TERRORYZM

studia
analizy
prewencja

TERRORISM
PREVENTION
Centre of Excellence

CSS CENTRALNY OŚRODEK
SZKOLENIA I EDUKACJI ABW
im. gen. dyw. Stefana Roweckiego „Grota"

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

Redakcja językowa i korekta części polskojęzycznej BookEdit, www.bookedit.pl

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 w marcu 2022 r.

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

SPIS TREŚCI

Szanowni Państwo!

Ataki na World Trade Center i Pentagon z 11 września 2001 r. stały się punktem zwrotnym w stosunkach międzynarodowych i uświadomiły światowej społeczności ogrom niebezpieczeństw, jaki niesie za sobą terroryzm. Służby specjalne krajów NATO zostały zobligowane do przeorientowania swoich strategii walki z terroryzmem.

Agencja Bezpieczeństwa Wewnętrznego, której 20. rocznicę powstania obchodzimy w tym roku, jest jednym z najważniejszych filarów systemu antyterrorystycznego Rzeczypospolitej Polskiej. Ma to podstawy w zapisach ustawy o działaniach antyterrorystycznych, która weszła w życie w 2016 r. Zadania Agencji realizują dwie wyspecjalizowane i ściśle współdziałające jednostki organizacyjne: Centrum Antyterrorystyczne – prowadzące działania operacyjno-rozpoznawcze oraz Centrum Prewencji Terrorystycznej – zajmujące się szeroko pojętą profilaktyką antyterrorystyczną.

Terroryzm, który od lat stanowi poważne zagrożenie bezpieczeństwa wewnętrznego wielu państw, wciąż ewoluuje. Z tego względu służby specjalne muszą stale zwiększać swój potencjał antyterrorystyczny i dostosowywać go do nowych wyzwań. Działania te są realizowane m.in. poprzez zacieśnianie współpracy między krajowymi ogniwami systemu antyterrorystycznego a światem akademickim reprezentowanym przez badaczy zjawiska terroryzmu.

Od czasu tragicznych wydarzeń z 2001 r. ukazało się w Polsce niemal 300 publikacji tematycznych, których autorami bądź współautorami są polscy naukowcy. Wiele z nich miało istotny wpływ nie tylko na kształt krajowego systemu antyterrorystycznego, lecz także na regionalną politykę bezpieczeństwa. Doceniając znaczenie polskich badań, w 20. rocznicę ataków na WTC i Pentagon podjąłem decyzję, aby w ramach ABW powołać czasopismo naukowe poświęcone tematyce terrorystycznej.

Periodyk „Terroryzm – studia, analizy, prewencja" jest w założeniu platformą wymiany myśli naukowej i doświadczeń. Łączy świat akademicki i przedstawicieli instytucji oraz służb, które od ponad 15 lat współpracują ze sobą w ramach Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, będącego centrum koordynacji systemu antyterrorystycznego RP. Chciałbym, aby na łamach czasopisma toczyła się dyskusja o tym, w jakim kierunku rozwija się zagrożenie terrorystyczne, jak powinny reagować służby specjalne, instytucje antyterrorystyczne i kontrterrorystyczne oraz organy i gremia międzynarodowe budujące odporność wspólnoty euroatlantyckiej na ataki terrorystyczne. Bardzo ważnym elementem nowego czasopisma będą również zagadnienia z zakresu prewencji terrorystycznej. Miarą sukcesu każdego systemu antyterrorystycznego jest bowiem skuteczność, z jaką zapobiega on tego rodzaju atakom, oraz sprawność działania organów państwowych w sytuacjach kryzysowych.

Zachęcając Państwa do lektury pierwszego numeru, zapraszam jednocześnie do współtworzenia czasopisma naukowego „Terroryzm – studia, analizy, prewencja" poprzez dzielenie się na jego łamach swoją wiedzą teoretyczną i praktyczną.

Szef Agencji Bezpieczeństwa Wewnętrznego
płk Krzysztof Wacławek

Szanowni Państwo!

Dotychczasowe doświadczenia krajów zachodnich w walce z terroryzmem pokazują, że potrafią one osiągnąć operacyjną przewagę nad terrorystami, jeśli stworzą skuteczny mechanizm koordynacji i kooperacji antyterrorystycznej, funkcjonujący na poziomie współpracy międzynarodowej, międzyresortowej i wewnątrzinstytucjonalnej. Inicjatywy badawczo-naukowe powiązane z tą problematyką stanowią cenne wsparcie systemu antyterrorystycznego. Ich intensyfikowanie leży w interesie wszystkich służb i instytucji odpowiedzialnych za bezpieczeństwo państwa.

Jedną z takich inicjatyw jest powołany w ramach Agencji Bezpieczeństwa Wewnętrznego nowy periodyk naukowy „Terroryzm – studia, analizy, prewencja". Na jego łamach będą prezentowane materiały naukowe i edukacyjne dotyczące wyzwań związanych z walką z terroryzmem stojących przed Polską i innymi krajami członkowskimi NATO. Poruszana tematyka będzie obejmować m.in.: aspekty prawno-organizacyjne zwiększania skuteczności systemów antyterrorystycznych, sposoby budowania odporności na ataki terrorystyczne, nowe technologie jako narzędzia w rękach terrorystów, kwestie historyczne związane z terroryzmem i ich przełożenie na współczesne realia, działania edukacyjne na rzecz bezpieczeństwa antyterrorystycznego prowadzone dla różnych grup społecznych. Zagraniczna afiliacja części członków rady naukowej, recenzentów i autorów oraz anglojęzyczny przekład czasopisma mają umożliwić dotarcie do szerszego audytorium.

W pierwszym numerze nowego periodyku znajdą Państwo artykuły poświęcone m.in.: wybranym cechom terroryzmu XXI w., prawnym aspektom walki z terroryzmem w RP i UE, 15-leciu Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, radykalizacji prowadzącej do terroryzmu i metodom zapobiegania temu zjawisku stosowanym we Francji, wykorzystaniu cyberprzestrzeni do aktywności terrorystycznej, bezzałogowym statkom powietrznym używanym do ataków

terrorystycznych na obiekty infrastruktury energetycznej, jak również aktywności nowej jednostki pionu antyterrorystycznego ABW – Centrum Prewencji Terrorystycznej.

Zapraszając do lektury czasopisma „Terroryzm – studia, analizy, prewencja", wyrażam nadzieję, że spełni ono swoją misję zacieśnienia współpracy pomiędzy różnymi środowiskami zaangażowanymi w działania na rzecz ochrony antyterrorystycznej oraz poszerzy perspektywę widzenia tych działań. Wierzę również, że będzie się ono systematycznie rozwijać, zyskując liczne grono czytelników i sympatyków.

Redaktor naczelny czasopisma
„Terroryzm – studia, analizy, prewencja"
dr Damian Szlachter

DOI: 10.4467/27204383TER.22.001.15417

ORCID: 0000-0003-4892-6112

KRZYSZTOF KAROLCZAK

Terroryzm XXI wieku – wybrane aspekty

Abstrakt

W artykule została zarysowana problematyka wybranych aspektów terroryzmu w XXI w. Uwzględniając perspektywę historyczną, opisano modus operandi stosowany przez sprawców zamachów (zamachowiec samobójca, samotny wilk) wraz z przykładami najbardziej spektakularnych zamachów: dekapitacja, zastosowanie broni chemicznej, zamachy przy użyciu pojazdów. Do tekstu zostały dołączone dwa wykresy: „Liczba zamachów terrorystycznych na świecie (lata 2006–2019)" i „Najbardziej aktywne grupy przeprowadzające zamachy na świecie w 2019 r. według liczby zamachów".

Słowa kluczowe:

terroryzm, zamach terrorystyczny, zamachowiec samobójca, dekapitacja, samotny wilk, broń chemiczna, zamachy przy wykorzystaniu pojazdów

W nowe tysiąclecie świat wchodził triumfalnie i z nadzieją. Wizja Francisa Fukuyamy „końca historii"[1], zwycięstwa liberalnej demokracji, miała oznaczać zakończenie zimnej wojny i podziału świata na dwa zwalczające się polityczno-militarne bloki. Objęcie w tym nowym porządku świata przywództwa, które nie mogłoby być przez nikogo zakwestionowane, przez jedno mocarstwo – Stany Zjednoczone Ameryki gwarantować miało już tylko szczęśliwą przyszłość.

[1] F. Fukuyama, *Koniec historii*, tłum. T. Bieroń, M. Wichrowski, Poznań 1996.

Rok 2001, początek nie tylko nowego wieku, ale i tysiąclecia, stał się przełomowy w historii światowego terroryzmu. O ile do tamtej pory był on zjawiskiem co najwyżej międzynarodowym (w myśl maksymy: z terroryzmem międzynarodowym mamy do czynienia wówczas, kiedy terroryści z jednego kraju dokonują zamachu na terytorium drugiego w interesie trzeciego), o tyle po 11 września 2001 r. stał się ze względu na swój charakter i zasięg zjawiskiem globalnym. Oczywiście przyczynił się do tego w dużej mierze fakt, że tego dnia Stany Zjednoczone, będące mocarstwem o zasięgu globalnym, zostały zaatakowane na swoim terytorium po raz pierwszy od II wojny światowej. Ponadto o przeprowadzenie zamachów na World Trade Center i Pentagon oskarżona została organizacja Al-Kaida, która chociaż już wcześniej dokonywała zamachów w różnych rejonach świata[2], to do tamtej pory była klasyczną w swej strukturze organizacją hierarchiczną. Szybko jednak przerodziła się w organizację sieciową ogarniającą swoim zasięgiem całą kulę ziemską.

Terroryzm XXI wieku

Przez dwa tysiące lat udokumentowanej historii metody działań terrorystów ulegały zmianom wraz z postępem technologicznym, ale było to raczej dodawanie kolejnych nowych narzędzi do tych już istniejących, sprawdzonych. Zakładając prawdziwość tezy, że pierwszymi terrorystami byli działający w I w. naszej ery w Palestynie sykariusze[3] dokonujący

[2] M.in. 7 VIII 1998 r. w dwu stolicach państw Afryki Wschodniej, Nairobi (Kenia) i Dar es-Saalam (Tanzania), prawie jednocześnie (w odstępie kilkuminutowym) wysadzone zostały w powietrze budynki ambasad Stanów Zjednoczonych – pod gruzami pierwszej śmierć poniosło 12 Amerykanów, 32 obywateli innych państw i 247 Kenijczyków, a rannych zostało 6 Amerykanów, 13 obywateli innych państw oraz ponad 5 tys. Kenijczyków; w drugim zamachu śmierć poniosło 10 osób, rannych zostało 77. Notabene to przy okazji tych zamachów światowa opinia publiczna dowiedziała się o działalności Osamy bin Ladena i Al-Kaidy. Wiek XX zakończył się również zamachem na amerykańskich żołnierzy, do którego przyznała się Al-Kaida: 12 X 2000 r. w adeńskim (Jemen) porcie w cumujący niszczyciel USS Cole uderzyła wyładowana po brzegi materiałem wybuchowym motorówka, powodując powstanie wielkiej wyrwy w burcie okrętu i śmierć 17 marynarzy (39 zostało rannych).

[3] Sykariusze – najbardziej skrajny odłam żydowskich zelotów walczących z rzymskimi okupantami; por. W. Laqueur, *Terrorism*, London 1980, s. 18–19.

zamachów (zabójstw) przy użyciu krótkiego miecza, sztyletu, *sica*[4], można by powiedzieć, że po dwóch tysiącach lat historia zatoczyła koło, jako że dzisiejsi zamachowcy również bardzo często posługują się nożem lub mieczem[5].

Modus operandi terrorystów w XXI wieku

W XXI w. terroryści posługują się tymi samymi metodami co ich poprzednicy, dostosowując je do potrzeb i możliwości. Dlatego ich najczęstszy sposób działania to zamachy bombowe, taranowanie pojazdami przechodniów i atakowanie przypadkowych osób nożem.

Zamachy samobójcze

Światowy terroryzm w pierwszych latach XXI w. zdominowany został przez zamachowców samobójców (takimi też byli zamachowcy 11 września 2001 r.). Zamachowcy samobójcy często noszą materiały wybuchowe pod ubraniem (do potocznego języka trafiła nazwa „pas szahida"), w plecakach (jak zamachowcy z Londynu 7 lipca 2005 r.), a nawet chowają je w ramach rowerów. Często, aby wyrządzić jeszcze większe szkody, zamachowcy samobójcy jeżdżą pojazdami wypełnionymi materiałami wybuchowymi.

Współczesna historia zamachów samobójczych jako przemyślanej taktyki działań terrorystów jest stosunkowo krótka – można ją datować od początku lat 80. XX w. Analitycy wskazują na dynamikę wzrostu ich liczby: „Od 1983 r. zamachy samobójcze stały się ulubioną taktyką terrorystyczną grup powstańczych od Sri Lanki przez Czeczenię po Afganistan. Jednym ze wskaźników tej rosnącej preferencji jest liczba ataków, która wzrosła z 1 w 1981 r. do ponad 500 w 2007 r."[6].

W społeczeństwach cywilizacji zachodniej te zamachy wywoływały szok, gdyż niezgodne są z dogmatami religii chrześcijańskiej. Jednak

[4] Jednosieczny nóż o długości 40–45 cm. Współcześnie w języku hiszpańskim *sicario* oznacza płatnego zabójcę, we włoskim i portugalskim zaś mordercę na zlecenie.

[5] Do mitu sykariuszy nawiązali ultraortodoksyjni Żydzi z powstałej w 2005 r. grupy Sikrikim, atakujący świecką społeczność Izraela.

[6] Cyt. za: J. Kiras, hasło: „suicide bombing", *Encyclopedia Britannica*, 13 XI 2019 r., https://www.britannica.com/topic/suicide-bombing [dostęp: 28 XI 2021].

dla wyznawców innych religii samobójstwo nie jest zabronione, a przez niewierzących problem ten w ogóle nie jest rozważany (jeśli już, to w kategoriach moralnych). Co więcej, nawet w islamie, który przez wiele lat nie dopuszczał do działalności terrorystycznej kobiet, w pewnym momencie przyzwolono na dokonywanie przez nie zamachów samobójczych (pierwsze takich misji podejmowały się jednak nie muzułmanki, ale Tamilskie Tygrysice; jedna z nich, Thenmozhi Rajaratnam, 21 maja 1991 r. zabiła w takim zamachu b. premiera Indii Rajiva Gandhiego). W Rosji pojawiły się tzw. czarne wdowy (*smiertnice*) – Czeczenki, a w Izraelu – szahidki, Palestynki, członkinie Armii Róż[7].

Pomimo że dzieci otaczane są w każdej społeczności szczególną opieką, to nierzadko biorą udział w konfliktach zbrojnych lub są wykorzystywane do przeprowadzania zamachów terrorystycznych, w tym samobójczych.

Generalnie liczba zamachów samobójczych stanowiła nikły procent zamachów terrorystycznych. Riaz Hassan w artykule *What Motivates the Suicide Bombers? Study of a comprehensive database gives a surprising answer* podaje informację, iż w latach 1981–2006 dokonano 1200 zamachów samobójczych, co stanowiło zaledwie 4 proc. wszystkich zamachów, przy czym zabitych w nich zostało 14 599 osób, co stanowiło 32 proc. wszystkich ofiar[8]. Dlatego też ze względu na ich spektakularność organizacje terrorystyczne bardzo chętnie wykorzystują tę metodę działania.

Dekapitacja: nowa/stara metoda wojny psychologicznej

Uśmiercanie poprzez ścięcie głowy nie jest pomysłem nowym, a tym bardziej nie wymyślili tej metody islamscy fundamentaliści. Jako sposób wykonania sądowego wyroku śmierci metoda ta znana jest od tysiącleci. Dekapitacja była stosowana przez władze wobec przeciwników politycznych i pospolitych przestępców w starożytności (w Chinach, w państwach Bliskiego Wschodu), w wiekach średnich (w Europie), w czasach nowożytnych (nadal w Europie), a i dzisiaj kara ta stosowana jest w Arabii Saudyjskiej. Zmieniano tylko narzędzie: mogły to być

[7] Por. B. Victor, *Army of Roses. Inside the World of Palestinian Women Suicide Bombers*, London 2004.

[8] R. Hassan, *What Motivates the Suicide Bombers? Study of a comprehensive database gives a surprising answer*, „YaleGlobal", 3 IX 2009 r. [dostęp: 28 XI 2021].

topór, miecz, gilotyna, ale niezależnie od tego, czym posługiwał się kat, egzekucja była wykonywana publicznie i odgrywała podwójną rolę – zarówno kary za prawdziwe (lub wyimaginowane, jak zdarzało się często np. podczas rewolucji francuskiej) zbrodnie, jak i ostrzeżenia dla innych, którym miała uzmysławiać, co może ich czekać, gdy sprzeciwią się władzy.

Do tej metody w XXI w. powrócili islamscy fundamentaliści. Już kilka miesięcy po rozpoczęciu wojny z terroryzmem, 23 stycznia 2002 r., w Pakistanie uprowadzony został amerykański dziennikarz Daniel Pearl, a następnie 1 lutego zabity przez porywaczy. Umieszczony w Internecie film z egzekucji zatytułowano *The Slaughter of the Spy-Journalist, the Jew Daniel Pearl*, a przedstawiał on ostatnie sekundy życia dziennikarza, jego oświadczenie, w którym przyznawał się do swojego żydowskiego pochodzenia (przy czym przez wielu analityków uznane ono zostało za zmanipulowane), oraz scenę dekapitacji. Jego ciało odnaleziono i zidentyfikowano 16 maja. Do uprowadzenia i zabicia Amerykanina przyznała się nieznana do tamtej pory organizacja National Movement for the Restoration of Pakistani Sovereignty, ale pakistańskie władze oskarżyły i aresztowały kilku członków Al-Kaidy, w tym szejka Ahmeda Saeeda Omara, który nawet przyznał się do zabójstwa Pearla i został skazany na karę śmierci (kary nie wykonano)[9]. Zawsze też powinniśmy pamiętać, że taka sama śmierć spotkała 7 lutego 2009 r. w Pakistanie polskiego geologa Piotra Stańczaka, który kilka miesięcy wcześniej uprowadzony został przez talibów.

Nagrania wideo dekapitacji uprowadzonych przez iracką Al-Kaidę pojawiły się w 2004 r. w Internecie i były też emitowane przez katarską telewizję Al-Dżazira. Egzekutorem miał być lider ugrupowania Abu Musab al-Zarkawi (choć podważali te informacje ludzie go znający), który zastąpił na listach najbardziej groźnych terrorystów Osamę bin Ladena. Al-Zarkawi ponoć osobiście odciął głowę Nicholasowi „Nickowi" Bergowi (7 maja 2004 r.) i Owenowi Eugenowi „Jackowi" Armstrongowi (20 września 2004 r.). Amerykanie 6 czerwca 2006 r. przeprowadzili nalot bombowy na dom al-Zarkawiego, w którym się ukrywał. Al-Zarkawi zginął, a egzekucje uprowadzonych zakładników przestały być metodą

[9] Szejk Omar odwołał swoje zeznania w 2007 r., kiedy do zabicia Pearla przyznał się Chalid Szajch Muhammad.

stosowaną na masową skalę w walce islamskich fundamentalistów z Zachodem, choć sporadycznie się zdarzały.

W 2014 r. za sprawą Państwa Islamskiego światową opinię publiczną zelektryzowało zastosowanie po raz kolejny dekapitacji jako metody nie tylko likwidacji przeciwnika, lecz także zastraszenia i wymuszenia realizacji żądań ugrupowania. Pomiędzy 25 lipca 2014 r. a 10 sierpnia 2015 r. w 24 egzekucjach zamordowano w ten sposób co najmniej 300 osób (zagranicznych dziennikarzy, żołnierzy syryjskich i kurdyjskich, pracowników organizacji humanitarnych, chrześcijańskich uchodźców z Etiopii)[10].

Samotny wilk (ang. *lone wolf*)

Według mediów nową kategorię terrorystów w XXI w. stanowią zamachowcy niebędący członkami jakiegokolwiek ugrupowania, niedziałający na rozkaz jakiegoś swojego dowódcy, nierealizujący żadnego konkretnego, globalnego planu, ale samotnicy, którzy przygotowywali i przeprowadzali zamachy samodzielnie, bez żadnej pomocy z zewnątrz, określani jako samotne wilki. Nic bardziej mylnego – choć oczywiście należy odróżnić atak pojedynczego zamachowca na polityka (w historii, również naszej, było takich wielu, by przypomnieć Michała Piekarskiego, który zaatakował czekanem króla Zygmunta III Wazę) od zamachu terrorystycznego. Za pierwszych samotnych wilków można uznać zarówno Antoniego Berezowskiego, który 6 czerwca 1867 r. dokonał w Paryżu nieudanego zamachu na cara Aleksandra II, jak i związanych ze środowiskiem anarchistów Sante Giovanni'ego Caserio, zabójcę prezydenta Francji Marie-François Sadi Carnota (24 czerwca 1894, Lyon), oraz Luigiego Lucheni, zabójcę cesarzowej Austrii Elżbiety (10 września 1896 r., Genewa), czy w końcu Leona Czolgosza, który 6 września 1901 r. śmiertelnie postrzelił w Buffalo prezydenta Stanów Zjednoczonych Wiliama McKinleya.

W drugiej połowie XX w. takich samotnych wilków też było wielu. Do historii terroryzmu przeszli m.in. dwaj Amerykanie – Theodore Kaczynski „Unambomber" i Timothy.

Theodore'a Kaczynskiego być może należałoby zakwalifikować jako reprezentanta nurtu ekologicznego lub, sięgając do pojęć XIX w.,

[10] https://edition.cnn.com/2015/04/19/africa/libya-isis-executions-ethiopian-christians/ [dostęp: 20 XI 2021].

luddystę, choć sam o sobie pisał, że protestuje przeciwko nowoczesnej technologii[11]. Przez 17 lat rozsyłał on do polityków, naukowców, szefów korporacji listy-bomby, które zabiły 3 osoby i zraniły 29. Aresztowany został 3 kwietnia 1996 r. i skazany na karę dożywotniego więzienia.

Timothy McVeigh głosił skrajnie prawicowe poglądy, uznawał rząd w Waszyngtonie za okupacyjny (ZOG – *Zionist Occupation Government*). Dokonał zamachu bombowego na budynek władz federalnych w Oklahoma City (19 kwietnia 1995 r.), w którego wyniku zginęło 168 osób. Został aresztowany i skazany na karę śmierci.

Samotnym wilkiem był również Austriak Franz Fuchs, który w latach 1993–1997 z pobudek ksenofobicznych jako członek Salzburger Eidgenossenschaft – Bajuwarische Befreiungsarmee (Konfederacja Salzburska – Bawarska Armia Wyzwoleńcza) rozsyłał listy-pułapki bombowe do polityków (m.in. burmistrza Wiednia Helmuta Zilka), polityków Partii Zielonych czy działaczy organizacji humanitarnych. Został aresztowany, osądzony i w 1999 r. skazany na karę dożywotniego wiezienia (26 lutego 2000 r. popełnił samobójstwo).

W XXI w. samotne wilki atakują głównie przypadkowe ofiary, choć robią to, jak mówią, w imię jakiejś idei. Najbardziej spektakularnego, tragicznego w skutkach zamachu dokonał 22 lipca 2011 r. Norweg Anders Behring Breivik[12], wyznający skrajnie prawicowe poglądy. Napisał i w dniu zamachu opublikował w sieci manifest *2083 – A European Declaration of Independence* (2083 – Europejska Deklaracja Niepodległości), będący kompilacją tekstów rasistowskich, ksenofobicznych, antyfeministycznych, islamofobicznych, ale i wprost zaczerpniętych z manifestu Theodore'a Kaczynskiego. Breivik najpierw dokonał zamachu bombowego w Oslo na siedzibę premiera (zginęło 8 osób), a następnie przeniósł się na wyspę Utøya, na której z broni palnej zmasakrował uczestników obozu młodzieżówki norweskiej Partii Pracy. Zginęło 69 osób. Aresztowany, pomimo wielu wątpliwości co do jego stanu umysłowego, Breivik uznany został za poczytalnego i skazany na najwyższy możliwy wymiar kary, czyli 21 lat więzienia (z możliwością nieograniczonego jego przedłużania).

[11] Swoje poglądy przedstawił w manifeście *Industrial Society and Its Future*, opublikowanym po raz pierwszy 19 IX 1995 r. przez dzienniki „The New York Times" i „The Washington Post".

[12] W czerwcu 2017 r. zmienił nazwisko na Fjotolf Hansen.

W zasadzie można by potraktować ten przypadek jak jeden z wielu ataków dokonanych przez osoby zaburzone psychicznie (u Breivika zdiagnozowano m.in. zaburzenia urojeniowe oraz narcystyczne zaburzenia osobowości – uważał się za regenta Norwegii). Do takich należało choćby ostrzelanie 1 października 2017 r. przez Stephena Paddocka uczestników koncertu muzyki country odbywającego się pod kasynem Luxor Las Vegas – zginęło wówczas 60, a rany odniosło 411 osób. W kinie Century 16 Theater w miejscowości Aurora w stanie Kolorado podczas premiery filmu *Mroczny rycerz powstaje* James Holmes 20 lipca 2012 r. zranił z broni palnej 58 osób. Te ataki nie były jednak zamachami terrorystycznymi. To zaś, że Breivik, jak sam przyznał, dokonał zamachów z pobudek politycznych, oraz jego zachowanie podczas procesu (wykonywanie gestu faszystowskiego pozdrowienia) pozwala zakwalifikować czyn jako terrorystyczny.

