TERRORYZM

studia
analizy
prewencja

TERRORISM
PREVENTION
Centre of Excellence

CENTRALNY OŚRODEK
SZKOLENIA I EDUKACJI ABW

Zespół redakcyjny dr Damian Szlachter (redaktor naczelny)
Agnieszka Dębska (sekretarz redakcji, skład)

Redakcja językowa i korekta Aleksandra Dąbała, Aneta Olkowska, Grażyna Osuchowska

Projekt okładki Aleksandra Bednarczyk

ISSN 2720-4383
e-ISSN 2720-6351

Artykuły zamieszczone w czasopiśmie są recenzowane

Artykuły wyrażają poglądy autorów

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną
Wersja online czasopisma jest dostępna na stronie www.abw.gov.pl/wyd/

Czasopismo jest dostępne w Portalu Czasopism Naukowych Uniwersytetu Jagiellońskiego pod adresem: https://www.ejournals.eu/Terroryzm/

Materiały do czasopisma należy składać przez panel redakcyjny dostępny pod adresem: https://ojs.ejournals.eu/Terroryzm/about/submissions

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota”
ul. Nadwiślańczyków 2, 05-462 Wiązowna

Kontakt
tel. (+48) 22 58 58 671
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Numer zamknięto i oddano do druku we wrześniu 2022 r.

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

SPIS TREŚCI

Szanowni Państwo!

W dniu 26 kwietnia 2022 r. w Centralnym Ośrodku Szkolenia i Edukacji ABW odbyła się uroczysta inauguracja nowego czasopisma naukowego „Terroryzm – studia, analizy, prewencja" (T-SAP). Udział w niej wzięli przedstawiciele ośrodków analitycznych (Polskiego Instytutu Spraw Międzynarodowych, Ośrodka Studiów Wschodnich, Instytutu Zachodniego), środowiska akademickiego, administracji państwowej oraz służb mundurowych tworzących system antyterrorystyczny RP.

Spotkanie rozpoczął Szef ABW płk Krzysztof Wacławek, który opowiedział o nowej inicjatywie wydawniczej ABW. Po wystąpieniach prelegentów uczestnicy zostali poproszeni o wzięcie udziału w anonimowym badaniu ankietowym. Jego celem było uzyskanie odpowiedzi na pytania dotyczące postrzegania zjawiska terroryzmu oraz wytypowanie najbardziej prawdopodobnych kierunków rozwoju zagrożeń terrorystycznych w RP. Takie badanie zostało przeprowadzone w Polsce po raz pierwszy, a jego wyniki zamieszczono w tym numerze periodyku.

Planujemy, że badania ankietowe będą realizowane cyklicznie. Liczymy, że otrzymane w ten sposób dane staną się merytorycznym wsparciem w dyskusji poświęconej kierunkom i wariantom rozwoju systemu antyterrorystycznego w RP oraz w budowaniu międzynarodowych inicjatyw w tym zakresie. Tego typu autorskie projekty o charakterze badawczo-naukowym będą zatem stale obecne na łamach T-SAP, aby czasopismo naukowe ABW mogło wypełniać swoją misję zacieśnienia współpracy między różnymi środowiskami zaangażowanymi w działania na rzecz ochrony antyterrorystycznej.

W drugim numerze periodyku znajdą Państwo artykuły poświęcone m.in.: zadaniom organów ochrony prawnej w zakresie zwalczania terroryzmu w Polsce, roli stopni alarmowych w systemie antyterrorystycznym, finansowaniu terroryzmu w ujęciu historycznym, możliwym scenariuszom rozwoju zagrożeń terrorystycznych w kontekście wojny w Ukrainie, a także

studium przypadku sprawcy zamachów terrorystycznych na norweskiej wyspie Utøya. Zamieszczono w nim również recenzję nowo wydanej książki Tomasza Aleksandrowicza poświęconej metodom prognozowania zagrożeń terrorystycznych.

Zapraszając do lektury czasopisma T-SAP, wyrażam nadzieję, że materiały prezentowane na jego łamach spotkają się z Państwa zainteresowaniem i będą istotnym wkładem w dyskusję publiczną nad budowaniem odporności polskiego społeczeństwa na zagrożenia o charakterze terrorystycznym.

Redaktor naczelny
dr Damian Szlachter

DOI: 10.4467/27204383TER.22.017.16337

ORCID: 0000-0002-6685-8769

PIOTR BURCZANIUK

Zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce – perspektywa prawna

Abstrakt

W artykule podjęto temat zadań i uprawnień organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce i zaprezentowano go z perspektywy prawnej. Pomimo istnienia literatury poświęconej polskiemu prawodawstwu antyterrorystycznemu ta tematyka wciąż pozostaje ciekawa i niewyczerpana, głównie z uwagi na brak kompleksowych, a jednocześnie zwięzłych opracowań ujmujących zadania wskazanych organów z perspektywy czterech faz realizowania czynności antyterrorystycznych. Składają się na nie działania zapobiegające zdarzeniom o charakterze terrorystycznym – powierzone do koordynacji Szefowi Agencji Bezpieczeństwa Wewnętrznego oraz działania w zakresie przygotowania do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym, reagowania w przypadku wystąpienia takich zdarzeń oraz odtwarzania zasobów przeznaczonych do reagowania na te zdarzenia – powierzone do koordynacji Ministrowi Spraw Wewnętrznych i Administracji.

Opisu przedmiotowej problematyki dokonano z perspektywy systemu antyterrorystycznego, zarówno w ujęciu podmiotowym – przez wskazanie organów zaliczanych do tego systemu i ich zadań, jak i przedmiotowym – przez przedstawienie procedur działania antyterrorystycznego, w ramach których są realizowane uprawnienia tych organów.

Niniejsze opracowanie jest próbą całościowego omówienia tej problematyki, z uwzględnieniem ponad sześciu lat doświadczeń związanych z funkcjonowaniem *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*.

Słowa kluczowe:

polskie ustawodawstwo antyterrorystyczne, ustawa o działaniach antyterrorystycznych, Agencja Bezpieczeństwa Wewnętrznego, minister spraw wewnętrznych i administracji

Jak wskazuje się w doktrynie prawniczej, (...) *do grupy pozakonstytucyjnych organów ochrony prawa należy zaliczyć prokuraturę oraz inne organy ścigania karnego. Odpowiadają one kryteriom organu ochrony prawa i znajdują pełne oparcie ustawowe.* (...) *Do grupy pozakonstytucyjnych organów ścigania karnego zalicza się liczne organy ścigania o proweniencji resortowej, wojskowej i administracyjnej*[1]. W ramach niniejszego opracowania przeprowadzono analizę zadań i uprawnień tych organów w zakresie zwalczania terroryzmu w Polsce. Punktem wyjścia i osią spajającą te rozważania jest analiza postanowień *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[2], która weszła w życie 2 lipca 2016 r. To właśnie w tej ustawie, jak wskazano w jej art. 1, określono zasady prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie realizowania tych działań i tym samym stworzono *de iure* system antyterrorystyczny w Polsce.

Warto zacząć od podkreślenia, że we wspomnianej ustawie zmaterializowały się zarówno postulaty doktryny prawniczej, jak i wnioski płynące z analiz prowadzonych od początku XXI w. w obszarze nauk o bezpieczeństwie, zakładające niezbędność istnienia takiej ustawy (...) *nie tylko dlatego, że zagrożenie terroryzmem w Polsce jest, w porównaniu z wieloma państwami Europy, znacząco wyższe, ale także dlatego, że działania antyterrorystyczne organów i innych instytucji państwa muszą wkraczać w sferę wolności i praw obywatelskich, a to już zagadnienie mające jednoznacznie kontekst konstytucyjny, konwencyjny (Konwencja Europejska z 1950 r.) i unijny*[3]. Ponadto dodawano wówczas, że:

> (...) w Polsce wciąż brakuje krajowego dokumentu, który określałby służbom mundurowym oraz instytucjom cywilnym zaangażowanym w przeciwdziałanie terroryzmowi ramy i granice podejmowanych działań oraz wskazywałby, do jakiego „stanu" dążymy i za pomocą jakich dopuszczalnych środków, zgodnych z ogólnie przyjętą strategią działania państwa, chcemy go osiągnąć. Brakuje także mechanizmu z wyraźnie zaznaczonym ośrodkiem decyzyjnym, który łączyłby wszystkie niezbędne obszary w jeden zintegrowany, ponadresortowy i ogólnonarodowy system walki z terroryzmem[4].

---

1 F. Prusak, *Niesądowe organy ochrony prawnej*, Warszawa 2004, s. 83.

2 Tekst jednolity: DzU z 2021 r. poz. 2234, ze zm.

3 L. Paprzycki, *Czy Polsce potrzebna jest ustawa antyterrorystyczna?*, w: *Terroryzm. Materia ustawowa?,* K. Indecki, P. Potejko (red.), Warszawa 2009, s. 6.

4 M. Adamczuk, P. Siejczuk, *Strategia obrony przed terroryzmem – cele i funkcje w systemie przeciwdziałania terroryzmowi*, w: *Problemy prawno-organizacyjne zwalczania terroryzmu w Polsce,* J. Szafrański, K. Liedel (red.), Szczytno 2011, s. 91.

Pomimo tak wyraźnie formułowanych postulatów oraz wieloetapowych działań organizacyjnych nakierowanych na stworzenie w Polsce systemu antyterrorystycznego, realizowanych głównie w ramach prac Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych[5], dopiero ustawa o działaniach antyterrorystycznych doprowadziła do formalnego ustanowienia tego systemu i jednocześnie precyzyjnie określiła m.in. zadania i obowiązki organów ścigania karnego w tym zakresie. Jak wskazano w uzasadnieniu do projektu tej ustawy, jej podstawowym celem było (...) *podniesienie efektywności polskiego systemu antyterrorystycznego, a tym samym zwiększenie bezpieczeństwa wszystkich obywateli RP*[6]. Miało to nastąpić m.in. przez wzmocnienie mechanizmów koordynacji działań, doprecyzowanie zadań poszczególnych służb i organów oraz zasad współpracy między nimi. Podczas prac legislacyjnych zwracano uwagę, że obowiązujące przepisy w zakresie zwalczania terroryzmu mają charakter rozproszony i nie zapewniają odpowiednich instrumentów prawnych i organizacyjnych pozwalających skutecznie przeciwdziałać istniejącym zagrożeniom. Nowa regulacja miała zintegrować działania organów ścigania karnego właściwych w sprawie zwalczania terroryzmu oraz jasno zarysować ich odpowiedzialność za poszczególne segmenty tych działań. W ten sposób miała bezpośrednio wpłynąć na (...) *szybkość i prawidłowość procesu decyzyjnego na poziomie strategicznym*[7].

Ustawa o działaniach antyterrorystycznych została konstrukcyjnie podzielona na siedem rozdziałów[8], przy czym fundament zawartych w niej rozwiązań został oparty na wyodrębnionych czterech fazach podejmowania czynności antyterrorystycznych. Składają się na nie: 1) działania zapobiegające zdarzeniom o charakterze terrorystycznym – powierzone Szefowi ABW; 2) przygotowanie do przejmowania kontroli nad zdarzeniami

[5] Szerzej na temat genezy systemu antyterrorystycznego w Polsce zob. P. Chomentowski, *Polski system antyterrorystyczny. Prawno-organizacyjne kierunki ewolucji*, Warszawa 2014, s. 81–95; M. Cichomski, I. Idzikowska-Ślęzak, *Poziom strategiczny polskiego systemu antyterrorystycznego – 15 lat Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*, „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 66–89.

[6] Rządowy projekt ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw, druk nr 516, https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=516 [dostęp: 25 IV 2022].

[7] Tamże.

[8] Szerzej na temat zakresu regulacyjnego ustawy zob. P. Burczaniuk, *Prawne aspekty walki z terroryzmem w krajowym porządku prawnym na tle wyzwań kształtowanych prawodawstwem europejskim*, „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 40–46.

o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć; 3) reagowanie w przypadku wystąpienia takich zdarzeń; 4) odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia – powierzone ministrowi właściwemu do spraw wewnętrznych. Podział na wymienione fazy jest elementem wspólnym systemu antyterrorystycznego ustanowionego tą ustawą i systemu, z którego de facto on wyewoluował, tj. systemu zarządzania kryzysowego określonego w *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[9]. W ustawie o działaniach antyterrorystycznych wymienione fazy zostały potraktowane w nieidentyczny sposób. Na pierwszy plan wysunięto dwa etapy – działania zapobiegające zdarzeniom (uregulowane w rozdziale 2) oraz podejmowanie czynności kontrterrorystycznych (uregulowane w rozdziale 4). Dużą wartością tej ustawy, na co zwraca uwagę Piotr Chorbot, jest to, że (...) *do momentu uchwalenia niniejszej ustawy nie było tak jednoznacznego rozdzielenia odpowiedzialności kompetencyjnej w kontekście problematyki antyterrorystycznej*[10].

Ustawa o działaniach antyterrorystycznych, aktualnie najważniejszy akt z punktu widzenia rozważań dotyczących zadań organów ścigania karnego w obszarze walki z terroryzmem, jest uzupełniona regulacjami sektorowymi, zwłaszcza objętymi przepisami kompetencyjnymi poszczególnych służb i organów. Bez ich uwzględnienia rozważania będące przedmiotem niniejszego opracowania nie byłyby kompletne.

Zasygnalizowania wymaga również to, że w szerokim ujęciu zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce wynikają z *Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[11], ustanawiającej mechanizmy przeciwdziałania finansowaniu terroryzmu, jak również z regulacji poświęconych stanom nadzwyczajnym, które z uwagi na ograniczenia objętościowe niniejszego opracowania nie zostaną szerzej omówione.

---

[9] Tekst jednolity: DzU z 2022 r. poz. 261, ze zm.

[10] P. Chorbot, *Ustawa o działaniach antyterrorystycznych. Komentarz do niektórych regulacji*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (red.), Warszawa 2017, s. 68.

[11] Tekst jednolity: DzU z 2022 r. poz. 593, ze zm.

Działania zapobiegające zdarzeniom o charakterze terrorystycznym

Szczególna pozycja Szefa ABW

Zgodnie z art. 3 ust. 1 ustawy o działaniach antyterrorystycznych Szef ABW odpowiada za zapobieganie zdarzeniom o charakterze terrorystycznym. Wybór przez ustawodawcę Szefa ABW na koordynatora działań organów ścigania karnego w fazie zapobiegania zdarzeniom terrorystycznym jawi się jako oczywisty, przede wszystkim w świetle przepisów kompetencyjnych ABW, doświadczeń, jakie ma ta służba, oraz jej zdolności organizacyjnych w tym obszarze, związanych głównie z jednostkami funkcjonującymi w jej strukturze – Centrum Antyterrorystycznym (CAT) oraz Centrum Prewencji Terrorystycznej (CPT).

Nawiązując do kompetencji ABW, trzeba wskazać, że zgodnie z art. 5 ust. 1 pkt 1 i 2 lit. a *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[12] do zadań Agencji należy rozpoznawanie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny oraz zapobieganie tym zagrożeniem, jak również rozpoznawanie i wykrywanie przestępstw, zwłaszcza terroryzmu, oraz zapobieganie im. Jak podkreśla Magdalena Gołaszewska, (...) *jako element zagrożenia bezpieczeństwa wewnętrznego bez wątpienia należy zakwalifikować także rozpoznawanie zagadnień związanych z działalnością terrorystyczną*[13]. Z kolei Tomasz Batory wskazuje, że (...) *przestępstwem ujętym w art. 5 ust 1 pkt 2 lit. a ustawy o ABW oraz AW jest terroryzm. Jednak odmiennie niż w wypadku szpiegostwa pojęcie to nie odnosi się do jednego artykułu KK. Warto zaznaczyć, iż KK nie posługuje się w ogóle nomenklaturą «terroryzm», ale pojęciem «przestępstwo o charakterze terrorystycznym». Definicja tego pojęcia została zawarta w art. 115 § 20 Kodeksu karnego*[14].

Tak wyrażona właściwość ABW oznacza, że spośród wszystkich polskich organów ścigania karnego to właśnie ta służba ma najszersze kompetencje w zakresie walki z terroryzmem. Jest to zresztą znamienna cecha

[12] Tekst jednolity: DzU z 2022 r. poz. 557, ze zm.

[13] M. Gołaszewska, *Zadania ABW w zakresie zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny*, w: *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (red.), Warszawa 2021, s. 46.

[14] T. Batory, *Zadania ABW w zakresie rozpoznawania, zapobiegania i wykrywania przestępstw*, w: *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (red.), Warszawa 2021, s. 73.

europejskich służb specjalnych o charakterze wewnętrznym, które z reguły mają wyznaczone zadania dotyczące szpiegostwa i terroryzmu. W kontekście powyższego zwraca uwagę, że poprzednik prawny ABW, jakim był Urząd Ochrony Państwa, już od chwili jego utworzenia 10 maja 1990 r. miał, zgodnie z art. 2 ust. 2 pkt 1 i 2 *Ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa*[15], wyznaczone zadania w zakresie rozpoznawania zagrożeń godzących m.in. w bezpieczeństwo państwa (obejmujących bez wątpienia zagrożenia terrorystyczne) i przeciwdziałania im oraz – wprost wyrażone – zadania w zakresie wykrywania przestępstw, m.in. terroryzmu, i zapobiegania im.

Ustawa o ABW oraz AW w art. 21 ust. 1 dookreśliła, że zadania ABW wskazane w art. 5, w tym te nakierowane na zwalczanie terroryzmu, są realizowane poprzez wykonywanie przez funkcjonariuszy ABW:

1) na poziomie identyfikacji i eliminacji zagrożeń – czynności operacyjno-rozpoznawczych i analityczno-informacyjnych w celu pozyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego;
2) na poziomie zwalczania przestępstw – czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych w celu rozpoznawania, wykrywania przestępstw i zapobiegania im oraz ścigania ich sprawców.

Szczegółowo te uprawnienia zostały ujęte w rozdziale 4 ustawy o ABW oraz AW. Warto zwrócić uwagę na doprecyzowanie w ustawie o działaniach antyterrorystycznych uprawnień ABW w zakresie działań antyterrorystycznych zapobiegających zdarzeniom o charakterze terrorystycznym. Analiza zakresu tych uprawnień pozwala postawić tezę, że w tej fazie walki z terroryzmem ustawodawca położył największy nacisk na znaczenie czynności analityczno-informacyjnych oraz operacyjno-rozpoznawczych. Należy to ocenić jako działanie racjonalne, gdyż w tej fazie służby mierzą się głównie z zagrożeniami terrorystycznymi, a nie z przestępstwami (poza czynnościami sprawczymi w zakresie przygotowania lub usiłowania), które z kolei są dominantą w fazie kolejnej, związanej z wystąpieniem już zdarzenia o charakterze terrorystycznym.

W przypadku czynności analityczno-informacyjnych ustawodawca podkreślił znaczenie wymiany informacji, ich agregacji i dalszej dystrybucji. Nałożył na Szefa ABW zadania w zakresie:

[15] DzU z 1990 r. nr 30 poz. 180.

1) koordynacji czynności analityczno-informacyjnych podejmowanych przez służby specjalne (w rozumieniu art. 11 ustawy o ABW oraz AW) – art. 5 ust. 1 ustawy;
2) koordynacji wymiany informacji przekazywanych przez Policję, Straż Graniczną, Straż Marszałkowską, Służbę Ochrony Państwa, Państwową Straż Pożarną, Generalnego Inspektora Informacji Finansowej, Krajową Administrację Skarbową, Żandarmerię Wojskową i Rządowe Centrum Bezpieczeństwa, dotyczących:
   a) zdarzeń o charakterze terrorystycznym (zdefiniowanych w art. 2 pkt 7 ustawy jako sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 kk, lub zagrożenie zaistnienia takiego przestępstwa),
   b) danych o osobach:
      – podejmujących działalność na rzecz organizacji terrorystycznych lub organizacji związanych z działalnością terrorystyczną lub członkach tych organizacji,
      – poszukiwanych, 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,
      – 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,
      – uczestniczących w szkoleniach terrorystycznych lub podejmujących podróż w celu popełnienia przestępstwa o charakterze terrorystycznym,

   przez gromadzenie, przetwarzanie i analizowanie tych informacji – art. 5 ust. 1 ustawy. Dane o wskazanych osobach podlegają ponadto wpisaniu do rejestru prowadzonego przez Szefa ABW, zgodnie z art. 6 ust. 1 ustawy, tworzonego z zachowaniem wymogów dotyczących ochrony informacji niejawnych;

3) odbierania od służb specjalnych i wskazanych powyżej podmiotów informacji służących realizacji działań antyterrorystycznych (zdefiniowanych jako działania organów administracji publicznej polegające na zapobieganiu zdarzeniom o charakterze terrorystycznym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć, reagowaniu w przypadku wystąpienia takich zdarzeń oraz usuwaniu ich skutków, w tym odtwarzaniu zasobów przeznaczonych do reagowania na nie). Informacje te muszą być przekazywane jako zaklasyfikowane do jednego z incydentów określonych jako katalog w rozporządzeniu wydanym przez ministra właściwego do spraw wewnętrznych, w porozumieniu z ministrem właściwym do spraw finansów publicznych i Ministrem Obrony Narodowej oraz po zasięgnięciu opinii Szefa ABW[16]. Wykaz ten zawiera obecnie listę 12 incydentów pogrupowanych w dwa obszary, tj. incydenty zagrażające bezpieczeństwu RP oraz incydenty związane z zagranicznymi przedstawicielstwami RP i obywatelami RP poza jej terytorium – art. 5 ust. 3 ustawy;
4) odbierania od organów administracji publicznej, właścicieli i posiadaczy obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej będących w ich posiadaniu informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury administracji publicznej lub infrastruktury krytycznej, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych istotnych z punktu widzenia bezpieczeństwa państwa – art. 4 ust. 2 ustawy;
5) nieodpłatnego dostępu do danych zgromadzonych w rejestrach publicznych i ewidencjach prowadzonych zarówno przez wskazanych powyżej w pkt 1 i 2 uczestników systemu antyterrorystycznego, jak i przez ministrów kierujących działami administracji rządowej, Szefa Urzędu do Spraw Cudzoziemców, Prezesa Urzędu Komunikacji Elektronicznej, Prezesa Urzędu Lotnictwa Cywilnego, Prezesa Państwowej Agencji Atomistyki, Zakład Ubezpieczeń Społecznych,

[16] Aktualnie jest to *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym* (DzU z 2017 r. poz. 1517 oraz *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 5 lutego 2019 r. zmieniająca rozporządzenie w sprawie katalogu incydentów o charakterze terrorystycznym,* DzU z 2019 r. poz. 317).

Prezesa Kasy Rolniczego Ubezpieczenia Społecznego, Komisję Nadzoru Finansowego, Głównego Geodetę Kraju, jednostki samorządu terytorialnego, Prokuratora Generalnego oraz jednostki organizacyjne im podległe lub przez nie nadzorowane – art. 11 pkt 1 ustawy.

Co ważne, na podstawie ustawy Szef ABW jest organem upoważnionym do otrzymywania i agregacji informacji, ale jednocześnie jest źródłem ich dystrybucji. Informacje są przekazywane:

1) zgodnie z art. 7 ustawy – na potrzeby najważniejszych organów państwa. Szef ABW ma obowiązek niezwłocznego przekazywania informacji mogących mieć istotne znaczenie dla zapobiegania zdarzeniom o charakterze terrorystycznym Prezydentowi Rzeczypospolitej Polskiej, Prezesowi Rady Ministrów, ministrowi właściwemu do spraw wewnętrznych, Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw zagranicznych, Ministrowi Koordynatorowi Służb Specjalnych, jeżeli został powołany[17];
2) zgodnie z art. 6 ust. 2 ustawy – na potrzeby innych służb specjalnych oraz wymienionych uczestników systemu antyterrorystycznego (Policji, Straży Granicznej, Straży Marszałkowskiej, Służbie Ochrony Państwa, Państwowej Straży Pożarnej, Generalnemu Inspektorowi Informacji Finansowej, Krajowej Administracji Skarbowej, Żandarmerii Wojskowej i Rządowemu Centrum Bezpieczeństwa), jak i innych organów administracji publicznej, w zakresie ich właściwości. Są to informacje (także w postaci bieżących analiz stanu zagrożenia zdarzeniem o charakterze terrorystycznym):
   a) służące realizacji działań antyterrorystycznych, klasyfikowanych zgodnie z katalogiem incydentów o charakterze terrorystycznym,
   b) zawarte w wykazie osób;

[17] Zakres normowania obejmujący w art. 7 ustawy „informacje mogące mieć istotne znaczenie dla zapobiegania zdarzeniom o charakterze terrorystycznym" i nakazujący odpowiednie stosowanie art. 18 ustawy o ABW oraz AW istotnie różnicuje się z zakresem normowania art. 6 ust. 3 ustawy, w którym jest mowa o „informacjach służących realizacji działań antyterrorystycznych". Przy szczególnym zakresie zastosowania art. 7, obejmującym najważniejsze organy państwowe, przemawia to za jego interpretacją i stosowaniem w szerokim zakresie, obejmującym m.in. informacje objęte niektórymi zakazami. Aktualne pozostają rozważania na temat korelacji art. 18 i art. 39 ust. 3 ustawy o ABW oraz AW podjęte w: P. Burczaniuk, *Zadania Szefa ABW w zakresie obowiązków informacyjnych*, w: *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (red.), Warszawa 2021, s. 17–39.

3) zgodnie z art. 4 ust. 1 ustawy – organom administracji publicznej, właścicielom i posiadaczom obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej. Są to informacje niezbędne do przeciwdziałania wystąpieniu zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze administracji publicznej lub infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, usunięcia tego rodzaju zagrożenia albo jego zminimalizowania.

Należy dodać, że zgodnie z art. 4 ust. 3 ustawy 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 ma prawo wydawać polecenia organom i podmiotom wskazanym powyżej w pkt 3 (z wyłączeniem najważniejszych osób w państwie) w celu przeciwdziałania tym zagrożeniom, ich usunięcia albo minimalizacji. Organy i podmioty mają obowiązek poinformować Szefa ABW o podjętych działaniach w tym zakresie. Omawiane uprawnienie Szefa ABW zostało implementowane do systemu antyterrorystycznego z systemu zarządzania kryzysowego, a dokładnie z art. 12a wspomnianej już ustawy o zarządzaniu kryzysowym, obowiązującym od września 2009 r.[18] do wejścia w życie ustawy antyterrorystycznej.

W przypadku czynności operacyjno-rozpoznawczych zgodnie z art. 8 ustawy Szefowi ABW powierzono ich koordynację w zakresie podmiotowym, gdy te czynności są podejmowane przez służby specjalne, Policję, Straż Graniczną, Krajową Administrację Skarbową i Żandarmerię Wojskową, oraz przedmiotowym, gdy dotyczą zdarzeń o charakterze terrorystycznym. Jedynym ustawowym doprecyzowaniem tego zadania jest otrzymane przez Szefa ABW uprawnienie wydawania wymienionym podmiotom zaleceń mających na celu usunięcie bądź zminimalizowanie zaistniałego zagrożenia terrorystycznego. Jak wskazuje Michał Gabriel-Węglowski, (...) *powstaje pytanie o wiążący charakter tych zaleceń.* (...) *Wynikająca jednak z niniejszej ustawy przewodnia rola ABW w przeciwdziałaniu zagrożeniu terrorystycznemu przemawia za przyjęciem, że wydane zalecenia każdorazowo*

[18] Dodanym *Ustawą z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym* (DzU z 2009 r. nr 131 poz. 1076).

wymagają wdrożenia przez pozostałe służby[19]. Ponadto z samej funkcji koordynacyjnej pełnionej przez Szefa ABW można wysnuć wniosek o zobowiązaniu wymienionych podmiotów do informowania go o zamiarze i prowadzeniu czynności operacyjno-rozpoznawczych dotyczących zdarzeń o charakterze terrorystycznym. Brak bowiem takiej informacji funkcjonalnie uniemożliwiałby wypełnianie przez Szefa ABW przypisanego mu zadania koordynacyjnego, w tym też wydawanie omówionych zaleceń. Na marginesie warto zwrócić uwagę, że w ramach rozwiązań dotyczących czynności operacyjno-rozpoznawczych ustawa przyznała Szefowi ABW dwa nowe uprawnienia do:

1) prowadzenia czynności inwigilacyjnych wobec cudzoziemców[20] – art. 9 ustawy;
2) dostępu do 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 pkt 2 ustawy.

Ponadto ustawa o działaniach antyterrorystycznych wprowadziła wiele kompleksowych zmian do ustawy o ABW oraz AW, których celem było podniesienie zdolności państwa w zakresie zapobiegania zagrożeniom terrorystycznym, a stanowiących sferę podstawowej odpowiedzialności ABW, w tym m.in. uprawnienia do:

1) tajnej współpracy z ABW sprawcy przestępstwa szpiegostwa lub podejrzanego o popełnienie przestępstwa o charakterze terrorystycznym – art. 22b ustawy o ABW oraz AW;
2) sporządzania oceny bezpieczeństwa systemów teleinformatycznych w celu zapobiegania i przeciwdziałania zdarzeniom o charakterze terrorystycznym oraz ich zwalczania – art. 32a ustawy o ABW oraz AW;
3) udzielania na żądanie Szefa ABW informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji systemów teleinformatycznych, w przypadku powzięcia informacji o wystąpieniu zdarzenia

[19] M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*, art. 8, Warszawa 2018, https://sip.lex.pl/#/commentary/587754148/551588/gabriel-weglowski-michal-dzialania-antyterrorystyczne-komentarz?cm=URELATIONS [dostęp: 28 IV 2022].

[20] Szczegółowe rozważania dotyczące tego uprawnienia pozostają poza zakresem tematycznym niniejszego opracowania. Zob. szerzej: M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*...

o charakterze terrorystycznym dotyczącego tych systemów – art. 32b ustawy o ABW oraz AW;

4) dokonywania przez ABW blokady dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym – art. 32c ustawy o ABW oraz AW.

Jak wynika z powyższego, ustawa o działaniach antyterrorystycznych uczyniła Szefa ABW odpowiedzialnym za zapobieganie zdarzeniom o charakterze terrorystycznym i wyposażyła go w dwa zasadnicze uprawnienia służące realizacji tego zadania w postaci funkcji koordynacyjnej nad czynnościami analityczno-informacyjnymi oraz operacyjno-rozpoznawczymi podejmowanymi w tym obszarze. Jak już wskazano, wybór przez ustawodawcę Szefa ABW do realizacji tego zadania był wyborem oczywistym, również z uwagi na posiadane ponadtrzydziestoletnie (uwzględniając okres funkcjonowania UOP) doświadczenie, z którego aktualnie korzystają przede wszystkim dwie wspomniane już jednostki organizacyjne ABW, tj. CAT oraz CPT.

Centrum Antyterrorystyczne odpowiada za koordynację działań podmiotów odpowiedzialnych za ochronę antyterrorystyczną Polski. Stąd też, jak się wydaje, założenie, że w CAT pełnią służbę nie tylko funkcjonariusze ABW, lecz także przedstawiciele pozostałych uczestników systemu antyterrorystycznego Polski. W art. 14 ustawy o działaniach antyterrorystycznych oraz w aktach wykonawczych wydanych na jej podstawie stworzono system organizacyjny, na którym w aspekcie praktycznym opiera się działanie CAT ABW i koordynacyjna rola Szefa ABW. Sprowadza się to do możliwości oddelegowania przedstawicieli innych służb specjalnych oraz Policji, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Generalnego Inspektora Informacji Finansowej, Krajowej Administracji Skarbowej, Żandarmerii Wojskowej i Rządowego Centrum Bezpieczeństwa do służby lub pracy w ABW. Osoby te realizują (...) *zadania w ramach kompetencji instytucji, którą reprezentują*[21]. Wybór tych podmiotów przez ustawodawcę nie jest przypadkowy, gdyż bez wątpienia stanowią one elementy systemu antyterrorystycznego RP, w którym każdy z nich, w zakresie swoich właściwości i z uwzględnieniem koordynacyjnej roli Szefa ABW, realizuje zadania na rzecz przeciwdziałania terroryzmowi.

[21] Serwis Rzeczpospolitej Polskiej gov.pl, Centrum Antyterrorystyczne (CAT ABW), https://www.gov.pl/web/mswia/abw [dostęp: 27 IV 2022].

Znaczenie innych służb

Zadania kontrterrorystyczne, w zakresie zbliżonym do zadań ABW, powierzono Agencji Wywiadu, która zgodnie z art. 6 ust. 1 pkt 5 i 7a ustawy o ABW oraz AW rozpoznaje m.in. międzynarodowy terroryzm i ekstremizm oraz zdarzenia o charakterze terrorystycznym skierowane przeciwko obywatelom lub mieniu RP poza granicami państwa, przeciwdziała i zapobiega im, z wyłączeniem zdarzeń o charakterze terrorystycznym wymierzonych przeciwko personelowi lub mieniu Sił Zbrojnych RP, przy czym te zadania wykonuje poza granicami RP.

Zadania kontrterrorystyczne są realizowane również przez pozostałe służby specjalne, w tym Służbę Kontrwywiadu Wojskowego. Zgodnie z art. 5 ust. 1 pkt 2a *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[22] SKW rozpoznaje i wykrywa zdarzenia i przestępstwa o charakterze terrorystycznym godzące w bezpieczeństwo potencjału obronnego państwa, Siły Zbrojne RP oraz jednostki organizacyjne Ministerstwa Obrony Narodowej i zapobiega im. Z kolei Służba Wywiadu Wojskowego, podobnie jak Agencja Wywiadu, zajmuje się zgodnie z art. 6 ust. 1 pkt 2 lit. b i pkt 3a ustawy o SKW oraz SWW rozpoznawaniem zagrożeń międzynarodowym terroryzmem i przeciwdziałaniem im oraz rozpoznawaniem zdarzeń o charakterze terrorystycznym wymierzonych przeciwko personelowi i mieniu Sił Zbrojnych RP poza granicami państwa, przeciwdziałaniem i zapobieganiem tym zdarzeniom oraz zwalczaniem ich skutków.

Dla funkcjonowania systemu antyterrorystycznego w Polsce duże znaczenie mają zadania w zakresie zwalczania terroryzmu przypisane Policji, które – co podkreśla się w doktrynie prawniczej[23] – w fazie zapobiegania zdarzeniom terrorystycznym nie są wymienione wprost w *Ustawie z dnia 6 kwietnia 1990 r. o Policji*[24]. Można je jednak wywieźć z brzmienia art. 1 ust. 2 pkt 1–3 tej ustawy, który wskazuje, że podstawowe zadania Policji obejmują:

1) ochronę życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra;
2) ochronę bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz w środkach

[22] Tekst jednolity: DzU z 2022 r. poz. 502, ze zm.

[23] Por. M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*...

[24] Tekst jednolity: DzU z 2021 r. poz. 1882, ze zm.

transportu publicznego i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania;
3) inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi.

W omawianym systemie ustawodawca przyznał ważne miejsce również Straży Granicznej, której zadania kontrterrorystyczne, podobnie jak w przypadku Policji, nie są wyrażone wprost, lecz funkcjonalnie wynikają z roli, jaką ta formacja odgrywa w ochronie granicy państwowej, kontroli ruchu granicznego oraz zapobieganiu i przeciwdziałaniu nielegalnej migracji (art. 1 ust. 1 *Ustawy z dnia 12 października 1990 r. o Straży Granicznej*[25]). Na mocy art. 1 ust. 2 pkt 5d tej ustawy Straż Graniczna ma obowiązek współdziałania z innymi organami i służbami w zakresie rozpoznawania zagrożeń terroryzmem i przeciwdziałania im.

Istotnym elementem systemu antyterrorystycznego w Polsce jest także Służba Ochrony Państwa, pomimo – analogicznie jak w przypadku Policji i Straży Granicznej – braku wyrażonej wprost kompetencji ustawowej, z uwagi na właściwość ogólną sprowadzającą się do ochrony osób i obiektów oraz rozpoznawania skierowanych przeciw nim przestępstw i zapobiegania im (art. 2 ust. 1 *Ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa*[26]). Podobną rolę w tym systemie odgrywa Straż Marszałkowska, realizująca zadania w zakresie ochrony Sejmu i Senatu (art. 1 ust. 1 *Ustawy z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej*[27]).

Działania pozostające w gestii Ministra Spraw Wewnętrznych i Administracji

Jak już wcześniej wspomniano, zgodnie z art. 3 ust. 2 ustawy o działaniach antyterrorystycznych minister właściwy do spraw wewnętrznych odpowiada za trzy z czterech faz podejmowania czynności antyterrorystycznych, tj. za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w wyniku zaplanowanych przedsięwzięć, reagowanie

[25] Tekst jednolity: DzU z 2022 r. poz. 1061, ze zm.

[26] Tekst jednolity: DzU z 2021 r. poz. 575, ze zm.

[27] Tekst jednolity: DzU z 2019 r. poz. 1940, ze zm.

w przypadku wystąpienia takich zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia.

W doktrynie prawniczej wskazuje się, że (...) *jednym z najistotniejszych rozwiązań ustawy o działaniach antyterrorystycznych z perspektywy przygotowania do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym oraz reagowania w przypadku wystąpienia takich zdarzeń, było przeniesienie na grunt ustawy instytucji stopni alarmowych i stopni alarmowych CRP*[28]. Z kolei fundamentem fazy reagowania stały się rozwiązania ujęte w rozdziale 4 ustawy, poświęconym działaniom na miejscu zdarzenia o charakterze terrorystycznym, w tym działaniom kontrterrorystycznym. Najważniejszy dla tego rozdziału art. 18 określa sposób wyznaczania kierującego działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym, podejmowanymi przez właściwe służby lub organy w ramach ich ustawowych zadań. Zasadniczo kierujący jest wyznaczany przez Komendanta Głównego Policji. W przypadku gdy do takiego zdarzenia dochodzi na obszarach lub w obiektach należących do Ministra Obrony Narodowej, przez niego nadzorowanych albo administrowanych, kierującego wyznacza ten minister. W ośmiu punktach zawartych w art. 20 ust. 1 ustawy zostały określone uprawnienia kierującego działaniami antyterrorystycznymi.

Z przedstawionych regulacji jasno wynika, że zadania koordynacyjne w tych trzech fazach powierzone Ministrowi Spraw Wewnętrznych i Administracji mogą być przez niego realizowane poprzez podmioty mu podległe lub przez niego nadzorowane, których listę określa *Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji*[29]. Zalicza się do nich: Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego Państwowej Straży Pożarnej, Komendanta Służby Ochrony Państwa, Szefa Obrony Cywilnej Kraju, Szefa Urzędu do Spraw Cudzoziemców, Inspektora Nadzoru Wewnętrznego (oraz dyrektora Zakładu Emerytalno-Rentowego MSWiA, który ze względu na zakres zadań nie uczestniczy w systemie antyterrorystycznym).

[28] Zob. szerzej: M. Cichomski, M. Horoszko, I. Idzikowska, *Przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym oraz reagowanie w przypadku wystąpienia takich zdarzeń w świetle rozwiązania ustawy o działaniach antyterrorystycznych – w kontekście zadań resortu spraw wewnętrznych*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 283.

[29] DzU z 2019 r. poz. 2264.

W tym kontekście należy wskazać, że ustawą o działaniach antyterrorystycznych ustawodawca znowelizował ustawy kompetencyjne wskazanych służb i wzmocnił ich uprawnienia niezbędne do realizacji tych zadań[30]. Bez wątpienia najważniejszą służbą w tym zakresie pozostaje Policja. Zgodnie z art. 1 ust. 2 pkt 3a ustawy o Policji jednym z podstawowych zadań tej formacji mundurowej jest prowadzenie działań kontrterrorystycznych w rozumieniu ustawy o działaniach antyterrorystycznych. Na marginesie trzeba wspomnieć, że 5 kwietnia 2019 r. wydzielono w składzie Policji służbę kontrterrorystyczną[31], dookreślając ją jednocześnie w art. 5c ustawy o Policji. Zgodnie z tą regulacją służbę kontrterrorystyczną Policji stanowią Centralny Pododdział Kontrterrorystyczny Policji „BOA" oraz samodzielne pododdziały kontrterrorystyczne Policji, które są odpowiedzialne za prowadzenie działań kontrterrorystycznych oraz wspieranie działań jednostek organizacyjnych Policji w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił i środków oraz specjalistycznej taktyki działania. W świetle omawianego znaczenia Policji dla realizacji zadań w zakresie kierowania działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym warto dodać, że ustawa o działaniach antyterrorystycznych przewidziała możliwość użycia oddziałów i pododdziałów Sił Zbrojnych RP do pomocy Policji w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego i tylko w sytuacji, gdy użycie oddziałów i pododdziałów Policji okaże się niewystarczające lub może okazać się niewystarczające. Nie bez znaczenia pozostaje w tym kontekście, przewidziane w art. 23 ustawy, uprawnienie do specjalnego użycia broni podczas działań kontrterrorystycznych. Stanowi ono odstępstwo od zasad używania broni palnej uregulowanych w *Ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej*[32], polegające na jej użyciu przeciwko osobie dokonującej zamachu albo biorącej lub przetrzymującej zakładnika, którego

[30] Zmiany wprowadzono w: *Ustawie z dnia 6 kwietnia 1990 r. o Policji, Ustawie z dnia 12 października 1990 r. o Straży Granicznej, Ustawie z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej* (t.j. DzU z 2021 r. poz. 869, ze zm. – w zakresie organizacji krajowego systemu ratowniczo-gaśniczego), *Ustawie z dnia 16 marca 2001 r. o Biurze Ochrony Rządu* (zmiany te zostały uwzględnione w *Ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa*).

[31] *Ustawa z dnia 9 listopada 2018 r. o zmianie ustawy o Policji oraz niektórych innych ustaw* (DzU z 2019 r. poz. 15). Wcześniej pododdziały antyterrorystyczne wchodziły w skład Policji (od wejścia w życie ustawy o Policji 10 maja 1990 r. do 12 października 1995 r.).

[32] Tekst jednolity: DzU z 2022 r. poz. 1416.

skutkiem może być śmierć lub bezpośrednie zagrożenie życia lub zdrowia tej osoby.

Ustawa o działaniach antyterrorystycznych uregulowała w sposób odrębny problematykę koordynacji działań służb i organów w przypadku zdarzenia o charakterze terrorystycznym poza granicami RP. Powierzono ją ministrowi właściwemu do spraw zagranicznych, we współpracy z Ministrem Koordynatorem Służb Specjalnych, a jeżeli zdarzenie zostało wymierzone przeciwko personelowi lub mieniu Sił Zbrojnych RP, wówczas koordynuje je Minister Obrony Narodowej, we współpracy z ministrem właściwym do spraw zagranicznych (art. 19 ustawy). Ustawa dopuściła również prowadzenie działań antyterrorystycznych na zasadach w niej określonych poza granicami RP, na akwenach polskiej strefy odpowiedzialności SAR, zgodnie z *Międzynarodową konwencją o poszukiwaniu i ratownictwie morskim, sporządzoną w Hamburgu dnia 27 kwietnia 1979 r.*[33]

Prokuratura i postępowanie przygotowawcze

Ważny element rozwiązań przewidzianych w ustawie o działaniach antyterrorystycznych stanowią przepisy szczególne dotyczące postępowania przygotowawczego. Jak wskazuje Wojciech Olsztyn, (...) *do tej pory wszelkie czynności procesowe odbywały się na zasadach kodeksu karnego oraz kodeksu postępowania karnego*[34]. Zmianę w tym zakresie wprowadziły właśnie uregulowania objęte rozdziałem V ustawy o działaniach antyterrorystycznych. Na podstawie art. 25 ustawy w przypadku podejrzenia lub usiłowania popełnienia albo przygotowania przestępstwa o charakterze terrorystycznym, w celu wykrycia lub zatrzymania albo przymusowego doprowadzenia osoby podejrzewanej, a także w celu znalezienia rzeczy mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym, prokurator może wydać postanowienie o przeprowadzeniu przeszukania pomieszczeń i innych miejsc znajdujących się na wskazanym w postanowieniu obszarze lub zatrzymaniu osoby podejrzewanej, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że osoba podejrzewana lub

[33] DzU z 1988 r. nr 27 poz. 184.

[34] W. Olsztyn, *Nowe rozwiązania w obszarze działań operacyjno-rozpoznawczych oraz procesowych wynikające z ustawy o działaniach antyterrorystycznych*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 329.

wymienione rzeczy na tym obszarze się znajdują. Takiego przeszukania i zatrzymania można dokonać o każdej porze doby.

Postępowanie przygotowawcze prowadzone w związku z podejrzeniem popełnienia przestępstwa o charakterze terrorystycznym znacznie usprawniło uprawnienie wynikające z art. 26 ustawy, umożliwiające sporządzenie postanowienia o przedstawieniu zarzutów na podstawie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych. Ponadto w tym przypadku sąd, na wniosek prokuratora, może zastosować tymczasowe aresztowanie na okres nieprzekraczający 14 dni, a samoistną przesłanką zastosowania tego tymczasowego aresztowania jest uprawdopodobnienie popełnienia, usiłowania lub przygotowania do popełnienia przestępstwa o charakterze terrorystycznym.

Ustawa o działaniach antyterrorystycznych znacznie znowelizowała regulacje Kodeksu karnego, wprowadzając m.in. karalność stadium przygotowania do popełnienia przestępstw przeciwko pokojowi, ludzkości oraz przestępstw wojennych określonych w: art. 117 kk (wszczęcie lub prowadzenie wojny napastniczej), art. 118 kk (ludobójstwo), art. 118a kk (udział w masowym zamachu przeciwko grupie ludności), art. 120 kk (stosowanie środków masowej zagłady), art. 122 kk (prowadzenie działań wojennych w sposób niezgodny z prawem międzynarodowym), art. 123 kk (zbrodnie wojenne przeciwko jeńcom wojennym lub ludności cywilnej), art. 124 kk (inne przypadki naruszenia prawa międzynarodowego podczas prowadzenia działań zbrojnych) oraz art. 125 kk (uszkadzanie lub przywłaszczenie dóbr kultury) oraz dodając w art. 259a i 259b nowe typy czynów zabronionych dotyczące prowadzenia działalności przez zagranicznych bojowników.

Podsumowanie

W powyższym tekście dokonano usystematyzowania oraz omówienia zadań i uprawnień organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce, analizując je również przez pryzmat ponad sześciu lat doświadczeń związanych z funkcjonowaniem ustawy o działaniach antyterrorystycznych. Można stwierdzić, że wspomniana ustawa odegrała swoją rolę, gdyż uporządkowała zadania oraz zespoliła działania organów ścigania karnego, wyposażając je jednocześnie w nowoczesne narzędzia umożliwiające realizację tych zadań. O jakości tej ustawy świadczy pozytywna ocena

merytoryczna, m.in. wyrażona w 2018 r. przez Jukkę Savolainena, dyrektora ds. odporności w Europejskim Centrum Doskonalenia przeciwko Zagrożeniom Hybrydowym w Helsinkach (HybridCoE). Uznał on, że ustawa to godny naśladowania przykład w zakresie rozwiązań legislacyjnych, które mogą posłużyć za rozwiązania modelowe oraz stanowić istotny wkład w rozwój ustawodawstw krajowych państw UE i NATO w kontekście „odporności prawnej" na zagrożenia o charakterze hybrydowym[35]. Równie pozytywnie wypadła praktyczna weryfikacja rozwiązań zawartych w tej ustawie – nie doszło do zastosowania w praktyce wielu jej rozwiązań dotyczących działań antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym.

Biorąc jednak pod uwagę, że walki z terroryzmem nigdy nie można uznać za temat zamknięty, analiza modus operandi sprawców działań terrorystycznych powinna nieustannie iść w ślad za analizą potrzeb zmian prawnych, podejmowanych zarówno na poziomie poszczególnych państw, jak i przede wszystkim w ramach wspólnoty międzynarodowej borykającej się z tożsamymi zagrożeniami. W tym kontekście można wysunąć kilka postulatów legislacyjnych, które płyną z doświadczeń związanych ze stosowaniem ustawy o działaniach antyterrorystycznych.

Po pierwsze, od czasu jej powstania zwracano uwagę na nierównowagę treściową rozwiązań nią objętych względem poszczególnych faz podejmowania czynności antyterrorystycznych. Jak wskazano wcześniej, ustawodawca położył główny nacisk merytoryczny na rozwiązania objęte fazą działań zapobiegających zdarzeniom o charakterze terrorystycznym (wobec której przepisy ustawy wypełniają blisko połowę jej treści, tj. 12 z 26). Warto zastanowić się, czy pozostały zakres rozwiązań obejmujących trzy pozostałe fazy działań, tj. przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w wyniku zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń, odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia, stanowi kompleksowe instrumentarium, które w praktyce pozwoli zarządzać odpowiedzią na zdarzenia terrorystyczne. Zagadnienie to wymaga – jak się wydaje – szczegółowych analiz, które powinien podejmować przede wszystkim odpowiedzialny za nie resort spraw wewnętrznych. Jednak skuteczność działań pierwszej fazy koordynowanej przez Szefa ABW często czyni te rozważania teoretycznymi, gdyż doświadczenia praktyczne mogą

[35] Por. S. Żaryn, *Polska antyterrorystycznym wzorem*, wGospodarce, 28 XII 2018 r., https://wgospodarce.pl/opinie/58189-polska-antyterrorystycznym-wzorem [dostęp: 29 IV 2022].

płynąć jedynie z przeprowadzanych ćwiczeń, w tym jakże ważnych ćwiczeń zarządzania kryzysowego NATO – CMX (ang. Crisis Management Exercise).

Po drugie, pomimo szerokiego uregulowania działań podejmowanych w pierwszej fazie realizowania czynności antyterrorystycznych ewentualnego doprecyzowania – głównie z uwagi na brak definicji ustawowych – wymaga współpraca przy czynnościach operacyjno-rozpoznawczych podejmowanych przez poszczególne służby, zarówno specjalne, jak i te o charakterze policyjnym. Dotyczy to zwłaszcza zasadności doprecyzowania zasad i sposobu sprawowania koordynacyjnej roli przez Szefa ABW, z uwzględnieniem zadań dotyczących nadzoru i kontroli działalności służb oraz koordynowania ich działalności powierzonych Prezesowi Rady Ministrów oraz Ministrowi Koordynatorowi Służb Specjalnych.

Po trzecie, w najbliższym czasie najważniejszym wyzwaniem, z którym będzie musiał się zmierzyć prawodawca krajowy i europejski, będzie zapewne konieczność dostosowania regulacji antyterrorystycznych do zmieniającego się paradygmatu zagrożeń bezpieczeństwa państwa (wspólnoty międzynarodowej). Pojawienie się zagrożeń ujmowanych łącznie jako zagrożenia asymetryczne (hybrydowe), w których źródłem zagrożenia może być zarówno inne państwo, jak i podmiot pozapaństwowy, a zakres stosowanych działań niekonwencjonalnych prowadzi do rozmycia zakresów definicyjnych klasycznych przestępstw, głównie takich, jak terroryzm, szpiegostwo czy wojna napastnicza, wymaga – w celu właściwego im przeciwdziałania – dokonania istotnych modyfikacji. Zmiany będą musiały być wprowadzone zarówno na poziomie regulacji karnej materialnej, procesowej, jak i, a może przede wszystkim, ustrojowej organów ochrony prawnej, na czele z przepisami kompetencyjnymi (zadaniami i uprawnieniami) służb specjalnych. Ta problematyka powinna stać się przedmiotem odrębnych, szerzej zakrojonych rozważań.

Bibliografia

Burczaniuk P., *Prawne aspekty walki z terroryzmem w krajowym porządku prawnym na tle wyzwań kształtowanych prawodawstwem europejskim*, „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 29–65.

Chomentowski P., *Polski system antyterrorystyczny. Prawno-organizacyjne kierunki ewolucji*, Warszawa 2014.

Cichomski M., Idzikowska-Ślęzak I., *Poziom strategiczny polskiego systemu antyterrorystycznego – 15 lat Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*, „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 66–89.

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz*, Warszawa 2018, Lex/el.

Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016.

Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego, P. Burczaniuk (red.), Warszawa 2021.

Problemy prawno-organizacyjne zwalczania terroryzmu w Polsce, J. Szafrański, K. Liedel (red.), Szczytno 2011.

Prusak F., *Niesądowe organy ochrony prawnej*, Warszawa 2004.

Terroryzm. Materia ustawowa?, K. Indecki, P. Potejko (red.), Warszawa 2009.

Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia, P. Burczaniuk (red.), Warszawa 2017.

Źródła internetowe

Żaryn S., *Polska antyterrorystycznym wzorem*, wGospodarce, 28 XII 2018 r., https://wgospodarce.pl/opinie/58189-polska-antyterrorystycznym-wzorem [dostęp: 29 IV 2022].

Akty prawne

Międzynarodowa konwencja o poszukiwaniu i ratownictwie morskim, sporządzona w Hamburgu dnia 27 kwietnia 1979 r. (DzU z 1988 r. nr 27 poz. 184).

Ustawa z dnia 9 listopada 2018 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (DzU z 2019 r. poz. 15).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. DzU z 2022 r. poz. 593, ze zm.).

Ustawa z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej (t.j. DzU z 2019 r. poz. 1940, ze zm.).

Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (t.j. DzU z 2021 r. poz. 575, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2021 r. poz. 2234, ze zm.).

Ustawa dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (t.j. DzU z 2022 r. poz. 1416).

Ustawa z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym (DzU z 2009 r. nr 131 poz. 1076).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2022 r. poz. 261, ze zm.).

Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. DzU z 2022 r. poz. 502, ze zm.).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. DzU z 2022 r. poz. 557).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2022 r. poz. 1138).

Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (t.j. DzU z 2021 r. poz. 869, ze zm. – w zakresie organizacji krajowego systemu ratowniczo-gaśniczego).

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j. DzU z 2022 r. poz. 1061, ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. DzU z 2021 r. poz. 1882, ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (DzU z 1990 r. nr 30 poz. 180).

Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (DzU z 2019 r. poz. 2264).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 5 lutego 2019 r. zmieniająca rozporządzenie w sprawie katalogu incydentów o charakterze terrorystycznym (DzU z 2019 r. poz. 317).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym (DzU z 2017 r. poz. 1517).

DOI: 10.4467/27204383TER.22.018.16338

ORCID: 0000-0003-3707-7856
ORCID: 0000-0002-2012-4954

MARIUSZ CICHOMSKI
ILONA IDZIKOWSKA-ŚLĘZAK

Stopnie alarmowe – praktyczny i prawny wymiar ich stosowania

Abstrakt

Stopnie alarmowe – jako instytucja prawna unormowana obecnie w rozdziale 3. *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*, mająca swój rodowód jeszcze w *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* – w przypadku ich zastosowania w istotny sposób mogą oddziaływać zarówno na organy administracji publicznej, jak i na wiele podmiotów, a w określonych przypadkach na ogół społeczeństwa. Siedem lat funkcjonowania stopni alarmowych w aktualnej formule pozwala na podjęcie próby ich opisu i dokonania kilkuaspektowej oceny.

W artykule omówiono stopnie alarmowe na dwóch płaszczyznach – rzeczywistego wykorzystywania tej instytucji prawnej, zwłaszcza w kontekście tego, czy i w jakich przypadkach są one zarządzane, oraz adekwatności rozwiązań prawnych z perspektywy założonych celów, z uwzględnieniem zarówno praktycznego wymiaru stosowania stopni alarmowych, jak i poprawności konstrukcyjnej.

Słowa kluczowe:

stopnie alarmowe, stopnie alarmowe CRP, ustawa o działaniach antyterrorystycznych, terroryzm, zagrożenia o charakterze terrorystycznym

Podstawy prawne i istota stopni alarmowych

Należy nadmienić, że stopnie alarmowe nie są instytucją prawną, która w Polsce obowiązuje dopiero od 2016 r., tj. od chwili wprowadzenia ich do polskiego porządku prawnego przepisami prawa powszechnie obowiązującego, czyli *Ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[1].

Po raz pierwszy stopnie alarmowe w kontekście zagrożeń o charakterze terrorystycznym wprowadzono na grunt polski *Zarządzeniem nr 74 Prezesa Rady Ministrów z dnia 12 października 2011 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego*[2], które na krótko przed wejściem w życie ustawy o działaniach antyterrorystycznych zastąpiono *Zarządzeniem nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego*[3]. Oba te zarządzenia wydano na podstawie art. 7 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[4]. Wprowadzały one wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego, uwzględniający przedsięwzięcia i procedury wynikające z Systemu Reagowania Kryzysowego Organizacji Traktatu Północnoatlantyckiego (NATO)[5] oraz określały organy odpowiedzialne za ich uruchamianie. Oprócz wspomnianego wykazu przedsięwzięć wynikających z członkostwa Polski w NATO zawarto tu również stopnie alarmowe, a od momentu wejścia w życie zarządzenia nr 18 z 2 marca 2016 r. – również stopnie alarmowe dla zagrożeń w cyberprzestrzeni RP, nazwane „stopniami alarmowymi CRP".

