówiła oskarżona. Z tej publikacji wynikało, że von Flotow poszukiwany od jakiegoś czasu listem gończym został zatrzymany. Kiedy podczas transportu do aresztu podjął próbę ucieczki, policjanci oddali w jego kierunku kilka strzałów. Flotow zginął na miejscu.

Następnie trybunał omówił stosunki między de Camp a Sosnowskim. Wskazał, że de Camp przez długi czas była jego kochanką. Rozdzielił ich spór. Jednak gdy w październiku 1933 r. de Camp leżała na łożu śmierci, kazała przyjść Sosnowskiemu. Zwróciła wtedy jego uwagę na to, że niemiecka służba kontrwywiadowcza oraz inne służby obserwują go. Zaleciła, żeby opuścił Niemcy, a jeśli tego nie zrobi, żeby zachował środki ostrożności przed „dobranym kręgiem znajomych". Ponieważ dręczyło ją sumienie, dodała również, że sama przyprowadziła jedną agentkę, Xenię Heuer, niejakiemu Flotowowi lub Flottwellowi[43].

Dalej czytamy, że po dłuższym czasie Heuer spotkała Sosnowskiego 10 grudnia 1933 r. na balu u Karola Ernsta, w salonach ogrodu zoologicznego w Berlinie. Sosnowski poprosił ją wówczas, aby go odwiedziła. Heuer skorzystała z tego zaproszenia. Wzięła udział w wielkim przyjęciu zorganizowanym w jego mieszkaniu. Podczas tej imprezy zdradziła mu misję von Flotowa. Tak przynajmniej wynika z zeznań Lei Kruse, współskazanej w procesie głównym Sosnowskiego (*Hauptprozess Sosnowski*)[44].

Następnie zostały przytoczone zeznania Kruse oraz wyjaśnienia oskarżonej Heuer.

Biorąc pod uwagę zgromadzony materiał dowodowy, trybunał uznał, że w sprawie, niestety, nie można było wszystkiego wyjaśnić, ponieważ Flotow i de Camp zmarli. Nie było jasne, od kogo tancerka Kruse dowiedziała się, że Flotow otrzymał od Abwehry 50 marek. Nie można było wykluczyć, że Sosnowski – przy swojej rozległej sieci szpiegowskiej – dowiedział się o tym z innych źródeł. Nie dało się też odeprzeć argumentu, że oskarżona Heuer nie podała nazwiska von Flotowa jako nazwiska osoby przygotowanej przez Abwehrę do rozpracowania Sosnowskiego. Zaakcentowano, że oskarżona zajmowała takie stanowisko od początku. Już

[42] BArch, R 3017/14987, t. 2, *Urteil in der Strafsache gegen Xenia Heuer*, s. 2–3.
[43] Tamże, s. 5.
[44] Tamże, s. 5–6.

podczas pierwszego przesłuchania zdecydowanie zaprzeczyła, że zakomunikowała Sosnowskiemu o Flotowie i swojej roli w jego misji[45].

W ocenie trybunału wszystko to, co oskarżona opowiedziała o Sosnowskim podczas przesłuchań przed policją, przed sędzią śledczym oraz na rozprawie głównej, uwzględniając ukazujące się wtedy artykuły prasowe o nim, niezliczone plotki podobnej treści oraz zabiegi kontrwywiadowcze ujawnione mu w grudniu 1933 r.[46], nie mogło być uważane za tajemnicę państwową. Konstatacja sądu znalazła także potwierdzenie w opinii biegłego wojskowego z RWM[47].

Sąd wskazał, że także z subiektywnego punktu widzenia zachodziły uzasadnione wątpliwości co do skazania Heuer. Oskarżona nie otrzymała bowiem żadnego zadania od RWM, miała do czynienia jedynie z von Flotowem. W prasie zaś przeczytała, że von Flotow był poszukiwany listem gończym i został zastrzelony. Nikt nie zdementował tych informacji, nikt nie wstawił się za Flotowem. Abwehra nie przysłała do niej jego następcy (Heuer twierdziła, że bezowocnie czekała na taką osobę). Nie było żadnych dowodów na to, że Flotow był agentem RWM. Jako laik oskarżona mogła przyjąć, że miała do czynienia z oszustem. Sąd przywołał jej wyjaśnienia, w których opisywała von Flotowa jako amatora, w kiepskim garniturze i z brudnym kołnierzykiem. Podczas spotkania z nią prosił ją o pożyczkę, wspominał o rodzinie w Meklemburgii cierpiącej niedostatek, a nawet rzucił się na resztki jej jedzenia. Mówił także, że wynajmująca mu mieszkanie pani Schlegel chciała go wyrzucić z lokalu z powodu zaległości w opłacaniu czynszu[48].

Sąd dał też wiarę zeznaniom, w których oskarżona wskazała, że między 1 maja 1933 r. a jej rozmową z Sosnowskim minęło osiem miesięcy. Gdyby więc rzeczywiście chciała go ostrzec, zrobiłaby to wcześniej. Ponadto czytamy, że Sosnowski był przez długi czas w Berlinie osobą znaną, nienagabywaną ani tym bardziej zatrzymywaną. Chodził w lśniącym polskim mundurze oficerskim z odznaczeniami. Organizował wielkie przyjęcia (na 50–60 osób), na których można było spotkać oficerów, urzędników, osoby występujące w operze i filmie.

Xenia Heuer została uniewinniona z braku dowodów. Zwolniono ją także z kosztów postępowania[49]. Tym samym sąd nie dał wiary zeznaniom Lei Kruse, a pojawiające się wątpliwości rozstrzygnął na korzyść oskarżonej. Można zatem zaobserwować, jak niewiele z tez przedstawionych w akcie oskarżenia utrzymało się w końcowym orzeczeniu[50].

Sygnalizowaną już sprawę odstępu czasowego między zatrzymaniem Sosnowskiego a zatrzymaniem Heuer oraz przeprowadzonym w jej mieszkaniu przeszukaniem można wyjaśnić w ten sposób, że podczas przeszukania nie znaleziono u niej żadnych materiałów o charakterze szpiegowskim, a więc uzasadniających jej tymczasowe aresztowanie. Trybunał wskazał w wyroku jedynie na środki antykoncepcyjne oraz wizytówki i notatki adresowe. Przesłanki uzasadniające aresztowanie Heuer pojawiły się natomiast na skutek zeznań złożonych przez Leę Kruse.

---

[45] Tamże, s. 7.

[46] W innym miejscu uzasadnienia trybunał wskazał na październik 1933 r. jako moment, w którym Maria de Camp na łożu śmierci powiedziała Sosnowskiemu o działalności Abwehry przeciwko niemu. Była to najprawdopodobniej omyłka pisarska, skoro de Camp zmarła w grudniu 1933 r.

[47] BArch, R 3017/14987, t. 2, *Urteil in der Strafsache gegen Xenia Heuer*, s. 7–8.

[48] Tamże, s. 8.

[49] BArch, R 3017/14987, t. 2, *Urteil in der Strafsache gegen Xenia Heuer*, s. 8–9. Wyrok został podpisany przez skład orzekający, tj. bez sędziego dodatkowego Stutzera.

[50] Trzeba pamiętać, że wyrok wydany przez Trybunał Ludowy był ostateczny i nie przysługiwał od niego środek odwoławczy.

Sprawa Xeni Heuer dowodzi, że niemiecki kontrwywiad stosował różne metody rozpracowania Sosnowskiego. Poza klasycznymi czynnościami operacyjno-rozpoznawczymi, jak podsłuch telefoniczny, kontrola korespondencji czy obserwacja, dążył także do jego infiltracji. Temu miało służyć nawiązanie kontaktu przez von Flotowa z Heuer i wprowadzenie go do towarzystwa polskiego oficera.

Wydaje się, że omówiona sprawa nie zakończyła się powodzeniem organów ścigania. Nie można jej nawet określić mianem dobrze przeprowadzonej akcji Abwehry. Nie chodzi tutaj tylko o brak sukcesu w postaci dotarcia Flotowa do Sosnowskiego, ponieważ tragicznej śmierci Flotowa nie można było przewidzieć. Błąd niemieckiego kontrwywiadu w tej sprawie polegał na wybraniu do tego zadania złej osoby. Godne uwagi są tutaj wyjaśnienia oskarżonej Heuer, którym dał wiarę Trybunał Ludowy i które legły u podstaw oceny wiarygodności von Flotowa. Na ich podstawie jawi nam się on jako osoba niedostosowana pod względem wizerunkowym i społecznym do środowiska, w które miał wejść. Sosnowski i jego znajomi należeli do elity Berlina, a to oznaczało najlepsze ubrania, eleganckie restauracje i drogie prezenty. Można przypuszczać, że von Flotow – ze swoimi problemami finansowymi, cierpiący niedostatek – nie zostałby zaakceptowany przez tzw. towarzystwo. Być może zostałby przejrzany przez Benitę von Falkenhayn, osobę spostrzegawczą i doświadczoną, określaną jako znawczynię ludzkich charakterów, podczas planowanego na początek maja 1933 r. spotkania w jej domu.

Kolejną sprawą jest powierzenie odpowiedzialnego zadania z zakresu zwalczania obcego szpiegostwa osobie, która została dyscyplinarnie usunięta z SA oraz z NSDAP[51]. Samo podanie przez von Flotowa funkcjonariuszowi Abwehry informacji, że został usunięty z SA, powinno obudzić czujność służb i potrzebę weryfikacji tej okoliczności. Dobranie przez kontrwywiad do współpracy w tajnej misji osoby poszukiwanej listem gończym, było wielkim nieporozumieniem.

Analiza sprawy Xeni Heuer pozwala wysnuć wniosek, że w związku z aresztowaniem Sosnowskiego i likwidacją placówki „In-3" prowadzono czynności również poza kręgiem osób będących wówczas lub wcześniej współpracownikami polskiego wywiadu. Potwierdza to wskazane w wyroku przeszukanie przeprowadzone u Xeni Heuer 28 lutego 1934 r., tj. nazajutrz po zatrzymaniu polskiego oficera.

Można wreszcie wyodrębnić nie jeden proces karny, a kilka postępowań odpowiadających wątkom w całej sprawie. W ramach wątku głównego – mamy proces przeciwko Jerzemu Sosnowskiemu i jego agentkom, w ramach wątku pobocznego zaś – proces przeciwko Xeni Heuer.

Jeśli chodzi o czynności wymierzone w Sosnowskiego przeprowadzane przez niemieckie organy ścigania, warto wskazać zdarzenie, do którego doszło w 1932 r. Po przekazaniu swojej łączniczce – Marii Runge – materiałów wywiadowczych Sosnowski wracał pieszo do domu. W oknach własnego apartamentu zauważył słaby odblask światła. Gdy wszedł do mieszkania, zobaczył dwóch mężczyzn opróżniających jego biurko przy świetle latarek. Najpierw wyjął rewolwer i obezwładnił złodziei, a następnie zadzwonił po policję. Na miejsce przybył komisarz z dwoma funkcjonariuszami. Dało się zauważyć, że komisarz starał się ukryć, iż zna jednego ze złodziei. Złodzieje ci – Kehlmann i Schulze – stanęli przed sądem i zostali skazani. W ramach odbycia kary mieli trafić do więzienia Berlin-Moabit. Tak się jednak nie stało. Jak się okazało, nigdy tam nie dotarli[52]. Ustalił to

[51] BArch, R 3017/14987, t. 2, *Urteil in der Strafsache gegen Xenia Heuer*, s. 5. Trybunał szerzej nie badał okoliczności usunięcia von Flotowa z SA i NSDAP, nie to przecież było przedmiotem jego rozstrzygnięcia.

[52] H. Ćwięk, *Rotmistrz Sosnowski*..., s. 115; W. Kurpis, *Berlińska misja*..., s. 112–116.

na polecenie Sosnowskiego jego służący. Poszlaki wskazujące na rozpoznanie złodzieja przez komisarza policji oraz fakt niedotarcia przez skazanych do miejsca odbywania kary wskazują, że mogli oni działać na polecenie policji lub Abwehry. Być może byli nawet funkcjonariuszami jednej ze służb. Przemawia za tym jeszcze jedna okoliczność, dotychczas chyba niezauważona. W. Kurpis podaje[53], że polski oficer nie wątpił w wierność swojego służącego, który, jego zdaniem, o jego nieobecności w domu w danym momencie mógł się wygadać przez przypadek. Sosnowski spotykał się ze swoją kurierką pod pozorem kontaktów intymnych w różnych hotelach. Te spotkania trwały zazwyczaj do późnych godzin nocnych. Tylko zbieg okoliczności sprawił, że owego dnia wrócił wcześniej do domu i nakrył mężczyzn na gorącym uczynku. Można więc przypuszczać, że służący polskiego oficera był współpracownikiem niemieckich służb, policji lub kontrwywiadu, i że to on poinformował o romantycznym wyjściu swego pracodawcy. Za taką wersją wydarzeń przemawia również brak śladów włamania w mieszkaniu Sosnowskiego oraz brak strat materialnych poniesionych w wyniku nieudanej kradzieży. Wydaje się wielce prawdopodobne, że rzekomi „złodzieje" weszli do apartamentu drzwiami, a otworzyli je kluczami otrzymanymi od służącego Sosnowskiego.

Ostatnią z kobiet Sosnowskiego była wspominana już Lea Kruse, znana także jako Lea Niako i Rita Pasci[54]. Sosnowski poznał ją w Budapeszcie, dokąd udał się na spotkanie z oficerem Oddziału II, któremu zdał relację z działalności Abwehry przeciwko sobie. Kruse była tancerką estradową, marzyła o występach w filmach. Sosnowski ściągnął ją do Berlina, zachęcając swoimi znajomościami i obiecując angaż w jednej z wytwórni filmowych. Zorganizował dla niej kilka przyjęć, jednak oczekiwana propozycja występu w filmie nie nadchodziła. Zamiast tego Sosnowski postanowił włączyć ją do swojej siatki szpiegowskiej. Znając metody działania Abwehry, przygotował ją na wypadek kontaktu z niemieckim kontrwywiadem. Kruse podjęła współpracę z Abwehrą, o czym później poinformowała Sosnowskiego. Ten jednak nie zwrócił na to należytej uwagi. Spodziewał się zapewne, że Kruse okaże się dla Niemców podobnym kontaktem, jak jego poprzednie kobiety. Nie przewidział jednak zmiany jej nastawienia. Z czasem zadania wywiadowcze i podejmowane ryzyko zaczęły ją przerażać. Opierając się na uzyskanych od niej informacjach, podjęto decyzję o zatrzymaniu Sosnowskiego i członków jego siatki[55].