Wątpliwości takich nie budzą zamachy przeprowadzone przez wyznawców islamu, którzy, choć niezwiązani z żadnym z ugrupowań dżihadystycznych, swoje indywidualne akcje przeprowadzali, akcentując podczas nich swoje wyznanie wiary (*Allah akbar*).

Na przykład Wielka Brytania stała się w 2017 r. miejscem dwóch zamachów przeprowadzonych przez fanatycznych wyznawców islamu, z których jeden może być przypisany samotnemu wilkowi. Pięćdziesięciodwuletni obywatel brytyjski Khalid Masood[13] 22 marca wjechał prowadzonym przez siebie samochodem na chodnik Westminster Bridge i Bridge Street, ranił ponad 50 osób (w tym 4 śmiertelnie), a następnie rozbił pojazd na ogrodzeniu pałacu Westminster. Wysiadł, przedostał się na dziedziniec Parlamentu, gdzie śmiertelnie ranił policjanta. Chwilę potem został zastrzelony.

Broń chemiczna w rękach terrorystów

Członkowie japońskiej sekty buddyjskiej Aum shinri-Kyō (Najwyższa Prawda) 20 marca 1995 r. dokonali przy użyciu sarinu, gazu bojowego, zamachu terrorystycznego w tokijskim metrze. W jego wyniku zginęło 13 osób, skutki zatrucia gazem odczuło około 6 tys. (wiele z tych osób do

[13] T. Batchelor, *Khalid Masood. London attacker has no links to Isis or al-Qaeda, says Met Police*, „Independent", 17 III 2017, https://www.independent.co.uk/news/uk/home-news/khalid-masood-london-attack-isis-al-qaeda-no-links-police-a7652696.html [dostęp: 27 XII 2021].

dziś choruje, a nawet jest nadal hospitalizowanych). Był to najbardziej znany, najbardziej tragiczny w skutkach zamach terrorystyczny dokonany przy użyciu broni chemicznej i nierzadko przedstawiany jako pierwszy w historii, a później, z perspektywy czasu, jako jedyny taki zamach. Choć medialnie taka informacja była (i jest nadal) bardzo atrakcyjna i nośna, to nie jest ona zgodna z prawdą. Aum pierwszą próbę zastosowania sarinu przeprowadziła dziewięć miesięcy wcześniej, 27 czerwca 1994 r. w dzielnicy Kita-Fukashi miasta Matsumoto w prefekturze Nagano. Rozpylony tam gaz spowodował śmierć siedmiu i poważne zatrucie ponad 200 mieszkańców miasta[14]. Amerykańskie źródła podają, powołując się przy tym na zeznania członków Aum sądzonych w procesach po zamachu w 1995 r., że sekta pomiędzy rokiem 1990 a 1995 przeprowadziła 17 zamachów lub ich prób przy użyciu broni chemicznej i biologicznej: czterokrotnie sarinu, również cztery razy gazu VX (silnie trującego fosforo- i siarkoorganicznego związku chemicznego typu fosfonianu) oraz fosgenu i cyjanku sodu, a ponadto czterech bakterii wąglika i trzech toksyny botulinowej (jadu kiełbasianego)[15]. Współcześnie po broń chemiczną sięgają grupy fundamentalistów islamskich.

Już w 2004 r. amerykańskie służby specjalne alarmowały o możliwości dokonania na terytorium Stanów Zjednoczonych zamachu, do którego terroryści mogą użyć broni chemicznej, wskazywali nawet konkretnie na chlor, o wiele łatwiej dostępny niż inne trujące gazy (choćby użyty przez Aum sarin), a mogący przynieść porównywalne jak one skutki[16]. Związane to było z pożarem zbiorników z chlorem w Atlancie (25 maja 2004 r.), które spowodowało skażenie przez toksyczną chmurę 5 mil^2 (13 km^2) przedmieść miasta Conyers i konieczność ewakuacji około 10 tys. mieszkańców. Hospitalizowanych było 9 osób z objawami zatrucia gazem[17]. Eksperci zwracali przy tym uwagę, że wprawdzie

[14] Informacje na ten temat zob. m.in.: D.E. Kaplan, A. Marshall, *The Cult at the End of the World*, New York 1996, s. 137–146; D.W. Brackett, *Holy terror. Armageddon in Tokyo*, New York 1996, s. 27–43.

[15] *Al Qaeda and the Threat of Chemical and Biological Weapons*, Stratfor Global Intelligence, 4 XII 2004 r., https://www.stratfor.com/analysis/al-qaeda-and-threat-chrmical-and-biological-weapons [dostęp: 20 III 2015].

[16] *Chlorine as a Weapon?*, Stratfor Global Intelligence, 28 V 2004 r., https://www.stratfor.com/analysis/chlorine-weapon [dostęp: 16 III 2015].

[17] *Chlorine-tinged cloud of smoke forces evacuations east of Atlanta*", Associated Press, 25 V 2004 r., https://www.accessnorthga.com/detail.php?n=168143 [dostęp: 22 III 2015].

ze względu na jego powszechne stosowanie do oczyszczania wody łatwo chlor zdobyć (choćby np. dokonując napadu na transportujące go cysterny samochodowe czy kolejowe), to jednak jest on równie groźny dla zaatakowanych, jak i tych, którzy chcą się nim posłużyć jako bronią. Amerykańscy analitycy nie brali pod uwagę, że dla zamachowca samobójcy nie stanowiłoby to przeszkody.

Autorzy przytaczanej analizy zwracają uwagę na potencjalne zagrożenie, ale przyznają, że Al-Kaida preferuje wykorzystywanie klasycznych ładunków wybuchowych, jak np. w Madrycie, ze względu na ich większą skuteczność niż broń chemiczna (w Madrycie zginęły 193 osoby, w Tokio – 13). Są one ponadto tańsze w produkcji: koszt skonstruowania ładunków zdetonowanych w Madrycie szacowno na 10 tys. dolarów wobec milionów dolarów zaangażowanych przez Aum w jej program CBW[18]. I z tego też powodu prawdopodobieństwo użycia broni chemicznej przez terrorystów, podobnie jak i innych rodzajów broni masowego zniszczenia (zagłady), np. broni atomowej, jest raczej teoretyczne, a nie realne.

W opublikowanej w 2010 r. pracy Rolfa Mowatt-Larssena *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality? A Timeline of Terrorists' Efforts to Acquire WMD*[19] znaleźć można informacje o przygotowaniach Al-Kaidy do produkcji broni masowego zniszczenia, głównie atomowej, ale również chemicznej i biologicznej. Już przed zamachami 11 września 2001 r. Midhat al-Mursi (pseud. Abu Khabab) organizował w Afganistanie szkolenia członków organizacji w użyciu takiej broni, na przełomie lat 2002 i 2003 zaś Abu Musab al-Zarkawi, zastępca Bin Ladena, planował dokonanie w Europie zamachów przy użyciu rycyny i cyjanku. Grupa działająca w Bahrajnie przygotowywała w tym samym czasie specjalne urządzenie (arab. *mobtaker*, wynalazek), za pomocą którego chciała rozpylić w nowojorskim metrze cyjanowodór.

Rok 2007 przyniósł serię zamachów w Iraku, w których użyto bomb wypełnionych chlorem. W trzech atakach 16 marca (dwóch w okolicach Faludży oraz w pobliżu Ar-Ramadi) zginęło 8 osób (w tym 6 żołnierzy

[18] *Al Qaeda and the Threat of Chemical and Biological Weapons*, Stratfor Global Intelligence, 4 XII 2004 r., https://www.stratfor.com/analysis/al-qaeda-and-threat-chemical-and-biological-weapons [dostęp: 20 III 2015].

[19] R. Mowatt-Larssen, *Al Qaeda Weapons of Mass Destruction Threat. Hype or Reality? A Timeline of Terrorists' Efforts to Acquire WMD*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2010, http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf [dostęp: 22 III 2015].

amerykańskich), a kilkaset zostało rannych[20]. Ponownie w pobliżu Ar-Ramadi 6 kwietnia zdetonowanie wyładowanej trotylem i zbiornikami z chlorem ciężarówki spowodowało śmierć 27 osób (był to już dziewiąty tego typu zamach w pobliżu Ar-Ramadi)[21]. Wypełniony pojemnikami z chlorem samochód 3 czerwca wysadzony został w powietrze w odległości 200 metrów od wjazdu na teren amerykańskiej bazy w Bakubie (stolicy prowincji Dijala), powodując zatrucie gazem ponad 60 żołnierzy.

Interesujące jest to, że jeszcze PRZED tą serią zamachów analitycy Stratfor zadawali pytanie: *Chemical Strikes – the Beginning of a Trend?*[22]. W irackim Ar-Ramadi bowiem 30 stycznia eksplodowała ciężarówka wyładowana pojemnikami z chlorem, a 20 lutego w położonym na północ od Bagdadu Al-Tadżi doszło do podobnego ataku. Zdarzenia te nie zostały odnotowane przez media, ponieważ nie pociągnęły za sobą żadnych ofiar, ale pozwoliły autorom sformułować kilka ogólnych wniosków dotyczących potencjalnego wykorzystywania chloru w zamachach terrorystycznych. Końcowy był w sumie optymistyczny: choć faktycznie chlor może znaleźć zastosowanie przy produkcji bomb, to jednak ze względu na małą skuteczność jako środek śmiercionośny i „niesterowalność" powstałą w wyniku jego rozpylenia trującą chmurą nie będzie stanowił realnego zagrożenia.

A jednak po kilku latach po chlor sięgnęła kolejna organizacja terrorystyczna: Państwo Islamskie. ISIS wykorzystało prawdopodobnie ładunki z chlorem 15 września 2014 r. w położonej na północ od Bagdadu miejscowości Duluja, walczący zaś z nim na terytorium Iraku i Syrii Kurdowie oskarżają je o co najmniej dwukrotne użycie bomb z chlorem przeciwko peszmergom (bojownikom kurdyjskim): 23 stycznia i 14 marca 2015 r. Gen. Aziz Waisi, komendant oddziałów żandarmerii wojskowej Zervani, w udzielonym 16 marca 2015 r. wywiadzie uzupełnił te informacje o jeszcze jedną, mówiąc o użyciu przez ISIS chloru w walkach

[20] *Iraq. Chlorine Attacks Kill 8, Injure Hundreds*, Stratfor Global Intelligence, 16 III 2007 r., https://www.stratfor.com/situation-report/iraq-chlorine-attacks-kill-8-injure-hundreds [dostęp: 16 III 2015].

[21] *Iraq. Chlorine Truck Bomb Kills 27*, Stratfor Global Intelligence, 6 IV 2007 r., https://www.stratfor.com/situation-report/iraq-chlorine-truck-bomb-kills-27 [dostęp: 16 III 2015].

[22] *Geopolitical Diary: Chemical Strikes – the Beginning of a Trend?*, Stratfor Global Intelligence, 21 II 2007 r., https://www.stratfor.com/geopolitical-diary/geopolitical-diary-chemical-stikes-begining-of-a-trend [dostęp: 20 III 2015].

w górskim regionie Sindżar[23]. Być może to w konsekwencji styczniowego wydarzenia 24 stycznia Amerykanie zaatakowali przy użyciu dronów konwój samochodów jadący szosą w pobliżu Mosulu i zabili Abu Malika, głównego konstruktora bomb chemicznych dla ISIS.

Terroryzm XXI wieku – nowa era?

Trzymając się definicji terroryzmu jako zmiennej w miejscu i czasie metody walki służącej osiągnięciu celów politycznych, należy odpowiedzieć na pytanie: czy dziś mamy do czynienia z kolejną jego generacją (falą)? Odpowiedzi jednoznacznej nie można jednak udzielić, bo gra polityczna, w której wykorzystywany jest terroryzm, nie jest zero-jedynkowa. Jeśli bowiem terroryzm miałby być nadal uważany za metodę stosowaną wyłącznie przez jednostki (grupy) antypaństwowe, to oczywiście nie mamy do czynienia z jakimś nowym zjawiskiem. Jeśli jednak przychylimy się do twierdzenia, że terroryzm może być stosowany również przez instytucje państwa, to należałoby zweryfikować dotychczasowe podejście formalnoprawne i uznać, że mamy do czynienia, podobnie jak z wojną, z kolejną jego generacją (falą).

W większości dotychczasowych prób definiowania terroryzmu podkreślano, że warunkiem sine qua non uznania jakiegoś działania za terrorystyczne (a przynajmniej za zagrożenie) jest użycie przemocy fizycznej, a począwszy od 1937 r. (konwencji genewskiej), że ma ono charakter antypaństwowy[24]. Takie wynikające z politycznej kalkulacji regulacje prawne pozwalały rządzącym na legitymizację zwalczania nie tylko rzeczywistego zagrożenia przestępczością terrorystyczną o podłożu politycznym, ale po prostu zwalczania opozycji. Jakiekolwiek próby innego umiejscowienia terroryzmu w systemie prawnym skazane były na niepowodzenie,

[23] *Update 3-Kurds report more chlorine attacks, Iraq pauses Tikrit offensive*, Reuters, 16 III 2015 r., http://www.reuters,com/article/2015/03/16/mideast-crisis-iraq-idUSL6N0WI1OA20150316 [dostęp: 20 III 2015].

[24] Artykuł 2 *Konwencji o Zapobieganiu i Przeciwdziałaniu Terroryzmowi* z 16 XI 1937 r. za „akt terroryzmu" uznawał „akt kryminalny wymierzony w państwo z intencją lub nadzieją na wytworzenie stanu strachu w umysłach pojedynczych osób, grup osób lub całego społeczeństwa". Cyt. za: *Convention for the Prevention and Punishment of Terrorism. Opened for Signature AT Geneva, November 16, 1937*, w: *Control of Terrorism: International Documents*, Y. Alexander, M.B. Browne, A.S. Nanes (red.), przedm. R.S. Cline, New York 1979, s. 20–21.

a czasami wręcz na oskarżenia osób proponujących takie rozwiązania o popieranie terroryzmu. Dopiero w ostatnich latach pojawiło się nowe spojrzenie na problematykę terroryzmu, w którym dostrzeżono nie tylko jego antypaństwowy charakter. W wydanej w 2012 r. *Encyclopedia of Applied Ethics*[25] w haśle „Terrorism" jej autorzy piszą m.in.:

> Terrorism is defined as a destructive method of political action which uses violence to cause fear for political ends. While some political goals may be achieved only through the use of terrorism, terrorists often kill or injure noncombatants or the innocent in order to maximize terror and to seek widespread publicity for their actions. Contemporary terrorism is often conceived in terms of war. While terrorism may be perpetrated by individuals against a state, states can enact policies of terrorism against their own citizens or subjects of another nation or country[26].

W drugiej połowie XX w. kraje Europy Zachodniej mierzyły się z terroryzmem separatystycznym (Wielka Brytania – Irlandzkiej Armii Republikańskiej, IRA, Hiszpania – Kraju Basków i Wolności, ETA) oraz o podłożu ideologicznym (lewicowym i prawicowym). Na lata 70. i 80. przypada apogeum działalności takich ugrupowań, jak: Frakcja Czerwonej Armii czy Wehrsportgruppe Hoffmann w RFN, Czerwone Brygady czy Ordine Nero (Czarny Porządek) we Włoszech i wielu innych. Nie było w tamtych latach państwa z kręgu cywilizacji zachodniej, którego bezpieczeństwo nie byłoby zagrożone terroryzmem. Po zamachach z 11 września 2001 r. społeczeństwa państw Zachodu zostały zastraszone przez terroryzm islamskich fundamentalistów. Ale nie dlatego, że wtedy ten się narodził (na Bliskim Wschodzie organizacje islamskie, m.in. Bractwo Muzułmańskie, Hamas, Hezbollah, odwołujące się do dżihadu

[25] *Encyclopedia of Applied Ethics. Second Edition*, R. Chadwick, D. Callahan, P. Singer (red.), Oxford 2012.

[26] „Terroryzm jest definiowany jako destrukcyjna metoda działania politycznego, która wykorzystuje przemoc do wywoływania strachu dla [osiągnięcia] celu politycznego. Podczas gdy niektóre cele polityczne można osiągnąć tylko za pomocą terroryzmu, terroryści często zabijają lub ranią osoby niebiorące udziału w walce lub niewinne w celu maksymalizacji terroru i uzyskania szerokiego rozgłosu swoich działań. Współczesny terroryzm jest często pojmowany w kategoriach wojny. Podczas gdy terroryzm może być popełniany przez jednostki przeciwko państwu, państwa mogą wprowadzać politykę terroryzmu przeciwko własnym obywatelom lub poddanym innego narodu lub kraju" (tłum. aut.).

istniały i działały od dziesięcioleci), ale dlatego, że niejako zapukał bezpośrednio do ich drzwi. Do tamtego czasu Europejczycy i Amerykanie dowiadywali się co najwyżej z mediów o zamachach przeprowadzanych np. w Bejrucie na ambasadę Stanów Zjednoczonych (18 kwietnia 1983 r. – zginęły 63 osoby), koszary wojsk amerykańskich i francuskich (23 października 1983 r. – zginęło 241 żołnierzy amerykańskich i 58 francuskich, w sumie śmierć poniosło 299 osób) czy innych, jeśli zamachy dotyczyły obywateli ich krajów. Zamachy na wszystkich pozostałych były co najwyżej odnotowywane, a czasami zupełnie pomijane w serwisach informacyjnych. Jednak 11 września 2001 r. przekonali się, że zamachy terrorystyczne ze strony islamskich fundamentalistów zagrażają im bezpośrednio, i kolejne lata dobitnie to udokumentowały. Od tego też dnia i wypowiedzenia przez prezydenta Stanów Zjednoczonych George'a W. Busha wojny terroryzmowi wszystkie zamachy terrorystyczne, niezależnie od tego, w którym zakątku świata były dokonywane, przypisywano Al-Kaidzie. A z Al-Kaidą powiązane miały być inne organizacje fundamentalistów islamskich (szacunkowe dane mówiły nawet o kilkudziesięciu ugrupowaniach[27]) działające w kilkudziesięciu państwach[28].

[27] Według Departamentu Stanu USA przed atakiem 11 IX 2001 r. ugrupowaniami współpracującymi z Bazą były: Komitet Doradczy ds. Reform (Sudan/Afganistan), Asbat al-Ansar (Liban), Ansar al-Islam/Bojownicy Islamu (iracki Kurdystan), Harakat ul-Ansar/Mudżahedin (Pakistan), Al-Badar (Pakistan), Zbrojna Grupa Islamska/GIA (Algieria), Grupa Saafi na rzecz Prozelityzmu i Walki/GPSD (Algieria), Talaa'l al-Fateh (Egipt), Groupe Roubaix (Francja), Harakat ul Jihad (Pakistan), Jaish Mohammed (Pakistan), Jamiat Ulema-e-Pakistan (Pakistan), Jamiat Ulema-e-Islam (Pakistan), Hezbollah (Liban), Hezb ul-Mujahideen/Partia Świętych Wojowników (Pakistan), Al-Gama'a al-Islamiyya (Egipt), al-Hadith (Pakistan), Hamas (Autonomia Palestyńska), Bayt al-Imam (Jordania), Islamska Święta Wojna (Autonomia Palestyńska), Islamski Ruch Uzbekistanu (Uzbekistan), al-Jihad (Bangladesz), al-Jihad (Egipt), grupa al-Jihad (Jemen), Laskar e-Toiba (Pakistan), Libańska Liga Partyzancka (Liban), Libijska Grupa Islamska (Libia), Islamski Front Wyzwolenia Moro (Filipiny), Ruch Partyzancki (Kaszmir), Abu Sajjaf (Filipiny), Al-Ittihad al-Islamiya/Jedność Islamu (Somalia), Dżemaja Islamija (Indonezja), Związek Ulemów Afganistanu (Afganistan) – dane za: Y. Alexander, M.S. Swetnam, *Siewcy śmierci. Osama bin Laden i inni szefowie al-Qaidy*, tłum. J. Kozłowski, Warszawa 2001, s. 49 i źródła własne.

[28] Bliski Wschód – Egipt, Irak, Iran, Izrael, Jordania, Kuwejt, Liban, Maroko, Autonomia Palestyńska, Arabia Saudyjska, Sudan, Syria, Tunezja, Turcja, Zjednoczone Emiraty Arabskie, Jemen; Azja – Afganistan, Bangladesz, Chiny, Indie (Kaszmir), Indonezja, Malezja, Myanmar, Pakistan, Filipiny; Europa – Albania, Belgia, Bośnia i Hercegowina, Chorwacja, Dania, Francja, Niemcy, Włochy, b. Jugosławia (Kosowo), Luksemburg, Holandia, Hiszpania, Szwecja, Szwajcaria, Wielka Brytania; Wspólnota Niepodległych Państw (b. ZSRR) – Azerbejdżan, Federacja Rosyjska, Czeczenia,

Kamieniami milowymi w historii zamachów w Europie w XXI w. i przypisywanych Al-Kaidzie stały się zamachy z 11 kwietnia 2004 r. w Madrycie, w których zginęły 193 osoby, a ponad 2 tys. zostało rannych, oraz wymierzone w system transportu publicznego skoordynowane zamachy samobójcze w Londynie z 7 lipca 2005 r., w których zginęły 52 osoby, a ponad 700 zostało rannych. Potem co prawda nastąpiło kilka lat przerwy w atakowaniu przez islamskich terrorystów Europy, ale wraz ze wzrostem w siłę Państwa Islamskiego przyszła ich kolejna fala. To wówczas doszło we Francji do zamachu 7 stycznia 2015 r. na redakcję satyrycznego czasopisma „Charlie Hebdo" (jako odwet za zamieszczenie karykatur Mahometa, zginęło 12 osób) oraz zamachów 13 listopada tego roku w Paryżu, które spowodowały śmierć 130 osób i obrażenia ponad 350 (pod względem jednorazowej liczby ofiar największego zdarzenia we Francji od czasów II wojny światowej)[29]. W 2016 r. Europejczykami wstrząsnęły kolejne zamachy: 22 marca 2016 r. w Belgii – dwa w porcie lotniczym Bruksela w Zaventem i jeden przy stacji metra Maelbeek/Maalbeek w Brukseli (bomby zabiły 35 i zraniły 316 osób), 14 lipca zaś w Nicei. Tam Mohamed Lahouaiej-Bouhlel wjechał w tłum spacerujący po Promenadzie Anglików, zabijając 86 i raniąc 458 osób. Później zamachów na mniejszą skalę było wiele, choć od początku 2020 r. ich liczba spadła. Nie stało się tak w wyniku działań kontrterrorystycznych, ale pandemii koronawirusa COVID-19, która sprawiła potencjalnym terrorystom problemy choćby logistyczne. Czy to oznacza, że zagrożenie zamachami terrorystycznymi zmalało? (bo o całkowitym zniknięciu nie może być mowy). Z perspektywy europejskiej może taką tezę dałoby się postawić, ale już dla innych regionów świata wydaje się ona fałszywa. Co prawda dostępne źródła nie uwzględniają jeszcze zbiorczych danych z lat 2020–2021, ale śledząc doniesienia agencji informacyjnych, nie obserwuje się jakichś radykalnych spadków liczby zamachów. W przeszłości zdarzały się takie lata, że liczba ta spadała o 50 proc. w stosunku do lat wcześniejszych (np. wg Statista w 2012 r. dokonano 6771 zamachów,

Tadżykistan, Uzbekistan; Afryka – Algieria, Komory, Dżibuti, Erytrea, Etiopia, Kenia, Libia, Mauretania, Nigeria, Senegal, Somalia, Republika Południowej Afryki, Sudan, Tanzania, Uganda, Zair; Ameryka Północna i Południowa – Kanada, Stany Zjednoczone Ameryki, Argentyna, Brazylia, Paragwaj, Urugwaj – w sumie 67 (!) państw – dane za: Y. Alexander, M.S. Swetnam, *Siewcy śmierci…*, s. 50.

[29] Opis zamachów zob. np. https://www.britannica.com/event/Paris-attacks-of-2015 [dostęp: 20 III 2015].

a w 2006 r. – 14 371), co i tak nie napawa optymizmem. Można też zaobserwować terytorialne czasowe przesunięcia częstotliwości dokonywania zamachów, ale w XXI w. nadal najbardziej zagrożonymi obszarami są Bliski Wschód, Afryka Północna, Sahel, subkontynent indyjski.

W opublikowanym we wrześniu 2018 r. przez Departament Stanu dorocznym raporcie o terroryzmie (*Country Reports on Terrorism 2017*[30]) można znaleźć taką informację:

> Pomimo naszych sukcesów terrorystyczny krajobraz stał się w 2017 r. bardziej złożony. ISIS, Al-Kaida i ich partnerzy okazali się odporni, zdeterminowani i zdolni do przystosowania się, a także dostosowali się do zwiększonej presji antyterrorystycznej w Iraku, Syrii, Afganistanie, Libii, Somalii, Jemenie i wszędzie indziej. [Organizacje terrorystyczne] stały się bardziej rozproszone i tajne, zaczęły korzystać z Internetu, by zainspirować ataki swoich wyznawców na odległość, i w rezultacie stały się mniej podatne na konwencjonalne działania wojskowe. Co więcej, powrót lub przybycie nowych bojowników biorących udział w walkach za granicą przyczyniły się do wzrostu liczby doświadczonych, rozwiniętych i połączonych sieci terrorystycznych, które mogą planować i przeprowadzać ataki[31].