Warto jednak zauważyć, że dopiero ustawą o działaniach antyterrorystycznych wprowadzono system określania stopni alarmowych i stopni alarmowych CRP, które byłyby powszechnie obowiązujące i tym samym miałyby walor skuteczności poza organami, służbami i instytucjami również dla innych jednostek organizacyjnych oraz społeczeństwa, ponieważ (...) *dotychczasowy system, obowiązujący na podstawie zarządzenia nr 18 Prezesa Rady Ministrów z 2 marca 2016 r. w sprawie wykazu przedsięwzięć*

---

1 Tekst jednolity: DzU z 2021 r. poz. 2234, ze zm.

2 Niepublikowane (przyp. red.).

3 Tekst zarządzenia zob. https://www.stawiguda.pl/userfiles/OC/Komunikaty_zew/Zarz%C4%85dzenie%20nr%2018%20Prezesa%20Rady%20Ministr%C3%B3w%20z%20dnia%202%20marca%202016%20r.pdf.

4 Tekst jednolity: DzU z 2022 r. poz. 261, ze zm.

5 NATO Crisis Response System Manual.

i procedur systemu zarządzania kryzysowego obejmował wyłącznie administrację rządową[6].

System ten został w dużej mierze transponowany z przepisów zawartych w załączniku nr 1 wspomnianego zarządzenia nr 18 z 2 marca 2016 r. obowiązujących w chwili wejścia w życie ustawy o działaniach antyterrorystycznych. Dokonanie przedmiotowej zmiany uzasadniano tym, że stopnie alarmowe dotyczą nie tylko organów administracji rządowej, lecz także innych jednostek organizacyjnych oraz obywateli, w związku z czym za niewystarczające uznano ich uregulowanie na poziomie zarządzenia. Wprowadzenie systemu stopni alarmowych na poziomie aktu prawa powszechnie obowiązującego umożliwiło jednocześnie rozszerzenie katalogu podmiotów obowiązanych do podjęcia stosownych działań (ograniczonego wcześniej do organów administracji rządowej)[7]. W komentarzu do ustawy o działaniach antyterrorystycznych zwrócono dodatkowo uwagę, że poszczególnym stopniom zagrożenia przypisano określone kolory[8]. *W Polsce oznaczenia barwne stosowane były również w przeszłości, ustawa o działaniach antyterrorystycznych nie wprowadza jednak takiej klasyfikacji*[9].

Należy również, w ślad za uzasadnieniem projektu ustawy o działaniach antyterrorystycznych, podkreślić, że system stopni alarmowych jest niezależny od możliwości wprowadzenia stanów nadzwyczajnych, przewidzianych w:

– *Ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości*

---

[6] P. Chorbot, *Ustawa o działaniach antyterrorystycznych. Komentarz do niektórych regulacji*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia,* P. Burczaniuk (red.), Warszawa 2017, s. 71.

[7] Uzasadnienie do projektu ustawy o działaniach antyterrorystycznych, https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=516 [dostęp: 2 VII 2022]; por. M. Cichomski, M. Horoszko, I. Idzikowska, *Przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym oraz reagowanie w przypadku wystąpienia takich zdarzeń w świetle rozwiązań ustawy o działaniach antyterrorystycznych – w kontekście zadań resortu spraw wewnętrznych,* w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 283–287.

[8] Por. *Kolory, stopnie i terminologia NATO. Jak odczytać alerty terrorystyczne*, TVP Info, 23 III 2016 r., https://www.tvp.info/24554977/kolory-stopnie-i-terminologia-nato-jak-odczytac-alerty-terrorystyczne [dostęp: 7 XII 2018].

[9] P. Łabuz, T. Safjański, W. Zubrzycki, *Ustawa o działaniach antyterrorystycznych. Komentarz*, Warszawa 2019, dostęp przez System Informacji Prawnej Legalis, sip.legalis.pl [dostęp: 20 VII 2022].

konstytucyjnym organom Rzeczypospolitej Polskiej[10] – w odniesieniu do zagrożenia o charakterze terrorystycznym lub działań w cyberprzestrzeni jako przesłanki do wprowadzenia stanu wojennego i użycia Sił Zbrojnych RP;
– *Ustawie z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*[11] – w odniesieniu do zagrożenia o charakterze terrorystycznym lub zdarzenia w cyberprzestrzeni jako przesłanki do wprowadzenia stanu klęski żywiołowej i użycia Sił Zbrojnych RP;
– *Ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym*[12] – w odniesieniu do zagrożenia o charakterze terrorystycznym lub działań w cyberprzestrzeni jako przesłanki do wprowadzenia stanu wyjątkowego i użycia Sił Zbrojnych RP.

Przygotowując rozwiązania ustawy o działaniach antyterrorystycznych dotyczące systemu stopni alarmowych, założono, że jeśli te instrumenty zostaną wykorzystane i okażą się niewystarczające w zapobieganiu zagrożeniom lub reagowaniu na nie, będzie to stanowiło przesłankę do wprowadzenia odpowiedniego stanu nadzwyczajnego. W związku z powyższym w wymienionych ustawach pozostawiono przepisy odnoszące się do zagrożeń o charakterze terrorystycznym[13]. Wydaje się to oczywiste zarówno z perspektywy konstytucyjnych podstaw ustaw dotyczących stanów nadzwyczajnych (art. 228 *Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r.*[14]), jak i przesłanek wprowadzenia poszczególnych stanów nadzwyczajnych (zwłaszcza stanu wyjątkowego, który zgodnie z art. 230 Konstytucji RP może być wprowadzony w razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego).

Konstrukcja stopni alarmowych w świetle uregulowań ustawy o działaniach antyterrorystycznych może być rozpatrywana na kilku płaszczyznach, w tym:
– przedmiotowej – w tym zakresie można wyodrębnić stopnie alarmowe sensu stricto oraz stopnie alarmowe CRP,
– stopnia zagrożenia – w czterostopniowej skali,

[10] Tekst jednolity: DzU z 2017 r. poz. 1932, ze zm.

[11] Tekst jednolity: DzU z 2017 r. poz. 1897.

[12] Tekst jednolity: DzU z 2017 r. poz. 1928.

[13] Uzasadnienie do projektu ustawy o działaniach antyterrorystycznych…

[14] DzU z 1997 r. nr 78 poz. 483, ze zm.

– miejscowej – dotyczy stopni alarmowych obowiązujących na terenie Polski, w tym na całym terytorium lub na określnych obszarach, i poza jej granicami, ale w ramach polskiej jurysdykcji.

W przypadku pierwszej z płaszczyzn na podstawie art. 15 ustawy o działaniach antyterrorystycznych można rozróżnić dwa rodzaje stopni alarmowych: 1) stopnie alarmowe sensu stricto (określenie wprowadzone na potrzeby niniejszego artykułu) oraz 2) stopnie alarmowe CRP, wprowadzane w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej.

Wyodrębnienie kategorii „stopnie alarmowe sensu stricto" wynika z tego, że ustawodawca posługuje się terminem „stopnie alarmowe" w dwóch okolicznościach: 1) w celu określenia poszczególnych stopni, które mogą być wprowadzone w przypadku zagrożenia wystąpieniem wszystkich kategorii zdarzeń o charakterze terrorystycznym oraz 2) wystąpienia takiego zdarzenia poza zdarzeniami w cyberprzestrzeni – art. 15 ust. 1 ustawy o działaniach antyterrorystycznych. Ustawodawca używa tego pojęcia również jako ogólnego określenia stosowanego dla całości tej instytucji prawnej (zarówno stopni alarmowych sensu stricto, jak i stopni alarmowych CRP), co ma swoje odzwierciedlenie m.in. w tytule rozdziału 3. ustawy o działaniach antyterrorystycznych – *Stopnie alarmowe,* a zatem traktującym łącznie o wszystkich rodzajach stopni alarmowych, w tym stopniach alarmowych CRP (można wówczas mówić o stopniach alarmowych sensu largo).

Rozpatrując stopnie alarmowe w kontekście stopnia zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, ustawodawca wzorował się na terminologii stosowanej w ramach systemu reagowania kryzysowego NATO i wprowadził czterostopniową skalę stopni alarmowych – analogiczną w przypadku stopni alarmowych sensu stricto i stopni alarmowych CRP. W przypadku stopni alarmowych sensu stricto wyróżnił:

– pierwszy stopień alarmowy – stopień ALFA,
– drugi stopień alarmowy – stopień BRAVO,
– trzeci stopień alarmowy – stopień CHARLIE,
– czwarty stopień alarmowy – stopień DELTA.

W przypadku stopni alarmowych CRP odpowiednio:

– pierwszy stopień alarmowy CRP – stopień ALFA-CRP,
– drugi stopień alarmowy CRP – stopień BRAVO-CRP,
– trzeci stopień alarmowy CRP – stopień CHARLIE-CRP,
– czwarty stopień alarmowy CRP – stopień DELTA-CRP.

Na analogię przyjętej systematyki wskazują również określone łącznie dla obu kategorii stopni alarmowych, tj. stopni alarmowych sensu stricto i stopni alarmowych CRP, przesłanki wprowadzania poszczególnych z nich w zależności od natężenia zagrożenia oraz od szczegółowości i wiarygodności informacji na jego temat.

Zarówno pierwszy stopień alarmowy, jak i pierwszy stopień alarmowy CRP można wprowadzić w sytuacji, w której uzyskano informację o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, jednak zarówno rodzaj tego potencjalnego zagrożenia, jak i jego zakres są trudne do przewidzenia.

Kolejne stopnie alarmowe i stopnie alarmowe CRP wprowadza się wraz ze wzrostem szczegółowości i wiarygodności dostępnych informacji, jak też wynikającego z nich prawdopodobieństwa wystąpienia zdarzenia o charakterze terrorystycznym.

Stopień alarmowy BRAVO i stopień alarmowy BRAVO-CRP ma zastosowanie w przypadku zwiększonego i przewidywalnego zagrożenia, gdy konkretny cel ataku nadal nie jest zidentyfikowany. Z kolei możliwość wprowadzenia stopni alarmowych CHARLIE i CHARLIE-CRP ustawodawca uzależnił od wystąpienia łącznie lub osobno kilku przesłanek, z których jako pierwszą wskazał faktyczne wystąpienie zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym, o ile ten atak jednocześnie godzi w bezpieczeństwo lub porządek publiczny albo w bezpieczeństwo RP, albo w bezpieczeństwo innego państwa czy organizacji międzynarodowej, ale jednocześnie oddziałuje na RP i staje się dla niej potencjalnym zagrożeniem. Ponadto ustawodawca przewidział możliwość wprowadzenia trzeciego stopnia alarmowego (zarówno sensu stricto, jak i stopnia alarmowego CRP), w przypadku jeśli informacje o planowanym zdarzeniu o charakterze terrorystycznym na terytorium RP są wiarygodne i potwierdzone. Jako trzecią przesłankę wskazał, że uzyskane informacje są wiarygodne i potwierdzone, a odnoszą się do planowanego zdarzenia o charakterze terrorystycznym, (...) *którego skutki mogą dotyczyć obywateli polskich przebywających za granicą lub instytucji polskich albo polskiej infrastruktury mieszczących się poza granicami Rzeczypospolitej Polskiej*[15].

Przesłankami wprowadzenia czwartego stopnia (scharakteryzowanymi przez ustawodawcę łącznie w odniesieniu do stopni sensu stricto

[15] Ustawa o działaniach antyterrorystycznych, art. 15 ust. 5 pkt 3.

i stopni CRP), podobnie jak w przypadku wprowadzenia trzeciego stopnia mogącymi wystąpić łącznie lub osobno, są:

- wystąpienie zdarzenia o charakterze terrorystycznym, przy czym, jak przy wprowadzeniu trzeciego stopnia alarmowego, zdarzenie to godzi w bezpieczeństwo lub porządek publiczny albo bezpieczeństwo RP, albo bezpieczeństwo innego państwa lub organizacji międzynarodowej i jednocześnie stwarza zagrożenie dla RP;
- informacje świadczące o zaawansowanej fazie przygotowań do zdarzenia o charakterze terrorystycznym na terytorium RP;
- informacje wskazujące na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym, które ma być wymierzone w obywateli polskich przebywających za granicą lub w instytucje polskie, lub w polską infrastrukturę mieszczącą się poza granicami RP, które jednocześnie świadczą o nieuchronności zajścia takiego zdarzenia.

Ze względów praktycznych ustawodawca przewidział możliwość wprowadzania stopni zarówno wyższych, jak i niższych niż uprzednio wprowadzone, z pominięciem stopni pośrednich. Co istotne – w ustawie zawarto także możliwość wprowadzania kategorii stopni alarmowych sensu stricto i stopni alarmowych CRP rozdzielnie lub łącznie, przy czym poziom określony dla jednej kategorii nie determinuje w żaden sposób poziomu określonego dla drugiej, np. w 2022 r. są utrzymywane jednocześnie drugi stopień alarmowy sensu stricto, czyli stopień alarmowy BRAVO, oraz trzeci stopień alarmowy CHARLIE-CRP.

Z uwagi na możliwość uwarunkowania miejscowego zakresu obowiązywania danego stopnia, o czym będzie mowa dalej przy omawianiu trzeciej ze wskazanych powyżej płaszczyzn rozpatrywania stopni alarmowych, ustawodawca przewidział także możliwość jednoczesnego obowiązywania na danym terenie różnych stopni alarmowych i wskazał w art. 15 ust. 10 ustawy o działaniach antyterrorystycznych, że w tego rodzaju sytuacji należy wykonywać zadania przewidziane dla stopnia wyższego.

Mając na uwadze związek stopni alarmowych z dodatkowymi obowiązkami po stronie instytucji publicznych, a także, w niektórych przypadkach, z ograniczeniami swobód obywatelskich, w ustawie podkreślono, że zarówno stopnie alarmowe sensu stricto, jak i stopnie alarmowe CRP odwołuje się (...) *niezwłocznie po minimalizacji zagrożenia lub skutków*

zdarzenia będącego przesłanką do ich wprowadzenia[16]. Można tu dostrzec jeszcze jeden zamiar ustawodawcy – stopnie alarmowe nie mają służyć ogólnemu i bieżącemu opisowi poziomu zagrożenia terrorystycznego w Polsce, a powinny być wprowadzane jedynie w przypadku wystąpienia mniej lub bardziej skonkretyzowanego zagrożenia (albo w przypadku wystąpienia zdarzenia o charakterze terrorystycznym) i możliwie pilnie odwoływane po jego ustaniu (chyba że w samym zarządzeniu o wprowadzeniu stopnia alarmowego jest zawarta norma derogacyjna). W związku z tym nie wprowadzono konstrukcji „stopnia zerowego". Samo obowiązywanie stopnia alarmowego ma natomiast obligować określone podmioty do podjęcia ponadstandardowych i adekwatnych do zagrożenia działań. Przykładowo – na podstawie ogólnej oceny sytuacji geopolitycznej w Europie Środkowo-Wschodniej można stwierdzić, że poziom zagrożenia terrorystycznego w Polsce jest średni, a nie znikomy czy niski, i jednocześnie nie wprowadzać stopnia alarmowego.

Przechodząc do trzeciej płaszczyzny rozpatrywania stopni alarmowych, należy zauważyć, że w art. 16 ust. 1 przewidziano możliwość obszarowego ograniczenia miejsca, na którym wprowadzane stopnie alarmowe będą miały zastosowanie, przy czym ustawodawca również w tym przypadku nie ograniczył tej możliwości jedynie do stopni alarmowych sensu stricto, ale dopuścił jej zastosowanie również do stopni alarmowych CRP. W praktyce stopnie alarmowe CRP zarządzano dotychczas tylko na terytorium całego kraju (nie można jednak wykluczyć, że informacja o ewentualnym zagrożeniu mogłaby dotyczyć np. systemów teleinformatycznych określonego organu, w rezultacie czego nieuzasadnione byłoby wprowadzanie stopnia alarmowego CRP na terenie całego państwa). Ustawa przewiduje możliwość wprowadzenia obu kategorii stopni alarmowych:

- na całym terytorium RP,
- na obszarze jednej lub kilku jednostek podziału terytorialnego kraju,
- na obszarze określonym w sposób inny niż przez odniesienie do jednostek podziału terytorialnego kraju,
- dla określonych obiektów jednostek organizacyjnych administracji publicznej, prokuratury, sądów lub innych obiektów infrastruktury administracji publicznej lub infrastruktury krytycznej[17].

[16] Tamże, art. 15 ust. 10.

[17] Tamże, art. 16 ust. 1 pkt 1–4.

We wskazanym przepisie zawarto także możliwość wprowadzenia stopnia alarmowego rozumianego sensu stricto lub stopnia alarmowego CRP także w przypadku, gdy (...) *skutki zdarzenia o charakterze terrorystycznym mogą dotyczyć obywateli polskich przebywających za granicą Rzeczypospolitej Polskiej lub instytucji polskich albo polskiej infrastruktury mieszczących się poza granicami Rzeczypospolitej Polskiej innych niż placówki zagraniczne Rzeczypospolitej Polskiej w rozumieniu ustawy z dnia 21 stycznia 2021 r. o służbie zagranicznej*[18] (t.j. DzU z 2022 r. poz. 1076, ze zm. – przyp. red.).

Z kolei w art. 16 ust. 2 ustawy przewidziano możliwość wprowadzenia ww. kategorii stopni alarmowych:

- dla określonych placówek zagranicznych RP w rozumieniu ustawy o służbie zagranicznej,
- w odniesieniu do systemów teleinformatycznych ministra właściwego do spraw zagranicznych.

Procedura wprowadzania stopni alarmowych pozostaje zróżnicowana, ale nie ze względu na te dwie kategorie przedmiotowe rozróżnienia stopni (stopnie alarmowe sensu stricto i stopnie alarmowe CRP), lecz w zależności od zakresu ich obszarowego obowiązywania.

Organem wprowadzającym stopnie alarmowe w drodze zarządzenia – w wariancie, który na potrzeby artykułu można określić jako podstawowy – jest Prezes Rady Ministrów. W sytuacjach skatalogowanych w art. 16 ust. 1, a zatem odnoszących się przede wszystkim do terytorium kraju, przed wydaniem tego rodzaju zarządzenia zasięga on opinii ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego – organów odpowiedzialnych za bezpieczeństwo wewnątrz kraju. Wskazanie ich jest logiczną konsekwencją art. 3 ustawy o działaniach antyterrorystycznych, zgodnie z którym Szef ABW odpowiada za zapobieganie zdarzeniom o charakterze terrorystycznym, a minister właściwy do spraw wewnętrznych za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia.

W sytuacjach opisanych w art. 16 ust. 2, a więc w przypadku wprowadzania stopni alarmowych w placówkach zagranicznych RP lub w odniesieniu do systemów teleinformatycznych pozostających w gestii ministra właściwego do spraw zagranicznych (czyli – jak można zakładać – w obu

[18] Tamże, art. 16 ust. 1 pkt 5.

przypadkach poza granicami kraju, ale w obszarach polskiej jurysdykcji), podmiotami opiniującymi są minister właściwy do spraw zagranicznych oraz Szef Agencji Wywiadu.

Rozwiązanie to – zgodne z zakresem kompetencji poszczególnych organów opiniujących – ma również bezpośrednie przełożenie na wariant, który możemy określić wariantem szczególnym wprowadzania stopni alarmowych, to jest w sytuacji niecierpiącej zwłoki. W wariancie szczególnym stopień alarmowy w drodze zarządzenia wprowadza – odpowiednio w obszarach określonych w art. 16 ust. 1 oraz w przypadku wskazanym w wymienionym już art. 16 ust. 1 pkt 5 – minister właściwy do spraw wewnętrznych po zasięgnięciu opinii Szefa ABW, a w odniesieniu do placówek zagranicznych RP i systemów teleinformatycznych – minister właściwy do spraw zagranicznych po zasięgnięciu opinii Szefa AW.

W obu wariantach szczególnych, uzależnionych od obszaru obowiązywania stopni alarmowych, organ wprowadzający stopień alarmowy niezwłocznie zawiadamia Prezesa Rady Ministrów.

Prezes Rady Ministrów natychmiast przekazuje informację o wprowadzeniu stopnia alarmowego, a także informację o zmianie lub odwołaniu stopnia alarmowego Prezydentowi Rzeczpospolitej Polskiej oraz marszałkom obu Izb Parlamentu.

W tym miejscu warto odnotować, że przed przeniesieniem systemu stopni alarmowych na grunt przepisów prawa powszechnie obowiązującego, we wspomnianych zarządzeniach – nr 74 z 12 października 2011 r. i nr 18 z 2 marca 2016 r. – obszar obowiązywania stopnia alarmowego był tym, co determinowało organ upoważniony do jego wprowadzania.

O ile w obowiązujących przepisach takim organem jest Prezes Rady Ministrów, a w wyjątkowych sytuacjach minister właściwy do spraw wewnętrznych lub minister właściwy do spraw zagranicznych, o tyle na gruncie wspomnianych zarządzeń przewidywano możliwość wprowadzania stopni alarmowych przez Prezesa Rady Ministrów jedynie w sytuacji, gdy dotyczyło to całego terytorium kraju lub kilku województw. W innych przypadkach do wprowadzenia stopnia alarmowego byli uprawnieni:

– ministrowie lub kierownicy urzędów centralnych – w odniesieniu do wszystkich lub wybranych kierowników podległych, podporządkowanych i nadzorowanych jednostek organizacyjnych, formacji i urzędów,

– wojewodowie – w stosunku do obszarów, obiektów i urządzeń według właściwości miejscowej, na obszarze całego lub części województwa[19].

Ponadto w zarządzeniu nr 18 Prezesa Rady Ministrów z 2 marca 2016 r. przewidziano możliwość wprowadzenia stopnia alarmowego w polskich przedstawicielstwach dyplomatycznych i urzędach konsularnych w drodze decyzji ministra właściwego do spraw zagranicznych.

Na gruncie ustawy o działaniach antyterrorystycznych, z uwagi na powszechnie obowiązujący charakter stopni alarmowych, ustawodawca zdecydował o ograniczeniu kompetencji w zakresie możliwości ich wprowadzania i o centralizacji uprawnień.

Jak już wspomniano, wprowadzenie stopnia alarmowego sensu stricto lub stopnia alarmowego CRP stanowi podstawę do realizacji przez instytucje publiczne, tj. organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego, określonych przedsięwzięć, których podstawowym celem jest minimalizacja zagrożenia. Ustawodawca, mając na względzie opisane powyżej różnice proceduralne wynikające z kompetencji poszczególnych organów, w zależności od obszaru terytorialnego, na którym wprowadza się stopień alarmowy, przewidział odrębne akty wykonawcze regulujące zakres przedsięwzięć wykonywanych w czasie obowiązywania poszczególnych stopni alarmowych sensu stricto i stopni alarmowych CRP.

W przypadku trybu wprowadzania stopnia alarmowego, o którym mowa w art. 16 ust. 1, do wydania stosownego rozporządzenia upoważniony jest Prezes Rady Ministrów, a w przypadku trybu wynikającego z art. 16 ust. 2 – minister właściwy do spraw zagranicznych. W pierwszym przypadku akt wykonawczy odnosi się podmiotowo do przedsięwzięć realizowanych w ramach kompetencji ustawowych przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego, a w drugim wyłącznie do kierowników placówek zagranicznych RP. W obu sytuacjach wytycznymi do wydania aktów wykonawczych są: minimalizacja skutków zdarzeń o charakterze terrorystycznym oraz zapewnienie sprawności przepływu informacji.

[19] Por. załącznik nr 5 do zarządzenia nr 74 Prezesa Rady Ministrów z 12 października 2011 r. i załącznik nr 1 do zarządzenia nr 18 Prezesa Rady Ministrów z 2 marca 2016 r.

Na poziomie ustawy zwrócono także uwagę na to, że poza wspomnianymi aktami organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego są zobowiązani także do realizacji innych przedsięwzięć, które bądź wynikają wprost z ich kompetencji ustawowych, bądź wynikają z przedsięwzięć i procedur zarządzania kryzysowego – jeśli te zostały przewidziane dla danego stopnia alarmowego, a nie określono ich we wspomnianych aktach wykonawczych.

Na poziomie samej ustawy o działaniach antyterrorystycznych przewidziano również dodatkowe kompetencje i obowiązki poszczególnych organów, zależne od wprowadzanych stopni alarmowych.

We wspomnianym rozdziale 3., zatytułowanym *Stopnie alarmowe*, w art. 17 przewidziano powołanie tzw. sztabu koordynacyjnego, do którego ustawowo określonych zadań należy rekomendowanie zmiany lub odwołania stopnia alarmowego oraz rekomendowanie form i zakresu współpracy służb i organów wchodzących w skład sztabu i biorących udział w jego pracach. W skład sztabu wchodzą przedstawiciele wyznaczeni przez służby specjalne oraz przez Policję, Straż Graniczną, Straż Marszałkowską, Służbę Ochrony Państwa, Państwową Straż Pożarną, Generalnego Inspektora Informacji Finansowej, Krajową Administrację Skarbową, Żandarmerię Wojskową i Rządowe Centrum Bezpieczeństwa, tj. podmioty uczestniczące w wymianie informacji dotyczących zdarzeń o charakterze terrorystycznym, koordynowanej przez Szefa ABW na podstawie art. 5 ust. 1 ustawy o działaniach antyterrorystycznych. Z kolei do udziału w pracach sztabu Szef ABW może powołać fakultatywnie, w zależności od rodzaju zdarzenia, które było podstawą do wprowadzenia stopnia alarmowego, przedstawicieli innych organów administracji publicznej oraz Prokuratora Generalnego. Powołanie sztabu koordynacyjnego stanowi obowiązek Szefa ABW w przypadku wprowadzenia któregokolwiek ze stopni alarmowych – bez względu na to, czy jest to stopień alarmowy sensu stricto czy stopień alarmowy CRP, oraz na jakim poziomie (ALFA, BRAVO, CHARLIE, DELTA) jest on określony. Obowiązek ten dotyczy wyłącznie stopni wprowadzanych w trybie, o którym mowa w art. 16 ust. 1 ustawy o działaniach antyterrorystycznych, czyli na terytorium kraju. Brakuje analogicznego obowiązku nałożonego na Szefa AW uczestniczącego w procedurze wydawania stopni alarmowych w trybie, o którym mowa w art. 16 ust. 2 tej ustawy.

Od wprowadzenia określonego stopnia alarmowego sensu stricto, ale już nie od stopnia alarmowego CRP, w dalszych przepisach jest uzależnione:

– **wprowadzenie zakazu odbywania zgromadzeń lub imprez masowych (art. 21 ustawy)** – jako kompetencję ministra właściwego do spraw wewnętrznych, działającego z własnej inicjatywy lub na wniosek Szefa ABW lub Komendanta Głównego Policji, w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego. Zakaz obszarowo odnosi się do tego terenu, który objęto stopniem alarmowym, a czasowo – do czasu, na jaki zarządzono stopień alarmowy. Przesłanką jego wprowadzenia jest konieczność ochrony życia i zdrowia ludzi lub bezpieczeństwa publicznego. Na ministrze właściwym do spraw wewnętrznych spoczywa również obowiązek poinformowania Marszałka Sejmu i Marszałka Senatu, którzy przekazują z kolei tę informację odpowiednio posłom i senatorom. Zakaz skutkuje wydaniem odpowiednio przez organ gminy decyzji o zakazie zgromadzenia lub o jego rozwiązaniu w trybach określonych w *Ustawie z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach*[20] lub wprowadzeniem przez wojewodę, w drodze decyzji administracyjnej, zakazu przeprowadzenia imprezy masowej lub jej przerwaniem, zgodnie z przepisami *Ustawy z 20 marca 2009 r. o bezpieczeństwie imprez masowych*[21]. Decyzje te mają zastosowanie w odniesieniu do wszystkich zgromadzeń oraz imprez masowych w czasie obowiązywania stopnia alarmowego i na obszarze jego obowiązywania w części objętej właściwością miejscową danego organu administracji publicznej i przysługują od nich środki odwoławcze określone w wymienionych ustawach – prawo o zgromadzeniach i ustawie o bezpieczeństwie imprez masowych;
– **użycie oddziałów lub pododdziałów Sił Zbrojnych RP do pomocy oddziałom i pododdziałom Policji (art. 22 ustawy)** – jako kompetencję Ministra Obrony Narodowej działającego na wniosek ministra właściwego do spraw wewnętrznych, w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego. Tryb określony w art. 22 ustawy o działaniach antyterrorystycznych jest uproszczeniem i jednocześnie usprawnieniem procedur w stosunku do trybu przewidzianego w przepisach art. 18 *Ustawy z dnia 6 kwietnia 1990 r. o Policji*[22] dzięki przygotowaniu Sił Zbrojnych RP do ich użycia, tj. rozpoczęciu planowania, pozyskiwaniu informacji i podjęciu

[20] Tekst jednolity: DzU z 2022 r. poz. 1389.

[21] Tekst jednolity: DzU z 2022 r. poz. 1466.

[22] Tekst jednolity: DzU z 2021 r. poz. 1882, ze zm.

współpracy z organami administracji publicznej, bezpośrednio po wprowadzeniu trzeciego lub czwartego stopnia alarmowego i przed wydaniem decyzji przez Ministra Obrony Narodowej. Z uwagi na szczególną kategorię zagrożeń, jakimi są zdarzenia o charakterze terrorystycznym, w tym trudną do oszacowania liczbę ofiar i nieprzewidywalny przebieg i skutki takich zdarzeń – w sytuacji dużego prawdopodobieństwa wystąpienia lub wystąpienia zdarzenia o charakterze terrorystycznym, z jakim mamy do czynienia w trzecim i czwartym stopniu alarmowym – ustawodawca przewidział możliwość użycia i wykorzystania środków przymusu bezpośredniego i broni palnej. Mogą one być użyte w działaniach kontrterrorystycznych przez oddziały i pododdziały Wojsk Specjalnych wspierające Policję w sposób przewidziany w *Ustawie z dnia 11 marca 2022 r. o obronie Ojczyzny*[23], z zastrzeżeniem dopuszczalności użycia broni palnej w przypadkach określonych w art. 23 ust. 1 ustawy o działaniach antyterrorystycznych. Oznacza to w praktyce, że żołnierze Wojsk Specjalnych będą mogli korzystać ze środków przymusu bezpośredniego i broni palnej w zakresie swoich ustawowych kompetencji, to jest (...) *w zakresie ochrony niepodległości państwa, niepodzielności jego terytorium oraz zapewnienia bezpieczeństwa i nienaruszalności jego granic* (...) *w sposób adekwatny do zagrożenia oraz w granicach zasad określonych w wiążących Rzeczpospolitą Polską ratyfikowanych umowach międzynarodowych oraz międzynarodowym prawie zwyczajowym*[24];

– **sprawdzenie zabezpieczeń obiektów na obszarze objętym stopniem alarmowym (art. 12 ustawy)** – jako obowiązek odpowiednio Policji lub Żandarmerii Wojskowej, w przypadku wprowadzenia drugiego lub wyższego stopnia alarmowego. Policja została w ustawie zobowiązana do sprawdzenia zabezpieczeń obiektów infrastruktury krytycznej, Żandarmeria Wojskowa natomiast do sprawdzenia obiektów należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, lub też administrowanych przez te komórki i jednostki organizacyjne. Z obowiązkiem tym powiązano także dodatkową kompetencję Szefa ABW, który w uzgodnieniu z ministrem właściwym

[23] DzU z 2022 r. poz. 655, ze zm.

[24] Ustawa o Policji, art. 11 ust. 4.

do spraw wewnętrznych może wydać Policji zalecenie szczególnego zabezpieczenia poszczególnych obiektów, uwzględniające rodzaj zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym.

Przechodząc od regulacji ustawowych do przedsięwzięć określonych we wspomnianych wcześniej aktach wykonawczych, należy w pierwszej kolejności odnieść się do *Rozporządzenia Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP*[25]. W rozporządzeniu wskazano zgodnie z delegacją ustawową, że jego głównym adresatem są organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego. Jednak w § 1 ust. 2 zwrócono uwagę, że te podmioty realizują przedsięwzięcia w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP (...) *we współpracy z właścicielami, posiadaczami samoistnymi i posiadaczami zależnymi obiektów infrastruktury krytycznej w zakresie ochrony tych obiektów*. Zgodnie z § 2 ust. 2 tego rozporządzenia na potrzeby tej współpracy na wyżej wymienionych właścicieli, posiadaczy samoistnych oraz posiadaczy zależnych infrastruktury krytycznej nałożono obowiązek uwzględniania szczegółowego zakresu przedsięwzięć określonego rozporządzeniem. Rozwiązanie to z perspektywy poprawności legislacyjnej może wzbudzać wątpliwości co do zgodności z treścią upoważnienia ustawowego, a określony powyżej obowiązek nałożony na podmioty, niewymienione wprost w delegacji, powinien raczej stanowić normę ustawową.

Szczegółowy zakres przedsięwzięć określono w załączniku do przedmiotowego rozporządzenia. Niezależnie od niego w § 3 rozporządzenia wskazano, że organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego określą (...) *procedury realizacji przedsięwzięć w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP, w tym moduły zadaniowe dla każdego stopnia, zawierające w szczególności wykaz zadań do wykonania*[26] (wydaje się,

[25] DzU z 2016 r. poz. 1101. Zmiany do rozporządzenia wprowadzono następującymi aktami prawnymi: *Obwieszczeniem Prezesa Rady Ministrów z dnia 27 lipca 2016 r. o sprostowaniu błędów* (DzU z 2016 r. poz. 1116) oraz *Rozporządzeniem Prezesa Rady Ministrów z dnia 4 marca 2022 r. zmieniające rozporządzenie w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP* (DzU z 2022 r. poz. 538).

[26] Przykład tego rodzaju procedury stanowi *Zarządzenie nr 16 Ministra Spraw Wewnętrznych i Administracji z dnia 2 lipca 2019 r. w sprawie realizacji zadań związanych z opiniowaniem, wprowadzaniem, zmianą lub odwołaniem stopni alarmowych lub stopni alarmowych CRP* (niepublikowane).

że ten przepis jako nakładający określone dodatkowe obowiązki powinien w przyszłości zostać przeniesiony na grunt ustawowy).

W § 4 rozporządzenia zawarto obowiązek informacyjny nałożony na adresatów rozporządzenia wobec Rządowego Centrum Bezpieczeństwa. Zgodnie z rozporządzeniem po otrzymaniu informacji o wprowadzeniu stopnia alarmowego lub stopnia alarmowego CRP organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego niezwłocznie potwierdzają Rządowemu Centrum Bezpieczeństwa otrzymanie informacji o wprowadzeniu stopnia alarmowego lub stopnia alarmowego CRP. Przekazują także raport o stanie realizacji zadań wynikających z wprowadzonego stopnia w czasie nie dłuższym niż 12 godzin od rozpoczęcia obowiązywania stopnia. O ile z perspektywy funkcjonalnej ten przepis nie budzi zastrzeżeń i zamyka procedurę związaną z wprowadzaniem, odwoływaniem i zmienianiem stopni alarmowych oraz informowaniem o tym fakcie podmiotów właściwych do podjęcia niezbędnych działań, o tyle z perspektywy prawno-legislacyjnej powinien on znaleźć precyzyjne oparcie w przepisach merytorycznych ustawy, a ewentualny tryb przekazywania informacji powinien zostać uwzględniony w upoważnieniu do wydania tego aktu wykonawczego.

Zakres przedsięwzięć zawarty we wspomnianym załączniku został określony odrębnie zarówno dla każdego z czterech stopni alarmowych sensu stricto, jak i każdego stopnia alarmowego CRP, przy czym w odniesieniu do każdego kolejnego stopnia, począwszy od stopni alarmowych ALFA i ALFA-CRP, wskazano, że w przypadku jego wprowadzenia należy wykonać zadania wymienione dla stopni niższych danej kategorii (stopni alarmowych sensu stricto albo stopni alarmowych CRP) oraz kontynuować te zadania lub sprawdzić ich wykonanie.

Podobną konstrukcję przewidziano również w *Rozporządzeniu Ministra Spraw Zagranicznych z dnia 7 czerwca 2022 r. w sprawie szczegółowego zakresu przedsięwzięć wykonywanych przez kierowników placówek zagranicznych Rzeczypospolitej Polskiej w poszczególnych stopniach alarmowych lub stopniach alarmowych CRP*[27]. Szczegółowy zakres przedsięwzięć przewidzianych w wymienionych rozporządzeniach dla poszczególnych stopni alarmowych przedstawiono w tabelach.

[27] DzU z 2022 r. poz. 1251.

Tabela 1. Zakres przedsięwzięć przewidzianych w rozporządzeniach dla stopni alarmowych sensu stricto.

Stopień alarmowy sensu stricto	Zadania organów administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego[a]	Zadania kierowników placówek zagranicznych[b]
ALFA	1) prowadzenie, przy użyciu Policji, Straży Granicznej lub Żandarmerii Wojskowej, wzmożonej kontroli dużych skupisk ludności, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym, w tym imprez masowych i zgromadzeń publicznych; 2) prowadzenie, w ramach realizacji zadań administratorów obiektów, wzmożonej kontroli obiektów użyteczności publicznej oraz innych obiektów, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym; 3) zalecenie podległemu personelowi informowania odpowiednich służb w przypadku zauważenia: nieznanych pojazdów na terenie instytucji publicznych lub innych ważnych obiektów, porzuconych paczek i bagaży lub jakichkolwiek innych oznak nietypowej działalności; 4) poinformowanie podległego personelu o konieczności zachowania zwiększonej czujności w stosunku do osób zachowujących się w sposób wzbudzający podejrzenia; 5) zapewnienie dostępności w trybie alarmowym członków personelu niezbędnych do wzmocnienia ochrony obiektów; 6) przeprowadzanie kontroli pojazdów wjeżdżających oraz osób wchodzących na teren obiektów; 7) sprawdzanie, na zewnątrz i wewnątrz, budynków będących w stałym użyciu pod kątem podejrzanych zachowań osób oraz w poszukiwaniu podejrzanych przedmiotów;	1) poinformowanie członków personelu placówki zagranicznej i członków ich rodzin o wprowadzeniu pierwszego stopnia alarmowego (stopień ALFA); 2) poinformowanie członków personelu placówki zagranicznej o konieczności zachowania wzmożonej czujności w przypadku podejrzanych zachowań osób i poszukiwania podejrzanych przedmiotów; 3) wprowadzenie stałych, całodobowych dyżurów członków personelu placówki zagranicznej; 4) uruchomienie procedury wzmożonych kontroli pojazdów oraz osób wjeżdżających lub wchodzących na teren placówki zagranicznej (zwracanie szczególnej uwagi na zawartość pojazdów i bagażu osób); 5) poinformowanie członków personelu placówki zagranicznej o konieczności prowadzenia kontroli pojazdu przed wejściem do niego i jego uruchomieniem; 6) ograniczenie podróży służbowych; 7) ograniczenie do niezbędnego minimum ruchu pojazdów i osób w obrębie placówki zagranicznej; 8) ograniczenie do minimum liczby wejść i wjazdów dla pieszych i pojazdów używanych na terenie placówki zagranicznej; 9) wzmocnienie kontroli przesyłek pocztowych, kurierskich oraz innych dostaw wpływających do placówki zagranicznej; 10) wzmocnienie kontroli nad czynnościami związanymi z usługami realizowanymi dla placówki zagranicznej przez podmioty zewn.;

[a] Załącznik do rozporządzenia Prezesa Rady Ministrów z 25 lipca 2016 r.

[b] Załącznik nr 1 do rozporządzenia Ministra Spraw Zagranicznych z 7 czerwca 2022 r.

	8) sprawdzenie działania środków łączności wykorzystywanych w celu zapewnienia bezpieczeństwa; 9) dokonanie, w ramach realizacji zadań administratorów obiektów, sprawdzeń działania instalacji alarmowych, przepustowości dróg ewakuacji oraz funkcjonowania systemów rejestracji obrazu; 10) dokonanie przeglądu wszystkich procedur, rozkazów oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych; 11) prowadzenie akcji informacyjno-instruktażowej dla społeczeństwa dotyczącej potencjalnego zagrożenia, jego skutków i sposobu postępowania	11) sprawdzanie na zewnątrz i wewnątrz budynków zabezpieczenia placówki zagranicznej; 12) zamknięcie wejść i zabezpieczenie nieużywanych regularnie budynków oraz pomieszczeń placówki zagranicznej; 13) sprawdzenie działania systemów łączności funkcjonujących na potrzeby placówki zagranicznej; 14) dokonanie przeglądu wszystkich procedur, szczegółowych wymagań osobowych i logistycznych oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych; 15) sprawdzanie działania instalacji alarmowych, systemów rejestracji obrazu oraz przepustowości dróg ewakuacyjnych; 16) dokonanie przeglądu zastępczych źródeł energii (agregatów prądotwórczych), zbiorników na wodę, schronów i innych miejsc ochrony dla członków personelu placówki zagranicznej; 17) przeprowadzenie przeglądu terenu i budynku placówki zagranicznej oraz dokonanie niezbędnych napraw i remontów; 18) informowanie odpowiednich służb w przypadku zauważenia: nieznanych pojazdów zaparkowanych lub poruszających się w sposób podejrzany (np. wielokrotne objeżdżających obiekty placówki zagranicznej) lub porzuconych paczek i bagaży, lub innych nietypowych zachowań; 19) podjęcie działań przygotowawczych związanych z zabezpieczeniem przedmiotów i materiałów o szczególnej wartości; 20) podjęcie innych działań organizacyjnych i wykonawczych zwiększających stan ochrony placówki zagranicznej; 21) nawiązanie bezpośredniego kontaktu z lokalnymi organami administracji odpowiedzialnymi za zarządzanie kryzysowe i bezpieczeństwo;

		22) prowadzenie monitoringu nietypowych zdarzeń mających miejsce w bezpośrednim sąsiedztwie placówki zagranicznej; 23) rezygnowanie z organizacji spotkań i imprez okolicznościowych o charakterze otwartym na terenie placówki zagranicznej; 24) przygotowywanie i przekazywanie okresowych informacji o sytuacji w kraju urzędowania do Ministerstwa Spraw Zagranicznych, o ustalonych godzinach; 25) przygotowywanie i przekazywanie uzupełniających oraz doraźnych informacji o sytuacji w kraju urzędowania do Ministerstwa Spraw Zagranicznych; 26) dokonanie przeglądu materiałów niejawnych pod kątem wyselekcjonowania materiałów podlegających ewentualnemu ewakuowaniu (szczególnie dokumentów niejawnych wykonanych w egzemplarzu pojedynczym, dokumentów niejawnych niezbędnych do funkcjonowania placówki zagranicznej, dzienników ewidencji, protokołów zniszczenia dokumentów niejawnych) oraz materiałów niejawnych przewidzianych do zniszczenia w przypadku wprowadzenia jednego z wyższych stopni alarmowych. Zgromadzenie materiałów niejawnych w punkcie obsługi dokumentów niejawnych placówki zagranicznej; 27) dokonanie przeglądu i aktualizacji komunikatów oraz informacji skierowanych do obywateli polskich podróżujących do państwa przyjmującego i publikowanych na stronach internetowych Ministerstwa Spraw Zagranicznych i placówki zagranicznej; 28) sprawdzenie aktualności planu ewakuacji, a zwłaszcza wykazu dokumentów oraz przedmiotów uznanych za ważne ze względu na interes Rzeczpospolitej Polskiej
BRAVO	1) wprowadzenie przez Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej	1) poinformowanie członków personelu placówki zagranicznej o możliwych formach ataku;

	lub Komendanta Głównego Żandarmerii Wojskowej obowiązku noszenia broni długiej oraz kamizelek kuloodpornych przez umundurowanych funkcjonariuszy lub żołnierzy bezpośrednio realizujących zadania związane z zabezpieczeniem miejsc i obiektów, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym; 2) wprowadzenie dodatkowych kontroli pojazdów, osób oraz budynków publicznych w rejonach zagrożonych; 3) wzmocnienie ochrony środków komunikacji publicznej; 4) sprawdzenie funkcjonowania zasilania awaryjnego; 5) ostrzeżenie personelu o możliwych formach zdarzenia o charakterze terrorystycznym; 6) zapewnienie dostępności w trybie alarmowym personelu wyznaczonego do wdrażania procedur działania na wypadek zdarzeń o charakterze terrorystycznym; 7) sprawdzenie i wzmocnienie ochrony ważnych obiektów publicznych; 8) wprowadzenie zakazu wstępu do przedszkoli, szkół i uczelni osobom postronnym; 9) sprawdzenie systemu ochrony obiektów ochranianych przez specjalistyczne uzbrojone formacje ochronne; 10) wprowadzenie kontroli wszystkich przesyłek pocztowych kierowanych do urzędu lub instytucji; 11) zamknięcie i zabezpieczenie nieużywanych regularnie budynków i pomieszczeń; 12) dokonanie przeglądu zapasów materiałowych i sprzętu, w tym dostępności środków i materiałów medycznych, z uwzględnieniem możliwości wykorzystania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym	2) zapewnienie dostępności w trybie alarmowym członków personelu placówki zagranicznej niezbędnych przy realizacji czynności na rzecz wzmocnienia ochrony placówki zagranicznej; 3) wzmocnienie ochrony placówki zagranicznej; 4) sprawdzenie placówki zagranicznej; 5) dokonanie przeglądu systemów ochrony oraz stanu posiadanych zapasów materiałowych i sprzętu; 6) przeprowadzenie, bezpośrednio przy wejściu do placówki zagranicznej, kontroli osób wchodzących na jej teren oraz ich bagaży; 7) wprowadzanie nieregularnych patroli do kontrolowania pojazdów oraz budynków użytkowanych na potrzeby placówki zagranicznej, a także osób przebywających na terenie placówki; 8) wystąpienie do miejscowych władz o zwiększenie ochrony placówki zagranicznej i jej personelu; 9) wydanie zaleceń członkom personelu placówki zagranicznej i członkom ich rodzin dotyczących ograniczenia lub zaniechania kontaktów z ludnością miejscową, a także opuszczania miejsca zamieszkania bez uzasadnionej przyczyny; 10) uzgodnienie z Zespołem Zarządzania Kryzysowego w Ministerstwie Spraw Zagranicznych możliwości odesłania do kraju tych członków personelu placówki zagranicznej i ich rodzin, których dalszy pobyt na placówce nie jest konieczny; 11) dokonanie aktualizacji wykazu obywateli polskich przebywających w państwie przyjmującym i państwach pozostających we właściwości terytorialnej placówki zagranicznej; 12) powiadomienie obywateli polskich przebywających w państwie przyjmującym (bez względu na cel pobytu) o grożącym niebezpieczeństwie i zalecenie im powrotu do kraju;

		13) stworzenie warunków do udzielania pomocy obywatelom polskim przebywającym w państwie przyjmującym oraz do ułatwienia im powrotu do kraju; 14) przystosowanie (w razie potrzeby i przy wykorzystaniu dostępnych środków) piwnic oraz innych pomieszczeń o wzmocnionej konstrukcji z przeznaczeniem na schrony lub inne miejsca ukrycia o podobnym charakterze; 15) uzupełnienie zapasów materiałowych, w tym lekarstw i środków opatrunkowych, wody, paliw, części zamiennych do agregatów prądotwórczych i samochodów oraz zalecenie członkom rodzin personelu placówki zagranicznej zgromadzenia odpowiednich zapasów własnych, szczególnie żywności, wody, lekarstw i środków opatrunkowych; 16) wstrzymanie wszelkiego rodzaju prac budowlanych, montażowych lub renowacyjnych w obiektach placówki zagranicznej, z wyłączeniem robót będących na ukończeniu, prowadzonych przez pracowników krajowych delegowanych przez Ministerstwo Spraw Zagranicznych lub przez pracowników miejscowych, jeżeli wykonanie tych prac ma istotny wpływ na stan bezpieczeństwa placówki zagranicznej; 17) odwołanie członków personelu placówki zagranicznej z urlopów, z wyjątkiem osób przebywających poza granicami państwa przyjmującego; 18) ustanowienie i utrzymywanie stałej łączności z Ministerstwem Spraw Zagranicznych, innymi polskimi instytucjami i placówkami zagranicznymi oraz z misjami dyplomatycznymi innych państw Unii Europejskiej, a także z przedstawicielami Polonii i obywatelami polskimi przebywającymi w państwie przyjmującym; 19) przygotowanie placówki zagranicznej do okresowego zakwaterowania na jej terenie wszystkich członków personelu i ich rodzin

		(z wyłączeniem pracowników miejscowych) lub członków personelu i ich rodzin (z wyłączeniem pracowników miejscowych) zamieszkujących w szczególnie zagrożonych miejscach; 20) zniszczenie wybranych materiałów niejawnych niezakwalifikowanych do ewakuacji zgodnie z planem ewakuacji zatwierdzonym przez kierownika placówki zagranicznej oraz protokołem zniszczenia
CHARLIE	1) wprowadzenie, na polecenie ministra właściwego do spraw wewnętrznych, całodobowych dyżurów we wskazanych urzędach lub jednostkach organizacyjnych organów administracji publicznej; 2) wprowadzenie dyżurów dla osób funkcyjnych odpowiedzialnych za wprowadzanie procedur działania na wypadek zdarzeń o charakterze terrorystycznym; 3) sprawdzenie dostępności obiektów wyznaczonych na zastępcze miejsca czasowego pobytu na wypadek ewakuacji ludności; 4) ograniczenie do minimum liczby miejsc ogólnodostępnych w obiekcie i rejonie obiektu; 5) wprowadzenie, w uzasadnionych przypadkach, ścisłej kontroli osób i pojazdów przy wejściu i wjeździe na teren obiektów; 6) ograniczenie możliwości parkowania pojazdów przy obiektach chronionych; 7) wydanie broni i amunicji oraz środków ochrony osobistej uprawnionym osobom, wyznaczonym do wykonywania zadań ochronnych; 8) wprowadzenie dodatkowego całodobowego nadzoru nad miejscami, które tego wymagają, do tej pory nieobjętych nadzorem; 9) zapewnienie ochrony środków transportu służbowego poza terenem obiektu, wprowadzenie kontroli pojazdu przed wejściem do niego i jego uruchomieniem	1) wprowadzenie dyżurów dla osób odpowiedzialnych za wdrożenie procedur działania na wypadek aktów terrorystycznych lub sabotażu; 2) ograniczenie do minimum liczby miejsc ogólnodostępnych w placówce zagranicznej; 3) wprowadzenie ścisłej kontroli osób i pojazdów przy wejściu i wjeździe na teren placówki zagranicznej; 4) wzmocnienie służby ochronnej placówki zagranicznej oraz zwiększenie częstotliwości patrolowania obiektów ujętych w planach ochrony; 5) wprowadzenie całodobowego nadzoru osobowego nad miejscami podlegającymi ochronie; 6) dokonanie przeglądu dostępnej bazy i środków medycznych pod kątem możliwości wykorzystania ich w przypadku ataku terrorystycznego lub sabotażu; 7) przygotowanie, zgodnie z wykazem, o którym mowa przy stopniu alarmowym ALFA – w pkt 28, do zniszczenia dokumentów oraz przedmiotów uznanych za ważne ze względu na interes Rzeczpospolitej Polskiej, które nie zostały zniszczone po wprowadzeniu stopnia alarmowego BRAVO i nie zostały przeznaczone do ewakuacji; 8) dokonanie wycofania z banków, po uzgodnieniu z Ministerstwem Spraw Zagranicznych, części lub całości środków pieniężnych będących w dyspozycji placówki zagranicznej;

		9) przygotowanie placówki zagranicznej do całkowitej ewakuacji; 10) przeprowadzenie częściowej ewakuacji członków personelu placówki zagranicznej, których wyjazd nie zakłóci funkcjonowania placówki zagranicznej, oraz ich rodzin; 11) sprawdzenie możliwości ukrycia członków personelu placówki zagranicznej poza budynkiem placówki i uzyskanie potwierdzenia w tym zakresie od miejscowych władz; 12) rozwiązanie umowy o pracę z pracownikami miejscowymi lub całkowite odsunięcie tych pracowników od wykonywania zadań merytorycznych placówki zagranicznej; 13) zabezpieczenie dokumentów, przedmiotów oraz dóbr kultury zgodnie z uprzednio ustalonym wykazem; 14) zakwaterowanie w obiektach placówki zagranicznej członków personelu (z wyłączeniem pracowników miejscowych) zamieszkałych w szczególnie zagrożonych miejscach; 15) określenie głównych przedsięwzięć przygotowawczych związanych z zawieszeniem działalności placówki zagranicznej lub jej likwidacją; 16) przygotowanie do ewakuacji wyselekcjonowanych materiałów niejawnych, dzienników ewidencji i protokołów zniszczenia, o których mowa przy stopniu alarmowym ALFA w pkt 26
DELTA	1) wprowadzenie, w uzasadnionych przypadkach, ograniczeń komunikacyjnych w rejonach zagrożonych; 2) przeprowadzenie identyfikacji wszystkich pojazdów znajdujących się już w rejonie obiektu oraz, w uzasadnionych przypadkach, ich relokacji poza obszar obiektu; 3) kontrolowanie wszystkich pojazdów wjeżdżających na teren obiektu i ich ładunku;	1) zapewnienie zaplecza logistycznego oraz medyczno-sanitarnego, odpowiednio do skali możliwego zagrożenia; 2) ewakuowanie placówki zagranicznej, a w przypadku braku takiej możliwości – zniszczenie materiałów niejawnych, dzienników ewidencji i protokołów zniszczenia zgodnie z wykazem, o którym mowa przy stopniu alarmowym ALFA – w pkt 28;

	4) kontrolowanie wszystkich wnoszonych na teren obiektu przedmiotów, w tym walizek, torebek, paczek; 5) przeprowadzanie częstych kontroli na zewnątrz budynku i na parkingach; 6) ograniczenie liczby podróży służbowych osób zatrudnionych w obiekcie i wizyt osób niezatrudnionych w instytucji; 7) przygotowanie się do zapewnienia ciągłości funkcjonowania organu w przypadku braku możliwości realizacji zadań w dotychczasowym miejscu pracy	3) powiadomienie właściwych władz państwa przyjmującego o czasowym zawieszeniu działalności placówki zagranicznej lub zamiarze czasowego zawieszenia działalności oraz ewakuacji personelu placówki lub jego części, a także zażądanie ochrony na trasie ewakuacji oraz ułatwień na przejściach granicznych; 4) uzgodnienie z Ministerstwem Spraw Zagranicznych zakresu ewakuacji, miejsca, terminu i sposobu jej przeprowadzenia, sposobu postępowania z pozostawionym mieniem, zadań politycznych, a także organizacji łączności do czasu zakończenia ewakuacji; 5) przeprowadzenie całkowitej ewakuacji placówki zagranicznej na polecenie Przewodniczącego Zespołu Zarządzania Kryzysowego w Ministerstwie Spraw Zagranicznych lub jego zastępcy; 6) w przypadku braku łączności z Ministerstwem Spraw Zagranicznych samodzielne podjęcie decyzji o ewakuacji

Źródło: Opracowanie własne na podstawie *Rozporządzenia Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP* oraz *Rozporządzenia Ministra Spraw Zagranicznych z dnia 7 czerwca 2022 r. w sprawie szczegółowego zakresu przedsięwzięć wykonywanych przez kierowników placówek zagranicznych Rzeczypospolitej Polskiej w poszczególnych stopniach alarmowych lub stopniach alarmowych CRP*.

Tabela 2. Zakres przedsięwzięć przewidzianych w rozporządzeniach dla stopni alarmowych CRP.

Stopień alarmowy CRP	Zadania organów administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego[a]	Zadania kierowników placówek zagranicznych[b]
ALFA-CRP	1) wprowadzenie wzmożonego monitorowania stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, zwanych dalej „systemami", szczególnie z wykorzystaniem zaleceń Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za system reagowania zgodnie z właściwością, oraz monitorowanie i weryfikowanie, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej, sprawdzanie dostępności usług elektronicznych, dokonywanie, w razie potrzeby, zmian w dostępie do systemów; 2) poinformowanie personelu instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, szczególnie personelu odpowiedzialnego za bezpieczeństwo systemów; 3) sprawdzenie kanałów łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym właściwymi dla rodzaju stopnia alarmowego CRP, dokonanie weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji; 4) dokonanie przeglądu procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP,	1) poinformowanie członków personelu placówki zagranicznej i członków ich rodzin o wprowadzeniu odpowiedniego stopnia alarmowego CRP; 2) wprowadzenie dyżurów członków personelu placówki zagranicznej odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych lub za realizację zadań z zakresu bezpieczeństwa placówki w celu analizy i oceny stanów odbiegających od przyjętych standardów; 3) sprawdzenie kanałów łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym właściwymi dla rodzaju stopnia alarmowego CRP, z pracownikami wydziału właściwego w sprawach reagowania na incydenty bezpieczeństwa teleinformatycznego w komórce właściwej do spraw bezpieczeństwa teleinformatycznego w Ministerstwie Spraw Zagranicznych oraz z innymi podmiotami świadczącymi wsparcie w przedmiotowym zakresie; 4) informowanie na bieżąco dyrektora komórki organizacyjnej właściwej do spraw bezpieczeństwa teleinformatycznego w Ministerstwie Spraw Zagranicznych oraz pracowników tej komórki odpowiedzialnych za sprawy reagowania na incydenty bezpieczeństwa teleinformatycznego o efektach przeprowadzanych działań

[a] Załącznik do rozporządzenia Prezesa Rady Ministrów z 25 lipca 2016 r.