[53] Tamże, s. 114–115. Na odmienny pogląd Sosnowskiego wskazuje fragment aktu oskarżenia, według którego ostrzegał on swoją współpracowniczkę Leę Kruse o swoim służącym Spieglu. BArch, R 3017/14987, t. 2, *Anklageschrift in der Strafsache gegen von Sosnowski und Genossen*, s. 110. Akt oskarżenia został podzielony na dwie części: w pierwszym tomie znajdują się strony od 1 do 85, natomiast pozostałe są przechowywane w tomie drugim.

[54] W. Kurpis, *Berlińska misja…*, s. 123.

[55] Tamże, s. 122–132; H. Ćwięk, *Rotmistrz Sosnowski...*, s. 119 i 121; H. Ćwięk i M. Zgórniak podają, że Kruse zdradziła Sosnowskiego z zazdrości, miała bowiem znaleźć w jego mieszkaniu materiały, z których wynikało, że obiecał on małżeństwo Benicie von Falkenhayn. Wydaje się to wątpliwe. Po pierwsze należy rozważyć, jakie to materiały mogła znaleźć Kruse. Nawet jeśli swego czasu Sosnowski złożył taką obietnicę, to czy sensowne byłoby sporządzanie przez niego notatki na ten temat, którą mogłaby znaleźć Kruse? Czy sporządziłby projekt umowy majątkowej między nim a Benitą? Po drugie, nawet jeśli Kruse znalazła dowód tego rodzaju obietnicy, to czy mogła traktować ją jako aktualną? Trzeba bowiem zważyć, że wtedy stosunki między Jerzym a Benitą były inne niż wcześniej. Benita w październiku 1932 r. zawarła nowy związek małżeński z inżynierem von Bergiem, w którym była szczęśliwa. Czy Kruse mogła być zazdrosna o nieaktualną obietnicę? Wypada również założyć, że w towarzystwie nie było tajemnicą, iż dawniej Sosnowski miał zażyłe kontakty z Benitą. Tym trudniej sądzić, aby mogło to wywoływać zazdrość.

Jakub Dej

Przeciwdziałanie finansowaniu terroryzmu w świetle polskiego prawa krajowego[1]

Przestępstwo o charakterze terrorystycznym i przestępstwa pochodne w kodeksie karnym

Mimo podwyższonego poziomu zagrożenia w państwach zachodnich oraz przynależności Polski do koalicji antyterrorystycznej, poziom zagrożenia zamachem terrorystycznym w naszym kraju od lat[2] utrzymuje się na niskim poziomie[3]. Śledztwa dotyczące przestępstw o charakterze terrorystycznym (tab. 1) prowadzone przez Agencję Bezpieczeństwa Wewnętrznego wskazują jednak, że w Polsce występują incydenty terrorystyczne. Znane są przypadki: działania na terenie RP komórek wsparcia logistycznego organizacji terrorystycznych, aktywności propagującej, wychwalającej lub ułatwiającej działalność terrorystyczną, udziału Polaków w działalności terrorystycznej prowadzonej poza granicami naszego państwa (ang. *foreign fighters*), a także podejrzanych transakcji, które mogą mieć związek z finansowaniem terroryzmu.

Tab. 1. Liczba śledztw związanych z przestępstwami o charakterze terrorystycznym prowadzonych przez ABW.

Rok	Liczba śledztw prowadzonych w zw. z art. 115 § 20
2009	9
2010	5
2011	5
2012	3
2013	7
2014	2

Źródło: Opracowanie własne na podstawie raportów z działalności ABW.

Agencja Bezpieczeństwa Wewnętrznego wskazuje na istnienie ryzyka zamachu terrorystycznego w związku z działalnością tzw. samotnych wilków (ang. *lone wolves*) oraz możliwością wykorzystania Polski jako celu zastępczego. Dlatego podjęcie stosownych środków zapobiegawczych, w tym wprowadzenie do systemu prawnego odpo-

[1] Fragment rozdziału 1 pracy licencjackiej pt. *Przeciwdziałanie finansowaniu terroryzmu w świetle obowiązującego prawa*, która zajęła III miejsce w konkursie szefa ABW na najlepszą pracę magisterską/licencjacką z dziedziny bezpieczeństwa wewnętrznego (V edycja). Redakcja dokonała niezbędnych poprawek oraz zmiany numeracji przypisów (przyp. red.).

[2] Wyjątek stanowi 2012 r., w którym *Zarządzeniem nr 56 Prezesa Rady Ministrów z dnia 27 czerwca 2012 r. w sprawie wprowadzenia stopnia alarmowego* podniesiono stopień alarmowy do poziomu ALFA w związku z organizacją Mistrzostw Europy w Piłce Nożnej EURO 2012 oraz wzmożonym ruchem imigrantów wywołanym tzw. arabską wiosną.

[3] *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r.*, [online], http://bs.net.pl/sites/default/files/media/rozne/raport_2015_int.pdf [dostęp: 8 VIII 2016].

wiednich regulacji umożliwiających zwalczanie terroryzmu, jest bardzo ważne. Ponadto Polska jako sygnatariusz wszystkich umów międzynarodowych omawianych w rozdziale II[4] oraz jako członek Unii Europejskiej jest zobowiązana do dostosowania przepisów prawa krajowego do prawa międzynarodowego oraz wspólnotowego.

W okresie międzywojennym w polskim prawie karnym nie występowała definicja normatywna przestępstwa terrorystycznego. Działalność przestępcza charakterystyczna dla terroryzmu była kwalifikowana jako czyny kryminalne. W 1935 r. R. Lemkin zaproponował wprowadzenie do prawa karnego przestępstw terroryzmu wewnętrznego i terroryzmu międzynarodowego, w których strona podmiotowa przestępstwa miała znaczenie decydujące o charakterze przestępstwa (w celu wywołania powszechnego niepokoju lub przestraszenia albo w celu wywołania powszechnego niepokoju lub zakłócenia stosunków międzynarodowych). Po II wojnie światowej mianem aktów terrorystycznych określano każdą działalność opozycyjną, a przede wszystkim działalność Armii Krajowej i innych organizacji niepodległościowych. Według Krzysztofa Wiaka kodeks karny z 19 kwietnia 1969 r.[5] typizował w art. 126 przestępstwo, które było uznawane przez ówczesne środowisko naukowe za „zamach terrorystyczny", a jego zastosowanie miało na celu rozbijanie środowisk opozycyjnych wobec ówczesnego systemu politycznego i władzy politycznej. Kolejne propozycje regulacji koncentrowały się na stronie podmiotowej przestępstwa (*wywołanie stanu przestraszenia*, *poważnego zakłócenia życia społecznego* itp.), motywując to faktem, że owa przestępczość może godzić w różne dobra chronione prawem[6]. Wskazano również na potrzebę usankcjonowania *przedpola aktu terrorystycznego*, przez które rozumiano udział w związku terrorystycznym, kierowanie związkiem terrorystycznym oraz przekazywanie środków finansowych na realizację celów owych organizacji. Nowelizacja kodeksu karnego z 6 czerwca 1997 r.[7] uwzględniła zobowiązania wynikające z przyjętych przez RP umów międzynarodowych wypracowanych w ramach ONZ. Kryminalizacji poddano m.in. przejęcie kontroli nad statkiem powietrznym lub wodnym, wzięcie zakładnika oraz umieszczanie niebezpiecznych urządzeń lub substancji na statku wodnym lub powietrznym. Wraz z nowelizacją kodeksu karnego z 16 kwietnia 2004 r.[8], wynikającą z potrzeby dostosowania prawa polskiego do unijnego, przyjęto przepisy bezpośrednio regulujące terroryzm, wprowadzając do słowniczka wyrażeń ustawowych legalną definicję przestępstwa o charakterze terrorystycznym (art. 115 § 20 kk). Zmiany miały na celu implementację standardów wynikających z przyjętej *Decyzji ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu*[9]. Zgodnie z treścią art. 115 § 20 kk:

> Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

[4] Polska jest sygnatariuszem *Międzynarodowej konwencji o zwalczaniu finansowania terroryzmu, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r.* (Dz.U. z 2004 r. Nr 263 poz. 2620), *Europejskiej konwencji o zwalczaniu terroryzmu, sporządzonej w Strasburgu dnia 27 stycznia 1977 r.* (Dz.U. z 1996 r. Nr 117 poz. 557), *Konwencji Rady Europy o zapobieganiu terroryzmowi, sporządzonej w Warszawie dnia 16 maja 2005 r.* (Dz.U. z 2008 r. Nr 161 poz. 998) oraz *Konwencji Rady Europy o praniu, ujawnianiu, zajmowaniu, i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzonej w Warszawie dnia 16 maja 2005 r.* (Dz.U. z 2008 r. Nr 165 poz. 1028).

[5] *Ustawa z dnia 19 kwietnia 1969 r. – Kodeks karny* (Dz.U. Nr 13 poz. 94).

[6] K. Wiak, *Prawnokarne środki przeciwdziałania terroryzmowi,* Lublin 2009, s. 214–226.

[7] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137).

[8] *Ustawa z dnia 16 kwietnia 2004 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* (Dz.U. Nr 93 poz. 889).

[9] Dz.Urz. UE L. Nr 164 z 22 VI 2002 r., s. 3.

1) poważnego zastraszenia wielu osób;

2) zmuszenia organu władzy publicznej RP lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności;

3) wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu.

Ta definicja składa się z dwóch części – obiektywnej i subiektywnej[10]. Pierwsza z nich ma charakter formalny i dotyczy ustawowego zagrożenia karą, która grozi za popełnienie przestępstwa o charakterze terrorystycznym (z górną granicą co najmniej pięciu lat). Definicję odniesiono do czynów objętych kryminalizacją w kodeksie karnym, nie tworząc przy tym nowego *sui generis* czynu zabronionego. Powyższy wykaz jest szerszy i ogólniejszy niż proponowany przez Radę Unii Europejskiej, która w decyzji ramowej dotyczącej zwalczania terroryzmu określiła dziewięć kategorii przestępstw[11]. Wydaje się, że jest to słuszne rozwiązanie, zważywszy na ciągłe ewoluowanie i elastyczność modus operandi terrorystów. Ponadto decyzja ramowa Rady UE określiła tylko minimalne standardy regulacji tej kwestii, zostawiając państwom członkowskim swobodę w implementacji decyzji. Druga część definicji przestępstwa o charakterze terrorystycznym ma wymiar materialny i dotyczy strony podmiotowej przestępstwa. Sprawca przestępstwa musi działać z bezpośrednim zamiarem osiągnięcia jednego z wymienionych celów, co oznacza, że sprawcą tego czynu może być tylko osoba działająca umyślnie. Dość wiernie odwzorowano treść decyzji ramowej[12] określającą subiektywne znamiona przestępstwa, a zmiany niektórych zwrotów wynikały z potrzeby dostosowania wyrażeń do polskiego prawa[13]. Aby czyn zabroniony został uznany za przestępstwo o charakterze terrorystycznym, obie przesłanki (obiektywna i subiektywna) muszą zostać spełnione łącznie.

Wraz z *Ustawą z dnia 25 czerwca 2009 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw*[14] wprowadzono do kodeksu karnego typizację czynu zabronionego – finansowania przestępstwa o charakterze terrorystycznym (art. 165a). Zgodnie z jego treścią (…) *kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w celu sfinansowania przestępstwa o charakterze terrorystycznym, podlega karze pozbawienia wolności od lat 2 do 12*[15]. Przyczyną wprowadzenia tego przepisu była potrzeba realizacji zobowiązań wynikających z przyjętej przez Polskę międzynarodowej konwencji ONZ o zwalczaniu finansowania terroryzmu[16], nałożenie w rezolucji Rady Bezpieczeństwa ONZ obowiązku penalizacji finansowania terroryzmu[17], a także obowiązek wdrożenia dyrektywy w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania

[10] *Kodeks karny. Komentarz*, R.A. Stefański (red.), Warszawa 2015, s. 709.

[11] K. Wiak, *Prawnokarne środki*…, s. 230–232.

[12] *Decyzja ramowa Rady 2002/475/WSiSW*…

[13] K. Wiak, *Prawnokarne środki*…, s. 242–244.

[14] Dz.U. Nr 166 poz. 1317.

[15] Art. 165a *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny* ...

[16] *Międzynarodowa konwencja o zwalczaniu finansowania terroryzmu*....

[17] *Rezolucja Rady Bezpieczeństwa ONZ 1368 (2001) z 12 września 2001 r.* (S/RES/1368) oraz *Rezolucja Rady Bezpieczeństwa ONZ 1373 (2001) z 28 września 2001 r.* (S/RES/1373).

terroryzmu[18] przyjętej przez Radę UE i Parlament Europejski. Umiejscowienie przepisu w rozdziale XX kodeksu karnego – *Przestępstwa przeciwko bezpieczeństwu powszechnemu* – wskazuje na przedmiot przestępstwa. Jego sprawcą może być ten, kto swoim umyślnym postępowaniem wypełni znamiona czynu zabronionego i może ponieść odpowiedzialność za swoje czyny w rozumieniu prawa. Czyn zabroniony musi być popełniony z zamiarem bezpośrednim zabarwionym (celem musi być sfinansowanie przestępstwa o charakterze terrorystycznym). Czyny sprawcze, tj. gromadzenie, przekazywanie i oferowanie, należy rozumieć zgodnie z wykładnią gramatyczną[19]. Przedmioty czynności sprawczej, tj. środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome bądź nieruchomości, powinny być rozumiane zgodnie z definicjami przyjętymi w ustawach sektorowych.

W podsumowaniu powyższych rozważań na temat regulacji karnoprawnych problematyki terroryzmu i jego finansowania warto pochylić się nad raportem ekspertów MONEYVAL, stworzonym w ramach mechanizmu wzajemnej ewaluacji. Raport dotyczył wdrażania rekomendacji FATF[20] i stanu systemów AML i CFT[21] w Polsce[22]. W dokumencie wskazano m.in. na zbyt wąskie ujęcie definicyjne przestępstwa o charakterze terrorystycznym, co ma uniemożliwiać zastosowanie art. 165a kk do niektórych spraw związanych z przestępstwami konwencyjnymi[23] zawartymi w dokumentach stanowiących załącznik do *Międzynarodowej Konwencji o Zwalczaniu Finansowania Terroryzmu przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r.*[24] Oceniający zaproponowali wprowadzenie kryminalizacji przekazywania funduszy organizacjom terrorystycznym (…) *w jakimkolwiek celu*. Wskazali również na potrzebę kryminalizacji czynu (art. 165a kk) – z zamiarem ewentualnym, a nie tylko bezpośrednim zabarwionym.

Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu

Jak wynika z raportów Generalnego Inspektora Informacji Finansowej (dalej: GIIF), w Polsce, mimo niskiego poziomu zagrożenia zamachem terrorystycznym, występują incydenty związane z finansowaniem terroryzmu (tab. 2). Na podstawie zestawienia liczby powiadomień przekazanych przez GIIF do ABW oraz postępowań prowadzonych przez GIIF w związku z podejrzeniem finansowania terroryzmu nie można wskazać na jednoznaczną tendencję wzrostową lub malejącą występowania omawianego zjawiska w Polsce, ale ogólnie stwierdzić jego występowanie.

[18] *Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu* (Dz.Urz. UE L Nr 309 z 25 XI 2005 r., s. 15).

[19] K. Wiak, *Prawnokarne środki…*, s. 280–285.

[20] Financial Action Task Force, Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy.

[21] AML (z ang. Anti-Money Laundering) – zespół procedur i przepisów prawa stworzony na potrzeby walki z procederem prania brudnych pieniędzy; CFT (z ang. Combating the Financing of Terrorism) – zespół procedur i przepisów prawa stworzony na potrzeby walki z procederem finansowania terroryzmu.

[22] Zob. szerzej: *Report on Fourth Assessment Visit – Poland* [online], MONEYVAL, 2013, http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/PL4-MERMONEYVAL(2013)2_en.pdf [dostęp: 8 VIII 2016].

[23] Eksperci MONEYVAL jako przykład wskazali czyn polegający na sfinansowaniu kradzieży materiałów nuklearnych. Ten czyn, zgodnie z art. 2 pkt 5 lit. c, jest uznany za przestępstwo konwencyjne *Międzynarodowej konwencji w sprawie zwalczania aktów terroryzmu jądrowego, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 13 kwietnia 2005 r.* (Dz.U. z 2010 r. Nr 112 poz. 740), która stanowi część załącznika do *Międzynarodowej konwencji o zwalczaniu finansowania terroryzmu*…

[24] *Report on Fourth Assessment Visit – Poland…*, s. 60.

Tab. 2. Liczba spraw prowadzonych przez GIIF w związku z podejrzeniem finansowania terroryzmu.

Rok	Liczba powiadomień przekazanych przez GIIF do ABW w związku z podejrzeniem finansowania terroryzmu	Liczba postępowań prowadzonych przez GIIF w związku z podejrzeniem finansowania terroryzmu
2006	3	8
2007	14	7
2008	15	8
2009	21	11
2010	30	19
2011	19	15
2012	17	12
2013	9	7
2014	26	20
Łącznie	154	107

Źródło: Opracowanie własne na podstawie sprawozdań GIIF z realizacji *Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (tekst jednolity: Dz.U. z 2016 r. poz. 299) w latach 2006–2014.

M. Kędzierski wskazuje, że nie można uznać tego wskaźnika za wystarczający do określenia skali zagrożenia terroryzmem w Polsce, zważywszy na wąskie pole działalności GIIF, ograniczone do formalnoprawnego obiegu finansowo-gospodarczego[25]. Zgodnie z informacją Biura Prokuratury Generalnej[26], w latach 2009–2013 nie wszczęto żadnych spraw z art. 165a kk, co stoi w sprzeczności z wnioskami płynącymi z analizy statystyk GIIF. Oszacowanie skali zjawiska jest o tyle kłopotliwe, że trudno ustalić, kiedy ma się do czynienia z finansowaniem terroryzmu w Polsce (np. przetransferowane do Polski środki finansowe pochodzące z Bośni i Hercegowiny, które zostały przesłane przez Polaka przekazem pieniężnym do Niemiec, skąd trafiły do Syrii od obywatela Turcji posiadającego wizę długoterminową wydaną przez Czechy, umożliwiającą pobyt i podejmowanie pracy na terenie całej Unii Europejskiej). Mimo trudności z określeniem skali występowania tego procederu w Polsce, założenie, które wskazuje na słuszność podejmowania przez państwo działań wyprzedzających oraz zobowiązania międzynarodowe Polski nie pozostawiają pola do dyskusji nad potrzebą pełnego uregulowania kwestii przeciwdziałania finansowaniu terroryzmu.

Najważniejszym dokumentem w polskim systemie prawnym określającym zwalczanie finansowania terroryzmu jest *Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[27]. Zawiera ona rekomen-

[25] M.A. Kędzierski, *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce – autoreferat*, [online], http://depotuw.ceon.pl/bitstream/handle/item/951/AUTOPREZENTACJA.docx?sequence=4 [dostęp: 26 V 2015], s. 5.

[26] Tamże, s. 8.

[27] Dz.U. z 2010 r. Nr 46 poz. 276, ze zm.

dacje FATF oraz rozwiązania wypracowane na poziomie globalnym (dokumenty wypracowane na forum ONZ) oraz regionalnym (dokumenty wypracowane na forum UE i RE), w których tworzeniu Polska uczestniczyła lub została do ich wprowadzenia zobowiązana. Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu była nowelizacją ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł, która, jak sama nazwa wskazuje, ograniczała się do problematyki prania pieniędzy oraz nielegalnych źródeł pochodzenia funduszy. Przedmiotem znowelizowanej ustawy są zasady i tryb przeciwdziałania procederowi prania brudnych pieniędzy oraz finansowania terroryzmu. Określono w niej podmioty będące częścią systemów AML i CFT oraz szczególne środki stosowane do zwalczania powyższych przestępstw. Ustawa zostanie omówiona tylko w części związanej ze zwalczaniem finansowania terroryzmu oraz w obszarach najistotniejszych, zważywszy na zakres przedmiotowy i specyfikę tego artykułu. Warto jednak nadmienić, że rozwiązania prawne dotyczące zwalczania finansowania terroryzmu i prania brudnych pieniędzy są w większości takie same.

W przepisach ogólnych ustawy wymieniono wszystkie instytucje obowiązane[28] do stosowania jej zapisów oraz jednostki współpracujące[29], a także wytłumaczono wyrażenia istotne z punktu widzenia ustawy i nadano im definicje legalne. Finansowanie terroryzmu zostało uznane za czyn określony w art. 165a kk, co jest rozwiązaniem słusznym[30]. Wprowadzenie do ustawy pojęcia b e n e f i c j e n t r z e c z y w i s t y[31] jest istotne z punktu widzenia podniesienia skuteczności ścigania osób, które próbują ukrywać swoją działalność przestępczą, wykorzystując do tego tzw. słupy[32] lub podmioty gospodarcze[33].

Instytucje obowiązane muszą rejestrować każdą przeprowadzoną transakcję, jeśli:

- jej wartość przekracza 15 000 euro,
- składa się ona z więcej niż jednej operacji finansowej, w celu uniknięcia obowiązku rejestracji,
- dotyczy ona kasyn – zakupu lub sprzedaży żetonów o wartości wyższej lub równej 1000 euro,

[28] Zgodnie z art. 2 wyżej wymienionej ustawy są to: instytucje i oddziały instytucji finansowych, kredytowych, pieniądza elektronicznego i płatnicze; banki i oddziały banków; NBP; firmy inwestycyjne i banki powiernicze; domy maklerskie, spółki handlowe, Krajowy Depozyt Papierów Wartościowych S.A.; podmioty prowadzące działalność w zakresie gier losowych, zakładów wzajemnych i gier na automatach; zakłady ubezpieczeń; fundusze i towarzystwa inwestycyjne; spółdzielcze kasy oszczędnościowo-kredytowe; operatorzy pocztowi; notariusze w ograniczonym zakresie; podmioty prowadzące działalność w zakresie usług prowadzenia ksiąg rachunkowych, wymiany walut; przedsiębiorcy prowadzący domy aukcyjne, antykwariaty, działalność factoringową, działalność w zakresie obrotu metalami lub kamieniami szlachetnymi i półszlachetnymi, sprzedaż komisową lub pośrednictwo w obrocie nieruchomościami; stowarzyszenia posiadające osobowość prawną, przedsiębiorcy przyjmujący płatności za towary w gotówce równej lub przekraczające 15 000 euro; instytucje i oddziały płatnicze.

[29] Organy administracji rządowej i samorządowej, inne państwowe jednostki organizacyjne, NBP, KNF i NIK.

[30] W akcie prawnym poprzedzającym obecną ustawę było zawarte odrębne pojęcie a k t t e r r o r y s t y c z n y, które nie było skorelowane z obowiązującymi przepisami prawa karnego.

[31] Jest to osoba fizyczna (lub osoby fizyczne), która ma wpływ na osobę prawną lub sprawuje nad nią kontrolę, ma powyżej 25% głosów w zgromadzeniu wspólników i sprawuje kontrolę nad co najmniej 25% majątku osoby prawnej (art. 2 ust. 1a).

[32] S ł u p e m określa się osobę trzecią, która dokonuje wszystkich czynności formalnoprawnych, nie będąc przy tym rzeczywistym beneficjentem korzyści wynikających z dokonanych przez nią czynności.

[33] M. Hara, R. Kierzynka P. Kołodziejski, *Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Komentarz*, Warszawa 2014, s. 41.

- wskazuje ona na prawdopodobieństwo powiązania transakcji z praniem pieniędzy lub finansowaniem terroryzmu,
- jest ona dokonywana przy pomocy adwokata, radcy prawnego bądź zagranicznego prawnika i dotyczy obrotu nieruchomościami i przedsiębiorstwami, zarządzania rachunkami, inwestowania w kapitał zakładowy i akcyjny oraz zarządzania spółkami lub przedsiębiorstwami (art. 8 ustawy).

Rejestrowanie transakcji jest niezmiernie ważne dla prowadzenia czynności analitycznych, a w sytuacji wytypowania podejrzanej transakcji – dla dalszych czynności procesowych. Obowiązek rejestrowania powiązanych operacji finansowych będących w rzeczywistości jedną transakcją wynika z potrzeby przeciwdziałania wyrafinowanym metodom (rozdrabnianie transakcji gotówkowych, ang. *structuring*), których celem jest obejście obowiązku rejestracji[34]. Rekomendacje FATF zalecają rejestrację transakcji powyżej określonej kwoty. Ustawodawca rozszerzył to zalecenie o obowiązek rejestrowania również tych transakcji, które nie przekraczają wskazanej kwoty, ale szczególne okoliczności transakcji uzasadniają jej rejestrację[35]. Takie podejście zwiększa skuteczność przeciwdziałania finansowaniu terroryzmu.

Obowiązki nałożone na podmioty prowadzące kasyna gry wyglądają nieco inaczej, ze względu na specyfikę tego typu działalności. Przyjęcie mniejszej kwoty progowej w wysokości 1000 euro (a nie 15 000 euro) wynika z tego, że przy wykorzystywaniu kasyn gry do prania pieniędzy obracano o wiele niższymi sumami pieniędzy[36]. W tym przypadku pozostanie przy kwocie 15 000 euro spowodowałoby, że mechanizm zwalczania omawianego procederu byłby nieskuteczny. Ustawodawca rozszerzył przepisy unijne[37] i zobowiązał podmioty prowadzące kasyna gry do rejestrowania transakcji, a nie tylko do ustalania tożsamości klientów kasyn, jak wymaga tego dyrektywa.

Instytucje obowiązane na bieżąco analizują transakcje swoich klientów (art. 8a ustawy). Weryfikacja danych dotyczących transakcji klienta ma na celu wykrycie operacji podprogowych (powiązanych) oraz operacji podejrzanych[38]. Bieżący monitoring jest prowadzony zgodnie z wypracowanymi procedurami, algorytmami i modelami w ramach danej instytucji, tworzonymi na podstawie środków bezpieczeństwa finansowego zastosowanych wobec klienta.

Środki bezpieczeństwa finansowego polegają na:

- identyfikacji i weryfikacji tożsamości klienta,
- identyfikacji beneficjenta rzeczywistego oraz ustaleniu struktur własności i zależności klienta,
- uzyskiwaniu informacji o celach operacji finansowych prowadzonych przez klienta oraz jego stosunkach gospodarczych z innymi uczestnikami obrotu gospodarczego, a także na bieżącym ich monitorowaniu i aktualizowaniu (art. 8b ust. 3 ustawy).

---

[34] Symptomami rozdrabniania transakcji gotówkowych mogą być m.in. częste dokonywanie operacji finansowych z tego samego rachunku tego samego dnia w różnych oddziałach bankowych (kasjerów), dokonywanie w krótkim czasie przelewów na jeden rachunek z kilku rachunków, obecność osób trzecich przy dokonywaniu wpłat lub wypłat przez tzw. smerfów (słupy), zob. M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu…*, s. 96–98.

[35] Tamże, s. 92.

[36] Tamże, s. 98.

[37] *Dyrektywa 2001/97/WE Parlamentu Europejskiego i Rady z 4 grudnia 2001 r. zmieniająca dyrektywę Rady 91/308/EWG w sprawie uniemożliwienia korzystania z systemu finansowego w celu prania pieniędzy* [online], http://orka.sejm.gov.pl/Drektywy.nsf/all/32001L0097/$File/32001L0097.pdf [dostęp: 4 V 2015].

[38] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu…*, s. 114.

Stosowanie wskazanych środków jest oparte na zasadzie „poznaj swojego klienta" (ang. *Know Your Customer Policy*) i są zgodne z wcześniej omawianą tzw. III dyrektywą[39], która obliguje instytucje zobowiązane do stosowania (…) *środków należytej staranności wobec klienta* (art. 8 dyrektywy). Identyfikacja klienta oraz beneficjenta rzeczywistego polega na zgromadzeniu danych i ich zweryfikowaniu na podstawie dokumentów (np. dowodu osobistego) i informacji dostępnych publicznie (np. KRS, REGON, NIP, PESEL). Wymagane informacje zostały określone w katalogach: osoby fizyczne i ich przedstawiciele (art. 9 ust. 1 pkt 1 ustawy), osoby prawne (art. 9 ust. 1 pkt 2 ustawy) oraz jednostki organizacyjne niemające osobowości prawnej (art. 9 ust. 1 pkt 3 ustawy). W przypadku podmiotu prowadzącego kasyna lub salony gry identyfikację i weryfikację tożsamości klienta przeprowadza się przy wejściu klienta do kasyna lub salonu (art. 9c ustawy).