Kilka miesięcy później, zupełnie nie biorąc pod uwagę ostrzeżeń ekspertów, na potwierdzenie sukcesów w wojnie z terroryzmem i pokonaniu ISIS prezydent Stanów Zjednoczonych Donald Trump zapowiedział wycofanie wojsk amerykańskich z Syrii i Iraku[32], co rzecz jasna spotkało się z falą krytyki i poskutkowało symboliczną rezygnacją generała Jamesa Mattisa ze stanowiska sekretarza obrony. Analitycy Departamentu Stanu w cytowanym raporcie przestrzegali, że ISIS mimo utraty terytorium nie zaniechało działalności. Sięgnęło przy tym po nowe metody polegające na wykorzystywaniu swoich sympatyków rozsianych po całym świecie i stosowaniu niekonwencjonalnych technik przeprowadzania zamachów.

---

[30] *Country Report on Terrorism 2017*, United States Department of State Publication, Bureau of Counterterrorism, Washington 2018.

[31] Tamże, s. 8.

[32] Plany te potwierdził już w 2021 r. prezydent Joe Biden.

> Grupa zachęcała sympatyków, żeby użyli wszelkiej dostępnej broni – np. dużych pojazdów – przeciwko miękkim celom i przestrzeni publicznej. Coraz częściej odpowiedzialność za podejmowanie decyzji, gdzie, kiedy i jak dokonać zamachu, rozpraszała się na rodzimych terrorystów zainspirowanych lub wydelegowanych przez ISIS do prowadzenia operacji daleko od strefy działań wojennych. W 2017 r. obserwowaliśmy takie ataki w Manchesterze w Wielkiej Brytanii; w Barcelonie w Hiszpanii; na Synaju w Egipcie; w Marawi na Filipinach; w Nowym Jorku i w wielu innych miejscach[33].

Podobnie zagrożenia ze strony ISIS zdefiniowano w kolejnym raporcie Departamentu Stanu:

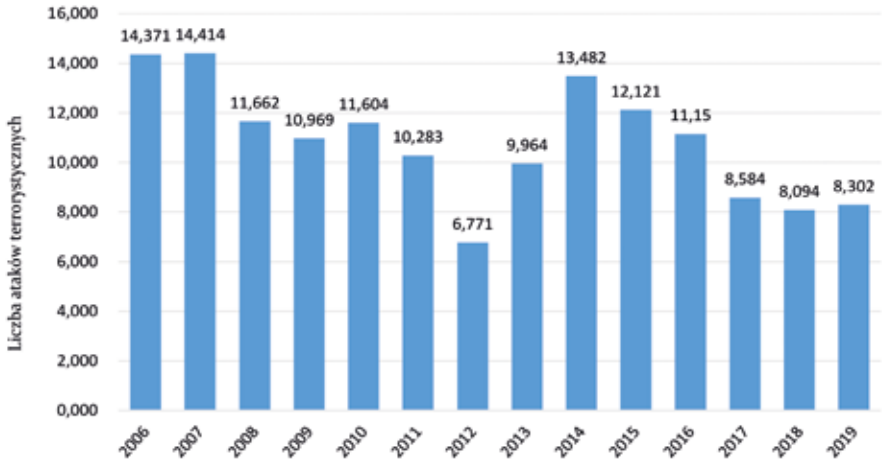
> W 2019 r. Europa nadal borykała się z wieloma zagrożeniami i niepokojami terrorystycznymi (...). Pomimo całkowitej utraty terytorium geograficznego ISIS nadal działało, podżegając do ataków na symboliczne cele europejskie i przestrzeń publiczną oraz rekrutując osoby z krajów europejskich. Większość tych incydentów miała miejsce w Europie Zachodniej i Rosji i polegała na prostych akcjach przeprowadzonych łatwymi do wykonania metodami z użyciem do zranienia lub zabicia pieszych powszechnie dostępnych narzędzi i pojazdów[34].

I nic nie wskazuje na to, by zagrożenie zamachami terrorystycznymi ze strony środowisk dżihadystycznych miało w trzeciej dekadzie XXI w. zmaleć.

[33] Tamże.

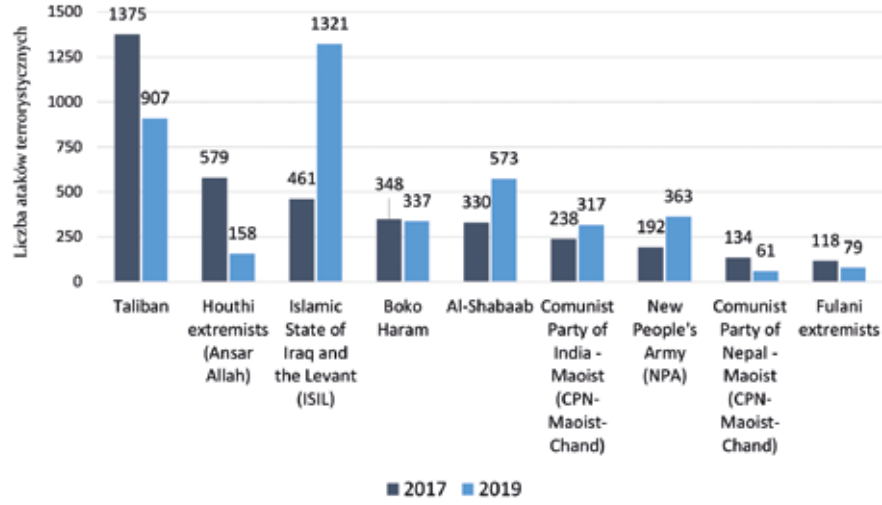
[34] *Country Reports on Terrorism 2019*, United States Department of State Publication, Bureau of Counterterrorism, Washington 2019, s. 60.

Postscriptum (statystyki)



Wykres 1. Liczba zamachów terrorystycznych na świecie (lata 2006–2019).

Źródło: https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/.



Wykres 2. Najbardziej aktywne grupy przeprowadzające zamachy na świecie w 2019 r. według liczby zamachów.

Źródło: https://statista.com/statistics/937553/terrorism-most-active-perpetrator-groups--worldwide/.

Bibliografia

Alexander Y., Swetnam M.S., *Siewcy śmierci. Osama bin Laden i inni szefowie al-Qaidy*, tłum. J. Kozłowski, Warszawa 2001.

Brackett D.W., *Holy terror. Armageddon in Tokyo*, New York 1996.

Country Report on Terrorism, United States Department of State Publication, Bureau of Counterterrorism, Washington, 2005–2019.

Encyclopedia of Applied Ethics. Second Edition, R. Chadwick, D. Callahan, P. Singer (red.), Oxford 2012.

Convention for the Prevention and Punishment of Terrorism. Opened for Signature AT Geneva, November 16, 1937, w: *Control of Terrorism. International Documents*, Y. Alexander, M.B. Browne, A.S. Nanes (red.), przedm. R.S. Cline, New York 1979.

Fukuyama F., *Koniec historii*, tłum. T. Bieroń, M. Wichrowski, Poznań 1996.

Hassan R., *What Motivates the Suicide Bombers? Study of a comprehensive database gives a surprising answer*, „YaleGlobal", 3 VIII 2009 r.

Kaplan D.E., Marshall A., *The Cult at the End of the World*, New York 1996.

Karolczak K., *Terroryzm. Nowy paradygmat wojny w XXI wieku*, Warszawa 2010.

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

Laqueur W., *Terrorism*, London 1980.

Laqueur W., *The New Terrorism. Fanaticism and the Arms of Mass Destruction*, London 2001.

Patterns of Global Terrorism, United States Department of State Publication, Bureau of Counterterrorism, Washington, 2001–2004.

Victor B., *Army of Roses. Inside the World of Palestinian Women Suicide Bombers*, London 2004.

Źródła internetowe

Al Qaeda and the Threat of Chemical and Biological Weapons, Stratfor Global Intelligence, 4 XII 2004 r., https://www.stratfor.com/analysis/al-qaeda-and-threat--chrmical-and-biological-weapons [dostęp: 20 III 2015].

Chlorine as a Weapon?, Stratfor. Global Intelligence, 28 V 2004 r., https://www.stratfor.com/analysis/chlorine-weapon [dostęp:16 III 2015].

Chlorine-tinged cloud of smoke forces evacuations east of Atlanta, Associated Press, 25 V 2004 r., https://www.accessnorthga.com/detail.php?n=168143 [dostęp: 22 III 2015].

Geopolitical Diary. Chemical Strikes – the Beginning of a Trend?, Stratfor Global Intelligence, 21 II 2007 r., https://www.stratfor.com/geopolitical-diary/geopolitical-diary-chemical-stikes-begining-of-a-trend [dostęp: 20 III 2015].

Iraq: Chlorine Attacks Kill 8, Injure Hundreds, Stratfor Global Intelligence, 16 III 2007 r., https://www.aljazeera.com/ [dostęp: 16 III 2015].

https://www.bbc.com/news/world.

https://edition.cnn.com/.

https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/terro--rism.

https://www.reuters.com/.

https://www.stratfor.com/situation-report/iraq-chlorine-attacks-kill-8-injure-hundreds [dostęp: 16 III 2015].

Iraq. Chlorine Truck Bomb Kills 27, Stratfor Global Intelligence, 6 IV 2007 r., https://www.stratfor.com/situation-report/iraq-chlorine-truck-bomb-kills-27 [dostęp: 16 III 2015].

Kiras J., hasło „*suicide bombing*", w: *Encyclopedia Britannica*, 13 XI 2019 r., https://www.britannica.com/topic/suicide-bombing [dostęp: 28 XI 2021].

Mowatt-Larssen R., *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality? A Timeline of Terrorists' Efforts to Acquire WMD*, Cambridge 2010, http://belfer-center.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf [dostęp: 22 III 2015].

Update 3-Kurds report more chlorine attacks, Iraq pauses Tikrit offensive, Reuters, 16 III 2015 r., http://www.reuters,com/article/2015/03/16/mideast-crisis-iraq-idU SL6N0WI1OA20150316 [dostęp: 20 III 2015].

DOI: 10.4467/27204383TER.22.002.15418

ORCID: 0000-0002-6685-8769

PIOTR BURCZANIUK

Prawne aspekty walki z terroryzmem w krajowym porządku prawnym na tle wyzwań kształtowanych prawodawstwem europejskim

Abstrakt

W artykule podjęto temat prawnych aspektów walki z terroryzmem w krajowym porządku prawnym na tle wyzwań kształtowanych prawodawstwem europejskim. Analizowane zagadnienie jest ciekawe z uwagi na brak szerszych i aktualnych analiz prowadzonych w obszarze nauk prawnych, poświęconych przedstawieniu i eksplikacji prawodawstwa obejmującego przedmiotowo problematykę walki z terroryzmem. Niniejsze opracowanie jest próbą wypełnienia tej luki badawczej.

W celu kompleksowego przybliżenia tematu i realizacji celów postawionych w artykule rozważania poprowadzono w sześciu zasadniczych częściach. We wstępie zakreślono tezę pracy oraz jej cele, następnie kolejno: dokonano analizy kształtowania regulacji prawnych prawa krajowego nakierowanych na przeciwdziałanie terroryzmowi; omówiono znaczenie ustawy o działaniach terrorystycznych w normatywnym systemie zwalczania terroryzmu w Polsce, z uwzględnieniem perspektywy i doświadczeń pięciolecia jej obowiązywania; zaprezentowano aktualny stan prawny Unii Europejskiej w obszarze terroryzmu; opisano perspektywy i wyzwania regulacyjne prawa polskiego na tle działań legislacyjnych organów UE; dokonano podsumowania prowadzonych rozważań, zakreślając perspektywy i wyzwania regulacyjne stojące przed prawodawcą krajowym na tle kierunków projektowanych rozwiązań legislacyjnych w Unii Europejskiej.

Słowa kluczowe:

polskie ustawodawstwo antyterrorystyczne, europejskie prawodawstwo antyterrorystyczne, ustawa o działaniach terrorystycznych, antyterroryzm, walka z terroryzmem

Wstęp

W doktrynie prawniczej jako wynik prowadzonych analiz rodzajów i zakresów rozwiązań prawnych przyjmowanych w wybranych państwach i nakierowanych celowościowo na zwalczanie zjawiska terroryzmu wskazuje się dwa główne ich modele, tj. tzw. ustawodawstwo antyterrorystyczne formalne i ustawodawstwo antyterrorystyczne materialne. Jak wskazuje P. Chomentowski, (...) *w pierwszym wypadku będziemy mówili o państwach, które w swoim porządku prawnym mają jeden lub kilka aktów rangi ustawowej, który bezpośrednio i wyłącznie dotyczy całości obszaru walki z terroryzmem. Drugi przypadek to cały system rozproszonych w różnych ustawach przepisów traktujących o trybie i środkach stosowanych do walki z terroryzmem*[1].

Przyjmując za punkt wyjścia ów dualistyczny podział regulacji antyterrorystycznych, należy wskazać, że podstawowym celem niniejszego artykułu jest próba syntetycznego opisu zakresu regulacji tworzących polski system antyterrorystyczny na tle zmian, które w nim zaszły w związku z przyjęciem *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (wspomnianą ustawą *de iure* zastąpiono model materialny modelem formalnym). Omówienie tych regulacji nie jest jednak możliwe bez odniesienia do prawodawstwa Unii Europejskiej, które, jak w rozporządzeniach UE, przez skutek bezpośredniego obowiązywania współtworzy system krajowy albo też, jak w dyrektywach, wyznacza kierunek krajowych działań legislacyjnych. Wreszcie, sięgnięcie do źródeł prawodawczych UE jest niezbędne do uchwycenia zachodzących lub projektowanych zmian w tych regulacjach, których zakres coraz częściej dotyka problematyki zagrożeń bezpieczeństwa państwa nazywanych „asymetrycznymi" lub „hybrydowymi". Omówieniu tych zagadnień poświęcone będą poszczególne części niniejszego opracowania.

Rys historyczny

Jak podkreśla M. Gołaszewska, (...) *w polskim systemie prawnym pojęcie „terroryzm" nie zostało legalnie zdefiniowane*. (...) *jest natomiast raczej terminem o charakterze naukowym, obrazującym stan zagrożenia społecznego*

[1] P. Chomentowski, *Polski system antyterrorystyczny. Prawno-organizacyjne kierunki ewolucji*, Warszawa 2014, s. 47.

wywołanego czynem o charakterze terrorystycznym[2]. Biorąc powyższe pod uwagę, należy wskazać, że problematyka terroryzmu w krajowym systemie prawnym została podjęta przez ustawodawcę stosunkowo późno, gdyż dopiero ustawą z 27 września 2002 r.[3], która z dniem 1 grudnia 2002 r. wprowadziła zmiany w *Ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł*[4], m.in. uzupełniając jej tytuł o zwrot „oraz o przeciwdziałaniu finansowaniu terroryzmu". Jak wskazywano w uzasadnieniu do projektu ustawy zmieniającej:

> (...) zaproponowana zmiana tytułu ustawy wiąże się z faktem objęcia przedmiotowym projektem problematyki przeciwdziałania finansowaniu terroryzmu. Wprowadzenie regulacji związanych z tą problematyką stanowi jeden z elementów służących realizacji postanowień rezolucji Rady Bezpieczeństwa ONZ nr 1373 (2001) w sprawie zwalczania terroryzmu międzynarodowego oraz zaleceń Grupy Zadaniowej ds. Zwalczania Prania Pieniędzy funkcjonującej pod auspicjami OECD (FATF). Zaproponowane rozwiązania odnoszą się wyłącznie do kwestii przekazywania przez Generalnego Inspektora instytucjom obowiązanym informacji o osobach, co do których zachodzi uzasadnione podejrzenie, że pomagają one lub uczestniczą w popełnieniu aktów terrorystycznych oraz stwarzają możliwość inicjowania procedury blokady środków finansowych znajdujących się na rachunku[5].

Ustawa ta wprowadziła więc pierwszą quasi-definicję „terroryzmu" do polskiego systemu prawnego, uznając za „akt terrorystyczny" przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne, przestępstwa przeciwko bezpieczeństwu powszechnemu oraz

---

[2] 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. 46–47.

[3] *Ustawa z dnia 27 września 2002 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł* (DzU z 2002 r. nr 180 poz. 1500).

[4] Tekst pierwotny został ogłoszony w DzU z 2000 r. nr 116 poz. 1216.

[5] *Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł*, http://orka.sejm.gov.pl/proc4.nsf/opisy/338.htm [dostęp: 22 XI 2021].

przestępstwa określone w art. 134 i 136 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny*[6], zwanej dalej kodeksem karnym. Definicja ta została ukształtowana przedmiotowo, odwołując się do określonych typów czynów zabronionych objętych kodeksem karnym, który, co istotne, nie definiował wówczas pojęcia przestępstwa o charakterze terrorystycznym.

W prawie karnym materialnym zmiany w tym zakresie zostały wprowadzone przez ustawodawcę dopiero w 2004 r., kiedy to na mocy ustawy z 16 kwietnia 2004 r.[7] uzupełniono od 1 maja 2004 r. kodeks karny o definicję przestępstwa o charakterze terrorystycznym, rozumianego jako czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: 1) poważnego zastraszenia wielu osób, 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu. Ponadto wprowadzono zmiany w brzmieniu art. 258 tego kodeksu, który penalizuje udział w zorganizowanej grupie przestępczej, rozszerzając go o grupę albo związek mające na celu popełnienie przestępstwa o charakterze terrorystycznym oraz różnicując odpowiedzialność w zależności od zaangażowania, tzn. zakładania, kierowania lub też udziału w takiej grupie. Jak wskazywano w uzasadnieniu do ustawy zmieniającej, miała ona na celu:

> (...) dostosowanie prawa polskiego do wymagań instrumentów prawnych Unii Europejskiej, przyjętych w latach 2001–2002, w ramach tzw. „nowego acquis". Decyzja ramowa z dnia 13 czerwca 2002 r. o zwalczaniu terroryzmu zobowiązuje państwa członkowskie do przyjęcia jednolitej definicji przestępstwa o charakterze terrorystycznym. Celem takiego działania nie jest tu li tylko osiągnięcie skutku teoretyczno-systemowego. Fakt, że dany typ przestępstw kwalifikowany jest jako przestępstwo o charakterze terrorystycznym, ma bowiem wpływ na zaostrzenie wymiaru kary za nie[8].

---

[6] Obecne brzmienie ustawy opublikowane w DzU z 2020 r. poz. 1444.

[7] *Ustawa z dnia 16 kwietnia 2004 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* (DzU z 2004 r. nr 93 poz. 889).

[8] *Uzasadnienie do rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*, http://orka.sejm.gov.pl/proc4.nsf/opisy/2407.htm [dostęp: 22 XI 2021].

Z uwagi na to, że państwa członkowskie były zobowiązane do implementowania rozwiązań prawnych przewidzianych w powołanej decyzji ramowej do końca 2002 r., przełożyło się to na konieczność ich przyjęcia przez Polskę wraz z przystąpieniem do Unii.

Jak wskazuje T. Batory, (...) *dokonując dekodowania przestępstw o charakterze terrorystycznym na podstawie zapisów Kodeksu karnego, mając na względzie typizację przestępstw w części szczególnej owego, należy wskazać, iż chodzi tu o następujące przestępstwa: Art. 118 (Eksterminacja), Art. 118a (Zamach przeciwko ludności), Art. 119 (Przemoc i groźba bezprawna), Art. 120 (Środki masowej zagłady), Art. 127 i 128 (Zamach stanu), Art. 134 (Zamach na życie Prezydenta), Art. 140 (Zamach terrorystyczny), Art. 148 (Zabójstwo), Art. 163 (Spowodowanie niebezpiecznych zdarzeń), Art. 164 (Bezpośrednie niebezpieczeństwo), Art. 165 (Inne niebezpieczeństwa), Art. 165a (Sfinansowanie przestępstwa o charakterze terrorystycznym), Art. 166 (Piractwo), Art. 167 (Niebezpieczne urządzenia lub substancje), Art. 170 (Rozbójnictwo morskie), Art. 173 (Katastrofa), Art. 174 (Niebezpieczeństwo katastrofy), Art. 252 (Wzięcie zakładnika), Art. 255a (Rozpowszechnianie treści mogących ułatwić popełnienie przestępstwa), Art. 258 § 2 i § 4 (Zorganizowana grupa i związek przestępczy), Art. 259a (Przekroczenie granicy RP w celu popełnienia przestępstwa o charakterze terrorystycznym)*[9].

Na kanwie analizy zmian obu wskazanych powyżej ustaw należy wysnuć podstawowy wniosek, że wprowadzenie problematyki zwalczania terroryzmu do krajowego prawodawstwa nie było wynikiem wewnętrznych analiz i postulatów legislacyjnych, lecz bezpośrednim następstwem konieczności dostosowania polskiego systemu prawa do wymogów wynikających z członkostwa w Organizacji Narodów Zjednoczonych oraz trwającego procesu integracji z Unią Europejską.

W tym kontekście podobnego charakteru nabiera dokonana w 2009 r. duża reforma[10] systemu przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu, uwzględniająca w krajowych regulacjach prawnych wymogi

[9] 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. 73–74.

[10] Dokonana *Ustawą z dnia 25 czerwca 2009 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw* (DzU z 2009 r. nr 166 poz. 1317).

wprowadzone Dyrektywą 2005/60/WE Parlamentu Europejskiego i Rady z 26 października 2005 r.[11] oraz Dyrektywą Komisji 2006/70/WE z 1 sierpnia 2006 r. ustanawiającą środki wykonawcze do dyrektywy 2005/60/WE[12]. Na mocy tej reformy uchylono w pierwszej z analizowanych ustaw definicję pojęcia „akt terrorystyczny", wprowadzając definicję pojęcia „finansowanie terroryzmu", rozumianego jako czyn zabroniony – wprowadzony jako nowy – w art. 165a kodeksu karnego. Jak wskazywano w uzasadnieniu do ustawy reformującej, (...) *wymóg penalizacji finansowania terroryzmu przewidziany został w międzynarodowej konwencji o zwalczaniu finansowania terroryzmu, która została ratyfikowana przez RP* (...). *Do kwestii finansowania terroryzmu odnosi się również dyrektywa 2005/60/WE. W tym zakresie regulacja powyższa ma na celu nie tylko pełną implementację dyrektywy, ale również ujednolicenie stosowania standardów międzynarodowych*[13]. Analizując zmiany w gałęzi prawa karnego nakierowane na przeciwdziałanie terroryzmowi, należy zauważyć, że ustawodawca na mocy nowelizacji[14], która weszła w życie 14 listopada 2011 r., dodał do kodeksu karnego w art. 255a nowy typ czynu zabronionego nakierowany na rozpowszechnianie treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym. Wprowadzenie tych zmian, podobnie jak poprzednio, było następstwem konieczności implementacji regulacji unijnych, w tym wypadku decyzji ramowej Rady 2008/919/WSiSW z 21 listopada 2008 r. zmieniającej decyzję ramową 2002/475/WSiSW w sprawie zwalczania terroryzmu, poszerzającej katalog

---

[11] *Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu* (Dz. Urz. UE L 309/13 z 24 XI 2005 r.).

[12] *Dyrektywa Komisji 2006/70/WE z dnia 1 sierpnia 2006 r. ustanawiająca środki wykonawcze do dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady w odniesieniu do definicji osoby zajmującej eksponowane stanowisko polityczne, jak również w odniesieniu do technicznych kryteriów stosowania uproszczonych zasad należytej staranności wobec klienta oraz wyłączenia z uwagi na działalność finansową prowadzoną w sposób sporadyczny lub w bardzo ograniczonym zakresie* (Dz. Urz. UE L 214/29 z 4 VIII 2006 r.).

[13] *Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw*, http://orka.sejm.gov.pl/proc6.nsf/opisy/1660.htm [dostęp: 22 XI 2021].

[14] *Ustawa z dnia 29 lipca 2011 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary* (DzU z 2011 r. nr 191 poz. 113).

„przestępstw związanych z działalnością terrorystyczną" o przestępstwo nawoływania do popełnienia przestępstwa terrorystycznego, rekrutacji na potrzeby terroryzmu oraz szkolenia na potrzeby terroryzmu.