[b] Załącznik nr 2 do rozporządzenia Ministra Spraw Zagranicznych z 7 czerwca 2022 r.

	zwłaszcza dokonanie weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania organizacji, oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu; 5) sprawdzenie aktualnego stanu bezpieczeństwa systemów i ocena wpływu zagrożeń na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń; 6) informowanie na bieżąco o efektach przeprowadzanych działań zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego właściwych dla rodzaju działania organizacji oraz współdziałających centrów zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji	
BRAVO-CRP	1) zapewnienie dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów; 2) wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych	1) zapewnienie gotowości do niezwłocznego podejmowania działań przez członków personelu placówki zagranicznej odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych lub za realizację zadań z zakresu bezpieczeństwa placówki; 2) w razie potrzeby dokonywanie zmian w dostępie do infrastruktury teleinformatycznej w porozumieniu z dyrektorem komórki organizacyjnej właściwej do spraw bezpieczeństwa teleinformatycznego w Ministerstwie Spraw Zagranicznych oraz pracownikami tej komórki odpowiedzialnymi za sprawy reagowania na incydenty bezpieczeństwa teleinformatycznego
CHARLIE-CRP	1) wprowadzenie całodobowych dyżurów administratorów systemówkluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;	przygotowanie się do ograniczenia operacji na serwerach w celu ich szybkiego i bezawaryjnego zamknięcia, po uprzednim uzyskaniu zgody dyrektora komórki organizacyjnej właściwej ds. bezpieczeństwa teleinformatycznego w Ministerstwie Spraw Zagranicznych lub pracowników tej

	2) dokonanie przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku; 3) przygotowanie się do uruchomienia planów umożliwiających zachowanie ciągłości działani po wystąpieniu potencjalnego ataku, w tym: dokonanie przeglądu i ewentualnego audytu planów awaryjnych oraz systemów, przygotowanie się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamkniecia	komórki odpowiedzialnych za sprawy reagowania na incydenty bezpieczeństwa teleinformatycznego
DELTA-CRP	1) uruchomienie planów awaryjnych lub planów ciągłości działania organizacji w sytuacjach awarii lub utraty ciągłości działania; 2) stosownie do sytuacji przystąpienie do realizacji procedur przywracania ciągłości działania	nie określono dodatkowych zadań wyłącznie dla stopnia DELTA-CRP

Źródło: Opracowanie własne na podstawie *Rozporządzenia Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP* oraz *Rozporządzenia Ministra Spraw Zagranicznych z dnia 7 czerwca 2022 r. w sprawie szczegółowego zakresu przedsięwzięć wykonywanych przez kierowników placówek zagranicznych Rzeczypospolitej Polskiej w poszczególnych stopniach alarmowych lub stopniach alarmowych CRP*.

W kontekście powiązania przepisów prawnych z systemem stopni alarmowych warto również zwrócić uwagę na rozwiązania przyjęte w *Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[28]. Zgodnie z art. 36 ust. 7 pkt 5 tej ustawy Zespół do spraw Incydentów Krytycznych, będący organem pomocniczym w sprawach obsługi incydentów krytycznych[29] zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV[30] i koordynującym

[28] Tekst jednolity: DzU z 2020 r. poz. 1369, ze zm.

[29] Incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, wolności i praw obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV (CSIRT – Computer Security Incident Response Team; wyjaśnienie nazw w następnym przypisie – przyp. red.).

[30] CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej; CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy

działania podejmowane przez nie oraz Rządowe Centrum Bezpieczeństwa, (...) *w przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 15 ust. 2 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (stopnie alarmowe CRP)*, przygotowuje w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego.*

Analiza przypadków wprowadzenia stopni alarmowych

Tempo procesu legislacyjnego związanego z przygotowaniem ustawy o działaniach antyterrorystycznych, a także termin, z jakim ustawa weszła w życie – zgodnie z art. 65 ustawy, z wyjątkiem jednego artykułu, weszła ona w życie przy skróconym wobec standardowego, a wynikającego z *Ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych*[31], vacatio legis, tj. po upływie siedmiu dni od dnia ogłoszenia – były związane z dążeniem projektodawcy, w tym wypadku Rady Ministrów[32], do wprowadzania nowych rozwiązań przed konkretnymi wydarzeniami, jakie w 2016 r. odbyły się w Polsce: szczytem NATO w Warszawie i 31. Światowymi Dniami Młodzieży w Krakowie. Te wydarzenia, szczególnie trudne pod względem zagwarantowania niezbędnych środków bezpieczeństwa, nie tylko były organizowane na podstawie szczególnego i epizodycznego ustawodawstwa[33], lecz także wymagały szczególnych rozwiązań

Instytut Badawczy; CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa ABW.

[31] Tekst jednolity: DzU z 2019 r. poz. 1461. Standardowy termin vacatio legis – 14 dni po dniu ogłoszenia – art. 4 ust. 1 ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych.

[32] Rządowy projekt, za którego przygotowanie odpowiadała Kancelaria Prezesa Rady Ministrów, we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji (Ocena skutków regulacji do projektu ustawy o działaniach antyterrorystycznych).

[33] *Ustawa z dnia 18 marca 2016 r. o szczególnych rozwiązaniach związanych z organizacją wizyty Jego Świątobliwości Papieża Franciszka w Rzeczypospolitej Polskiej oraz Światowych Dni Młodzieży – Kraków 2016* (t.j. DzU z 2017 r. poz. 685) oraz *Ustawa z dnia 16 marca 2016 r. o szczególnych rozwiązaniach związanych z organizacją Szczytu Organizacji Traktatu Północnoatlantyckiego w Rzeczypospolitej Polskiej w Warszawie w 2016 roku* (t.j. DzU z 2016 r. poz. 379, ze zm.).

o charakterze systemowym. Wspomniane wydarzenia stały się więc katalizatorem przeprowadzenia kompleksowego uporządkowania rozwiązań prawnych w odniesieniu do polskiego systemu antyterrorystycznego. Warto zauważyć, że pierwotny projekt rządowy w wersji skierowanej do Sejmu zawierał jeszcze krótszy termin wejścia w życie ustawy – dzień następujący po dniu ogłoszenia, jednak ze względu na standardy konstytucyjne dokonano jego wydłużenia.

Wprawdzie w uzasadnieniu do ustawy o działaniach antyterrorystycznych nie wskazano bezpośrednio, że termin wejścia w życie ustawy ma ścisłe powiązanie ze wspomnianymi wyżej wydarzeniami, ale jest to oczywiste zarówno w kontekście przebiegu debaty sejmowej, jak i samej strony normatywnej. Ustawa o działaniach antyterrorystycznych nowelizowała bowiem ustawę o szczególnych rozwiązaniach dotyczących organizacji wizyty papieża Franciszka w RP oraz Światowych Dni Młodzieży w Krakowie w 2016 r.

W tym kontekście można stwierdzić, że instytucja prawna stopni alarmowych została wykorzystana po raz pierwszy na podstawie przepisów ustawy o działaniach antyterrorystycznych – w ramach zabezpieczeń wspomnianych przedsięwzięć.

W okresie, w którym stopnie alarmowe były unormowane w zarządzeniach wydanych na podstawie ustawy o zarządzaniu kryzysowym, a więc przed wejściem w życie ustawy o działaniach antyterrorystycznych, stopnie alarmowe zostały wprowadzone tylko raz – w odniesieniu do organizacji w Polsce Turnieju Finałowego UEFA EURO 2012. Wprowadzenie wówczas stopnia alarmowego wiązało się z ujawnieniem przez Straż Graniczną pakunku zawierającego materiały wybuchowe i telefon ze zdjęciem Stadionu Narodowego, które były umieszczone na tratwie pływającej po Bugu[34]. Jak wskazywał ówczesny rzecznik Ministerstwa Spraw Wewnętrznych: *Po przeanalizowaniu sprawy stwierdzono, że nie istnieje zagrożenie dla bezpieczeństwa osób lub miejsc w Polsce. Jednak biorąc pod uwagę fakt, że jest to pierwszy tego typu istotny sygnał podczas Euro 2012, dotyczący możliwości wystąpienia*

[34] Por. *Tusk: Stopień alarmowy nie zmienia poziomu bezpieczeństwa na Euro 2012*, Dziennik Gazeta Prawna, 28 VI 2012 r., https://www.gazetaprawna.pl/wiadomosci/artykuly/628995,tusk-stopien-alarmowy-nie-zmienia-poziomu-bezpieczenstwa-na-euro-2012.html [dostęp: 2 VII 2022]; *Pierwszy stopień alarmowy w Polsce. Grozi nam zamach?*, Wprost, 28 VI 2012 r., https://sport.wprost.pl/euro-2012/330817/pierwszy-stopien-alarmowy-w-polsce-grozi-nam-zamach.html [dostęp: 2 VII 2022].

zdarzenia o charakterze terrorystycznym, zdecydowano o wprowadzeniu pierwszego stopnia alarmowego w czterostopniowej skali[35].

Na podstawie ustawy o działaniach antyterrorystycznych stopnie alarmowe, poza stopniami, o których mowa w art. 16 ust. 2 tej ustawy, czyli w odniesieniu do placówek zagranicznych RP i systemów teleinformatycznych ministra właściwego do spraw zagranicznych, były wprowadzane w następujących przypadkach[36]:

- **szczyt NATO w Warszawie, 2016 r.** – na obszarze miasta stołecznego Warszawy wprowadzono pierwszy stopień alarmowy (ALFA), który obowiązywał od 7 do 10 lipca 2016 r.;
- **31. Światowe Dni Młodzieży w Krakowie, 2016 r.** – na całym terytorium RP wprowadzono pierwszy stopień alarmowy (ALFA) i drugi stopień alarmowy CRP (BRAVO-CRP), które obowiązywały od 20 lipca do 1 sierpnia 2016 r.;
- **24. sesja Konferencji Stron Ramowej Konwencji ONZ w sprawie zmian klimatu (COP24) w Katowicach, 2018 r.** – na obszarze województwa śląskiego oraz miasta Krakowa wprowadzono pierwszy stopień alarmowy (ALFA), który obowiązywał od 26 listopada do 15 grudnia 2018 r.;
- **spotkanie ministerialne dotyczące bezpieczeństwa na Bliskim Wschodzie w Warszawie, 2019 r.** – na obszarze miasta stołecznego Warszawy wprowadzono pierwszy stopień alarmowy (ALFA) i drugi stopień alarmowy CRP (BRAVO-CRP), które obowiązywały od 11 do 15 lutego 2019 r.;
- **wybory do Parlamentu Europejskiego, 2019 r.** – na całym terytorium RP wprowadzono drugi stopień alarmowy CRP (BRAVO-CRP), który obowiązywał od 23 do 27 maja 2019 r.;
- **obchody 80. rocznicy wybuchu II wojny światowej, 2019 r.** – na całym terytorium RP wprowadzono pierwszy stopień alarmowy (ALFA) i pierwszy stopień alarmowy CRP (ALFA-CRP), które obowiązywały od 28 sierpnia do 3 września 2019 r.;

---

[35] *Pierwszy stopień alarmowy. Znaleźli ładunki wybuchowe*, TVN24, 27 VI 2012 r., https://tvn24.pl/polska/pierwszy-stopien-alarmowy-znalezli-ladunki-wybuchowe-ra261245-3500262 [dostęp: 2 VII 2022].

[36] *Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP*, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [dostęp: 2 VII 2022].

- **wybory do Sejmu i Senatu, 2019 r.** – na całym terytorium RP wprowadzono drugi stopień alarmowy CRP (BRAVO-CRP), który obowiązywał od 10 do 14 października 2019 r.;
- **uroczystości upamiętniające 75. rocznicę wyzwolenia niemieckiego nazistowskiego obozu koncentracyjnego i zagłady Auschwitz-Birkenau, 2020 r.** – na obszarze województwa małopolskiego wprowadzono drugi stopień alarmowy (BRAVO), na pozostałym terytorium RP wprowadzono pierwszy stopień alarmowy (ALFA); dodatkowo na całym terytorium RP wprowadzono pierwszy stopień alarmowy CRP (ALFA-CRP). Stopnie alarmowe obowiązywały od 23 do 29 stycznia 2020 r.;
- **wybory Prezydenta Rzeczpospolitej Polskiej, 2020 r.** – na całym terytorium RP wprowadzono drugi stopień alarmowy CRP (BRAVO-CRP), który obowiązywał od 26 do 29 czerwca 2020 r. oraz od 10 do 13 lipca 2020 r.;
- **Szczyt Cyfrowy ONZ – IGF 2021 (the UN Internet Governance Forum) w Katowicach, 2021 r.** – na całym terytorium RP wprowadzono pierwszy stopień alarmowy CRP (ALFA-CRP), który obowiązywał od 5 do 10 grudnia 2021 r.;
- **wystąpienie potencjalnego ryzyka dla bezpieczeństwa systemów teleinformatycznych w związku z identyfikowanymi zagrożeniami będącymi następstwem napiętej sytuacji w regionie:**
  - na całym terytorium RP wprowadzono pierwszy stopień alarmowy CRP (ALFA-CRP), który obowiązywał od 18 do 23 stycznia 2022 r. oraz od 15 do 21 lutego 2022 r.;
  - na całym terytorium RP wprowadzono trzeci stopień alarmowy CRP (CHARLIE-CRP), który obowiązuje od 21 lutego 2022 r. do 30 listopada 2022 r.;
- **wystąpienie zwiększonego i przewidywalnego zagrożenia zdarzeniem terrorystycznym wynikającego z masowego napływu na terytorium Rzeczpospolitej Polskiej uchodźców z terenu Ukrainy:**
  - na obszarze województwa lubelskiego oraz podkarpackiego wprowadzono drugi stopień alarmowy (BRAVO), który obowiązywał od 28 lutego do 15 kwietnia 2022 r.;
  - na całym terytorium RP wprowadzono drugi stopień alarmowy (BRAVO), który obowiązuje od 16 kwietnia 2022 r. do 30 listopada 2022 r.

Po przeanalizowaniu tego zestawienia można stwierdzić, że w zdecydowanej większości przypadków wprowadzenie stopnia alarmowego wiązało się z organizacją w Polsce istotnych wydarzeń o wymiarze międzynarodowym lub udziałem przedstawicieli innych państw (łącznie siedem tego rodzaju przypadków). Charakter tych przedsięwzięć był różny, tak jak i sama w nich rola Polski i władz państwowych – od organizatora (np. obchody 80. rocznicy wybuchu II wojny światowej), współorganizatora (np. spotkanie ministerialne dotyczące bezpieczeństwa na Bliskim Wschodzie współorganizowane ze Stanami Zjednoczonymi Ameryki, które odbyło się w Warszawie) do państwa goszczącego czy wręcz udostępniającego swoje terytorium, podczas gdy samo przedsięwzięcie miało charakter quasi-eksterytorialny (COP24 czy IGF 2022, których organizatorem były różne agendy Organizacji Narodów Zjednoczonych).

Stopnie alarmowe wprowadzano również trzykrotnie w związku z wyborami, w 2022 r. zaś były wprowadzane, a następnie przedłużane (na podstawie oddzielnie wydawanych zarządzeń Prezesa Rady Ministrów) z powodu sytuacji za wschodnią granicą Polski.

Ostatni z tych przypadków jest odrębny od dotychczasowych. Pierwszą różnicą jest to, że stopnie alarmowe nie zostały wprowadzone jako skutek planowej organizacji określonego rodzaju przedsięwzięcia, jak uroczystości, spotkania międzynarodowe czy wybory, lecz w kontekście wydarzeń niezależnych od działań polskich władz. Do tych wydarzeń należy zaliczyć celowy atak Białorusi wymierzony w Polskę i ogólnie Unię Europejską, w postaci rozmyślnie spowodowanego i odgórnie napędzanego kryzysu migracyjnego na granicy polsko-białoruskiej, stanowiącej jednocześnie zewnętrzną granicę UE, który należy postrzegać w kategoriach ataku o charakterze hybrydowym. Drugim wydarzeniem skutkującym wprowadzeniem stopni alarmowych jest zbrojny atak Federacji Rosyjskiej na Ukrainę oraz wynikające z tego konsekwencje – z jednej strony niespotykany wcześniej napływ do Polski uchodźców z terenu konfliktu (Ukrainy), z drugiej zaś zagrożenia różnego rodzaju działaniami hybrydowymi ze strony Rosji, w tym w cyberprzestrzeni.

Drugą zasadniczą różnicę w stosunku do wcześniejszych okoliczności związanych z wprowadzeniem stopni alarmowych jest okres, na który zostały one przyjęte. W tym wypadku po raz pierwszy obowiązują nie kilka lub kilkanaście dni, lecz kilka miesięcy. Jak słusznie wskazują autorzy komentarza do ustawy o działaniach antyterrorystycznych Paweł Łabuz, Tomasz Safjański i Waldemar Zubrzycki:

> Stopnie alarmowe i stopnie alarmowe CRP wprowadza się w uzasadnionych przypadkach, jednak wiąże się to z licznymi utrudnieniami zarówno dla funkcjonowania różnych instytucji, jak też obywateli. Niewątpliwie, ich wdrożenie ma również ogromny wpływ na funkcjonowanie służb i formacji odpowiedzialnych za zapewnianie bezpieczeństwa obywatelom i obiektom RP, działających również w trybie alarmowym, a więc niecodziennym i nienaturalnym, w odniesieniu do sytuacji anormalnych i niekonwencjonalnych. Utrzymanie takiego stanu na dłuższą metę powodować będzie znaczne zakłócenia ich funkcjonowania, może również okazać się niemożliwe. Dlatego stopnie alarmowe odwołuje się bezzwłocznie po zminimalizowaniu zagrożenia lub skutków zdarzenia, które było przesłanką do wprowadzenia odpowiedniego stopnia alarmowego. Może to oznaczać całkowite jego zniesienie albo obniżenie stopnia alarmowego w kilkustopniowej skali[37].

We wskazanym przypadku przesłanka wprowadzenia stopnia alarmowego istniała przez dłuższy czas, co uzasadniało utrzymanie tego stopnia ze wszystkimi tego funkcjonalnymi wyzwaniami dla organów administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego, ale także, w pewnym zakresie, dla właścicieli, posiadaczy samoistnych i posiadaczy zależnych obiektów infrastruktury krytycznej. Jednocześnie ogłoszenie stopnia alarmowego na dłuższy czas jest obarczone ryzykiem zagrożenia rutyną, a przez to spadkiem koncentracji w zakresie realizacji przedsięwzięć wynikających z przepisów prawa na poziomie jednostkowym, podczas gdy stopnie alarmowe mają właśnie zapewniać podwyższony stopień gotowości.

Z perspektywy przedmiotowej można wskazać, że stopnie wprowadzano w różnych konfiguracjach, tzn. zarówno samodzielnie stopnie alarmowe sensu stricto (np. szczyt NATO w 2016 r. czy COP24) oraz stopnie alarmowe CRP (np. wymienione wcześniej wybory), jak i jednocześnie oba rodzaje stopni alarmowych (np. Światowe Dni Młodzieży) w zależności od charakteru zagrożenia. W przypadku łączenia stopni alarmowych sensu stricto i stopni alarmowych CRP zazwyczaj stopień alarmowy CRP był wyższy w czterostopniowej skali. Warto też zauważyć, że w przypadku stopni alarmowych sensu stricto najwyższy z dotychczas wprowadzanych to drugi stopień alarmowy BRAVO, podczas gdy w przypadku stopni alarmowych CRP wykorzystywano trzeci stopień alarmowy CHARLIE-CRP.

[37] P. Łabuz, T. Safjański, W. Zubrzycki, *Ustawa o działaniach antyterrorystycznych. Komentarz*...

Stopnie alarmowe to zatem wielokrotnie wykorzystywany instrument w wymiarze prewencyjnym – dotychczas były one stosowane jako narzędzie służące podniesieniu poziomu gotowości na wypadek wystąpienia zdarzenia o charakterze terrorystycznym, a nie jako konsekwencja wystąpienia zdarzenia o charakterze terrorystycznym. Uprawnione organy ogłaszają zaś stopnie alarmowe w sposób elastyczny, m.in. w zakresie:

- rodzaju okoliczności stanowiących podstawę ich wprowadzenia – od zabezpieczenia planowych przedsięwzięć do reakcji na zagrożenia zewnętrzne;
- zakresu terytorialnego – stosowane na terenie całego kraju lub określonych jego obszarach jak miasta czy województwa, a także w niektórych polskich placówkach zagranicznych;
- wyznaczania poziomu stopnia w ramach czterostopniowej skali – od pierwszego stopnia alarmowego ALFA do drugiego stopnia alarmowego BRAVO oraz od pierwszego stopnia alarmowego ALFA-CRP do trzeciego stopnia alarmowego CHARLIE-CRP;
- typu stosowanych stopni – oddzielnie stopnie alarmowe sensu stricto i stopnie alarmowe CRP oraz łącznie;
- czasowym – czas dostosowany do danego wydarzenia, z którym są one powiązane lub okresu trwania danego zagrożenia;
- adekwatności – zdarzały się przypadki podwyższenia stopnia lub zmiany zakresu terytorialnego jego obowiązywania.

Adekwatność rozwiązań – podsumowanie

Efektywność mechanizmów wprowadzania stopni alarmowych oraz adekwatność przedsięwzięć realizowanych po wprowadzeniu stopni była kilkakrotnie poddawana ocenie w ramach Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych[38]. Członkowie Zespołu nie zgłaszali jednak żadnych propozycji zmian w tym zakresie, co może świadczyć o prawidłowej konstrukcji instytucji stopni alarmowych.

System stopni alarmowych ustanowiony na gruncie przepisów ustawy o działaniach antyterrorystycznych został pozytywnie oceniony podczas

[38] Powołany *Zarządzeniem nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych* [podstawa prawna utworzenia Zespołu: art. 12 ust. 1 pkt 3 i ust. 2 *Ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów* (t.j. DzU z 2022 r. poz. 1188) – przyp. red.].

wizyty Dyrekcji Wykonawczej Organizacji Narodów Zjednoczonych ds. Zwalczania Terroryzmu (UN CTED) w grudniu 2019 r. Jej celem było dokonanie ewaluacji rezolucji Rady Bezpieczeństwa ONZ w zakresie walki z terroryzmem wdrożonych do polskiego systemu prawnego[39].

Autorzy zgadzają się również ze stanowiskiem wyrażonym przez Piotra Chorbota, że korzyścią wynikającą z wprowadzenia przepisów dotyczących stopni alarmowych i stworzenia na ich podstawie odpowiednich algorytmów postępowania jest możliwość przećwiczenia koordynacji działania właściwych służb i innych podmiotów, a (...) *wszelkie przepisy ustanawiane w celu kreacji właściwych postaw i polegające na ćwiczeniu reakcji na zagrożenie pozwalają lepiej przygotować służby do działania, a tym samym – zwiększyć standard bezpieczeństwa RP*[40].

Po przeanalizowaniu szybkości uruchamiania procedury dotyczącej wprowadzania stopni alarmowych warte rozważenia pozostaje wprowadzenie przepisu jednoznacznie wskazującego, że wnioski i opinie, o których mowa w art. 16 ust. 1 oraz 2 ustawy o działaniach antyterrorystycznych (wnioski i opinie ministra właściwego do spraw wewnętrznych i Szefa ABW stanowiące podstawę do wydania zarządzenia o wprowadzeniu stopnia), przekazane także ustnie, telefonicznie, za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 *Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*[41] lub za pomocą innych środków łączności uznaje się za dostarczone w sposób skuteczny. Ich treść oraz istotne motywy takiego załatwienia sprawy utrwala się w formie pisemnej. To znane już obecnie krajowemu ustawodawstwu rozwiązanie[42] pozwoliłoby na zagwarantowanie szybkości i skuteczności działań bez oczekiwania na obieg dokumentów. Wprawdzie ustawa o działaniach antyterrorystycznych nie wskazuje wprost na obowiązek pisemnej formy przestawienia wymaganych wniosków i opinii, ale mając na uwadze skutki wprowadzenia stopnia oraz ewentualne ograniczenia wolności i praw obywateli (np. zakaz organizowania zgromadzeń i imprez masowych – art. 21 ustawy), wydaje się,

[39] Por. M. Cichomski, I. Idzikowska-Ślęzak, *Poziom strategiczny polskiego systemu antyterrorystycznego – 15 lat Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych,* „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 76.

[40] P. Chorbot, *Ustawa o działaniach antyterrorystycznych. Komentarz...*, s. 73.

[41] Tekst jednolity: DzU z 2020 r. poz. 344.

[42] Na przykład art. 11h ust. 11 *Ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych* (t.j. DzU z 2021 r. poz. 2095, ze zm.).

że proponowane rozwiązanie miałoby istotne znaczenie oraz dawałoby gwarancję skuteczności realizowanych czynności.

Przepisy ustawy powinny również jednoznacznie wskazywać, który organ jest właściwy do realizacji obowiązków informacyjnych (wymienionych w art. 16 ust. 3 ustawy o działaniach antyterrorystycznych) wobec Prezydenta RP, Marszałka Sejmu i Marszałka Senatu – w przypadku wprowadzenia stopnia alarmowego w trybie szczególnym, tj. w przypadku niecierpiącym zwłoki.

Kolejnym tematem jest ewentualne, wzmiankowane we wcześniejszej części opracowania, doprecyzowanie art. 16 ust. 4 ustawy, zgodnie z którym wprowadzenie stopnia alarmowego lub stopnia alarmowego CRP jest podstawą realizacji przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego określonego rodzaju przedsięwzięć (m.in. jednoznacznie wskazanie wśród adresatów tej normy właścicieli, posiadaczy samoistnych i posiadaczy zależnych obiektów infrastruktury krytycznej). Obecne brzmienie tego przepisu nie koreluje z brzmieniem przepisów wykonawczych wydanych na podstawie ust. 5 tego artykułu. W rozporządzeniu Prezesa Rady Ministrów z 25 lipca 2016 r. uwzględniono rolę właścicieli, posiadaczy samoistnych i posiadaczy zależnych obiektów infrastruktury krytycznej. Rozwiązanie to oddaje ratio legis ustawodawcy.

W odniesieniu do tego rozporządzenia poza wątpliwościami prawno-legislacyjnymi opisanymi we wcześniejszej części warto również wskazać, że przynajmniej dwa z zawartych w nim rozwiązań, tj.:

- wprowadzenie zakazu wstępu do przedszkoli, szkół i uczelni publicznych osobom postronnym – w przypadku wprowadzenia drugiego lub wyższego stopnia alarmowego,
- wprowadzenie, na polecenie ministra właściwego do spraw wewnętrznych, całodobowych dyżurów we wskazanych urzędach lub jednostkach organizacyjnych organów administracji publicznej – przewidziane dla trzeciego stopnia alarmowego

powinny docelowo stać się normami ustawowymi.

Pierwsze z nich – jako wkraczające w sferę wolności i praw obywatelskich – może być wdrożone w celu wypełnienia obowiązku wynikającego z art. 31 ust. 3 Konstytucji RP, zgodnie z którym ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i jedynie wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, dla ochrony środowiska,

zdrowia i moralności publicznej albo wolności i praw innych osób. Drugie zaś – gdy zachodzi potrzeba objęcia kompetencjami ministra właściwego do spraw wewnętrznych podmiotów, które mu nie podlegają i nie są przez niego nadzorowane. Ponadto kwestie związane z obiegiem informacji o stopniach alarmowych, zawarte w przywoływanym rozporządzeniu, powinny znaleźć swoją precyzyjną podstawę w upoważnieniu ustawowym.

Wskazane powyżej kierunki ewentualnych zmian mają jednak charakter wyłącznie uzupełniający lub stricte prawny i nie wpływają na całokształt oceny stopni alarmowych, które stały się jednym z najistotniejszych elementów ustawy o działaniach antyterrorystycznych, a wielokrotność wykorzystywania tej instytucji prawnej w różnych okolicznościach i wariantach świadczy o skuteczności i adekwatności przyjętych rozwiązań.

Bibliografia

Chorbot P., *Ustawa o działaniach antyterrorystycznych. Komentarz do niektórych regulacji*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia,* P. Burczaniuk (red.), Warszawa 2017.

Cichomski M., Horoszko M., Idzikowska I., *Przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym oraz reagowanie w przypadku wystąpienia takich zdarzeń w świetle rozwiązań ustawy o działaniach antyterrorystycznych – w kontekście zadań resortu spraw wewnętrznych*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016.

Cichomski M., Idzikowska-Ślęzak I., *Poziom strategiczny polskiego systemu antyterrorystycznego – 15 lat Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*, „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 66–89.

Źródła internetowe

Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [dostęp: 2 VII 2022].

Kolory, stopnie i terminologia NATO. Jak odczytać alerty terrorystyczne, TVP Info, 23 III 2016 r., https://www.tvp.info/24554977/kolory-stopnie-i-terminologia-nato-jak-odczytac-alerty-terrorystyczne [dostęp: 7 XII 2018].

Łabuz P., Safjański T., Zubrzycki W., *Ustawa o działaniach antyterrorystycznych. Komentarz*, Warszawa 2019, dostęp przez System Informacji Prawnej Legalis, sip.legalis.pl [dostęp: 20 VII 2022].

Pierwszy stopień alarmowy w Polsce. Grozi nam zamach?, Wprost, 28 VI 2012 r., https://sport.wprost.pl/euro-2012/330817/pierwszy-stopien-alarmowy-w-polsce-grozi-nam-zamach.html [dostęp: 2 VII 2022].

Pierwszy stopień alarmowy. Znaleźli ładunki wybuchowe, TVN24, 27 VI 2012 r., https://tvn24.pl/polska/pierwszy-stopien-alarmowy-znalezli-ladunki-wybuchowe-ra261245-3500262 [dostęp: 2 VII 2022].

Tusk: Stopień alarmowy nie zmienia poziomu bezpieczeństwa na Euro 2012, Dziennik Gazeta Prawna, 28 VI 2012 r., https://www.gazetaprawna.pl/wiadomosci/artykuly/628995,tusk-stopien-alarmowy-nie-zmienia-poziomu-bezpieczenstwa-na-euro-2012.html [dostęp: 2 VII 2022].

Uzasadnienie do projektu ustawy o działaniach antyterrorystycznych, https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=516 [dostęp: 2 VII 2022].

Akty prawne

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (t.j. DzU z 1997 r. nr 78, poz. 483, ze zm.).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (DzU z 2022 r. poz. 655, ze zm.).

Ustawa z dnia 21 stycznia 2021 r. o służbie zagranicznej (t.j. DzU z 2022 r. poz. 1076, ze zm.).

Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t.j. DzU z 2021 r. poz. 2095, ze zm.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2020 r. poz. 1369, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2021 r. poz. 2234, ze zm.).

Ustawa z dnia 18 marca 2016 r. o szczególnych rozwiązaniach związanych z organizacją wizyty Jego Świątobliwości Papieża Franciszka w Rzeczypospolitej Polskiej oraz Światowych Dni Młodzieży – Kraków 2016 (t.j. DzU z 2017 r. poz. 685).

Ustawa z dnia 16 marca 2016 r. o szczególnych rozwiązaniach związanych z organizacją Szczytu Organizacji Traktatu Północnoatlantyckiego w Rzeczypospolitej Polskiej w Warszawie w 2016 roku (t.j. DzU z 2016 r. poz. 379, ze zm.).

Ustawa z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach (t.j. DzU z 2022 r. poz. 1389).

Ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (t.j. DzU z 2022 r. poz. 1466, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2022 r. poz. 261, ze zm.).

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 (t.j. DzU z 2017 r. poz. 1932, ze zm.).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. DzU z 2020 r. poz. 344).

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. DzU z 2017 r. poz. 1928).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. DzU z 2017 r. poz. 1897).

Ustawa z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (t.j. DzU z 2019 r. poz. 1461).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2022 r. poz. 1138).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. DzU z 2021 r. poz. 1882, ze zm.).

Rozporządzenie Ministra Spraw Zagranicznych z dnia 7 czerwca 2022 r. w sprawie szczegółowego zakresu przedsięwzięć wykonywanych przez kierowników placówek zagranicznych Rzeczypospolitej Polskiej w poszczególnych stopniach alarmowych lub stopniach alarmowych CRP (DzU z 2022 r. poz. 1251).

Rozporządzenie Prezesa Rady Ministrów z dnia 4 marca 2022 r. zmieniające rozporządzenie w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (DzU z 2022 r. poz. 538).

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (DzU z 2016 r. poz. 1101).

Zarządzenie nr 16 Ministra Spraw Wewnętrznych i Administracji z dnia 2 lipca 2019 r. w sprawie realizacji zadań związanych z opiniowaniem, wprowadzaniem, zmianą lub odwołaniem stopni alarmowych lub stopni alarmowych CRP (niepublikowane).

Zarządzenie nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego, https://www.stawiguda.pl/userfiles/OC/Komunikaty_zew/Zarz%C4%85dzenie%20nr%2018%20Prezesa%20Rady%20Ministr%C3%B3w%20z%20dnia%202%20marca%202016%20r.pdf.

Zarządzenie nr 74 Prezesa Rady Ministrów z dnia 12 października 2011 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego (niepublikowane).

Zarządzenie nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, zmienione zarządzeniem nr 95 Prezesa Rady Ministrów z 4 września 2008 r., zarządzeniem nr 74 Prezesa Rady Ministrów z 21 września 2009 r., zarządzeniem nr 18 Prezesa Rady Ministrów z 3 kwietnia 2014 r., zarządzeniem nr 84 Prezesa Rady Ministrów z 18 września 2015 r., zarządzeniem nr 86 Prezesa Rady Ministrów z 5 lipca 2016 r., zarządzeniem nr 32 Prezesa Rady Ministrów z 27 kwietnia 2017 r., zarządzeniem nr 160 Prezesa Rady Ministrów z 9 listopada 2017 r., zarządzeniem nr 92 Prezesa Rady Ministrów z 7 czerwca 2018 r. oraz zarządzeniem nr 37 Prezesa Rady Ministrów z 8 kwietnia 2021 r.

Obwieszczenie Prezesa Rady Ministrów z dnia 27 lipca 2016 r. o sprostowaniu błędów (DzU z 2016 r. poz. 1116).

DOI: 10.4467/27204383TER.22.019.16339

ORCID: 0000-0003-1514-7657

MICHAŁ PIEKARSKI

Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych

Abstrakt

W artykule został omówiony problem wykorzystania zamachów terrorystycznych jako narzędzia wojny hybrydowej. Za pomocą scenariuszowej metody prognozowania dokonano analizy prawdopodobnego przebiegu ataków na terytorium Rzeczpospolitej Polskiej.

Słowa kluczowe:

terroryzm,
zamach terrorystyczny,
wojna hybrydowa

W związku z sytuacją na Ukrainie 28 lutego 2022 r. wprowadzono w Polsce, po raz pierwszy od chwili wejścia w życie *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[1], stopień alarmowy BRAVO na terenie dwóch województw – podkarpackiego i lubelskiego. W dniu 15 kwietnia 2022 r. przedłużono czas jego obowiązywania oraz rozszerzono zasięg terytorialny na cały kraj. W czasie pisania niniejszego artykułu czas obowiązywania był wydłużony do końca czerwca. Wprowadzenie stopnia alarmowego BRAVO jest interesujące pod kątem badań nad potencjalnymi zagrożeniami terrorystycznymi na terytorium Rzeczpospolitej Polskiej.

[1] Tekst jednolity: DzU z 2021 r. poz. 2234, ze zm.

Podjęcie takich decyzji oznacza bowiem, że zgodnie z ustawą zaistniało (...) *zwiększone i przewidywalne zagrożenie wystąpieniem zdarzenia o charakterze terrorystycznym*[2]. W tej sytuacji nasuwa się pytanie o to, jaki jest możliwy charakter tego rodzaju zagrożeń w świetle aktualnej sytuacji międzynarodowej, przede wszystkim agresywnej polityki Federacji Rosyjskiej.

Celem niniejszego artykułu jest wskazanie i omówienie scenariuszy zagrożeń terrorystycznych na terytorium RP w kontekście zagrożeń hybrydowych. Poszukiwanie odpowiedzi na postawione pytanie badawcze samo w sobie jest wyzwaniem metodologicznym, gdyż nie doszło do wystąpienia zdarzeń o charakterze terrorystycznym, a jedynie mamy do czynienia z podwyższonym ryzykiem ich zaistnienia. To oznacza, że odpowiedź będzie miała charakter prognostyczny. W związku z powyższym za podstawę metodologiczną badań przyjęto scenariuszową metodę prognozowania, która polega na analizowaniu za pomocą scenariuszy możliwego przebiegu przyszłych trendów i ocenie ich wpływu na aktualnie diagnozowany problem. Scenariusze są uporządkowanymi opisami trendów oraz ich wpływu na badany obszar, a wynikiem ich zastosowania jest opis możliwego stanu końcowego lub – częściej – kilku możliwych stanów końcowych. Metodę tę wykorzystuje się m.in. w analizach z zakresu bezpieczeństwa i gospodarki[3]. W literaturze przedmiotu podaje się kilka różnych, jakkolwiek pod pewnymi względami podobnych, etapów procesu tworzenia i analizy scenariusza. Przykładowo Jay Ogilvy wyróżnia ich osiem, począwszy od wstępnych działań, na implementacji wniosków kończąc. Są to:

1. Wskazanie kluczowego zagadnienia (ang. *focal issue)*.
2. Identyfikacja najważniejszych czynników.
3. Opis czynników zewnętrznych.
4. Wskazanie krytycznych niepewności.
5. Opis wewnętrznej logiki scenariusza.
6. Stworzenie samych scenariuszy.
7. Analiza implikacji i dostępnych opcji.
8. Analiza wczesnych wskaźników odróżniających scenariusze.

Dla porównania Hannah Kosow i Robert Gaßner podają pięć etapów.

---

[2] Ustawa o działaniach antyterrorystycznych, art. 15 ust. 4.

[3] Szerzej w: J. Ogilvy, *Scenario Planning and Strategic Forecasting*, Forbes, 8 I 2015 r., https://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/?sh=2de3fee5411a [dostęp: 18 V 2022].

Należą do nich:

1. Identyfikacja pola scenariusza.
2. Identyfikacja najważniejszego czynnika.
3. Analiza najważniejszego czynnika.
4. Generowanie scenariuszy.
5. Transfer scenariuszy (aplikacja)[4].

W pierwszej kolejności trzeba zatem zidentyfikować główny temat scenariusza. W przypadku badań opisywanych w niniejszej pracy było to zadanie łatwe, gdyż został on sformułowany w pytaniu badawczym. Wynika z niego także najważniejszy czynnik mający wpływ na analizowane scenariusze, tj. możliwe wykorzystanie zamachów terrorystycznych w działaniach hybrydowych prowadzonych przez Rosję na terenie Polski. Konieczne jest więc przeanalizowanie zagadnienia działań hybrydowych oraz wykorzystania w nich narzędzi terrorystycznych. Umożliwi to skonstruowanie scenariuszy i poddanie ich analizie, a ponadto pozwoli na ocenę możliwego wykorzystania zasobów systemu bezpieczeństwa państwa, a przede wszystkim jego integralnej części – systemu antyterrorystycznego.

Opisu najważniejszych czynników oraz konstruowania scenariuszy dokonano na podstawie dwóch zbiorów informacji. Pierwszym są dostępne, wiarygodne informacje dotyczące dotychczasowej rosyjskiej polityki i sposobu użycia siły w stosunkach międzynarodowych. Drugim – informacje na temat możliwych sposobów dokonywania zamachów terrorystycznych, zarówno w szerszej, strategicznej skali, jak i na poziomie taktycznym i technicznym.

Metoda scenariuszowa była już zastosowana w analizie polskiego systemu antyterrorystycznego[5]. Za jej pomocą klarownie przedstawiono wyzwania związane ze współczesnym charakterem tego rodzaju zagrożeń. Dodatkową wartością jest łatwość wykorzystania tego rodzaju analiz w celach szkoleniowych i dydaktycznych[6].

[4] H. Kosow, R. Gaßner, *Methods of Future and Scenario Analysis. Overview, Assessment, and Selection Criteria*, https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf [dostęp: 22 VI 2022].

[5] M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020, s. 158–207.

[6] Por. J. Sovolainen i in., *Hybrid CoE Working Paper 5. Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans*, https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf [dostęp: 29 IV 2022].

Analiza zagrożeń hybrydowych w kontekście zagrożeń terrorystycznych – uwagi ogólne

W literaturze przedmiotu nie ma jednej, precyzyjnej, ogólnie przyjętej definicji zagrożeń hybrydowych. Na sposób ich postrzegania niewątpliwy wpływ miały dwa konflikty zbrojne. Pierwszym z nich była wojna Izraela z Hezbollahem, która przez część analityków została nazwana hybrydową[7]. Drugim, skutkującym częstszym i szerszym użyciem tego terminu, są wydarzenia w Ukrainie mające swój początek w 2014 r. Aneksja Krymu została bowiem przeprowadzona przy pomocy oddziałów wojskowych używających siły w ograniczonym zakresie, występujących początkowo bez oznaczeń przynależności państwowej. Po tym sukcesie Rosjanie rozpoczęli działania w Donbasie, w których posługiwali się nieregularnymi formacjami zbrojnymi, złożonymi zarówno z miejscowych prorosyjskich ochotników czy najemników, jak i z żołnierzy wojsk specjalnych oraz sił regularnych przysłanych z Rosji, mimo że oficjalnie nie brała ona czynnego udziału w tej wojnie[8]. Nie oznacza to jednak, że o zagrożeniach hybrydowych mówi się tylko w kontekście tych dwóch konfliktów. Powstają prace poświęcone szerszym analizom tego pojęcia i kontekstom jego stosowania. Na przykład Robert Seely w artykule z 2017 r. zwraca uwagę, że termin „hybrydowy" w odniesieniu do konfliktów zbrojnych jest używany najczęściej w jednym z trzech kontekstów: 1) „zamrożonych", długotrwałych konfliktów będących skutkiem polityki Rosji na obszarze postradzieckim, 2) wojen nowej generacji, często utożsamianych z tezami przypisywanymi rosyjskim wojskowym, zwłaszcza Siergiejowi Gierasimowowi, oraz 3) kinetycznych i niekinetycznych działań służb wywiadowczych określanych jako środki aktywne[9]. Charakteryzuje on również narzędzia wykorzystywane przez Rosję jako należące do jednego z sześciu obszarów: 1) rządzenie (obejmuje także sferę kultury, religii i prawa), 2) gospodarka i energia, 3) polityka i przemoc polityczna, 4) siła militarna, 5) dyplomacja oraz 6) działania informacyjne i dezinformacyjne. W tych szeroko ujętych kategoriach mieszczą się węższe formy działań – na przykład wykorzystywanie kultury, w tym organizacji kulturalnych, w celach politycznych, wykorzystywanie energii do szantażu energetycznego, zabójstwa na tle politycznym, tworzenie prorosyjskich

[7] F. Hoffman, *Conflict in the 21st Century: The Rise of the Hybrid Wars,* https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 29 IV 2022].

[8] Szerzej w: L.M. Nadolski, *Kampania zimowa w 2015 roku na Ukrainie,* Bydgoszcz 2017, s. 43–44.

[9] R. Seely, *Defining Contemporary Russian Warfare,* „The RUSI Journal" 2017, t. 162, nr 1, s. 50–59.

organizacji, także zbrojnych. Środki należące do wymienionych powyżej kategorii mogą być stosowane jednocześnie. Co ważne, dochodzi do zatarcia tradycyjnych podziałów między użyciem siły militarnej a użyciem środków pozamilitarnych oraz między pokojem a wojną. Taki sposób wykorzystania tych środków przez państwo prowadzi do zjawiska użycia jako broni (narzędzia polityki) licznych narzędzi i czynników, określanych w języku angielskim jako *weaponisation*. Jak pisze Mark Galeotti, może to się przejawiać m.in. w wykorzystywaniu pomocy humanitarnej i medycznej, zorganizowanych grup przestępczych, prawa międzynarodowego, kultury i informacji w celach politycznych[10]. Autorzy raportu *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*[11] wskazują, że zagrożenia hybrydowe mają następujące cechy:

- korzystają z szerokiego spektrum narzędzi wojskowych, politycznych, gospodarczych, cywilnych i informacyjnych,
- w nietradycyjny sposób atakują sfery funkcjonowania społeczeństwa podatne na atak,
- w nowatorski sposób synchronizują używane środki,
- w sposób intencjonalny wykorzystują niepewność, niejasność i sposób postrzegania otoczenia przez atakowane państwo, by ograniczyć ryzyko wykrycia,
- mogą zostać zauważone i zidentyfikowane w późnej fazie realizacji.

Te wszystkie czynniki nie lokują jednoznacznie zagrożeń terrorystycznych w obrębie działań hybrydowych. Na możliwość wystąpienia działań terrorystycznych jako elementu działań hybrydowych zwracają jednak uwagę różni badacze problemu. Przemysław Gasztold i Aleksandra Gasztold wskazują, że wspomniana już wojna Izraela z Hezbollahem była konfliktem pomiędzy państwem a organizacją stosującą metody terrorystyczne, która mogła być wykorzystywana przez inne państwo (Iran) do prowadzenia działań terrorystycznych przeciwko innym państwom[12].

[10] M. Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, New York–London 2022.

[11] P.J. Cullen, E. Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, The Multinational Capability Development Campaign, 2017 r., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, s. 10 [dostęp: 20 V 2022].

[12] A. Gasztold, P. Gasztold, *The Polish Counterterrorism System and Hybrid Warfare Threats*, „Terrorism and Political Violence" 2020, https://www.tandfonline.com/doi/abs/10.1080/09546553.2020.1777110?journalCode=ftpv20 [dostęp: 28 V 2022].

Autorzy ci zauważają ponadto, że techniki typowe dla terroryzmu są stosowane podczas konfliktu zbrojnego w Ukrainie.

Interesujące spostrzeżenia na temat zagrożeń hybrydowych można odnaleźć również w literaturze z lat wcześniejszych. W artykule opublikowanym w 1998 r. Andrzej Makowski i Krzysztof Kubiak analizują możliwość wykorzystania czynnika militarnego w sposób niejawny i pośredni w działaniach prowadzonych tak, aby utrudnić lub uniemożliwić wskazanie ich faktycznego organizatora. Chodziło o działania wymierzone w ważne obiekty wojskowe i gospodarcze, osoby zajmujące kluczowe stanowiska w państwie w celu wywołania poczucia zagrożenia wśród mieszkańców atakowanego kraju, podważenia ich zaufania do władz i instytucji państwowych, skomplikowania sytuacji międzynarodowej i wywołania niepokojów społecznych[13]. Autorzy wspomnianego artykułu wskazują, że do takich działań mogą zostać zaangażowane osoby zamieszkujące terytorium danego państwa, które strona atakująca pozyska do współpracy, członkowie zagranicznych organizacji terrorystycznych lub przestępczych (de facto najemnicy), jak również żołnierze, zwłaszcza wojsk specjalnych, państwa atakującego, biorący udział w działaniach upozorowanych na akcje lokalnych ugrupowań ekstremistycznych. Uwagi te korespondują z treścią artykułu Łukasza Skonecznego z 2015 r.[14] Zauważył on, że działania hybrydowe mogą być stosowane właśnie po to, aby nie dopuścić do przekroczenia progu użycia siły, ponieważ byłoby to jednoznacznie zinterpretowane jako otwarta agresja, a więc zmuszałoby do zareagowania na przykład sojuszników zaatakowanego państwa. Użycie metod terrorystycznych, które ten autor także zalicza do grupy środków mogących mieć zastosowanie w działaniach hybrydowych, pozwala wykreować sytuację niejasną i niepewną pod względem reakcji.

Te ogólne analizy nie prowadzą jednak do szczegółowych wniosków na temat możliwych scenariuszy sytuacji kryzysowych. Terroryzm jest bowiem zjawiskiem zróżnicowanym i niejednolitym pod względem strategii oraz taktyk działania. Wynikają one przede wszystkim z ideologii organizacji stosujących metody terrorystyczne, środowiska, w którym działają, reakcji atakowanych państw oraz innych zmiennych. Na dobór taktyki mają z kolei wpływ m.in. bieżące uwarunkowania, przyjęta szersza strategia,

---

[13] A. Makowski, K. Kubiak, *Terroryzm jako sposób prowadzenia wojny?*, „Raport – wojsko – technika – obronność" 1998, nr 4, s. 41–43.

[14] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego", wydanie specjalne: *Wojna hybrydowa*, s. 39–50.

sytuacja operacyjna, wyszkolenie i uzbrojenie[15]. Ważną zmienną jest prowadzenie działań terrorystycznych bezpośrednio lub pośrednio przez państwo. Bartosz Bolechów pisze o kilku stopniach wspierania działalności terrorystycznej przez państwo, tj.: pełnej kontroli (terroryzm państwowy), rekrutacji i szkoleniu osób do działań terrorystycznych przez organy państwowe, znacznym stopniu kontroli nad organizacją terrorystyczną, dostarczaniu wsparcia grupie wysoce autonomicznej, pomocy dla grupy faktycznie niezależnej, wsparciu biernym[16]. W przypadku działań hybrydowych najbardziej prawdopodobne są cztery pierwsze stopnie, zapewniające wpływ na dobór celów i metod działania. Wsparcie państwowe oznacza zapewnienie szkolenia, finansowania, wyposażenia, informacji rozpoznawczych, bezpiecznego schronienia oraz innych form pomocy (np. wsparcie ideologiczne lub dyplomatyczne)[17]. Płynie z tego ważny wniosek, że tego rodzaju działania wspomagane lub prowadzone przez aktora państwowego będą mogły być realizowane z wykorzystaniem większych zasobów niż zasoby będące w dyspozycji organizacji terrorystycznych niemających takiej protekcji. Należy zatem przyjąć, że w analizie poświęconej prowadzeniu działań terrorystycznych w ramach szerzej postrzeganych działań hybrydowych jednym z zasadniczych czynników, które muszą zostać uwzględnione, jest udział podmiotów mogących wspierać lub realizować ich działania hybrydowe oraz cele polityczne.

Działania hybrydowe w środowisku bezpieczeństwa Polski

Z analizy dotyczącej środowiska bezpieczeństwa Polski wynika, że obecnie jednym z głównych czynników, które je kształtują, są agresywne działania Federacji Rosyjskiej. W obowiązującej aktualnie *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* wskazano, że (...) *Federacja Rosyjska prowadzi również działania poniżej progu wojny (o charakterze hybrydowym), niosące ryzyko wybuchu konfliktu (w tym niezamierzonego, wynikającego z gwałtownej eskalacji w rezultacie incydentu, szczególnie militarnego), a także podejmuje wszechstronne i kompleksowe działania za pomocą środków*

[15] Szerzej w: B. Bolechów, *Polityka antyterrorystyczna w świetle badań nad terroryzmem*, Wrocław 2012, s. 134–174.

[16] Tamże, s. 173.

[17] Tamże, s. 174.

pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych[18]. Działania poniżej progu wojny, w tym działania o charakterze hybrydowym, pozostają, jak już wspomniano, istotnym środkiem prowadzenia polityki, służącym podmiotom państwowym i pozapaństwowym do osiągania swoich celów. W aktywności Rosji, także podczas wojny z Ukrainą, jest widoczna strategia zakładająca odtworzenie i utrzymanie jej dawnej potęgi, jak również postrzeganie Zachodu jako zagrożenia. Aby to zagrożenie zneutralizować, Rosja dąży do wyparcia albo ograniczenia amerykańskiej obecności w Europie oraz do zminimalizowania wpływów europejskich i kontrolowania tego kontynentu. Marek Menkiszak pisze, że Federacja Rosyjska wyznaczyła sobie cztery główne cele strategiczne. Są to:

1. *Strategiczna kontrola nad obszarem postradzieckim (z czasowym wyłączeniem państw bałtyckich).*
2. *Stworzenie buforowej strefy bezpieczeństwa w Europie Środkowej.*
3. *Minimalizacja wpływów i obecności USA w Europie.*
4. *Maksymalizacja wpływów Rosji w Europie*[19].

Ich osiągnięcie umożliwiłoby stworzenie nowej architektury bezpieczeństwa europejskiego, w której Rosja odgrywałaby ważną rolę gospodarczą i polityczną. Działania hybrydowe są jednym z narzędzi pozwalających na wywieranie presji na państwa regionu. Ich celem może być wymuszenie określonego zachowania na państwach sąsiadujących z Rosją oraz zniechęcenie państw sojuszniczych do udzielenia pomocy zaatakowanym. To może się przekładać na bardziej szczegółowe cele operacyjne dotyczące poszczególnych państw. Autor niniejszego opracowania w 2019 r. zidentyfikował na przykład następujące cele działań hybrydowych wymierzonych w Polskę:

1. Uniemożliwienie użycia polskich i sojuszniczych sił zbrojnych oraz infrastruktury (dróg, linii kolejowych, portów, lotnisk, miejsc postojowych) w działaniach pomocowych dla Litwy, Łotwy i Estonii.
2. Zmuszenie Polski do wycofania się z wszelkich działań sprzecznych z interesami Rosji.
3. Potencjalnie – zmuszenie Polski do umożliwienia ustanowienia połączenia lądowego Rosji z Obwodem Kaliningradzkim lub

[18] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, s. 6 [dostęp: 22 VI 2022].

[19] M. Menkiszak, *Strategiczna kontynuacja, taktyczna zmiana. Polityka bezpieczeństwa europejskiego Rosji*, Warszawa 2019, s. 12.

przynajmniej doprowadzenie do przerwania połączenia lądowego Polski z Litwą.

4. Potencjalnie – zmuszenie Polski do usunięcia sił amerykańskich i innych sił NATO ze swojego terytorium[20].

Warto zauważyć, że kryzys migracyjny w 2021 r. był elementem działań hybrydowych i wyraźnie wpisywał się w punkt drugi z wyżej wymienionych, gdyż inspirowana przez władze białoruskie – za ewidentną wiedzą i zgodą władz Rosji – migracja osób do Polski (oraz innych państw UE) była odwetem za wsparcie prodemokratycznych protestów na Białorusi. Podczas tego kryzysu nie tylko została wywarta bezpośrednia presja na państwa i społeczeństwa, w tym służby odpowiedzialne za ochronę granic, lecz także starano się stworzyć narrację pokazującą Polskę, Litwę i Łotwę jako państwa niechętne uchodźcom i łamiące prawa człowieka. Dążono również do spolaryzowania opinii publicznej na tle kryzysu i wywołania kolejnych podziałów wewnętrznych[21].

To oznacza, że działania terrorystyczne jako część działań hybrydowych mogą być prowadzone z zamiarem osiągnięcia podobnych celów i można dopatrywać się podobieństw między nimi a kryzysem migracyjnym. Widoczne są cztery elementy, które charakteryzują działania terrorystyczne będące częścią działań hybrydowych i czynią je podobnymi do innych stosowanych narzędzi, na przykład presji migracyjnej.

Po pierwsze, państwo, które staje się celem działań terrorystycznych, jest zmuszone zmierzyć się przede wszystkim z bieżącym zagrożeniem bezpieczeństwa wewnętrznego. Może to oznaczać przekierowanie zasobów systemu bezpieczeństwa państwa na działania antyterrorystyczne oraz kontrterrorystyczne, zwłaszcza jeśli siły i środki przeznaczone do wykonywania tych zadań okażą się lub mogą okazać się niewystarczające. Koszty związane z samymi atakami oraz utrzymywaniem zasobów potrzebnych do ich powstrzymywania mogą także być wyższe niż korzyści wynikające z polityki prowadzonej przez atakowane państwo, co będzie prowadzić do jej szybkiej zmiany.

Po drugie, ataki terrorystyczne mogą wywołać nowe podziały społeczne oraz pogłębić istniejące, zwłaszcza jeśli są prowadzone przez państwo,

[20] M. Piekarski, *Polish Armed Forces and hybrid war: current and required capabilities*, „The Copernicus Journal of Political Studies" 2019, nr 1, s. 43–64.

[21] Szerzej w: A.M. Dyner, *Kryzys graniczny jako przykład działań hybrydowych*, Polski Instytut Spraw Międzynarodowych, 2 II 2022 r., https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych [dostęp: 22 VI 2022].

które pozoruje działania bytów faktycznie istniejących lub celowo wykreowanych (ataki pod fałszywą flagą).