Zakres stosowania środków bezpieczeństwa finansowego zależy od poziomu ryzyka finansowania terroryzmu, który jest określany na podstawie oceny ryzyka dokonanej w wyniku analizy klienta (art. 8b ust. 1 ustawy). W zależności od oceny instytucje obowiązane mogą stosować uproszczone lub wzmożone środki staranności wobec klienta[40], co umożliwia efektywniejsze zarządzanie zasobami ludzkimi i technicznymi przez angażowanie ich na tych obszarach, które wskazują na większe ryzyko wystąpienia finansowania terroryzmu. W przypadku braku możliwości zastosowania środków bezpieczeństwa finansowego wobec klienta podmiot zobowiązany nie przeprowadza transakcji, nie zawiera umowy z klientem lub ją unieważnia oraz informuje o zdarzeniu GIIF (art. 8b ust. 5 ustawy). Uproszczone środki bezpieczeństwa wobec klienta (odstąpienie od niektórych środków bezpieczeństwa finansowego – art. 8b ust. 3 pkt 1–3 ustawy) mogą mieć zastosowanie wobec tych klientów, którzy charakteryzują się wysoką wiarygodnością i niską oceną ryzyka (np. organy administracji publicznej, instytucje finansowe mające siedzibę na terenie państwa członkowskiego UE) oraz w stosunku do przypadków, które charakteryzują się brakiem ryzyka wykorzystania ich do finansowania terroryzmu lub jego niskim poziomem (np. umowy ubezpieczeniowe na życie o niskiej składce – art. 9d ust. 1–2 ustawy). Wzmożone środki bezpieczeństwa mogą mieć zastosowanie wobec: klientów, których identyfikacja przebiegała bez bezpośredniego kontaktu w zakresie stosunków transgranicznych z instytucjami będącymi korespondentami z państw trzecich oraz wobec osób zajmujących eksponowane stanowisko polityczne[41] (art. 9e ust. 2–4 ustawy). Instytucje obowiązane podejmują w takim przypadku czynności polegające na: uzyskaniu uwiarygadniających lub uzupełniających informacji z dodatkowych rzetelnych i wiarygodnych źródeł, pogłębionej analizie ryzyka, uzyskaniu zgody właściwych organów instytucji obowiązanej do nawiązania współpracy lub zawarcia umowy (w przypadku instytucji korespondujących i osób zajmujących eksponowane stanowisko) oraz ograniczeniu usługi realizacji transakcji na odległość[42].

Instytucje obowiązane mają za zadanie sporządzić w formie pisemnej, a następnie wprowadzić w życie, wewnętrzną procedurę w zakresie przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (art. 10a). Dokument określa i uszczegóławia sposób wykonywania obowiązków nałożonych na instytucje obowiązane, wynikających

[39] *Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu...*

[40] Zob. art. 11 i 13 *Dyrektywy 2005/60/WE…*

[41] W rozumieniu art. 2 ust. 1f pkt a, b, c omawianej ustawy.

[42] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu…*, s. 163.

z ustawy. Owa procedura powinna zawierać m.in. metodologię dokonywania analizy i oceny ryzyka przez pracowników instytucji. Ocena ryzyka przeprowadzana w wyniku jego analizy jest elementem newralgicznym, ponieważ to od niej zależy zakres stosowania środków bezpieczeństwa finansowego, a co za tym idzie – skuteczność wykrywania finansowania terroryzmu i przeciwdziałania temu przestępstwu.

Analizę ryzyka tworzy się, przy uwzględnieniu czterech kryteriów: ekonomicznego, geograficznego, przedmiotowego i behawioralnego (art. 10a ust. 3 ustawy)[43]. Kryterium ekonomiczne polega na założeniu, że celem działalności gospodarczej jest zysk, i że każde działanie będące odstępstwem od tego założenia jest podejrzane. Kryterium geograficzne dotyczy transakcji, których nadawcą lub odbiorcą jest podmiot zarejestrowany w państwie lub regionie o wysokim poziomie przestępczości lub (i) będącym obszarem działalności organizacji terrorystycznych, konfliktów (np. Afganistan, Irak, Syria), lub w państwie o niskich standardach przeciwdziałania finansowaniu terroryzmu i praniu pieniędzy (raje podatkowe[44], państwa upadłe) oraz zwalczania tych zjawisk. Kryterium przedmiotowe polega na uznaniu za ryzykowne z punktu widzenia finansowania terroryzmu i prania pieniędzy niektórych obszarów działalności gospodarczej (np. obrót złomem, handel paliwami płynnymi, obrót metalami szlachetnymi). Kryterium behawioralne polega na ocenie nietypowego zachowania klienta (np. zdenerwowanie, brak wiedzy klienta w zakresie prowadzonej przez siebie działalności gospodarczej, próba zamaskowania twarzy, udział osób trzecich).

Aby wewnętrzne procedury związane ze zwalczaniem terroryzmu i przeciwdziałaniem temu zjawisku były odpowiednio wdrażane i realizowane, instytucja obowiązana musi zapewnić pracownikom odpowiedzialnym za realizację zadań wskazanych w omawianej ustawie (art. 10a ust. 4) odpowiedni poziom wyszkolenia. Ponadto, podmiot musi wskazać osobę odpowiedzialną za wykonanie obowiązków określonych w ustawie (art. 10b).

W Polsce organami właściwymi w sprawach zwalczania finansowania terroryzmu jest minister właściwy do spraw instytucji finansowych oraz Generalny Inspektor Informacji Finansowej (art. 3 ustawy). GIIF realizuje zwłaszcza zadania analityczne, tj. uzyskuje, gromadzi, przetwarza i dystrybuuje informacje o podejrzanych transakcjach oraz wykonuje zadania prewencyjne, czyli wstrzymuje transakcje, blokuje rachunki, szkoli pracowników instytucji obowiązanych oraz kontroluje i egzekwuje przestrzeganie przepisów omawianej ustawy (art. 4)[45]. GIIF uzyskuje informacje od instytucji obowiązanych oraz jednostek współpracujących w różnym zakresie. W myśl przepisów ustawy instytucje obowiązane zostały zobligowane do przekazywania do GIIF informacji o transakcjach określonych w art. 8 ust. 1 i 3[46] oraz do udostępniania ich na żądanie tej instytucji (art. 11 ust. 1 i art. 13a). W przypadku adwokatów, radców prawnych, prawników zagranicznych, biegłych rewidentów oraz doradców podatkowych istnieje klauzula wyłączająca ten obowiązek, gdy informacje zostały pozyskane w trakcie reprezentowania klienta na podstawie pełnomocnictw procesowych lub udzielania porady

[43] Tamże, s. 102–106, 194–195.

[44] Listy rajów podatkowych zawierają: *Rozporządzenie Ministra Finansów z dnia 23 kwietnia 2015 r. w sprawie określenia krajów i terytoriów stosujących szkodliwą konkurencję podatkową w zakresie podatku dochodowego od osób prawnych* (Dz.U. z 2015 r. poz. 600) oraz *Rozporządzenie Ministra Finansów z dnia 23 kwietnia 2015 r. w sprawie określenia krajów i terytoriów stosujących szkodliwą konkurencję podatkową w zakresie podatku dochodowego od osób fizycznych* (Dz.U. z 2015 r. poz. 599).

[45] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu…*, s. 65.

[46] Tj. transakcjach ponadprogowych, transakcjach powiązanych przekraczających próg, transakcjach podejrzanych.

prawnej w tej sprawie (art. 11 ust. 5). Prokuratura, ABW, CBA oraz jednostki podległe lub nadzorowane przez ministra właściwego do spraw wewnętrznych zostały zobowiązane do informowania o podejrzeniu popełnienia przestępstwa, przedstawieniu zarzutów oraz wszczęciu i zakończeniu postępowania w sprawie przestępstwa, o którym mowa w art. 165a kk (art. 14 ustawy). Organy kontroli skarbowej, podatkowe i celne zostały zobowiązane do informowania o wszystkich okolicznościach wskazujących na możliwość popełnienia przestępstwa, o którym mowa w art. 165a kk (art. 15a ust. 3 ustawy). Organy Straży Granicznej oraz organy celne zostały zobowiązane do przekazywania informacji w sprawie kontroli środków finansowych przewożonych przez granice Unii Europejskiej[47] oraz informacji związanych z przewożeniem wartości dewizowych lub krajowych środków płatniczych[48]. Ponadto na wniosek GIIF jednostki współpracujące, w zakresie swoich kompetencji, mają obowiązek przekazać informacje niezbędne (inne niż wymienione wcześniej) do realizacji zadań związanych ze zwalczaniem finansowania terroryzmu (art. 15a ustawy).

W przypadku uzasadnionego podejrzenia, że przeprowadzona (lub przeprowadzana) transakcja albo klient mogą mieć związek z popełnieniem przestępstwa finansowania terroryzmu, uruchamia się procedury wstrzymania transakcji[49] lub blokady rachunku[50] (rozdział 5 ustawy). Wstrzymanie transakcji dotyczy wskazanej operacji finansowej, a blokada rachunku ma zastosowanie do wszystkich środków zgromadzonych na rachunku. Oznacza to, że dla dysponenta rachunku blokada jest bardziej dolegliwym środkiem niż wstrzymanie transakcji, a więc ten drugi mechanizm powinien być stosowany tylko wtedy, gdy pierwszy jest niewystarczający[51]. Procedura wstrzymania transakcji lub blokady rachunku może zostać zainicjowana przez zawiadomienie GIIF przez instytucję obowiązaną lub w wyniku własnych działań analitycznych GIIF (art. 16 ust. 1 oraz art. 18a). W obu przypadkach instytucje muszą powziąć uzasadnione podejrzenie o możliwym związku transakcji lub dysponenta rachunku z przestępstwem z art. 165a kk. Instytucja obowiązana, która przesłała zawiadomienie do GIIF, wstrzymuje transakcje na nie dłużej niż 24 godziny (art. 16 ust 4). W ciągu 24 godzin od momentu wpłynięcia zawiadomienia od instytucji GIIF ma czas na podjęcie decyzji o wstrzymaniu transakcji lub blokadzie rachunku na okres nie dłuższy niż 72 godziny (art. 18). Wraz z podjęciem decyzji GIIF niezwłocznie przesyła do właściwej prokuratury zawiadomienie o podejrzeniu przestępstwa oraz całą posiadaną dokumentację na temat wstrzymanej transakcji lub zablokowanego rachunku. Prokurator może podjąć decyzję o wstrzymaniu transakcji lub blokadzie rachunku na okres nie dłuży niż trzy miesiące (art. 19). Jeśli w czasie oznaczonym w postanowieniu prokuratora nie zostanie wydane postanowienie o zabezpieczeniu majątkowym, blokada rachunku lub wstrzymanie transakcji zostają anulowane (art. 19 ust. 4).

[47] Zgodnie z rozporządzeniem wwożenie na terytorium UE lub wywożenie z terytorium UE kwot powyżej 10 000 euro podlega obowiązkowi złożenia deklaracji. Zob. *Rozporządzenie (WE) nr 1889/2005 Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie kontroli środków pieniężnych wwożonych do Wspólnoty lub wywożonych ze Wspólnoty* (Dz.Urz. UE L 309 z 25 XI 2005 r., s. 9).

[48] Obowiązki rezydentów i nierezydentów związane z wywozem za granicę i przywozem do kraju wartości dewizowych lub krajowych środków płatniczych reguluje rozdział 5 *Ustawy z dnia 27 lipca 2002 r. – Prawo dewizowe* (tekst jednolity: Dz.U. z 2012 r. poz. 826).

[49] Tj. czasowe ograniczenie dysponowania wartościami majątkowymi i korzystania z nich polegające na uniemożliwieniu przeprowadzenia określonej transakcji przez instytucję obowiązaną (art. 2 ust. 5 ustawy).

[50] Tj. czasowe ograniczenie dysponowania wszystkimi wartościami majątkowymi zgromadzonymi na rachunku i korzystania z nich, w tym również przez instytucję obowiązaną (art. 2 ust. 6 ustawy).

[51] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu…*, s. 225.

Blokowanie rachunku lub wstrzymanie transakcji przez GIIF, a później przez prokuratora, ma charakter nietrwały i przejściowy. Ten okres służy do przeprowadzenia wielu czynności procesowych. Prokurator, aby postanowić o wstrzymaniu transakcji lub blokadzie rachunku na czas oznaczony, musi najpierw wszcząć śledztwo, co wynika z kodeksu postępowania karnego. Wydanie postanowienia o zabezpieczeniu majątkowym wymaga również czasu, zważywszy na potrzebę uzasadnienia zastosowania środka prawnego na podstawie przesłanki przewidzianej w art. 295 § 4 kpk.

W rozdziale 5a ustawy określono zasady i procedurę zamrażania wartości majątkowych – mechanizmu ograniczającego przeciwko osobom, grupom i podmiotom. Jego wprowadzenia wymagały decyzja 2001/500/WSiSW[52] oraz dyrektywa 2005/60/WE[53], a także III Specjalna Rekomendacja FATF. Instytucja obowiązana dokonuje zamrożenia[54] wartości majątkowych (z wyłączeniem rzeczy ruchomych i nieruchomości) na podstawie prawa wspólnotowego oraz przepisów zawartych w omawianej ustawie (art. 20d ustawy). Wskazane podstawy prawne zwracają uwagę na specyficzny zbiór przesłanek, który sprowadza się do zamrażania wartości majątkowych na podstawie bezpośredniego stosowania wykazu osób, grup i podmiotów wymienionych w:

- rozporządzeniu ministra właściwego do spraw instytucji finansowych, w sprawie wykazu osób, grup i podmiotów, wobec których stosuje się powyższy mechanizm[55],
- rozporządzeniu Rady UE (WE) nr 2580/2001 z 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mającym na celu zwalczanie terroryzmu[56].

Instytucje obowiązane są zobligowane do stosowania wykazu osób, grup i podmiotów będącego załącznikiem do rozporządzenia wykonawczego do rozporządzenia Rady nr 2580/2001 bezpośrednio, tj. bez znaczenia, czy dana osoba, grupa lub podmiot zostały wpisane na „krajową listę". Taka interpretacja została wielokrotnie potwierdzona przez Trybunał Sprawiedliwości[57]. Trybunał wskazał ponadto, że państwa członkowskie nie powinny stosować środków, które mogłyby utrudnić stosowanie w tej sprawie prawa wspólnotowego.

Na koniec warto zwrócić uwagę na odpowiedzialność pieniężną i karną za nieprzestrzeganie przepisów omawianej ustawy. Instytucje obowiązane (z wyjątkiem NBP) w przypadku niedopełnienia obowiązku przewidzianego w przepisach ustawy

[52] *Decyzja ramowa Rady 2001/500/WSiSW z dnia 26 czerwca 2001 r. w sprawie prania brudnych pieniędzy oraz identyfikacji, wykrywania, zamrożenia, zajęcia i konfiskaty narzędzi oraz zysków pochodzących z przestępstwa* (Dz.U. L 182 z 5 VII 2001 r. poz. 1).