Poza dwoma analizowanymi aktami ustawowymi ważne miejsce w krajowych regulacjach prawnych poświęconych zjawisku terroryzmu zajęła uchwalona *Ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[15], która określiła organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania, w tym w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym. Co ważne, na mocy nowelizacji[16] tej ustawy (weszła w życie 19 września 2009 r.) rozszerzono zakres jej definicji legalnych o pojęcie „zdarzenia o charakterze terrorystycznym", pod którym rozumiano sytuację powstałą na skutek czynu określonego w art. 115 § 20 kodeksu karnego lub zagrożenie zaistnienia takiego czynu, mogącego doprowadzić do sytuacji kryzysowej. Ponadto dodano do ustawy art. 12a, który regulował współpracę w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym między organami administracji publicznej oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej. Mocą tego przepisu podkreślono rolę organów administracji rządowej właściwych w sprawach rozpoznawania, zapobiegania i zwalczania zagrożeń, w tym szczególną rolę Szefa ABW, który otrzymał ustawowe upoważnienie do udzielania zaleceń w celu ochrony infrastruktury krytycznej organom i podmiotom zagrożonym działaniami o charakterze terrorystycznym oraz przekazywania do tych podmiotów niezbędnych informacji służących przeciwdziałaniu tym zagrożeniom, także uzyskanych w toku działalności operacyjnej[17].

Trzeba pamiętać, że problematyka zagrożeń terrorystycznych była również podejmowana przez ustawodawcę w regulacjach dotyczących stanów nadzwyczajnych. *Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym*[18] w art. 2 brzmienia pierwotnego wskazywała, że uzasadnieniem dla skierowania do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego jest zaistnienie sytuacji

[15] Tekst jednolity: DzU z 2022 r. poz. 261.

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

[17] Por. *Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym*, http://orka.sejm.gov.pl/proc6.nsf/opisy/1699.htm [dostęp: 22 XI 2021].

[18] Tekst pierwotny ogłoszony w DzU z 2002 r. nr 113 poz. 985.

szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami terrorystycznymi, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych. Podobnie *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*[19] w art. 2 brzmienia pierwotnego dawała podstawę Prezydentowi Rzeczypospolitej Polskiej do wprowadzenia, na wniosek Rady Ministrów, stanu wojennego na części albo na całym terytorium państwa w razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami terrorystycznymi, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji.

Tematyka zagrożeń terrorystycznych jest istotna również w ustawodawstwie ustrojowym organów ochrony prawnej, w szczególności w *Ustawie z dnia 6 kwietnia 1990 r. o Policji*, *Ustawie z dnia 12 października 1990 r. o Straży Granicznej*, *Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, zwanej dalej ustawą o ABW oraz AW, a także innych aktach prawa obejmujących wybrane aspekty dotyczące określonego rodzaju zagrożeń[20]. Zawarto w nich problematykę działań antyterrorystycznych z perspektywy zakresu powierzonych danej służbie zadań i przyznanych uprawnień oraz zasad współdziałania i wymiany informacji.

Szczegółowe procedury działania zaś były ujmowane w aktach prawnych o charakterze wewnętrznie obowiązującym oraz w bliżej niesformalizowanych dokumentach tworzonych zarówno na poziomie Rady Ministrów czy też poszczególnych resortów oraz służb i instytucji, jak i w porozumieniach o charakterze administracyjnym pomiędzy nimi. Istotne zadania związane m.in. z opracowywaniem projektów standardów i procedur w zakresie zwalczania terroryzmu oraz występowania z wnioskiem do właściwych ministrów w celu podjęcia działań legislacyjnych zmierzających do usprawnienia metod i form zwalczania terroryzmu wykonywał i wykonuje istniejący od 25 października 2006 r.

---

[19] Tekst pierwotny ogłoszony w DzU z 2002 r. nr 156 poz. 1301.

[20] Szczegółowy wykaz podstawowych ustaw regulujących zakres zadań realizowanych w odniesieniu do poszczególnych rodzajów zagrożeń terrorystycznych przez właściwe podmioty stanowił załącznik nr 1 do *Narodowego Programu Antyterrorystycznego na lata 2015–2019* (MP z 2014 r. poz. 1218).

Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych[21], działający jako organ pomocniczy Rady Ministrów.

Analiza zarysowanego powyżej rozwoju prawodawstwa krajowego, który był nakierowany na przeciwdziałanie zagrożeniom terrorystycznym w ujęciu historycznym, pozwala wysnuć tezę, że przebiegał on zgodnie z modelem materialnym, tworząc system przepisów rozproszonych w różnych ustawach i innych aktach normatywnych i nienormatywnych.

Opisanemu rozwojowi regulacji prawnych systemu antyterrorystycznego towarzyszyła wieloletnia debata, (...) *czy zwalczanie terroryzmu może stanowić materię ustawową, a jeśli tak, czy przeciwdziałanie temu zagrożeniu dla bezpieczeństwa można ująć w jednej kompleksowej ustawie*[22]. Wśród prób opracowania takiej ustawy na uwagę zasługują prace Zespołu Zadaniowego do Spraw Usystematyzowania Krajowych Regulacji i Rozwiązań Prawnych Dotyczących Przeciwdziałania Terroryzmowi[23], który opracował wstępny projekt założeń do projektu ustawy o gromadzeniu i przetwarzaniu informacji w celu rozpoznawania zagrożeń o charakterze terrorystycznym. Uwzględniając rekomendacje tego Zespołu, powołano Zespół Zadaniowy do opracowania szczegółowych założeń do projektu ustawy o rozpoznawaniu, przeciwdziałaniu i zwalczaniu terroryzmu[24]. W ramach tego gremium nie udało się jednak wypracować zakładanych założeń, a na poziomie politycznym podjęto decyzję o zakończeniu prac w tym zakresie[25].

Wobec niepowodzenia działań legislacyjnych wskazanych zespołów przystąpiono do prac nad dokumentem strategicznym o charakterze

---

[21] Powołany *Zarządzeniem nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*.

[22] K. Indecki, P. Potejko, *Wstęp*, w: *Terroryzm. Materia ustawowa?*, K. Indecki, P. Potejko (red.), Warszawa 2009, s. 4.

[23] Powołany *Decyzją nr 5 Przewodniczącego Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych z 10 czerwca 2008 r*.

[24] Powołany *Decyzją nr 6 Przewodniczącego Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych z 12 stycznia 2009 r*.

[25] 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. 280.

nienormatywnym dotyczącym zapobiegania i reagowania na zagrożenia terrorystyczne. Rezultatem tego było przyjęcie *Narodowego Programu Antyterrorystycznego na lata 2015–2019*[26], w którym przedstawiono przede wszystkim diagnozę zjawiska terroryzmu i systemu antyterrorystycznego Rzeczypospolitej Polskiej, cel główny i cele szczegółowe programu oraz mechanizmy jego realizacji.

Kolejną decyzję o podjęciu prac nad ustawą kompleksowo regulującą kwestie prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi do prowadzenia tych działań podjęto 2 grudnia 2015 r. na posiedzeniu Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, projekt zaś opracowany przez Ministerstwo Spraw Wewnętrznych i Administracji we współpracy z Agencją Bezpieczeństwa Wewnętrznego stał się podstawą rządowych prac legislacyjnych prowadzonych w kwietniu 2016 r. Projekt ustawy, która ostatecznie została uchwalona 10 czerwca 2016 r., zmieniając model legislacji antyterrorystycznej z modelu materialnego na model formalny, uwzględniał doświadczenia zebrane przez zespoły pracujące w latach 2008–2009 oraz nowe, powstałe w związku z funkcjonowaniem Narodowego Programu Antyterrorystycznego.

Szczególne znaczenie ustawy o działaniach antyterrorystycznych w normatywnym systemie zwalczania terroryzmu w Polsce

Ustawa o działaniach antyterrorystycznych[27] weszła w życie 2 lipca 2016 r., tuż przed odbywającym się w dniach 8–9 lipca 2016 r. szczytem państw członkowskich Sojuszu Północnoatlantyckiego w Warszawie oraz zaplanowanymi na 26–31 lipca 2016 r. Światowymi Dniami Młodzieży w Krakowie. Te wydarzenia – co często wskazywano podczas prac legislacyjnych – wpłynęły na przyśpieszenie prac nad ustawą.

Jak wskazuje się w doktrynie:

> (...) po wielu latach swego rodzaju „chaosu prawnego" w działaniach antyterrorystycznych – również w Polsce – dostrzeżono potrzebę wzmocnienia narzędzi przeciwdziałania i zwalczania

[26] *Uchwała 252 z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (MP z 2014 r. poz. 1218).

[27] Tekst pierwotny ogłoszono w DzU z 2016 r. poz. 904.

> zagrożeń terrorystycznych, jak również reagowania na te zagrożenia. (...) Od wielu lat eksperci zajmujący się bezpieczeństwem publicznym wskazywali, że polskie służby w razie zamachów nie działają tak szybko i sprawnie, jak ich odpowiednicy w Londynie, Paryżu czy Brukseli. Powodem tego był brak jednoznacznych reguł i procedur odpowiedzialności za dany obszar działań i wynikający z tego chaos i rozmycie odpowiedzialności[28].

Aby temu przeciwdziałać, prawodawca polski przyjął ustawę, której podstawowym celem stało się:

> (...) podniesienie efektywności polskiego systemu antyterrorystycznego, a tym samym zwiększenie bezpieczeństwa wszystkich obywateli RP, poprzez:
> – wzmocnienie mechanizmów koordynacji działań;
> – doprecyzowanie zadań poszczególnych służb i organów oraz zasad współpracy między nimi;
> – zapewnienie możliwości skutecznych działań w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego;
> – zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń;
> – dostosowanie przepisów karnych do nowych typów zagrożeń o charakterze terrorystycznym[29].

Jak wyraźnie podkreślano w uzasadnieniu do projektu ustawy:

> (...) regulacja ma charakter integrujący działania podmiotów polskiego systemu antyterrorystycznego z jasnym wskazaniem odpowiedzialności w poszczególnych obszarach. Zastosowanie w ustawie systemowego podejścia do problematyki zagrożeń o charakterze terrorystycznym pozwoli na wykorzystanie potencjału wszystkich służb, organów i instytucji posiadających ustawowe kompetencje do realizowania działań antyterrorystycznych.

[28] A. Tyburska, B. Jewartowski, *Ustawa antyterrorystyczna wobec zjawiska współczesnego terroryzmu*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 263.

[29] U*zasadnienie do rządowego projektu ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw*, https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=516 [dostęp: 24 XI 2021].

> Regulacja będzie miała również bezpośredni wpływ na szybkość i prawidłowość procesu decyzyjnego na poziomie strategicznym[30].

Konstrukcyjnie ustawa została podzielona na 7 rozdziałów. W rozdziale 1 zawarto najistotniejsze dla funkcjonowania ustawy definicje legalne pojęć, takich jak:

- „działania antyterrorystyczne", rozumiane 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 (art. 2 pkt 1 ustawy);
- „działania kontrterrorystyczne", rozumiane jako działania wobec sprawców, osób przygotowujących przestępstwo o charakterze terrorystycznym, o którym mowa w art. 115 § 20 kodeksu karnego, lub pomagających w jego dokonaniu, prowadzone w celu wyeliminowania bezpośredniego zagrożenia życia, zdrowia lub wolności osób lub mienia przy wykorzystaniu specjalistycznych sił i środków oraz specjalistycznej taktyki działania (art. 2 pkt 2 ustawy);
- „miejsce zdarzenia o charakterze terrorystycznym", rozumiane jako przestrzeń otwarta lub zamknięta, w której nastąpiło zdarzenie o charakterze terrorystycznym lub w której wystąpił lub miał wystąpić jego skutek, oraz przestrzeń, w której występują zagrożenia związane ze zdarzeniem o charakterze terrorystycznym (art. 2 pkt 6 ustawy);
- „zdarzenie o charakterze terrorystycznym", rozumiane jako sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 kodeksu karnego, lub zagrożenie zaistnienia takiego przestępstwa.

Główną treść materialną ustawy zawarto w rozdziałach 2 i 4, opartych konstrukcyjnie na wyodrębnieniu dwóch głównych etapów podejmowania czynności antyterrorystycznych. Za pierwszy z nich, uregulowany w rozdziale 2, uznano etap zapobiegania zdarzeniom o charakterze terrorystycznym, w którym odpowiedzialność i rolę

[30] Tamże.

koordynacyjną przypisano Szefowi ABW. Za istotne elementy działań tego etapu ustawodawca uznał po pierwsze, nałożenie obowiązku na organy administracji publicznej, właścicieli i posiadaczy obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej – współpracy z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego przy realizacji działań antyterrorystycznych, a w szczególności niezwłocznego przekazywania Szefowi ABW 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. Jednocześnie Szef ABW otrzymał nowe uprawnienia, w tym w szczególności:

- wydawania poleceń organom i podmiotom, które są zagrożone tymi zdarzeniami, mających na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację, oraz przekazywanie im informacji niezbędnych do osiągnięcia tego celu (art. 4 ustawy);
- koordynacji czynności analityczno-informacyjnych podejmowanych przez służby specjalne oraz koordynacji wymiany informacji (ich gromadzenia, przetwarzania i analizowania) 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 zdarzeń o charakterze terrorystycznym oraz danych o osobach związanych z działaniami terrorystycznymi, które klasyfikuje się zgodnie z tzw. katalogiem incydentów o charakterze terrorystycznym, określonym w *Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym*[31] (art. 5 ustawy);
- koordynacji czynności operacyjno-rozpoznawczych dotyczących zdarzeń o charakterze terrorystycznym, podejmowanych przez służby specjalne oraz Policję, Straż Graniczną, Krajową Administrację Skarbową i Żandarmerię Wojskową, a także wydawanie

[31] DzU z 2017 r. poz. 1517, ze zm.

tym służbom zaleceń mających na celu usunięcie bądź minimalizację zaistniałego zagrożenia terrorystycznego (art. 8 ustawy);
- prowadzenia wykazu osób związanych z działaniami terrorystycznymi oraz udzielania informacji z tego wykazu, także w postaci bieżących analiz stanu zagrożenia zdarzeniem o charakterze terrorystycznym (art. 6 ustawy);
- zarządzania niejawnego prowadzenia czynności wobec cudzoziemców w zakresie uzyskiwania i utrwalania treści rozmów prowadzonych przy użyciu środków technicznych, obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne, treści korespondencji oraz danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych (art. 9 ustawy);
- nieodpłatnego dostępu do danych i informacji zgromadzonych w rejestrach publicznych i ewidencjach oraz obrazu zdarzeń rejestrowanego przez urządzenia rejestrujące obraz umieszczone w obiektach użyteczności publicznej, przy drogach publicznych i innych miejscach publicznych (art. 11 ustawy);
- nadania funkcjonariuszom ABW, Policji i Straży Granicznej uprawnienia do pobierania obrazu linii papilarnych oraz utrwalania wizerunku twarzy i pobierania materiału DNA (art. 10 ustawy).

Ponadto do ustawy wprowadzono rozwiązania ułatwiające oddelegowanie do ABW pracowników lub funkcjonariuszy 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, co jest niezmiernie istotne z perspektywy organizacji i funkcjonowania Centrum Antyterrorystycznego ABW, tj. statutowej jednostki organizacyjnej ABW[32], odpowiedzialnej za rozpoznawanie zagrożeń terrorystycznych, realizującej zadania przy ścisłej współpracy z innymi służbami i instytucjami państwowymi oraz organizacjami międzynarodowymi[33].

---

[32] *Zarządzenie nr 163 Prezesa Rady Ministrów z dnia 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (MP z 2018 r. poz. 927).

[33] Por. *Zwalczanie terroryzmu*, https://www.abw.gov.pl/pl/zadania/zwalczanie-terroryzmu/5,Zwalczanie-terroryzmu.html [dostęp: 24 XI 2021].

Warto dodać, że ustawa dała, w rozdziale 3, możliwość wprowadzenia przez Prezesa Rady Ministrów jednego z czterech stopni alarmowych i stopni alarmowych CRP, które odznaczają się walorem powszechnie obowiązującej informacji nakierowanej poza organami, służbami i instytucjami również na inne jednostki organizacyjne i społeczeństwo. System ten został w dużej mierze transponowany z obowiązującego wcześniej załącznika nr 1 do *Zarządzenia nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego*[34]. *Stosowanie katalogu stopni alarmowych wynika ze zobowiązań Polski jako członka Organizacji Traktatu Północnoatlantyckiego (NATO)*[35].

Za drugi etap podejmowania czynności kontrterrorystycznych, uregulowany w rozdziale 4 ustawy, uznano etap obejmujący 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 którym odpowiedzialność i rolę koordynacyjną przypisano ministrowi właściwemu do spraw wewnętrznych. Ustawodawca zdefiniował pojęcie kierującego działaniami antyterrorystycznymi podejmowanymi przez właściwe służby lub organy w ramach ich ustawowej kompetencji na miejscu zdarzenia o charakterze terrorystycznym, którym zostaje przedstawiciel Komendanta Głównego Policji (lub przedstawiciel Ministra Obrony Narodowej – w przypadku zdarzenia na terenie obszarów wojskowych). Tak wyznaczony kierujący działaniami antyterrorystycznymi zyskał prawo, gdy jest to uzasadnione sytuacją na miejscu zdarzenia o charakterze terrorystycznym, m.in. zarządzenia ewakuacji osób lub mienia z miejsca zdarzenia o charakterze terrorystycznym i z jego otoczenia do wskazanego miejsca, obiektu lub obszaru oraz wstrzymania albo ograniczenia ruchu pojazdów albo ruchu kolejowego w miejscu zdarzenia o charakterze terrorystycznym i w jego otoczeniu, albo też żądania nieodpłatnego korzystania z nieruchomości lub nieodpłatnego przejęcia do używania ruchomości, w tym także przedmiotów i urządzeń, czy też żądania udzielenia pomocy od instytucji, organizacji, przedsiębiorców i osób fizycznych lub wydawania im polecenia.

[34] MP z 2016 r. poz. 233.

[35] *Uzasadnienie do rządowego projektu ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw,* https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=516 [dostęp: 24 XI 2021].

Ponadto w ramach tego etapu w ustawie zawarto możliwość wprowadzenia zakazu odbywania zgromadzeń lub imprez masowych na obszarze lub w obiekcie objętym stopniem alarmowym, na zasadach określonych w art. 21. Ustawodawca przewidział również możliwość użycia Sił Zbrojnych RP do pomocy oddziałom Policji w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego, na zasadach określonych w art. 22. Należy zwrócić uwagę, że w ramach działań tego etapu dopuszczono tzw. specjalne użycie broni, oznaczające możliwość użycia broni palnej przeciwko osobie dokonującej zamachu albo biorącej lub przetrzymującej zakładnika, którego skutkiem może być śmierć lub bezpośrednie zagrożenie życia lub zdrowia tej osoby, jeżeli jest to niezbędne do przeciwdziałania bezpośredniemu, bezprawnemu, gwałtownemu zamachowi na życie lub zdrowie człowieka lub do uwolnienia zakładnika, a użycie broni palnej w sposób wyrządzający możliwie najmniejszą szkodę jest niewystarczające i przeciwdziałanie takiemu zamachowi lub uwolnienie zakładnika w inny sposób nie jest możliwe.

W rozdziale 5 ustawy prawodawca wprowadził przepisy szczególne dotyczące fazy postępowania karnego w zakresie postępowania przygotowawczego, dotyczące specjalnego trybu dokonywania czynności procesowych, przeszukania pomieszczeń lub zatrzymania osoby podejrzewanej o przestępstwa o charakterze terrorystycznym, a także sporządzenia postanowienia o przedstawieniu zarzutów oraz zarządzenia tymczasowego aresztowania.

Ustawa wprowadziła też liczne zmiany w przepisach kompetencyjnych i pragmatycznych organów ochrony prawnej, będące głównie następstwem wprowadzonych w ustawie rozwiązań kierunkowych opartych na wyodrębnieniu dwóch głównych etapów podejmowania czynności antyterrorystycznych. W szczególności zwraca uwagę, że w ramach tych zmian dodano do kodeksu karnego, poprzez art. 259a, nowy typ czynu zabronionego w postaci przestępstwa przekraczania granicy Rzeczypospolitej Polskiej w celu popełnienia przestępstwa o charakterze terrorystycznym oraz, poprzez art. 259b, instytucję nadzwyczajnego złagodzenia kary lub warunkowego zawieszenia wykonania kary w stosunku do sprawcy powyższego przestępstwa, który dobrowolnie odstąpił od popełnienia m.in. przestępstwa o charakterze

terrorystycznym[36]. Ponadto, na mocy przepisów nowelizacyjnych zawartych w ustawie, zmieniono istotnie ustawę o ABW oraz AW, m.in.:

- rozszerzając właściwość ABW o rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych, doprecyzowanych zakresowo (art. 5 ust. 1 pkt 2a ustawy o ABW oraz AW);
- wprowadzając uprawnienie ABW do prowadzenia tzw. tajnej współpracy ze sprawcą przestępstwa szpiegostwa lub podejrzanym o popełnienie przestępstwa o charakterze terrorystycznym;
- nadając ABW uprawnienia dostępowe do tajemnicy bankowej (art. 34a ustawy o ABW oraz AW);
- dodając ciąg uprawnień ABW w zakresie bezpieczeństwa teleinformatycznego, tj.:
  a) dokonywania oceny bezpieczeństwa systemów teleinformatycznych (art. 32a ustawy o ABW oraz AW);
  b) udzielania na żądanie Szefa ABW informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji systemów teleinformatycznych przez podmioty, o których mowa w art. 5 ust. 1 pkt 2a ustawy o ABW oraz AW (art. 32b ustawy o ABW oraz AW);
  c) stosowania 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);
  d) prowadzenia rejestru zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych (art. 32d ustawy o ABW oraz AW);
  e) wydawania przez Szefa ABW rekomendacji w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych (art. 32e ustawy o ABW oraz AW).

Należy wskazać, że ustawa o działaniach antyterrorystycznych od dnia jej uchwalenia była nowelizowana sześciokrotnie, przy czym

[36] Brzmienie art. 259a i art. 259b zostało zmienione z dniem 22 czerwca 2021 r. na mocy art. 1 pkt 2 *Ustawy z dnia 20 kwietnia 2021 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* (DzU z 2021 r. poz. 1023). Usunięto z nich zwrot „na terytorium innego państwa" oraz zmieniono wymiar kary za przestępstwo z art. 259a na karę pozbawienia wolności od 3 miesięcy do lat 5.

zmiany te miały charakter przede wszystkim dostosowujący do reorganizacji i zmian w poszczególnych służbach.

Tak ukształtowana ustawa o działaniach antyterrorystycznych spotkała się z pozytywnym odbiorem i oceną międzynarodową, w tym m.in. została zaprezentowana w 2018 r. przez Jukkę Savolainena, dyrektora ds. odporności w Europejskim Centrum Doskonalenia przeciwko Zagrożeniom Hybrydowym w Helsinkach (HybridCoE), jako 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. *Bez wątpienia więc pozytywne oceny ustawy antyterrorystycznej na forach międzynarodowych i jej wpływ na kształtowanie prawodawstwa europejskiego to niewątpliwy sukces i powód do satysfakcji dla autorów ustawy*[37].

Podsumowując dokonany opis rozwiązań prawnych wprowadzonych ustawą o działaniach antyterrorystycznych, trzeba jeszcze raz podkreślić, że zmieniała ona krajowy model ustawodawstwa antyterrorystycznego z rozproszonego modelu materialnego na skoncentrowany model formalny. W ten sposób ustawa ta stała się, wraz z uchwaloną 1 marca 2018 r. nową ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[38], źródłem polskich regulacji, które bezpośrednio kształtują prawny rdzeń obszaru walki z terroryzmem.

Prawo europejskie a terroryzm – stan aktualny

Problematyka przeciwdziałania terroryzmowi stanowi istotne zagadnienie objęte prawodawstwem Unii Europejskiej. Wyspecyfikowanie i analiza zakresu oddziaływania tego prawodawstwa nie jest jednak prosta, w szczególności z uwagi na charakter źródeł prawa Unii Europejskiej.

---

[37] S. Żaryn, *Polska antyterrorystycznym wzorem*, wGospodarce.pl, https://wgospodarce.pl/opinie/58189-polska-antyterrorystycznym-wzorem [dostęp: 25 XI 2021].

[38] Tekst pierwotny ogłoszony w DzU z 2018 r. poz. 723. Podstawowym celem ustawy było dostosowanie polskich przepisów do przepisów *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE* oraz znowelizowanych zaleceń Financial Action Task Force (FATF).

Trzeba przypomnieć, że do źródeł prawa UE należy w pierwszej kolejności tzw. prawo pierwotne, na które składają się traktaty zawierane przez państwa członkowskie, a wśród nich zarówno traktaty założycielskie Wspólnot Europejskich i Unii Europejskiej (tj. traktat paryski z 1951 r., traktaty rzymskie z 1957 r. i Traktat z Maastricht z 1992 r.) oraz tzw. traktaty rewizyjne, tzn. umowy zawarte między państwami członkowskimi zmieniające i uzupełniające traktaty założycielskie, jak i traktaty akcesyjne (o przystąpieniu poszczególnych państw do UE). Do prawa pierwotnego zalicza się również załączniki (w formie protokołów) dołączone do wskazanych umów, ogólne zasady prawa oraz Kartę praw podstawowych Unii Europejskiej. Z kolei do prawa wtórnego, tworzonego przez instytucje Unii na podstawie prawa pierwotnego, zalicza się – zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej[39] – rozporządzenia, dyrektywy, decyzje, zalecenia i opinie. Wymienione akty prawne różnią się od siebie w szczególności mocą i zakresem obowiązywania. I tak, rozporządzenie ma zasięg ogólny oraz wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich, z kolei dyrektywa wiąże każde państwo członkowskie, do którego jest kierowana, w odniesieniu do osiągniętego rezultatu pozostawia jednak organom krajowym swobodę wyboru formy i środków. Decyzja wiąże w całości, ale ma charakter indywidualny i konkretny, co oznacza, że każda z nich jest skierowana do ściśle określonego grona adresatów i dotyczy ściśle określonych spraw czy sytuacji, zalecenia zaś (sugerują podjęcie określonych działań) i opinie (zawierają określone oceny) – nie mają mocy wiążącej.