Po trzecie, sposób reakcji państwa, który może prowadzić do ograniczenia praw, wolności i swobód obywatelskich, na przykład przez wprowadzanie zaostrzonych środków bezpieczeństwa, może skutkować kolejnymi podziałami społecznymi.

Po czwarte, należy mieć na uwadze, że działania prowadzone bezpośrednio przez aktora państwowego lub z jego wsparciem będą charakteryzować się potencjalnie szerszym zakresem środków bojowych, taktyk i technik działania, wykraczających poza obserwowane w ostatnich latach modus operandi sprawców zamachów terrorystycznych, którzy takim wsparciem nie dysponowali.

Te cztery elementy pozwalają doprecyzować scenariusze możliwych sytuacji kryzysowych. Nie jest bowiem zasadne analizowanie każdego możliwego przypadku zamachu terrorystycznego, lecz jedynie takich, które mieszczą się w tak zarysowanych warunkach brzegowych.

Możliwe scenariusze ataków

W niniejszej, zasadniczej części artykułu została przedstawiona analiza scenariuszy (z ich możliwymi wariantami) dotyczących wykorzystania terroryzmu jako narzędzia wojny hybrydowej. Scenariusze podzielono według kryterium potencjalnego celu ataku. Ten cel, a dokładniej jego rodzaj, jest czynnikiem porządkującym wewnętrzną logikę scenariusza, czyli możliwe korzyści i ograniczenia z punktu widzenia sprawców. Drugim czynnikiem ważnym dla wewnętrznej logiki scenariusza jest współistnienie innych form nacisku. Przy konstruowaniu scenariuszy wzięto pod uwagę stan prawny i organizacyjny w maju 2022 r. Pytaniem otwartym, na które w czasie powstawania artykułu nie można było udzielić odpowiedzi, jest wpływ konfliktu w Ukrainie na aktywność militarną i pozamilitarną Rosji.

Scenariusz 1. Zamach terrorystyczny wymierzony w infrastrukturę i sprzęt wojskowy

Słowo „wojna", będące jednym z członów pojęcia wojny hybrydowej, budzi skojarzenia z siłami zbrojnymi. Prawdopodobnym scenariuszem może zatem wydawać się atak na obiekty wojskowe. Instalacje wojskowe z definicji są ważne dla obronności państwa. Ich uszkodzenie lub zniszczenie oznacza

zmniejszenie potencjału obronnego państwa, a więc zwiększa podatność na presję militarną, w tym przypadku ze strony Rosji. Te same mechanizmy mogą zaistnieć w sytuacji ataku na przebywające w Polsce oddziały i pododdziały sił zbrojnych państw sojuszniczych. Należy jednak zauważyć, że osłabienie w ten sposób potencjału militarnego jest zadaniem trudnym. Przykładowo według dostępnych danych Siły Zbrojne Rzeczypospolitej Polskiej posiadały w 2021 r. 797 czołgów, 1611 bojowych wozów piechoty, 751 dział i moździerzy[22]. Trudno się spodziewać, aby jakiekolwiek działania terrorystyczne zdołały odczuwalnie osłabić ich potencjał. Część infrastruktury można względnie łatwo zastąpić inną. Na przykład zniszczone lub uszkodzone stałe stacje radiolokacyjne systemu Backbone mogą zostać zastąpione urządzeniami mobilnymi. Przy tym części obiektów nie byłoby łatwo zaatakować metodami typowymi dla organizacji terrorystycznych.

Sytuacja zmienia się, gdy możliwe cele zawęzi się jedynie do obiektów trudnych do łatwego zastąpienia, których uszkodzenie będzie miało wyraźny wpływ na zdolności SZ RP. Dla przykładu mniejszym zasobem pod względem liczebności są samoloty bojowe. Siły Powietrzne są wyposażone obecnie w 48 samolotów F-16C/D Block 52+, 29 samolotów MiG-29 oraz 18 samolotów Su-22M4/UM3K[23], przy czym dwa ostatnie typy zostaną wkrótce wycofane na rzecz 32 samolotów F-35A. Dokonanie ataku skutkującego zniszczeniem lub uszkodzeniem nawet tylko kilku samolotów bojowych spowoduje szkody w mieniu wojskowym, które należy szacować na dziesiątki milionów dolarów. Ponadto oznacza to trwałe lub czasowe wyłączenie z eksploatacji samolotów, których nie będzie można użyć do szkolenia i innych działań, na przykład rozpoznawczych lub ochrony własnej i sojuszniczej przestrzeni powietrznej.

Opisywany scenariusz miał swój odpowiednik w rzeczywistości. W 1981 r. celem ataku terrorystycznego stała się baza lotnicza Muñiz na wyspie Portoryko. Sprawcy zdołali podłożyć ładunki wybuchowe pod 11 samolotów typu A-7D i F-104[24]. Gdyby podobny atak zdarzył się w Polsce, zniszczenie lub uszkodzenie już ośmiu samolotów F-16 skutkowałoby wyeliminowaniem jednej szóstej posiadanych maszyn tego typu. Atak mógłby zostać dokonany przez infiltrację bazy lotniczej lub za pomocą

[22] *The Military Balance 2021*, The International Institute for Strategic Studies.

[23] Tamże.

[24] https://www.globalsecurity.org/wmd/ops/secmuniz.pdf [dostęp: 28 V 2022].

bezzałogowych statków powietrznych, zwłaszcza jeśli sprawcy byliby w stanie rozpoznać dogodną okazję do tego rodzaju działań.

Potencjalnymi celami ataków w SZ RP mogą być również inne urządzenia i systemy występujące w niewielkiej liczbie i trudne do szybkiego odtworzenia. Oczywistym ograniczeniem jest w tym przypadku konieczność identyfikacji przez sprawców adekwatnych celów ataku (urządzeń, sprzętu wojskowego) oraz uzyskanie dostępu do atakowanego obiektu, aby m.in. pozyskać informacje na temat jego działalności oraz zabezpieczeń.

Należy przy tym mieć na uwadze nie tylko stricte materialne i wojskowe konsekwencje takiego scenariusza. Skuteczny atak będzie bowiem bardzo łatwy do wykorzystania w działalności propagandowej i dezinformacyjnej, eksponującej fakt, że doszło do zamachu na obiekt wojskowy i zniszczenia sprzętu wojskowego. Może to obniżyć poziom zaufania społecznego do sił zbrojnych oraz polityki obronnej państwa.

Scenariusz 1a. Zamach terrorystyczny wymierzony w personel wojskowy

Scenariusz zakłada atak wymierzony nie w sprzęt wojskowy, lecz w żołnierzy. Atak może zostać przeprowadzony na terenie wojskowym (jak w przypadku zamachu z Fort Hood w 2008 r.) lub poza terenami i obiektami wojskowymi (jak w przypadku ataków we Francji w 2013 r.)[25] i następnie wykorzystany propagandowo. Z punktu widzenia sprawców istotnym wariantem tego scenariusza jest możliwość dokonania ataku na osoby przebywające poza obiektami wojskowymi – w miejscach zamieszkania, miejscach publicznych (środki transportu, placówki handlowe) i innych łatwo dostępnych, gdyż ułatwia to jego zaplanowanie i przeprowadzenie. Także zdobycie informacji na temat celu (konkretnej osoby lub osób) może być prostsze. Celem może być przede wszystkim personel wymagający długotrwałego szkolenia i trudny do zastąpienia. Są to osoby takie, jak:

- kadra dowódcza, zwłaszcza osoby w stopniach generalskich,
- personel latający oraz żołnierze wojsk specjalnych, członkowie załóg jednostek pływających,
- osoby zajmujące specjalistyczne stanowiska, zwłaszcza związane z obsługą ważnych systemów uzbrojenia oraz wsparcia i zabezpieczenia i mające dostęp do informacji wrażliwych,

[25] Szerzej w: M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020.

- osoby mogące w przyszłości zająć ważne stanowiska (osoby uczęszczające na kursy, szkolenia, kształcące się w akademiach wojskowych).

Atak na takie osoby oznacza, że podobnie jak w scenariuszu poprzednim jest możliwe zadanie poważnych strat siłom zbrojnym. Pozbawienie wojska osoby mającej specjalistyczną wiedzę i kwalifikacje może mieć negatywne skutki psychologiczne, podobnie jak w poprzednim scenariuszu. Należy zauważyć, że konsekwencje miękkie (psychologiczne i społeczne) będą poważniejsze niż twarde. Na przykład skuteczny zamach na dowódcę oddziału lub związku taktycznego spowoduje, że jego miejsce szybko zajmie osoba będąca na stanowisku zastępcy dowódcy. W przypadku innego personelu również jest mało prawdopodobne, aby jedna osoba była jedyną mającą unikalne kompetencje, w związku z czym będzie możliwe jej zastąpienie inną. Jednak skutki psychologiczne mogą być poważne zarówno dla sił zbrojnych, jak i dla społeczeństwa, gdyż atak na żołnierza, zwłaszcza zajmującego stanowisko dowódcze, może podważyć zaufanie społeczne do sił zbrojnych, a także mieć negatywny wpływ na morale żołnierzy.

W tym scenariuszu atak może mieć formę zabójstwa lub uprowadzenia osoby (na podobieństwo uprowadzenia gen. Jamesa Doziera w 1981 r. we Włoszech[26]). Ten drugi wariant należy ocenić jako bardziej skomplikowany i wiążący się z większym ryzykiem dla sprawców. Możliwe jest bowiem rozpowszechnianie wizerunku uprowadzonej osoby, zmuszenie jej do wygłoszenia oświadczenia o treści podyktowanej przez sprawców lub wręcz dokonanie egzekucji i upublicznienie jej nagrania. Co ważne, uprowadzona osoba może zostać nakłoniona lub zmuszona do ujawnienia informacji niejawnych. W tym scenariuszu zagrożone są także rodziny osób, które mogą być celem ataku. Ponadto należy brać pod uwagę ewentualność ataku wymierzonego w przebywających w Polsce żołnierzy sił zbrojnych państw sojuszniczych. Wówczas grupą docelową przekazu generowanego przez taki atak byłaby także opinia publiczna państw sojuszniczych.

Scenariusz 1b. Zamach terrorystyczny wymierzony w infrastrukturę i sprzęt służb policyjnych, wywiadowczych lub kontrwywiadowczych

Scenariusz jest odpowiednikiem scenariusza 1, z tą różnicą, że celem ataku są obiekty i wyposażenie wykorzystywane przez służby policyjne (Policję, Straż Graniczną) lub służby specjalne. Także w tym przypadku prawdopodobnym

[26] T. Philips, *The Dozier Kidnapping: Confronting the Red Brigades*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/phillips.pdf [dostęp: 28 V 2022].

celem są ważne urządzenia, trudne do szybkiego odtworzenia lub zastąpienia, jak również wywołanie zakłóceń w ich pracy, które utrudnią bieżące funkcjonowanie tych służb. Należy wskazać, że w przeciwieństwie do większości instalacji wojskowych obiekty służb policyjnych, takie jak placówki Straży Granicznej czy komendy Policji, są miejscem wykonywania czynności z udziałem osób cywilnych. Zamach wymierzony w siedzibę komendy Policji może więc znacznie obniżyć poziom zaufania do tej służby.

Scenariusz 1c. Zamach terrorystyczny wymierzony w personel służb policyjnych, wywiadowczych lub kontrwywiadowczych

Scenariusz jest odpowiednikiem scenariusza 1a. Jedyną różnicą jest tożsamość osoby lub osób, które są celem zamachu. Mogą to być przede wszystkim ludzie zajmujący ważne stanowiska w służbie śledczej lub kontrterrorystycznej Policji, komendanci Policji oraz osoby na kluczowych stanowiskach w służbach wywiadowczych i kontrwywiadowczych. Także w tym przypadku istotne może być psychologiczne i medialne znaczenie takiego ataku, podobnie jak w scenariuszu 1a.

Scenariusz 2. Atak na obiekt infrastruktury krytycznej

Scenariusz zakłada atak wymierzony w systemy oraz wchodzące w ich skład obiekty, urządzenia, instalacje i usługi, uznawane za infrastrukturę krytyczną w myśl przepisów *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[27], w tym zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, transportowe, zaopatrzenia w żywność i wodę, zapewniające ciągłość działania administracji publicznej.

Celem zamachu na takie obiekty może być zarówno zakłócenie lub uniemożliwienie ich funkcjonowania, jak i wywołanie lęku w społeczeństwie oraz podważenie zaufania obywateli do władz. Z tego powodu najbardziej prawdopodobnym celem ataku będą te obiekty i systemy, których zakłócenie okaże się najszybciej odczuwalne i możliwe do wykorzystania propagandowego. Można wskazać kilka możliwych wariantów tego scenariusza, które różnią się szczegółowym celem ataku.

Scenariusz 2a. Atak na infrastrukturę elektroenergetyczną

Scenariusz zakłada przeprowadzenie ataku wymierzonego w system elektroenergetyczny, a więc odpowiedzialny za wytwarzanie i dystrybucję

[27] Tekst jednolity: DzU z 2022 r. poz. 261, ze zm.

energii elektrycznej. Aby taki atak był skuteczny, sprawcy muszą zakłócić lub przerwać jeden z tych procesów. W Polsce energia elektryczna jest wytwarzana w elektrowniach różnego typu – cieplnych, wodnych, wiatrowych, jak również może być importowana z państw sąsiednich. Z uwagi na specyfikę obiektów energetycznych i ich zróżnicowanie zakłócenie lub przerwanie ich pracy może być trudne. Potencjalnie łatwiejszy byłby atak na sieć przesyłową. Jest ona położona na dużym obszarze i składa się z linii napowietrznych oraz punktów węzłowych (stacji elektroenergetycznych). Atak na takie instalacje, poprzez ostrzał z broni palnej, mechaniczne przewrócenie słupów czy podłożenie urządzeń wybuchowych, może doprowadzić do przerwania dostaw prądu do odbiorców, jak również spowodować przerwanie linii prowadzących z elektrowni[28]. W kontekście wojny hybrydowej należy uznać za prawdopodobne, że atak może zostać dokonany w sposób skoordynowany i doprowadzić do przerwania sieci zasilającej jedną lub nawet kilka dużych aglomeracji miejskich. Skonstruowanie urządzeń wybuchowych pozwalających na przerwanie linii z powodu wysadzenia słupów powinno być względnie łatwe w przypadku korzystania ze wsparcia służb wywiadowczych i wojsk specjalnych państwa, w tym przypadku Rosji, lub działań prowadzonych bezpośrednio przez te służby i wojska. Ataki na system elektroenergetyczny mogą być kontynuowane również po przywróceniu dostaw.

Konsekwencje tego rodzaju ataków mogą okazać się katastrofalne. Przerwanie dostaw energii do dużej aglomeracji miejskiej będzie oznaczać zahamowanie produkcji przemysłowej, działalności sektora usług, zakłócenie pracy szpitali oraz systemów komunikacyjnych i telekomunikacyjnych. Awaryjne, lokalne źródła zasilania (np. generatory) mogą zapewnić energię tylko niektórym odbiorcom i tylko przez określony czas. Prawdopodobne jest zaistnienie efektu kaskadowego, ponieważ wystąpią kolejne sytuacje kryzysowe. Przykładowo przerwanie dostaw prądu może wymusić ewakuację pacjentów szpitali, a jako że nie będą one mogły przyjmować nowych chorych, więc i te osoby będą musiały zostać przetransportowane do innych miast. Można spodziewać się także paraliżu systemu komunikacyjnego oraz innych systemów.

Atak tego rodzaju, nawet skutkujący tylko częściowym pozbawieniem zasilania, będzie wykorzystany w działaniach psychologicznych, mających

[28] Szerzej w: *IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector*, https://info.publicintelligence.net/DHS-ElectricGridAttacks.pdf [dostęp: 22 VI 2022].

na celu podważenie zaufania do władz państwowych oraz instytucji odpowiedzialnych za bezpieczeństwo państwa, i może mieć dalekosiężne skutki społeczne i polityczne.

Scenariusz 2b. Atak na infrastrukturę paliwową

Scenariusz zakłada atak wymierzony w instalacje i systemy służące do produkcji, transportu oraz dystrybucji paliw płynnych. Podobnie jak w przypadku infrastruktury energetycznej także te systemy składają się z miejsc wytwarzania lub importu paliw (rafinerie, kopalnie, platformy wydobywcze, terminale przeładunkowe) oraz infrastruktury transportowej. Zasadnicze różnice polegają w tym przypadku na możliwości magazynowania paliw (ropy naftowej, benzyny, gazu ziemnego) oraz zróżnicowaniu metod ich transportu (rurociągi, transport kolejowy, transport drogowy).

Szczególnie atrakcyjne z punktu widzenia sprawców mogą być ataki na infrastrukturę przeładunkową, magazyny paliw oraz transporty. Zakłócenie dostaw może nie tylko prowadzić do lokalnych braków paliw, lecz także mieć szersze konsekwencje. Przykładowo atak na morskie instalacje przeładunkowe gazu (terminal w Świnoujściu czy planowana instalacja pływająca w Zatoce Gdańskiej) może stanowić element działań powiązanych z presją ekonomiczną i polityczną, np. spowodowaniem kryzysu przez obce państwo występujące jednocześnie z ofertą wznowienia dostaw drogą lądową czy też innych korzyści[29].

Tego rodzaju zamach może być jedynie wstępem do akcji dezinformacyjnej, w której będą przedstawiane fałszywe informacje, sugerujące dużo większe straty i zakłócenia w dostawach paliw. To z kolei ma prowadzić do nieprzemyślanych działań osób prywatnych (np. wykupywania paliw w handlu detalicznym), co zaobserwowano po cyberataku na rurociąg Colonial Pipeline w USA.

Scenariusz 2c. Atak na infrastrukturę transportową

W tym scenariuszu atak jest wymierzony w obiekty i systemy związane z transportem drogowym, kolejowym, morskim i lotniczym. Może to być atrakcyjna opcja dla państwa prowadzącego działania hybrydowe z uwagi na znaczenie tych obiektów dla systemu obronnego państwa oraz funkcjonowania gospodarki. Dla przykładu, gdyby udało się zablokować ruch

[29] Szerzej w: M. Piekarski, *Bezpieczeństwo dostaw surowców energetycznych do Polski drogą morską*, „Wschodnioznawstwo" 2020, t. 14, s. 177–195.

w porcie morskim takim jak Gdańsk, wywołałoby to poważne konsekwencje gospodarcze związane z opóźnieniami w transporcie towarów, które musiałyby oczekiwać na udrożnienie portu lub zostać przeładowane w innym miejscu, co jest czasochłonne. Do próby blokady szlaków komunikacyjnych może dojść w czasie kryzysu i wówczas atak miałby szersze konsekwencje.

Jest to widoczne w kontekście wojny w Ukrainie. Polska to w tym przypadku państwo tranzytowe, przez które są transportowane środki pomocy dla zaatakowanego kraju, w tym sprzęt wojskowy. Jednocześnie w początkowym etapie konfliktu przez Polskę przemieszczały się duże grupy uchodźców, jak również było przewożone zboże, którego Ukraina nie mogła eksportować z powodu zablokowania czarnomorskich portów. Podjęcie działań terrorystycznych mających na celu sparaliżowanie choćby jednego dużego węzła kolejowego, takiego jak węzeł krakowski czy wrocławski, mogłoby w takiej sytuacji mocno skomplikować te formy pomocy Ukrainie.

Scenariusz 3. Atak na cel symboliczny

Scenariusz zakłada przeprowadzenie ataku na cel mający znaczenie nie gospodarcze lub militarne, lecz przede wszystkim symboliczne. Mogą to być osoby, miejsca lub przedmioty, takie jak miejsca kultu religijnego, zabytki, pomniki, oraz wydarzenia typu manifestacje czy imprezy masowe.

Tego rodzaju atak ma na celu wywołanie polaryzacji w społeczeństwie. Szczególnie atrakcyjne dla sprawców jest przeprowadzenie ataku pod fałszywą flagą, a więc w sposób upozorowany na działania innego aktora (organizacji lub ruchu ekstremistycznego). Po ataku możliwe jest dokonanie kolejnego, również mającego sugerować działania osób o innej (przeciwnej) orientacji ideologicznej. Celem jest suponowanie istnienia konfliktu głębszego niż faktycznie istniejący, sprowokowanie faktycznych napięć i rozpętanie spirali przemocy. Należy w tym scenariuszu spodziewać się szczególnie nasilonych działań dezinformacyjnych. Możliwe jest, że wykorzystywane środki techniczne będą ograniczone, z uwagi na konieczność zachowania pozorów działań osób lub grup niezwiązanych z aktorem państwowym i niewspieranych przez niego. Można wskazać trzy warianty tego scenariusza.

Scenariusz 3a. Zamach na osobę powszechnie znaną

Scenariusz zakłada przeprowadzenie prowokacji z wykorzystaniem zabójstwa, spowodowania uszczerbku na zdrowiu lub uprowadzenia osoby powszechnie znanej ze swojej działalności politycznej, społecznej lub

medialnej. Bardziej istotna jest w tym przypadku rozpoznawalność takiej osoby (w tym wywołana kontrowersyjnymi wypowiedziami) niż zajmowane przez nią aktualnie stanowisko. Może to być ktoś, kto nigdy nie zajmował stanowisk państwowych ani nie zasiadał w parlamencie. Atak na taką osobę byłby upozorowany na działanie osób z przeciwnego końca spektrum ideologicznego, a jego celem byłoby sprowokowanie osób identyfikujących się z wartościami i poglądami prezentowanymi przez ofiarę do nadmiernej reakcji emocjonalnej, podsycanej przez działania dezinformacyjne. Mogą one sugerować błędne działania organów państwowych prowadzących czynności dochodzeniowo-śledcze i operacyjno-rozpoznawcze bądź brak takich działań, a nawet wskazywać na udział w zamachu osób powiązanych ze służbami państwowymi.

Scenariusz 3b. Zamach w trakcie uroczystości, manifestacji lub innego wydarzenia o charakterze publicznym

Scenariusz zakłada, że celem zamachu jest uroczystość, manifestacja czy inne wydarzenie zorganizowane przez władze państwowe, samorządowe, organizację pozarządową lub wyznaniową. Celem ataku byłoby przede wszystkim wywołanie strachu, możliwe jest także spowodowanie ofiar w ludziach. Także w tym scenariuszu sprawcy będą dążyć do upozorowania ataku na czyn dokonany przez inną niż wspierana przez Rosję organizację (ruch) ekstremistyczną, pozostającą w opozycji do podmiotu organizującego dane wydarzenie.

Z uwagi na prawdopodobieństwo dużej liczby zabitych i rannych taki atak może prowadzić do silnej polaryzacji oraz skrajnych reakcji i być wykorzystany w końcowej fazie działań hybrydowych. Możliwe jest także dokonanie zamachu w sposób, który podważyłby wiarygodność organów państwowych. Należy się zatem spodziewać, że atak podczas uroczystości katolickich zostałby upozorowany na atak lewicowych ekstremistów, a zamach podczas lewicowej manifestacji – na atak organizacji skrajnie prawicowej.

Scenariusz 3c. Zamach na obiekt symboliczny

Scenariusz zakłada zamach wymierzony nie w osoby, lecz w mienie w postaci obiektów, takich jak pomniki, muzea, świątynie i inne obiekty mające znaczenie symboliczne dla społeczeństwa lub jego części. W tym przypadku atak miałby na celu jedynie wywołanie rozgłosu i zainteresowania mediów oraz opinii publicznej, stymulowanych działaniami dezinformacyjnymi.

Te czynniki sprawiają, że może to być atak, który okaże się wstępem do dalszych działań.

Scenariusz 4. Atak wykazujący nieefektywność działania służb

Ostatni spośród analizowanych scenariuszy jest szczególnym przypadkiem ataku. Jego celem nie byłoby bowiem zadanie strat, lecz przede wszystkim wykazanie nieefektywności polskich służb policyjnych i sił zbrojnych. W planie ataku zostałyby uwzględnione zidentyfikowane wcześniej deficyty systemu bezpieczeństwa państwa. Możliwe są dwa warianty. Zdarzenie stanowiłoby tak poważne wyzwanie, że reakcja na nie byłaby niemożliwa lub byłaby pośpieszna i prowizoryczna. Takim przypadkiem mogłaby być sytuacja zakładnicza o wysokim stopniu skomplikowania, np. na pokładzie jednostki pływającej (np. promu pasażerskiego) lub dużego budynku użyteczności publicznej. Sprawcy mogą deklarować wolę przedostania się wraz z zakładnikami do Rosji lub na Białoruś bądź też doprowadzić – co jest mniej prawdopodobne – do sytuacji, w której siłowa próba jej rozwiązania skutkowałaby dużą liczbą ofiar śmiertelnych. W każdym przypadku w gruncie rzeczy chodziłoby nie o osiągnięcie celu taktycznego, lecz o wykazanie nieefektywności polskich władz i służb, które nie zdołały rozwiązać sytuacji w sposób korzystny dla Polski. Stanowiłoby to podstawę do działań dezinformacyjnych i politycznych, a być może także militarnych. Takie ryzyko istnieje zwłaszcza na obszarach morskich, gdzie jest możliwe nawet doprowadzenie do zainscenizowanej operacji „odbicia" przez siły rosyjskie rzekomo uprowadzonej jednostki. Skuteczna operacja, zakończona ujęciem lub zabiciem bezpośrednich sprawców zdarzenia przez rosyjskie wojska specjalne lub jednostki kontrterrorystyczne FSB, zostałaby następnie wykorzystana propagandowo i politycznie jako „dowód" na niezdolność Polski do zapewnienia bezpieczeństwa na obszarach morskich oraz potwierdzenie skuteczności aparatu bezpieczeństwa Rosji.

Podsumowanie

Najważniejszym wnioskiem płynącym z przedstawionych scenariuszy jest konieczność stałego uwzględniania zagrożeń o charakterze terrorystycznym w działaniach na rzecz budowania odporności na zagrożenia hybrydowe. Kolejnym jest to, że zagrożenia terrorystyczne jako element wojny hybrydowej będą pochodną działań obcego państwa, co oznacza, że

preferencje w zakresie wyboru celów oraz metod dokonywania ataków byłyby odmienne niż w innych znanych nurtach terroryzmu. O ile w przypadku ataków sprawców należących do organizacji islamskich fundamentalistów lub wspierających je typowym wyborem były cele miękkie (kluby nocne, zakłady pracy, środki transportu pasażerskiego), o tyle przy zagrożeniach hybrydowych bardziej prawdopodobne są ataki na obiekty infrastruktury krytycznej czy obiekty wojskowe, a tylko jeden zestaw scenariuszy uwzględnia ataki na cele miękkie i tylko jeden z tego zestawu – ataki mogące skutkować dużą liczbą ofiar wśród osób cywilnych.

Zasadne jest więc uwzględnienie scenariuszy omówionych w artykule zarówno w planowaniu działań antyterrorystycznych, organizowaniu działań kontrterrorystycznych, jak i szerzej – w przygotowaniach do przeciwdziałania zagrożeniom hybrydowym. Należy przy tym pamiętać, że omawiane scenariusze wskazują na konieczność hybrydowej reakcji na tego rodzaju zagrożenia. Oprócz samych działań antyterrorystycznych i kontrterrorystycznych niezbędne będzie prowadzenie innych działań, w tym z zakresu przeciwdziałania dezinformacji i walki informacyjnej.

Bibliografia

Bolechów B., *Polityka antyterrorystyczna w świetle badań nad terroryzmem*, Wrocław 2012.

Galeotti M., *The Weaponisation of Everything: A Field Guide to the New Way of War*, New York–London 2022.

Makowski A., Kubiak K., *Terroryzm jako sposób prowadzenia wojny?*, „Raport – wojsko – technika – obronność" 1998, nr 4, 41–43.

Menkiszak M., *Strategiczna kontynuacja, taktyczna zmiana. Polityka bezpieczeństwa europejskiego Rosji*, Warszawa 2019.

Nadolski L.M., *Kampania zimowa w 2015 roku na Ukrainie*, Bydgoszcz 2017.

Piekarski M., *Bezpieczeństwo dostaw surowców energetycznych do Polski drogą morską*, „Wschodnioznawstwo" 2020, t. 14, s. 177–195.

Piekarski M., *Polish Armed Forces and hybrid war: current and required capabilities*, „The Copernicus Journal of Political Studies" 2019, nr 1, s. 43–64.

Piekarski M., Wojtasik K., *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020.

Seely R., *Defining Contemporary Russian Warfare*, „The RUSI Journal" 2017, t. 162, nr 1, s. 50–59.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego", wydanie specjalne: *Wojna hybrydowa*, s. 39–50.

The Military Balance 2021, The International Institute for Strategic Studies.

Źródła internetowe

Cullen P.J., Reichborn-Kjennerud E., *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, The Multinational Capability Development Campaign, 2017 r., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf [dostęp: 20 V 2022].

Dyner A.M., *Kryzys graniczny jako przykład działań hybrydowych*, Polski Instytut Spraw Międzynarodowych, 2 II 2022 r., https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych [dostęp: 22 VI 2022].

Gasztold A., Gasztold P., *The Polish Counterterrorism System and Hybrid Warfare Threats*, „Terrorism and Political Violence" 2020, https://www.tandfonline.com/doi/abs/10.1080/09546553.2020.1777110?journalCode=ftpv20 [dostęp: 28 V 2022].

Hoffman F., *Rise of the hybrid wars*, https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 29 IV 2022].

https://www.globalsecurity.org/wmd/ops/secmuniz.pdf [dostęp: 28 V 2022].

IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector, https://info.publicintelligence.net/DHS-ElectricGridAttacks.pdf [dostęp: 22 VI 2022].

Kosow H., Gaßner R., *Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria*, https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf [dostęp: 22 VI 2022].

Ogilvy J., *Scenario Planning and Strategic Forecasting*, Forbes, 8 I 2015 r., https://www.forbes.com/sites/stratfor/2015/01/08/scenario=-planning-and-strategic-forecasting/?sh-2de3fee5411a [dostęp: 18 V 2022].

Philips T., *The Dozier Kidnapping: Confronting the Red Brigades*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/phillips.pdf [dostęp: 28 V 2022].

Sovolainen J. i in., *Hybrid CoE Working Paper 5 Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans*, https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf [dostęp: 29 IV 2022].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 22 VI 2022].

Akty prawne

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2021 r. poz. 2234, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2022 r. poz. 261, ze zm.).

DOI: 10.4467/27204383TER.22.020.16340

ORCID: 0000-0001-9815-6035

KRZYSZTOF IZAK

Anders Behring Breivik. Studium przypadku skrajnie prawicowego terrorysty – samotnego wilka (część 1)

Abstrakt

Celem artykułu jest przedstawienie charakterystyki Andersa Behringa Breivika, w tym wpływu doświadczeń z dzieciństwa i wczesnej młodości na kształtowanie się jego osobowości, a także opisanie jego działalności i przygotowań do ataków przeprowadzonych 22 lipca 2011 r. w Oslo i na wyspie Utøya, jak również ich przebiegu. Autor poszukiwał odpowiedzi na pytania, czy istniała możliwość zapobieżenia tym zamachom oraz jaki wpływ miały one na nastroje społeczne, charakter zmian w kształtowaniu polityki bezpieczeństwa wewnętrznego w Norwegii i podniesienie sprawności działania służb bezpieczeństwa tego państwa. Podjął również próbę przeanalizowania, jaki poziom zagrożenia podobnym atakiem istnieje obecnie w Polsce. Wnioski płynące z tej analizy zostały wzbogacone o przemyślenia dotyczące następstw agresji Rosji na Ukrainę.

Słowa kluczowe:

Anders Breivik, aktywny strzelec, manifest, samotny wilk, terrorysta

W styczniu 2022 r. w światowych miediach pojawiły się doniesienia na temat złożenia przez Andersa Behringa Breivika wniosku o warunkowe zwolnienie z więzienia po odbyciu 10 lat kary pozbawienia wolności z zasądzonych 21 lat, na które został skazany w 2012 r. za zabójstwo 77 osób. Osoby zebrane w sali sądowej Breivik przywitał hitlerowskim gestem, a podczas swojego

wystąpienia wyrażał skrajne poglądy. Zapewniał jednak, że się zmienił i na wolności nie będzie już stosował przemocy. Twierdził, że można być nazistą, nie będąc wojownikiem, i odciął się od przemocy, terroryzmu oraz wytyczonych celów opisanych w swoim manifeście zatytułowanym *2083 – A European Declaration of Independence*[1] (2083 – Europejska Deklaracja Niepodległości). Wyraził opinię, że nie może ponosić odpowiedzialności za swoje czyny, ponieważ nie ze swojej winy został zindoktrynowany w internecie. Zapowiedział, że przez następne 50 lat będzie walczył w nordyckim ruchu oporu albo założy niewojowniczy ruch nacjonalistyczny w Europie. Oświadczył, że pracuje dla państwa nordyckiego i jest kandydatem do parlamentu z ramienia partii nazistowskiej. Na sali sądowej zaprezentował tekst pt. *Zatrzymać ludobójstwo naszych białych narodów*, czyli znany w prawicowych kręgach ekstremistycznych pogląd o zdominowaniu Zachodu przez imigrantów obcych etnicznie i kulturowo. Jedną z ulotek Breivik umieścił w kieszonce garnituru, aby była lepiej widoczna, drugą natomiast przykleił do teczki, którą pokazywał w trakcie posiedzenia sądu. Przekonywał także, że może zrezygnować z działalności politycznej, jeśli taki warunek postawi sąd. Wówczas będzie gotów przenieść się np. na Svalbard (norweski archipelag na Oceanie Arktycznym) i zająć się biznesem albo w ogóle opuścić Zachód. Sąd odrzucił jego prośbę o zwolnienie warunkowe. Złożenie przez Breivika takiego wniosku prokurator Hulda Karlsdottir nazwała zabiegiem o charakterze public relations, mającym na celu poprawę warunków jego przetrzymywania i przypomnienie o sobie. Niekorzystne dla osadzonego były również opinie psychiatry i władz więziennych. Teoretycznie może on ponownie wystąpić o zwolnienie warunkowe za rok i powtarzać tę prośbę co 12 miesięcy. Bardziej prawdopodobne jest jednak, że będzie on przetrzymywany za kratami do śmierci na podstawie zasądzania kolejnych lat pozbawienia wolności, na co zezwala norweskie prawo karne[2].

Ataki terrorystyczne przeprowadzane w pierwszej dekadzie XXI w. utwierdzały międzynarodową opinię publiczną w przekonaniu, że radykalny

---

[1] Zob. A. Berwick, *2083. A European Declaration of Independence. De laude novae militiae. Peuperes commilitiones Christi Templique Solomonici*, London 2011, https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf, s. 1437 [dostęp: 1 II 2022].

[2] J. Potocka, *Hitlerowskie pozdrowienie i nowe hasła. Breivik chce wyjść na wolność*, RMF24, 18 I 2022 r., https://www.rmf24.pl/raporty/raport-zamachy-w-norwegii/fakty/news-hitlerowskie-pozdrowienie-i-nowe-hasla-breivik-chce-wyjsc-na,nId,5777148#crp_state=1 [dostęp: 18 I 2022]; A. Grochot, *Anders Breivik zostanie w więzieniu. Sąd odrzucił jego wniosek*, RMF24, 1 II 2022 r., https://www.rmf24.pl/fakty/swiat/ news-anders-breivik-zostanie-w-wiezieniu-sad-odrzucil-jego-wniose,nId,5806130#crp_state=1 [dostęp: 1 II 2022].

islam stanowi główne zagrożenie bezpieczeństwa i ładu światowego. Ten przekaz wzmacniały działania w ramach wojny z terroryzmem ogłoszonej przez prezydenta George'a W. Busha po atakach terrorystycznych w USA z 11 września 2001 r. Krwawe zamachy dokonywane przez islamskich ekstremistów w Europie, od Rosji po Hiszpanię, spowodowały, że prawie każde kolejne tego rodzaju zdarzenie natychmiast przypisywano Al-Ka'idzie lub organizacjom i osobom zainspirowanym ideologią i działalnością ugrupowania Osamy bin Ladena[3]. Nie inaczej było tuż po doniesieniach o ataku terrorystycznym w Oslo i masakrze na wyspie Utøya, do których doszło 22 lipca 2011 r. Zanim ujęto ich sprawcę, jeden z polskich ekspertów od terroryzmu wygłosił w telewizji opinię, że stoją za tym islamscy radykałowie. Podobne głosy pojawiały się w Norwegii i innych państwach do momentu, gdy okazało się, że sprawcą ataku jest Anders Breivik, nieznany wówczas szerzej norweski skrajny nacjonalista.

Celem niniejszego artykułu jest przedstawienie charakterystyki Breivika i jego działalności oraz opisanie przygotowań do ataku i jego przebiegu. Autor poszukiwał odpowiedzi na pytania, czy istniała możliwość zapobieżenia zamachowi oraz jaki wpływ miał on na nastroje społeczne, charakter zmian w kształtowaniu polityki bezpieczeństwa wewnętrznego w Norwegii i podniesienie sprawności działania służb bezpieczeństwa tego państwa. Podjął również próbę przeanalizowania, czy obecnie istnieje zagrożenie podobnym atakiem w Polsce. Zaistnienie takiego zdarzenia wydaje się realne nie tylko z powodu pojawienia się naśladowców Breivika, którzy dali o sobie znać w różnych państwach, lecz także z uwagi na radykalizację postaw i nastrojów społecznych oraz ostry dyskurs polityczny w Polsce, nieco złagodzony w ostatnim czasie z powodu sytuacji w Ukrainie. Wnioski płynące z tej analizy zostały wzbogacone o przemyślenia dotyczące następstw agresji Rosji na Ukrainę. Jeśli nie dojdzie do eskalacji działań wojennych, można założyć, że jej skutkiem będą ataki terrorystyczne za naszą wschodnią granicą. Do zamachów może dojść także na terytorium Polski. Należy również liczyć się z działaniami dywersyjnymi. Wojna w Ukrainie, jak każda inna, ułatwi dostęp do broni, amunicji i materiałów wybuchowych. Ich posiadanie przez ekstremistów może mieć tragiczne konsekwencje. W przypadku rozszerzenia działań wojennych na inne państwa część wniosków sformułowanych na końcu artykułu będzie nieaktualna z uwagi na nowe

[3] Wyjątkiem był atak na pociągi kolei podmiejskiej w Madrycie przeprowadzony 11 III 2004 r. Zaraz po poinformowaniu szefa rządu o tych wydarzeniach premier José Luis Rodríguez Zapatero ogłosił w telewizji, że za atakiem stoją terroryści z ETA.

zagrożenia i wyzwania, których skalę trudno obecnie przewidzieć. Stan wojny zmieni optykę postrzegania zagrożenia terrorystycznego.

W artykule autor posłużył się następującymi metodami badawczymi: historyczną – pozwalającą prześledzić życiorys Breivika, behawioralną – przy analizie jego zachowań, porównawczą, za pomocą której skonfrontował działalność Breivika i innych terrorystów motywowanych antyimigrancką, rasistowską ideologią.

Biografia zamachowca

W swojej książce poświęconej casusowi Breivika Elżbieta Czykwin napisała:

> Kluczem do zrozumienia trajektorii życia Andersa Breivika zdaje się analiza jego więzi rodzinnych. Zostały one naruszone w poważny sposób od urodzenia. Matka, która była niewątpliwie najważniejszą osobą w jego życiu, wniosła do kadłubowej rodziny bagaż psychiczny obciążający ich relacje w zasadniczym stopniu. Wenche nie radziła sobie z samą sobą, czego symptomem było zarówno niechciane i dość przypadkowe pierwsze dziecko, jak i niechciane drugie. Rozwód ujawnił wyraźnie niestabilność jej psychiki, chorobę dwubiegunową i trudności w ułożeniu sobie relacji z mężem. Patologiczny bagaż dzieciństwa stał się udziałem nie tylko jej, lecz także Andersa[4].

W dorosłym życiu Breivik wykazywał cechy emocjonalnej deprywacji, narcyzmu i mizoginizmu. To w połączeniu z poczuciem wyobcowania, nienawiścią, wyznawaniem skrajnie prawicowej ideologii i wpływem gier komputerowych doprowadziło go do dokonania wielokrotnego zabójstwa na niespotykaną skalę. Unni Turrettini wskazała na podobieństwa traumatycznego dzieciństwa Breivika do doświadczeń Timothy'ego McVeigha[5] i Theodore'a

[4] E. Czykwin, *Anders Breivik. Między dumą a wstydem*, Warszawa 2019, s. 87. W tej części artykułu większość informacji dotyczących Breivika została zaczerpnięta z tej książki.

[5] Dnia 19 IV 1995 r. Timothy McVeigh zdetonował samochód wypełniony 2,5 t materiałów wybuchowych przy budynku federalnym w Oklahoma City. Eksplozja spowodowała częściowe zawalenie się obiektu i śmierć 169 osób (ponad 500 zostało rannych). Śledztwo wykazało, że sprawca był związany z ruchem radykalnie prawicowej milicji stanu Michigan, jakich wiele do tej pory działa w USA. McVeigh został skazany na karę śmierci.

Kaczynskiego[6], które miały wpływ na ich dorosłe życie przepełnione nienawiścią i agresją[7].

Anders Behring Breivik urodził się 13 lutego 1979 r. w Oslo. Jego matka, Wenche Behring (zm. w 2013 r.), pochodziła z ubogiej rodziny. Już jako kilkuletnia dziewczynka opiekowała się swoją matką sparaliżowaną w wyniku porodu, która obwiniała ją o swoje kalectwo i nienawidziła. Ojciec Wenche zmarł wcześnie, a rodzina była wykluczona z lokalnej społeczności. Notabene siostra Breivika w pewnym sensie powieliła los matki i w wieku kilku lat przejęła funkcje opiekuńcze w rodzinie. Wenche ukończyła kurs pielęgniarski i pracowała w szpitalu jako salowa. Momentem przełomowym w jej życiu było poznanie Jensa Breivika, dyplomaty, starszego od niej o 12 lat rozwodnika i ojca trójki dzieci. Pół roku po przyjściu na świat Andersa rodzina wyjechała do Londynu, gdzie Jens został oddelegowany do pracy w ambasadzie Norwegii. Po kolejnych sześciu miesiącach Wenche zażądała rozwodu i wróciła z Andersem i jego przyrodnią siostrą Elisabeth do Oslo, gdzie zajęła mieszkanie byłego już męża. Matka nie dawała sobie rady z dziećmi, szczególnie z Andersem, na co zwracał uwagę Bernevernet – norweska instytucja państwowa zajmująca się działalnością na rzecz zapewnienia właściwych warunków socjalnych i wykształcenia dzieciom i młodzieży pochodzących z trudnych środowisk. Bernevernet nie przekazał jednak Andersa do rodziny zastępczej. Matka była niewykształconą salową, ojciec należał do elity. Breivik aspirował do statusu ojca, ale czuł, że w norweskim społeczeństwie zajmuje niską pozycję odziedziczoną po matce. Miał przy tym okazję zobaczyć świat ojca. Do szkoły uczęszczał w najelegantszej dzielnicy Oslo, a wcześniej chodził do przedszkola z wnukiem norweskiego króla. Miał poczucie przynależności do elity, a z drugiej strony zdawał sobie sprawę, że od kolegów dzieli go przepaść materialna. Był również przeciętnym uczniem. Sąsiedzi nie lubili go z powodu jego arogancji, nieuprzejmości, braku wychowania i prześladowania słabszych

[6] Theodore D. Kaczynski, znany jako „Unabomber", w latach 1978–1995 przesyłał ładunki wybuchowe pocztą. W wyniku ich eksplozji zginęły 3 osoby, a 29 zostało rannych. Kaczynski sprzeciwiał się niszczeniu środowiska naturalnego przez współczesny przemysł i postanowił z tym walczyć. Przez wiele lat, mimo najdłuższego i najdroższego śledztwa w historii FBI, pozostawał nieuchwytny. Został zidentyfikowany w 1995 r., gdy amerykańskie media opublikowały jego manifest. Poglądy w nim zawarte rozpoznał brat „Unabombera" i wydał go władzom. Zamachowiec został aresztowany w 1996 r. Sąd skazał go na dożywotne więzienie bez możliwości zwolnienia warunkowego. Karę odbywa w więzieniu w Kolorado.

[7] U. Turrettini, *The Mystery of the Lone Wolf Killer: Anders Behring Breivik and the Threat of Terror in Plain Sight*, New York 2015, s. 16–31.

od siebie. Wyraźną przyjemność sprawiało mu przyglądanie się cierpieniom innych dzieci i zwierząt, dla których sam był okrutny. W tym okresie jego relacje z ojcem układały się poprawnie. Jens ożenił się ponownie i zamieszkał we Francji. Anders bywał u niego i nawet polubił nową żonę ojca. W wieku 13 lat dostał się do gimnazjum. Zaczął budować swoją tożsamość przez uczestnictwo w subkulturze grafficiarzy. Przyjął wówczas pseudonim „Morg" i starał się zdominować grupę podobnych mu młodych ludzi. Szczególnie dobrze czuł się w towarzystwie grafficiarzy pochodzących ze środowiska arabskich imigrantów. W tym czasie graffiti nie postrzegano społecznie jako niewinny, artystyczny wyraz kreatywności młodych, lecz jako działalność nielegalną, chuligańską, rodzaj wandalizmu ściganego przez policję. Breivik również został przez nią zatrzymany. Reakcją Jensa na zaangażowanie syna w środowisko grafficiarzy było zerwanie z nim kontaktów, zgodnie z umową, jaką między sobą zawarli. Z czasem „Morg" został jednak wykluczony z tego środowiska za próbę narzucenia mu swej dominacji. Stracił w nim pozycję i był poniżany. Wyrok wydany przez społeczność grafficiarzy przypieczętował zmarginalizowanie Andersa przez kolegów w szkole.

W wieku 16 lat Breivik dostał się do prestiżowego Liceum Handlowego w Oslo. Przestał używać języka ulicy, prezentował się jako chłopak otwarty i sympatyczny. Zaczął uważać się za metroseksualnego[8]. Spędzał dużo czasu przed lustrem, nosił makijaż. Poddał się nawet operacji plastycznej nosa. Jednak w sensie osobowościowym nie był metroseksualny, w jego przypadku można raczej mówić o pozie. Od okresu dorastania Breivik poświęcał wiele czasu na trening siłowy, zaczął przyjmować sterydy anaboliczne, przez co wyglądał na dużego i silnego. W trakcie nauki w Liceum Handlowym pracował w charakterze telemarketera i był dobrym sprzedawcą. Zaczął grać na giełdzie i na jednej tylko transakcji zarobił 200 tys. koron (ok. 90 tys. zł). W związku z tym w 1998 r. porzucił szkołę i powziął plan zostania milionerem. Widział też siebie jako członka loży masońskiej. Upatrywał w tym możliwość wybicia się i znalezienia wśród elity. Nie znał jednak nikogo, kto mógłby go wprowadzić do masonerii. Pragnął być kimś

[8] Terminu „metroseksualny" użył po raz pierwszy w 1994 r. Mark Simpson, felietonista „The Independent". Neologizm ten, wywodzący się ze słów „metropolia" i „heteroseksualizm", odnosi się do stereotypu zakochanego w sobie mężczyzny, mieszkańca wielkiego miasta, skoncentrowanego na własnej aparycji, kojarzonego raczej z kobiecą dbałością o urodę oraz przejawiającego stereotypowo kobiece cechy osobowości, takie jak: uczuciowość, wrażliwość, delikatność, ciepło, empatia.

z nadania, z tytułu, a nie tym, kto pracą i oddaniem innym zasługuje sobie na szacunek i społeczną aprobatę. Nie miał matury, ale chwalił się, że przeczytał wystarczająco dużo, by być tytułowanym „bachelor of small business and management" (licencjat z małego biznesu i zarządzania), jak i tym, że zapoznał się ze wszystkimi lekturami obowiązującymi na studiach ekonomicznych. Do 2001 r. pracował w firmie telemarketingowej Direkte Respons Senteret, w której awansował na stanowisko szefa działu obsługi klienta. Jeszcze w Liceum Handlowym zaczął widzieć swoje miejsce w prawicowej Partii Postępu (norw. Fremskrittspartiet). Poznał Lene Langemyr, aktywistkę młodzieżówki tej partii. Lene została adoptowana przez rodzinę norweską jako porzucone w Indiach półtoramiesięczne hinduskie niemowlę. Uważała jednak, że Norwegia powinna zaostrzyć politykę imigracyjną oraz wzmocnić armię. Antyimigranckie hasła już w latach 80. XX w. były źródłem wzrastającej popularności Partii Postępu, będącej w opozycji do Partii Pracy (norw. Arbeiderpartiet)[9]. Lene i Anders zaczęli myśleć o karierze politycznej. Łączyły ich nie tylko ambicje polityczne związane z Partią Postępu, antyimigrancka retoryka, stygmat odrzucenia z dzieciństwa, lecz także zamiłowanie do broni. Anders był ekspertem w tej dziedzinie. Było to zadziwiające, tym bardziej że pominięto go w poborze ze względu na karalność (malowanie graffiti). On sam twierdził, że uzyskał zwolnienie ze służby wojskowej ze względu na opiekę nad chorą matką. Politycznym celem Breivika było znalezienie się na liście wyborczej radnych w Oslo. Nie był jednak dobrym mówcą. Jego atut stanowiła stała obecność w cyberprzestrzeni, co utrudniało mu jednak osobisty udział w życiu partyjnym. To sprawiło, że nie został umieszczony na liście partyjnej ani nawet wezwany na rozstrzygającą rozmowę. Czuł się upokorzony, zwłaszcza że znaleźli się na niej Lene i jego partyjny przełożony, którzy zostali radnymi miejskimi.

W 2001 r. Breivik założył działającą na granicy prawa firmę E-Commerce Group, która sprzedawała dyplomy-gadżety (w Polsce podobne produkty oferowane w internecie, w tym repliki dowodów osobistych czy praw jazdy, są nazywane dokumentami kolekcjonerskimi), np. ukończenia dowolnych studiów na którejkolwiek uczelni, w przystępnej cenie ok. 100 dolarów. Jego firma zastrzegała sobie na stronach internetowych, że dyplomy są oferowane jako rekwizyty i ozdoby. Podpisy na nich były fikcyjne, elektronicznie wygenerowane, nikt więc nie mógł wnieść pozwu o naruszenie dóbr osobistych. Z drugiej strony te dokumenty mogły być wykorzystywane

[9] Do 2011 r. działała jako Norweska Partia Pracy (norw. Det norske Arbeiderparti).

przez imigrantów do legalizacji pobytu, a wysyłane poza Europę – stanowić podstawę do uzyskania wizy państwa, w którym była zlokalizowana uczelnia wydająca oryginalne dyplomy. W swojej firmie Anders zatrudnił matkę (do sprzątania i prania) oraz pochodzącego z Indonezji grafika, który miał tworzyć wzory dokumentów. Początkowo miał on wątpliwości co do legalności tego rodzaju działań, jednak za 30 tys. koron miesięcznie podjął się tej pracy i okazał się bardzo sprawnym projektantem. Breivik zaoferował mu wyższą pensję w zamian za pracę na czarno, ale grafik nie przyjął oferty. Jednak i ta firma nie przetrwała zbyt długo, podobnie jak kolejne, w tym zajmująca się wynajmem powierzchni reklamowej na bilboardach.

W lutym 2004 r. Anders pojechał wraz z matką na Maltę w ramach dziesięciodniowej wycieczki. Być może właśnie wtedy obudziła się w nim fascynacja krzyżowcami. W tym czasie zaczął też szukać dziewczyny w serwisach internetowych krajów Europy Wschodniej. Uważał bowiem, że taka kobieta będzie mu uległa i podporządkowana, w przeciwieństwie do wyzwolonych Norweżek. W białoruskim serwisie randkowym zamówił za 100 euro dane kontaktowe kobiet i wyselekcjonował z nich dwie, po czym matka zdecydowała o ostatecznym wyborze. Padł on na Nataszę z Mińska, która mieszkała w bloku położonym w robotniczej dzielnicy i słabo mówiła po angielsku. W 2005 r. Anders odwiedził ją w Mińsku, a ona, na jego zaproszenie i z zakupionym przez niego biletem, przyjechała potem do Oslo. Rozstali się jednak bez większych emocji. On uważał ją za łowczynię posagów, ona jego za męskiego szowinistę. Zdaniem niektórych Breivik miał skłonności homoseksualne i dlatego nie układało mu się w związkach z kobietami, ale przyczyną mogła być też jego nieumiejętność nawiązywania relacji i więzi z ludźmi. Pewnego razu Wenche z synem zostali zaproszeni do kuzyna matki, który okazał się członkiem loży masońskiej. Breivik, który – jak już wspomniano – marzył o wstąpieniu do tej wspólnoty, zapytał wuja o taką możliwość. Ten podkreślił znaczenie braterstwa masonów, wartości chrześcijańskich, szlachetności, pokory i tolerancji. Andersowi nie chodziło jednak o poczucie wspólnoty. Pragnął stać ponad innymi. Dzięki protekcji wuja Breivik mimo trudności miał zostać przyjęty do loży. Tak się nie stało, ponieważ nowa fascynacja sprawiła, że nie miał na nic czasu, nawet na udział w uroczystej ceremonii przyjęcia do masonerii. Tą fascynacją stały się gry komputerowe. Nie przeszkadzało mu to później sfotografować się w eleganckim stroju przyozdobionym symbolami masonerii. Nie był to jedyny ubiór, który miał go dowartościować i ujawnić jego próżność. Robił sobie zdjęcia również w wojskowym mundurze galowym oficera, z przypiętymi

odznaczeniami i baretkami odznaczeń, kombinezonie płetwonurka sił specjalnych marynarki czy też kombinezonie przeciwchemicznym[10].

Po skończeniu 27 lat Anders wprowadził się z powrotem do matki. Jako „Andersnordic" przez dwa lata grał w grę komputerową po 17 godzin na dobę, co pozwoliło mu stać się przywódcą gildii „Virtue" (Cnota). Otrzymał też tytuł „Justicar". Przewodniczenie gildii nakładało na niego obowiązek podtrzymywania motywacji uczestników, którzy często podobnie jak Breivik popadali w uzależnienie. On uzależnił się pod wpływem „World of Warcraft". Łaknącym sukcesu jednostkom pokroju Breivika gra ta może bardzo odpowiadać, gdyż oferuje przejrzystą strukturę awansu i drogi do jego osiągnięcia. Zaszyty w rodzinnym domu coraz bardziej zagłębiał się w świat magów i walki na miecze. Potrzebę elitaryzmu, sukcesu i więzi zaspokajał w wirtualnym świecie. Kilka lat spędzonych na grach pozwoliło mu też poznać inny wirtualny świat, w tym środowisko muzułmańskich ekstremistów. Zgłębiał w sieci wiedzę na temat islamu, *Koranu* i wypraw krzyżowych. Zainteresował się również stronami antymuzułmańskimi i antyimigracyjnymi, szczególnie portalem Stormfront, którego hasło: „White Pride, World Wide" (Biała duma, cały świat) przypadło mu do gustu. Pragnął walczyć o czystość Europy białego człowieka, czyli jak twierdził – bronić Europy przed Eurabią (arabskimi wpływami na kontynencie). Coraz więcej myślał o islamizacji Europy. Swoimi przekonaniami na temat zagrożeń, jakie niosą za sobą imigranci z krajów arabskich, zamęczał swoje nieliczne otoczenie. Matka miała nadzieję, że to chwilowy etap, który minie, gdy jej syn znajdzie w końcu pracę i kandydatkę na żonę. Znajomi zbywali jego wykłady i coraz rzadziej zapraszali na spotkania towarzyskie. Z czasem Breivik zaczął tworzyć alternatywną rzeczywistość. Marzyło mu się powołanie ogólnoeuropejskiego ruchu oporu przeciwko islamowi, na którego czele miał sam stanąć. Aby przekazać światu swoje, jak mniemał odkrywcze i rewolucyjne idee, postanowił napisać książkę. Nie miał talentu pisarskiego ani charyzmy przywódczej, dlatego w swoim „dziele" posługiwał się głównie tendencyjnie wybieranymi fragmentami *Koranu* i innych tekstów, często po prostu przekopiowanych. Znaleźć tam można m.in. odniesienia do manifestu wspomnianego Theodore'a Kaczynskiego. Selekcjonował fakty, aby pasowały do jego tezy. Wszędzie widział teorie spiskowe. Problem z islamem porównał do pękniętego kranu. Kiedy woda

[10] *Profile: Anders Behring Breivik*, BBC, 12 IV 2012 r., https://www.bbc.com/news/world-europe-14259989 [dostęp: 14 V 2012].

zalewa łazienkę, najpierw należy zająć się usunięciem usterki, a nie jej wycieraniem. Wodą byli dla niego muzułmanie, uszkodzonym kranem – norweski rząd i partie lewicowe. To może tłumaczyć, dlaczego Breivik zaatakował nie imigrantów, tylko rządową dzielnicę Oslo oraz zjazd młodzieżówki Partii Pracy[11].