[53] *Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu…*

[54] Tj. zapobieganie przenoszeniu, zmianie i wykorzystaniu wartości majątkowych lub przeprowadzaniu transakcji w jakikolwiek sposób, który może spowodować zmianę ich wielkości, wartości, miejsca, własności, posiadania, charakteru, przeznaczenia lub jakąkolwiek inną zmianę umożliwiającą korzystanie z wartości majątkowych (art. 2 ust. 6 ustawy).

[55] Zgodnie z art. 20d, ust. 3 minister właściwy do spraw instytucji finansowych w porozumieniu z ministrem właściwym do spraw zagranicznych może określić omawiane rozporządzenie, ale nie musi. Obecnie nie istnieje krajowa lista osób, grup i podmiotów, wobec których podmioty zobowiązane powinny stosować mechanizm zamrażania wartości majątkowych.

[56] *Rozporządzenie Rady (WE) nr 2580/2001 z dnia 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu* (Dz.U. UE L 344 z 28 XII 2001 r. poz. 70) oraz *Rozporządzenie Wykonawcze Rady (UE) nr 790/2014 z dnia 22 lipca 2014 r. dotyczące wykonania art. 2 ust. 2 rozporządzenia (WE) nr 2580/2001 w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu oraz uchylenia rozporządzenia wykonawczego (UE) nr 125/2014* (Dz.U. UE L 217 z 23 VII 2014 r. poz. 1).

[57] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu…*, s. 242.

o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu podlegają karze pieniężnej (art. 34a i 34b). Karę, w drodze decyzji administracyjnej, nakłada Generalny Inspektor Informacji Finansowej, który sprawuje kontrolę nad instytucjami obowiązanymi (z wyłączeniem NBP) do przestrzegania przepisów dotyczących zwalczania finansowania terroryzmu (art. 34c)[58]. Kara pieniężna nie może być większa niż 75 000 zł, a w niektórych przypadkach nie większa niż 100 000 zł. Wprowadzenie sankcji finansowych dla instytucji obowiązanych nieprzestrzegających przepisów dotyczących zwalczania finansowania terroryzmu stanowi realizację obowiązku implementacji art. 39 ust. 1 i 2 dyrektywy 2005/60/WE[59], który zobowiązuje państwa członkowskie do stosowania środków sankcyjnych w stosunku do osób fizycznych i prawnych objętych regulacjami prawnymi dotyczącymi zwalczania finansowania terroryzmu. Podobnie jak stosowanie kar pieniężnych, przepisy karne (rozdział 8 ustawy) również mają na celu umożliwienie egzekwowania przepisów omawianej ustawy. Zgodnie z art. 116 kk stosuje się do nich przepisy ogólne kodeksu karnego. Czyny określone w tym rozdziale są uznane za występki (art. 7 kk) oraz podlegają ściganiu z urzędu. W ustawie poddano penalizacji: niedopełnienie obowiązków wskazanych w ustawie (art. 35 ust. 1), nielegalne ujawnianie lub wykorzystywanie informacji zgromadzonych na podstawie ustawy (art. 36 ust. 2) oraz utrudnianie realizacji zadań wynikających z ustawy przez GIIF lub inne organy odpowiedzialne za przeprowadzanie czynności kontrolnych w instytucjach obowiązanych (art. 36 i 37a). Jak wskazuje M. Hara, przepisy karne ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu są swoistą „pierwszą linią obrony" w rozumieniu prawnokarnym, której celem jest niedopuszczenie do sfinansowania przestępstwa o charakterze terrorystycznym (omawiany wcześniej art. 165a kk)[60].

Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu jest na bieżąco aktualizowana i dostosowywana do prawa wspólnotowego oraz innych zobowiązań międzynarodowych. Mechanizmy i rozwiązania prawne znajdujące się w ustawie są w znacznej części powieleniem standardów wypracowanych na poziomie międzynarodowym. W niektórych jednak przypadkach przepisy ustawy przewyższają wymogi Unii Europejskiej, co wydaje się pozytywnym symptomem wskazującym na świadomą i przemyślaną implementację prawa wspólnotowego (np. III dyrektywa nakłada obowiązek identyfikacji tożsamości klientów kasyn, a polskie przepisy nakładają na instytucję obowiązaną również rejestrację samej transakcji).

Konkluzje

Finansowanie terroryzmu nie pozostawało bezkarne przed wprowadzeniem oddzielnego przepisu typizującego to przestępstwo[61]. Ten czyn był uznawany za przygotowanie dokonania przestępstwa o charakterze terrorystycznym (art. 16 kk), pomocnictwo

[58] W 2014 r. GIIF wydał 40 decyzji administracyjnych o nałożeniu kary pieniężnej od 200 do 700 000 zł – łącznie na sumę 2 658 400 zł. Zob. szerzej: *Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2014 r.*, Ministerstwo Finansów, Warszawa 2015.

[59] Art. 39 ust. 1 i 2 *Dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu…*

[60] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu…*, s. 328.

[61] M.A. Kędzierski, *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Warszawa 2014, s. 113–114.

w dokonaniu przestępstwa o charakterze terrorystycznym (art. 18 § 3 kk) lub udział w zorganizowanej grupie albo związku przestępczym (art. 258). Takie rozwiązanie nadal jest uznawane za słuszne przez Komisję Kodyfikacji Prawa Karnego przy Ministrze Sprawiedliwości[62]. W opinii Komisji z 18 lutego 2014 r. dotyczącej realizacji aktualnych zaleceń Komitetu MONEYVAL wskazano, że finansowanie terroryzmu wyczerpuje znamiona czynu pomocnictwa lub udziału w grupie lub związku mającym na celu popełnienie przestępstwa, zakładaniu takiej grupy lub związku albo kierowaniu nimi, a więc nie ma potrzeby typizacji nowego czynu. Ten pogląd jest sprzeczny z prawem międzynarodowym, prawem wspólnotowym oraz standardami FATF, dlatego propozycja usunięcia typizacji finansowania terroryzmu jest mało realna.

Podczas analizy aktów prawa polskiego określających problematykę zwalczania finansowania terroryzmu, można dojść do wniosku, że zachodzi wysoka spójność między międzynarodowymi standardami i krajowymi regulacjami prawnymi. Wynika to zapewne z tego, że system przeciwdziałania finansowaniu terroryzmu w Polsce był budowany od początku na podstawie rozwiązań prawnych przewidzianych w prawie międzynarodowym, a więc nie pojawił się problem dostosowywania przepisów prawnomiędzynarodowych do systemu już istniejącego w Polsce. Duży wpływ na implementację przepisów prawa międzynarodowego ma również charakter wydanych decyzji, które są wiążące dla państwa polskiego, oraz duże zaangażowanie polskich instytucji w prace różnego rodzaju środowisk zajmujących się problematyką zwalczania terroryzmu[63]. Pomimo wysokiego poziomu spójności prawa polskiego z prawem międzynarodowym, istnieją braki wskazywane przez ekspertów MONEVYAL, a także sprzeczne poglądy ekspertów Komisji Kodyfikacji Prawa Karnego w sprawie implementacji niektórych rozwiązań prawnych.

[62] *Opinia Komisji Kodyfikacyjnej Prawa Karnego przy Ministrze Sprawiedliwości z dnia 18.02.2014 r. dotycząca realizacji aktualnych zaleceń Komitetu MONEYVAL w sprawie przeciwdziałania praniu brudnych pieniędzy i innych* [online], http://bip.ms.gov.pl/pl/dzialalnosc/komisje-kodyfikacyjne/komisja-kodyfikacyjna-prawa-karnego/opinie-komisji-kodyfikacyjnej-prawa-karnego/download,2663,1.html, s. 9 [dostęp: 28 V 2015].

[63] Na przykład współpraca w ramach UE: Stały Komitet ds. Współpracy Operacyjnej w Zakresie Bezpieczeństwa Wewnętrznego „COSI", Grupa Robocza ds. Terroryzmu „WPT", Grupa Robocza ds. Terroryzmu – Kwestie Międzynarodowe „COTER", Grupa Robocza ds. Zastosowania Szczególnych Środków w celu zwalczania Terroryzmu „CP 931"; Współpraca w ramach NATO: Program Obrony przed Terroryzmem „DAT"; Współpraca w ramach ONZ: Komitet Antyterrorystyczny „CTC"; Współpraca w ramach RE: Komitet Ekspertów ds. Oceny Systemów Zwalczania Procederu Prania Pieniędzy i Finansowania Terroryzmu „MONEYVAL"; Współpraca w ramach Klubu Berneńskiego: Grupa Antyterrorystyczna „CTG"; Współpraca w ramach OBWE: Finansowa Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy „FATF". Zob. szerzej: *Uchwała nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (M.P. z 2014 r. poz. 1218).

IV
DOKUMENTY I SPRAWOZDANIA

Zbigniew Małysz

Sprawozdanie z eksperckiego seminarium dyskusyjnego pt. „Jaka powinna być polska ustawa antyterrorystyczna?" zorganizowanego przez Centrum Badań nad Terroryzmem Collegium Civitas

Zagadnienia dotyczące bezpieczeństwa osobowego oraz instytucjonalnego są jednymi z najbardziej istotnych spraw we współczesnym świecie. Badania psychologiczne Abrahama Maslowa lokują bezpieczeństwo na drugim miejscu w hierarchii podstawowych potrzeb człowieka (zaraz po zaspokojeniu potrzeb fizjologicznych). Można zaryzykować twierdzenie, że bezpieczeństwo jest aktualnie jednym z trzech – oprócz pewności zatrudnienia (pracy) i ochrony zdrowia – obszarów szczególnej troski społecznej. Dlatego niezwykle istotne i ważne społecznie jest dokładne monitorowanie środowiska bezpieczeństwa państwa oraz jego potencjalnych zagrożeń.

Współcześnie na świecie dokonują się dość gwałtowne przemiany społeczno-polityczne oraz obyczajowe, które są wymuszone globalizacją handlu i wymianą informacji. Na te procesy nakładają się przetasowania geopolityczne sugerujące, że zbliża się koniec pokojowego rozwiązywania konfliktów, co wykazują wnioski z historyczno-socjologicznych badań porównawczych oraz klasyczny w psychologii eksperyment Calhouna. Coraz większym problemem jest ekspansja różnorodnie motywowanego terroryzmu jako działania zapełniającego powstającą próżnię społeczną wynikającą z braku sensu egzystencji i poczucia przynależności (stanu anomii), a także kryzysu tożsamości (zwłaszcza społeczeństw zachodnich i potomków migrantów muzułmańskich na Zachodzie) będących ze swej natury immanentnym zagrożeniem bezpieczeństwa tak jednostkowego, jak i grupowego.

Mając na względzie powyższe oraz toczącą się w dyskursie publicznym debatę na temat konieczności zwalczania terroryzmu i stworzenia tzw. ustawy antyterrorystycznej (dalej: UA), Centrum Badań nad Terroryzmem Collegium Civitas (CBnT CC) zorganizowało 17 lutego 2016 r. w siedzibie Collegium Civitas w Pałacu Kultury i Nauki w Warszawie seminarium eksperckie poświęcone tej tematyce. To wydarzenie miało ogromną wartość, gdyż zaproszeni goście i prelegenci są najbardziej doświadczonymi specjalistami akademickimi i praktykami działań kontr- i antyterrorystycznych[1] oraz analizy informacji w Polsce.

W dyskusji moderowanej przez Grzegorza Cieślaka (eksperta CBnT CC, koordynatora Zespołu Analiz Zamachów Bombowych CBnT CC) wzięli udział:

- prof. Daniel Boćkowski (Uniwersytet w Białymstoku, ekspert w zakresie Bliskiego Wschodu i współczesnego świata islamu),

[1] Nie są to pojęcia tożsame i pokrywające się zakresami – najogólniej przyjmuje się, że antyterroryzm odnosi się do ogółu działań związanych z przeciwdziałaniem terroryzmowi, a kontrterroryzm to fizyczne zwalczanie terroryzmu (tzw. działania kinetyczne). Szczegółowe wyjaśnienie różnic dotyczących kontrterroryzmu i antyterroryzmu oraz ich rozumienia w literaturze przedmiotu można znaleźć w następujących publikacjach: K. Jałoszyński, *Koncepcja współczesnych działań antyterrorystycznych*, Warszawa 2003; tenże, *Współczesny wymiar antyterroryzmu*, Warszawa 2008; tenże, *Jednostka kontrterrorystyczna – element działań bojowych w systemie bezpieczeństwa antyterrorystycznego*, Szczytno 2011; *Siły zbrojne w walce z terroryzmem*, M. Wiatr, J. Stelmach, M. Busłowicz (red.), Wrocław 2016. Przy uwzględnieniu powyższego, w niniejszej publikacji terminy k o n t r - i a n t y t e r r o r y s t y c z n y są stosowane w odniesieniu do wszelkiego typu działań i struktur mających na celu zwalczanie terroryzmu.

- prof. Kuba Jałoszyński (Wyższa Szkoła Policji w Szczytnie, były dowódca warszawskiego pododdziału antyterrorystycznego, twórca centralnej jednostki antyterrorystycznej Policji),
- Piotr Niemczyk (Niemczyk i Wspólnicy, były zastępca dyrektora Zarządu Wywiadu UOP oraz ekspert Sejmowej Komisji ds. Służb Specjalnych),
- dr Witold Sokała (Uniwersytet Jana Kochanowskiego w Kielcach, ekspert w zakresie wyzwań i zagrożeń asymetrycznych oraz roli służb specjalnych i mediów w polityce bezpieczeństwa).

Wstęp do spotkania stanowiło wystąpienie dr. Krzysztofa Liedela (dyrektora CBnT CC), podczas którego szczegółowo i ciekawie omówił on rozwój polskiego systemu antyterrorystycznego i jego podstawy prawne. Następnie głos zabrał Grzegorz Cieślak, zwracając uwagę na konieczność szybkiego uchwalenia dobrze napisanej i merytorycznie przygotowanej przez ekspertów UA. Podkreślił, że można mieć wątpliwości co do jej formy i efektywności, co wynika ze specyfiki terroryzmu jako zjawiska wyjątkowo łatwo adaptującego się do zmieniających się warunków i niepoddającego się kategoryzacji. Wskazał, że współcześnie sam sposób walki z terroryzmem ulega zmianie i zyskuje charakter proaktywny, ofensywny, wielopłaszczyznowy (w większości krajów) i wielopodmiotowy (podkreślił także dominującą rolę Agencji Bezpieczeństwa Wewnętrznego w zwalczaniu terroryzmu w Polsce i przeciwdziałaniu temu zjawisku). Zagrożenie terroryzmem nieuchronnie wytwarza potrzebę ściślejszej współpracy i koordynacji poszczególnych struktur kontr- i antyterrorystycznych, a w dalszej kolejności – ich „usieciowienia". Na zakończenie swojej wypowiedzi moderator wskazał, że w kontekście niniejszego seminarium jego główne pytanie brzmi: *Jaka powinna być polska ustawa antyterrorystyczna, tak aby zaspokoić oczekiwania tych, którzy będą jej podmiotami?*

Profesor Jałoszyński stwierdził, że na podstawie informacji medialnych oczekiwał, iż przedmiotem seminarium będzie dyskusja nad treścią powstającej UA i tym, co jeszcze można w niej udoskonalić. Niestety, jak dotychczas taki akt prawny nie powstał. Według niego UA powinna mieć charakter kompetencyjny, tzn. jasno określać kompetencje podmiotów kontr- i antyterrorystycznych, ich miejsce w hierarchii i łańcuchu dowodzenia oraz zakres odpowiedzialności. Prelegent podkreślił także, że współcześnie istnieje wiele podmiotów antyterrorystycznych, co prowadzi do dublowania się ich kompetencji i marnowania środków finansowych państwa. W związku z tym UA powinna wprowadzić także pewne zmiany w zakresie funkcjonowania służb specjalnych.