Na kanwie powyższego należy wskazać, że prawodawstwo Unii Europejskiej nakierowane na przeciwdziałanie terroryzmowi jest po pierwsze, zróżnicowane charakterem źródła prawa, w którym zostało ono uregulowane, co bezpośrednio przekłada się na zakres mocy jego oddziaływania. Po drugie, zauważalny jest dualizm tematycznego sposobu regulowania problematyki terroryzmu w Unii Europejskiej, gdzie albo poszczególne zagadnienia ujmowane są w wyodrębniony zakresowo przedmiotowy akt normatywny, albo też zagadnienia te są ujmowane łącznie z innymi uregulowaniami obszaru bezpieczeństwa.

[39] DzU z 2004 r. nr 90 poz. 864/2.

Analizując przepisy prawa pierwotnego, należy wskazać, że Traktat o Unii Europejskiej[40] tylko w jednym miejscu odnosi się bezpośrednio do problematyki terroryzmu. W art. 42, w zw. z art. 41 (systemowo zlokalizowanymi w sekcji 2 dot. wspólnej polityki bezpieczeństwa i obrony), wskazano że UE może podejmować, zgodnie z zasadami Karty Narodów Zjednoczonych, misje poza jej terytorium w celu utrzymania pokoju, zapobiegania konfliktom i wzmacniania międzynarodowego bezpieczeństwa. Takie misje, przy których prowadzeniu UE może użyć środków cywilnych i wojskowych, obejmują wspólne działania rozbrojeniowe, misje humanitarne i ratunkowe, misje wojskowego doradztwa i wsparcia, misje zapobiegania konfliktom i utrzymywania pokoju, misje zbrojne służące zarządzaniu kryzysowemu, w tym misje przywracania pokoju i operacje stabilizacji sytuacji po zakończeniu konfliktów. Co istotne, zgodnie z Traktatem wszystkie te misje mogą przyczyniać się do walki z terroryzmem, w tym poprzez wspieranie państw trzecich w zwalczaniu terroryzmu na ich terytoriach.

Z kolei Traktat o funkcjonowaniu Unii Europejskiej dotyka problematyki terroryzmu zdecydowanie szerzej, zarówno w Części trzeciej, poświęconej polityce i działaniom wewnętrznym Unii, jak i w Części piątej, w której określono prawne podstawy działań zewnętrznych Unii.

W tym zakresie w Tytule V Części trzeciej Traktatu dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości przyjęto w art. 75, że jeżeli wymaga tego realizacja celów, o których mowa w artykule 67 (tzw. obowiązków UE) w odniesieniu do zapobiegania terroryzmowi i działalności powiązanej oraz zwalczania tych zjawisk, Parlament Europejski i Rada, w drodze rozporządzeń zgodnie ze zwykłą procedurą ustawodawczą, określają zakres stosowania środków administracyjnych dotyczących przepływu kapitału i płatności, takich jak zamrożenie funduszy, aktywów finansowych lub zysków z działalności gospodarczej, które należą do osób fizycznych lub prawnych, grup lub innych podmiotów innych niż państwa, są w ich posiadaniu lub dyspozycji. Rada, na wniosek Komisji, przyjmuje środki w celu wdrożenia tych ram. Akty te muszą zawierać niezbędne przepisy w zakresie gwarancji prawnych. Co istotne, na podstawie przedmiotowej delegacji organy Unii wydały 75 aktów prawa pochodnego rangi rozporządzenia, w których wprowadzano środki ograniczające wobec wybranych państw,

[40] DzU z 2004 r. nr 90 poz. 864/30.

w tym m.in. Iranu, Iraku, Konga, Białorusi, Liberii, Somalii, Libanu, Uzbekistanu.

W ramach tego samego Tytułu V Części trzeciej Traktatu w art. 83 wskazano, że Parlament Europejski i Rada, w drodze dyrektyw zgodnie ze zwykłą procedurą ustawodawczą, mogą ustanowić normy minimalne odnoszące się do określania przestępstw oraz kar w dziedzinach szczególnie poważnej przestępczości o wymiarze transgranicznym, wynikające z rodzaju lub skutków tych przestępstw lub ze szczególnej potrzeby wspólnego ich zwalczania. Do dziedzin tej przestępczości Traktat zaliczył terroryzm, oprócz takich rodzajów przestępstw, jak handel ludźmi oraz seksualne wykorzystywanie kobiet i dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcja, fałszowanie środków płatniczych, przestępczość komputerowa i przestępczość zorganizowana. Na podstawie przedmiotowej delegacji organy Unii wydały m.in. *Dyrektywę Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW*[41], będącej jednym z najważniejszych aktów prawa pochodnego UE w dziedzinie terroryzmu.

Wskazana delegacja stała się również podstawą wydania *Decyzji Rady (UE) 2018/889 z dnia 4 czerwca 2018 r. w sprawie zawarcia, w imieniu Unii Europejskiej, Konwencji Rady Europy o zapobieganiu terroryzmowi*[42], w której zatwierdzono w imieniu Unii *Konwencję Rady Europy o zapobieganiu terroryzmowi* z 16 maja 2005 r.[43], w odniesieniu do spraw wchodzących w zakres kompetencji Unii oraz *Decyzję Rady (UE) 2018/890 z dnia 4 czerwca 2018 r. w sprawie zawarcia, w imieniu Unii Europejskiej, Protokołu dodatkowego do Konwencji Rady Europy o zapobieganiu terroryzmowi*[44].

Ta sama część Traktatu stała się miejscem określenia zasad współpracy policyjnej w UE, której elementem jest powołanie Europolu (Agencji Unii Europejskiej ds. Współpracy Organów Ścigania). Jego zadaniem zgodnie z art. 88 Traktatu jest wspieranie i wzmacnianie działań organów policyjnych i innych organów ścigania państw członkowskich, jak również ich wzajemnej współpracy w zapobieganiu i zwalczaniu

[41] Dz. Urz. UE L 88/6 z 31 III 2017 r.

[42] Dz. Urz. UE L 159/1 z 22 VI 2018 r.

[43] Dz. Urz. UE L nr 159/3 z 22 VI 2018 r.

[44] Dz. Urz. UE L 159/15 z 22 VI 2018 r.

poważnej przestępczości dotykającej dwóch lub więcej państw członkowskich, terroryzmu oraz form przestępczości naruszających wspólny interes objęty polityką Unii.

Z kolei w Części piątej Traktatu dotyczącej działań zewnętrznych Unii został umieszczony art. 222 ustanawiający tzw. klauzulę solidarności, zgodnie z którą Unia i jej państwa członkowskie działają wspólnie w duchu solidarności, jeżeli jakiekolwiek państwo członkowskie stanie się przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej, lub katastrofy spowodowanej przez człowieka. W tym zakresie Unia mobilizuje wszystkie będące w jej dyspozycji instrumenty, w tym środki wojskowe udostępnione jej przez państwa członkowskie, w celu: po pierwsze, zapobiegania zagrożeniu terrorystycznemu na terytorium państw członkowskich; po drugie, ochrony instytucji demokratycznych i ludności cywilnej przed ewentualnym atakiem terrorystycznym; po trzecie, udzielenia pomocy państwu członkowskiemu na jego terytorium, na wniosek jego władz politycznych, w przypadku ataku terrorystycznego. Ponadto, jak dodano w ust. 2, jeżeli państwo członkowskie stało się przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej, lub katastrofy spowodowanej przez człowieka, na prośbę jego władz politycznych inne państwa członkowskie udzielają mu pomocy. W tym celu państwa członkowskie koordynują swoje działania w ramach Rady. Jednocześnie w ust. 3 określono, że na wspólny wniosek Komisji i wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa, Rada przyjmuje decyzję określającą warunki zastosowania przez Unię niniejszej klauzuli solidarności. Decyzja taka została wydana 24 czerwca 2014 r.[45]

Kierując niniejsze rozważania w stronę prawa pochodnego UE, należy wskazać, że jednym z najważniejszych – o ile nie najważniejszym – aktem normatywnym UE dotykającym problematyki zagrożeń terrorystycznych jest wskazana powyżej dyrektywa 2017/541 w sprawie zwalczania terroryzmu. Weszła ona w życie 20 kwietnia 2017 r., zastępując – co wskazuje jej tytuł – *Decyzję ramową Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu*, która była uznawana za podstawę działań państw członkowskich, służących zwalczaniu terroryzmu, w przedmiocie sprawowania wymiaru sprawiedliwości w sprawach karnych. Nowa dyrektywa, na co wskazuje jej art. 1,

[45] Dz. Urz. UE L 192/53 z 1 VII 2014 r.

ustanowiła normy minimalne dotyczące definicji przestępstw i sankcji w dziedzinie przestępstw terrorystycznych, przestępstw dotyczących grupy terrorystycznej oraz przestępstw związanych z działalnością terrorystyczną, jak również określiła środki ochrony i wsparcia ofiar terroryzmu i pomocy tym ofiarom. Jak wskazano w motywach 6–8 nowej dyrektywy:

> (...) biorąc pod uwagę zmieniający się charakter zagrożeń terrorystycznych oraz prawne zobowiązania Unii i państw członkowskich wynikające z prawa międzynarodowego, należy dokonać we wszystkich państwach członkowskich dalszego zbliżenia definicji przestępstw terrorystycznych, przestępstw dotyczących grupy terrorystycznej oraz przestępstw związanych z działalnością terrorystyczną, tak by definicja ta obejmowała czyny związane zwłaszcza z zagranicznymi bojownikami terrorystycznymi i finansowaniem terroryzmu bardziej kompleksowo. Takie czyny powinny także podlegać karze, w przypadku gdy doszło do nich za pośrednictwem internetu, w tym mediów społecznościowych. Ponadto transgraniczny charakter terroryzmu wymaga prowadzenia zdecydowanych i skoordynowanych działań i współpracy zarówno w państwach członkowskich i między tymi państwami, jak również z i między właściwymi agencjami i organami Unii zajmującymi się zwalczaniem terroryzmu, w tym Eurojustem i Europolem. W tym celu należy efektywnie wykorzystywać dostępne narzędzia i zasoby w zakresie współpracy, takie jak wspólne zespoły dochodzeniowo-śledcze i spotkania koordynacyjne organizowane przy pomocy Eurojustu. Globalny charakter terroryzmu wymaga podjęcia działań na szczeblu międzynarodowym, co oznacza, że Unia i jej państwa członkowskie muszą zacieśnić współpracę z odpowiednimi państwami trzecimi. Zdecydowane i skoordynowane działania i współpraca są również niezbędne do celów zabezpieczania i pozyskiwania dowodów elektronicznych. Niniejsza dyrektywa zawiera wyczerpujący wykaz poważnych przestępstw, takich jak ataki na życie ludzkie, stanowiących czyny umyślne, które można zakwalifikować jako przestępstwa terrorystyczne wyłącznie w przypadku, gdy zostały popełnione w określonym celu terrorystycznym, mianowicie aby poważnie zastraszyć ludność, bezprawnie zmusić rząd lub organizację międzynarodową do podjęcia lub zaniechania działania lub aby poważnie zdestabilizować lub zniszczyć podstawowe struktury polityczne, konstytucyjne, gospodarcze lub społeczne danego państwa lub danej organizacji

> międzynarodowej. Groźby popełnienia takich czynów umyślnych również należy uznawać za przestępstwa terrorystyczne, jeżeli obiektywne przesłanki wskazują, że dopuszczono się ich, kierując się jednym z wymienionych celów terrorystycznych. Natomiast czynów, których celem jest na przykład zmuszenie rządu do podjęcia lub zaniechania jakiegokolwiek działania, ale których nie umieszczono w wyczerpującym wykazie poważnych przestępstw, nie uznaje się zgodnie z niniejszą dyrektywą za przestępstwa terrorystyczne.

Zgodnie z art. 28 dyrektywy, jej postanowienia powinny być wprowadzone na poziomie właściwych regulacji ustawowych, wykonawczych i administracyjnych państw członkowskich do 8 września 2018 r. W Polsce ta dyrektywa została implementowana *Ustawą z dnia 20 kwietnia 2021 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*[46]. Jak wskazywano w uzasadnieniu do przedmiotowego projektu ustawy:

> (...) z uwagi na fakt wcześniejszej implementacji przez Polskę między innymi *decyzji ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu* (Dz. Urz. UE L 164 z 22 VI 2002, str. 3), dotyczącej tego samego obszaru, zdecydowaną większość przepisów dyrektywy 2017/541 należy uznać za implementowaną. Przykładowo, w art. 115 § 20 k.k. istnieje już definicja przestępstwa o charakterze terrorystycznym, w art. 165a jest penalizowane finansowanie przestępstwa o charakterze terrorystycznym, a w art. 258 § 2 i 4 jest penalizowana działalność w ramach grupy przestępczej o charakterze terrorystycznym. Na marginesie należy wspomnieć, iż dyrektywa 2017/541 ma charakter przekrojowy i dotyka nie tylko obszaru prawa karnego, ale także tematów powiązanych, takich jak np. ochrona praw ofiar terroryzmu. Tutaj również jednak zdecydowana większość prac wdrożeniowych została już wykonana przy okazji implementacji wcześniejszych instrumentów unijnych, takich jak dyrektywa *Parlamentu Europejskiego i Rady 2012/29/UE z dnia 25 października 2012 r. ustanawiająca normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw oraz zastępująca decyzję ramową Rady 2001/220/WSiSW* (Dz. Urz. UE L 315 z 14 XI 2012 r., str. 57). Ponadto niektóre postulaty zawarte

[46] DzU z 2021 r. poz. 1023.

w dyrektywie nie wymagają działań legislacyjnych, a wyłącznie organizacyjnych[47].

Wspólne dla wszystkich państw członkowskich ramy prawne określone omówioną dyrektywą 2017/541 w sprawie zwalczania terroryzmu stanowią punkt odniesienia dla wymiany informacji i współpracy między właściwymi organami krajowymi państw członkowskich prowadzonymi w EU na podstawie:

- *Decyzji ramowej Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi*[48];
- *Decyzji ramowej Rady 2002/465/WSiSW z dnia 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych*[49];
- *Decyzji Rady 2005/671/WSiSW z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy dotyczącej przestępstw terrorystycznych*[50];
- *Decyzji ramowej Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania Państw Członkowskich Unii Europejskiej*[51], ustanawiającej zasady, według których organy ścigania Państw Członkowskich mogą dokonywać skutecznej i sprawnej wymiany istniejących informacji i danych wywiadowczych w celu prowadzenia dochodzeń karnych lub operacji wywiadowczych dotyczących poważnych przestępstw, w tym przestępczości zorganizowanej i terroryzmu;
- *Decyzji Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej*[52], która w rozdziale 4 zawiera przepisy dotyczące warunków dostarczania informacji służących zapobieganiu przestępstwom terrorystycznym;

[47] *Uzasadnienie do rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*, https://www.sejm.gov.pl/Sejm9.nsf/PrzebiegProc.xsp?nr=867 [dostęp: 2 XII 2021].

[48] Dz. Urz. UE L 190/1 z 18 VII 2002 r.

[49] Dz. Urz. UE L 162/1 z 20 VI 2002 r.

[50] Dz. Urz. UE L 253/22 z 29 IX 2005 r.

[51] Dz. Urz. UE L 386/89 z 29 XII 2006 r.

[52] Dz. Urz. UE L 210/1 z 6 VIII 2008 r.

– *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013*[53].

Jednocześnie w ostatnich latach na poziomie Unii, dla skutecznego zwalczania terroryzmu, podkreśla się konieczność prowadzenia efektywnej wymiany pomiędzy właściwymi organami państw członkowskich a agencjami Unii informacji, które właściwe organy uznają za istotne z punktu widzenia zapobiegania przestępstwom terrorystycznym, wykrywania tych przestępstw, prowadzenia postępowań przygotowawczych lub oskarżania w ich sprawie. Wymiana ta powinna być prowadzona zgodnie z prawem krajowym i obowiązującymi ramami prawnymi Unii, takimi jak:

– *Decyzja Rady 2005/671/WSiSW z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy dotyczącej przestępstw terrorystycznych*,
– *Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II)*[54],
– *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania*[55].

W prawodawstwie UE zwraca się uwagę, aby opisana powyżej wymiana informacji była zgodna z unijnymi przepisami dotyczącymi ochrony danych osobowych, określonych *Dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW*[56], i pozostawała

[53] Dz. Urz. UE L 180/1 z 29 VI 2013 r.

[54] Dz. Urz. UE L 205/63 z 7 VIII 2007 r.

[55] Dz. Urz. UE L 119/132 z 4 V 2016 r.

[56] Dz. Urz. UE L 119/89 z 4 V 2016 r.

bez uszczerbku dla unijnych przepisów dotyczących współpracy między właściwymi organami krajowymi w ramach postępowań karnych, zawartych w takich aktach, jak m.in. *Dyrektywa Parlamentu Europejskiego i Rady 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych*[57].

Ponadto państwa członkowskie muszą przyjąć środki ochrony, wsparcia i pomocy w odpowiedzi na szczególne potrzeby ofiar terroryzmu, zgodnie z *Dyrektywą Parlamentu Europejskiego i Rady 2012/29/UE z dnia 25 października 2012 r. ustanawiającą normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw oraz zastępującą decyzję ramową Rady 2001/220/WSiSW*[58]. Jednocześnie pomoc udzielana ofiarom w dochodzeniu roszczeń odszkodowawczych pozostawać ma bez uszczerbku i stanowić uzupełnienie pomocy, którą ofiary terroryzmu otrzymują od organów pomocniczych zgodnie z *Dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającą rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającą dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE*[59]. Należy dodać, że w porządku prawnym Unii Europejskiej w sposób przedmiotowo wyodrębniony uregulowano, poprzez Dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r.[60], wspólne przepisy dotyczące zapobiegania wykorzystywaniu unijnego systemu finansowego Unii do prania pieniędzy lub finansowania terroryzmu.

Kończąc zwięzłe – z uwagi na wymogi niniejszego opracowania – rozważania omawiające stan aktualny prawa europejskiego o charakterze antyterrorystycznym, należy dodać, że pozostaje ono zgodne z innymi działaniami normatywnymi wspólnoty międzynarodowej kreowanymi w szczególności w ramach Organizacji Narodów Zjednoczonych i Rady Europy oraz w swoisty sposób jest nimi inspirowane. Spośród tych działań bez wątpienia na plan pierwszy wysuwa się Konwencja Rady Europy o zapobieganiu terroryzmowi[61], sporządzona w Warszawie 16 maja 2005 r.,

[57] Dz. Urz. UE L 130/1 z 1 V 2014 r.

[58] Dz. Urz. UE L 315/57 z 14 XI 2012 r.

[59] Dz. Urz. UE L 261/2 z 6 VIII 2004 r.

[60] Dz. Urz. UE L 141/73 z 5 VI 2015 r.

[61] DzU z 2008 r. nr 161 poz. 998.

której celem, zgodnie z jej art. 2, jest wzmocnienie wysiłków Stron w zapobieganiu terroryzmowi i negatywnym skutkom, jakie terroryzm wywiera na pełne korzystanie z praw człowieka, w szczególności prawa do życia, zarówno poprzez środki podejmowane na poziomie krajowym, jak i poprzez współpracę międzynarodową, z należytym uwzględnieniem istniejących wielostronnych lub dwustronnych traktatów lub porozumień między Stronami. Jak wskazywano w uzasadnieniu do wniosku o ratyfikację tej Konwencji, jest ona (...) *pierwszym aktem prawa międzynarodowego, którego celem jest kompleksowe uregulowanie współpracy międzypaństwowej – nie w zakresie zwalczania i karania popełnionych już przestępstw o charakterze terrorystycznym – ale w dziedzinie zapobiegania terroryzmowi. Jej celem jest penalizacja czynów poprzedzających i przygotowujących dokonanie aktu terrorystycznego*[62].

Perspektywy i wyzwania regulacyjne prawa polskiego na tle działań legislacyjnych organów UE

Mówiąc o perspektywach i wyzwaniach regulacyjnych prawa polskiego na tle działań legislacyjnych organów UE, należy zacząć od swoistego podsumowania procesu implementacji postanowień przytaczanej już dyrektywy 2017/541 w sprawie zwalczania terroryzmu, który powinien zakończyć się do 8 września 2018 r. Należy zwrócić uwagę, że zgodnie z art. 29 tej dyrektywy, do 8 marca 2020 r. Komisja miała przedstawić Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym oceniła, w jakim zakresie państwa członkowskie przyjęły środki niezbędne do wykonania tej dyrektywy, do 8 września 2021 r. zaś Parlamentowi Europejskiemu i Radzie – sprawozdanie oceniające uzyskane wartości wynikające ze stosowania niniejszej dyrektywy. Komisja Europejska w opracowanym dla Parlamentu Europejskiego raporcie ewaluacyjnym w sprawie stopnia implementacji i zastosowania na szczeblu krajowym tzw. dyrektywy antyterrorystycznej (datowanym na 24 listopada 2021 r.)[63]

[62] *Uzasadnienie do wniosku o ratyfikację Konwencji Rady Europy o zapobieganiu terroryzmowi*, https://archiwum.bip.kprm.gov.pl/ftp/kprm/dokumenty/070423u2uz.pdf [dostęp: 3 XII 2021].

[63] Raport nr 13478/21 from the Commission to he European Parliament and the Council based on Article 29(2) of Directive (EU) 2017/541 of the European Parliament and of the Ciuncil of 15 March 2017 on combating terrorism and replacing Council Framework

wskazała na konieczność ustanowienia pojedynczych punktów kontaktowych dla ofiar terroryzmu, których – zgodnie z raportem – wciąż brakuje w Polsce. Może to w nadchodzącej przyszłości niekorzystnie wpływać na proces uzyskiwania pomocy lub sprawnego dochodzenia roszczeń związanych z aktem terrorystycznym, pod którego wpływem ucierpieli polscy obywatele. W raporcie podkreślono m.in., że planowane działania Komisji będą się koncentrować na zwiększeniu poziomu ochrony oraz przyjęciu efektywnych działań na rzecz usprawnienia sytuacji ofiar terroryzmu.

W dokumencie tym wskazano również, że dalsze prace Komisji będą ukierunkowane na dokonanie przeglądu działań mających na celu przeciwdziałanie brutalnemu ekstremizmowi w państwach członkowskich UE. W ramach tego działania pojawiają się plany szczególnej dyskusji w gronie państw członkowskich, poświęconej stosowaniu wdrożonych przepisów dyrektywy do brutalnych aktów terrorystycznych o charakterze ultraprawicowym.

Przedstawiając perspektywy kierunków działań legislacyjnych UE wyznaczających trendy zmian w prawie krajowym, należy zwrócić uwagę na opublikowany 24 lipca 2020 r. przez Komisję Europejską komunikat w sprawie strategii UE w zakresie unii bezpieczeństwa[64]. Jak wskazuje A. Kozioł, strategia ta (...) *ma na celu wsparcie państw członkowskich w walce ze zmieniającymi się zagrożeniami i budowę odporności w perspektywie długoterminowej przez zwalczanie klasycznych i hybrydowych zagrożeń w środowisku fizycznym i cyfrowym*[65].

Analizując poszczególne rozważania strategii, zwraca uwagę, że w jej pkt 2 pt. *Szybko zmieniający się krajobraz zagrożeń dla bezpieczeństwa w Europie* wskazano, że:

> (...) kryzys związany z COVID-19 uwidocznił również, że podziały społeczne i prekaryjność są źródłem podatności na zagrożenia dla bezpieczeństwa. Rośnie przez to ryzyko bardziej wyrafinowanych i hybrydowych ataków podmiotów państwowych i niepaństwowych wykorzystujących słabe punkty. Sprawcy posługują się

Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

[64] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0605&from=EN [dostęp: 15 II 2022].

[65] A. Kozioł, *Nowy plan zwalczania terroryzmu w UE*, „Biuletyn Polskiego Instytutu Spraw Międzynarodowych" 2021, nr 33 (2231).