Pragnienie autorytetu i więzi było w Breiviku zbyt silne, aby mogło pozostać niewyrażone. Anders znalazł więc kogoś, z kim podzielał poglądy i bez reszty się identyfikował. Był to bloger Peder Are Nøstvold Jensen, znany w sieci pod pseudonimem „Fjordman". Głosił on hasła nienawiści do imigrantów, które łączył z apokaliptycznymi proroctwami. Taka narracja wnosiła element transcendentności i przypominała nieco wirtualny świat gier, w którym Anders mentalnie przebywał w ciągu ostatnich kilku lat. Zwrócił się do „Fjordmana" słowami: *Keep up the good work mate. You are a true hero of Europe* (Kontynuuj swoją dobrą robotę, przyjacielu. Jesteś prawdziwym bohaterem Europy). W mailu do niego, w którym Anders chciał zarekomendować swoją książkę, napisał: *Duża część posiadanej przeze mnie wiedzy pozostaje niedostępna dla większości ludzi, nawet dla Ciebie*[12]. W innym liście ocenił: *Pokonanie Eurabii jest genialne*[13]. „Fjordman" go jednak zignorował, a więc i tym razem Breivik poczuł się osamotniony. Skoncentrował się więc na pisaniu manifestu, co spowodowało, że coraz bardziej oddalał się od środowiska graczy „World of Warcraft". Podobnie jak w grach podążał jednak mentalnie w kierunku coraz większego autorytaryzmu i okrucieństwa. Opowiadał się za deportacją wszystkich muzułmanów z Europy. Aby dotrzeć ze swoimi ideami do jak największej liczby ludzi, zapragnął założyć konserwatywną gazetę. Przy okazji proponował i rozwijał nierealistyczne projekty i chwalił się swoimi wpływami w Partii Postępu i loży masońskiej. Kiedy w 2009 r. Partia Postępu po raz kolejny przegrała wybory do Stortingu (parlamentu norweskiego), Breivik zwrócił się do niej o pomoc w utworzeniu nowej gazety. Odmowa spowodowała, że ponownie doznał upokorzenia i doświadczył wyalienowania.

---

[11] A. Sobańda, *Skąd wziął się Breivik i czy można go było powstrzymać? Przejmująca opowieść o Norwegii*, Dziennik, 21 VIII 2015 r., https://kultura.dziennik.pl/ksiazki/artykuly/498350,-jeden-z-nas-przejmujaca-opowiesc-o-norwegii-autorstwa-asne-seierstad.html [dostęp: 24 VIII 2015].

[12] Å. Seierstad, *Jeden z nas. Opowieść o Norwegii*, Warszawa 2013, s. 71. Książka, o której Breivik wspominał w liście do „Fjordmana", to jego słynny manifest, nad którym pracował.

[13] Tamże.

Przygotowania do zamachu

W swoim manifeście Breivik stwierdził, że dziewięcioletni plan przygotowań do ataków terrorystycznych rozpoczął w 2002 r., kiedy miał 23 lata. W celu ich sfinansowania utworzył własną firmę programistyczną. Swój pierwszy milion koron miał zarobić w wieku 24 lat. Stracił dwa miliony na spekulacjach giełdowych, ale wciąż posiadał dwa miliony koron na sfinansowanie ataku[14]. Informacje, w których Anders kreuje się na człowieka finansowego sukcesu, są sprzeczne z jego biografią. W opisywanym przez niego okresie posiadał on wspomnianą już firmę E-Commerce Group. Mimo popytu na wytwarzane przez nią dokumenty, trudno uznać, aby handel nimi przyniósł Breivikowi milionowe zyski. W kolejnych latach też nie mógł zajmować się planowaniem zamachu, ponieważ bez reszty pochłaniały go gry komputerowe. Lekceważenie ze strony „Fjordmana" mogło wywołać w Andersie chęć pokazania jemu i innym, że stać go na wiele więcej niż tylko napisanie książki. Myśl o przelaniu krwi w imię jedynej słusznej idei mogła narodzić się w głowie Breivika już w trakcie jej pisania. Kolejne części manifestu pokazują nasilanie się radykalizacji. Z początku jest on dość umiarkowany, zawiera treści i koncepcje krążące wówczas w internecie. Potem wyrażane opinie stają się coraz bardziej radykalne, a pod koniec słowa Breivika są jawnym nawoływaniem do walki i przelewania krwi. Rewolucji kulturowej, przywracającej Norwegii czystość rasy, miała przewodniczyć organizacja Knights Templar, którą Breivik powołał na kartach swojego „dzieła", a siebie uczynił w niej najwyższym rangą Komandorem Antykomunistycznego Ruchu Oporu Przeciwko Islamizacji Europy i Norwegii. Breivik gardził lewicowymi poglądami, był przeciwny feministkom, równouprawnieniu, tolerancji dla mniejszości seksualnych. Główne zagrożenie widział jednak w imigrantach, którzy jego zdaniem niszczyli kulturę i społeczeństwo Europy. Wyrazem postępującej radykalizacji Breivika było podjęcie przygotowań do zamachu. Ich rozpoczęcie należy datować na 2009 r. W dniu 18 maja Anders zarejestrował wtedy jednoosobową firmę Geofarm, mającą rzekomo prowadzić działalność rolniczą, w tym uprawę warzyw. W następnym roku w piwnicy domu, w którym mieszkała matka, zaczął gromadzić środki chemiczne[15].

[14] *Norway gunman claims he had nine-year plan to finance attacks,* The Guardian, 25 VII 2011 r., https://www. theguardian.com /world/2011/jul/25/norway-gunman-attack-funding-claim [dostęp: 27 I 2022].

[15] A. Sobańda, *Skąd wziął się Breivik...*

Część jego planu opierała się na użyciu broni palnej. Na początku 2009 r. Breivik został zatrzymany podczas rutynowej kontroli w pobliżu miasta Wetzlar, niedaleko Frankfurtu nad Menem. Norweg miał przy sobie amunicję i części uzbrojenia. Amunicję zarekwirowano, ale części pozwolono mu zatrzymać, ponieważ uznano, że nie można z nich zbudować sprawnej broni. Informacji o tym zdarzeniu nie przesłano norweskiej policji[16]. W końcu sierpnia 2010 r. Breivik wyjechał do Pragi, gdzie spędził sześć dni. Przeglądając internet, zorientował się, że w Czechach można dość łatwo nielegalnie zdobyć broń. Zamierzał kupić karabinek AK-47, pistolet Glock, granaty ręczne i RPG-7. Miał nadzieję, że te dwa ostatnie produkty otrzyma w charakterze bonusu. Zapewnił sobie alibi w postaci prospektu dotyczącego wydobycia i sprzedaży minerałów w Czechach, aby w razie potrzeby móc wyjaśnić cel pobytu. Ku swojemu zaskoczeniu nie kupił żadnej broni palnej w Pradze. Postanowił zrezygnować z jej zdobycia za granicą i spróbować nabyć legalnie w Norwegii. Uzyskanie pozwolenia na broń, mimo że siedem lat wcześniej kupił dwa pistolety, okazało się trudniejsze, niż przypuszczał. Należało bowiem wykazać się regularną obecnością w którymś z klubów strzeleckich. W związku z tym Breivik zapisał się do klubu strzeleckiego w Oslo, w którym odbył 15 godzin treningu w strzelaniu z karabinu. Ćwiczył też umiejętność celowania w grze komputerowej „Call of Duty: Modern Warfare", osadzonej w realiach współczesnych konfliktów. Jak napisał w manifeście, ta gra pomogła mu w poprawieniu koncentracji i szybkości reakcji. W klubie strzeleckim otrzymał pozwolenie na zakup broni krótkiej i długiej. Kupił pistolet Glock 17, karabinek półautomatyczny Sturm Ruger Mini-14 kalibru 5,56 mm, 300 sztuk nabojów karabinowych i 150 sztuk amunicji do pistoletu, celownik laserowy, dodatkowy spust ułatwiający szybkie strzelanie i bagnet karabinowy. Pistolet nazwał Mjølnir, od młota nordyckiego boga Thora, a karabin – Gugnir, od nazwy włóczni Odyna, która zawsze trafiała w cel. Na broni wyrył odpowiednie runy. Innym przedmiotom, które przerabiał według własnego uznania, również nadawał imiona i traktował je jak amulety[17].

[16] *Anders Breivik był zatrzymany przez niemiecką policję dwa lata przed zamachem na wyspie Utöya. Miał przy sobie amunicję i części uzbrojenia. Został wypuszczony na wolność*, Wirtualna Polska, 14 I 2016 r., https://wiadomosci.wp.pl/anders-breivik-byl-zatrzymany-przez-niemiecka-policje-dwa-lata-przed-zamachem-na-wyspie-utoya-mial-przy-sobie-amunicje-i-czesci-uzbrojenia-zostal-wypuszczony-na-wolnosc-6027685648360577a [dostęp: 15 I 2016].

[17] E. Czykwin, *Anders Breivik…*, s. 98; M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020, s. 18.

Zdobywanie środków chemicznych było newralgiczną fazą działań Breivika, gdyż w ten sposób najłatwiej można było wzbudzić podejrzenia i zostać zdekonspirowanym. Substancje chemiczne do wyprodukowania materiału wybuchowego kupował za pośrednictwem internetu lub osobiście. W grudniu 2010 r. nabył we wrocławskiej firmie sprzedaży internetowej Keten 0,3 kg azotynu sodu (środek używany w Norwegii do konserwacji mięsa). Zapłacił kartą 10 euro. W tym samym miesiącu zamówił w tym samym polskim sklepie 150 kg proszku aluminiowego, za co zapłacił przelewem 2 tys. euro. Sproszkowane aluminium zwiększa siłę wybuchu ładunku. Breivik napisał w manifeście, że tę substancję w ilości do 100 kg można bez wzbudzania podejrzeń nabyć w Polsce. Kupowanie chemikaliów w naszym kraju nie było wówczas problemem[18]. W zamówieniu podał, że proszek jest mu potrzebny jako składnik farby do zabezpieczania łodzi. W rzeczywistości dwie kupione w Polsce substancje były mu niezbędne do skonstruowania detonatora. Po dokonaniu tych zakupów Breivik znalazł się na czarnej liście brytyjskich służb specjalnych[19]. Nie wykluczono wówczas jego osobistych kontaktów z Łukaszem Mikusiem, właścicielem Ketenu, który kilkakrotnie przebywał w Szwecji[20]. Breivik kontaktował się

[18] Po zamachach w Norwegii sytuacja w Polsce diametralnie się zmieniła. Na sklepy internetowe oferujące środki chemiczne podwójnego zastosowania nałożono obowiązek rejestrowania danych personalnych klientów, rodzaju i ilości zamawianych substancji oraz informowania Agencji Bezpieczeństwa Wewnętrznego lub Policji o złożeniu zamówienia.

[19] Keten był legalnie działającą firmą zajmującą się sprzedażą substancji chemicznych. Polska ustawa o materiałach wybuchowych oraz rozporządzenie ministra gospodarki nie wymagały wówczas posiadania pozwolenia na nabywanie i przechowywanie większości wyrobów pirotechnicznych. Koncesji wymagała sprzedaż gotowych materiałów wybuchowych. Wrocławska firma, w której Breivik zakupił składniki do produkcji bomby, także nie musiała mieć koncesji.

[20] Łukasz Mikuś był pasjonatem chemii. Po ukończeniu studiów otworzył sklep internetowy z chemikaliami. W 2001 r. został prawomocnie skazany za przestępstwa z użyciem materiałów wybuchowych. W jednym przypadku chodziło o zakup i posiadanie 2 kg trotylu oraz amunicji do broni strzeleckiej. W drugim – skonstruował i przesłał ładunek wybuchowy Ryszardowi H. Przesyłka eksplodowała w czasie sortowania na Poczcie Głównej we Wrocławiu. Policja zarządziła wówczas ewakuację i przeszukanie budynku, mieszkania Mikusia, odbiorcy paczki oraz kilkunastu innych osób, które utrzymywały kontakty z Mikusiem. Ryszard H. był wówczas członkiem śląskiego gangu „Danona". Grupa została rozbita w 2002 r. Według Centralnego Biura Śledczego bandyci podłożyli ładunek wybuchowy w pobliżu agencji towarzyskiej w Rydułtowach. W eksplozji rannych zostało pięć osób, w tym trzy ciężko. Właściciel lokalu stracił rękę, ciężko ranny został też jeden ze strażników miejskich wezwanych na miejsce ataku. Za udział w grupie przestępczej Ryszarda H. skazano na 5 lat więzienia. Zob. M. Rybak *Wrocławianin, który sprzedał chemikalia Breivikowi,*

z jeszcze jednym sklepem internetowym, mającym siedzibę w Pobiedziskach pod Poznaniem, w którym kupił lont. Sklep był popularny i polecany na forach, również wśród Norwegów, ponieważ jego właściciel, Tomasz P., nie zadawał klientom niewygodnych pytań. Pod pseudonimem „Czort" publikował on również na forach internetowych filmy instruktażowe i materiały reklamowe dotyczące oferty swojego sklepu. Wszystkie nawiązywały do konstruowania ładunków wybuchowych. Kilka miesięcy przed zamachem w Oslo transakcje zawierane przez Tomasza P. wzbudziły podejrzenia programu „Global Shield", skupiającego urzędy celne z krajów NATO, które nadzorują obrót towarami przydatnymi do produkcji ładunków wybuchowych. Norweski urząd celny przesłał do norweskiego kontrwywiadu listę 41 podejrzanych transakcji. Widniało na niej nazwisko Breivika, jednak jego osoba nie wzbudziła podejrzeń służb specjalnych. Według informacji „Global Shield" Breivik kupił jedynie lont, który nie znajdował się na liście towarów zastrzeżonych[21].

W swoim manifeście przyszły zamachowiec wspominał, że podczas zakupów, nie tylko w Polsce, udawał właściciela firmy prowadzącej badania związane z rolnictwem lub sugerował, że jest pirotechnikiem i chce urządzić niskobudżetowy pokaz fajerwerków na ślubie siostry. Polska zostaje w nim wymieniona kilkadziesiąt razy. Breivik zaznaczył, że w tym kraju można kupić AK-47 i legalnie wypróbować karabinek na strzelnicy. Jego idolem był król Jan III Sobieski, który powstrzymał Turków pod Wiedniem. Norweg wymienił również polskie ugrupowania nacjonalistyczne. Zaliczył do nich Samoobronę RP, Ligę Polskich Rodzin, Narodowe Odrodzenie Polski, Ligę Obrony Suwerenności oraz Prawo i Sprawiedliwość. W manifeście zacytował *Zniewolony umysł* Czesława Miłosza[22]. Zamówienia przez internet na większość substancji chemicznych składał w grudniu 2010 r., kiedy pracownicy poczty byli zbyt zajęci, by dostrzec w nich coś podejrzanego. Gromadził je w piwnicy domu, w którym mieszkała matka. Dzięki założonej w 2009 r. firmie Geofarm mógł bez wzbudzania podejrzeń kupić nawóz, który posłużył jako główny składnik materiału wybuchowego. Wiosną 2011 r. wynajął opuszczone gospodarstwo rolne Vålstua w gminie

miał kiedyś problemy z prawem, „Gazeta Wrocławska", 22 XI 2011 r.; B. Kittel, J. Jabrzyk, *Czy Polak pomógł Breivikowi*, TVN24, 22 XI 2011 r., https://tvn24.pl/polska/ czy-polak-pomogl-breivikowi-ra191578-3531692 [dostęp: 23 XI 2011].

[21] M. Kącki, *Breivik kupił lont w Polsce*, „Gazeta Wyborcza", 23 VIII 2011 r.

[22] J. Haszczyński i in., *Robił zakupy we Wrocławiu, podziwiał Jana III Sobieskiego*, „Rzeczpospolita", 26 VII 2011 r.

Åmot w hrabstwie Hedmark. Sporządził listę najważniejszych urządzeń, narzędzi i składników chemicznych wraz z orientacyjnym kosztem ich zakupu. Było to niezbędne z uwagi na ograniczony czas przygotowań i posiadany kapitał. Inspirował się przy tym zamachem przeprowadzonym w USA przez wspomnianego wcześniej Timothy'ego McVeigha. Na potrzeby rzekomej uprawy warzyw zakupił nawóz amonowy, czyli azotan amonu. Jak się później okazało, na farmie pozostała ilość wystarczająca do wyprodukowania jeszcze jednego ładunku wybuchowego. Być może Breivik przeliczył się z siłami, zabrakło mu czasu, pieniędzy lub wszystkiego jednocześnie[23]. Na portalu e-Bay zamówił sproszkowaną siarkę jako materiał dla artystów plastyków, a saletrę chilijską kupił w aptece w pobliskim miasteczku. Miał przygotowaną szczegółową legendę na każdy zakup. Mówił na przykład, że potrzebuje środka do czyszczenia akwarium albo konserwacji mięsa. Lont miał być rzekomo wykorzystany w trakcie zabawy sylwestrowej. Precyzyjnie policzył i doświadczalnie zbadał, ile czasu zajmie jego spalenie się, aby zdążyć z ucieczką. W celu uzyskania kwasu acetylosalicylowego potrzebował kilku kilogramów aspiryny. Nie chcąc wzbudzić podejrzeń, kupował jedynie po dwa opakowania w różnych aptekach w Oslo. Do stolicy podróżował kilkakrotnie w odstępach dwutygodniowych. W aptekach pojawiał się elegancko ubrany. Dla niepoznaki początkowo wybierał droższe odpowiedniki aspiryny, a dopiero później tańsze. Zakup kwasu siarkowego (30 l) również wymagał sprytu. Nabywał go w niewielkich ilościach u różnych sprzedawców związanych głównie z branżą samochodową. Zamiast trzech ton azotanu amonu wziął sześć – niepotrzebną połowę zamówił dla niepoznaki. Z Chin sprowadził 60 wodoszczelnych worków używanych do transportu i przechowywania chemikaliów oraz płynną nikotynę. W Ikei kupił trzy stalowe pojemniki, które planował przerobić na detonatory. Na farmę przewiózł również chemikalia zgromadzone wcześniej w Oslo[24].

W budynku gospodarczym systematycznie produkował materiał wybuchowy. Nie był to zwykły ładunek ANFO wytworzony na bazie wspomnianego azotanu amonu. ANFO powstaje przez nasączanie azotanu amonu jednym z paliw płynnych, jednak tak przygotowany materiał wybuchowy trudno detonuje. Zazwyczaj do wywołania eksplozji używa się detonatorów, a w celu zwiększenia jej siły dodaje się pyłu aluminiowego. Breivik zaczął samodzielnie konstruować ładunek wybuchowy o dużej mocy na podstawie

[23] E. Czykwin, *Anders Breivik...*, s. 90–91.

[24] Tamże, s. 93–94.

informacji czerpanych z internetu. Przede wszystkim przystąpił do pracochłonnego odwirowywania w blenderach granulek nawozu, aby uzyskać czysty azotan amonu wolny od antyhigroskopijnej otuliny, który następnie polewał olejem napędowym. Pracował systematycznie, nasączając nim równomiernie każdą 50-kilogramową ilość pozbawionego peletek nawozu. Następnie pakował substancję do dwuwarstwowych worków sprowadzonych z Chin. Każdy worek zaklejał i odstawiał na bok. Praca postępowała powoli, a on działał pod presją czasu. Kiedy zdał sobie sprawę, że nie zdoła w pełni zrealizować planu, odwirował z peletek tylko część nawozu, a pozostałą również zapakował do worków. Miało to wpływ na zmniejszenie siły rażenia ładunku wybuchowego. Praca była niebezpieczna. Po długim okresie oczyszczania azotanu amonu, co wiązało się z unoszeniem w powietrzu dużej ilości pyłów chemicznych, napisał: *Na pewno w ciągu dwunastu miesięcy umrę na raka. Tyle tego gówna musiało mi się dostać do płuc, chociaż używałem maski*[25]. Stodołę, w której się przygotowywał, wypełniały szkodliwe substancje lotne, żrące płyny i pył aluminiowy. Ponadto gotował na prymitywnej kuchence 30 litrów kwasu siarkowego, aby zwiększyć jego stężenie przez odparowanie wody. Unoszący się odór spowodował, że postanowił podgrzewać kwas nocą. Nie używał prawie żadnych specjalistycznych środków ochronnych. Pracował w masce z filtrem przeciwkwasowym, grubym fartuchu ochronnym i gumowych rękawicach. Zagrożenie wybuchem było bardzo duże. Breivik miał tego świadomość, ponieważ czytał ostrzeżenia na opakowaniach. Obawiał się, że ewentualna eksplozja nie zabije go od razu, tylko zostanie mocno poparzony lub straci ręce. W takim przypadku planował popełnienie samobójstwa przez strzelenie sobie w głowę z karabinu za pomocą stóp. Inny etap pracy polegał na przygotowaniu odpowiedniego detonatora. Za inicjujący materiał wybuchowy miał mu służyć diazodinitrofenol, znany również jako dinitrobenzenodiazotlenek. Anders posiadał wszystkie związki chemiczne niezbędne do jego wyprodukowania, z wyjątkiem kwasu pikrynowego, który musiał samodzielnie wyprodukować[26]. Pierwsza wytworzona przez niego próbka nie uległa zapaleniu. Do tego niepowodzenia dołączyła awaria komputera, a Anders potrzebował go na bieżąco podczas kolejnych faz produkcji materiału wybuchowego. Zbyt pracochłonne okazało się również uzyskanie

[25] Å. Seierstad, *Jeden z nas…*, s. 247.

[26] Zob. *Diazodinitrofenol*, Vortal Młodego Chemika, 4 XII 2011 r., https://www.vmc.org.pl/pirotechnika/materiay-wybuchowe/inicjujce/item/297-diazodinitrofenol [dostęp: 31 I 2022].

kwasu acetylosalicylowego z pokruszonych tabletek aspiryny. Początkowo próbował je rozdrabniać tłuczkiem, ale ta metoda była niewydajna. Tabletki przykrywał więc folią i rozbijał ciężką hantlą. W końcu udało mu się otrzymać pożądany związek chemiczny. Wpadł również na pomysł użycia małej betoniarki do wymieszania saletry chilijskiej z pyłem aluminiowym mimo obaw, że jakaś iskra spowoduje detonację. Okazało się to jednak bezpieczne i znacznie skracało czas produkcji. Jednym z ostatnich etapów pracy nad bombą było przetestowanie lontu. Doświadczenie zakończyło się sukcesem[27]. Część kupionej amunicji Anders zmodyfikował – napełnił naboje trucizną w postaci płynnej nikotyny sprowadzonej wcześniej z Chin. W kolejnej partii nabojów odciął czubki, które zastąpił ołowianymi. Miało to zwiększyć śmiertelność w wyniku postrzału. W sklepie sportowym kupił obcisłą bluzę, z której wykonał imitację policyjnego munduru. Miesiąc przed planowanym atakiem zaczął odczuwać braki finansowe. Już wcześniej zaciągnął pożyczki na kwotę 28 750 euro za pomocą dziewięciu kart kredytowych, które wymagały spłaty[28]. Jej brak groził wpisaniem na listę dłużników, a to z kolei uniemożliwiało wynajęcie samochodu. Dzięki finansowej ekwilibrystyce udało mu się odwlec krytyczny moment do połowy lipca. Jak to bywało już wcześniej, działał na granicy prawa lub je łamał. Fakt, że pieniądze skończyły mu się dopiero pod koniec prac przygotowawczych, oznaczał, że dysponował sporymi sumami, mimo że nie pracował.

Kondycję podczas przygotowań do zamachu Breivik utrzymywał dzięki treningowi siłowemu i zażywaniu sterydów anabolicznych. Odwagi nabierał z pomocą gier internetowych, zwłaszcza dodatku „Cataclysm" do gry „World of Warcraft". Morale i motywację pomagała mu podtrzymywać kontemplacja, którą stosował trzy razy w tygodniu podczas spacerów. W trudnych chwilach sięgał po jedzenie, które traktował jako nagrodę. Korzystał też z odżywki białkowej w celu zwiększenia masy mięśniowej oraz stosował preparat z ostropestu plamistego, aby chronić wątrobę przed wpływem sterydów. Poza tym gromadził różnego rodzaju tabletki, aby poczuć przypływ energii tuż przed właściwą akcją. W sytuacji zagrożenia sięgał po Red Bulla oraz inne środki[29]. Kilkakrotnie mogło dojść do zdekonspirowania Breivika. Jednym z takich zdarzeń był przyjazd pod koniec czerwca 2011 r.

[27] E. Czykwin, *Anders Breivik...*, s. 98–101.

[28] A. Berwick, *2083. A European Declaration of Independence...*, s. 1437.

[29] E. Czykwin, *Anders Breivik...*, s. 94–95.

córki właściciela farmy. Pojawiła się wieczorem i przenocowała. Anders był zdecydowany ją zabić, gdyby znalazła coś podejrzanego. Tak się jednak nie stało, więc puścił ją wolno. W przygotowaniach przeszkadzali mu również inni nieproszeni goście. Jeden z nich zaoferował usunięcie kamieni i nawiezienie pola. Breivik stanowczo odmówił. Podejrzewał, że sąsiad zorientował się, do czego służy mu nawóz, i zgłosił to na policję. Kiedy na jego podwórku pojawił się obcy samochód, był prawie pewien, że został zdemaskowany. Tymczasem byli to przypadkowi goście, czterech Polaków[30]. Okoliczni farmerzy dostrzegali nietypowe zachowanie Breivika (zawiesił na przykład kłódkę na drzwiach, co nie leżało w miejscowym zwyczaju), byli jednak zbyt zajęci letnimi pracami, aby poświęcać uwagę izolującemu się sąsiadowi.

Ostatnią fazę przygotowań do zamachu Breivik zaczął realizować 2 maja i trwała ona 81 dni. Każdy dzień pracy szczegółowo opisał w dzienniku stanowiącym część jego manifestu[31]. Dziennik zakończył konkluzją, że wiedza, którą zdobył w trakcie pracy nad przygotowaniem wszystkich części składowych bomby, pozwoliłaby innej osobie działającej według jego wskazówek skrócić ten czas z 81 do 29 dni. Podał również szacunkowe skrócenie tego czasu, gdyby do takiej pracy przystąpiła większa liczba osób. W przypadku dwóch osób wynosiłby on 20 dni, trzech – 16 dni, czterech – 13 dni, a pięciu – 12 dni. Wskazał też skalę ryzyka dekonspiracji w zależności od liczby osób zaangażowanych w przygotowanie ładunku wybuchowego – od 30 proc. w przypadku jednej osoby do 90–95 proc., gdy zostałoby wtajemniczonych pięć osób[32]. Potencjalni naśladowcy otrzymali szczegółową informację na temat poszczególnych faz budowy bomby[33]. Zamachowiec wyznaczył sobie 22 lipca 2011 r. jako osobisty D-Day. Termin ten był ważny z kilku powodów: był to lipcowy piątek po godzinach pracy, a więc moment, kiedy wielu funkcjonariuszy przebywało na urlopie lub rozpoczynało weekendowy odpoczynek. Gro Harlem Brundtland z Partii Pracy, trzykrotna premier Norwegii, miała wtedy zaplanowane wystąpienie dla uczestników młodzieżówki tego ugrupowania, podczas jej obozu na wyspie Utøya niedaleko Oslo. Breivik chciał zabić także urzędującego i obecnego

[30] Tamże, s. 103–104.

[31] A. Berwick, *2083. A European Declaration of Independence…*, s. 1454–1470.

[32] Tamże, s. 1470–1471.

[33] Tamże, s. 1438–1453.

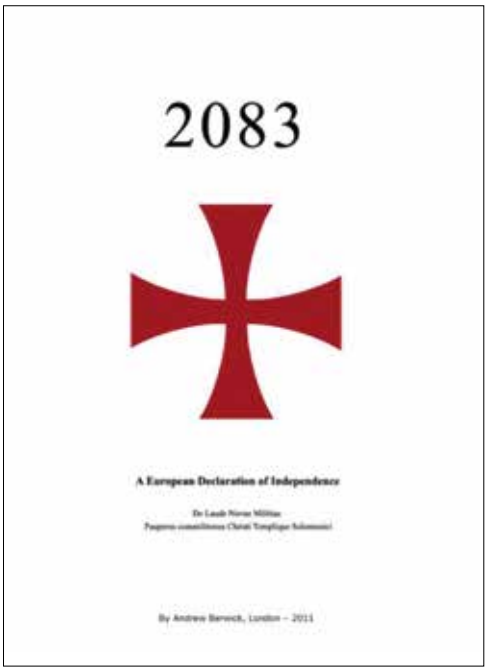
w pracy tego dnia premiera Norwegii Jensa Stoltenberga[34]. W dniach 19–20 lipca Anders załadował materiał wybuchowy o wadze 950 kg (źródła podają również, że było to 1050 kg) do wypożyczonej kilka dni wcześniej furgonetki marki Volkswagen Crafter, przerobionej na bombę VBIED (ang. *Vehicle-Borne Improvised Explosive Device*). Na przodzie samochodu znajdował się napis „Czyszczenie kanalizacji". Dysponował również pojazdem marki Fiat Doblo, także wypożyczonym[35]. W dniu 21 lipca oba pojazdy zaprowadził do Oslo i zatankował. Następnie zaparkował volkswagena przy centrum ogrodniczym. Przesiadł się do fiata, w którym znajdowały się broń i amunicja. Samochód zaparkował przy placu Hammersborg, naprzeciwko dzielnicy rządowej. Szybko przeszedł się po niej, żeby sprawdzić, czy nie pojawiły się jakieś nowe blokady. Kilkakrotnie podczas pobytu w Oslo monitorował już ten obszar. Taksówką pojechał do domu matki. Następnego dnia przed opuszczeniem domu włączył komputer, aby przesłać na 1 tys. adresów poczty elektronicznej plik zawierający wspomniany już manifest pod nazwą *2083. A European Declaration of Independence*, z krzyżem templariuszy i łacińskim podtytułem *De laude novae militiae. Peuperes commilitiones Christi Templique Solomonici* (Pochwały nowego wojownika. Ubodzy Rycerze Chrystusa i Świątyni Salomona), podpisany jego pseudonimem, z miejscem i datą wydania (zob. rysunek). Na końcu Breivik zamieścił siedem swoich fotografii[36]. Opracowanie liczy 1515 stron i jest drugim pod względem objętości tekstem o charakterze ideologicznym, po dziele Mustafy Setmariana Nasara alias Abu Musab al-Suri pt. *Dawa al-mukawama al-islamijja al-alamijja* (Wezwanie do islamskiego światowego oporu) opublikowanym w cyberprzestrzeni w 2004 r. i liczącym 1604 strony. Krótką, ale interesującą analizę manifestu Breivika przeprowadził Ryszard M. Machnikowski[37].

[34] E. Czykwin, *Anders Breivik...*, s. 92.

[35] S. Death, *Anders Breivik massacre: Norway's worst nightmare*, The Guardian, 25 III 2015 r., https://www.theguardian.com/world/2015/feb/22/anders-breivik-massacre-one-of-us-anne-seierstad [dostęp: 28 IV 2015].

[36] A. Berwick, *2083. A European Declaration of Independence...*, s. 1.

[37] R.M. Machnikowski, *Zabójcze idee. Co próbują nam przekazać terroryści?*, Łódź 2020, s. 157–170.



Rysunek. Strona tytułowa manifestu Andersa Breivika.

Źródło: https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf [dostęp: 1 II 2022].

Przebieg ataku

Dnia 22 lipca 2011 r. po godzinie 12.00 Breivik wrócił w pobliże centrum ogrodniczego, gdzie poprzedniego dnia zaparkował furgonetkę. Wsiadł do niej tylnymi drzwiami. Przebrał się w imitację munduru policyjnego. Na bluzę nałożył kamizelkę kuloodporną. Wysiadł z przedziału bagażowego, gdzie była umieszczona bomba, i usiadł za kierownicą. Podjechał w pobliże siedemnastopiętrowego budynku mieszczącego Ministerstwo Sprawiedliwości i Kancelarię Premiera. Wprawdzie na łańcuchu między dwoma słupami wisiała tablica informująca o zakazie wjazdu, ale swobodnie ją ominął. Kiedy skręcił w stronę wejścia do budynku, zobaczył, że najlepsze miejsce do zaparkowania zostało zajęte przez dwa samochody. Z tego powodu musiał postawić volkswagena inaczej, niż planował, ponieważ siła wybuchu skupiłaby się nie na budynku, tylko w przeciwnym kierunku. A zakładał zniszczenie całego biurowca, podobnie jak wspomniany Timothy McVeigh.

Zdenerwowany zapalił lont wystający z otworu w ściance oddzielającej kabinę od części bagażowej. Obawiał się, że może zginąć od przedwczesnej eksplozji z powodu oparów wydobywających się z worków, ale ta nie nastąpiła. Zabrał kluczyki, ale zapomniał o telefonie komórkowym, który zostawił na desce rozdzielczej, i wysiadł. Zamknął auto na klucz i rozejrzał się. W fazie planowania zamachu wziął pod uwagę możliwość pojawienia się agentów ochrony lub policjantów, których musiałby zlikwidować, ale nikogo nie było. Mimo wszystko wyjął pistolet i z bronią w ręku zaczął się oddalać od samochodu. Dwóch strażników monitorujących na ekranach budynek nie zauważyło furgonetki. O nieprawidłowo zaparkowanym samochodzie poinformowała ich jedna z recepcjonistek w biurowcu. W tym czasie Breivik znajdował się już poza zasięgiem kamer. Minął mężczyznę z bukietem róż, który zdziwił się na widok policjanta z bronią w ręku wsiadającego do fiata doblo. Zanotował markę i numer rejestracyjny pojazdu: VH 24605. O godz. 15.25 nastąpił wybuch. Premier Jens Stoltenberg, który następnego dnia miał mieć wystąpienie na Utøi, rozmawiał przez telefon, kiedy usłyszał huk. Jego rzecznik prasowy, który został poraniony szkłem, zadzwonił z bezpośredniego telefonu i upewnił się, że premier nie ucierpiał. Breivik o wybuchu dowiedział się z samochodowego radia, gdy przerwano nadawanie programu i poinformowano o silnej eksplozji w dzielnicy rządowej[38].

Pierwszy radiowóz przyjechał na miejsce zdarzenia trzy minuty po eksplozji. Jednocześnie w ten rejon skierowano dziesięć karetek pogotowia. Rannym pierwszej pomocy udzielili przechodnie. W Szpitalu Uniwersyteckim w Oslo ogłoszono stan alarmowy. Dziewięć minut po wybuchu na policyjny telefon alarmowy zadzwonił mężczyzna przedstawiający się jako Andreas Olsen. Poinformował, że kilka minut wcześniej mijał dziwnie zachowującego się mężczyznę w mundurze policyjnym, z bronią w ręku, idącego od strony dzielnicy rządowej. Podał dane samochodu, którym odjechał rzekomy policjant. To właśnie Olsen szedł z bukietem róż i zwrócił uwagę na Breivika. Telefon odebrała dyżurująca policjantka, która kartkę z zanotowaną marką i numerem rejestracyjnym samochodu zaniosła do sali i położyła na biurku szefowej. Oficer dyżurna rozmawiała w tym momencie przez telefon. W tym czasie Breivik stał w korku przy stołecznej operze. Komenda Okręgowa Policji w Oslo nie miała żadnych procedur powiadamiania, więc oficer dyżurna z centrali operacyjnej, zamiast koordynować akcję z dowodzącym na miejscu zdarzenia, uznała, że ważniejsze będzie

[38] Å. Seierstad, *Jeden z nas*..., s. 287–292.

telefoniczne wzywanie funkcjonariuszy na służbę. W krytycznej fazie nie było kontaktu między oficer dyżurną w centrali a dowódcą w terenie, który kierował pracami zabezpieczającymi i ratunkowymi w dzielnicy rządowej. Tymczasem Breivik wciąż stał w korku. Obawiał się, że z powodu ataku terrorystycznego zamknięto całe miasto i zablokowano ulice wyjazdowe ze stolicy. Jednak nie zrobiono tego, nie rozważano nawet takiej możliwości. Wszystkie dostępne patrole kierowano do dzielnicy rządowej, aby przyłączyły się do trwających tam działań ratunkowych. Wysłano też Beredskapstroppen – Delta, jednostkę specjalną norweskiej policji, której członkowie są przeszkoleni do wykonywania niebezpiecznych operacji[39]. Eksplozja spowodowała śmierć siedmiu osób, ósma zmarła w szpitalu, a 209 osób zostało rannych. Zniszczenia było widać nawet w promieniu kilometra od epicentrum wybuchu. W sposobie działania policji w Oslo niewiele wskazywało na to, że w Norwegii doszło do ataku terrorystycznego i istnieje duże zagrożenie kolejnym. Kiedy inne okręgi policyjne oferowały wsparcie, stolica je na ogół odrzucała, mimo że wielu najbardziej strategicznych obiektów w Oslo nadal nie zabezpieczono. Policja zamknęła wszystkie drogi, ale tylko te prowadzące do i z centrum stolicy, główny dworzec kolejowy, duże centra handlowe (City i Byporten), siedziby norweskiej agencji prasowej NTB, dzienników „Verdens Gang" i „Aftenposten" oraz telewizji TV2[40]. Atak w dzielnicy rządowej przypisano początkowo islamskim terrorystom i Al-Ka'idzie. Taką opinię wyrażali eksperci w telewizji.

Tymczasem pracownicy administracji parlamentu poprosili o dodatkową ochronę, ponieważ przed budynkiem nie było uzbrojonych strażników. Policja poinformowała ich, że muszą radzić sobie we własnym zakresie. Szefowi ochrony parlamentu polecono pozamykać budynki na klucz. O ochronę policyjną poprosiła administracja głównej siedziby Partii Pracy, o to samo zwrócił się również Dom Ludu[41]. Wszystkim odmówiono i doradzono ewakuację ludzi. W 2011 r. norweska policja dysponowała tylko jednym helikopterem, a w lipcu jego załoga przebywała na urlopie. Z powodu kolejnych cięć budżetowych w policji nie obowiązywał żaden

[39] Tamże, s. 293–295.

[40] E. Czykwin, *Anders Breivik*..., s. 16.

[41] Tradycja Domów Ludu (norw. Folkets Hus) jest znana w całej Skandynawii od XIX w. Powstawały one wraz z rozwojem ruchu robotniczego jako miejsca zebrań i spotkań. W Norwegii pierwszy Dom Ludu został zbudowany w latach 90. XIX w. Obecnie są w nich organizowane konferencje, różnego rodzaju uroczystości, domy te prowadzą również działalność rozrywkowo-rekreacyjną.

system wzywania załogi z urlopu. Jeden z pilotów sam zgłosił się na służbę tuż po godz. 16.00, po usłyszeniu o wybuchu w wiadomościach. Powiedziano mu, że nie jest potrzebny. Jednocześnie Delta dwukrotnie w ciągu następnej godziny prosiła o helikopter. Odpowiedź brzmiała, że nie jest on dostępny, chociaż stał na ziemi w pełni przygotowany do lotu. Policja nie podjęła też żadnych działań w celu zmobilizowania załóg helikopterów wojskowych lub wykorzystania maszyn cywilnych. Po wybuchu w Oslo nie ogłoszono niezwłocznie alarmu krajowego. Taki alarm uruchamiał specjalne procedury przesyłania ważnych meldunków do wszystkich komend policji w kraju. W razie alarmu krajowego w komendach okręgowych obowiązywały określone zasady działania. W komendzie dla miejscowości Asker i Baerum wiązało się to z ustawieniem blokady policyjnej na drodze E16 w okolicy Sollihøgda, którędy jechał Breivik. Ponadto komunikacja między poszczególnymi organami i jednostkami policji była niejasna i nieprecyzyjna. Brakowało konkretnych informacji i decyzji[42].

O godz. 15.55, czyli pół godziny po eksplozji, w komendzie policji ktoś przypadkiem zwrócił uwagę na kartkę z danymi samochodu podanymi przez Andreasa Olsena. Skontaktowano się z nim telefonicznie i poproszono o powtórzenie zgłoszenia. Następnie przekazano stosowne dane patrolom w stolicy. Nie zwrócono się jednak do mediów o podanie informacji na temat poszukiwanego pojazdu i uzbrojonego mężczyzny ubranego w mundur policjanta. Nie powiadomiono również Centrali Ruchu Drogowego w Oslo, która dysponowała rozległym systemem kamer. Istniał plan stworzony na wypadek zagrożenia terrorystycznego, ale nie został wdrożony. Nie wykorzystano też istniejących możliwości i zasobów. Breivik tymczasem wyjechał z Oslo. O godzinie 16.03 przejeżdżał obok komisariatu policji w miejscowości Sandvika, a o 16.16 minął wspomnianą Sollihøgdę, zmierzając w kierunku Utøi. O godz. 16.43 Centrala Policji Kryminalnej (norw. Kripos) nadała komunikat: *Alarm krajowy – wybuch. Niewykluczona bomba (bomby) w centrum Oslo. Wzywamy do wypatrywania niedużego szarego samochodu dostawczego, możliwy nr rej. 24605. Związek między wybuchem a pojazdem jest obecnie niejasny. W razie odnalezienia samochodu należy powiadomić dyżurnego w Kripos albo K.O.P. Oslo w celu otrzymania dalszych instrukcji. Zachować ostrożność wobec kierowcy i pojazdu. Z poważaniem, oficer dyżurny Kripos*[43]. Nie przekazano ani słowa o tym, że kierowca tego samochodu, którego liter

[42] Å. Seierstad, *Jeden z nas...*, s. 298–300.

[43] Tamże, s. 304.

z numeru rejestracyjnego Kripos nie zamieściło w komunikacie, był ubrany w mundur policjanta. Poza tym niewiele komend odebrało tę wiadomość. Albo nie włączono na czas urządzeń odbiorczych, albo częstotliwości alarmowe były źle ustawione. Dotyczyło to również komendy dla Nordre Buskerud, na której terenie przebywał już Breivik. Znajdowała się ona w odległości kilku kilometrów od przystani promowej na jeziorze Tyrifjorden. Breivik zaparkował samochód w pewnej odległości od tej przystani i czekał na prom, który przewiózłby go na wyspę. Zainteresowanym młodym ludziom, którzy również czekali na jednostkę pływającą, powiedział, że z powodu ataku w Oslo musi dostać się na wyspę, aby zapewnić bezpieczeństwo młodzieży przebywającej tam na obozie. Gdy prom MS Thorbjørn przypłynął z Utøi do przystani, pasażerowie wsiedli na pokład i łódź skierowała się z powrotem w stronę wyspy. Bagaż Breivika stanowiła skrzynia na kółkach i karabin owinięty w folię. Wśród pasażerów znajdowała się m.in. Monika Bøsei, kierowniczka ośrodka na Utøi. O 17.10 prom dobił do brzegu. Jego kapitan pomógł Breivikowi przenieść skrzynię na brzeg, uznając, że znajduje się w niej sprzęt do wykrywania materiałów wybuchowych. Do fałszywego policjanta podszedł Trond Bernsten, jeden z dwóch strażników (nieuzbrojonych) pilnujących porządku na wyspie. Breivik przedstawił się jako Martin Nilsen (tożsamość jego dawnego kolegi)[44].

W tym czasie na Utøi, wyspie o wymiarach ok. 500 na 300 metrów, przebywało ok. 600 młodych ludzi należących do młodzieżówki Partii Pracy. O godz. 17.22 Breivik oddał pierwsze strzały. Ofiarą był Bernsten. Po nim została zastrzelona Monika Bøsei. Do leżących Breivik oddał jeszcze po dwa strzały w głowę. Kapitan promu, który widział zajście, zaczął biec w głąb wyspy, krzycząc do napotkanych ludzi, aby uciekali. Drugi ze strażników, Rune Havdal, otrzymał strzał w plecy, kiedy biegł w kierunku zagajnika. Zabójca podszedł do leżącego i oddał strzał w głowę. Była to jego trzecia ofiara. Breivik nie spieszył się. Szedł spokojnie za największą grupą uciekającej młodzieży. Planował zastrzelić jak najwięcej osób, a inne postraszyć, aby wskoczyły do jeziora i utonęły. W ciągu pięciu minut zastrzelił 9 osób. Następnie wszedł do budynku ośrodka, w którym dokonał masowego mordu znajdujących się tam chłopców i dziewcząt[45]. Około godz. 17.29 przebywająca na wyspie córka oficera Komendy Głównej Policji zadzwoniła do będącego na służbie ojca i powiadomiła go o umundurowanym

[44] Tamże, s. 308.

[45] Tamże, s. 311–320.

mężczyźnie, który zabija uczestników obozu. Mieszkańcy terenów wokół jeziora, zaalarmowani odgłosami wystrzałów i widokiem dymu unoszącego się z wyspy, wezwali służby ratunkowe. Pierwsze jednostki – wóz strażacki i patrol policji – przybyły w okolice przystani promowej o godz. 17.38. Potem nadjechały karetki pogotowia. Okoliczni mieszkańcy ruszyli łodziami na pomoc i wyławiali nastolatków, którzy wpław uciekali z wyspy. Za radą sołtysa w najbliższej wsi utworzono centrum logistyczne w odległym o 3 km hotelu z polem golfowym, które miało służyć jako lądowisko. Decyzja została podyktowana także tym, że przy przystani stał samochód zamachowcy i istniało podejrzenie, że mogą znajdować się w nim materiały wybuchowe. Na nabrzeże przybył z sąsiedniego okręgu oficer operacyjny Policji Kryminalnej, który przejął dowodzenie. Równocześnie przybył śmigłowiec medyczny, z lekarzem anestezjologiem na pokładzie, który także był instruktorem ratownictwa medycznego i dzięki temu znał większość personelu służb ratowniczych w okolicy. Przejął kierowanie służbami medycznymi. Akcja była niezwykle trudna z powodu braku odpowiednich systemów łączności. Posługiwano się głównie telefonami komórkowymi, co wydłużało czas przekazywania informacji, ponieważ jedna rozmowa blokowała połączenie z innym rozmówcą oczekującym na połączenie – funkcjonariuszem policji, lekarzem czy pracownikiem pogotowia. Ponadto część obszaru znajdowała się poza zasięgiem telefonii komórkowej. Posiadane krótkofalówki również zawodziły. Akcję ratowniczą dodatkowo utrudniała pogoda. W utworzonym centrum dowodzenia co 15–20 minut odbywały się krótkie odprawy. W akcji uczestniczyło 50 jednostek różnych służb. W trakcie dokonywania mordu Breivik dwukrotnie zatelefonował na alarmowy numer policji i przedstawił się z imienia i nazwiska jako członek antykomunistycznego ruchu oporu. Podał też miejsce, w którym się znajdował, oraz zgłosił chęć oddania się w ręce funkcjonariuszy. Następnie przerywał rozmowę i kontynuował zabijanie. W Oslo zapadła decyzja o użyciu Delty. Brak śmigłowca spowodował, że jej funkcjonariusze musieli skorzystać z samochodu. Wyruszyli ok. godz. 17.30 i musieli przebijać się przez zakorkowane miasto. Gdy dotarli na brzeg jeziora Tyrifjorden, czekała na nich łódź motorowa. Niestety o godz. 18.11 utknęła ona na środku akwenu z powodu przeładowania. Wsparcia udzielili okoliczni mieszkańcy ze swoimi łodziami. O godz. 18.27 oddział Delty dobił do brzegu wyspy[46]. Posuwał się w stronę huku wystrzałów w szyku ubezpieczającym. W ciągu ostatnich

[46] M. Piekarski, K. Wojtasik, *Polski system*..., s. 20–21.

siedmiu minut Breivik zastrzelił jeszcze pięć osób: cztery dziewczyny i jednego chłopca. O godz. 18.34 zamachowiec, nie stawiając żadnego oporu, oddał się w ręce funkcjonariuszy Delty, których zaskoczył widok białego mężczyzny. Czekał on na ich przybycie, ale nie przerywał mordowania. W ciągu 72 minut zastrzelił 67 osób. Strzelał w tułów i głowę. Łącznie oddał 186 strzałów, a więc średnio ponad dwa strzały na minutę. Pozostał mu zatem jeszcze duży zapas amunicji. Doprowadził również do śmierci dwóch kolejnych osób, z których jedna spadła z wysokiego klifu, a druga utonęła, gdy starała się odpłynąć od wyspy. Ponadto 32 osoby zostały ciężko ranne, ale przeżyły. W ciągu godziny i 12 minut Breivik postrzelił łącznie 99 osób, zatem zabicie lub ranienie każdej z nich zajmowało mu przeciętnie mniej niż minutę. Ponad 70 osób odniosło obrażenia wynikające z prób ucieczki z wyspy i towarzyszącego temu stresu. Większość ofiar Breivika zabitych na Utøi miała od 14 do 18 lat. Zamachowiec liczył, że na wyspie zastanie byłą premier Gro Harlem Bruntland, ale ta kilka godzin wcześniej wróciła do Oslo. Zamierzał zdekapitować ją nożem, a zdarzenie sfilmować i zamieścić w internecie[47]. Wśród rannych znajdował się Adrian Pracoń, obywatel Norwegii polskiego pochodzenia, który w książce zrelacjonował swoje przeżycia[48].

Wnioski

Po przeanalizowaniu biografii Breivika można wysnuć wniosek, że państwo norweskie, od lat prowadzące opiekuńczą politykę wobec obywateli, w tym konkretnym przypadku całkowicie zawiodło. Matce Andersa i jemu samemu była potrzebna opieka psychologiczna. Środowisko, w którym Breivik się wychowywał, w dużym stopniu przyczyniło się do jego problemów. Po zamachu w Oslo służby państwowe również zawiodły na całej linii.

[47] R.M. Machnikowski, *Zabójcze idee…*, s. 158.

[48] A. Pracoń, *Masakra na wyspie Utøya*, Bielsko Biała 2013. W sądzie Breivik powiedział, że oszczędził Praconia, ponieważ miał on prawicowy wygląd. Nawet jeśli terrorysta rzeczywiście tak ocenił Praconia, to miała to być jego ostatnia ofiara. Breivik był już w tym momencie bardzo zmęczony. Pracoń jest zadeklarowanym homoseksualistą i jego wygląd mógł mieć znaczenie dla Andersa, ale w innym sensie niż opisał on to w sądzie. Jeden z jego przyjaciół zeznał, że Breivik jest ukrytym homoseksualistą. Do tej pory nie wiadomo, czy to prawda, ani co tak naprawdę go powstrzymało przed zastrzeleniem Praconia. Zob. I. Grelowska, *Anders Breivik. Nakręcony do zbrodni*, Interia, 20 IX 2019 r., https://styl.interia.pl/magazyn/news-anders-breivik-nakrecony-do-zbrodni,nId,3213764 [dostęp: 21 IX 2019].

Terrorysta po zdetonowaniu bomby w stolicy bez trudu przedostał się na wyspę. Nie zabezpieczono po tym zdarzeniu domu premiera. Mimo że tzw. mężczyzna z różami zawiadomił policję o podejrzanym zachowaniu Breivika, podał jego rysopis i numery rejestracyjne samochodu, to notatka utknęła na czyimś biurku. Nie zamknięto dróg, nie wysłano śmigłowca. Pilot, który usłyszał o wydarzeniach w telewizji, zgłosił się sam, ale został odesłany do domu. Podczas masakry nad Utøyą pojawił się śmigłowiec, jednak nie należał on do policji, a do jednej ze stacji telewizyjnych. Operator filmował Breivika strzelającego do przerażonych ludzi. Upłynął długi czas, zanim funkcjonariusze Delty znaleźli się na brzegu jeziora, a potem dotarli do wyspy i to tylko dzięki pomocy okolicznych mieszkańców. Kiedy przybyli na miejsce, Breivik się poddał i pozostało go tylko aresztować. Miał już nawet przygotowane zdjęcie na tę okoliczność. Gdyby nie błędy i zaniedbania, to można było, jeśli nie zapobiec tym tragicznym zdarzeniom przez otoczenie przyszłego zamachowca odpowiednią opieką na etapie jego dorastania, to znacznie ograniczyć liczbę ofiar, a nawet przeszkodzić Breivikowi w dotarciu do Utøi. Teraz należy mieć tylko nadzieję, że resztę życia spędzi on w więzieniu, choćby z tego względu, że nigdy nie okazał żadnego współczucia ani dla ofiar, ani dla ich rodzin. Ponadto zdaniem Elżbiety Czykwin w jego przypadku nie ma żadnych szans na resocjalizację. Granica, którą przekroczył, gdy zabił tyle osób, spowodowała tak duże zmiany w jego mózgu i osobowości, że powrót do normalności nie jest już możliwy[49].

Naśladowcy Breivika mieli podobne poglądy, zbliżone problemy i cechy osobowości, które w konsekwencji doprowadziły ich do skrajnej przemocy. Ich motywacją była również ideologia rasistowska i nienawiść do imigrantów lub osób o ciemnym kolorze skóry. Oprócz wymienionych już naśladowców, podobne przypadki, aczkolwiek nie tak dramatyczne, ale również z ofiarami śmiertelnymi, lub próby przeprowadzenia ataków terrorystycznych odnotowano m.in. w Niemczech, Francji, Wielkiej Brytanii, Szwecji, Estonii, Rosji, Czechach i Słowacji. Niektórych z tych sprawców inspirował Anders Breivik, inni natomiast zostali nazwani „Breivikami" przez media. Przykład Norwega pokazał, że nie tylko islamski terroryzm, który do niedawna pozostawał największym zagrożeniem, lecz także skrajnie prawicowe ideologie coraz częściej znajdują swoich zwolenników, gotowych w ich imię mordować innych. Do czasu zamachów w Norwegii z 22 lipca 2011 r. prawie cały wysiłek był skupiony na zwalczaniu zagrożenia ze strony

[49] I. Grelowska, *Anders Breivik*...

islamskich ekstremistów, których działania koncentrują się na mordowaniu Amerykanów oraz ich sojuszników, a w szerszym zakresie – wszystkich niewiernych i muzułmanów niepodzielających jedynie słusznych poglądów propagowanych przez radykalnych kaznodziejów oraz ich zwolenników. Tymczasem rośnie w siłę sprzeciw wobec społeczeństwa multikulturowego w Europie oraz wzrastającej liczby mniejszości muzułmańskich. Poprawność polityczna i autocenzura prorządowych mediów w Europie Zachodniej, które milczą na temat negatywnych skutków obecności imigrantów z krajów podwyższonego ryzyka, w tym na temat wzrostu zagrożenia terrorystycznego i przestępczości pospolitej, sprawiły, że cyberprzestrzeń stała się główną platformą wymiany opinii na ten temat. Towarzyszą im często rasistowskie treści i wezwania do przemocy, a skrajnie prawicowe organizacje rosną w siłę i za pomocą antyimigranckich haseł zdobywają poparcie społeczne i miejsca w parlamencie. W ich cieniu radykalizują się kolejne jednostki będące naśladowcami Andersa Breivika. Tymczasem ignoruje się fakt, że atak z 22 lipca 2011 r. był wyrazem sprzeciwu wobec społeczeństwa wielokulturowego, mimo że kraje skandynawskie, a zwłaszcza Norwegia, należą do państw niezwykle tolerancyjnych i otwartych na obce kultury, a norweski wskaźnik poziomu życia od lat jest zaliczany do najwyższych na świecie.

Skrajna prawica rośnie w siłę w całej Europie, jednak w krajach UE najgorzej pod tym względem jest w Niemczech. Przez wiele lat niemieckie służby nie widziały tego zagrożenia lub je bagatelizowały, gdyż koncentrowały się na islamskich terrorystach. Wzrosła liczba ataków, których sprawcami są osoby kierujące się skrajnie prawicową ideologią, luźno związane z jakimiś strukturami organizacyjnymi lub bez żadnych tego rodzaju powiązań. Są to osoby działające samotnie, które dzięki internetowi i mediom społecznościowym uzyskały dostęp do manifestów ideologicznych, instrukcji dotyczących przeprowadzania ataków terrorystycznych czy sposobów pozyskania broni. To powoduje nasilanie się zagrożenia terrorystycznego. Rośnie popularność ideologii skrajnie prawicowej, zwłaszcza w kontekście antyimigranckiej i antymuzułmańskiej narracji. Cieszyła się ona szczególnie dużym poparciem po roku 2015, w którym odnotowano największy po II wojnie światowej napływ nielegalnych migrantów do Europy. Właśnie wtedy jeszcze bardziej uaktywnili się naśladowcy Breivika. Norweg stał się wzorem dla nowego typu terroryzmu, ponieważ zwolenników teorii białej supremacji i rzekomej groźby zastąpienia rodzimej ludności przez imigrantów z krajów muzułmańskich nie łączą formalne

struktury organizacyjne. Samotne wilki szukają inspiracji w sieci oraz – idąc za przykładem Breivika – przed przystąpieniem do operacji terrorystycznej zostawiają swoje przesłanie. W raporcie za 2019 r. australijski Institute for Economics and Peace wskazał na przykład, że wzrost w Niemczech terroryzmu motywowanego skrajnie prawicową ideologią to tylko część znacznie szerszego zjawiska obejmującego cały Zachód. W ciągu pięciu lat liczba zamachów przeprowadzonych przez osoby związane z tym środowiskiem wzrosła tu aż o 320 proc.[50] Z kolei w 2021 r. odnotowano w Niemczech więcej przestępstw o podłożu politycznym niż w latach wcześniejszych. Ponad 19 tys. z nich popełnili podejrzani z prawicowego spektrum politycznego, ponad 17 tys. przestępstw policja nie sklasyfikowała ideologicznie (były one związane ze społecznym sprzeciwem wobec decyzji władz dotyczących walki z pandemią), a ok. 9 tys. przypisała sprawcom motywowanym skrajnie lewicowymi poglądami politycznymi[51].