Po wystąpieniu prof. Jałoszyńskiego głos zabrał Piotr Niemczyk, który podkreślił znaczenie działań prewencyjnych i operacyjno-rozpoznawczych służb specjalnych. Jednocześnie wyraził wątpliwość, czy UA jest potrzebna. Jego zdaniem przeprowadzenie zamachu terrorystycznego i konieczność wykorzystania jednostek mundurowych oznaczają blamaż służb specjalnych. Ponadto wskazał, że w 2008 r. rozważano potrzebę napisania UA w celu powołania Centrum Antyterrorystycznego (CAT), okazało się jednak, że specjalna ustawa nie jest do tego wymagana. Stwierdził też, że obecnie nie ma potrzeby formułowania nowego aktu.

Prelegent podkreślił natomiast konieczność powstania jednej, jednolitej ustawy o czynnościach operacyjno-rozpoznawczych, kontroli operacyjnej itd. (zwrócił uwagę, że może istnieć jedna służba wykonująca te czynności bądź więcej tego typu podmiotów pod warunkiem dobrej koordynacji ich działań). Nadmienił, że od 2007 do 2011 r. nie udało się napisać takiej ustawy z powodu nadmiaru obowiązków specjalistów w tym zakresie. W związku z tym należy dążyć do uporządkowania sytuacji prawno-

-proceduralnej i przypisywania właściwych zadań odpowiednim służbom. Wskazał, że na obecnym etapie zagrożenia terrorystycznego w Polsce na razie nie ma takiej potrzeby, gdyż na terytorium naszego państwa nie przebywa zbyt wielu obcokrajowców, jak również brak silnych przesłanek wskazujących na duże prawdopodobieństwo przeprowadzenia ataku terrorystycznego. Istnieje za to możliwość rekrutacji do komórek terrorystycznych, rozpowszechniania treści terrorystycznych oraz upowszechniania tzw. hejtu internetowego, który może skutkować agresją fizyczną. Pojawia się tu problem granicy między wspomnianymi treściami a ich realnym skutkiem w formie aktu terrorystycznego oraz momentu, w którym należy interweniować, co może być przyczyną powstania państwa policyjnego. Pod koniec wypowiedzi Piotr Niemczyk zadał następujące pytania, które, według niego, wymagają wyjaśnienia przed opracowaniem UA:

1. Czym powinna być UA?
2. Jaka jest granica między terroryzmem religijnym a terroryzmem kryminalnym?
3. Kiedy mamy do czynienia z bandytyzmem?
4. W którym momencie zorganizowana grupa przestępcza zamienia się w grupę terrorystyczną i vice versa?
5. Czy ma to być ustawa uruchamiająca projekt społeczny edukowania, informowania i przygotowywania obywateli na to, jak mają się zachowywać w sytuacji zagrożenia bądź znalezienia się w sytuacji nadzwyczajnej?
6. Czy ma to być procedura działania poszczególnych komórek przeprowadzających odpowiednie czynności w przypadku wystąpienia sytuacji nadzwyczajnej, czy raczej kompleksowe potraktowanie regulacji związanych ze zwalczaniem terroryzmu, z czynnościami operacyjno-rozpoznawczymi włącznie?

W dalszej kolejności głos zabrał prof. Boćkowski. W kontekście tworzenia UA stwierdził, że najpierw trzeba jasno określić definicję tego, czym jest terroryzm. W dotychczasowym rozumieniu, w większości przypadków, owym pojęciem są określane działania kinetyczne. Ten sposób rozumowania nie obejmuje jednak tzw. terroryzmu informacyjnego i wykorzystania mediów w działaniach terrorystycznych. W dalszej kolejności, dopiero po jasnym zdefiniowaniu terroryzmu, należy wyznaczyć struktury odpowiedzialne za jego zwalczanie, połączyć ich kompetencje bądź nadać nowe, a także położyć nacisk na koordynację i współdziałanie już istniejących struktur.

Prelegent zasygnalizował też to, że trudno określić, kiedy terroryści poważnie zainteresują się Polską. Rozważał, jak wskazać obiektywny poziom zagrożenia, tak aby nie straszyć obywateli, i podkreślił rolę przekazu informacyjnego oraz jego znaczenie dla antyterroryzmu. Zwrócił uwagę, że dotychczasowe definicje nie ujmują najważniejszego aktualnie elementu terroryzmu, którym jest tzw. wojna informacyjna. Uczestniczą w niej podmioty państwowe, grupowe (organizacje niepaństwowe, w tym tzw. *trzeci sektor*, i (lub) ugrupowania terrorystyczne) oraz podmioty indywidualne i media, ale do końca nie wiadomo, w jakiej sferze należy ten typ wojny umieścić – czy zaliczyć ją do składowych terroryzmu, czy też rozpatrywać jako zagrożenie cybernetyczne. Ponadto zauważył, że wytworzonych w jej trakcie narracji nie sposób całkowicie kontrolować, mogą one (…) *zacząć żyć własnym życiem*, doprowadzając do wybuchu silnego hejtu i niezadowolenia społecznego.

Doktor Sokała wskazał, że UA (…) *ma po prostu poprawić nasze bezpieczeństwo.* Według jego słów Polska nie jest na razie krajem tzw. pierwszoplanowego zagrożenia terrorystycznego, ale jego poziom jest jednak wysoki. O ile aktualnie nie ma dużego prawdopodobieństwa przeprowadzenia przez islamistów ataku w Polsce, o tyle większe

niebezpieczeństwo grozi ze strony pojedynczych terrorystów, motywowanych racjami politycznymi, wpływem przekazu medialnego bądź zaburzeniami indywidualnymi (istnieje możliwość ostrej reakcji na „wydumane zagrożenie islamskie", np. w postaci polskiego Breivika) lub grup skrajnie prawicowych (lewicowych) wobec legalnie wybranej władzy w Polsce.

Prelegent wskazał, że współcześnie w przypadku nowych zagrożeń istnieje tendencja do wydawania *mających im odpowiadać* ustaw i rozporządzeń. Przy takim podejściu jednak UA nie rozwiąże wszystkich problemów. Wskazał też na problemy związane z zacieraniem się granic między wywiadem a kontrwywiadem w kontekście walki z terroryzmem, możliwość inspirowania działań terrorystycznych w Polsce przez „niezidentyfikowane państwa bądź organizacje pozarządowe" oraz na działalność inspirowanych i wykorzystywanych w tym celu tzw. pożytecznych idiotów. Zwrócił także uwagę, że najważniejsza w pracy wywiadowczej i antyterrorystycznej jest atmosfera pracy i etos ludzi, którzy się nią zajmują. Mówił też o możliwości zaistnienia sytuacji, w której uchwala się UA bez precyzyjnego określenia, czym jest terroryzm i jak go zwalczać. Jego zdaniem stworzyłoby to duże pole do nadużyć władzy przez polityków (chodzi tu o wykorzystywanie służb specjalnych).

Profesor Jałoszyński dodał, że UA jest potrzebna w Polsce z powodów czysto pragmatycznych. Jako przykład podał Federalne Biuro Śledcze USA (FBI) przed 11 września 2001 r. (stwierdził jednocześnie: *Lepiej napisać ją przed atakiem niż po*…). Ponadto ponownie podkreślił, że polska UA powinna jasno ustalić różnice kompetencyjne poszczególnych pododdziałów.

W odpowiedzi na te słowa moderator wskazał, że obecnie terroryzm jest zdefiniowany w art. 115 § 20 kk. W myśl tego paragrafu aktem terrorystycznym jest działanie o trzech enumeratywnie wymienionych cechach:

> Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:
>
> 1) poważnego zastraszenia wielu osób,
>
> 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
>
> 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu.

Grzegorz Cieślak stwierdził także, że używane w dyskusji pojęcie r y z y k a definiuje się jako wynik mnożenia prawdopodobieństwa przez skutek. Na zakończenie swej wypowiedzi moderator poprosił prelegentów o odpowiedź na pytanie, czy nie jest obecnie w Polsce tak, że potrzebujemy pewnego wspólnego standardu minimum działań antyterrorystycznych, np. w zakresie odpowiednich szkoleń dla społeczeństwa. W reakcji na to prof. Jałoszyński opisał skrótowo, jak ten problem został rozwiązany we Francji (francuska ustawa o zarządzaniu kryzysowym szczegółowo precyzuje procedury postępowania przez poszczególne podmioty w sytuacji zagrożenia terrorystycznego), gdyż – według jego słów – obecnie w Polsce tak naprawdę nie wiadomo, kto kogo ma słuchać w wypadku zagrożenia terrorystycznego. W odpowiedzi na to Piotr Niemczyk zauważył, że żadne działania antyterrorystyczne wywiadu nie mogą być w całości jawne.

W Polsce regulacja ustawowa stosownych procedur nie jest możliwa, ponieważ muszą one zachować klauzulę niejawności – w takim wypadku najpierw byłyby potrzebne delegacje ustawowe do niejawnych aktów wykonawczych. Wskazał także, że widzi potrzebę zwiększenia koordynacji działania służb oraz wdrożenia dużego projektu edukacyjnego uwrażliwiającego polskie społeczeństwo na to, jak ma się zachować w wypadku zagrożenia terrorystycznego.

Profesor Boćkowski wskazał, że w takim zakresie UA powinna teoretycznie koordynować działania prowadzone na podstawie wszystkich ustaw dotyczących terroryzmu przez poszczególne służby, tzn. powinna obejmować:

> (…) działania kinetyczne, definiowanie potencjalnych zagrożeń (nowa, rozszerzona definicja terroryzmu), rozpoznawanie zagrożeń (dostosowane do zmieniającej się rzeczywistości uprawnienia operacyjno-śledcze), przeciwdziałanie zaistniałym zagrożeniom (wspólne kanały obiegu informacji, rozszerzone uprawnienia operacyjno-śledcze, jednolity system dowodzenia w chwili zaistnienia zagrożenia), obowiązkowe kształcenie osób cywilnych (urzędnicy, samorząd, nauczyciele etc.) w rozpoznawaniu potencjalnych zagrożeń, reagowanie na rozpoznane zagrożenia terrorystyczne oraz potencjalne zagrożenia, jeśli nie do końca możemy przewidzieć mechanizm ich powstawania oraz pełną koordynację działań kontr/antyterrorystycznych,

którymi miałoby kierować zasugerowane przez prof. Boćkowskiego hipotetyczne Ministerstwo ds. Terroryzmu. Ponadto podkreślił, że w dzisiejszych czasach (…) *dobry terrorysta to martwy terrorysta*, gdyż celem terroryzmu ponowoczesnego i dżihadystycznego jest (…) *jak najwięcej ofiar*, ponieważ tylko to gwarantuje odpowiednią siłę przekazu. W związku z tym w momencie ataku terrorystycznego natychmiast muszą być podjęte odpowiednie kroki: od strzału snajperskiego po wiele podobnych rozwiązań. Inaczej mówiąc, powinniśmy przejść do proaktywnego zwalczania terrorystów przez ich fizyczną eliminację poza obszarem kraju oraz zdjąć odpowiedzialność prawną z ludzi, którzy mieliby wykonywać tego rodzaju zadania, i jednocześnie zapewnić im pełną ochronę prawną i anonimowość.

Doktor Sokała powiedział, że należy dokonać ewaluacji obecnych rozwiązań kontr- i antyterrorystycznych, a dopiero w dalszej kolejności je poprawiać, jeśli zajdzie taka potrzeba, lub napisać UA od podstaw. Jednocześnie przestrzegł laików przed projekcją własnych oczekiwań co do UA – wskazał, że nawet „ekspresowe" uchwalenie UA nie zapewni Polsce i Polakom bezpieczeństwa antyterrorystycznego. Należy także dążyć do prawnego usankcjonowania możliwości ofensywnego użycia wojskowych jednostek specjalnych w działaniach kontr- i antyterrorystycznych. Stanowczo podkreślił też, że aktualnie wykorzystanie żołnierzy polskich Wojsk Specjalnych zgodnie z ich wyszkoleniem i procedurami wojskowymi w czasie misji antyterrorystycznej w Polsce łamie obowiązujące prawo. Jedynym wyjściem jest postępowanie zgodnie z procedurami policyjnymi, które jest jednak poprzedzone czasochłonnym uzyskaniem zgody na działania policyjne na terenie kraju, często odbierającym najważniejszy element w walce z terroryzmem – element zaskoczenia. Następnie wskazał na brak możliwości legalnego korzystania z pomocy snajperów w sytuacji zagrożenia terrorystycznego w obowiązującym stanie prawnym.

W dalszej kolejności prelegenci odpowiadali na pytania słuchaczy i odnosili się do ich komentarzy.

Pierwszy z pytających wyraził zaniepokojenie stanem bezpieczeństwa państwa i przygotowaniem na potencjalne działania terrorystyczne, sposobem i jakością przygotowywania prawa w kontekście UA oraz działaniem polskiego systemu antyterrorystycznego (trzeba go zgrać i przeszkolić odpowiednie służby i jednostki). Równocześnie podkreślił konieczność przyjmowania najgroźniejszych scenariuszy, tj. konieczności bycia przygotowanym na rozbudowany tzw. atak sekwencyjny. Według niego policyjne siły antyterrorystyczne są zbyt mało liczne i nieprzygotowane na tego typu działanie, a jednocześnie nie jest możliwe wykorzystanie w takim przypadku wojskowych jednostek specjalnych zgodnie z ich przeznaczeniem. Odpowiadając, prof. Jałoszyński zauważył, że istnieje prawnie uregulowana możliwość wykorzystania na terenie Polski policyjnych jednostek specjalnych np. z Niemiec, Czech i Litwy (w ramach Stowarzyszenia ATLAS). Poruszył jednocześnie problem konieczności dokonania zmian przepisów warunkujących skorzystanie z pomocy policyjnych strzelców wyborowych, gdyż obecnie *Dowódca, który wyda strzelcowi wyborowemu rozkaz użycia broni, będzie odpowiadał za podżeganie do zabójstwa*[2].