> kombinacją cyberataków, niszczenia infrastruktury krytycznej, kampanii dezinformacyjnych i radykalizacji postaw w ramach narracji politycznej. Zmienia się charakter również tych zagrożeń, z którymi mieliśmy do czynienia już od długiego czasu. W 2019 r. w UE odnotowano tendencję spadkową, jeśli chodzi o ataki terrorystyczne. Wciąż duże zagrożenie dla obywateli UE stanowią jednak ataki dżihadystów organizowane z inicjatywy lub inspiracji Daisz i Al-Kaidy oraz powiązanych z nimi grup. Równocześnie wzrasta również zagrożenie ze strony brutalnego ekstremizmu prawicowego. Powodem do poważnych obaw są ataki o podłożu rasistowskim: antysemickie ataki terrorystyczne w Halle, które pociągnęły za sobą ofiary śmiertelne, przypomniały o potrzebie wzmożenia reakcji zgodnie z deklaracją Rady z 2018 r. Jedna na pięć osób w UE poważnie obawia się, że w ciągu najbliższych 12 miesięcy może nastąpić atak terrorystyczny. Zdecydowaną większość niedawnych ataków terrorystycznych stanowiły ataki przy zastosowaniu niezaawansowanej technologii, skierowane przez pojedynczych sprawców przeciwko osobom fizycznym w przestrzeni publicznej. Propaganda terrorystyczna w internecie nabrała nowego znaczenia za sprawą transmisji strumieniowej na żywo ataków w Christchurch. Zagrożenie ze strony osób o radykalnych poglądach pozostaje duże; może je jeszcze zwiększyć powrót zagranicznych bojowników terrorystycznych i ekstremistów wypuszczonych z więzienia[66].

W tym punkcie zwraca się również uwagę, że (...) *przestępcy i terroryści mają coraz łatwiejszy dostęp do broni palnej: mogą ją kupić na rynku internetowym albo wyprodukować dzięki nowym technologiom takim jak drukowanie przestrzenne*[67].

Z kolei w pkt 3 strategii pt. *Skoordynowana reakcja UE służąca całemu społeczeństwu* podkreśla się konieczność współdziałania wszystkich podmiotów w sektorze publicznym i prywatnym, gdyż zauważa się, że w obu tych sektorach ich główni gracze niechętnie dzielą się informacjami dotyczącymi bezpieczeństwa, co jest spowodowane albo obawami o naruszenie bezpieczeństwa narodowego, albo względami konkurencyjności.

---

[66] *Komunikat Komisji w sprawie strategii UE w zakresie unii bezpieczeństwa sporządzony w Brukseli dnia 24.7.2020 COM(2020) 605 final*, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0605&from=EN [dostęp: 3 XII 2021].

[67] Tamże.

Największą skuteczność działania zapewnia jednak współpraca. W pierwszej kolejności oznacza to intensywniejszą współpracę między państwami członkowskimi, w tym między organami ścigania, organami wymiaru sprawiedliwości i innymi organami publicznymi, a także współpracę z instytucjami i agencjami Unii w celu budowy porozumienia i komunikacji, co jest niezbędne do wypracowania wspólnych rozwiązań. Współpraca z sektorem prywatnym ma kluczowe znaczenie również z tego względu, że sektor przemysłowy jest właścicielem dużej części cyfrowej i niecyfrowej infrastruktury, która jest niezbędna do skutecznego zwalczania przestępczości i terroryzmu[68].

Strategia wyraźnie identyfikuje cztery strategiczne priorytety dla unii bezpieczeństwa: po pierwsze, środowisko bezpieczeństwa, które wytrzyma próbę czasu; po drugie, zajmowanie się ewoluującymi zagrożeniami; po trzecie, ochrona Europejczyków przed terroryzmem i przestępczością zorganizowaną; po czwarte, silny europejski ekosystem bezpieczeństwa.

W ramach pierwszego priorytetu położono nacisk na ochronę infrastruktury krytycznej i jej odporność, cyberbezpieczeństwo oraz ochronę przestrzeni publicznej. W ramach działań na rzecz poprawy cyberbezpieczeństwa wskazano, że musi ono przebiegać równolegle z walką z terroryzmem, ekstremizmem, radykalizmem i zagrożeniami hybrydowymi, a rozwiązania należy upatrywać w lepszych formach współpracy między służbami wywiadowczymi, Centrum Analiz Wywiadowczych UE i innymi organizacjami zajmującymi się bezpieczeństwem. Mówiąc zaś o ochronie przestrzeni publicznej, podkreślono, że:

> (...) niedawne ataki terrorystyczne były wymierzone w przestrzeń publiczną, w tym w miejsca kultu i węzły transportowe, z uwagi na jej otwarty i ogólnodostępny charakter. Nasilenie terroryzmu motywowanego ekstremizmem na tle politycznym lub ideologicznym sprawiło, że zagrożenie atakami nabrało jeszcze bardziej poważnego charakteru. Sytuacja ta wymaga zarówno ściślejszej ochrony fizycznej przestrzeni publicznej, jak i odpowiednich systemów wykrywania, bez uszczerbku dla swobód obywatelskich. Komisja zacieśni publiczno-prywatną współpracę w celu ochrony przestrzeni publicznej poprzez dostarczenie finansowania, wymianę doświadczeń i dobrych praktyk oraz konkretne wytyczne i zalecenia.

[68] Tamże.

> Podejście to będzie również obejmować podnoszenie świadomości, wprowadzenie wymogów dotyczących działania sprzętu do wykrywania zagrożeń i testowanie tego sprzętu, a także dokładniejsze sprawdzanie przeszłości osób w celu zapobiegania zagrożeniom wewnętrznym[69].

Zwrócono również uwagę, że rynek dronów stale się rozwija i generuje dodatkowe zagrożenia, gdyż urządzenia te mogą być używane przez przestępców i terrorystów do celów niezgodnych z prawem. Narażone są zwłaszcza przestrzenie publiczne, infrastruktura krytyczna, organy ścigania, granice państw, a nawet pojedyncze osoby fizyczne, które mogą być zaatakowane z ich użyciem. Komisja Europejska zwraca uwagę, że działania podjęte przez Europejską Agencję Bezpieczeństwa Lotniczego w zakresie m.in. rejestracji operatorów dronów i obowiązkowej zdalnej ich identyfikacji stanowią pierwszy krok. Konieczne są jednak dalsze działania, które powinny obejmować wymianę informacji, opracowanie wytycznych i dobrych praktyk do powszechnego użytku, w tym przez organy ścigania, czy też testowanie na szerszą skalę środków ochrony przed dronami.

W ramach drugiego priorytetu określono działania, które powinny być podjęte w obliczu zmieniających się zagrożeń. Zaliczono do nich cyberprzestępczość, zwalczanie nielegalnych treści w internecie i zagrożenia hybrydowe. Mówiąc o zwalczaniu nielegalnych treści w internecie, w strategii zwraca się uwagę, że wiele poważnych zagrożeń dla obywateli, takich jak m.in. terroryzm, szerzy się głównie w środowisku cyfrowym, a walka z nimi wymaga konkretnych działań zapewniających poszanowanie praw podstawowych.

Niezbędnym pierwszym krokiem jest szybkie zakończenie negocjacji w sprawie proponowanych przepisów dotyczących internetowych treści o charakterze terrorystycznym oraz zapewnienie ich wdrożenia. Pomocne w walce z wykorzystywaniem internetu przez terrorystów, brutalnych ekstremistów i przestępców do celów niezgodnych z prawem byłoby zacieśnienie dobrowolnej współpracy między organami ścigania a sektorem prywatnym w ramach Forum UE ds. Internetu[70].

Dla organów Unii istotnego znaczenia nabiera działająca w Europolu unijna jednostka ds. zgłaszania podejrzanych treści w internecie,

[69] Tamże.

[70] Tamże.

która ma nadal odgrywać kluczową rolę w monitorowaniu aktywności grup terrorystycznych w internecie i reakcji platform internetowych na tę aktywność.

Ważnym elementem strategii w kontekście terroryzmu jest priorytet trzeci, a w szczególności jego część pierwsza pt. *Terroryzm i radykalizacja postaw*, w której podkreślono, że zagrożenie terrorystyczne w UE jest nadal wysokie, główna odpowiedzialność zaś za zwalczanie terroryzmu i radykalizacji nadal spoczywa na państwach członkowskich. Niemniej jednak w obliczu wciąż rosnącego transgranicznego i międzysektorowego wymiaru zagrożenia konieczne jest rozwijanie współpracy i koordynacji w UE. Skuteczne wdrażanie unijnych przepisów o zwalczaniu terroryzmu, w tym środków ograniczających, ma priorytetowe znaczenie. Jednym z celów pozostaje objęcie transgranicznych przestępstw terrorystycznych zakresem kompetencji Prokuratury Europejskiej[71].

Zgodnie z dokumentem, działania Unii w tym zakresie będą koncentrować się na:

- przeciwdziałaniu radykalizacji połączonym ze wspieraniem spójności społecznej na szczeblu lokalnym, krajowym i europejskim;
- ograniczeniu dostępności materiałów chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ) oraz prekursorów materiałów wybuchowych, które mogą być przekształcane w broń wykorzystywaną do przeprowadzania ataków;
- skutecznym ściganiu sprawców przestępstw terrorystycznych, w tym zagranicznych bojowników terrorystycznych. Istotne w tym kontekście są trwające działania na rzecz pełnego wdrożenia przepisów o bezpieczeństwie granic i jak największego wykorzystania wszystkich odnośnych baz danych UE w celu wymiany informacji na temat znanych osób podejrzanych;
- rozwijaniu partnerstw antyterrorystycznych i współpracy z krajami w sąsiedztwie UE i poza nim, z wykorzystaniem wiedzy wypracowanej w ramach sieci unijnych ekspertów ds. bezpieczeństwa i zwalczania terroryzmu.

W ramach priorytetu czwartego zakładającego budowę silnego europejskiego ekosystemu bezpieczeństwa podkreślono, że opierać się on musi na czterech elementach, tj.: współpracy i wymianie informacji, znaczeniu silnych granic zewnętrznych, udoskonalaniu badań

[71] Tamże.

i innowacji w dziedzinie bezpieczeństwa oraz rozwijaniu umiejętności i zwiększaniu świadomości.

Bez wątpienia przedłożony przez Komisję plan oferuje wiele nowych rozwiązań, które z założenia podnieść mają skuteczność współpracy organów UE i państw członkowskich. Działania te będą wymagały jednak wielopoziomowych działań regulacyjnych Unii Europejskiej i ich późniejszej implementacji w państwach członkowskich, w czym osiągnięcie konsensusu może być problematyczne.

Bez wątpienia do takich wyzwań należeć będzie właściwe wdrożenie postanowień *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*[72], które wejdzie w życie 7 czerwca 2022 r. Podstawowym założeniem tego aktu normatywnego jest ustanowienie zharmonizowanych ram prawnych na potrzeby zapobiegania wykorzystywaniu Internetu do rozpowszechniania treści propagujących terroryzm poprzez wprowadzenie mechanizmu wydawania i weryfikowania nakazów usunięcia treści o charakterze terrorystycznym lub uniemożliwienia do nich dostępu.

Co istotne, w Polsce ABW ma obecnie, zgodnie z art. 32c ustawy o ABW oraz AW (dodanym ustawą o działaniach antyterrorystycznych), możliwość stosowania tzw. blokady dostępności, tzn. w celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, w drodze postanowienia może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym.

Analizując jednak przedmiotowe rozporządzenie, uprawnienia właściwego organu w tym zakresie powinny być zdecydowanie szersze i uwzględniać możliwość korzystania zarówno ze środków operacyjnych, jak i prawno-administracyjnych w ramach ustanowionego mechanizmu zabezpieczającego rynek cyfrowy przed zagrożeniami

[72] Dz. Urz. UE L 172/79 z 17 V 2021 r.

o charakterze terrorystycznym. W konsekwencji więc niezbędne będzie dokonanie zmian w prawie krajowym obejmujące:

- wskazanie organu właściwego do realizacji nowych zadań wynikających z rozporządzenia, w tym wydawania nakazów usunięcia (art. 3 rozporządzenia), weryfikowania nakazów usunięcia (art. 4 rozporządzenia), przedłużania okresu zachowania treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony na skutek wydanego nakazu usunięcia (art. 6 ust. 2 rozporządzenia), wydawania decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych (art. 5 rozporządzenia), nakładania kar administracyjnych (art. 18 rozporządzenia), publikacji sprawozdania (art. 8 rozporządzenia), przekazywania do Komisji Europejskiej rocznej informacji na podstawie art. 21 rozporządzenia;
- wyznaczenie przez organ właściwy punktu kontaktowego w celu realizacji zadań określonych w rozporządzeniu;
- ustanowienie mechanizmu skargowego w odniesieniu do wydanych nakazów usunięcia oraz innych decyzji wydawanych przez organ właściwy w związku z wykonywaniem zadań określonych w rozporządzeniu;
- wprowadzenie przepisów regulujących nakładanie administracyjnych kar pieniężnych przez organ właściwy za określone w rozporządzeniu naruszenia;
- ustanowienie mechanizmu monitorującego stosowanie rozporządzenia i przekazywanie w tym zakresie rocznej informacji do wiadomości Komisji Europejskiej.

Podsumowując rozważania niniejszej części, należy wskazać, że główna oś prac legislacyjnych Unii Europejskiej w obszarze przeciwdziałania terroryzmowi będzie w nadchodzącym czasie koncentrować się na wdrożeniu omówionej strategii UE w zakresie unii bezpieczeństwa oraz właściwej implementacji w państwach członkowskich poszczególnych regulacji będących jej wynikową.

Podsumowanie

Podsumowując rozważania podjęte w niniejszym artykule, należy wskazać po pierwsze, że na poziomie krajowym wprowadzona w 2016 r. ustawa o działaniach antyterrorystycznych zmieniała model ustawodawstwa antyterrorystycznego z rozproszonego modelu materialnego na skoncentrowany model formalny. W ten sposób ustawa ta, wraz z uchwaloną 1 marca 2018 r. nową ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, stała się filarem krajowych regulacji prawnych, które bezpośrednio kształtują rdzeń obszaru walki z terroryzmem.

Po drugie, antyterrorystyczne prawodawstwo europejskie jest wysoce zróżnicowane, zarówno pod względem charakteru źródła prawa – co bezpośrednio przekłada się na zakres mocy jego oddziaływania, jak i dualistycznej metodologii przedmiotowego sposobu regulowania problematyki terroryzmu, w związku z czym poszczególne zagadnienia ujmowane są w wyodrębniony zakresowo przedmiotowy akt normatywny albo też są ujmowane łącznie z innymi uregulowaniami obszaru bezpieczeństwa. Ich kształt zbliża się więc do modelu materialnego.

Po trzecie, przechodząc do poziomu prognoz, na podstawie analizy działań podsumowujących proces implementacji tzw. dyrektywy antyterrorystycznej oraz postanowień przyjętej strategii UE w zakresie unii bezpieczeństwa, należy wskazać, że działania legislacyjne UE będą przebiegały w kierunku dalszego zbliżenia prawodawstwa poszczególnych państwach członkowskich, zwłaszcza w zakresie jednolitego definiowania takich pojęć, jak „przestępstwo terrorystyczne", „przestępstwo dotyczące grupy terrorystycznej" oraz „przestępstwo związane z działalnością terrorystyczną", tak by definicje te obejmowały w sposób kompleksowy czyny związane w szczególności z działalnością zagranicznych bojowników terrorystycznych oraz kwestie finansowania terroryzmu. Dużego znaczenia nabiera też objęcie ich zakresem działań za pośrednictwem Internetu, w tym mediów społecznościowych. Transgraniczny charakter terroryzmu wymaga prowadzenia zdecydowanych, skoordynowanych działań i współpracy zarówno organów odpowiedzialnych za bezpieczeństwo w państwach członkowskich, jak i współpracy w tym zakresie między poszczególnymi państwami członkowskimi. Taka sama współpraca powinna być prowadzona między instytucjami państw członkowskich a właściwymi agencjami i organami Unii zajmującymi się zwalczaniem terroryzmu, w tym Eurojustem

i Europolem. Dodatkowo globalny charakter terroryzmu wymaga podjęcia działań na szczeblu międzynarodowym, co oznacza, że Unia i jej państwa członkowskie muszą i będą działać w kierunku zacieśniania współpracy z odpowiednimi państwami trzecimi. Dalsze prace Komisji mają być ukierunkowane na dokonanie przeglądu działań mających na celu przeciwdziałanie brutalnemu ekstremizmowi w państwach członkowskich UE, co bez wątpienia pozostanie elementem dyskusji politycznej i prawnej, zwłaszcza w kontekście wyraźnej próby pozostawienia poza debatą publiczną problematyki ekstremizmu o podłożu lewicowym.

Należy podkreślić, że walki z terroryzmem nigdy nie można uznać za temat zamknięty i zakończony, przeciwnie – przeobrażenia w charakterze zagrożeń terrorystycznych zmuszają do nieustanych działań nakierowanych na ich identyfikację, a w konsekwencji zmianę stanu prawnego, zarówno na poziomie krajowym, jak i międzynarodowym.

Bibliografia

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

Kozioł A., *Nowy plan zwalczania terroryzmu w UE*, „Biuletyn Polskiego Instytutu Spraw Międzynarodowych" 2021, nr 33 (2231).

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.

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

Żaryn S., *Polska antyterrorystycznym wzorem*, wGospodarce.pl, https://wgospodarce.pl/opinie/58189-polska-antyterrorystycznym-wzorem [dostęp: 25 XI 2021].

DOI: 10.4467/27204383TER.22.003.15419

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

MARIUSZ CICHOMSKI
ILONA IDZIKOWSKA-ŚLĘZAK

Poziom strategiczny polskiego systemu antyterrorystycznego – 15 lat Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych

Abstrakt

Artykuł ma na celu podsumowanie 15 lat funkcjonowania, powołanego Zarządzeniem nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r., Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, a także przedstawienie ewolucji realizowanych przez to gremium zadań. Zespół działający pod przewodnictwem ministra właściwego do spraw wewnętrznych i składający się z szefów resortów, służb i innych podmiotów realizujących zadania związane z zagrożeniami terrorystycznymi wyznacza podstawowe kierunki działań państwa w obszarze zapobiegania, przygotowania i reagowania na zagrożenia terrorystyczne. Jako organ pomocniczy Rady Ministrów m.in. monitoruje zagrożenia o charakterze terrorystycznym oraz przedstawia opinie i wnioski dla Rady Ministrów. W ramach prowadzonych prac przygotowywane są również propozycje zmierzające do usprawnienia metod i form przeciwdziałania zagrożeniom o charakterze terrorystycznym oraz wnioski do właściwych organów o podjęcie prac legislacyjnych. Działalność Zespołu nie ogranicza się jednak do sfery legislacji i dotyczy m.in. wypracowywania praktycznych rekomendacji mających na celu poprawę bezpieczeństwa antyterrorystycznego obiektów

Słowa kluczowe:

terroryzm, poziom strategiczny, koordynacja działań służb, legislacja, rozwiązania systemowe

mogących stanowić potencjalny cel ataku czy też uzgadniania procedur współdziałania właściwych służb, a także przygotowywania materiałów profilaktycznych skierowanych do różnych grup odbiorców. Działalność Zespołu została pozytywnie oceniona m.in. podczas ewaluacji przeprowadzonej przez ekspertów ONZ w grudniu 2019 r.

W październiku 2006 r., czyli 15 lat temu, utworzony został Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych[1] (MZds.ZT), który mimo diametralnych zmian w zakresie prawnym i organizacyjnym, jakie nastąpiły od tego czasu w polskim systemie antyterrorystycznym, stanowi do dnia dzisiejszego poziom strategiczny tego systemu i (...) *zapewnia współdziałanie administracji rządowej w zakresie przygotowania do zapobiegania zdarzeniom o charakterze terrorystycznym, przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć oraz do reagowania na nie*[2].

Niniejszy artykuł ma na celu podsumowanie 15 lat funkcjonowania MZds.ZT, a także przedstawienie, w jaki sposób ewoluowały realizowane przez to gremium zadania w zależności od aktualnych potrzeb wynikających ze zmieniających się zagrożeń o charakterze terrorystycznym, jak również zmian otoczenia prawnego regulującego funkcjonowanie polskiego systemu antyterrorystycznego. Opisane w artykule inicjatywy Zespołu, zmiany dotyczące zasad jego działania, ich uwarunkowania

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

[2] Tamże, § 2 ust. 1.

oraz oceny formułowane przez podmioty zewnętrzne mogą stanowić podstawę do odpowiedzi na pytania, na jakiego rodzaju zadaniach powinna koncentrować się aktywność niniejszego gremium oraz w jakim stopniu podejmowane w jego ramach inicjatywy przekładają się na funkcjonowanie całego systemu antyterrorystycznego.

Podstawę prawną utworzenia MZds.ZT stanowiło – i do dziś pozostaje aktualne – upoważnienie ogólne zawarte w *Ustawie z dnia 8 sierpnia 1996 r. o Radzie Ministrów*[3], zgodnie z którym Prezes Rady Ministrów (PRM), z własnej inicjatywy lub na wniosek członka Rady Ministrów (RM), może, w drodze zarządzenia, tworzyć organy pomocnicze Rady Ministrów lub Prezesa Rady Ministrów, a w szczególności rady i zespoły opiniodawcze lub doradcze w sprawach należących do zadań i kompetencji RM lub PRM. Prezes Rady Ministrów, tworząc tego rodzaju organy pomocnicze, określa ich nazwę, skład, zakres działania oraz tryb postępowania. Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych nie powstał zatem na podstawie szczególnej normy prawnej osadzonej w ustawodawstwie normującym zagadnienia dotyczące zagrożeń terrorystycznych, tylko generalnej normy stanowiącej podstawę dla tworzenia różnego typu organów pomocniczych.

Jak wspomniano powyżej, MZds.ZT jest powszechnie uznanym liderem poziomu strategicznego polskiego systemu antyterrorystycznego. Rola ta nie została usankcjonowana ustawowo, ale jest zwyczajowo wykorzystywana zarówno w dokumentach o charakterze analitycznym, jak i w formalnych dokumentach rządowych czy podczas międzynarodowych misji ewaluacyjnych dotyczących oceny różnych aspektów przygotowania Polski do radzenia sobie z zagrożeniami terrorystycznymi, m.in. w ocenach prowadzonych przez Komitet Ekspertów w przedmiocie ewaluacji metod przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu – MONEYVAL, działający przy Radzie Europy. Przykładem zaś formalnego dokumentu o charakterze rządowym określającym MZds.ZT jako poziom strategiczny polskiego systemu antyterrorystycznego, może być *Narodowy Program Antyterrorystyczny na lata 2015–2019*, który został przyjęty na podstawie *Ustawy z dnia 6 grudnia*

[3] Na podstawie art. 12 ust. 1 pkt 3 i ust. 2 tej ustawy (t.j.: DzU z 2021 r. poz. 178, ze zm.).

2006 r. o zasadach prowadzenia polityki rozwoju[4] jako uchwała Rady Ministrów[5]. W *Programie* zapisano:

> W przyjętym w Polsce systemie antyterrorystycznym RP wyróżnić można trzy poziomy:
> - strategiczny – w ramach którego podejmowane są przez Prezesa Rady Ministrów i Radę Ministrów kluczowe działania o charakterze systemowym w zakresie ochrony antyterrorystycznej kraju. Tworzenie polityki antyterrorystycznej państwa należy także do zadań organów opiniodawczo-doradczych, tj. Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, Kolegium ds. Służb Specjalnych i Rządowego Zespołu Zarządzania Kryzysowego (RZZK). Szczególną rolę w systemie odgrywa również minister właściwy do spraw wewnętrznych;
> - operacyjny – w ramach którego realizowane są zadania służące koordynacji wymiany informacji między poszczególnymi służbami i instytucjami wchodzącymi w skład systemu antyterrorystycznego RP, a także prowadzony jest bieżący monitoring i analiza zagrożeń o charakterze terrorystycznym. Zadania na tym poziomie koordynuje Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego oraz w odniesieniu do kwestii związanych z zarządzaniem kryzysowym Rządowe Centrum Bezpieczeństwa (RCB);
> - taktyczny – wykonywany przez poszczególne służby, organy i instytucje, w których zakresie właściwości pozostaje antyterrorystyczna ochrona kraju[6].

Doprecyzowując rolę MZds.ZT jako poziomu strategicznego systemu antyterrorystycznego, w *Programie* wskazano:

> Istotną rolę w zakresie wyznaczania podstawowych kierunków działań państwa w obszarze zapobiegania, przygotowania i reagowania na zagrożenia terrorystyczne odgrywa Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych będący organem pomocniczym Rady Ministrów. Do zadań Zespołu należy m.in. monitorowanie zagrożeń o charakterze terrorystycznym, ich analiza i ocena oraz przedstawianie opinii i wniosków dla Rady Ministrów.

[4] Na podstawie art. 19 ust. 2 tej ustawy (DzU z 2021 r. poz. 1057).

[5] *Uchwała nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (MP z 2014 r. poz. 1218).

[6] Tamże.

> Ważnym zadaniem Zespołu jest także inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej w zakresie zapobiegania przygotowania i reagowania na zagrożenia terrorystyczne. W ramach prowadzonych prac przygotowywane są również propozycje zmierzające do usprawnienia metod i form przeciwdziałania zagrożeniom o charakterze terrorystycznym, wraz z możliwością występowania z wnioskiem do właściwych organów o podjęcie prac legislacyjnych. Przewodniczący MZds.ZT może powoływać spośród członków i osób zaproszonych do udziału w jego pracach z głosem doradczym zespoły zadaniowe w celu realizacji konkretnych zadań[7].