Breivik i jego naśladowcy dowodzą, że podobne ataki terrorystyczne mogą zostać przeprowadzone w każdym miejscu na świecie. W Polsce również są obecne klasyczne prawicowe wzorce myślowe. Rasizm, nienawiść do Izraela, pogarda dla islamu, złość skierowana do zwolenników migracji i wolontariuszy niosących pomoc migrantom są czynnikami motywującymi do działania. Te w połączeniu z paranoją typową dla niektórych prawicowych ekstremistów mogą dać impuls do działań, które będą miały tragiczne konsekwencje. Po ataku w Norwegii polska policja i służby specjalne stanęły wobec nowych wyzwań w zakresie zapobiegania aktom terroryzmu. Zinstytucjonalizowano i zacieśniono współpracę między poszczególnymi służbami i jednostkami administracji państwowej i lokalnej, a w ramach ABW i Policji powstały wyspecjalizowane komórki, których zadaniem jest monitorowanie cyberprzestrzeni pod kątem zamieszczanych w niej rasistowskich treści[52]. Przyjęte rekomendacje pozwoliły zapobiec atakowi terrorystycznemu przygotowywanemu przez Brunona Kwietnia.

[50] J. Bielecki, *Naśladowcy Breivika rosną w Europie w siłę*, rp.pl, 23 II 2020 r., https://www.rp.pl/swiat/art. 871721-nasladowcy-breivika-rosna-w-europie-w-sile [dostęp: 24 II 2020].

[51] PAP, *Fala przestępstw politycznych w Niemczech. „Więcej niż kiedykolwiek w ciągu ostatnich 20 lat"*, InfoSecurity 24, 19 I 2022 r., https://infosecurity24.pl/za-granica/fala-przestepstw-politycznych-w-niemczech-wiecej-niz-kiedykolwiek-w-ciagu-ostatnich-20-lat [dostęp: 20 I 2022].

[52] Ta problematyka została szczegółowo przedstawiona w: *Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red. nauk.), Warszawa 2011.

Nie znaczy to jednak, że w pełni panuje się nad sytuacją w Polsce, ponieważ z roku na rok spada zaufanie społeczeństwa do państwa. Wyniki przeprowadzonych w 2020 r. badań dotyczących nastrojów Polaków okazały się na tyle złe, że zaskoczyły nawet samych autorów. Wprowadzane wówczas przez rząd różne tarcze, które miały chronić firmy w czasie pandemii koronawirusa, nie uspokoiły obywateli obawiających się braku pracy i pieniędzy. Nie wierzono w skuteczność proponowanych rozwiązań, a zaufanie do państwa okazało się wyjątkowo małe. Od tego czasu sytuacja ekonomiczna kraju uległa pogorszeniu. Spory w rządzie i podziały społeczne sprawiły, że po poprawie odnotowanej jesienią 2021 r. nastroje społeczne jeszcze bardziej się obniżyły[53]. Tę trudną sytuację częściowo zamaskował konflikt w Ukrainie. Polacy uświadomili sobie, że uciekinierzy zza wschodniej granicy stracili wszystko, ale uratowali życie. Zaangażowanie się dużej części społeczeństwa w pomoc dla Ukraińców oraz obrazy wojennych zniszczeń i ofiar pokazywane przez media na chwilę odciągnęły uwagę polskich obywateli od niepokojących informacji dotyczących sytuacji gospodarczej, inflacji, drożyzny czy pandemii koronawirusa. Wojna spowodowała również, że dalsza perspektywa życiowa przestała mieć dla ludzi większe znaczenie. Martwi ich najbliższa przyszłość. Obawiają się, że działania zbrojne zostaną przeniesione do naszego kraju, a konflikt nuklearny, jakkolwiek obecnie mało prawdopodobny, nie jest niemożliwy. Władimir Putin nie ma już nic do stracenia. Prognozowanie skali zagrożenia terrorystycznego, nie wspominając już o uwzględnianiu w tych prognozach samotnych wilków, jest bardzo utrudnione, ponieważ nie można przewidzieć rozwoju sytuacji na Ukrainie, a ona ma ogromny wpływ na bezpieczeństwo w naszym kraju. Z pewnością można jedynie stwierdzić, że zagrożenie to jest obecnie duże i nadal będzie wzrastać.

Rosyjska inwazja na Ukrainę zwiększyła także poziom zagrożenia terrorystycznego w sieci. Rosyjskie ataki na polską cyberprzestrzeń trwają od dłuższego czasu. Lęki i obawy obecne w społeczeństwie, podsycane przez aktywność trolli i rozpowszechniane fake newsy, wywołują nasilenie napięć społecznych. Niebagatelną rolę odgrywają w tym agenci wpływu. Na kilka

[53] *Tsunami uderzy w gospodarkę i finanse Polaków. Wyniki badań zszokowały nawet ich autorów*, Forbes, 12 V 2020 r., https://www.forbes.pl/gospodarka/nastroje-spoleczne-w-polsce-w-kwietniu-2020-badanie-irg-sgh-i-zpf-dr-slawomir-dudek/4mdqnw7 [dostęp: 14 III 2022]; PAP, *Jakie są nastroje społeczne w Polsce? Zaskakujące wyniki najnowszego sondażu*, DEON, 21 X 2021 r., https://deon.pl/swiat/jakie-sa-nastroje-spoleczne-w-polsce-zaskakujace-wyniki-najnowszego-sondazu, 1654190 [dostęp: 14 III 2022].

dni przed rosyjską agresją w polskiej cyberprzestrzeni nagle wzrosła liczba antyukraińskich i prorosyjskich komentarzy. Wiele z nich było fake newsami, ale dużą część stanowiły opinie autorów ze środowisk skrajnie prawicowych, którzy wcześniej mówili o zagrożeniu ze strony ukraińskich nacjonalistów, motywowanych w dużym stopniu dziedzictwem i ideologią Stepana Bandery oraz Organizacji Ukraińskich Nacjonalistów. We wpisach powielano m.in. wątki z przemówienia Putina, w którym argumentował uznanie przez Rosję niepodległości dwóch separatystycznych republik na wschodzie Ukrainy. Ta antyukraińska narracja była odtwarzana na skrajnie prawicowych forach[54]. Historycznie uzasadniana antyukraińskość nacjonalistycznych organizacji w Polsce (podobne resentymenty wobec Polski żywią skrajnie prawicowe organizacje ukraińskie) nie jest niczym szczególnym, tym bardziej że podczas przedłużającej się wojny wroga retoryka niemal zamilkła na portalach internetowych, na których zaczęła dominować neutralna publicystyka, nieodnosząca się do żadnej ze stron konfliktu na Ukrainie. W mediach społecznościowych wciąż jednak pojawiają się nienawistne komentarze. Sytuacja może zatrzymać się w przypadku przedłużającego się konfliktu na Ukrainie oraz wzrastającej liczby uciekinierów wojennych z tego kraju. Podziw dla determinacji obrońców, patriotycznie zmotywowanych i zjednoczonych, społeczne uznanie dla bohaterstwa Ukraińców, entuzjazm i pomoc niesiona uchodźcom będą stopniowo słabnąć i mogą zamieniać się w obojętność, a potem w niezadowolenie z obecności setek tysięcy przybyszów zza wschodniej granicy. Można przypuszczać, że za pogorszenie sytuacji ekonomicznej w Polsce i drożyznę będzie się obarczać winą uchodźców i UE. Można też założyć, że przebywający w Polsce Ukraińcy będą zbyt natarczywie wyrażać swój patriotyzm i szerzyć nacjonalistyczne idee, na przykład przez umieszczanie ukraińskich symboli i haseł na elewacjach budynków. To może nie spodobać się polskiemu społeczeństwu i rozpali aktywność krajowych ugrupowań nacjonalistycznych, stając się zarzewiem nienawiści, agresji, przemocy i wzajemnych oskarżeń. W początkowym okresie pojawienia się fali migracyjnej z Ukrainy tacy aktywiści „patrolowali" tereny w pobliżu przejść granicznych na Podkarpaciu i zachowywali się agresywnie wobec Azjatów i Afrykanów przekraczających granicę wraz z Ukraińcami. Wynika z tego, że wojna za wschodnią granicą nie

[54] Zob. *„Mądry Putin" i „sztuczne państwo Ukraina" – antyukraińskie narracje w polskiej sieci*, Konkret 24, 23 II 2022 r., https://konkret24.tvn24.pl/polska,108/madry-putin-i-sztuczne-panstwo-ukraina-antyukrainskie-narracje-w-polskiej-sieci,1097200.html [dostęp: 23 II 2022].

wpłynęła w istotny sposób na zachowania rasistowskie, może zmniejszyła ich skalę, ale nie wyeliminowała ich z przestrzeni publicznej.

W zależności od tego, jak zakończy się wojna w Ukrainie, będzie ona miała dalekosiężne skutki dla bezpieczeństwa w Europie i zagrożenia terrorystycznego. Dnia 27 lutego 2022 r. w Ukrainie zatrzymano trzech rosyjskich dywersantów. Przy jednym z nich znaleziono notatnik z adresem hotelu w Zgorzelcu (jego właścicielem okazała się osoba z przestępczą przeszłością), nazwami dwóch pobliskich miejscowości: Liberec w Czechach i Markersdorf w Niemczech oraz numerami telefonów i imionami dwóch osób: Igor i Artem. Przy drugim znajdował się dopisek „koordynator"[55]. Zagrożenie jest więc duże. Zwróciły na to uwagę również niemieckie służby, które szacują, że w ich kraju może działać od 200 do 2 tys. rosyjskich agentów. Ich cel stanowi nie tylko zbieranie informacji na temat polityków i firm krytykujących Rosję, lecz także mogą oni przygotowywać ataki na bazy sił NATO w Niemczech oraz akty sabotażu i dywersji. Rekrutują oni młodych mężczyzn, zwłaszcza w Niemczech Wschodnich, gdzie w ostatnich latach już kilkakrotnie doszło do tajemniczych eksplozji w zakładach zbrojeniowych i magazynach broni[56]. Działania destabilizujące i wywrotowe Rosja będzie prowadziła także w Polsce. Powstaje więc przestrzeń dla terrorystów kierujących się różną ideologią i sympatiami. Mogą one mieć podłoże antypolskie, antyrosyjskie, antyukraińskie, antynatowskie czy antyunijne. W każdym razie nowa grupa terrorystów może mieć ułatwione zadanie, jeśli chodzi o wybór celu i motywację. Niekoniecznie muszą oni kierować się rasistowską, antyimigrancką ideologią jak Anders Breivik, ale i jego następcy również mogą chcieć zaistnieć.

---

[55] M. Rybak, *Rosyjscy dywersanci, złapani na Ukrainie mieli w notesie adres hotelu w Zgorzelcu*, Wyborcza, 28 II 2022 r., https://wroclaw.wyborcza.pl/wroclaw/7,35771,28164136,-dywersanci-zlapani-przez-ukrainskie-sluzby-mieli-kartke-z.html [dostęp: 3 III 2022]; tenże, *„Wyborcza" ustaliła hotel w Zgorzelcu z notesu dywersantów złapanych na Ukrainie. Ma gangsterską przeszłość*, Wyborcza, 1 III 2022 r., https://wroclaw.wyborcza.pl/wroclaw/7,35771,28167910, wyborcza-ustalila-hotel-w-zgorzelcu-z-notesu-dywersantow.html [dostęp: 3 III 2022].

[56] V. Baran, *Niemcy. Służby: grożą nam akty dywersji*, Wirtualna Polska, 7 III 2022 r., https://wiadomosci.wp.pl/niemcy-sluzby-groza-nam-akty-dywersji-6744701005154912a [dostęp: 7 III 2022]; T. Waleński, *Stingery i Javeliny sieją strach u Rosjan. Ale broni dla Ukrainy może zabraknąć*, Wirtualna Polska, 11 III 2022 r., https://wiadomosci.wp.pl/moga-sie-pojawic-problemy-z-dostawami-sprzetu-wojskowego-do-ukrainy-6746062264457824a [dostęp: 11 III 2022].

Bibliografia

Czykwin E., *Anders Breivik. Między dumą a wstydem*, Warszawa 2019.

Haszczyński J. i in., *Robił zakupy we Wrocławiu, podziwiał Jana III Sobieskiego*, „Rzeczpospolita", 26 VII 2011 r.

Kącki M., *Breivik kupił lont w Polsce*, „Gazeta Wyborcza", 23 VIII 2011 r.

Machnikowski R.M., *Zabójcze idee. Co próbują nam przekazać terroryści?*, Łódź 2020.

Piekarski M., Wojtasik K., *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020.

Pracoń A., *Masakra na wyspie Utøya*, Bielsko Biała 2013.

Rybak M., *Wrocławianin, który sprzedał chemikalia Breivikowi, miał kiedyś problemy z prawem*, „Gazeta Wrocławska", 22 XI 2011 r.

Seierstad Å., *Jeden z nas. Opowieść o Norwegii*, Warszawa 2013.

Turrettini U., *The Mystery of the Lone Wolf Killer: Anders Behring Breivik and the Threat of Terror in Plain Sight*, New York 2015.

Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red. nauk.), Warszawa 2011.

Źródła internetowe

Anders Breivik był zatrzymany przez niemiecką policję dwa lata przed zamachem na wyspie Utöya. Miał przy sobie amunicję i części uzbrojenia. Został wypuszczony na wolność, Wirtualna Polska, 14 I 2016 r., https://wiadomosci.wp.pl/anders-breivik-byl-zatrzymany-przez-niemiecka-policje-dwa-lata-przed-zamachem-na-wyspie-utoya-mial-przy-sobie-amunicje-i-czesci-uzbrojenia-zostal-wypuszczony-na-wolnosc-6027685648360577a [dostęp: 15 I 2016].

Baran V., *Niemcy. Służby: grożą nam akty dywersji*, Wirtualna Polska, 7 III 2022 r., https://wiadomosci.wp.pl/niemcy-sluzby-groza-nam-akty-dywersji-674470100515-4912a [dostęp: 7 III 2022].

Berwick A., *2083. A European Declaration of Independence. De laude novae militiae. Peuperes commilitiones Christi Templique Solomonici*, London 2011, https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf [dostęp: 1 II 2022].

Bielecki J., *Naśladowcy Breivika rosną w Europie w siłę*, rp.pl, 23 II 2020 r., https://www.rp.pl/swiat/art.871721-nasladowcy-breivika-rosna-w-europie-w-sile [dostęp: 24 II 2020].

Death S., *Anders Breivik massacre: Norway's worst nightmare*, The Guardian, 25 II 2015 r., https://www.theguardian.com/world/2015/feb/22/anders-breivik-massacre-one-of-us-anne-seierstad [dostęp: 28 IV 2015].

Grelowska I., *Anders Breivik. Nakręcony do zbrodni*, Interia, 20 IX 2019 r., https://styl.interia.pl/magazyn/news-anders-breivik-nakrecony-do-zbrodni,nId,3213764 [dostęp: 21 IX 2019].

Grochot A., *Anders Breivik zostanie w więzieniu. Sąd odrzucił jego wniosek*, RMF24, 1 II 2022 r., https://www.rmf24.pl/fakty/swiat/news-anders-breivik-zostanie-w-wiezieniu-sad-odrzucil-jego-wniosek,nId,5806130#crp_state=1 [dostęp: 1 II 2022].

https://www.vmc.org.pl/pirotechnika/materiay-wybuchowe/inicjujce/item/297-diazodinitrofenol [dostęp: 31 I 2022].

Kittel B., Jabrzyk J., *Czy Polak pomógł Breivikowi*, TVN24, 22 XI 2011 r., https://tvn24.pl/polska/czy-polak-pomogl-breivikowi-ra191578-3531692 [dostęp: 23 XI 2011].

„Mądry Putin" i „sztuczne państwo Ukraina" – antyukraińskie narracje w polskiej sieci, Konkret 24, 23 II 2022 r., https://konkret24.tvn24.pl/polska,108/madry-putin-i-sztuczne-panstwo-ukraina-antyukrainskie-narracje-w-polskiej-sieci,1097200.html [dostęp: 23 II 2022].

Norway gunman claims he had nine-year plan to finance attacks, The Guardian, 25 VII 2011 r., https://www.theguardian.com/world/2011/jul/25/norway-gunman-attack-funding-claim [dostęp: 27 I 2022].

PAP, *Fala przestępstw politycznych w Niemczech. „Więcej niż kiedykolwiek w ciągu ostatnich 20 lat"*, InfoSecurity 24, 19 I 2022 r., https://infosecurity24.pl/za-granica/fala-przestepstw-politycznych-w-niemczech-wiecej-niz-kiedykolwiek-w-ciagu-ostatnich-20-lat [dostęp: 20 I 2022].

PAP, *Jakie są nastroje społeczne w Polsce? Zaskakujące wyniki najnowszego sondażu*, DEON, 21 X 2021 r., https://deon.pl/swiat/jakie-sa-nastroje-spoleczne-w-polsce-zaskakujace-wyniki-najnowszego-sondazu, 1654190 [dostęp: 14 III 2022].

Potocka J., *Hitlerowskie pozdrowienie i nowe hasła. Breivik chce wyjść na wolność*, RMF24, 18 I 2022 r., https://www.rmf24.pl/raporty/raport-zamachy-w-norwegii/fakty/news-hitlerowskie-pozdrowienie-i-nowe-hasla-breivik-chce-wyjsc-na,nId,5777148#crp_state=1 [dostęp: 18 I 2022].

Profile: Anders Behring Breivik, BBC, 12 IV 2012 r., https://www.bbc.com/news/world-europe-14259989 [dostęp: 14 V 2012].

Rybak M., *Rosyjscy dywersanci, złapani na Ukrainie mieli w notesie adres hotelu w Zgorzelcu*, Wyborcza, 28 II 2022 r., https://wroclaw.wyborcza.pl/wroclaw/7,35771,28164136,dywersanci-zlapani-przez-ukrainskie-sluzby-mieli-kartke-z.html [dostęp: 3 III 2022].

Rybak M., *„Wyborcza" ustaliła hotel w Zgorzelcu z notesu dywersantów złapanych na Ukrainie. Ma gangsterską przeszłość*, Wyborcza, 1 III 2022 r., https://wroclaw.wyborcza.pl/wroclaw/7,35771,28167910, wyborcza-ustalila-hotel-w-zgorzelcu-z-notesu-dywersantow.html [dostęp: 3 III 2022].

Sobańda A., *Skąd wziął się Breivik i czy można go było powstrzymać? Przejmująca opowieść o Norwegii*, Dziennik, 21 VIII 2015 r., https://kultura.dziennik.pl/ksiazki/artykuly/498350,jeden-z-nas-przejmujaca-opowiesc-o-norwegii-autorstwa-asne-seierstad.html [dostęp: 24 VIII 2015].

Tsunami uderzy w gospodarkę i finanse Polaków. Wyniki badań zszokowały nawet ich autorów, Forbes, 12 V 2020 r., https://www.forbes.pl/gospodarka/nastroje-spoleczne-w-polsce-w-kwietniu-2020-badanie-irg-sgh-i-zpf-dr-slawomir-dudek/4mdqnw7 [dostęp: 14 III 2022].

Waleński T., *Stingery i Javeliny sieją strach u Rosjan. Ale broni dla Ukrainy może zabraknąć*, Wirtualna Polska, 11 III 2022 r., https://wiadomosci.wp.pl/moga-sie-pojawic-problemy-z-dostawami-sprzetu-wojskowego-do-ukrainy-6746062264457824a [dostęp: 11 III 2022].

DOI: 10.4467/27204383TER.22.021.16341

ORCID: 0000-0003-4892-6112

KRZYSZTOF KAROLCZAK

Finansowanie terroryzmu – zarys problematyki

Abstrakt

W artykule omówiono podstawowe źródła finansowania terroryzmu XX-wiecznego i XXI-wiecznego: napady na banki, uprowadzenia dla okupu, przemyt i handel narkotykami. Jako specyficzne metody zostały wymienione również te, które stosowało Państwo Islamskie, m.in. handel ropą naftową wydobywaną na zajętych terenach, handel zabytkami i inne. Oddzielnie ujęto kwestie terroryzmu sponsorowanego przez państwa.

Słowa kluczowe:

finansowanie terroryzmu, napady na banki, uprowadzenia dla okupu, przemyt i handel narkotykami, Państwo Islamskie, terroryzm sponsorowany przez państwo

(...) *jedno pozostaje pewne – terroryzm jest biznesem wymagającym niskich nakładów finansowych*[1].

W artykule omówiono sposoby finansowania terroryzmu z uwzględnieniem perspektywy historycznej. Poznanie mechanizmów, jakie towarzyszą zjawisku finansowania terroryzmu, może potencjalnie pomóc w przeciwdziałaniu terroryzmowi oraz jego zwalczaniu. Terroryzm jest metodą

[1] Motto pochodzi z książki: W. Dietl, K. Hirschmann, R. Tophoven, *Terroryzm*, Warszawa 2009, s. 315.

działalności politycznej podlegającą zmianom w czasie, ale jednocześnie powtarzalną, co wynika z uwarunkowań społeczno-ekonomiczno-politycznych, w jakich funkcjonują ludzie stosujący terroryzm. Dlatego też warto przyjrzeć się, jak wyglądało finansowanie terroryzmu przez ostatnie 150 lat. Postęp technologiczny pozwala terrorystom korzystać z zaawansowanych rozwiązań technicznych, które mogą zagwarantować im sukces. W XIX w. korzystali oni z broni białej, palnej i bomb własnej produkcji, ale dopiero rozpowszechnienie środków transportu (samochodów, pociągów, samolotów) w XX w. ułatwiło terrorystom przemieszczanie się, transportowanie środków służących do przeprowadzenia zamachu, a nawet było narzędziem jego dokonania. Rewolucja technologiczna w informatyce w XXI w. umożliwiła terrorystom komunikowanie się nie tylko dzięki wykorzystaniu klasycznych metod (łącznicy, poczta, telefony stacjonarne), lecz także za pomocą sieci i systemów komputerowych (czyli w cyberprzestrzeni). W internecie mogą oni znaleźć również instrukcje, jak skonstruować ładunki wybuchowe, prowadzić nabór członków do swoich organizacji, a także przesyłać pieniądze. Wykorzystywanie przez terrorystów cyberprzestrzeni oraz poszukiwanie przez nich źródeł finansowania swojej działalności jest wyzwaniem dla służb specjalnych, które powinny zapobiegać zamachom, a nie tylko reagować na ich skutki.

W artykule ukazano, w jaki sposób były finansowane konkretne zamachy, a także jak organizacje terrorystyczne zdobywały środki na swoją działalność. Autor nie porusza kwestii przeciwdziałania finansowaniu terroryzmu – zarówno w skali krajowej, jak i międzynarodowej – oraz tzw. prania pieniędzy, ponieważ są to zagadnienia wymagające odrębnej analizy.

Historia terroryzmu oraz działalność ugrupowań uznawanych za terrorystyczne doczekały się setek opracowań. Ich autorzy rzadko jednak zajmowali się sprawami finansowymi, traktując je marginalnie. Prawdopodobnie zakładali, że terroryści dysponują środkami finansowymi na prowadzenie swojej działalności, bez wnikania w to, skąd te fundusze pochodzą. Dopiero szczegółowe, wielowątkowe analizy zjawiska terroryzmu pozwoliły na ustalenie źródeł finansowania działalności terrorystycznej. Tego rodzaju systematyczne badania zaczęto prowadzić dopiero od lat 90. XX w., również z tego powodu, że terroryzm (szczególnie po zamachach z 11 września 2001 r.) został uznany za jedno z największych zagrożeń współczesnego świata.

W ostatnich latach pojawiło się kilka propozycji systemowego spojrzenia na kwestie finansowania terroryzmu. Jedną z nich jest klasyfikacja

grup terrorystycznych pod kątem ich głównego źródła finansowania opracowana w 1987 r. przez Williama A. Tupmana z University of Exeter[2].

Tabela. Klasyfikacja grup terrorystycznych z uwzględnieniem źródeł finansowania[3].

Typy grup lub scenariuszy (działań)	Źródła finansowania
Terroryzm wewnętrzny	
Antykolonialne (nacjonalistyczne).	Sponsorowanie przez państwo, donacje.
Mniejszości etniczne, religijne i kulturowe.	Donacje, uprowadzenia, działalność kryminalna.
Mniejszości ideologiczne, lewicowe.	Rabowanie banków.
Mniejszości ideologiczne, prawicowe.	Indywidualni sponsorzy.
Grupy sponsorowane przez rząd.	Rządowi „pracodawcy".
Partyzantka miejska, tj. grupy wystarczająco duże, by miały szansę na obalenie rządu.	Donacje, podatek rewolucyjny.
Terroryzm międzynarodowy	
Emigracyjne.	Rabowanie banków i donacje.
Wspierające emigrację.	Finansowane przez „emigrantów".
Internacjonalistyczne.	Starające się korzystać z tzw. *war chest* (skrzyń wojennych) [w których zgodnie z tradycją są przechowywane zasoby, środki zdobyte w poprzednich działaniach].
Odgrywające rolę parawanu dla innych [grup] (*catspaws*).	Sponsorowane przez państwo.
Kontrrewolucyjne.	Sponsorowane przez państwo, również przez bogate osoby prywatne.
Islamskie grupy fundamentalistyczne (obecnie częściej nazywane dżihadowskimi).	Miłosierdzie [wiernych], osoby prywatne.
Niezorganizowani naśladowcy.	Finansowani przez wszystkich, rzeczywiście niezorganizowani, ale wielu wyszkoliło się w Afganistanie w oszustwach z użyciem kart kredytowych i upodabniają się w małej skali do przestępców w „białych kołnierzykach".

Źródło: *Funding of terrorist groups compared*, http://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/ [dostęp: 3 V 2022].

[2] Zob. *Funding of terrorist groups compared*, Money Jihad, 21 I 2013 r., http://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/ [dostęp: 3 V 2022].

[3] Tabela jest dokładnym tłumaczeniem tekstu oryginalnego. Tłumaczenia tekstu w tabeli oraz pozostałych tekstów w artykule pochodzą od autora (przyp. red.).

Od publikacji Tupmana upłynęło ponad 30 lat i przez ten czas pojawiło się wiele nowych źródeł finansowania terroryzmu. Choć można mieć zastrzeżenia nie tyle do samej klasyfikacji ugrupowań, ile do jednoznacznego wskazania źródeł pochodzenia funduszy posiadanych przez ugrupowania, warto jednak mieć ją w pamięci. Można bowiem ją potraktować jako wstęp do dalszych badań nad tym zjawiskiem, co z kolei pozwoli na skuteczne wstrzymanie zdobywania tych funduszy ze wskazanych źródeł.

W 2014 r. australijska agenda rządowa AUSTRAC[4] opracowała raport na temat źródeł finansowania terroryzmu w Australii. Ich precyzyjne wskazanie może być przydatne w badaniach dotyczących również innych obszarów geograficznych. Według autorów raportu[5]: *Kluczowe kanały wykorzystywane do pozyskiwania funduszy na finansowanie terroryzmu w Australii lub z Australii obejmują:*

- *organizacje charytatywne i organizacje non profit,*
- *samofinansowanie z legalnych źródeł,*
- *oszustwa, kradzieże i handel narkotykami,*
- *płatności okupu*.

Interesujące z punktu widzenia badania finansowania terroryzmu wydaje się to, co w raporcie napisano o samofinansowaniu działalności terrorystycznej z legalnych źródeł:

> Mniejsze grupy lub osoby działające samodzielnie mogą starać się finansować swoją działalność z legalnych źródeł, co pozwala im na stosunkowo ciche pozyskiwanie niewielkich lub umiarkowanych kwot. W takich przypadkach instytucjom finansowym może być trudno odróżnić transakcje mające na celu finansowanie działalności terrorystycznej od zwykłych, codziennych transakcji – w obu przypadkach środki pochodzą z legalnych źródeł, które raczej nie wzbudzą podejrzeń. W przypadku mniejszych grup ekstremistycznych i samotnych wilków samofinansowanie może zapewnić im wystarczające zasoby do przeprowadzenia nieskomplikowanego, ale silnego ataku. (...) Zaobserwowano, że małe, luźno zorganizowane australijskie grupy ekstremistów zbierają regularne składki od członków. W co najmniej

[4] Australian Transaction Reports and Analysis Centre – agencja rządu australijskiego odpowiedzialna za wykrywanie i powstrzymywanie przestępczych nadużyć wymierzonych w system finansowy państwa.

[5] *Terrorism financing in Australia 2014*, Serwis AUSTRAC, https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014 [dostęp: 3 V 2022].

> jednym przypadku australijskiego terroryzmu (...) do zebrania wkładów finansowych wykorzystano kasę znaną jako „sandooq"[6].

W tym fragmencie raportu pojawia się niespotykane w innych analizach pojęcie „sandooq" (urdu صندوق.) – (w niektórych analizach często pisze się o systemie hawala, jednak polega on na czymś innym). Słowo „sandooq" można przetłumaczyć jako „pudełko", które służy do przechowywania składek członków grupy planującej zamach terrorystyczny. W raporcie został opisany przypadek z Melbourne z 2005 r. Jedna osoba była skarbnikiem i posiadaczem sandooq, inna zatwierdzała członków grupy, którzy mogli korzystać ze środków zgromadzonych w kasie. Wszyscy członkowie wnosili wkład w fundusz, niektórzy wpłacali 100 dolarów australijskich miesięcznie. W momencie aresztowania grupy jej budżet wynosił ok. 19 tys. dolarów australijskich.

Wymienione w raporcie AUSTRAC sposoby finansowania działalności terrorystycznej nie są oczywiście jedynymi wykorzystywanymi przez terrorystów, o czym świadczy to, że w raporcie przytoczono przykłady odnoszące się jedynie do Australii (inne sposoby finansowania terroryzmu wraz z przykładami opisano w dalszej części artykułu).

Z tego samego roku co australijski raport pochodzi też opracowane przez redakcję „Forbesa" zestawienie 10 najbogatszych ugrupowań terrorystycznych[7]. Jego autor – Itai Zehorai, dziennikarz izraelskiego wydania „Forbesa", charakteryzując kolejne organizacje pod kątem regionu działania, celów działania, stosowanych metod i zasobów finansowych, wymienia również główne źródła ich finansowania.

1. ISIS:
   - roczny obrót: 2 mld dolarów,
   - główne źródła finansowania: handel ropą, porwania i okupy, ściąganie haraczy i podatków, napady na banki i grabieże.
2. Hamas:
   - roczny obrót: 1 mld dolarów,
   - główne źródła finansowania: podatki i opłaty, pomoc finansowa i darowizny (zwłaszcza z Kataru).

---

[6] Tamże.

[7] *The World's 10 Richest Terrorist Organizations*, Forbes, 12 XII 2014 r., http://www.forbes.com/sites/forbesinternational/2014/12/12/the-worlds-10-richest-terrorist-organizations/#336a6802ffae [dostęp: 22 V 2022].

3. FARC[8]:
   – roczny obrót: 700 mln dolarów,
   – główne źródła finansowania: produkcja i handel narkotykami, porwania i okup, wydobycie minerałów (zwłaszcza złota), opłaty i podatki.
4. Hezbollah:
   – roczny obrót: 500 mln dolarów,
   – główne źródła finansowania: pomoc finansowa i darowizny (zwłaszcza z Iranu), produkcja narkotyków i handel nimi.
5. Talibowie:
   – roczny obrót: 400 mln dolarów,
   – główne źródła finansowania: handel narkotykami (głównie produkcja opium i heroiny), opłaty i podatki od sponsorów, pomoc finansowa i darowizny.
6. Al-Ka'ida:
   – roczny obrót: 150 mln dolarów,
   – główne źródła finansowania: pomoc finansowa i darowizny, porwania, okup i handel narkotykami.
7. Lashkar-e-Taiba (Armia Sprawiedliwych):
   – roczny obrót: 100 mln dolarów,
   – główne źródła finansowania: pomoc finansowa i darowizny.
8. Al-Shabab:
   – roczny obrót: około 70 mln dolarów,
   – główne źródła finansowania: porwania i okup, nielegalny handel i działalność piracka, opłaty od sponsorów i podatki.
9. Real IRA:
   – roczny obrót: 50 mln dolarów,
   – główne źródła finansowania: przemyt i nielegalny handel, pomoc i darowizny.
10. Boko Haram:
    – roczny obrót: 25 mln dolarów,
    – główne źródła finansowania: porwania i okup, opłaty i podatki, ochrona, napady na banki i grabieże.

Po przeanalizowaniu tego zestawienia można zauważyć następującą prawidłowość – wszystkie wymienione sposoby zdobywania funduszy

[8] Fuerzas Armadas Revolucionarias de Colombia – kolumbijskie ugrupowanie partyzanckie. Obecnie działa legalnie jako partia Rewolucyjna Alternatywna Siła Ludowa.

należy kwalifikować w kategoriach przestępstw kryminalnych i niczym one się nie różnią od stosowanych przez organizacje przestępcze. Napady na banki (instytucje finansowe), uprowadzenia dla okupu, handel narkotykami są znane od dziesięcioleci jako metody działań zarówno indywidualnych kryminalistów, jak i zorganizowanych grup przestępczych. Różne są tylko cele, dla których dokonuje się tych przestępstw.

Finansowanie działalności z majątku osobistego zamachowca

Najłatwiej jest wskazać źródło finansowania zamachu dokonanego przez pojedynczego terrorystę, nazywanego – głównie przez media – samotnym wilkiem, niezwiązanego z żadnym środowiskiem oraz niebędącego członkiem żadnego ugrupowania, które mogłoby udzielić mu wsparcia (np. logistycznego) podczas przeprowadzenia akcji.

Łatwiej jest też wskazać sposób finansowania zamachów przeprowadzonych przez XIX-wiecznych terrorystów niż współczesnych. Wiąże się to z tym, że większości współczesnych zamachów dokonują członkowie ugrupowań, które nierzadko dysponują milionowymi funduszami, a te ugrupowania stały się swoistymi przedsiębiorstwami (instytucjami) finansowymi.

Przykładem zamachowca, który sam sfinansował swój zamach, jest Antoni Berezowski. Znane są – w przybliżeniu – koszt zamachu i źródło pieniędzy. Ten były powstaniec styczniowy (brał w nim udział jako szesnastolatek) od 1865 r. mieszkał w Paryżu i kiedy dowiedział się, że w czerwcu 1867 r. ma przyjechać z wizytą do Francji car Aleksander II, postanowił dokonać na niego zamachu. W tym czasie pracował jako ślusarz w warsztatach Kolei Północnej braci Gouin i dysponował niewielkimi zasobami finansowymi. W dniu 5 czerwca 1867 r. za 5 franków (według innych źródeł – za 9 franków) kupił dwulufowy pistolet. Ponieważ nie wystarczyło mu pieniędzy na kule, zastawił w lombardzie palto i za otrzymane 8 franków uzupełnił uzbrojenie. Koszt zamachu można zatem oszacować na kilkanaście franków[9]. Berezowskiego, który został złapany na miejscu zdarzenia, skazano na dożywotnią katorgę (zesłanie) na wyspie Nou w Nowej Kaledonii.

Znany jest też koszt zamachu na prezydenta Francji Marie-François Sadi Carnota, dokonanego w Lyonie 24 czerwca 1894 r. Sante Geronimo Caserio, Włoch z pochodzenia, po spędzeniu w 1892 r. pięciu miesięcy w więzieniu

[9] Do 1873 r. frank był oparty na parytecie srebra. Jeden frank zawierał 4,5 g czystego srebra.

pod zarzutem działalności w środowisku mediolańskich anarchistów udał się przez Szwajcarię do Francji, gdzie zamieszkał w małej miejscowości Cette (dzisiejsze Séte) w Langwedocji i rozpoczął pracę w wyuczonym zawodzie piekarza. Jednak po wydaniu wyroku śmierci na Auguste'a Vaillanta (sprawcy zamachu bombowego w Zgromadzeniu Narodowym z 9 grudnia 1893 r.) i nieułaskawieniu go przez prezydenta, Caserio postanowił dokonać zemsty. W dniu 23 czerwca 1894 r. odebrał wypłatę (20 franków), porzucił pracę, kupił za 5 franków w sklepie rzeźniczym nóż o piętnastocentymetrowym ostrzu i pojechał do Lyonu, w którym w tych dniach przebywał z wizytą Carnot. Następnego dnia w pobliżu budynków giełdy i Crédit Lyonnais, używając zakupionego noża, zaatakował prezydenta udającego się swoim powozem na galę urządzoną na jego cześć. Zadał tylko jeden cios (tu wersje są różne: w serce, w brzuch lub wątrobę), który okazał się śmiertelny. Caserio został pochwycony i po śledztwie oraz trwającym tylko dwa dni procesie skazano go na karę śmierci. Wyrok przez ścięcie na gilotynie wykonano 16 sierpnia 1894 r.

Oba przytoczone powyżej przykłady doskonale ilustrują to, że dla dokonania zamachu terrorystycznego nie są potrzebne znaczne zasoby finansowe. Współcześnie trudno jednak byłoby znaleźć egzemplifikacje takich „samowystarczalnych" zamachowców. Prawdopodobnie za takiego można uznać Theodore'a Kaczynskiego, Amerykanina o polskich korzeniach, któremu FBI nadało przydomek „Unabomber". Kaczynski, rezygnując ze świetnie zapowiadającej się kariery naukowej, porzucił cywilizację na rzecz życia na łonie natury (w lesie opodal miasta Lincoln w stanie Montana wybudował drewniany dom, uprawiał też ziemię) i podjął walkę z – jak sam ją nazywał – cywilizacją technologiczną. Przez 17 lat terroryzował ludzi ze świata nauki oraz korporacje, wysyłając do nich listy pułapki. W sumie nadał ich 16: pierwszy 25 maja 1978 r., ostatni 24 kwietnia 1995 r. W wyniku eksplozji bomb umieszczonych w listach zginęły trzy osoby, a rannych zostało 29. Po długotrwałym śledztwie, w wyniku denuncjacji przez własnego brata, został aresztowany i skazany w 1998 r. na karę dożywotniego więzienia.

Terrorystami korzystającymi z własnych środków finansowych byli również znani opinii publicznej, ze względu na skutki dokonanych przez nich zamachów, Timothy McVeigh (sprawca zamachu w Oklahoma City z 19 kwietnia 1995 r.) i Anders Breivik (22 lipca 2011 r. dokonał dwóch zamachów w Norwegii). Oprócz nich z dużą dozą prawdopodobieństwa należałoby dodać dziesiątki sprawców zamachów polegających

na wjechaniu samochodem w przechodniów czy zaatakowaniu nożem np. klientów galerii handlowych.

Finanse organizacji dokonującej zamachów terrorystycznych

Organizacja, której członkowie dokonują zamachów terrorystycznych, musi dysponować funduszami pozwalającymi nie tylko na wykonanie zleconego zadania, lecz także nierzadko na pomoc swoim członkom żyjącym w ukryciu. Z tego też powodu, kiedy organizacja nie może liczyć na wsparcie z zewnątrz, ucieka się do pospolitych przestępstw, które mają zapewnić jej dopływ gotówki.

Napady na banki i inne instytucje finansowe

Prostą, znaną na całym świecie metodą zdobycia pieniędzy były i są napady na banki lub inne miejsca, gdzie można zagarnąć potrzebne środki. Według *Encyklopedii terroryzmu*[10] w ciągu dwóch miesięcy 1972 r. Frakcja Czerwonej Armii (niem. Rote Armee Fraktion, RAF) dokonała sześciu napadów na banki, zdobywając 185 tys. dolarów. Nie są to jedyne tego typu akcje ukazujące skalę takich działań. Cytowana tam liderka RAF Ulrike Meinhof miała usprawiedliwiać napady na banki w następujący sposób: *Nikt nie uważa, że napad na bank sam w sobie cokolwiek zmienia. Jest to działanie uzasadnione, ponieważ w innym przypadku problem finansowy zupełnie nie mógłby być rozwiązany. Jest to taktycznie uzasadnione, ponieważ jest to akcja proletariacka. Jest to strategicznie uzasadnione, ponieważ służy finansowaniu partyzantów*[11]. Zupełnie inaczej brzmią w tym kontekście słowa byłego sierżanta armii brazylijskiej Pedra Loby de Oliveiry, który w 1968 r. wziął udział w napadzie na Banco Brasileiro de Descontinos w São Paulo:

> Kiedy idę podłożyć bombę, to jestem świadomy, że dla aparatu represji, jak i dla ludu będzie rzeczą oczywistą, jeśli zginę czy zostanę schwytany, że chodziło o akcję rewolucyjną. Jednakże napad na bank to coś zupełnie innego. Powoduje to kłopoty psychologiczne. Na bank napada się po to, żeby zrabować w nim pieniądze. Odczuwałem lęk, że lud nie zrozumie, po co nam były te pieniądze, nie pojmie sensu

[10] *Encyklopedia terroryzmu*, B. Zasieczna (red.), Warszawa 2004.

[11] Tamże, s. 243.

> naszej akcji. Jeśli bowiem zostaniemy aresztowani, to w prasie ukaże się informacja: taki a taki, schwytany podczas napadu na bank. Zadawałem sobie pytanie: w jaki sposób udowodnię ludowi, że pieniądze z napadu miały służyć rewolucji[12].

Tego typu skrupułów nie mieli członkowie Organizacji Bojowej Polskiej Partii Socjalistycznej, kiedy dokonywali, jak mówili, „ekspropriacji", rabując z wagonów pocztowych pieniądze przewożone z Kraju Przywiślańskiego do miast Carstwa Rosyjskiego. Robili to „dla rewolucji" i „w imię rewolucji". W akcji pod Rogowem, przeprowadzonej 8 listopada 1906 r., skradziono ponad 30 tys. rubli, 12 sierpnia 1907 r. pod Sławkowem – 14 tys. rubli, a 26 września 1908 r. pod Bezdanami – 200 812 rubli i 61 kopiejek.

Uprowadzenia dla okupu

Uprowadzenia dla okupu to od wielu dziesięcioleci jedna z podstawowych form działalności przestępczej. Jest to metoda prosta w realizacji, a jak pokazuje historia, bardzo często skuteczna. Świadomość tego w pewnym momencie dotarła do ugrupowań terrorystycznych, które postanowiły zdobywać w ten sposób fundusze na swoją działalność.

Tego typu akcję jako pierwsi przeprowadzili terroryści z Ameryki Łacińskiej[13]. W dniu 23 maja 1971 r. argentyńska organizacja o nazwie Ludowa Armia Rewolucyjna (hiszp. Ejército Revolucionario Popular, ERP) uprowadziła Stanleya Sylvestra, szefa zakładów Swift Meat Packing w Rosario (był on jednocześnie brytyjskim konsulem honorowym w tym mieście). Okazało się to jednak niestandardowym uprowadzeniem dla okupu, gdyż porywacze nie zażądali za jego uwolnienie pieniędzy, lecz rozdzielenia wśród biednej ludności jedzenia i ubrań o wartości 62,5 tys. dolarów. Firma przystała na to i Sylvester tydzień później został uwolniony.

W dniu 22 marca 1972 r. ERP uprowadziła Oberdana Sallustrę, dyrektora wykonawczego fabryki Fiata w Buenos Aires. I tym razem porywacze zażądali nie bezpośrednio pieniędzy, lecz m.in. rozdzielenia „pakietów prezentowych" o wartości 1 mln dolarów wśród biednych uczniów w szkołach na terytorium całego kraju. Tym razem pod presją władz nie doszło do

[12] K. Karolczak, *Lewicowy terroryzm w Ameryce Łacińskiej*, „Warsztat" 1984, nr 1, s. 46.

[13] Wszystkie informacje pochodzą z książki N. Antkol, M. Nudell, *No One Neutral. Political Hostage-Taking In the Modern World*, Ohio 1990, s. 48–51. Por. *Los actos terroritas del E.R.P. y Montoneros*, Buen Día Noticia, 31 VII 2018 r., https://buendianoticia.com/nota/10960/los-actos-terroristas-del-erp-y-montoneros [dostęp: styczeń–maj 2022].

realizacji żądania (oprócz „pakietów prezentowych" członkowie organizacji domagali się zwolnienia z więzień 50 członków ugrupowania i udzielenia im pozwolenia na przelot do Algierii, a także przywrócenia do pracy 250 pracowników Fiata w Córdobie. Po akcji policji mającej na celu uwolnienie Sallustry okazało się, że został on wcześniej zabity przez porywaczy.

Do kolejnych uprowadzeń doszło w 1973 r. Dnia 2 kwietnia ofiarą stał się Anthony R. DaCruz, menadżer Eastman Kodak Company w Buenos Aires, którego zwolniono 7 kwietnia po wypłaceniu okupu w wysokości 1,5 mln dolarów. W dniu 23 maja uprowadzono biznesmena Aarona Bellinsona (okup miał wynosić 1 mln dolarów), 6 czerwca porwano Charlesa Lockwooda (okup – 2 mln dolarów), a 18 czerwca – Johna R. Thompsona (okup – 3 mln dolarów). Warto zauważyć, że ofiarami porwań nie byli Argentyńczycy, lecz obywatele USA oraz Wielkiej Brytanii, którzy reprezentowali swoje firmy w Argentynie.

Al-Ka'ida również dokonywała uprowadzeń dla okupu. I chociaż po zamachach z 11 września 2001 r. Stany Zjednoczone starały się wymóc na swoich sojusznikach respektowanie stanowiska „z terrorystami się nie negocjuje", to po porwaniu 7 września 2004 r. dwóch Włoszek: Simony Pari i Simony Torretty, pracownic organizacji zajmującej się pomocą humanitarną (wraz z dwoma Irakijczykami), rząd włoski prawdopodobnie zapłacił 5 mln dolarów okupu. Cała czwórka została uwolniona 28 września 2004 r.

Uprowadzenia dla okupu stały się podstawowym źródłem dochodu dla Al-Ka'idy Islamskiego Maghrebu (arab. Tanzim al-Kaida bi Bilad al-Maghribang), ugrupowania znanego jako AQIM (ang. Al-Qaida in the Islamic Maghreb's), przekształconego w styczniu 2007 r. z Salafickiej Grupy Modlitwy i Walki (arab. Al-Dżama'a as-Salafijja li ad-Dawa wa al-Kital, fr. Groupe Salafite pour la Prédication et le Combat, GSPC). Organizacja działała początkowo na terytorium sześciu afrykańskich państw (Algierii, Mali, Mauretanii, Maroka, Nigru i Tunezji), a w latach następnych także w Libii oraz Czadzie, utrzymywała też kontakty z grupami dżihadu w innych krajach (np. Nigerii). Ze sporządzonego przez Stratfor zestawienia wysokości okupów[14], jakie AQIM otrzymała za osoby uprowadzone (głównie cudzoziemców) w latach 2008–2012, wynika, że budżet organizacji wzbogacił się z tego tytułu o prawie 83 mln dolarów.

[14] *Mali: Al Qaeda in the Islamic Maghreb's Ransom Revenue*, Stratfor, 15 X 2012 r., https://worldview.stratfor.com/article/mali-al-qaeda-islamic-maghrebs-ransom-revenue [dostęp: 3 II 2014].

Handel narkotykami i ich przemyt

Kolejnym źródłem finansowania działalności terrorystycznej AQIM i innych organizacji istniejących w krajach zachodniej i północnej Afryki, m.in. Obrońców Wiary (arab. Ansar ad-Din), Ruchu na rzecz Jedności i Dżihadu w Afryce Zachodniej (arab. Al-Dżama'at at-Tawhid wa al-Dżihad fi Ghabi Ifrakija) znanej jako MUJAO (fr. Mouvement pour l'Unicité et le Jihad en Afrique de l'Ouest) czy Boko Haram, jest handel narkotykami pochodzącymi z Ameryki Południowej i ich przerzut do Europy[15]. Według danych algierskich z 2012 r. wartość kokainy przemycanej przez Afrykę Północną do Europy wyniosła 1,6 mld euro, z czego zbrojne ugrupowania za swoje usługi (ochronę) miały otrzymać 310 mln euro.

Z produkcji i handlu narkotykami (głównie opium) podstawowe źródło dochodu uczynili talibowie[16] i to już po formalnym obaleniu ich władzy w Afganistanie. *Według amerykańskiego Specjalnego Inspektora Generalnego ds. Odbudowy Afganistanu (SIGAR) nielegalne uprawy maku i produkcja narkotyków odpowiada za niemal 60 proc. rocznych dochodów talibów. Jak informuje ONZ, talibowie każdego roku z sektora narkotykowego mogą czerpać zyski w wysokości 100–400 mln dolarów*[17].

Finanse ISIL/ISIS/IS

Ugrupowanie Islamskie Państwo w Iraku i Lewancie, istniejące pod tą nazwą od kwietnia 2013 r., znane jest również pod akronimem ISIS (ang. Islamic State of Iraq and Syria). Drugie „S" w akronimie oznacza „Al-Sham",

[15] Zob. szerzej: E. Basar, *Drug Trafficking in Africa*, Civil-Military Fusion Centre Presents, grudzień 2012 r., https://www.cimicweb.org/cmo/medbasin/Holder/Documents/r024%20CFC%20Monthly%20Thematic%20Report%20(07-DEC-12).pdf [dostęp: 3 II 2014]; C. Freeman, *Revealed: how Saharan caravans of cocaine help to fund al-Qaeda in terrorists' North African domain*, The Telegraph, 26 I 2013 r., http://www.telegraph.co.uk/news/worldnews/africaandindianocean/mali/9829099/Revealed-how-Saharan-caravans-of-cocaine-help-to-fund-al-Qaeda-in-terrorists-North-African-domain.html [dostęp: 2 IV 2014]; R.O. Idoumou, *Terrorists, traffickers forge union in African desert*, Magharebia, 24 II 2012 r., http://magharebia.com/en_GB/articles/awi/reportage/2012/02/24/reportage-01 [dostęp: 3 II 2014].

[16] B. Chellaney, *Taliban turning Afghanistan into narco-terrorist state*, The Japan Times, 24 XI 2021 r., https://www.japantimes.co.jp/opinion/2021/11/24/commentary/world-commentary/taliban-narco-terrorism/ [dostęp: 16 I 2022].

[17] *Afganistan jest największym na świecie producentem służącego do wytwarzania narkotyków maku*, Dziennik Gazeta Prawna, 25 VIII 2021 r., https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8231469,afganistan-producent-mak-narkotyki.html [dostęp: 12 VI 2022].

co może być tłumaczone jako „Syria", a nawet tylko Damaszek, ale w kontekście globalnego dżihadu odnoszono je do całego Lewantu, uznawanego wówczas za syryjską część Al-Ka'idy. Przyjmuje się, że ugrupowanie – którego początkiem była Grupa Jedności Boga i Dżihadu (arab. Dżama'at at-Tauhid wa-al-Dżihad) uchodząca za odłam Al-Ka'idy, działająca wcześniej w Iraku pod dowództwem Abu Musaba az-Zarkawiego, a po jego śmierci w 2006 r. przekształcona w Islamskie Państwo w Iraku – korzystało z funduszy Al-Ka'idy[18].

Ówczesny lider ISIS Abu Bakr al-Baghdadi (alias Abu Dua) miał zamiar zjednoczyć wszystkie syryjskie dżihadowskie grupy, co częściowo się powiodło, gdyż zebrał pod swoją komendą wiele małych oddziałów. W późniejszym czasie, określając ISIS, zaczęto używać w dyskursie publicznym sformułowania „Tak zwane Państwo Islamskie" lub „Daesh", czasami w spolszczonej wersji „Da'isz". Obie te nazwy traktowano jako określenia pejoratywne w celu zdyskredytowania przeciwnika. W 2013 r. według szacunków amerykańskiego wywiadu ISIS liczyło około 5 tys. bojowników, w większości zagranicznych, co powodowało częste starcia z innymi oddziałami rebelianckimi (m.in. Ahrar al-Sham, Ahfad al-Rasoul i Liwa Asifat al-Shamal) z powodu próby ich zdominowania przez ISIS. W czerwcu 2014 r. po ogłoszeniu przez al-Baghdadiego odnowienia kalifatu ugrupowanie zmieniło nazwę na Państwo Islamskie (arab. ad-Dawlah al-Islāmiyah, ang. Islamic State, IS). W tym czasie zajmowało coraz większe terytorium w Syrii i Iraku. Według szacunków US National Counterterrorism Center, NCTC jesienią 2014 r. Państwo Islamskie kontrolowało większość basenu Tygrysu i Eufratu o powierzchni ok. 210 tys. km^2, czyli w przybliżeniu tyle, ile wynosi powierzchnia Anglii[19]. Wraz z rozszerzaniem terytorium, nad którym ugrupowanie panowało, rosły również dochody tej organizacji.

Zgodnie z informacjami podawanymi przez zachodnich publicystów dochody Państwa Islamskiego pochodziły z wielu źródeł. Według nieoficjalnych szacunków od lata 2014 r. budżet wojenny organizacji miał powiększyć się w ciągu roku z 800 mln do 2 mld dolarów, z czego 1 mld pochodził z syryjskiej i irackiej ropy naftowej, 430 mln z rabunku banków w Mosulu i w radach prowincji, 100 mln z drukowania fałszywych pieniędzy oraz 40 mln z handlu antykami pochodzącymi z muzeów irackich. O podobnych

[18] Za: *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/Panstwo-Islamskie;5567242.html.

[19] Zob. *What is 'Islamic State'?*, BBC, 2 XII 2015 r., http://www.bbc.com/news/world-middle-east-29052144 [dostęp: 20 IX 2016].

kwotach pisze w swojej książce o ISIS brytyjski dziennikarz Benjamin Hall: *Dżihadyści* (...) *zgromadzili ogromne pieniądze (pod koniec 2014 roku ich majątek był wyceniany na miliard trzysta milionów do dwóch miliardów dolarów*[20].

Z kolei autorzy raportu *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*[21], opublikowanego w lutym 2015 r. przez Financial Action Task Force (FATF), wskazali pięć głównych źródeł finansowania Państwa Islamskiego (obecnie pozostają one takie same). W zależności od wielkości udziału w budżecie, jakim to quasi-państwo dysponowało w tamtym czasie, były to:

1) bezprawny przychód pochodzący z terytoriów okupowanych przez Państwo Islamskie, uzyskany z plądrowania banków, wymuszania, kontroli pól naftowych i rafinerii, kradzieży aktywów ekonomicznych oraz bezprawnego opodatkowania towarów i gotówki przesyłanych tranzytem przez te terytoria (podatek wynosił 2 proc. wartości tych towarów lub gotówki),
2) uprowadzenia dla okupu (rocznie IS potrafiło uzyskać sumy rzędu 30–50 mln dolarów),
3) donacje otrzymywane od organizacji non profit,
4) wsparcie materialne otrzymywane na zasadzie FTF (ang. *friend to friend*),
5) fundusze zdobywane za pośrednictwem nowoczesnych sieci komunikacyjnych (portale społecznościowe)[22].

Takie informacje o źródłach finansowania IS znajdują się w oficjalnym dokumencie FATF. Jeszcze więcej można dowiedzieć się na ten temat z artykułu Any Swanson *How the Islamic State makes its money* zamieszczonego w „Washington Post"[23], i choć jest to publikacja „tylko" prasowa, to jednak ukazała się w jednej z najbardziej prestiżowych gazet codziennych. Oprócz wymienionych źródeł w artykule wspomniano jeszcze o:

– handlu zabytkami znajdującymi się na terenach zajmowanych przez IS, często pochodzącymi z prywatnych kolekcji. Część z nich

[20] B. Hall, *ISIS. Państwo Islamskie*, przeł. P. Wolak, Warszawa 2015, s. 190.

[21] *Financing of the terrorist organisation Islamic State in Iraq and the Levant*, FATF, luty 2015 r., www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html [dostęp: 1 VI 2022].

[22] Tamże, s. 12.