Inny słuchacz stwierdził, że wystarczy skoordynować możliwości działania istniejących jednostek i struktur, a nie tworzyć UA. Doktor Sokała odpowiedział na to, że należy dokonać ewaluacji istniejącego stanu prawnego, poprawić stosowne akty prawne i dopiero na koniec, jeśli zajdzie taka potrzeba, przygotować UA. Odniósł się także do konieczności uregulowania oraz upowszechnienia dostępu obywateli do broni palnej. Zauważył, że o ile nie ma głębszego sensu posiadanie broni palnej przez obywateli w sytuacji konfliktu z licznym i dobrze wyposażonym przeciwnikiem (jak np. Specnaz), o tyle w sytuacji à la działania Breivika posiadanie broni przez większą liczbę ludzi (w tym oficerów rezerwy czy pracowników instytucji państwowych) mogłoby zapobiec potencjalnym atakom. Profesor Boćkowski dodał, że nie da się w sposób enumeratywny, za pomocą norm prawnych, uregulować możliwości taktycznego wykorzystania snajperów w działaniach kontr- i antyterrorystycznych w czasie pokoju – jedynym sposobem jest działanie w tzw. stanie wyższej konieczności.

Na zakończenie moderator podał dwa przykłady świadczące o konieczności uwzględnienia w UA zasady indywidualnej decyzyjności:

1) sierżant armii amerykańskiej ma decyzyjność na tym samym poziomie, co generał armii egipskiej lub saudyjskiej,
2) podczas ataku terrorystycznego 13 listopada 2015 r. w Paryżu udało się uniknąć większej liczby ofiar przy Stade de France tylko dzięki temu, że kierownik bezpieczeństwa poinformowany o możliwości wystąpienia zagrożenia terrorystycznego na stadionie zakazał wypuszczania znajdujących się na trybunach kibiców poza teren obiektu do czasu przyjazdu liczniejszych sił porządkowych i opanowania sytuacji. W Polsce, zgodnie z obecnie obowiązującymi przepisami, po ogłoszeniu alarmu terrorystycznego należałoby od razu wyprowadzić kibiców znajdujących się np. na Stadionie Narodowym na zewnątrz obiektu, na obszar oznaczony prostokątem z napisem *Teren ewakuacyjny*.

Tym samym Grzegorz Cieślak podkreślił potrzebę ustanowienia w przyszłej polskiej UA zasady jednoosobowej odpowiedzialności i decyzyjności podczas zagrożeń terrorystycznych. Wskazał, że konieczne jest wymuszenie debaty publicznej na temat bezpieczeństwa i przeciwdziałania terroryzmowi przez zastosowanie szeroko skonsultowanych i dopracowanych pragmatycznych rozwiązań systemowych uwzględniających zasadę decyzyjności.

[2] Szerzej: K. Jałoszyński, *Strzał ratunkowy*, „Special Ops Extra. Wydanie specjalne" 2016, nr 1, s. 42–52.

Pod koniec seminarium głos zabrało dwóch słuchaczy. Pierwszy z nich podkreślił, że 11 września 2001 r. jest już właściwie prehistorią i że obecnie obowiązują doskonalsze procedury postępowania oraz jest lepsza koordynacja działań służb niż wcześniej. Terroryzm jednak także przez ten czas ewoluował, w związku z czym polski system antyterrorystyczny również powinien być bardziej nowoczesny i elastycznie adaptować się do aktualnej sytuacji, zapewniając tym samym możliwość szybkiej reakcji.

Drugi słuchacz wskazał, że problem systemu bezpieczeństwa państwa w Polsce wynika z niewłaściwej perspektywy. Jego zdaniem konieczne jest stworzenie tzw. czerwonej komórki zajmującej się monitorowaniem zagrożeń bezpieczeństwa państwa oraz praktyczną ewaluacją istniejących struktur, procedur i zasadności stosowanych rozwiązań, która podlegałaby Prezydentowi RP (opcjonalnie ministrowi obrony narodowej i (lub) ministrowi spraw wewnętrznych oraz ministrowi koordynatorowi służb specjalnych). Ponadto podkreślił, że obecnie najbardziej niebezpieczną, a możliwą do wystąpienia na terenie Rzeczpospolitej Polskiej formą terroryzmu jest tzw. terroryzm państwowy stosowany przez nieprzychylne RP państwo ościenne (bazujący na niezwykle starannym i przemyślanym przygotowaniu działań o charakterze skarajnie terrorystyczno-dywersyjnym oraz dostępie do wielu środków i materiałów użytecznych w działaniach terrorystycznych niedostępnych „zwykłym" grupom terrorystycznym). Ta wypowiedź wywołała ożywione reakcje prelegentów i moderatora.

W dyskusji poruszano zagadnienia z siedmiu obszarów o szczególnym znaczeniu dla usprawnienia systemu bezpieczeństwa Rzeczpospolitej Polskiej:

1. Dokonanie przemyślanej ewaluacji struktur kontr- i antyterrorystycznych (aby nie mnożyć nadmiernie bytów), ich zakresów odpowiedzialności, sposobów funkcjonowania; zwiększenie możliwości wymiany danych między nimi w celu polepszenia efektywności funkcjonowania oraz maksymalnego uelastycznienia przepływu informacji i koordynacji działań („usieciowienia" systemu, tzw. reguła *plug and play*). Należałoby też przygotować model zoptymalizowanego, racjonalnego i bardziej efektywnego wykorzystania wyszkolonych kadr jednostek specjalnych oraz kontr- i antyterrorystycznych, a także ich przepływu między poszczególnymi instytucjami odpowiedzialnymi za bezpieczeństwo państwa (jako instruktorzy w Wojsku Polskim, Policji, Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Straży Granicznej, Biurze Ochrony Rządu, Centralnym Biurze Antykorupcyjnym, Żandarmerii Wojskowej oraz cywilnych instytucjach państwowych itp.) bądź po ich odejściu ze służby (mogliby być przyjmowani do jednostek antyterrorystycznych mniej obciążonych operacyjnie, jako instruktorzy lub specjaliści od bezpieczeństwa we wspomnianych cywilnych instytucjach państwowych, szkołach, uczelniach wyższych itp. – wymagałoby to stworzenia systemu „zachęt" dla tych funkcjonariuszy i operatorów oraz instytucji, a także odpowiedniego uregulowania prawnego powyższego stanu rzeczy)[3]. Dotyczy to zwłaszcza operatorów Wojsk Specjalnych RP (szczególnie JW GROM), funkcjonariuszy Biura Operacji Antyterrorystycznych Komendy Głównej Policji, Zarządu III Centralnego Biura Śledczego Policji oraz V Wydziału Antyterrorystycznego Agencji Bezpieczeństwa Wewnętrznego.

[3] Sprawą otwartą jest forma takiego działania: podejście „zindywidualizowane" vs. utworzenie Narodowego Centrum Szkoleniowego Wojsk Specjalnych i Jednostek Kontr- i Antyterrorystycznych prowadzącego zunifikowane i zestandaryzowane szkolenia dostosowane do różnorodnych potrzeb poszczególnych rodzajów wojsk i służb lub członków Obrony Terytorialnej i organizacji proobronnych.

2. Konieczność pragmatycznego podejścia do współpracy poszczególnych służb (instytucji) bezpieczeństwa państwa (wraz ze zwiększeniem środków finansowych z budżetu państwa – zwłaszcza w odniesieniu do działań rozpoznawczo-wywiadowczych Agencji Wywiadu i Służby Wywiadu Wojskowego oraz ofensywnego zwalczania terroryzmu przez Wojska Specjalne, Biuro Operacji Antyterrorystycznych KGP, Wydział V Antyterrorystyczny ABW i Centrum Antyterrorystyczne ABW w celu podniesienia poziomu koordynacji obecnie istniejących struktur (tzw. reguła kułaka[4]) np. przez:
   - ustanowienie niezależnej międzyresortowej i (lub) międzyinstytucjonalnej komórki bądź grupy roboczej koordynującej współpracę kontr- i antyterrorystyczną poszczególnych służb i Wojsk Specjalnych na obszarze Polski, monitorującej poziom zagrożeń terrorystycznych oraz uświadamiającej społeczeństwo co do możliwości ich zaistnienia na terenie kraju oraz za granicą,
   - prowadzenie rozbudowanych szkoleń dla funkcjonariuszy i społeczeństwa ukazujących sposoby działania w sytuacji zagrożenia terrorystycznego, np. przez utworzenie Narodowego Centrum Antyterrorystycznego (jako ministerstwa ds. terroryzmu) na wzór Agencji Bezpieczeństwa Wewnętrznego, Biura Bezpieczeństwa Narodowego, Rządowego Centrum Bezpieczeństwa bądź zwiększenie roli, zakresu obowiązków i odpowiedzialności Centrum Antyterrorystycznego Agencji Bezpieczeństwa Wewnętrznego,
   - zwiększenie roli i znaczenia oficerów łącznikowych między poszczególnymi jednostkami specjalnymi Policji, Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej, Biura Ochrony Rządu, Żandarmerii Wojskowej i Wojsk Specjalnych,
   - ujednolicenie standardów pozyskiwania, gromadzenia, przetwarzania i wymiany informacji między poszczególnymi służbami i wojskiem połączone z rozbudową merytoryczną i fizyczną istniejących baz danych (przepustowość), infrastruktury krytycznej i teleinformatycznej oraz uregulowaniem jej stanu prawnego w celu polepszenia możliwości przepływu informacji i ich dostępności dla zainteresowanych podmiotów.

   Zasadne wydaje się też „nieplanowane" pełnoskalowe (na terenie całego kraju) przećwiczenie współpracy poszczególnych elementów systemu bezpieczeństwa państwa na wypadek wspomnianych wyżej sekwencyjnych ataków terrorystycznych, połączone z wypracowaniem wspólnych procedur i zakresu odpowiedzialności poszczególnych jednostek i służb.

[4] Reguła „kułaka" postuluje zwiększenie przepływu informacji i interoperacyjności istniejących struktur kontr- i antyterrorystycznych, tak aby mimo zachowania odrębności strukturalnej i zadaniowej działały one jak jeden organizm (kułak) na zasadzie współpracy (wymienialności) elementów składowych (zasada *Plug and Play*). Wymagałoby to zwiększenia ilości i stopnia skomplikowania ćwiczeń zgrywających, polepszenia komunikacji między poszczególnymi służbami i jednostkami (kwestie odmienności sprzętowej, proceduralnej, ustanowienia wspólnych fizycznych kanałów komunikacji i wymiany danych itp.) oraz ustalenia podległości między jednostkami wojskowymi i policyjnymi na wypadek kryzysu i wojny. Do rozważenia pozostaje tu dowodzenie wyżej wymienionymi strukturami w czasie kryzysu (w przypadku ataku terrorystycznego, wojny hybrydowej) i wojny. Wydaje się, że w czasie kryzysu byłoby zasadne utrzymanie odrębności dowodzenia (Wojska Specjalne zaczynałyby działać jako tzw. *game changer*, gdyby już wszystkie inne struktury zawiodły), na czas wojny natomiast należałoby wprowadzić podległość (całości bądź części) jednostek kontr- i antyterrorystycznych Policji pod Wojska Specjalne, np. do zabezpieczenia mniej ważnych obiektów i działań oraz ochrony VIP-ów, zgodnie z ich policyjnym wyszkoleniem i wyposażeniem, tak aby maksymalnie wykorzystać potencjał systemu bezpieczeństwa państwa.

3. Dokonanie zmian prawnych umożliwiających zastosowanie jednostek Wojsk Specjalnych (bądź innych wydzielonych komponentów Sił Zbrojnych RP bądź ich całości) w reakcji na zagrożenia atakami terrorystycznymi na obszarze kraju[5], zgodnie z ich wojskowym wyszkoleniem, wyposażeniem i procedurami działania[6], połączone z maksymalnym uproszczeniem związanych z tym procedur, łańcucha dowodzenia oraz zapewnieniem operatorom Wojsk Specjalnych ochrony prawnej[7] i anonimowości[8]. Należałoby tu zastosować zasadę subsydiarności (Wojska Specjalne są wykorzystywane wtedy, gdy możliwości służb przeznaczonych do tego typu zadań okażą się lub mogą się okazać niewystarczające). Zasadne wydaje się ustawowe umożliwienie Wojskom Specjalnym i oficerom wywiadu wykonywania – zarówno w czasie pokoju, kryzysu, jak i wojny – mniej lub bardziej utajnionych zagranicznych misji typu *kill or capture* wobec jednostek i grup podejrzewanych o przygotowywanie zamachów terrorystycznych na terenie Polski, wobec obywateli polskich (w kraju i za granicą) oraz polskich władz państwowych, połączone z zapewnieniem ochrony prawnej i anonimowości uczestniczącym w nich operatorom. W związku z charakterystyką działań Wojsk Specjalnych najbardziej optymalne i celowe w szerszej perspektywie czasowej byłoby uchwalenie ustawy o Wojskach Specjalnych w celu wykorzystania pełnego spektrum zdolności tychże wojsk w czasie pokoju, kryzysu i wojny – zarówno w kraju, jak i za granicą.
4. Maksymalne zwiększenie mobilności poszczególnych jednostek Wojsk Specjalnych i jednostek kontr- i antyterrorystycznych (zwłaszcza przez zwiększenie możliwości transportu powietrznego[9]) oraz poziomu ich gotowości bojowej, tak aby w przypadku zagrożenia terrorystycznego (np. ataku sekwencyjnego) można było niezwłocznie wykorzystać szybko działające krajowe siły i środki (wraz z wypracowaniem odpowiednich procedur działania) bez konieczności proszenia o pomoc państw ościennych.
5. Dokonanie zmian w systemie prawnym przez nowelizację istniejących ustaw (zwiększenie poziomu ochrony prawnej dla operatorów i antyterrorystów oraz policjantów i funkcjonariuszy używających broni w sytuacjach zakładniczych lub terrorystycznych, wprowadzenie strzału ratunkowego, strzału na rozkaz, *kill shot* w przypadku snajperów, powiązane ze zniesieniem odpowiedzialności prawnej

[5] Zwłaszcza przez maksymalne uproszczenie systemu dowodzenia Wojskami Specjalnymi lub wspomnianymi wydzielonymi komponentami Sił Zbrojnych RP albo ich całością.