Jak zasygnalizowano na wstępie, MZds.ZT powstawał w diametralnie innym otoczeniu organizacyjnym i prawnym polskiego systemu antyterrorystycznego. Owo otoczenie organizacyjne, rozumiane na potrzeby niniejszego opracowania jako ramy instytucjonalne systemu, miało, w porównaniu do stanu obecnego, istotne ograniczenia w zakresie mechanizmów koordynacji i wsparcia współdziałania służb i innych podmiotów w odniesieniu do zagrożeń terrorystycznych. Posługując się przytoczonym powyżej wyodrębnieniem w systemie antyterrorystycznym trzech poziomów, podkreślić należy, że ówcześnie nie funkcjonowało jeszcze Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego, które zapewnia koordynację współdziałania i wymiany informacji w trybie całodobowym przy wykorzystaniu zasobów informacyjnych wszystkich uczestników systemu antyterrorystycznego. Nie istniało również Rządowe Centrum Bezpieczeństwa jako jednostka wspierająca wymianę informacji o zagrożeniach z perspektywy zarządzania kryzysowego. Z perspektywy prawnej zaś zaznaczyć należy, że nie tylko zakres uprawnień i sposób określenia zadań poszczególnych służb był węższy i mniej doprecyzowany, lecz przede wszystkim nie było ustawy normującej kluczowe mechanizmy koordynacyjne, jaką dopiero po latach z perspektywy momentu powołania MZds.ZT stała się *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[8].

W kontekście różnic systemowych przez lata modyfikowana również zadania przypisane MZds.ZT. Z czasem mniejszego znaczenia nabierały te związane z monitorowaniem i prognozowaniem zagrożeń, ważniejsze

[7] Tamże.

[8] DzU z 2021 r. poz. 2234.

natomiast stawały się te ukierunkowane na podejmowanie inicjatyw o charakterze systemowym. Przekształceniu uległ też sam sposób określania zadań poprzez ich dopasowanie do terminologii stosowanej w ustawie o działaniach antyterrorystycznych. Zmiany te zaprezentowano w poniższej tabeli.

Tabela. Zmiana zakresu zadań MZds.ZT.

MZds.ZT w 2006 r.	MZds.ZT w 2021 r.	Komentarz
Cel powołania		
Zespół zapewnia współdziałanie administracji rządowej w zakresie rozpoznawania, przeciwdziałania i zwalczania terroryzmu	Zespół zapewnia współdziałanie administracji rządowej w zakresie przygotowania do zapobiegania zdarzeniom o charakterze terrorystycznym, przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć oraz do reagowania na nie	Dostosowano terminologię do ustawy o działaniach antyterrorystycznych
Zadania		
Monitorowanie zagrożeń o charakterze terrorystycznym, ich analiza i ocena, a także przedstawianie opinii i wniosków dla Rady Ministrów	Monitorowanie zagrożeń o charakterze terrorystycznym, ich analiza i ocena, a także przedstawianie opinii i wniosków Radzie Ministrów	Nie dokonano zmian w tym zakresie
Opracowywanie projektów standardów i procedur w zakresie zwalczania terroryzmu, w szczególności standardów oceny występowania zagrożenia i określania jego poziomu	Opracowywanie projektów standardów i procedur w zakresie reagowania w przypadku wystąpienia zdarzeń o charakterze terrorystycznym	Dostosowano terminologię do ustawy o działaniach antyterrorystycznych, stąd zmiana wyrazu „zwalczanie" na „reagowanie" – ustawa o działaniach antyterrorystycznych wyróżnia cztery fazy działań: zapobieganie, przygotowywanie, reagowanie i odbudowę. Zrezygnowano z odwołania do opracowywania standardów i procedur w zakresie oceny występowania zagrożenia i określania jego poziomu – kwestia ta została unormowana w ustawie o działaniach antyterrorystycznych

Inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej, w szczególności w zakresie wykorzystania informacji oraz rozpoznawania, przeciwdziałania i zwalczania terroryzmu	Inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej w zakresie przygotowania do zapobiegania zdarzeniom o charakterze terrorystycznym, przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć oraz do reagowania na nie	Dostosowano terminologię i zakres do ustawy o działaniach antyterrorystycznych
Występowanie z wnioskiem do właściwych ministrów w celu podjęcia działań legislacyjnych zmierzających do usprawnienia metod i form zwalczania terroryzmu	Opracowywanie propozycji zmierzających do usprawnienia metod i form zapobiegania zdarzeniom o charakterze terrorystycznym, przygotowania do przejmowania kontroli nad tymi zdarzeniami i reagowania w przypadku wystąpienia takich zdarzeń oraz występowanie z wnioskiem do właściwych organów o podjęcie w tym zakresie prac legislacyjnych	Doprecyzowano zakres zadania i dostosowano terminologię i zakres do ustawy o działaniach antyterrorystycznych
Organizowanie współpracy z innymi państwami w zakresie zwalczania terroryzmu oraz koordynacja wymiany informacji i organizowanych wspólnych operacji	Nie uwzględniono tego rodzaju zadań	Koordynacja wymiany informacji odbywa się na poziomie operacyjnym systemu antyterrorystycznego i na podstawie ustawy o działaniach antyterrorystycznych stanowi zadanie Szefa ABW – art. 4–8 ustawy. Natomiast współpraca z innymi państwami realizowana jest przez poszczególne służby i inne podmioty systemu zarówno w drodze kontaktów bezpośrednich w ramach współpracy bilateralnej ze służbami partnerskimi, jak i poprzez wytypowane do tych zagadnień gremia i agendy organizacji międzynarodowych

Inicjowanie szkoleń i konferencji dotyczących zwalczania terroryzmu	Nie uwzględniono tego rodzaju zadań	Zrezygnowano z zadania – kwestia ta jest domeną poszczególnych służb i instytucji, a nie organu pomocniczego Rady Ministrów. W celu realizacji głównych inicjatyw szkoleniowych powołane zostało Centrum Prewencji Terrorystycznej ABW – utworzenie CPT ABW bezpośrednio wpisuje się w art. 3 ust. 1 ustawy o działaniach antyterrorystycznych, wskazujący Szefa ABW jako odpowiedzialnego za zapobieganie zagrożeniom antyterrorystycznym

W okresie funkcjonowania MZds.ZT również jego skład był dostosowywany z jednej strony – co oczywiste – do zmieniającej się struktury organizacyjnej administracji publicznej (przykładowo: przekształcenie Służby Celnej w Służbę Celno-Skarbową jako element Krajowej Administracji Skarbowej, przekształcenie Biura Ochrony Rządu w Służbę Ochrony Państwa czy utworzenie Rządowego Centrum Bezpieczeństwa), z drugiej zaś strony, co istotniejsze, miał on odpowiadać nowo zdefiniowanym potrzebom wynikającym z coraz szerszego podejścia do zagadnienia zagrożeń terrorystycznych. Obecnie w skład MZds.ZT wchodzą:

- przewodniczący – minister właściwy do spraw wewnętrznych;
- zastępcy – minister właściwy do spraw finansów publicznych, minister właściwy do spraw instytucji finansowych, minister obrony narodowej, minister właściwy do spraw zagranicznych, minister sprawiedliwości, a także minister – członek Rady Ministrów, koordynator Służb Specjalnych;
- sekretarz – osoba powołana przez przewodniczącego Zespołu spośród pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych;
- członkowie:
  - sekretarz stanu lub podsekretarz stanu wyznaczony przez ministra właściwego do spraw wewnętrznych, sprawujący nadzór nad prowadzeniem spraw objętych działem administracji rządowej – sprawy wewnętrzne w zakresie ochrony bezpieczeństwa i porządku publicznego,

- sekretarz stanu lub podsekretarz stanu wyznaczony przez ministra właściwego do spraw wewnętrznych, sprawujący nadzór nad prowadzeniem spraw objętych działem administracji rządowej – sprawy wewnętrzne w zakresie zarządzania kryzysowego, ochrony przeciwpożarowej i obrony cywilnej,
- sekretarz Kolegium do Spraw Służb Specjalnych lub osoba go zastępująca,
- szef Obrony Cywilnej Kraju lub jego zastępca,
- szef Agencji Bezpieczeństwa Wewnętrznego lub jego zastępca,
- szef Agencji Wywiadu lub jego zastępca,
- komendant Służby Ochrony Państwa lub jego zastępca,
- komendant główny Policji lub jego zastępca,
- komendant główny Straży Granicznej lub jego zastępca,
- komendant główny Państwowej Straży Pożarnej lub jego zastępca,
- szef Sztabu Generalnego Wojska Polskiego lub jego zastępca,
- dowódca Operacyjny Rodzajów Sił Zbrojnych lub jego zastępca,
- szef Służby Wywiadu Wojskowego lub jego zastępca,
- szef Służby Kontrwywiadu Wojskowego lub jego zastępca,
- komendant główny Żandarmerii Wojskowej lub jego zastępca,
- Generalny Inspektor Informacji Finansowej lub osoba go zastępująca,
- szef Krajowej Administracji Skarbowej lub jego zastępca,
- dyrektor Rządowego Centrum Bezpieczeństwa lub osoba go zastępująca.

Do udziału w pracach Zespołu, na prawach członka, zapraszany jest prokurator krajowy (lub jego przedstawiciel). W posiedzeniach uczestniczy również przedstawiciel Biura Bezpieczeństwa Narodowego.

Skład, w stosunku do tego z 2006 r., został rozszerzony w szczególności o wskazanych powyżej: ministra sprawiedliwości, szefa Sztabu Generalnego Wojska Polskiego, dowódcę Operacyjnego Rodzajów Sił Zbrojnych, dyrektora Rządowego Centrum Bezpieczeństwa, sekretarza Kolegium do Spraw Służb Specjalnych oraz dopraszanego do udziału w posiedzeniach prokuratora krajowego. Zapewniono zatem nieuwzględniony początkowo udział resortu sprawiedliwości i sformalizowano udział przedstawicieli prokuratury, co jest szczególnie istotne w zakresie kreowania polityki karnej w odniesieniu do penalizacji

przestępstw związanych z zagrożeniami terrorystycznymi (zresztą działalność MZds.ZT przełożyła się na zmiany w Kodeksie karnym). Rozszerzony został także udział przedstawicieli resortu obrony narodowej poprzez bezpośrednie zaangażowanie przedstawicieli Sił Zbrojnych Rzeczypospolitej Polskiej.

Z perspektywy 15-lecia funkcjonowania i po podsumowaniu działań MZds.ZT wydaje się, że najistotniejszą rolę odgrywają te związane z zainicjowaniem zmian legislacyjnych – z których część miała fundamentalne znaczenie dla polskiego systemu antyterrorystycznego – oraz wdrożeniem wspólnych procedur i algorytmów funkcjonowania służb i innych podmiotów oraz oceną zabezpieczenia antyterrorystycznego i wdrożeniem procedur mających na celu podniesienie ich standardów.

W odniesieniu do kwestii regulacji szczególną uwagę należy zwrócić na wspomnianą ustawę o działaniach antyterrorystycznych, *Ustawę z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera*[9] oraz *Ustawę z dnia 17 września 2021 r. o zmianie ustawy – Prawo lotnicze oraz ustawy o Straży Granicznej*[10], dotyczącą szczegółowych sprawdzeń pracowników sektora lotniczego.

Ustawa o działaniach antyterrorystycznych weszła w życie 2 lipca 2016 r., a jej zasadniczym celem – zgodnie z uzasadnieniem – było podniesienie efektywności polskiego systemu antyterrorystycznego, a tym samym zwiększenie bezpieczeństwa wszystkich obywateli RP poprzez wzmocnienie koordynacji działań służb i doprecyzowanie ich zadań, zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń oraz możliwości skuteczniejszego działania w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego, a także dostosowanie przepisów karnych do nowych typów zagrożeń o charakterze terrorystycznym.

O znaczeniu ustawy o działaniach antyterrorystycznych dla polskiego systemu antyterrorystycznego świadczy nie tylko wprowadzenie przez nią nowych rozwiązań prawnych, lecz również integracja jej przepisów z przepisami innych ustaw. Warto zaznaczyć, że ustawą dokonano zmiany treści aż 31 innych ustaw, co związane jest z tym, że mimo jej kompleksowego charakteru w innych aktach prawnych

[9] Tekst jednolity: DzU z 2019 r. poz. 1783.

[10] DzU z 2021 r. poz. 1898.

pozostawiono przepisy dotyczące kwestii przeciwdziałania i zwalczania terroryzmu, których włączenie do ustawy nie byłoby zasadne z punktu widzenia legislacyjnego i funkcjonalnego[11].

Ustawa o działaniach antyterrorystycznych jest również pozytywnie oceniana na arenie międzynarodowej. W grudniu 2019 r. odbyła się w Polsce wizyta Dyrekcji Wykonawczej Organizacji Narodów Zjednoczonych ds. Zwalczania Terroryzmu (UN CTED), której celem było dokonanie ewaluacji wdrożonych przez Polskę rezolucji Rady Bezpieczeństwa ONZ w zakresie walki z terroryzmem. Podczas wizyty zwrócono uwagę na ustawę o działaniach antyterrorystycznych jako na dokument regulujący w sposób kompleksowy podział odpowiedzialności w poszczególnych obszarach działań, a także na ustanowiony tym aktem system stopni alarmowych zgodny z wymogami NATO. Ustawa o działaniach antyterrorystycznych była również wysoko oceniona przez członków Europejskiego Centrum Doskonalenia przeciwko Zagrożeniom Hybrydowym w Helsinkach (HybridCoE), którzy zdecydowali się zaprezentować polskie przepisy jako modelowe rozwiązanie legislacyjne w tym przedmiocie.

Na przykładzie sposobu prowadzenia prac nad tzw. ustawą antyterrorystyczną, czyli późniejszą ustawą o działaniach antyterrorystycznych, widać jednak, że sam efekt zależny jest nie tylko od zaangażowania poziomu eksperckiego Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, lecz także od decyzji na poziomie politycznym, od których zależy rzeczywiste przyjęcie proponowanych przez Zespół rozwiązań. Prace nad spójną regulacją, która normowałaby kwestie antyterrorystyczne, podejmowane były kilkakrotnie i trwały wiele lat[12].

Decyzją Przewodniczącego MZds.ZT z 10 czerwca 2008 r. pod przewodnictwem przedstawiciela Ministerstwa Spraw Wewnętrznych

---

[11] 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. 281–282.

[12] Por. W. Zubrzycki, *Dzieje ustawy Antyterrorystycznej w Polsce*, w: *Polska ustawa antyterrorystyczna…*; a także 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…*

i Administracji został powołany Zespół Zadaniowy do Spraw Usystematyzowania Krajowych Regulacji i Rozwiązań Prawnych Dotyczących Przeciwdziałania Terroryzmowi. Do jego zadań należało m.in. dokonanie przeglądu obowiązujących w Polsce przepisów prawnych dotyczących przeciwdziałania i zwalczania terroryzmu oraz wypracowanie propozycji nowych rozwiązań prawno-organizacyjnych dotyczących zapobiegania i zwalczania zagrożeń terrorystycznych. W sprawozdaniu z prac Zespołu Zadaniowego przedstawiono m.in. założenia projektu ustawy o gromadzeniu i przetwarzaniu informacji w celu rozpoznawania zagrożeń o charakterze terrorystycznym oraz rekomendowano powołanie międzyresortowego zespołu do spraw opracowania ww. projektu ustawy. Następnie, m.in. mając na uwadze ww. rekomendację, decyzją Przewodniczącego MZds.ZT z 12 stycznia 2009 r. został powołany Zespół Zadaniowy do Opracowania Szczegółowych Założeń do Ustawy o Rozpoznawaniu, Przeciwdziałaniu i Zwalczaniu Terroryzmu, działający pod przewodnictwem przedstawiciela Agencji Bezpieczeństwa Wewnętrznego. Mimo przedstawionych przez Zespół Zadaniowy rekomendacji nie zdecydowano o rozpoczęciu procesu legislacyjnego w celu przyjęcia przedmiotowego projektu ustawy, nie opracowano także projektu założeń do projektu ustawy i decyzją ówczesnego kierownictwa MSWiA prace Zespołu zostały zakończone.

Kolejną inicjatywę podjęto w związku ze wzrostem zagrożenia terrorystycznego w Europie oraz podejmowanymi na forum Rady Europy i Organizacji Narodów Zjednoczonych działaniami mającymi na celu doprowadzenie do penalizacji działalności tzw. zagranicznych bojowników, którzy podejmują podróż zagraniczną w celu popełniania, planowania i przygotowania ataków terrorystycznych lub uczestnictwa w nich, a także w celu udzielania lub otrzymywania przeszkolenia terrorystycznego. W dniu 26 marca 2015 r. przewodniczący MZds.ZT powołał Zespół Zadaniowy do spraw przeglądu rozwiązań prawnych odnoszących się do zagrożeń terrorystycznych, działający pod przewodnictwem przedstawiciela ówczesnego Ministerstwa Spraw Wewnętrznych. Celem tego gremium nie było jednak opracowanie projektu kompleksowej ustawy regulującej przedmiotową tematykę, lecz przedstawienie propozycji zmian w obowiązujących aktach prawnych. Przedstawione przez Zespół Zadaniowy rekomendacje obejmowały – poza penalizacją działalności tzw. zagranicznych bojowników – propozycje zmian

prawnych mających na celu usprawnienie koordynacji służb i organów tworzących system antyterrorystyczny.

Jednak dopiero w 2015 r., w ramach kolejnej inicjatywy, udało się przygotować projekt ustawy o działaniach antyterrorystycznych, który został zaakceptowany. Projekt został przygotowany przez Ministerstwo Spraw Wewnętrznych i Administracji oraz Kancelarię Prezesa Rady Ministrów we współpracy z Agencją Bezpieczeństwa Wewnętrznego i przy wsparciu Zespołu Zadaniowego do opracowania koncepcji kompleksowej regulacji dotyczącej problematyki rozpoznawania, przeciwdziałania i zwalczania zagrożeń o charakterze terrorystycznym, powołanego przez przewodniczącego MZds.ZT 4 grudnia 2015 r.

Kolejną istotną regulację przyjętą m.in. dzięki współpracy w ramach MZds.ZT stanowi ww. ustawa o gromadzeniu i przetwarzaniu danych pasażerów linii lotniczych. Zgodnie z jej przepisami przewoźnicy lotniczy zostali zobligowani do przekazywania Straży Granicznej danych dotyczących przelotu pasażerów korzystających z ich linii. Informacje o pasażerach są przetwarzane w celu zapobiegania, wykrywania i zwalczania terroryzmu i innych przestępstw oraz ścigania ich sprawców. Obowiązek wprowadzenia nowych przepisów wynikał z unijnej *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania*[13].

Aktualnie na wejście w życie oczekują, przygotowane w ramach współpracy Straży Granicznej i Ministerstwa Infrastruktury zainicjowanej przez MZds.ZT, przepisy ustawy o zmianie ustawy – Prawo lotnicze oraz ustawy o Straży Granicznej. Również w tym przypadku potrzeba wydania nowych przepisów wynikała ze zmian w prawie unijnym, tj. wprowadzonych w *Rozporządzeniu wykonawczym Komisji (UE) 2019/103 z dnia 23 stycznia 2019 r. zmieniającym rozporządzenie wykonawcze (UE) 2015/1998 w odniesieniu do wyjaśnienia, harmonizacji i uproszczenia, a także wzmocnienia niektórych szczególnych środków ochrony lotnictwa*[14]. Powołany przez przewodniczącego MZds.ZT 2 kwietnia 2019 r. Zespół Zadaniowy do opracowania nowych rozwiązań w zakresie sprawdzania

[13] Dz. Urz. UE L 119/132 z 4 V 2016 r.

[14] Dz. Urz. UE L 21/13 z 24 I 2019 r.

pracowników sektora lotniczego dokonał analizy niezbędnych działań legislacyjnych i organizacyjno-technicznych, które powinny być wdrożone, aby dostosować polski porządek prawny do ww. rozporządzenia w zakresie przeprowadzania sprawdzenia życiorysu pracowników sektora lotniczego w kontekście ich przeszłości kryminalnej. Zespół ten opracował rónież nowe procedury dokonywania tych sprawdzeń oraz schemat wymiany informacji na ten temat, a finalnie przygotował projekt przepisów, za pomocą których procedury te będą realizowane.

Poza istotnym wkładem w legislację odnoszącą się do zagrożeń o charakterze terrorystycznym na szczególną uwagę zasługuje działalność MZds.ZT dotycząca wypracowywania rekomendacji odnoszących się do poprawy zabezpieczenia konkretnych obiektów, mogących – z uwagi na swoje znaczenie strategiczne dla bezpieczeństwa państwa czy kluczowe znaczenie z perspektywy zapewnienia konkretnych usług dla społeczeństwa, jak na przykład sprawnej komunikacji – stanowić potencjalny cel ataków. W ciągu ostatnich 15 lat MZds.ZT, w ramach prac powoływanych w tym celu kolejnych zespołów zadaniowych, dokonywał analizy i oceny zarówno poziomu zagrożenia terrorystycznego, jak i przygotowania pod kątem możliwości reagowania na zdarzenia o charakterze terrorystycznym, a także mechanizmów związanych z ewakuacją i przekazywaniem informacji w sytuacji wystąpienia zagrożeń, w stosunku do:

- terenów i budynków Kancelarii Prezydenta Rzeczypospolitej Polskiej;
- terenu i budynku Kancelarii Prezesa Rady Ministrów;
- obiektów Parlamentu (dwukrotnie w 2010 r. oraz na przełomie 2016 i 2017 r.);
- dworców kolejowych – Warszawa Centralna i Warszawa Śródmieście oraz kolejowego tunelu średnicowego w Warszawie (wypracowane rekomendacje przekazano do wykorzystania właściwym podmiotom, a także zarządcom innych podobnych obiektów na terenie kraju);
- warszawskiego metra;
- obiektów jądrowych w Świerku.

Rezultatem prac obejmujących wizyty studyjne ekspertów we wskazanych obiektach były rekomendacje dotyczące zmian zarówno o charakterze technicznym, jak i organizacyjnym i proceduralnym. W przypadku terenów i obiektów pozostających w zarządzie Kancelarii

Prezesa RM i Kancelarii Prezydenta RP efektem prac było również przyjęcie jednolitych planów ochrony tych obiektów, będących podstawą do opracowania szczegółowych instrukcji oraz ewentualnych dodatkowych mechanizmów współdziałania formacji odpowiedzialnej za ochronę najważniejszych osób w państwie, tj. Służby Ochrony Państwa, odpowiednio z Kancelarią Prezesa RM, Kancelarią Prezydenta RP oraz innymi właściwymi podmiotami, w tym służbami – Policją, Państwową Strażą Pożarną oraz służbami specjalnymi.

Wypracowywane rekomendacje przekazywano do realizacji właściwym podmiotom i resortom, a także – w miarę możliwości – monitorowano na forum MZds.ZT sposób i zakres ich realizacji. Część z rekomendacji kierowano do podmiotów spoza administracji rządowej, jak chociażby w przypadku podmiotu zarządzającego warszawskim metrem, w związku z czym MZds.ZT mógł służyć jedynie głosem doradczym, nie miał natomiast kompetencji do narzucenia zastosowania określonych rozwiązań związanych z ich wdrażaniem.

Na uwagę zasługują również prace powołanego 26 maja 2017 r. Zespołu Zadaniowego ds. opracowania standardów zabezpieczeń antyterrorystycznych i reguł współdziałania dotyczących infrastruktury krytycznej oraz zasad dokonywania sprawdzenia zabezpieczeń obiektów infrastruktury krytycznej zgodnie z przepisami ustawy o działaniach antyterrorystycznych. Należy podkreślić, że wdrożenie wypracowanych przez Zespół Zadaniowy standardów i rekomendacji pozostaje w dużej mierze uzależnione od podmiotów zarządzających tego rodzaju obiektami, a ze względu na potencjalnie wysokie koszty w porównaniu z niskim poziomem zagrożenia terrorystycznego w Polsce nie zawsze jest traktowane w sposób priorytetowy.

Nie bez znaczenia pozostaje także wkład MZds.ZT w usprawnienie procedur współdziałania właściwych służb i instytucji w kontekście zagrożeń terrorystycznych. Przed wejściem w życie ustawy o działaniach antyterrorystycznych dokumentem stanowiącym podstawę do organizacji współdziałania było porozumienie Szefa Agencji Bezpieczeństwa Wewnętrznego, Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego Żandarmerii Wojskowej i Komendanta Głównego Państwowej Straży Pożarnej z 21 stycznia 2014 r., zawarte na podstawie zasad wypracowanych przez powołany decyzją Przewodniczącego MZds.ZT z 13 sierpnia 2012 r. Zespół Zadaniowy ds. opracowania propozycji algorytmu współdziałania

i zarządzania na miejscu zdarzenia o charakterze terrorystycznym. Wypracowane wówczas zasady zostały następnie ustawą o działaniach antyterrorystycznych częściowo inkorporowane na grunt przepisów prawa powszechnie obowiązującego. Ponadto w rezultacie ustaleń podjętych na forum MZds.ZT 7 marca 2018 r. zawarto nowe porozumienie szefów ww. formacji w sprawie współdziałania na miejscu zdarzenia o charakterze terrorystycznym, stanowiące tym razem jedynie uzupełnienie na poziomie techniczno-organizacyjnym regulacji ustawowych.