[23] A. Swanson, *How the Islamic State makes its money*, The Washington Post, 18 XI 2015 r., https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money [dostęp: 18 X 2016].

została zniszczona, co pokazywano w filmach emitowanych głównie w sieci oraz w różnych prywatnych i państwowych stacjach telewizyjnych. Można jednak przyjąć, że stanowiło to pewnego rodzaju „zasłonę dymną", aby ukryć sprzedaż zabytków i traktowanie ich jako ważne źródło dochodów (przynajmniej w pierwszym okresie ekspansji). Świadczy o tym informacja przekazana kongresmenom przez Matthew Levitta z waszyngtońskiego Instytutu Polityki Bliskiego Wschodu (Washington Institute for Near East Policy), że w 2014 r. dzięki tym transakcjom IS zdobyło ponad 100 mln dolarów. Po handlu ropą zabytki stanowiły drugie co do wielkości źródło finansowania organizacji;

– dochodach z rolnictwa uzyskiwanych przez IS do zdobywania funduszy w legalny sposób. Wykorzystywali oni jeden z filarów islamu, czyli *zakat* (jałmużna), który jest obowiązkiem każdego muzułmanina (wynosi on 10 proc. dochodów). Ponieważ na terenach pozostających pod kontrolą IS jest uprawiane ok. 40 proc. całego irackiego zboża, dochody z jego sprzedaży wynosiły ok. 200 mln dolarów;
– sprzedaży dóbr materialnych Amerykanów (głównie samochodów, ale również wyposażenia mieszkań) przejętych na zajmowanych terenach;
– handlu lub wynajmie nieruchomości (domów, mieszkań) należących wcześniej do przedstawicieli irackiego establishmentu, osób, które uciekły z terenów okupowanych przez IS bądź zostały zabite;
– opłatach wnoszonych przez obcokrajowców, którzy, chcąc wstąpić w szeregi bojowników IS, są zmuszani do uiszczania swoistego rodzaju „wkupnego";
– dochodach ze sprzedaży fosforanów, cementu, siarki, a przede wszystkim ich form przetworzonych (kwasów). Mimo zaniżonych cen IS potrafiło z ich sprzedaży wygenerować w skali roku ok. 300 mln dolarów zysku;
– handlu ludźmi, przede wszystkim uprowadzonymi kobietami i dziewczętami (jazydkami i turkmeńskimi szyitkami), sprzedawanymi jako niewolnice seksualne.

Od początku istnienia IS jego władze postanowiły uniezależnić się od finansowej pomocy otrzymywanej z zewnątrz, choć oczywiście nie gardziły i nią. Biorąc jednak pod uwagę doświadczenia Al-Ka'idy, która z takich nielegalnych dotacji korzystała, stworzono w tym quasi-państwie quasi-rząd z ministerstwami, w tym Ministerstwem Ropy. Kierował nim do swojej

śmierci Tunezyjczyk Abu Sayyaf (prawdziwe nazwisko według Pentagonu to Fathi Ben Awn Ben Jildi Murad al-Tunisi)[24], który zginął w maju 2015 r. na skutek operacji amerykańskich sił specjalnych. Szura[25] zdecydowała, że IS może się usamodzielnić dzięki wpływom przede wszystkim z handlu ropą naftową i rozpoczęto działania zmierzające do realizacji tych planów. Zatrudniono miejscowych specjalistów pracujących już wcześniej na zajmowanych polach naftowych (m.in. Ajil i Allas w północno-wschodniej prowincji Iraku, Kirkuk czy al-Jibsa w syryjskiej prowincji Hassakeh i innych położonych w prowincji Deir ez-Zor), ściągano inżynierów i techników z Arabii Saudyjskiej lub z Europy, oferując im wysokie zarobki i dając gwarancje bezpieczeństwa zarówno dla nich, jak i ich rodzin. Nad sprawnym i niezakłóconym wydobyciem ropy i produkcją oleju napędowego miała czuwać Amniyat, tajna policja ISIS. Miała ona za zadanie patrolować tereny, na których jest wydobywana ropa, sprawdzać wszystkie transporty i karać nadzorujących wydobycie (nierzadko w bardzo brutalny sposób), gdyby dochodziło do jakichś nieprawidłowości[26].

Dzięki przesłuchaniu Abu Hajjara, pochwyconego przez wojska amerykańskie w czerwcu 2014 r. pod Mosulem, zdobyto informacje o miejscu ukrywania się ówczesnego szefa Rady Wojskowej ISIS Abu Abdulrahmana al-Bilawiego (co doprowadziło do jego zabicia), a przy okazji, co ważniejsze, zdobyto informacje na temat źródeł finansowania IS. Okazało się, że już w 2014 r. z 11 pól naftowych kontrolowanych przez IS w Iraku i Syrii wydobywano do 40 tys. baryłek ropy dziennie, która była przemycana i sprzedawana nielegalnie do Iranu, Kurdystanu, Turcji i Syrii. Sprzedaż przynosiła dochód w wysokości około 1,2 mln dolarów dziennie. Proceder

[24] G. Chazan, S. Jones, E. Solomon, *Isis Inc: how oil fuels the jihadi terrorists*, Financial Times, 15 X 2015 r., https://www.ft.com/content/b8234932-719b-11e5-ad6d-f4ed76f0900a [dostęp: 1 VI 2022].

[25] Shūra (arab. konsultacja) – rada konsultacyjna. W celu uwiarygodnienia w opinii publicznej istnienia IS Abu Bakr al-Baghdadi powołał taką radę. We wczesnej historii islamu była to rada elektorów, którą utworzył drugi kalif (władca społeczności muzułmańskiej) Umar I (634–644), aby wybrać swojego następcę. Obecnie w państwach muzułmańskich termin *shūrā* oznaczał radę stanu lub doradców suwerena (jak w Arabii Saudyjskiej), parlament (jak w Pakistanie) i sąd właściwy do rozstrzygania roszczeń obywateli i opinii publicznej przeciwko rządowi (jak w Afganistanie). Słowo *shūra* stanowi tytuł 42. sury *Koranu*, w którym wierzący są zachęcani do prowadzenia swoich spraw „w drodze wzajemnej konsultacji". Za: *Encyclopedia Britannica*, https://www.britannica.com/topic/shura [dostęp: 1 VI 2022].

[26] G. Chazan, S. Jones, E. Solomon, *Isis Inc: how oil fuels*...

był opłacalny, mimo że ropę sprzedawano po dumpingowych cenach, nierzadko niższych o 75 proc. od obowiązującej na rynkach światowych[27].

Niejasna natomiast była postawa Turcji. Okazało się, że sprzedaż ropy przez IS do Turcji (w pewnym momencie upubliczniona) odbywała się za cichym przyzwoleniem rządu tureckiego, a w handel bezpośrednio był zaangażowany syn prezydenta Recepa Erdoğana – Bilal. Według doniesień medialnych był on współwłaścicielem korporacji transportu morskiego BMZ Group Denizcilik, której tankowce rozprowadzały zakupioną nielegalnie ropę do odbiorców docelowych[28].

Terroryzm sponsorowany przez państwo

Metody finansowania działalności terrorystycznej wymienione w artykule bardzo często oznaczają popełnianie przestępstw kryminalnych. Jednak od lat 70. XX w. do języka naukowego, choć raczej należałoby powiedzieć – politycznego, wszedł termin „terroryzm sponsorowany przez państwo" (ang. *state-sponsored terrorism*). Ten termin został wprowadzony w USA po to, aby wskazywać państwa, które są uznawane przez waszyngtońską administrację za wrogie. Można je obarczać odpowiedzialnością za istnienie (działalność) organizacji terrorystycznych i wspieranie aktów międzynarodowego terroryzmu. W corocznych raportach Departamentu Stanu USA są wymieniane państwa oskarżane o sponsorowanie terroryzmu, przy czym lista tych państw zmieniała się przez ponad 40 lat. Obecnie są na niej cztery kraje[29]:

1) Syria – od 29 grudnia 1979 r.,
2) Iran – od 16 stycznia 1984 r.,
3) Koreańska Republika Ludowo-Demokratyczna – od 20 listopada 2017 r.,
4) Kuba – od 12 stycznia 2021 r.

Wcześniej na liście zamieszczono również Libię, Irak, Jemen Południowy i Sudan.

---

[27] Ch. Dalby, *Who Is Buying The Islamic State's Illegal Oil?*, Oil Price, 30 IX 2014 r., http://oilprice.com/Energy/Crude-Oil/Who-Is-Buying-The-Islamic-States-Illegal-Oil.html [dostęp: 1 VI 2022].

[28] Informacje na ten temat pojawiły się w wielu mediach. Zob. *Meet the Man Who Funds ISIS: Bilal Erdogan, the Son of Turkey's President*, Mint Press News, 30 XI 2015 r., http://www.mintpressnews.com/211624-2/211624 [dostęp: 15 X 2016].

[29] *State sponsors of terrorism*, U.S. Department of State, https://www.state.gov/state-sponsors-of-terrorism/ [dostęp: 13 V 2022].

W latach 70. XX w. na Zachodzie była szeroko rozpowszechniana teza o wspieraniu przez ZSRR i kraje socjalistyczne różnych lewicowych organizacji terrorystycznych. Nie ulega wątpliwości, że studentami Uniwersytetu Przyjaźni Narodów im. Patrice'a Lumumby w Moskwie były osoby, które później zostały terrorystami, a do najbardziej rozpoznawalnych należał Ilich Ramírez Sánchez, znany jako „Carlos" lub „Szakal". Wysuwanie takich oskarżeń można porównać do obciążania Francji zbrodniami Czerwonych Khmerów w Kambodży, ponieważ ich przywódca Pol Pot studiował na Sorbonie. Pewne jest to, że na terytorium NRD znajdowali schronienie członkowie RAF po przejściu na „emeryturę", co udowodniono po zjednoczeniu Niemiec. Nie jest to jednak jednoznaczne ze stwierdzeniem, że od 1968 r. NRD organizowała działalność terrorystyczną ugrupowań lewicowych na terytorium RFN.

Zaprezentowane w tekście sposoby finansowania organizacji terrorystycznych oraz dokonywanych przez nie zamachów to tylko wybrane przykłady. Autor ma nadzieję, że artykuł stanie się początkiem szeroko zakrojonych badań poświęconych temu zagadnieniu.

Bibliografia

Antkol N., Nudell M., *No One Neutral. Political Hostage-Taking In the Modern World*, Ohio 1990.

Dietl W., Hirschmann K., Tophoven R., *Terroryzm*, Warszawa 2009.

Encyklopedia terroryzmu, B. Zasieczna (red.), Warszawa 2004.

Hall B., *ISIS. Państwo Islamskie*, przeł. P. Wolak, Warszawa 2015.

Karolczak K., *Lewicowy terroryzm w Ameryce Łacińskiej*, „Warsztat" 1984, nr 1.

Karolczak K., *Terroryzm i polityka. Lata 2009–2013*, Warszawa 2014.

Źródła internetowe

Afganistan jest największym na świecie producentem służącego do wytwarzania narkotyków maku, Dziennik Gazeta Prawna, 25 VIII 2021 r., https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8231469,afganistan-producent-mak-narkotyki.html [dostęp: 12 VI 2022].

Basar E., *„Drug Trafficking In Africa", Civil-Military Fusion Centre Presents,* grudzień 2012 r., https://www.cimicweb.org/cmo/medbasin/Holder/Documents/r024%20CFC%20Monthly%20Thematic%20Report%20(07-DEC-12).pdf [dostęp: 3 II 2014].

Chazan G., Jones S., Solomon E., *Isis Inc: how oil fuels the jihadi terrorists,* Financial Times, 15 X 2015 r., https://www.ft.com/content/b8234932-719b-11e5-ad6d--f4ed76f0900a [dostęp: 1 VI 2022].

Chellaney B., *Taliban turning Afghanistan into narco-terrorist state,* The Japan Times, 24 XI 2021 r., https://www.japantimes.co.jp/opinion/2021/11/24/commentary/world-commentary/taliban-narco-terrorism/ [dostęp: 16 I 2022].

Dalby Ch., *Who Is Buying The Islamic State's Illegal Oil?*, Oil Price, 30 IX 2014 r., http://oilprice.com/Energy/Crude-Oil/Who-Is-Buying-The-Islamic-States-Illegal-Oil.html [dostęp: 1 VI 2022].

Encyclopedia Britannica, https://www.britannica.com/topic/shura [dostęp: 1 VI 2022].

Financing of the terrorist organisation Islamic State in Iraq and the Levant, FATF, luty 2015 r., www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html [dostęp: 1 VI 2022].

Freeman C., *Revealed: how Saharan caravans of cocaine help to fund al-Qaeda in terrorists' North African domain*, The Telegraph, 26 I 2013 r., http://www.telegraph.co.uk/news/worldnews/africaandindianocean/mali/9829099/Revealed-how-Saharan-caravans-of-cocaine-help-to-fund-al-Qaeda-in-terrorists-North-African-domain.html [dostęp: 2 IV 2014].

Funding of terrorist groups compared, Money Jihad, 21 I 2013 r., http://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/ [dostęp: 3 V 2022].

Idoumou R.O., *Terrorists, traffickers forge union in African desert*, Magharebia, 24 II 2012 r., http://magharebia.com/en_GB/articles/awi/reportage/2012/02/24/reportage-01 [dostęp: 3 II 2014].

Los actos terroritas del E.R.P. y Montoneros, Buen Día Noticia, 31 VII 2018 r., https://buendianoticia.com/nota/10960/los-actos-terroristas-del-erp-y-montoneros [dostęp: styczeń–maj 2022].

Mali: Al Qaeda in the Islamic Maghreb's Ransom Revenue, Stratfor, 15 X 2012 r., http://www.stratfor.com/analysis/mali-al-qaeda-islamic-maghrebs-ransom-revenue // https://worldview.stratfor.com/article/mali-al-qaeda-islamic-maghrebs-ransom-revenue [dostęp: 3 II 2014].

Meet the Man Who Funds ISIS: Bilal Erdogan, the Son of Turkey's President, Mint Press News, 30 XI 2015 r., http://www.mintpressnews.com/211624-2/211624 [dostęp: 15 X 2016].

State sponsors of terrorism, U.S. Department of State, https://www.state.gov/state-sponsors-of-terrorism/ [dostęp: 13 V 2022].

Swanson A., *How the Islamic State makes its money*, The Washington Post, 18 XI 2015 r., https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money [dostęp: 18 X 2016].

Terrorism financing in Australia 2014, Serwis AUSTRAC, https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014 [dostęp: 3 V 2022].

The World's 10 Richest Terrorist Organizations, Forbes, 12 XII 2014 r., http://www.forbes.com/sites/forbesinternational/2014/12/12/the-worlds-10-richest-terrorist-organizations/#336a6802ffae [dostęp: 22 V 2022].

What is 'Islamic State'?, BBC, 2 XII 2015 r., http://www.bbc.com/news/world-middle-east-29052144 [dostęp: 20 IX 2016].

DOI: 10.4467/27204383TER.22.022.16342

ORCID: 0000-0003-2763-9325

DAMIAN SZLACHTER

Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych (skrócony raport)

Dnia 26 kwietnia 2022 r. wśród uczestników spotkania inaugurującego nowy periodyk naukowy „Terroryzm – studia, analizy, prewencja" wydawany przez ABW zostało przeprowadzone pierwsze w Polsce badanie ankietowe dotyczące postrzegania zjawiska terroryzmu oraz przewidywanych, najbardziej prawdopodobnych kierunków rozwoju zagrożeń terrorystycznych w naszym kraju.

Respondentami byli przedstawiciele środowiska akademickiego i analitycznego zajmujący się studiami nad terroryzmem oraz przedstawiciele służb i instytucji należących do wspólnoty antyterrorystycznej RP. Badanie miało charakter anonimowy, wzięło w nim udział 94 respondentów, w tym 71 przedstawicieli administracji państwowej, 21 przedstawicieli środowiska akademickiego oraz 2 analityków współpracujących z ośrodkami badawczymi.

Kwestionariusz ankiety papierowej składała się z 11 pytań – pięć pytań półotwartych (pytania: 1, 2, 3, 5, 6), dwóch pytań zamkniętych (pytania: 7, 8) i czterech pytań wielokrotnego wyboru (pytania: 4, 9, 10, 11). W pytaniach wielokrotnego wyboru zadaniem respondentów było uszeregowanie odpowiedzi według skal 4-punktowej bądź 5-punktowej, podanych każdorazowo w instrukcji do pytania.

Uzyskane wyniki zostały poddane analizie statystycznej, a następnie przedstawione na wykresach. Liczby podane na wykresach zostały zaokrąglone do dwóch cyfr po przecinku.

Na następnej stronie przedstawiono najważniejsze ustalenia płynące z wyników badań ankietowych:

- 62,76% respondentów uznało ISIS (DAESH) za organizację stanowiącą największe zagrożenie bezpieczeństwa państw UE, Al-Ka'ida zajęła drugie miejsce z wynikiem 15,96% głosów, na trzecim miejscu wskazano służby specjalne FR z wynikiem 11,70% głosów.
- 61,70% respondentów uznało ISIS (DAESH) za organizację stanowiącą największe zagrożenie bezpieczeństwa krajów wschodniej części UE, służby specjalne FR zajęły drugie miejsce z wynikiem 17,02% głosów, na trzecim miejscu wskazano Al-Ka'idę z wynikiem 9,57% głosów.
- 53,19% respondentów uznało ISIS (DAESH) za organizację stanowiącą największe zagrożenie bezpieczeństwa RP, służby specjalne FR zajęły drugie miejsce z wynikiem 17,02% głosów, na trzecim miejscu wskazano Atomwaffen z wynikiem 14,89% głosów.
- Wśród typów obiektów, jakie pozostają w zainteresowaniu terrorystów planujących swoją aktywność na terenie UE, respondenci wskazali w pierwszej trójce następujące lokalizacje:
  - obiekty infrastruktury krytycznej (39,36% głosów),
  - otwarte przestrzenie publiczne (32,98% głosów),
  - infrastruktura turystyczna i obiekty sportowe (14,89% głosów).
- Wśród technologii, jakie są obecnie największym wyzwaniem dla służb, organów i instytucji mających zapewnić bezpieczeństwo teleinformatyczne usług, urządzeń lub obiektów mogących być celem ataków terrorystycznych w cyberprzestrzeni, respondenci wskazali w pierwszej trójce:
  - wysoce zaawansowaną technologię automatyzacji procesów sterowania (35,11% głosów),
  - sztuczną inteligencję (26,60% głosów),
  - przechowywanie danych w chmurze (22,34% głosów).
- Wśród narzędzi, urządzeń lub technologii, jakie są obecnie największym wyzwaniem dla służb, organów i instytucji mających zapewnić bezpieczeństwo fizyczne osób i obiektów mogących być celem ataków terrorystycznych, respondenci wskazali w pierwszej trójce:
  - bezzałogowe statki powietrzne (69,15% głosów),
  - improwizowane urządzenia wybuchowe (10,64% głosów),
  - druk 3D (8,51% głosów).
- 47,87% respondentów uznało, że w perspektywie 3-letniej Polska będzie krajem atrakcyjnym dla terrorystów międzynarodowych

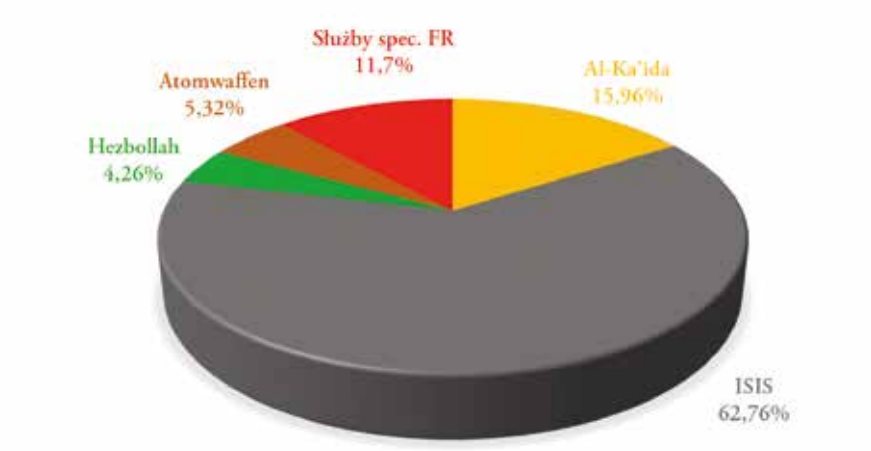
planujących swoją aktywność w UE, z kolei 19,15% respondentów było przeciwnego zdania.
- 90,43% respondentów uznało, że w perspektywie 3-letniej należy spodziewać się aktywności terrorystycznej prowadzonej w ramach działań hybrydowych podejmowanych na terytorium RP przez obce państwo.
- Wśród obiektów znajdujących się w RP, których poziom zagrożenia atakiem terrorystycznym w perspektywie 3-letniej był oceniany przez respondentów jako najwyższy, respondenci wskazali w pierwszej trójce:
  – obiekty energetycznej infrastruktury krytycznej (36,17% głosów),
  – system transportu publicznego (34,04% głosów),
  – bazy wojskowe wykorzystywane w ramach wschodniej flanki NATO (19,15% głosów).
- Wśród tematów badań na terroryzmem, którym należy nadać najwyższy priorytet, respondenci wskazali w pierwszej trójce następujące obszary:
  – proces radykalizacji prowadzący do terroryzmu (30,85% głosów),
  – wykrywanie i blokowanie propagandy terrorystycznej (23,40% głosów),
  – przeciwdziałanie finansowaniu terroryzmu (19,15% głosów).
- Wśród najważniejszych inicjatyw budujących współpracę antyterrorystyczną pomiędzy środowiskiem akademickim a instytucjami i służbami administracji państwowej, respondenci wskazali w pierwszej trójce następujące propozycje:
  – wspólne projekty badawczo-rozwojowe (45,74% głosów),
  – tworzenie sformalizowanych forów wymiany wiedzy i doświadczeń (39,36% głosów),
  – wydawanie wspólnych poradników w zakresie edukacji dla bezpieczeństwa (2,77% głosów).

Opracowanie statystyczne

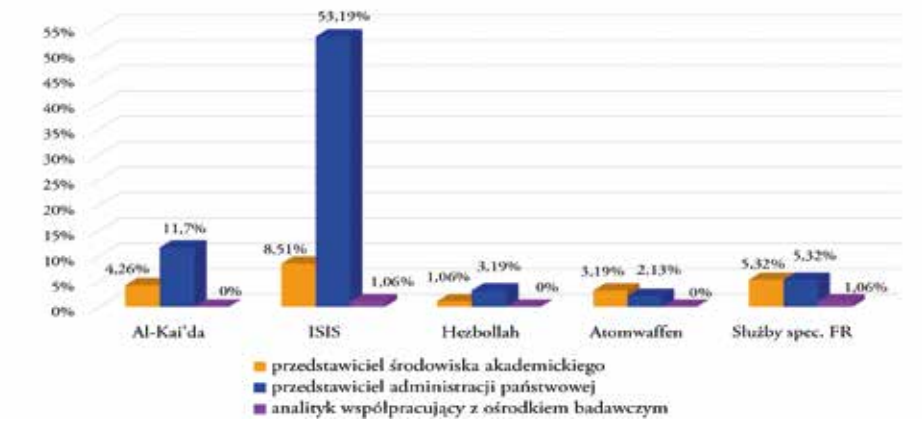
Podział respondentów ze względu na reprezentowane przez nich środowisko:
- 22% – przedstawiciele środowiska akademickiego,
- 76% – przedstawiciele administracji państwowej,
- 2% – analitycy współpracujący z ośrodkiem badawczym.

Pytanie 1. Która z organizacji terrorystycznych stanowi największe zagrożenie bezpieczeństwa państw Unii Europejskiej? (wybierz jedną odpowiedź)

a. Al-Ka'ida,
b. ISIS,
c. Hezbollah,
d. Atomwaffen,
e. Inna.



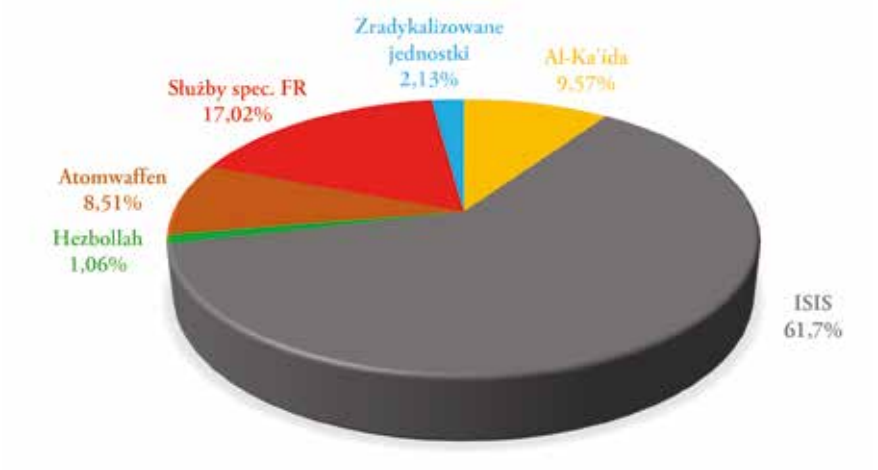
Wykres 1. Organizacje terrorystyczne stanowiące największe zagrożenie bezpieczeństwa państw UE.



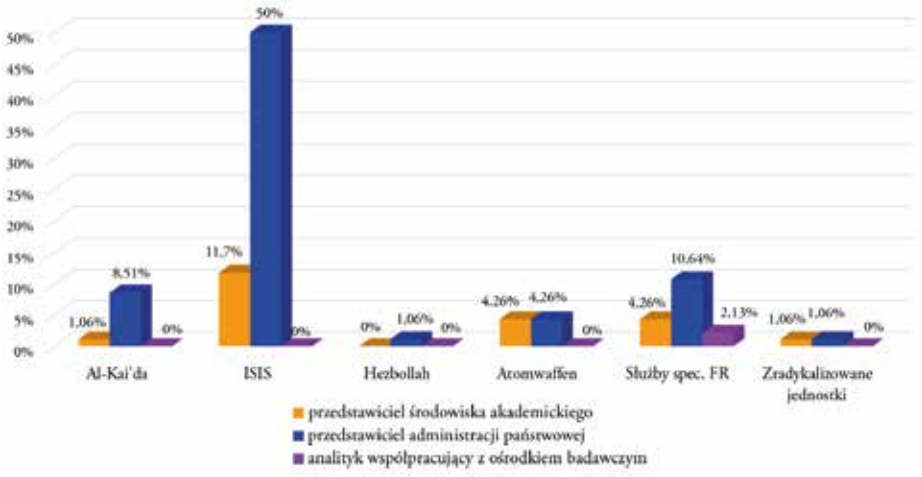
Wykres 1a. Organizacje terrorystyczne stanowiące największe zagrożenie bezpieczeństwa państw UE – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Pytanie 2. Która z organizacji terrorystycznych stanowi największe zagrożenie bezpieczeństwa wschodniej części Unii Europejskiej? (wybierz jedną odpowiedź)

a. Al-Ka'ida,
b. ISIS,
c. Hezbollah,
d. Atomwaffen,
e. Inna.



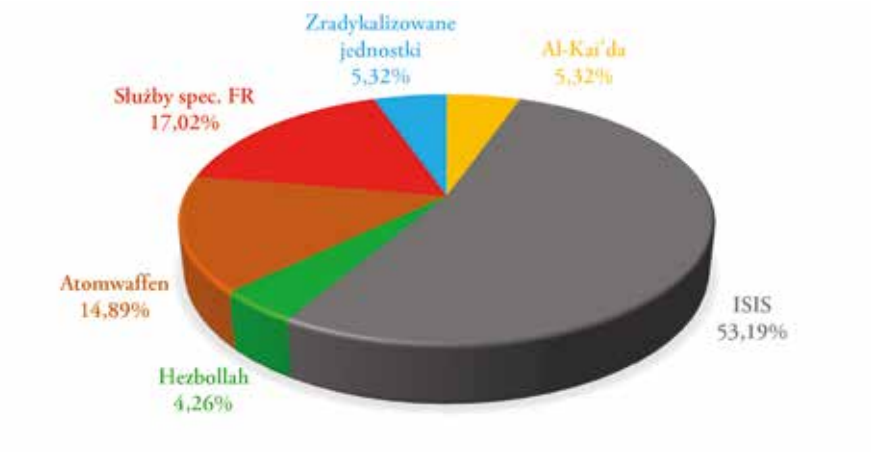
Wykres 2. Organizacje terrorystyczne stanowiące największe zagrożenie bezpieczeństwa wschodniej części UE.



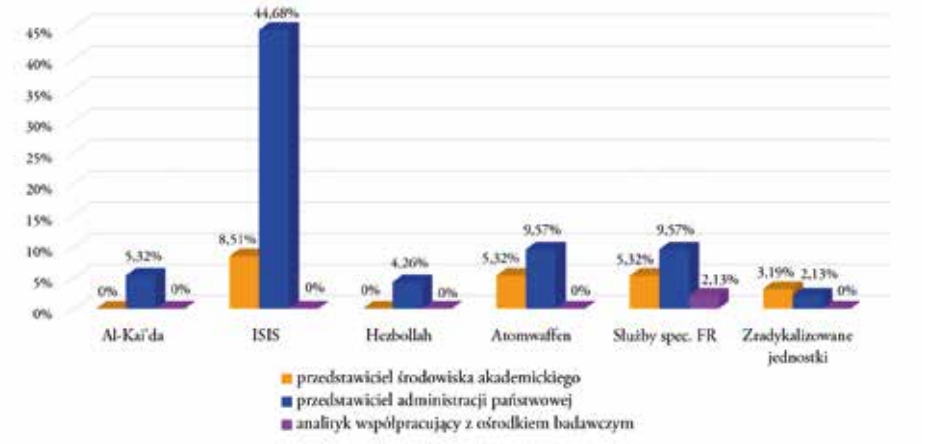
Wykres 2a. Organizacje terrorystyczne stanowiące największe zagrożenie bezpieczeństwa wschodniej części UE – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Pytanie 3. Która z organizacji terrorystycznych stanowi największe zagrożenie bezpieczeństwa RP? (wybierz jedną odpowiedź)

a. Al-Ka'ida,
b. ISIS,
c. Hezbollah,
d. Atomwaffen,
e. Inna.



Wykres 3. Organizacje terrorystyczne stanowiące największe zagrożenie bezpieczeństwa RP.

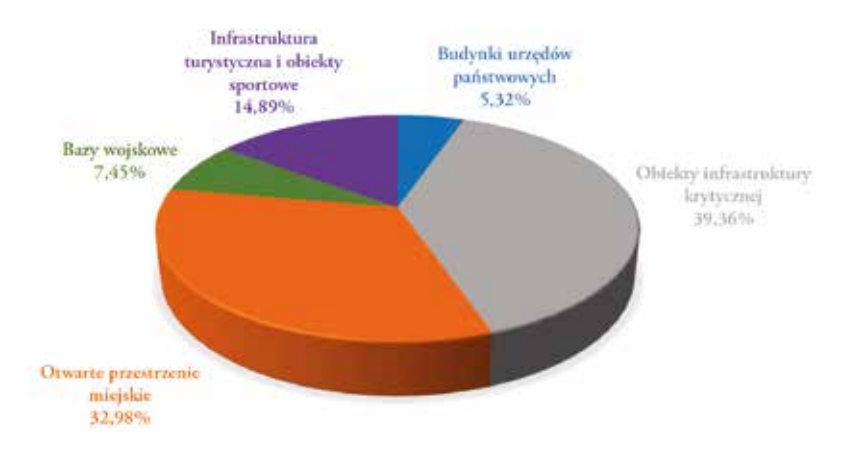


Wykres 3a. Organizacje terrorystyczne stanowiące największe zagrożenie bezpieczeństwa RP – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

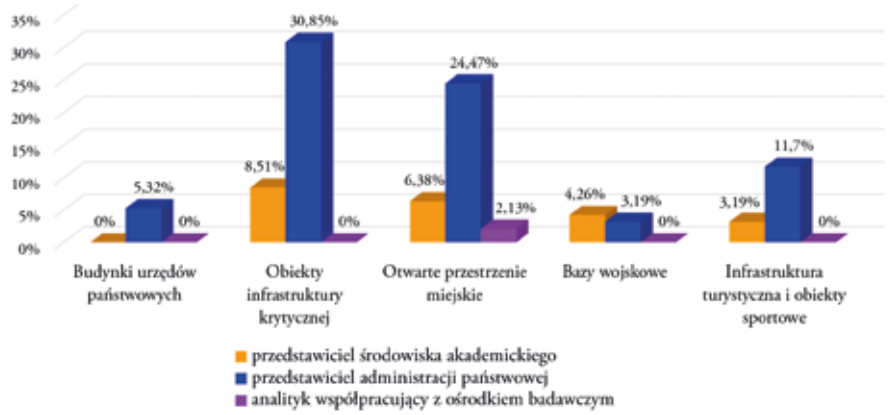
Pytanie 4. Jakimi obiektami interesują się dziś terroryści planujący swoją aktywność na terenie Unii Europejskiej? (uszereguj po prawej stronie od 1 do 5, przy czym 1 oznacza największy poziom zainteresowania)

a. Budynki urzędów państwowych,
b. Obiekty infrastruktury krytycznej,
c. Otwarte przestrzenie miejskie,
d. Bazy wojskowe,
e. Infrastruktura turystyczna i obiekty sportowe.

Obiekty oznaczone cyfrą 1



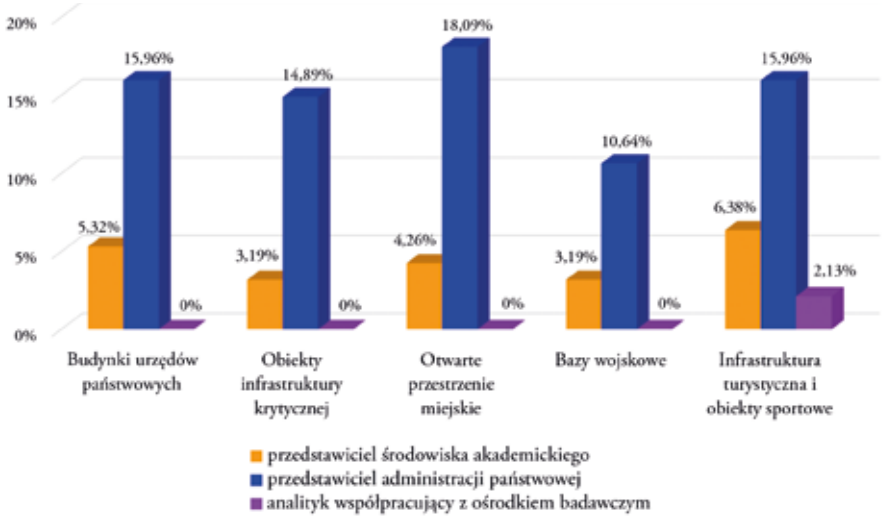
Wykres 4. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 1 (największy poziom zainteresowania).



Wykres 4a. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 1 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

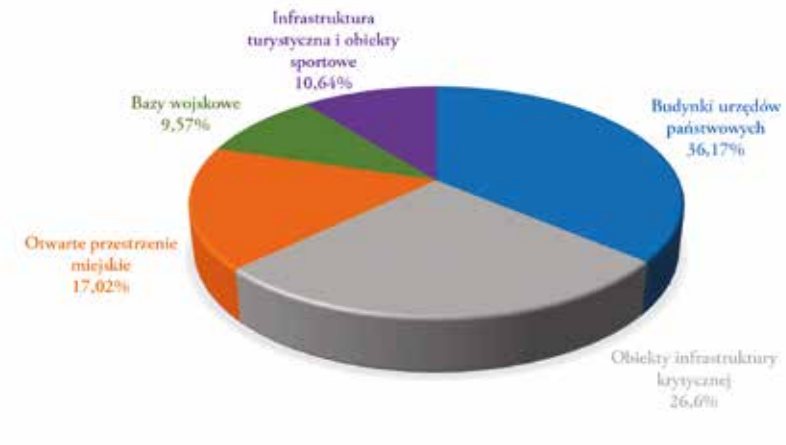
Obiekty oznaczone cyfrą 2

Wykres 4b. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 2.

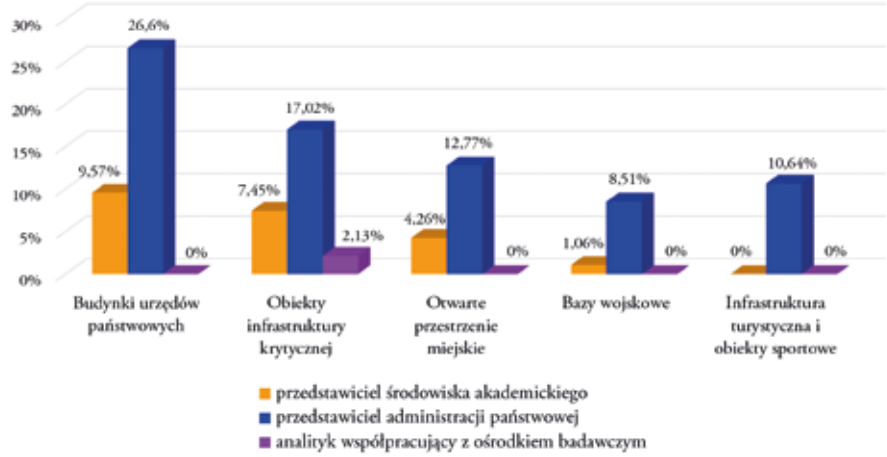


Wykres 4c. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 2 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Obiekty oznaczone cyfrą 3

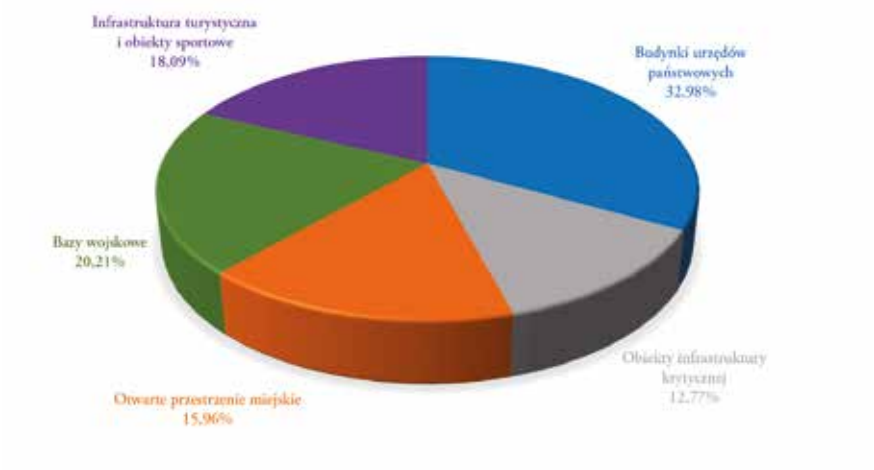


Wykres 4d. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 3.

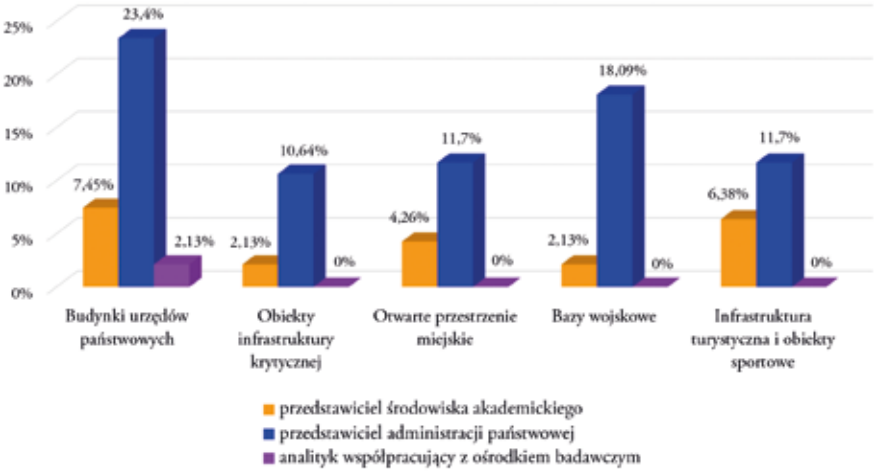


Wykres 4e. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 3 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Obiekty oznaczone cyfrą 4

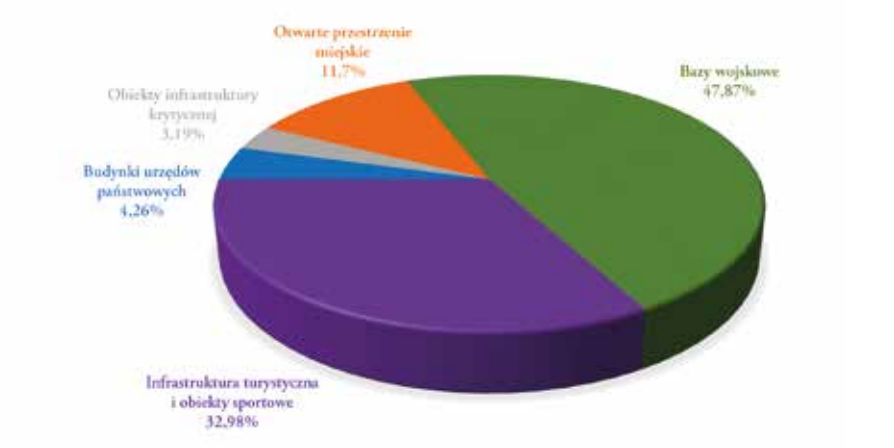


Wykres 4f. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 4.

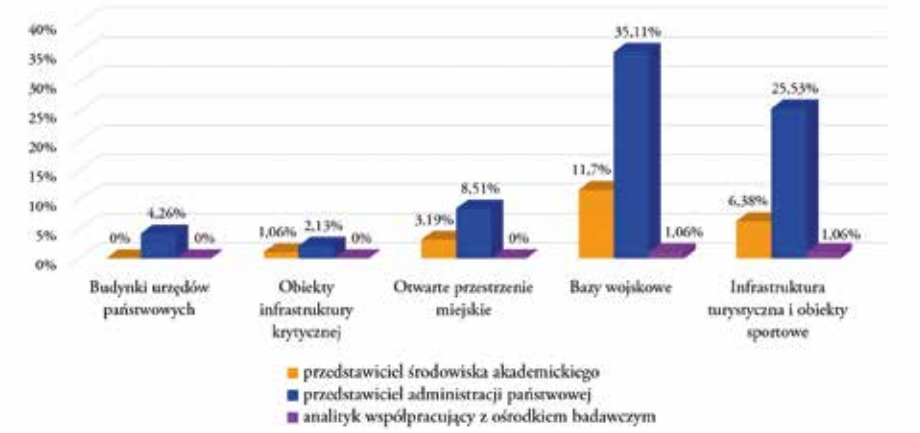


Wykres 4g. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 4 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Obiekty oznaczone cyfrą 5



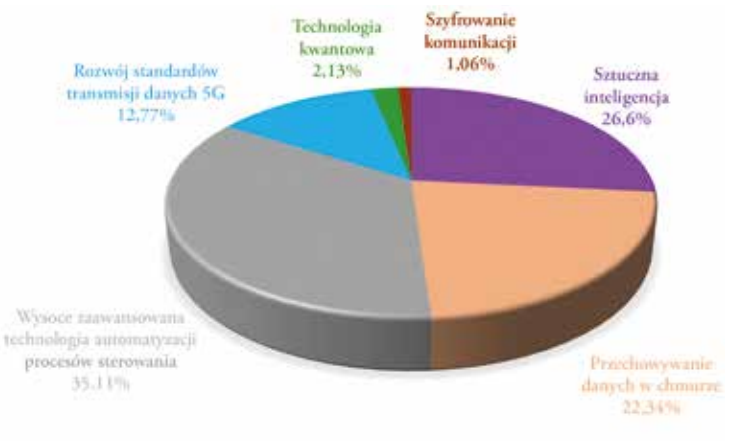
Wykres 4h. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 5.



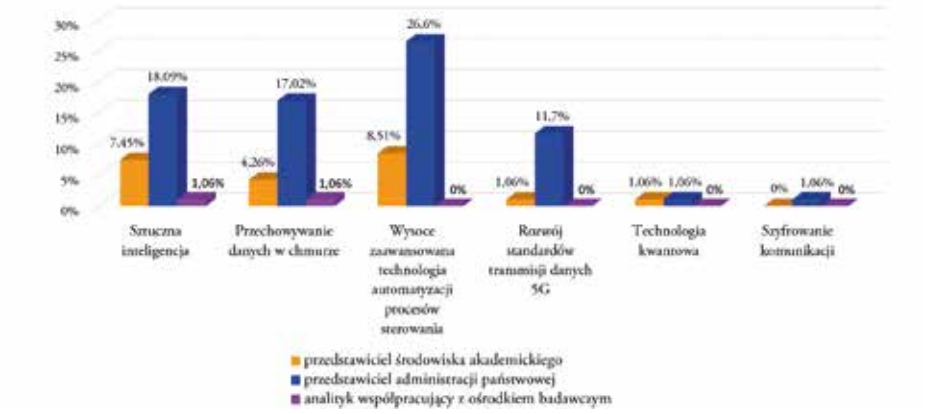
Wykres 4i. Udział poszczególnych typów obiektów, którymi interesują się terroryści planujący swoją aktywność na terenie UE, w grupie obiektów oznaczonych cyfrą 5 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Pytanie 5. Jakie technologie są dziś największym wyzwaniem dla służb, organów i instytucji mających zapewniać bezpieczeństwo teleinformatyczne usług, urządzeń lub obiektów mogących być celem ataków terrorystycznych w cyberprzestrzeni? (wybierz jedną odpowiedź)

a. Sztuczna inteligencja,
b. Przekazywanie danych do chmury,
c. Wysoce zaawansowana technologia automatyzacji procesów sterowania,
d. Rozwój standardów transmisji danych 5G,
e. Inna.



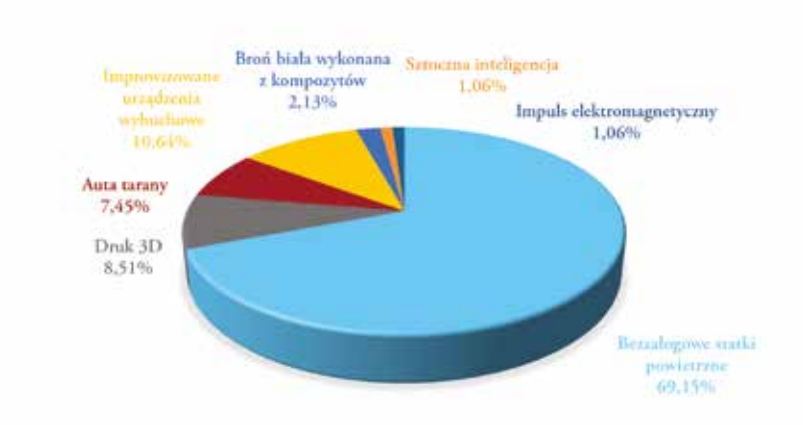
Wykres 5. Technologie, które są dziś największym wyzwaniem dla służb, organów i instytucji mających zapewniać bezpieczeństwo teleinformatyczne usług, urządzeń lub obiektów mogących być celem ataków terrorystycznych w cyberprzestrzeni.



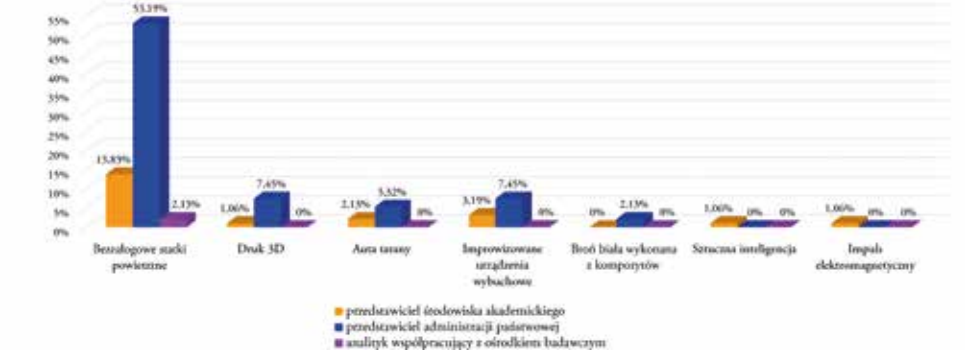
Wykres 5a. Technologie, które są dziś największym wyzwaniem dla służb, organów i instytucji mających zapewniać bezpieczeństwo teleinformatyczne usług, urządzeń lub obiektów mogących być celem ataków terrorystycznych w cyberprzestrzeni – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Pytanie 6. Jakie narzędzia, urządzenia lub technologie są dziś największym wyzwaniem dla służb, organów i instytucji mających zapewniać bezpieczeństwo fizyczne osób i obiektów mogących być celem ataków terrorystycznych? (wybierz jedną odpowiedź)

a. Bezzałogowe statki powietrzne,
b. Druk 3D,
c. Auta tarany,
d. Improwizowane urządzenia wybuchowe,
e. Broń biała wykonana z kompozytów,
f. Inne.



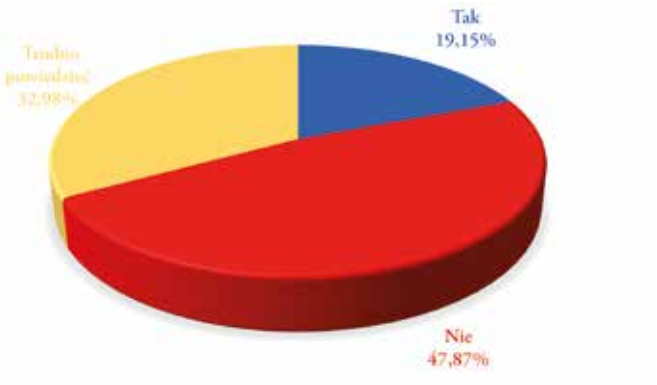
Wykres 6. Narzędzia, urządzenia lub technologie, które są dziś największym wyzwaniem dla służb, organów i instytucji mających zapewniać bezpieczeństwo fizyczne osób i obiektów mogących być celem ataków terrorystycznych.



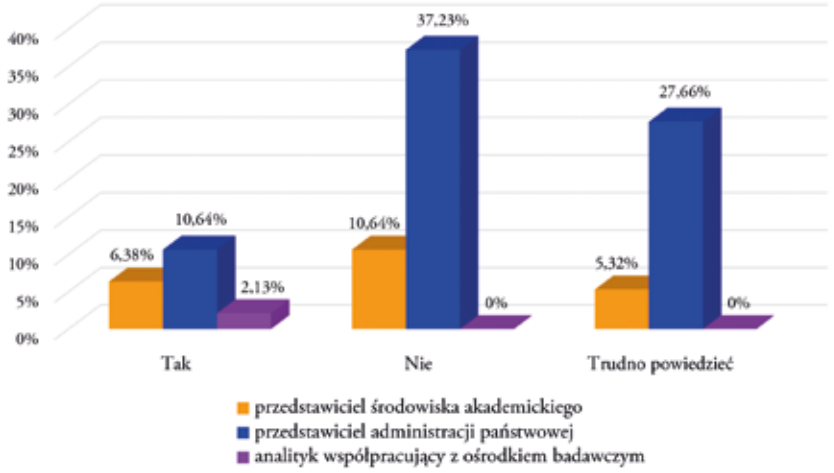
Wykres 6a. Narzędzia, urządzenia lub technologie, które są dziś największym wyzwaniem dla służb, organów i instytucji mających zapewniać bezpieczeństwo fizyczne osób i obiektów mogących być celem ataków terrorystycznych – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Pytanie 7. Czy w perspektywie 3-letniej Polska będzie krajem nieatrakcyjnym dla terrorystów międzynarodowych? (wybierz jedną odpowiedź)

a. Tak,
b. Nie,
c. Trudno powiedzieć.



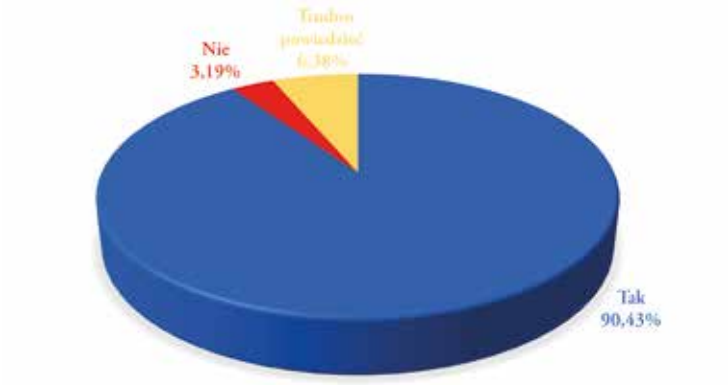
Wykres 7. Polska jako kraj nieatrakcyjny dla terrorystów międzynarodowych w ciągu najbliższych 3 lat.



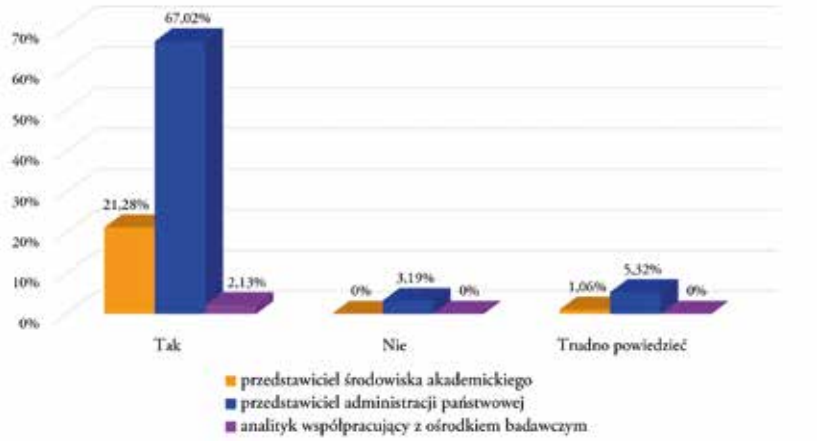
Wykres 7a. Polska jako kraj nieatrakcyjny dla terrorystów międzynarodowych w ciągu najbliższych 3 lat – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Pytanie 8. Czy w perspektywie 3-letniej należy spodziewać się wykorzystania aktywności terrorystycznej w ramach działań hybrydowych podejmowanych na terytorium RP przez obce państwo? (wybierz jedną odpowiedź)

a. Tak,
b. Nie,
c. Trudno powiedzieć.



Wykres 8. Prawdopodobieństwo wykorzystania aktywności terrorystycznej w ramach działań hybrydowych podejmowanych przez obce państwo na terytorium RP w ciągu najbliższych 3 lat.

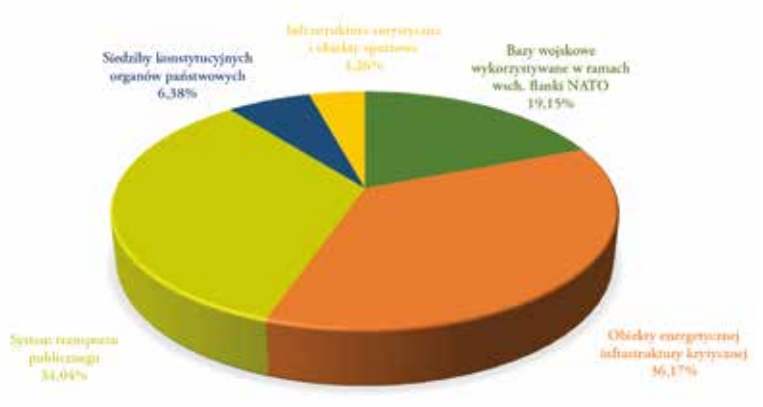


Wykres 8a. Prawdopodobieństwo wykorzystania aktywności terrorystycznej w ramach działań hybrydowych podejmowanych przez obce państwo na terytorium RP w ciągu najbliższych 3 lat – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

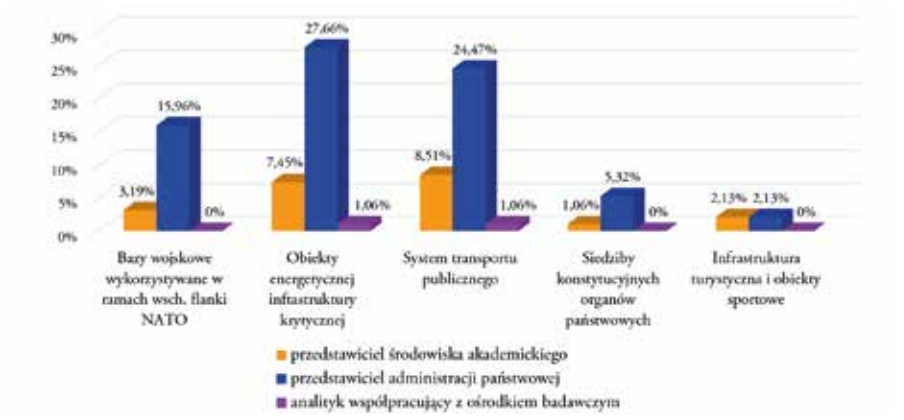
Pytanie 9. Jak w perspektywie 3-letniej będzie kształtować się w Polsce poziom zagrożenia atakiem terrorystycznym wskazanych obiektów? (uszereguj po prawej stronie od 1 do 5, przy czym 1 oznacza największy poziom zagrożenia)

a. Bazy wojskowe wykorzystywane w ramach wschodniej flanki NATO,
b. Obiekty energetycznej infrastruktury krytycznej,
c. System transportu publicznego,
d. Siedziby konstytucyjnych organów państwowych,
e. Infrastruktura turystyczna i obiekty sportowe.