[6] Wykorzystanie Wojsk Specjalnych w sytuacji o charakterze terrorystycznym lub zagrożenia atakiem terrorystycznym oznacza, że środki policyjne są niewystarczające i nieadekwatne do stopnia, skali i wielkości skutków zagrożenia, w związku z czym ograniczenie działania tychże wojsk do ram policyjnych jest niecelowe. Konieczne jest tu wyłączenie wobec Wojsk Specjalnych, całości sił zbrojnych bądź ich poszczególnych komponentów ograniczeń wynikających z ustawy o środkach przymusu bezpośredniego i broni palnej oraz przyjęcie zasad użycia uzbrojenia wynikających z ustawy o powszechnym obowiązku obrony RP i prawa międzynarodowego.

[7] To jest ograniczenia odpowiedzialności karnej operatorom i zapewnienia im bezpiecznego zakończenia operacji przez powstrzymywanie się od podejmowania wobec nich czynności prawnoprocesowych przez pewien czas (np. 72 godziny) od zakończenia działań.

[8] Kwestia zunifikowania i ustawowego uregulowania ochrony danych osobowych i wizerunku przed upublicznieniem w telewizji, prasie i Internecie, a tym samym – dostępu do nich dla potencjalnych terrorystów.

[9] Aby ograniczyć koszty, należałoby utworzyć działającą na obszarze całej Polski mieszaną, policyjno-wojskową grupę transportową o wysokim poziomie gotowości do działania, wyposażoną w helikoptery transportowo-szturmowe, transportowe i rozpoznawcze.

za tego typu działania[10]) i utworzenie nowej UA. Jak się okazało, istnieją w tym zakresie duże różnice zdań między przedstawicielami poszczególnych środowisk eksperckich. Dlatego, przy uwzględnieniu bezpieczeństwa państwa, należy dążyć do przygotowania „eksperckiej wersji" UA, aby ułatwić prace nad ustawą w Sejmie RP.

6. Zapewnienie odpowiedniego poziomu przeszkolenia i procedur działania, tzw. *first responders*, zwłaszcza funkcjonariuszom Policji, m.in. przez zwiększenie liczby i stopnia skomplikowania strzelań bojowych wraz z urealnieniem scenariuszy działań (problemy: zamachowcy – samobójcy i tzw. *active shooters*). Należy ponadto zapewnić im odpowiednio dobrane, adekwatne do zagrożenia środki ataku (wyposażenie policjantów w nowoczesne pistolety maszynowe i karabiny szturmowe), środki ochrony osobistej (wygodne kamizelki kuloodporne i hełmy) oraz środki komunikacji (nowoczesne kodowane radiostacje szerokopasmowe). Ujednolicenia i uregulowania prawnego wymagają standardy pracy oraz procedury i zakres uprawnień dotyczących tzw. taktyki czerwonej (*Tactical Combat Casualty Care*) wojskowych i policyjnych ratowników taktycznych wobec rannych i poszkodowanych w działaniach terrorystycznych lub antyterrorystycznych. W tym kontekście optymalne wydaje się bazowanie na doświadczonych kadrach oraz standardach i procedurach wypracowanych przez lata w Wojskach Specjalnych, Biurze Operacji Antyterrorystycznych KGP i Agencji Bezpieczeństwa Wewnętrznego wraz z jasnym i precyzyjnym ustaleniem zakresu działań i odpowiedzialności wymienionych ratowników taktycznych.
7. Konieczność utworzenia wspomnianej „czerwonej komórki" (bądź rozszerzenia działań i uprawnień Centrum Antyterrorystycznego Agencji Bezpieczeństwa Wewnętrznego w tym zakresie) mającej na celu ewaluację i maksymalne usprawnienie istniejących struktur bezpieczeństwa i procedur dotyczących ich funkcjonowania (tzw. reguła czarnego łabędzia).

[10] Przy uwzględnieniu odmienności religijnej i kulturowej potencjalnych terrorystów mogących działać w Polsce zasadne byłoby przekazanie części zadań snajperskich kobietom służącym w Wojskach Specjalnych i pododdziałach kontr- oraz antyterrorystycznych Policji i Agencji Bezpieczeństwa Wewnętrznego, a także odpowiednie nagłośnienie medialne tego typu działań.

O autorach

About the authors

Tomasz R. Aleksandrowicz – prof., dr hab., Wyższa Szkoła Policji w Szczytnie.

Jakub Dej – absolwent Wydziału Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego, laureat V edycji konkursu szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa.

Mirosław Dela – Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

Karol Falandys – dr, Wojskowa Akademia Techniczna w Warszawie.

Sławomir Gładysz – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Konrad Graczyk – doktorant w Katedrze Historii Prawa Wydziału Prawa i Administracji Uniwersytetu Śląskiego, laureat V edycji konkursu szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa.

Vitalij Hrebenuk – dr, Narodowa Akademia Służby Bezpieczeństwa Ukrainy.

Zbigniew Małysz – magister, Wydział Nauk Pedagogicznych Akademii Pedagogiki Specjalnej im. Marii Grzegorzewskiej w Warszawie.

Anatolij I. Maruschak – dr, Narodowa Akademia Służby Bezpieczeństwa Ukrainy.

Marcin Piotrak – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Elżbieta Posłuszna – dr hab., profesor nadzwyczajny w Instytucie Bezpieczeństwa Powietrznego Wydziału Bezpieczeństwa Narodowego i Logistyki Wyższej Szkoły Oficerskiej Sił Powietrznych w Dęblinie.

Mirosław Sikora – dr, Oddział IPN w Katowicach.

Janusz Wasilewski – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Rafał Wądołowski – doktorant Wydziału Prawa i Administracji Uniwersytetu Gdańskiego.

Informacje dla autorów „Przeglądu Bezpieczeństwa Wewnętrznego”

Redakcja zwraca się do autorów nadsyłających teksty do druku o stosowanie następujących zasad:

1. Wszystkie teksty należy przesyłać w postaci zapisu elektronicznego (Word, Open Office) na adres Redakcji: redakcja.pbw@abw.gov.pl.
2. Do artykułu należy dołączyć: bibliografię załącznikową (według schematu opisanego w pkt 10), streszczenie o objętości tekstu do pół strony wydruku komputerowego, notkę o autorze (zawód lub tytuł naukowy, miejsce pracy) oraz pięć słów kluczowych (w celu maksymalnie zwięzłego określenia tematyki artykułu – mają one ułatwić klasyfikację treści oraz wyszukiwanie artykułu w elektronicznych bazach danych; słowa kluczowe nie powinny być powtórzeniem tytułu). Streszczenie i słowa kluczowe powinny być przekazane również w języku angielskim.
3. Autorzy powinni wypełnić *Formularz zgody autora na publikację artykułu w czasopiśmie „PBW”* dostępny na stronie Agencji Bezpieczeństwa Wewnętrznego i przesłać go na adres Redakcji podany w pkt 1.
4. Wszelkie ilustracje, zdjęcia oraz schematy, które autor chciałby umieścić w artykule, powinny być dostarczone w oddzielnych oryginalnych plikach; ich wymiary powinny być nie mniejsze, niż te, które mają być otrzymane po wydruku oraz możliwie jak najlepszej jakości (min. 600 dpi). W przypadku dostarczenia ilustracji złej jakości Redakcja zastrzega sobie prawo do ich nieumieszczania.
5. Należy podać źródła wszystkich materiałów ilustracyjnych (zdjęć, rysunków, wykresów, schematów, tabel itd.).
6. Na końcu podpisu pod materiałem ilustracyjnym należy stawiać kropkę.
7. Odsyłacze do przypisów powinny być umieszczone w tekście przed znakami interpunkcyjnymi – kropką kończącą zdanie (wyjątek: skrót r. – rok lub podobny), przecinkiem itd.
8. Cytaty ze źródeł i literatury przedmiotu, nazwy ustaw i innych aktów prawnych, tytuły prac naukowych, utworów literackich, muzycznych, dramatycznych, obrazów, konkursów należy wyróżniać kursywą.
9. Nazwy wystaw, konferencji i sesji naukowych należy pisać antykwą i wyróżnić cudzysłowem.
10. W przypisach powinien być zachowany następujący schemat opisu:
    a) przypis zaczynamy wielką literą (wyjątek stanowi przypis internetowy) i kończymy kropką,
    b) przypis archiwalny: nazwa archiwum, po przecinku – nazwa zespołu, po przecinku – sygnatura, po przecinku – nazwa dokumentu (kursywą) lub jego opis (np.: list, sprawozdanie) i data, po przecinku – numer karty (strony),

PRZYKŁADY:
AIPN, OBUiAD w Krakowie, IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57;

APK, UWŚl., sygn. 736, sprawozdanie z działalności Policji Województwa Śląskiego za 1928 r. z 5 I 1929 r., k. 57;

c) druki zwarte: inicjał imienia, nazwisko autora, po przecinku – tytuł (kursywą), po przecinku – ewentualnie tom, po przecinku – miejsce i rok wydania, po przecinku – wydawnictwo, po przecinku – numery stron; po tytule publikacji zamieszczonej w pracy zbiorowej stawiamy przecinek i piszemy: w: i tytuł pracy (kursywą),

PRZYKŁAD:
W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, PWN, s. 36;

d) artykuły w czasopismach: inicjał imienia, nazwisko autora, po przecinku – tytuł (kursywą), po przecinku – tytuł czasopisma w cudzysłowie, dalej (bez przecinka) rok wydania, po przecinku – tom, zeszyt, numer, część (w opisie należy stosować cyfry arabskie), po przecinku – numery stron,

PRZYKŁAD:
W. Nowak, *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 13;

e) wydawnictwa internetowe: adres internetowy rozpoczynający się małą literą (bez podkreśleń i hiperłączy), po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:
http://www.pbw.gov/abw/cat.html [dostęp: 1 XII 2011];

f) artykuły lub dokumenty zamieszczone na stronach internetowych: tytuł artykułu (dokumentu) kursywą, dalej (bez przecinka) w nawiasie kwadratowym – informacja o trybie dostępu, po przecinku – adres internetowy, po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:
EU NAVFOR Somalia – mission [online], http://www.eunavfor.eu/about-us/mission/ [dostęp: 20 VII 2014];

g) podając numer strony, należy stosować skrót: s. 30; zakres stron należy zaznaczyć półpauzą bez świateł, np.: s. 24–27,
h) należy stosować oznaczenia: tamże, tenże, taż (jeżeli tego typu zwroty rozpoczynają przypis, należy stosować wielką literę), inicjał imienia, nazwisko autora, po przecinku – skrót tytułu (kursywą), po przecinku – numery stron; nie stosujemy skrótów: op. cit., loc. cit.,

PRZYKŁAD:

W. Nowak, *Służba*…, s. 12.
Tamże, s. 14;

i) po skrócie: zob. i por. nie stawiamy dwukropka,
j) po skrócie: cyt. za: stawiamy dwukropek.

11. Przy zestawianiu bibliografii załącznikowej kolejne pozycje szeregujemy w porządku alfabetycznym. Opis każdej pozycji rozpoczynamy od nazwiska autora, po nim umieszczamy inicjał imienia, kropkę, przecinek, a następnie według schematu przypisu – tytuł zapisany kursywą itd. W przypadku druków zwartych na końcu opisu bibliograficznego należy podać łączną liczbę stron, w przypadku artykułu w czasopiśmie lub w pracy zbiorowej – zakres stron.

PRZYKŁADY:

Kowalski W., *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 12–20.

Nowak W., *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, PWN, s. 32–47.

Sekretna wojna. Z dziejów kontrwywiadu II RP, Z. Nawrocki (red.), Poznań 2014, Zysk i S-ka, 542 s.

12. W tekście głównym należy stosować ogólnie przyjęte skróty (np., itp., m.in., rkps, mps, t., z. itd.), a także z reguły: r. (rok) i w. (wiek).
13. W tekście głównym, podając datę, nazwę miesiąca należy zapisywać słownie, np.: 3 lipca 1969 r. Wyjątek stanowi zapis podany w przypisie, gdy miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.
14. Różne sposoby zapisu daty stosowane w tekście głównym powinny być ujednolicone do następującej formy, np. 12 VIII 1946; nie należy zamieniać na liczbę rzymską nazw miesięcy pisanych słownie w tekstach źródłowych.
15. Przy podawaniu daty dostępu do źródeł internetowych miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.
16. W tekście głównym należy podawać pełne imię i nazwisko osoby, która jest wymieniana po raz pierwszy.
17. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp., jeśli są wymieniane w tekście po raz pierwszy.
18. Obce nazwy organizacji oraz skróty od nich utworzone powinny być pisane antykwą (tekstem prostym).
19. Nie należy stosować tzw. twardych spacji.
20. Ortografię i interpunkcję tekstu należy uwspółcześniać.
21. Wszelkie wyróżnienia w oryginalnym tekście dokumentu, dokonane przez jego twórcę, powinny być wyróżnione wytłuszczoną czcionką.
22. Nawiasy ukośne /…/ powinny być zamieniane na nawiasy półokrągłe (…).
23. Skróty słownikowe należy pozostawić bez rozwinięcia.
24. Uzupełnienie odautorskie, od Redakcji itp. należy podawać w nawiasach kwadratowych antykwą.

25. Opuszczenia pochodzące od wydawcy powinny być zaznaczone trzema kropkami w nawiasie okrągłym.
26. Opuszczenia w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie okrągłym.
27. Redakcja zastrzega sobie prawo do zwracania autorom tekstów opracowanych bez uwzględnienia powyższych zasad.
28. Redakcja zastrzega sobie prawo do dokonywania zmian i skrótów w porozumieniu z autorem.
29. Redakcja zwraca uwagę, że *ghostwriting*[*] i *guest authorship*[**] są przejawem nierzetelności naukowej, a wszelkie wykryte przypadki praktyk niezgodnych z zasadami etyki obowiązującej w nauce będą ujawniane, włącznie z powiadomieniem odpowiednich podmiotów (instytucji zatrudniających autorów, towarzystw naukowych, stowarzyszeń edytorów naukowych itp.).
30. Redakcja zwraca uwagę, że autorzy tekstów powinni w sposób przejrzysty, rzetelny i uczciwy prezentować rezultaty swojej pracy, a wszelkie przejawy nierzetelności naukowej, zwłaszcza łamanie i naruszanie zasad etyki obowiązujących w nauce, będą przez Redakcję dokumentowane.

[*] Z *ghostwriting* mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie publikacji, ale jego udział jako autora nie zostaje ujawniony lub choćby uwzględniony w podziękowaniach dołączonych do tekstu.

[**] Sytuacja określana też jako *honorary authorship* – osoba podana jako autor czy współautor tekstu miała znikomy udział lub wcale nie uczestniczyła w tworzeniu publikacji.