Obiekty oznaczone cyfrą 1

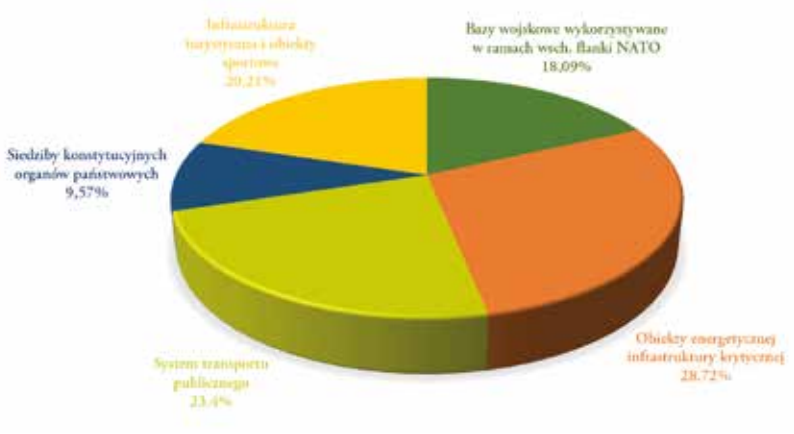


Wykres 9. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 1 (największy poziom zagrożenia).

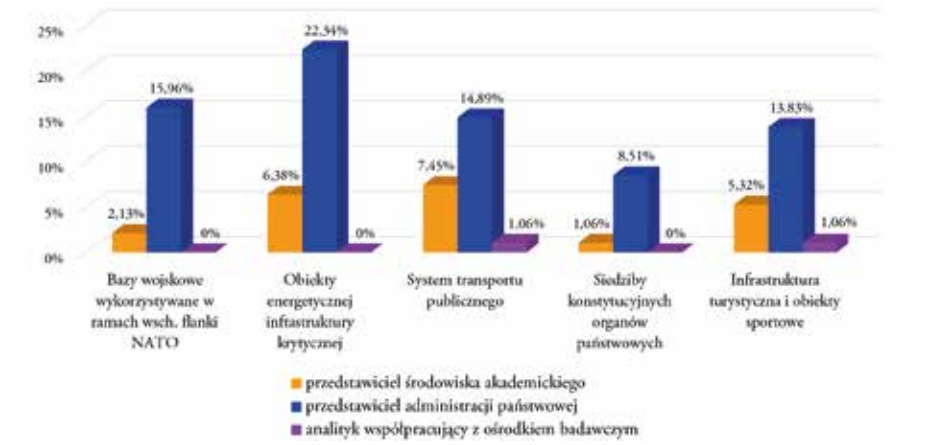


Wykres 9a. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 1 (największy poziom zagrożenia) – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Obiekty oznaczone cyfrą 2

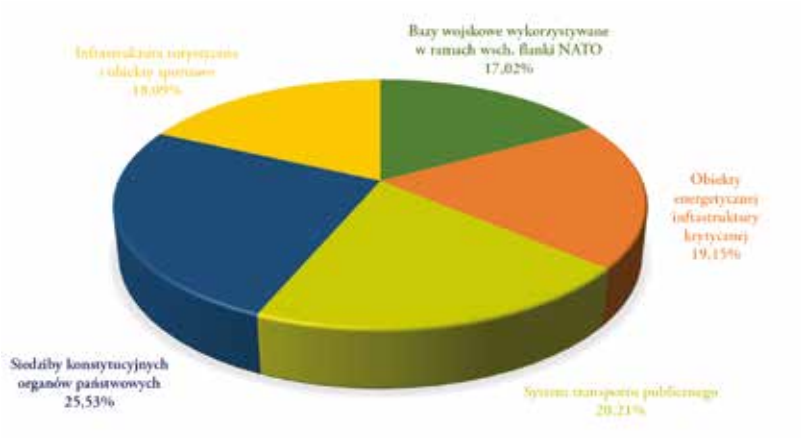


Wykres 9b. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 2.

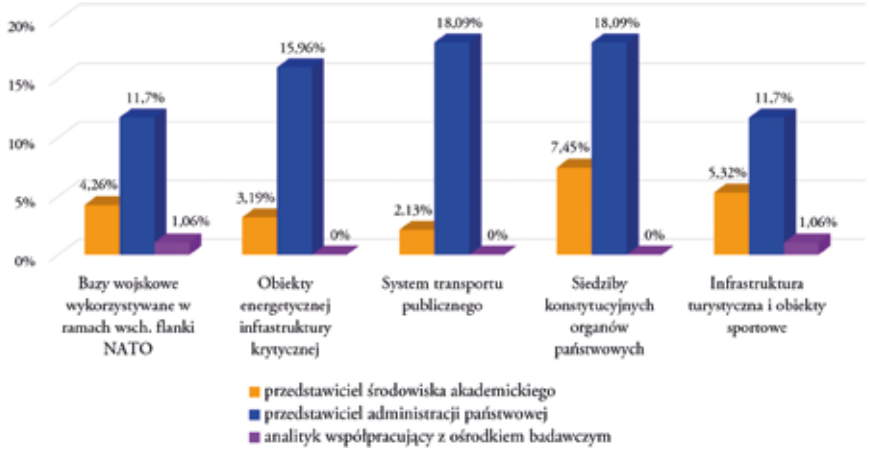


Wykres 9c. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 2 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Obiekty oznaczone cyfrą 3

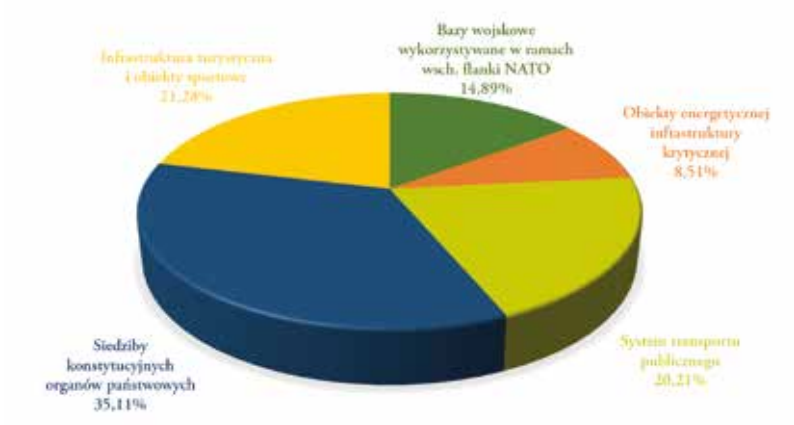


Wykres 9d. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 3.

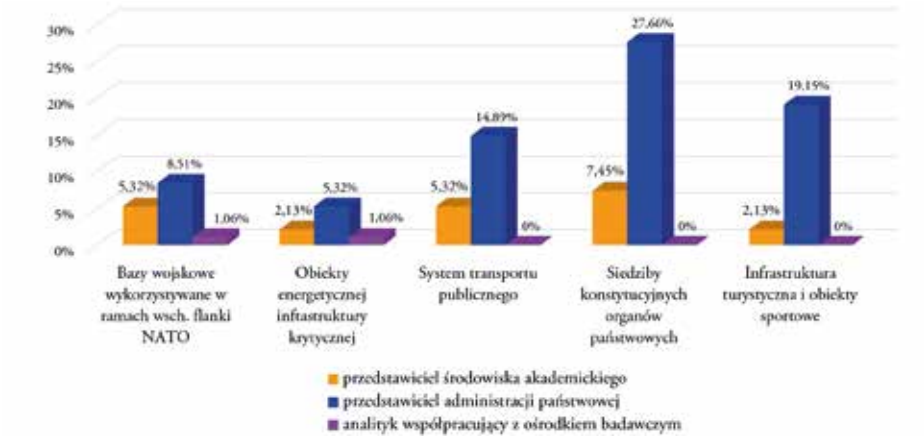


Wykres 9e. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 3 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Obiekty oznaczone cyfrą 4

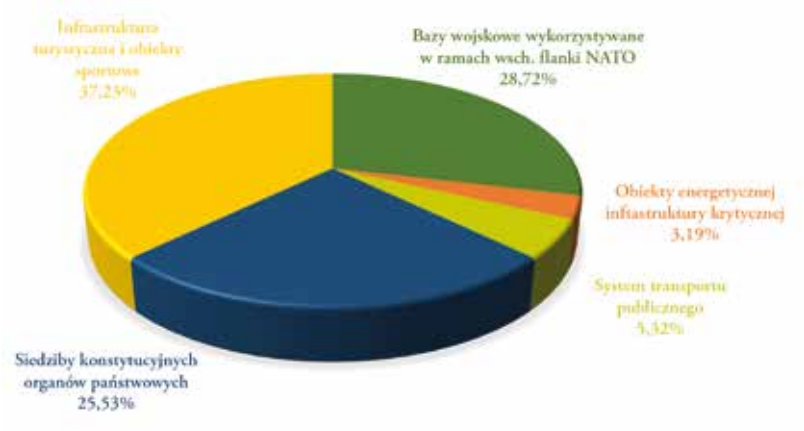


Wykres 9f. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 4.

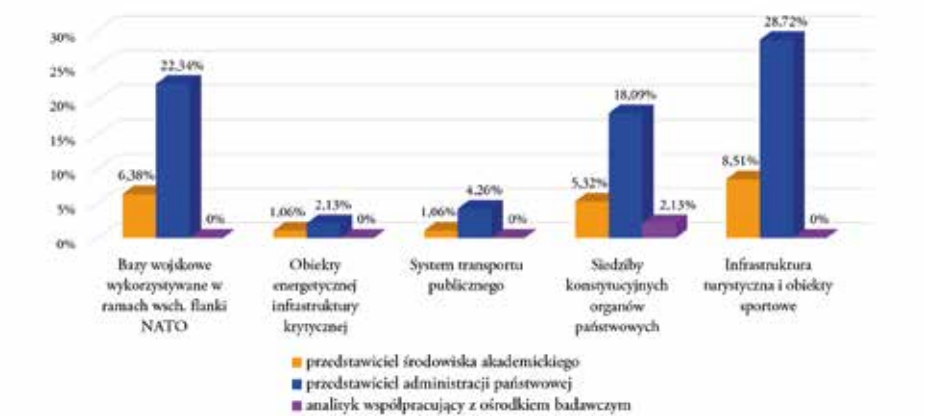


Wykres 9g. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 4 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Obiekty oznaczone cyfrą 5



Wykres 9h. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 5.

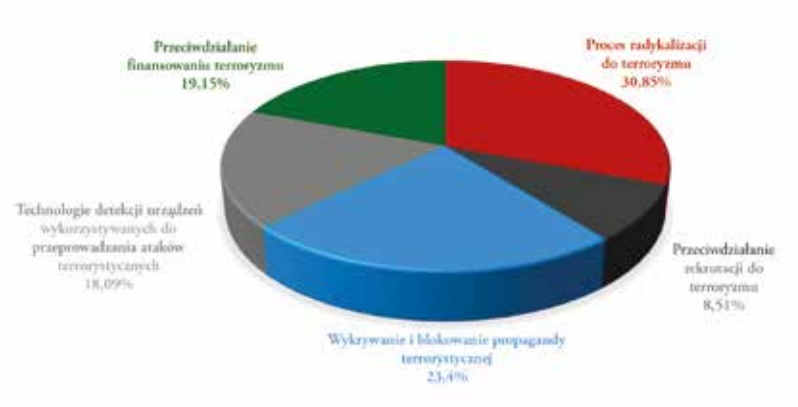


Wykres 9i. Udział poszczególnych typów obiektów w RP zagrożonych atakiem terrorystycznym w ciągu najbliższych 3 lat w grupie obiektów oznaczonych cyfrą 5 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Pytanie 10. Jak powinna wyglądać w Polsce hierarchia ważności tematów badań nad terroryzmem? (uszereguj po prawej stronie od 1 do 5, przy czym 1 oznacza najwyższy priorytet)

a. Proces radykalizacji prowadzący do terroryzmu,
b. Przeciwdziałanie rekrutacji do terroryzmu,
c. Wykrywanie i blokowanie propagandy terrorystycznej,
d. Technologie detekcji urządzeń wykorzystywanych do przeprowadzania ataków terrorystycznych,
e. Przeciwdziałanie finansowaniu terroryzmu.

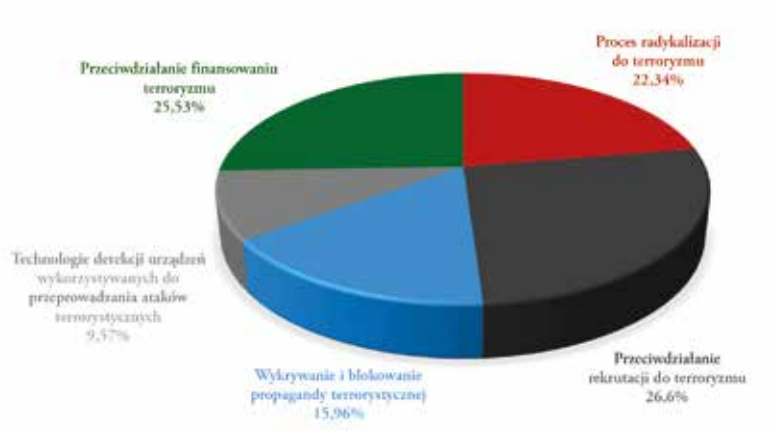
Tematy badań oznaczone cyfrą 1



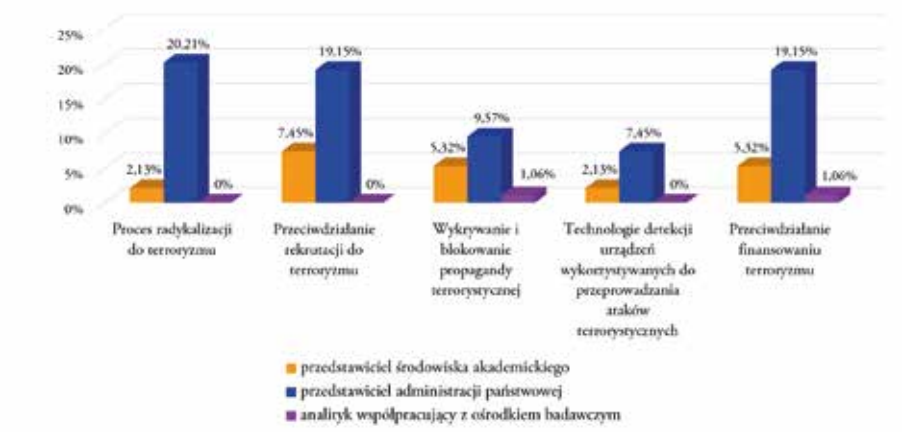
Wykres 10. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 1 (najwyższy priorytet).

Wykres 10a. Udział poszczególnych tematów badań w grupie tematów oznaczonych cyfrą 1 (najwyższy priorytet) – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Tematy badań oznaczone cyfrą 2

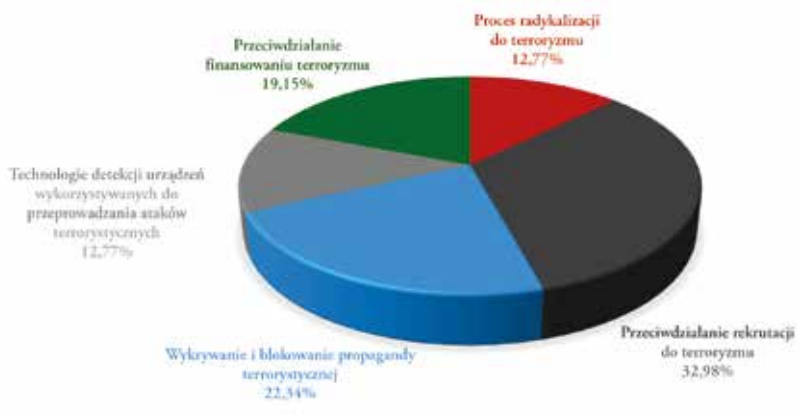


Wykres 10b. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 2.



Wykres 10c. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 2 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

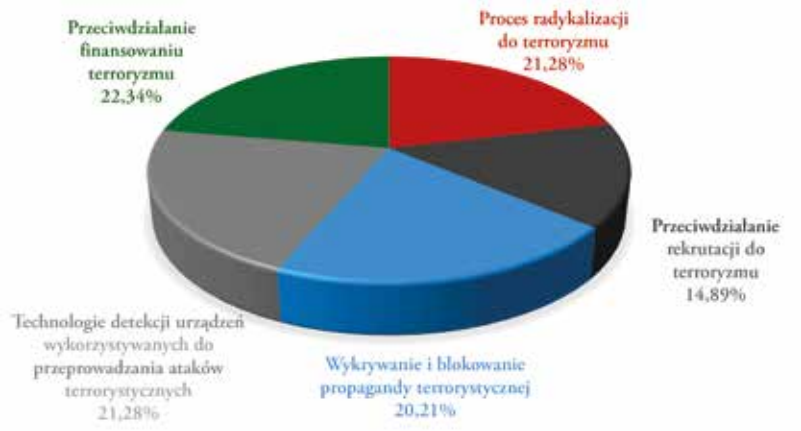
Tematy badań oznaczone cyfrą 3



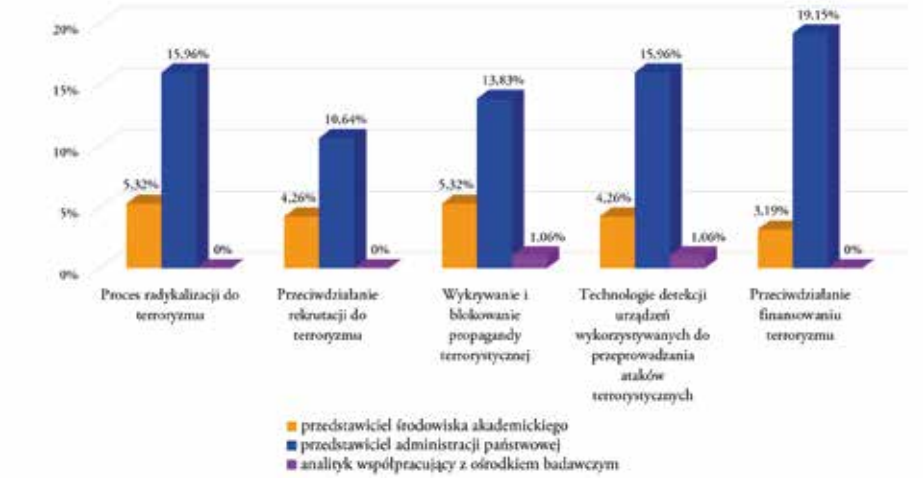
Wykres 10d. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 3.

Wykres 10e. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 3 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Tematy badań oznaczone cyfrą 4

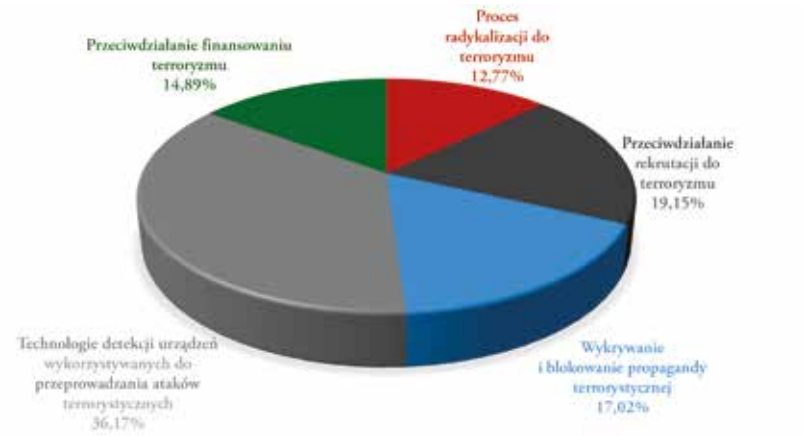


Wykres 10f. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 4.

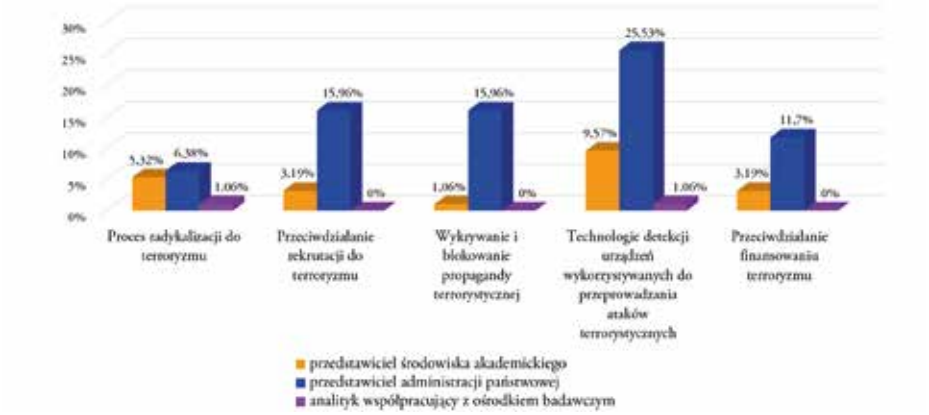


Wykres 10g. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 4 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Tematy badań oznaczone cyfrą 5



Wykres 10h. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 5.



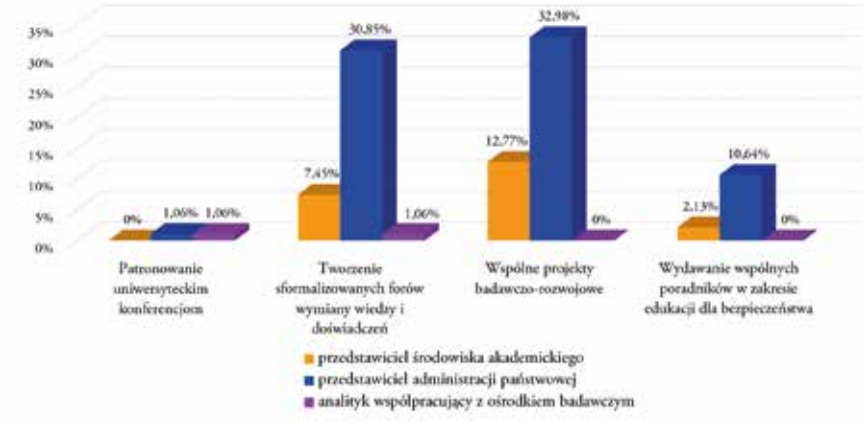
Wykres 10i. Udział poszczególnych tematów badań nad terroryzmem w grupie tematów oznaczonych cyfrą 5 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

11. Jakie inicjatywy budujące współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej należy szczególnie rozwijać? (uszereguj po prawej stronie od 1 do 4, przy czym 1 oznacza najważniejszą inicjatywę)

a. Patronowanie uniwersyteckim konferencjom,
b. Tworzenie sformalizowanych forów wymiany wiedzy i doświadczeń,
c. Wspólne projekty badawczo-rozwojowe,
d. Wydawanie wspólnych poradników w zakresie edukacji dla bezpieczeństwa.

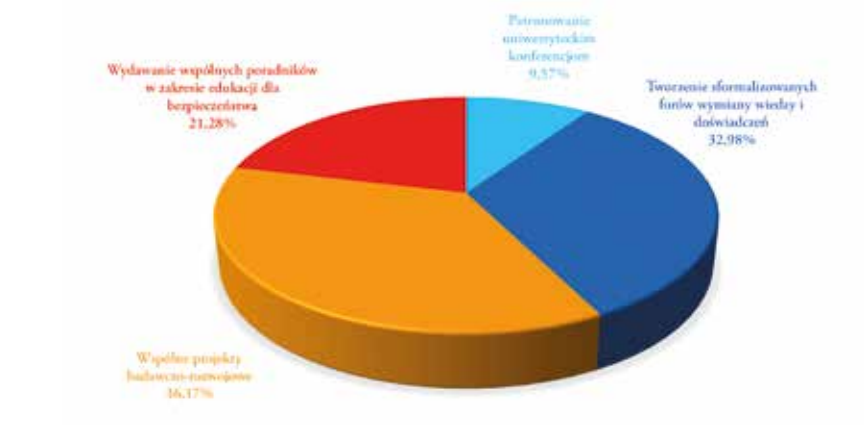
Inicjatywy oznaczone cyfrą 1

Wykres 11. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 1 (najważniejsza inicjatywa).



Wykres 11a. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 1 (najważniejsza inicjatywa) – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

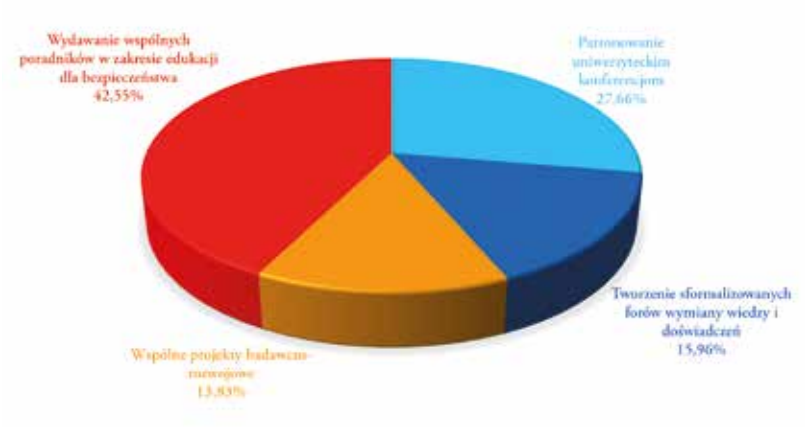
Inicjatywy oznaczone cyfrą 2



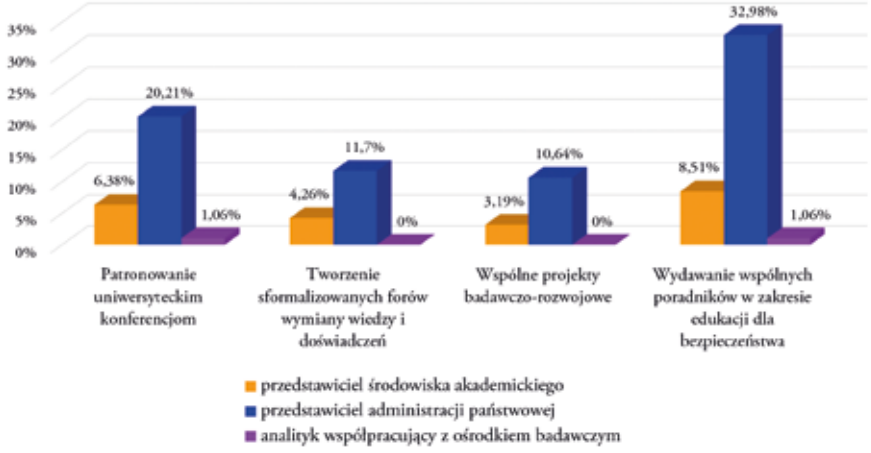
Wykres 11b. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 2.

Wykres 11c. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 2 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Inicjatywy oznaczone cyfrą 3

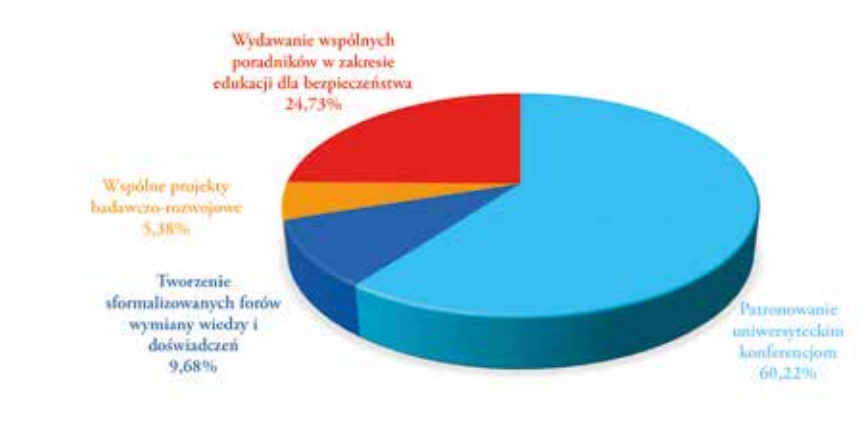


Wykres 11d. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 3.

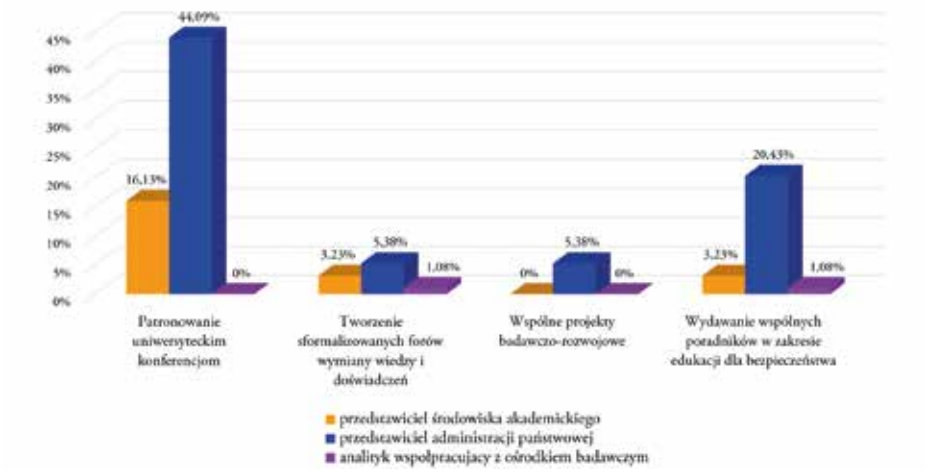


Wykres 11e. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 3 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

Inicjatywy oznaczone cyfrą 4



Wykres 11f. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 4 (93 respondentów, 1 respondent – brak odpowiedzi).



Wykres 11g. Udział poszczególnych inicjatyw budujących współpracę antyterrorystyczną między środowiskiem akademickim a instytucjami i służbami administracji państwowej w grupie inicjatyw oznaczonych cyfrą 4 – rozkład odpowiedzi z uwzględnieniem podziału na środowisko reprezentowane przez respondenta.

DOI: 10.4467/27204383TER.22.023.16343

ORCID: 0000-0003-4649-589X

ANNA ROŻEJ-ADAMOWICZ

Recenzja książki: Tomasz R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne*[1]

W skutecznej prewencji terrorystycznej ważną rolę odgrywa zwiększanie świadomości społecznej. Odpowiednio przygotowane organizacje i służby powinny przekazywać niezbędną wiedzę i uczyć zachowań ratujących życie w sytuacji pojawienia się zagrożenia. Dzięki temu można obniżyć poziom lęku i zwiększyć zdolność członków społeczeństwa do przeciwstawieniasię negatywnym zjawiskom i działaniom innych. Edukację należy prowadzić wielotorowo, dla różnych grup wiekowych i społecznych. Jej podstawą powinna być rzetelna wiedza, płynąca zarówno z poznania naukowego, jak i z doświadczenia.

O powiązaniach między nauką i praktyką oraz o roli prewencji terrorystycznej często wspomina Tomasz Aleksandrowicz w swojej monografii naukowej *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne,* która jest pierwszą na polskim rynku próbą zmierzenia się z tytułową

[1] T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne*, Warszawa 2022, Difin.

problematyką. Cel przyświecający tej publikacji to zaprezentowanie metodyki prognozowania zagrożeń terrorystycznych, tj. podstawowych metod, technik i narzędzi wykorzystywanych w tym procesie. Autor, profesor Wyższej Szkoły Policji w Szczytnie i ceniony ekspert w dziedzinie badań nad terroryzmem, opisuje te zagadnienia na tle rozwiązań krajowych i międzynarodowych, bazując na doświadczeniach państw, które mają długi staż w rozpoznawaniu i zwalczaniu terroryzmu, a zawarte w jego książce ustalenia porządkują wiedzę o tych rozwiązaniach. Podstawową metodą badawczą zastosowaną w jego pracy jest analiza systemowa.

Warto w tym miejscu wspomnieć, że prognozowanie to obecnie niezbędny element funkcjonowania zarówno państw, organizacji, jak i jednostek. Skuteczne strategie bezpieczeństwa nie mogą bowiem polegać wyłącznie na działaniach reaktywnych, lecz muszą się skupiać na antycypacji zagrożeń. Główną tezą książki Tomasza Aleksandrowicza jest stwierdzenie, że prawidłowo opracowana prognoza pozwala na określenie z dużym prawdopodobieństwem możliwości wystąpienia zagrożenia terrorystycznego, jednak zawsze jest to oszacowanie takiej możliwości, a nie pewność poznawcza.

Recenzowana monografia obejmuje 128 stron i składa się z wprowadzenia, siedmiu rozdziałów, zakończenia, aneksu oraz bogatej bibliografii, zawierającej wiele wartościowych, a przede wszystkim aktualnych opracowań, co warto podkreślić ze względu na charakter i dynamikę badanych procesów. Autor starannie przemyślał układ publikacji, który jest spójny i logiczny. We wprowadzeniu precyzyjnie określił cel i przedmiot badań, zakres poruszonej problematyki, założenia i ograniczenia badawcze, przedstawił swoje stanowisko wobec badanego przedmiotu, a także opisał strukturę monografii. Rozdziały 1–3 zostały podzielone na podrozdziały obejmujące zagadnienia szczegółowe. W kolejnych częściach książki ich wyodrębnianie nie było zasadne ze względu na poruszaną w nich problematykę. Książka jest napisana przystępnym językiem, momentami barwnym, gdyż autor nie stroni od odwołań do literatury pięknej, co dla czytelnika może być dodatkowym walorem. Warto podkreślić, że recenzowana publikacja jest tematycznie powiązana z dotychczasowym dorobkiem Tomasza Aleksandrowicza dotyczącym terroryzmu, jego rozpoznawania i zwalczania, co także przemawia za jej wysokim poziomem.

Autor monografii podjął się bardzo wymagającego zadania. Nie ulega bowiem wątpliwości, że prognozowanie to najtrudniejsza część analizy informacji. Należy wyjaśnić, że tworzenie prognozy opiera się na kilku

kategoriach informacji i danych. Przede wszystkim są to dane pochodzące z obszarów, które mogą być poddane poznaniu – te można analizować, wyciągać na ich podstawie wnioski, odpowiadać na klasyczne pytania analityczne: co? Co z tego wynika? Są to tzw. twarde dane, które można nazwać silnymi sygnałami dotyczącymi rozwoju sytuacji w przyszłości. Drugą kategorią są słabe sygnały, które są identyfikowane z trudnością. To zdarzenia (procesy) stanowiące nowość i albo znajdujące się poza sferą dostępną naszemu poznaniu, albo lekceważone. W języku angielskim niekiedy używa się w odniesieniu do nich określenia *slow burning issues*, gdyż są prawie niedostrzegalne, a ich oddziaływanie można zauważyć dopiero po dłuższym czasie od pojawienia się pierwszych symptomów. W przyszłości te słabe sygnały mogą jednak mieć istotny wpływ na rozwój sytuacji. W prognozowaniu konieczne jest również uświadomienie sobie obszarów niewiedzy i ich zakresu oraz podjęcie próby ich oszacowania. Należy też pamiętać, że są informacje i dane, o których wiedzieć nie chcemy. Przyczyny tej niechęci mogą być różne – od politycznych (konieczność podejmowania decyzji społecznie niepopularnych) po psychologiczne (dysonans poznawczy). Prognoza nigdy nie jest zatem pewnością – jej słuszność może być zweryfikowana wyłącznie po upływie określonego czasu, *post factum*. Dobrze przygotowana powoduje jednak, że jesteśmy mniej zaskoczeni przyszłością. Skuteczność prognozy rozumiana jako trafne określenie tego, co zdarzy się w przyszłości, nie stanowi – zwłaszcza w obszarze bezpieczeństwa – jedyne kryterium jej oceny. Na podstawie prognozy często podejmuje się decyzje uniemożliwiające zaistnienie zagrożeń, przed którymi przestrzega. To oznacza, że była ona zarówno słuszna, jak i skuteczna.

Uwagę na to, że klasyczne prognozowanie opiera się na analizie jedynie tego obszaru rzeczywistości, który byliśmy w stanie poznać, zwraca m.in. Andrzej Dawidczyk, specjalista w zakresie analiz strategicznych wykorzystujących metody jakościowe i ilościowe. W ten sposób otrzymujemy fragment obrazu przyszłości ograniczony naszymi przyzwyczajeniami, przyjętymi paradygmatami, ukrytymi założeniami, determinowany utartymi kanonami myślowymi. Zdaniem Dawidczyka istnieje też wspomniany już obszar znajdujący się poza sferą obserwacji, niedostępny poznaniu, w którym zachodzą procesy mające bezpośredni i niekiedy decydujący wpływ na rozwój sytuacji w przyszłości[2]. W opracowaniach dotyczących

[2] A. Dawidczyk, *Analiza strategiczna w dziedzinie bezpieczeństwa państwa. Wybrane metody*, Warszawa 2020.

teorii analizy informacji taką sytuację określono jako problem analizy przy braku wystarczającej ilości danych i nakazywano analitykom, by szukali tego, czego nie ma. Uprzytomnienie sobie, że istnieje konieczność takich poszukiwań intelektualnych, nazwano świadomością informacyjną. Podobnie David Omand, były agent brytyjskiego wywiadu i autor książek z zakresu bezpieczeństwa, zauważa, że nasza wiedza o otaczającym świecie jest zawsze fragmentaryczna, niekompletna i niekiedy popełniamy błędy w ocenie sytuacji. Nie dysponujemy bowiem wszystkimi potrzebnymi informacjami, a co więcej – odczuwamy niechęć do uznania, że nowe dane powinny zmienić wypracowany już obraz rzeczywistości. Mamy też trudności z rozumieniem motywacji przeciwnika, co wiąże się z brakiem znajomości kultury, w jakiej on funkcjonuje, oraz przekonań, jakie sobie wypracował[3]. Bobby W., analityk w Departamencie Analiz CIA, stwierdza, że (...) *nie istnieje taka technika prognozowania, która byłaby w stanie określić czas wystąpienia faktu zmieniającego trend (timing of nonlinearity)*[4]. Analityk wywiadu może sformułować prognozę dotyczącą zwiększenia wyrafinowania planów Al-Ka'idy i wzrostu napięcia na Bliskim Wschodzie, ale nie jest w stanie przewidzieć, kiedy samoloty uprowadzone przez terrorystów uderzą w wieże World Trade Center, ani kiedy samopodpalenie sprzedawcy ulicznego w Tunezji spowoduje wybuch niepokojów społecznych. Procesy prowadzące do zmian w aktywności są stopniowe, lecz gdy jakieś zjawisko zaczyna wykraczać poza obserwowany dotychczas schemat, stanowi to nieprzewidywalny wcześniej punkt krytyczny. Do wskazanych trudności związanych z prognozowaniem należy dodać powszechną walkę informacyjną, której elementami są dezinformacja i wprowadzanie w błąd, także tych starających się przewidzieć rozwój wydarzeń w przyszłości.

Dużym atutem książki Tomasza Aleksandrowicza jest to, że autor porusza jeden z najtrudniejszych i najbardziej skomplikowanych wątków analitycznych, do których należy prognozowanie zagrożeń terrorystycznych. Punktem wyjścia dla jego rozważań jest teza, że terroryści zawsze mają nad państwem przewagę, mogą bowiem zaatakować w wybranym przez siebie momencie, w wybrany przez siebie sposób i przeciwko wybranemu przez siebie celowi, państwo natomiast nie jest w stanie bronić przez cały czas przed każdym rodzajem zamachu każdego potencjalnego celu. Dotyczy to

[3] D. Omand, *How Spies Think. Ten Lessons in Intelligence,* London 2020.

[4] W. Bobby, *The Limits of Prediction – or How I Learned to Stop Worrying about Black Swans and Love Angels*, „Studies in Intelligence" 2019, t. 63, nr 4.

zwłaszcza państw demokratycznych, gdyż terroryści wykorzystują do przygotowania i przeprowadzenia swoich ataków podstawowe atrybuty demokracji, takie jak wolność słowa, dostęp do informacji, swoboda poruszania się czy prawo do prywatności. Te właściwości niestety sprzyjają istnieniu i rozwojowi terroryzmu. Dokonanie zamachu terrorystycznego np. w Korei Północnej jest mało prawdopodobne z uwagi na totalną inwigilację wszystkich osób przebywających na jej terytorium. Wolność i demokracja kosztują – w tym przypadku ceną jest zagrożenie zamachami terrorystycznymi.

We wprowadzeniu do książki autor sformułował niezwykle ciekawy problem badawczy, polegający na (...) *rozstrzygnięciu dylematu, czy jest możliwe prognozowanie zagrożeń terrorystycznych i jaka powinna być metodyka wypracowywania takich prognoz* (s. 9). Pisze, że podstawowym celem jego badań jest (...) *wypracowanie metodyki prognozowania zagrożeń terrorystycznych. Teza, którą autor pokusił się udowodnić, brzmi: istnieje możliwość prognozowania zagrożeń terrorystycznych przy wykorzystaniu w procesie ich opracowania odpowiedniej metodyki* (s. 9). Uzasadnia to przyjętą strukturę opracowania – od systematyzacji zagadnień teoretycznych z zakresu prognozowania (autor analizuje je w kontekście nauki o bezpieczeństwie) przez analizę przedmiotu prognozy, czyli współczesnego terroryzmu, po propozycję metodyki prognozowania w przedmiotowym zakresie na trzech poziomach: strategicznym, operacyjnym i taktycznym.

Pisząc o specyfice nauk o bezpieczeństwie (rozdział pierwszy), autor monografii podtrzymuje swój sformułowany znacznie wcześniej pogląd o wieloaspektowym charakterze tej dyscypliny (ma to swoje odzwierciedlenie również w przywoływanej przez niego literaturze). Jego wywody na ten temat prowadzą go do prawidłowego ustalenia przedmiotu i celu badań. Autor widzi ich sens w skutecznym zapewnianiu bezpieczeństwa państwa, czemu ma służyć właśnie prognozowanie zagrożeń terrorystycznych. Można uznać, że zawarcie rozważanej problematyki w ramach nauki o bezpieczeństwie jest w dużej mierze zasadne, jednak z zastrzeżeniami, o których w dalszej części recenzji.

Autor ujmuje naukę o bezpieczeństwie w sposób skłaniający do dyskusji, krążąc pomiędzy ujęciem szerokim a potrzebą jej osadzenia w bardziej ukonkretnionej warstwie celowościowej (celu naukowego). Po rozważaniach dotyczących interdyscyplinarności nauk o bezpieczeństwie formułuje bowiem pogląd, że (...) *podstawowym kryterium różnicującym nauki o bezpieczeństwie od innych dyscyplin naukowych jest przedmiot badań, który – pomimo sygnalizowanej obszerności – można sprowadzić do środowiska bezpieczeństwa*

podmiotu i jego reakcji na wynikające zeń szanse, wyzwania, zagrożenia i ryzyko (s. 34). Osadza tym samym rozważania w nurcie myślenia i działania strategicznego, odwołując się do najważniejszych kategorii porządkujących badania dotyczące bezpieczeństwa, wyprowadzane przez teoretyków z kręgu nauk wojskowych (wyzwań, zagrożeń itp.). Wskazuje przy tym, że tego rodzaju badania powinny pozostawać w ścisłej zależności z praktyką (rozdział drugi), co jest oczywiste w kontekście stałej potrzeby doskonalenia systemów bezpieczeństwa. To podejście wydaje się odpowiednie do poszukiwania właściwej metodyki prognozowania zagrożeń, nie tylko tych terrorystycznych. Istotne jest, że Tomasz Aleksandrowicz dostrzega i wykorzystuje dorobek innych autorów (np. Andrzeja Dawidczyka, Mirosława Sułka) opisujących różne metody i ich zastosowania w badaniach dotyczących bezpieczeństwa w rozmaitych jego wymiarach. Zdaniem recenzentki w kolejnych wydaniach książki warto byłoby uwzględnić w odwołaniach najnowszą pozycję autorstwa Andrzeja Dawidczyka i Justyny Jurczak pt. *Metodologia bezpieczeństwa w przykładach i zastosowaniach* (Warszawa 2022, Difin).

Niezmiernie interesującą częścią teoretycznego wprowadzenia do przedmiotu opracowania jest ta poświęcona amerykańskiej szkole analizy wywiadowczej. Autor odwołuje się tu zarówno do własnych licznych opracowań poświęconych tej problematyce, jak i do bogatej literatury przedmiotu oraz źródeł pierwotnych (dokumentów, relacji). Ta część monografii stanowi wstęp do autorskiej propozycji metodyki prognozowania, zawiera bowiem bardzo obszerny przegląd stosowanych w niej metod i technik oraz podejść.

Za równie wartościowy należy uznać kolejny (trzeci) rozdział, w którym przedstawiono analizę zagrożeń terrorystycznych jako przedmiotu prognozy. Autor swobodnie porusza się w tej problematyce, przywołując ustalenia autorytetów i wyniki najnowszych badań, a przede wszystkim weryfikując własne oceny i tezy zawarte we wcześniejszych opracowaniach. Ta część publikacji jest uzupełnieniem wiedzy opartej na autorskim dorobku Tomasza Aleksandrowicza, który prezentuje oryginalne podejście do przedmiotowego zagadnienia.

Rozdział czwarty został poświęcony ogólnym ustaleniom dotyczącym prognozowania zagrożeń terrorystycznych. Autor opisuje praktykę rozpoznawania tych zagrożeń i przeciwdziałania im, związaną z działalnością nie tylko służb oraz jednostek specjalnych, lecz także administracji odpowiadającej za bezpieczeństwo państwa. Pozostając w nurcie analitycznym wypracowanym w USA, uwzględnia w analizie również prawne i organizacyjne rozwiązania krajowe. Jest to duży atut monografii.

Rozdziały piąty, szósty i siódmy poświęcono prognozowaniu na poziomie odpowiednio: strategicznym, operacyjnym i taktycznym.

Opis poziomu strategicznego zawiera wzorzec bazy zdarzeń (zamachów) terrorystycznych w skali globalnej. Autor odwołuje się do istniejących rozwiązań tego typu i wskazuje potrzebę jednolitego wzorca opisu danych. Na poziomie strategicznym wyznacza się zasadnicze kierunki polityki antyterrorystycznej państwa oraz czerpie wiedzę potrzebną do prognozowania na poziomie operacyjnym (s. 92), który to wniosek można uznać za zasadny. Podstawowym celem prognozy zagrożeń terrorystycznych na poziomie strategicznym jest odpowiedź na zasadnicze pytania: czy takie zagrożenie istnieje? Czy w dającej się przewidzieć przyszłości możemy być zmuszeni do stawienia mu czoła? Z jakich kierunków zagrożenie może się pojawić? Jaki może mieć charakter? Jakich reakcji państwa wymaga na poziomie strategicznym? Jest to zatem klasyczna analiza i prognoza wieloczynnikowa, której rezultaty stanowią podstawę do podejmowania decyzji politycznych nie tylko związanych z prognozowanym zagrożeniem dla danego państwa, lecz także wynikających z jego zobowiązań prawnomiędzynarodowych, sojuszniczych, takich jak udział w konwencjach wielostronnych, umowach dwustronnych, porozumieniach, sojuszach, czy też wskazujących na potrzebę przystąpienia do takowych bądź intensyfikacji współpracy międzynarodowej w tym zakresie. W sferze polityki wewnętrznej ustalenia wynikające z prognozy strategicznej mogą (i powinny) stanowić podstawę decyzji o budowie systemu antyterrorystycznego, jego kształcie, elementach składowych i kierunkach rozwoju, a jeżeli taki system już istnieje – o kierunkach jego udoskonalania z uwzględnieniem zmian wskazanych w prognozie.

Punktem wyjścia budowy prognozy zagrożeń terrorystycznych na poziomie strategicznym jest stworzenie bazy danych zamachów w skali globalnej w określonym przedziale czasowym, co pozwala na określenie trendu w zagrożeniach. Oczywiście można korzystać z dostępnych publicznie baz, np. START, Global Terrorism Index (GTI) czy EU Terrorism Situation and Trend Report (Te-Sat), trzeba jednak zwrócić uwagę na wykorzystywaną w nich metodykę, a więc na to, jakie przypadki użycia przemocy są przez twórców poszczególnych baz kwalifikowane jako zamach terrorystyczny. Taka baza musi zawierać nie tylko informacje o dokonanych zamachach, lecz także wiele innych rekordów oraz mieć charakter relacyjny, a więc pozwalać na przeszukanie zgodnie z zadanymi kryteriami.

Opisane w kolejnym rozdziale poziom operacyjny i prognozowanie na tym poziomie odnoszą się do konkretnego podmiotu bezpieczeństwa.

Autor przedstawia w tej części procedury krajowe na podstawie dokumentów, obszernie je cytując. Jest to, zdaniem recenzentki, zabieg uprawniony w kontekście celu opracowania.

Prognozowanie na poziomie taktycznym również zostało opisane z uwzględnieniem dokumentów oraz wybranych tez zaczerpniętych z piśmiennictwa krajowego. Autor podkreśla powiązanie tego prognozowania z rozpoznaniem operacyjnym, a więc akcentuje praktyczny wymiar przedmiotowej działalności. Punktem wyjścia do tworzenia prognoz zagrożeń terrorystycznych na poziomie taktycznym jest kilka kategorii danych. Są to przede wszystkim ustalenia wynikające z prognozy na poziomie strategicznym, a więc dotyczące głównych kierunków zagrożeń, preferowanych celów zamachów i modus operandi, czasu politycznego (np. wybory, strajki i niepokoje społeczne, imprezy masowe). Na podstawie tych informacji można opracować kryteria wyboru celu, czasu oraz sposobu działania sprawców i dostosować je do lokalnych uwarunkowań. Przy tworzeniu prognozy na poziomie taktycznym należy wykorzystać dane zawarte w prognozie operacyjnej. Pozwalają one na wytypowanie potencjalnych celów (obiektów) ataków, a więc równocześnie na ukierunkowanie działań polegających na rozpoznaniu tych obiektów przez służby kontrterrorystyczne pod kątem charakterystyki terenu, rozkładu pomieszczeń, sposobu ochrony, zabezpieczeń technicznych czy procedur. Trzeba uwzględnić także dane pochodzące z bieżącego rozpoznania operacyjnego, które dotyczą stwierdzonych przygotowań do zamachu lub też zamachu już dokonanego (precyzyjnie: w toku), np. w przypadku wzięcia zakładników.

Warto w tym miejscu wspomnieć o koncepcji Tomasza Bajerowskiego i Anny Kowalczyk dotyczącej ryzyka urealnionego. Według nich (...) *istnieje potrzeba uzupełnienia metod oceny ryzyka o analizę wykonalności (możliwości realizacji) zdarzeń kryzysowych, w których wykonalność (możliwość) to deterministyczna waga zjawiska losowego*[5]. Proponują oni formułę szacowania ryzyka (metodą matematyczną) określonych zjawisk lub zdarzeń obejmującą wykonalność (możliwość) ich realizacji, ze szczególnym uwzględnieniem zjawisk niemalże nieprawdopodobnych, ale możliwych i mogących wywołać ekstremalne skutki. Autorzy rozgraniczają przy tym dwa pojęcia: prawdopodobieństwa i możliwości (wykonalności) zajścia zdarzenia.

[5] T. Bajerowski, A. Kowalczyk, *Feasibility (Possibility) and Probability in Risk and Crisis Management*, kopia maszynopisu w posiadaniu autorki.

Należy zauważyć, że pomiędzy prognozami zagrożeń terrorystycznych na poziomach strategicznym i operacyjnym zachodzi sprzężenie zwrotne. Ustalenia zawarte w prognozie strategicznej stanowią niejednokrotnie uzupełnienie prognoz operacyjnych, choćby w przypadku, gdy są wykazywane powiązania pomiędzy różnymi podmiotami (np. osobami czy firmami wmieszanymi w działalność terrorystyczną), a z prognozy operacyjnej wynika, że są one zaangażowane w rozpoznawaną sytuację.

Reasumując, opisana w monografii koncepcja prognozowania zagrożeń terrorystycznych sprowadza się do syntezy ogólnych metod prognozowania istniejących w nauce z wytycznymi w zakresie gromadzenia wiedzy w przedmiotowym zakresie. Tak zaprojektowany system rozpoznawania zagrożeń (częściowo oparty na już istniejących rozwiązaniach krajowych) jest wartościowym wkładem w rozwój teorii bezpieczeństwa oraz ważnym przyczynkiem do analizy istniejących rozwiązań na poziomie strategicznym, operacyjnym i taktycznym. Wiele ustaleń, założeń i koncepcji zawartych w monografii Tomasza Aleksandrowicza stanowi dobry punkt wyjścia do dalszej debaty naukowej, co jest kolejnym walorem tej książki.

Publikacją powinni zainteresować się przede wszystkim studenci i badacze z zakresu nauk o bezpieczeństwie, jak również osoby zajmujące się pracą analityczną, zarządzaniem kryzysowym oraz planowaniem działań antyterrorystycznych i kontrterrorystycznych w organach ścigania oraz instytucjach wywiadowczych należących do krajowego systemu walki z terroryzmem, który tworzą członkowie Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych. Książka Tomasza Aleksandrowicza może zostać również wykorzystana jako podręcznik na kursach analizy zagrożeń terrorystycznych organizowanych w środowiskach akademickich oraz w administracji państwowej. Warto rozważyć wydanie publikacji w języku angielskim, aby polska perspektywa prognozowania zagrożeń globalnych mogła uzupełnić literaturę dostępną w euroatlantyckich strukturach szkoleniowych.

O autorach

Dr Piotr Burczaniuk – adiunkt w Katedrze Teorii i Filozofii Prawa Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, radca prawny, członek Okręgowej Izby Radców Prawnych w Lublinie, członek Polskiego Towarzystwa Legislacji, ekspert ds. legislacji. Autor publikacji z zakresu teorii i filozofii prawa, prawa konstytucyjnego oraz prawa gospodarczego. Jego działalność naukowa jest związana z tworzeniem i stosowaniem prawa.

Mariusz Cichomski – prawnik, socjolog, absolwent studiów doktoranckich na Uniwersytecie Warszawskim. Od kilkunastu lat zajmuje się zawodowo zagadnieniami związanymi z terroryzmem, przestępczością zorganizowaną, nadzorem nad działalnością służb oraz legislacją.

Ilona Idzikowska-Ślęzak – politolog, od 2008 r. związana zawodowo z Ministerstwem Spraw Wewnętrznych i Administracji. Aktualnie kieruje wydziałem odpowiedzialnym za kwestie związane z terroryzmem, przestępczością zorganizowaną i organizacją Służby Ochrony Państwa.

Krzysztof Izak – emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Dr Krzysztof Karolczak – politolog, absolwent Wydziału Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego, doktor nauk humanistycznych w zakresie nauki o polityce. Do 2008 r. pracownik naukowy Instytutu Nauk Politycznych WDiNP UW. Wykładowca Wyższej Szkoły Zarządzania i Prawa im. Heleny Chodkowskiej w Warszawie, Warszawskiej Wyższej Szkoły Humanistycznej im. Bolesława Prusa (rektor), Collegium Civitas i Akademii Dyplomatycznej Ministerstwa Spraw Zagranicznych. Autor książek: *Encyklopedia terroryzmu* (1995 r.), *Terroryzm. Nowy paradygmat wojny w XXI wieku* (2010 r.), *Terroryzm i polityka. Lata 2009–2013* (2014 r.).

Dr Michał Piekarski – adiunkt w Zakładzie Studiów nad Bezpieczeństwem Instytutu Studiów Międzynarodowych Uniwersytetu Wrocławskiego. Zajmuje się analizą zjawiska wojny hybrydowej w Europie, współczesnego

terroryzmu, problematyką bezpieczeństwa morskiego państwa oraz zagadnieniami z zakresu kultury strategicznej Polski.

Dr Anna Rożej-Adamowicz – wiceprezes zarządu Inseqr sp. z o.o., ekspert ds. prowadzenia projektów związanych z cyberbezpieczeństwem, pełnomocnik ds. ochrony informacji niejawnych. Specjalizuje się w ocenie zagrożeń oraz konstruowaniu polityki bezpieczeństwa dla systemów IT przetwarzających informacje niejawne. Wykładowca akademicki oraz autor wielu publikacji z dziedziny bezpieczeństwa systemów teleinformatycznych i zarządzania nimi.