Efektem pracy MZds.ZT były także *Wytyczne Prezesa Rady Ministrów z 31 października 2021 r. w sprawie koordynacji wymiany informacji o zagrożeniach terrorystycznych* oraz katalog incydentów i zdarzeń zgłaszanych do Centrum Antyterrorystycznego ABW, który początkowo przyjęto uchwałą MZds.ZT. Oba te dokumenty zostały wykorzystane przy opracowywaniu przepisów ustawy o działaniach antyterrorystycznych. Obecnie katalog incydentów o charakterze terrorystycznym określa *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym*[15] wydane na podstawie ww. ustawy, a koordynacyjna rola Szefa ABW w odniesieniu do czynności analityczno-informacyjnych pozostałych służb polskiego sytemu antyterrorystycznego wynika wprost z art. 5 ust. 1 tej ustawy.

Nie bez znaczenia pozostaje także zaangażowanie MZds.ZT w opracowanie metodyki oględzin miejsc przestępstw o charakterze terrorystycznym i katastrof oraz identyfikacji ciał ofiar. Przygotowana po raz pierwszy w 2011 r. metodyka została następnie poddana ewaluacji w ramach Zespołu Zadaniowego powołanego decyzją Przewodniczącego MZds.ZT 28 lipca 2017 r. W wyniku prac MZds.ZT przyjęte zostało również rozwiązanie unormowane obecnie we wspomnianym porozumieniu z 7 marca 2018 r. w sprawie współdziałania na miejscu zdarzenia o charakterze terrorystycznym. Polegało ono na utworzeniu centralnego, nieetatowego zespołu wspierającego czynności dochodzeniowo-śledcze na miejscu zdarzenia spowodowanego użyciem materiału lub urządzenia wybuchowego, w tym mogącego zawierać substancję lub czynnik chemiczny, biologiczny lub radioaktywny. Możliwość szybkiego uruchomienia wspólnego zespołu składającego się z ekspertów z Policji,

[15] DzU z 2017 r. poz. 1517.

ABW, Straży Granicznej, Żandarmerii Wojskowej i Państwowej Straży Pożarnej, działającego przy wsparciu Prokuratury, stanowi niezwykle ważne narzędzie w przypadku wystąpienia tego rodzaju zdarzeń. Nieodzowne pozostaje również zapewnienie możliwie częstych treningów dla przedstawicieli tego Zespołu służących doskonaleniu ich współdziałania – dotychczas przeprowadzone ćwiczenia przy udziale wspomnianego Zespołu wykazały potrzebę kontynuacji przedmiotowej współpracy i zwiększyły wartość wymiany doświadczeń pomiędzy specjalistami w kwestii przeglądu w poszczególnych formacjach.

Zagrożenia CBRN – chemiczne, biologiczne, radiacyjne i nuklearne – niejednokrotnie stanowiły temat prac MZds.ZT z uwagi na komplikacje związane z zakresem odpowiedzialności poszczególnych podmiotów w przypadku reagowania na tę szczególną formę zagrożeń, cechujących się potencjalnie nieograniczoną i niekiedy trudną do przewidzenia skalą odziaływania. Rezultatami tych działań są m.in. przyjęty przez MZds.ZT *Algorytm postępowania i współdziałania w przypadku otrzymania niezidentyfikowanej przesyłki mogącej stanowić zagrożenie chemiczne, biologiczne lub radiacyjne*, a także materiał o charakterze profilaktycznym w formie ogólnodostępnej *Procedury działania instytucji otrzymującej podejrzana przesyłkę*.

Profilaktyka antyterrorystyczna w minionych latach stanowiła jeden z wielu aspektów działania MZds.ZT. W ramach działającego przy Mzds.ZT Zespołu Zadaniowego – Stałej Grupy Eksperckiej przygotowano i na bieżąco aktualizowano rządową stronę internetową antyterroryzm.gov.pl, na której publikowano materiały przygotowane na podstawie ustaleń MZds.ZT, jak np. wspomnianą *Procedurę działania instytucji otrzymującej podejrzaną przesyłkę,* instrukcję *Postępowanie w przypadku zagrożenia atakiem terrorystycznym, Instrukcję alarmową – zasady postepowania w przypadku uzyskania informacji o podłożeniu lub zlokalizowaniu urządzenia wybuchowego w obiekcie użyteczności publicznej,* poradniki skierowane do określonych grup odbiorców, np. opracowany przez Komendę Stołeczną Policji wspólnie z Urzędem m.st. Warszawy poradnik *Zasady postępowania w przypadku wtargnięcia napastnika na teren placówki oświatowej* czy przygotowana przez ABW publikacja *Zabezpieczenie antyterrorystyczne wielkopowierzchniowych obiektów handlowych. Uniwersalny poradnik*. Na stronie zamieszczano też podstawowe informacje dotyczące funkcjonowania polskiego systemu antyterrorystycznego, a także aktualne informacje o obowiązujących

stopniach alarmowych lub stopniach alarmowych CRP, wprowadzanych na podstawie przepisów ustawy o działaniach antyterrorystycznych. Po wejściu w życie przepisów *Ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami*[16] funkcjonująca dotychczas na serwerze ABW strona została przeniesiona jako zakładka *System antyterrorystyczny RP*[17] na stronę Biuletynu Informacji Publicznej MSWiA, przy czym w dalszym ciągu w zakładce dostępne są ww. materiały o charakterze profilaktycznym.

Istotnym osiągnięciem MZds.ZT w kontekście zagrożenia związanego z fałszywymi powiadomieniami o podłożeniu ładunków wybuchowych było opracowanie zasad obiegu informacji w tego rodzaju sytuacjach przy koordynacyjnej roli Centralnego Biura Śledczego Policji, co pozwoliło na systemową identyfikację zjawiska tzw. powiadomień kaskadowych, tj. powiadomień skierowanych jednocześnie do wielu instytucji lub dotyczących jednocześnie wielu obiektów. Działania te pozwoliły na zmniejszenie liczby ewakuacji stanowiących istotne utrudnienie nie tylko dla funkcjonowania podmiotów administracji publicznej czy sądownictwa, lecz także dla sektora prywatnego, co było związane z angażowaniem znacznych sił i środków po stronie służb. Przeprowadzenie ewakuacji skutkowało poniesieniem dużych strat finansowych, a nawet stwarzało zagrożenie dla życia i zdrowia, jak w przypadku ewakuacji szpitali.

Spośród wielu ważnych inicjatyw realizowanych przez ostatnie 15 lat na forum MZds.ZT nie sposób pominąć kwestii najpierw przygotowania projektu, a następnie koordynacji wdrażania *Narodowego Programu antyterrorystycznego na lata 2015–2019*.

W tym dokumencie, nad którym dyskusje toczyły się w ramach Zespołu Zadaniowego – Stałej Grupy Eksperckiej, który wspierał MZds.ZT na poziomie eksperckim, przedstawiono ówczesny poziom zagrożenia terrorystycznego, wskazano również – jeszcze przed przyjęciem ustawy o działaniach antyterrorystycznych – mechanizmy prowadzenia jego bieżącej oceny, a także elementy warunkujące skuteczność funkcjonowania systemu antyterrorystycznego RP. *Program* przewidywał podjęcie działań zmierzających do zapewnienia optymalnej współpracy podmiotów realizujących zadania w odniesieniu do przeciwdziałania i zwalczania

[16] Tekst jednolity: DzU z 2020 r. poz. 1062.

[17] https://www.gov.pl/web/mswia/system-antyterrorystyczny-rp [dostęp: 13 XII 2021].

zagrożeń o charakterze terrorystycznym. Jednym z zasadniczych celów dokumentu było także podnoszenie świadomości społecznej o zagrożeniach o charakterze terrorystycznym, zasadach zachowania w przypadku wystąpienia zdarzenia oraz formach i środkach zaangażowania państwa w przeciwdziałanie i zwalczanie terroryzmu. Cele szczegółowe *Programu* zakładały usprawnienie realizacji zadań przez podmioty polskiego systemu antyterrorystycznego w poszczególnych fazach zarządzania kryzysowego i działań antyterrorystycznych, to jest: zapobiegania, przygotowania, reagowania oraz odbudowy[18].

Zgodnie z określonym w *Programie* mechanizmem jego wdrażania koordynatorem *Programu*, w imieniu Rady Ministrów, był minister właściwy do spraw wewnętrznych, który realizował swoje zadania za pomocą Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych[19]. W *Programie* podkreślono również, jak już wcześniej wspomniano, rolę MZds.ZT w zakresie m.in. inicjowania, koordynowania i monitorowania działań podejmowanych przez właściwe organy administracji rządowej, a także opracowania propozycji usprawniających metody i formy zwalczania terroryzmu oraz występowania z wnioskiem do właściwych organów o podjęcie prac legislacyjnych, wynikających z *Zarządzenia nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*.

Główne narzędzie wdrażania *Programu* i jego bieżącego monitorowania stanowił tzw. *Plan działań*, będący jego integralną częścią. Określano w nim przedsięwzięcia o charakterze legislacyjnym i organizacyjnym (priorytety) kluczowe dla osiągnięcia większej skuteczności polskiego systemu antyterrorystycznego. W *Planie działań* wskazane były jednocześnie podmioty wiodące i współpracujące przy wykonaniu poszczególnych priorytetów. Zgodnie z mechanizmem wdrażania zdefiniowanym w *Programie* kierownicy poszczególnych służb, organów i instytucji, wymienionych jako podmioty wiodące w realizacji poszczególnych przedsięwzięć wynikających z *Planu działań*, byli zobowiązani do opracowania, w porozumieniu z kierownikami podmiotów

[18] Por. *Raport o stanie bezpieczeństwa w Polsce w 2016 r.*, s. 279, https://archiwumbip.mswia.gov.pl [dostęp: 13 XII 2021].

[19] Por. M. Cichomski, K. Więcek, *„Narodowy Program Antyterrorystyczny na lata 2015–2019" jako operacyjno-wdrożeniowy dokument służący realizacji polityki rozwoju*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11, s. 321–322.

współpracujących, harmonogramów realizacji każdego z priorytetów, w tym do określenia planowanych terminów ich wykonania. Harmonogramy te były następnie przekazywane do ministra właściwego do spraw wewnętrznych i omawiane oraz przyjmowane w ramach MZds.ZT. Zespół nie tylko na bieżąco monitorował realizację poszczególnych harmonogramów, lecz także dokonywał corocznej ewaluacji postępów we wdrażaniu *Programu* w formie raportu omawianego na posiedzeniu MZds.ZT, a następnie przedkładanego do wiadomości Radzie Ministrów[20]. Na forum MZds.ZT podejmowano również decyzje co do podziału środków w ramach rezerwy celowej przyznanej na realizację *Programu*.

Jednym z istotnych skutków wdrożenia *Narodowego Programu Antyterrorystycznego na lata 2015–2019* było wprowadzenie nowego modelu współdziałania służb w zakresie dokonywania oceny wiarygodności informacji o podłożeniu urządzenia wybuchowego, rozpoczęcie prac zmierzających do wdrożenia w Polsce mechanizmu gromadzenia i przetwarzania danych pasażerów linii lotniczych, które jest zgodne z przepisami dyrektywy w sprawie zarządzania danymi pasażerów linii lotniczych (PNR) w celu zapobiegania, wykrywania, prowadzenia dochodzeń i ścigania przestępstw terrorystycznych, czego finalizację stanowi wspomniana ustawa o przetwarzaniu danych dotyczących przelotu pasażera. Efektem *Programu* jest też zrealizowanie w 2016 r. cyklu szkoleń z zakresu profilaktyki antyterrorystycznej dla kadry kierowniczej i dydaktycznej szkół, w ramach którego przeszkolono ponad 98 tys. dyrektorów i pracowników placówek oświatowych, szkolenia dla przedstawicieli branży wielkopowierzchniowych obiektów handlowych w zakresie postępowania w sytuacji zagrożenia o charakterze terrorystycznym, szkolenia dla dyrektorów generalnych urzędów administracji rządowej dotyczące postępowania w przypadku otrzymania podejrzanej przesyłki oraz postępowania w przypadku uzyskania wiadomości o podłożeniu urządzenia wybuchowego w obiekcie instytucji publicznej.

Obecnie prace MZds.ZT prowadzone są przede wszystkim na podstawie rocznych harmonogramów przyjmowanych nieprzerwanie od początku istnienia Zespołu. Część ujmowanych w nich zdań ma charakter cykliczny, inne wynikają z bieżących potrzeb i ewolucji zagrożeń o charakterze terrorystycznym.

[20] Por. *Uchwała nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (MP z 2014 r. poz. 1218).

Do tych pierwszych należy w ostatnich latach zaliczyć dokonywaną przez ABW ocenę oraz prognozę zagrożenia terrorystycznego dla RP i jej obywateli, omawianie sytuacji bezpieczeństwa polskich turystów w wybranych państwach w związku z sezonem turystycznym, a także przygotowywanie przez Rządowe Centrum Bezpieczeństwa zestawienia wniosków z ćwiczeń z zakresu reagowania na zdarzenia o charakterze terrorystycznym czy sprawozdań Generalnego Inspektora Informacji Finansowej z realizacji *Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[21].

Ostatnie dwa lata funkcjonowania MZds.ZT przyniosły nowe wyzwanie – tym razem natury organizacyjnej. Sytuacja związana z pandemią COVID-19 nie pozostała bez wpływu na funkcjonowanie Zespołu, którego prace w dużej mierze są materią ustawowo chronioną jako niejawna. Wobec zmiany formuły spotkań na wirtualną większości gremiów o podobnym do MZds.ZT charakterze w przypadku tego Zespołu, ze względów bezpieczeństwa, podjęto decyzję o realizacji części jego prac w drodze wymiany korespondencji oraz o podejmowaniu wiążących ustaleń w trybie obiegowym. Potrzeba tych zmian znalazła swoje odzwierciedlenie w modyfikacji regulaminu prac Zespołu, który mimo utrudnień związanych z pandemią zachował ciągłość działania i realizuje przyjęte harmonogramy prac.

Podczas wspomnianej wizyty Dyrekcji Wykonawczej ONZ ds. Zwalczania Terroryzmu w grudniu 2019 r. nasz kraj został pozytywnie oceniony pod kątem przyjętych rozwiązań antyterrorystycznych o charakterze systemowym, jak również w odniesieniu do działań poszczególnych służb, podejmowanych w celu zwalczania tego rodzaju przestępczości. Eksperci ONZ wysoko ocenili nasze systemowe podejście do zagrożenia. Stwierdzili, że jakkolwiek Polska stoi w obliczu stosunkowo małego zagrożenia ze strony terroryzmu, podchodzi do tego problemu poważnie, wprowadzając wiele prawnych, instytucjonalnych i operacyjnych środków antyterrorystycznych. Uzyskanie tak wysokiej oceny nie byłoby możliwe bez działającego nieprzerwanie od 15 lat międzyinstytucjonalnego forum współpracy, jakim jest MZds.ZT.

Podsumowując, trzeba podkreślić, że Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych pomimo diametralnych zmian w otoczeniu prawnym, jakie zaszły od chwili jego powołania, nadal odgrywa

[21] Tekst jednolity: DzU z 2021 r. poz. 1132, ze zm.

rolę gremium o charakterze strategicznym, kluczowego w kontekście koordynacji przedsięwzięć mających na celu stworzenie podstaw prawnych i proceduralnych do zapobiegania zdarzeniom o charakterze terrorystycznym, przygotowania do przejmowania nad nimi kontroli i reagowania w przypadku wystąpienia tego rodzaju zdarzeń. Świadczy o tym przede wszystkim jego nieprzerwana od 2006 r. aktywność dotycząca inicjatyw o charakterze legislacyjnym i proceduralnym. Szczególnie ważna z perspektywy zapewniania możliwości skutecznej koordynacji przedsięwzięć w przedmiotowym zakresie oraz umożliwienia współpracy wielu służb i podmiotów polskiego systemu antyterrorystycznego pozostaje również ciągłość funkcjonowania niniejszego gremium, pozwalająca uniknąć działań podejmowanych ad hoc, bez należytej analizy ewolucji zagrożeń o charakterze terrorystycznym i skuteczności dotychczas wdrażanych przepisów i procedur.

Bibliografia

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., Więcek K., *„Narodowy Program Antyterrorystyczny na lata 2015–2019" jako operacyjno-wdrożeniowy dokument służący realizacji polityki rozwoju*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11, s. 313–327.

Zubrzycki W., *Dzieje ustawy antyterrorystycznej w Polsce*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016.

Źródła internetowe

Raport o stanie bezpieczeństwa w Polsce w 2016 r., https://archiwumbip.mswia.gov.pl [dostęp: 13 XII 2021].

https://www.gov.pl/web/mswia/system-antyterrorystyczny-rp [dostęp: 13 XII 2021].

Akty prawne

Rozporządzenie wykonawcze Komisji (UE) 2019/103 z dnia 23 stycznia 2019 r. zmieniające rozporządzenie wykonawcze (UE) 2015/1998 w odniesieniu do wyjaśnienia, harmonizacji i uproszczenia, a także wzmocnienia niektórych szczególnych środków ochrony lotnictwa (Dz. Urz. UE L 21 z 24 I 2019 r.).

Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE L 119/132 z 4 V 2016 r.).

Ustawa z dnia 17 września 2021 r. o zmianie ustawy – Prawo lotnicze oraz ustawy o Straży Granicznej (DzU z 2021 r. poz. 1898).

Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (DzU z 2020 r. poz. 1062).

Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (DzU z 2019 r. poz. 1783).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU z 2021 r. poz. 1132, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (DzU z 2021 r. poz. 2234).

Ustawa z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (DzU z 2021 r. poz. 1057).

Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów (DzU z 2021 r. poz. 178, ze zm.).

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

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 dnia 4 września 2008 r., zarządzeniem nr 74 Prezesa Rady Ministrów z dnia 21 września 2009 r., zarządzeniem nr 18 Prezesa Rady Ministrów z dnia 3 kwietnia 2014 r., zarządzeniem nr 84 Prezesa Rady Ministrów z dnia 18 września 2015 r., zarządzeniem nr 86 Prezesa Rady Ministrów z dnia 5 lipca 2016 r., zarządzeniem nr 32 Prezesa Rady Ministrów z dnia 27 kwietnia 2017 r., zarządzeniem nr 160 Prezesa Rady Ministrów z dnia 9 listopada 2017 r., zarządzeniem nr 92 Prezesa Rady Ministrów z dnia 7 czerwca 2018 r. oraz zarządzeniem nr 37 Prezesa Rady Ministrów z dnia 8 kwietnia 2021 r.

*Uchwała nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019" (*MP z 2014 r. poz. 1218).

DOI: 10.4467/27204383TER.22.004.15420

ORCID: 0000-0002-7082-8511

JĘDRZEJ ŁUKASIEWICZ

Bezzałogowe statki powietrzne jako źródło zagrożeń infrastruktury zaopatrzenia państw w energię elektryczną oraz proponowane metody ochrony tej infrastruktury

Abstrakt

Bezzałogowe statki powietrzne stanowią zagrożenie dla obiektów ważnych dla bezpieczeństwa państwa. Ich uniwersalność wynikająca z cech poszczególnych typów statków powietrznych powoduje, że skala sposobów ich użycia w atakach jest praktycznie nieograniczona. Dla bezpieczeństwa państwa niezwykle istotny jest system zaopatrzenia w energię elektryczną. Ze względu na rozległość sieci przesyłowych oraz znaczną liczbę punktów węzłowych tych sieci należy postawić pytanie, jak dalece system ten jest odporny na ataki terrorystyczne, zwłaszcza te przeprowadzone z zastosowaniem bezzałogowego statku powietrznego. W pracy autor dokonuje analizy ataku polegającego na spowodowaniu zwarcia instalacji elektrycznej z użyciem przewodu miedzianego podwieszonego pod bezzałogową platformę latającą. Implementacja opisanych w pracy zalecanych sposobów ochrony powinna doprowadzić do podniesienia poziomu bezpieczeństwa sieci przesyłowych.

Słowa kluczowe:

bezzałogowe statki powietrzne, sieć elektroenergetyczna, ochrona obiektów ważnych dla bezpieczeństwa państwa, profilaktyka antydronowa

Bezzałogowe statki powietrzne są źródłem zagrożeń dla obiektów ważnych dla bezpieczeństwa państwa. Bezzałogowe statki powietrzne (np. samolot, multirotor lub śmigłowiec) to urządzenia, które wykonują swoje misje bez obecności pilota na pokładzie. Mogą one atakować cele, także ludzi, wykorzystując algorytmy sztucznej inteligencji[1]. Informacje prasowe pokazują kolejne przykłady wykorzystania bezzałogowych statków powietrznych w działaniach wojennych, ale także w atakach terrorystycznych[2], w tym na system zaopatrzenia w energię elektryczną. Celem analizy przedstawionej w pracy jest określenie podatności sieci energetycznej na ataki prowadzone za pomocą bezzałogowych statków powietrznych oraz wskazanie metod zapobiegania atakom realizowanym za pomocą tego typu urządzeń na obiekty elektroenergetyczne w Polsce. Przeprowadzenie takiej analizy wydaje się uzasadnione, ponieważ doniesienia medialne uprawniają do sformułowania hipotezy, że sukces jednego tego typu ataku może wywołać trend do atakowania dronami obiektów sieci elektroenergetycznej w Europie, w tym w Polsce.

Struktura sieci elektroenergetycznej w Polsce

Energię elektryczną w Polsce produkują elektrownie: cieplne, wodne, wiatrowe, fotowoltaiczne oraz wykorzystujące biogaz lub biomasę. Część energii elektrycznej jest importowana z zagranicy[3]. Energia elektryczna od producenta do końcowego użytkownika jest przesyłana przez sieć elektroenergetyczną, złożoną z linii oraz stacji elektroenergetycznych. Każdy przesył energii generuje straty. Aby były one jak najniższe, do przesyłu energii na duże odległości wykorzystuje się sieci przesyłające energię o napięciach od 220 kV do 400 kV, zwanych najwyższymi napięciami. Do przesyłu energii elektrycznej na odległość do

[1] https://www.newscientist.com/article/2278852-drones-may-have-attacked-humans-fully-autonomously-for-the-first-time/ [dostęp: 30 XI 2021].

[2] https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html [dostęp: 30 XI 2021]; https://www.bbc.com/news/world-middle-east-59195399 [dostęp: 30 XI 2021]; https://www.reuters.com/world/middle-east/iran-backed-militia-behind-attack-iraqi-pm-sources-2021-11-08/ [dostęp: 30 XI 2021].

[3] *Energetyka, dystrybucja, przesył*, PTPiREE, http://ptpiree.pl/raporty/2021/raport_ptpiree_2021.pdf [dostęp: 30 XI 2021].

kilkudziesięciu kilometrów służą linie, w których napięcie wynosi 110 kV. Jest to wysokie napięcie. W lokalnych liniach rozdzielczych napięcie wynosi od 10 kV do 30 kV i jest to tzw. średnie napięcie. Średnie napięcie transformowane jest do niskiego napięcia wynoszącego 220/230 V lub 380/400 V. Niskie napięcie wykorzystywane jest przez końcowego odbiorcę[4]. Plan sieci elektroenergetycznej w Polsce uwzględniający planowane inwestycje przedstawiony jest na rysunku 1.

Rys. 1. Schemat sieci elektroenergetycznej w Polsce.

Źródło: https://www.pse.pl/obszary-dzialalnosci/krajowy-system-elektroenergetyczny/plan-sieci-elektroenergetycznej-najwyzszych-napiec/planowana [dostęp: 30 XI 2021].

System elektroenergetyczny w Polsce składa się z systemowych stacji elektroenergetycznych dla najwyższych napięć, stacji rozdzielczych napięć wysokich oraz stacji transformatorowych. Zgodnie z informacją

[4] https://www.pse.pl/obszary-dzialalnosci/krajowy-system-elektroenergetyczny/informacje-o-systemie [dostęp: 30 XI 2021].

udostępnioną przez Polskie Sieci Energetyczne SA obecnie na obszarze Polski wykorzystuje się 281 linii najwyższego napięcia o łącznej długości 15 316 km oraz 109 stacji najwyższych napięć. Liniami wysokiego, średniego i niskiego napięcia zarządzają: Enea Operator, Energa-Operator, Polska Grupa Energetyczna Dystrybucja, Innogy Stoen Operator oraz Tauron Dystrybucja. Całkowita długość przyłączy zarządzanych przez ww. operatorów wynosi 169 076 km. Obsługa wyżej opisanych linii wymagała zbudowania 111 stacji najwyższego, 1537 wysokiego oraz 262 989 średniego napięcia[5]. Linie najwyższego napięcia oraz linie wysokiego napięcia wykonane są z kabli, które nie są izolowane. Linie średniego napięcia zazwyczaj nie są izolowane. Na liniach średniego napięcia stosuje się izolację, gdy przebiegają one przez las. Linie niskiego napięcia są izolowane[6]. Linie napowietrzne są wyposażone w zdalnie sterowane rozłączniki i sygnalizatory zwarcia, które pozwalają na szybką lokalizację usterki.

Uszkodzenie instalacji elektrycznej za pomocą bezzałogowego statku powietrznego

Zagrożenia dla sieci elektroenergetycznych zostały zauważone już dawno[7], a doniesienia o atakach na elementy sieci ukazywały się w środkach masowego przekazu[8].

W dniu 4 listopada 2021 r. zostały opublikowane informacje zawarte w raporcie Joint Intelligence Bulletin (JIB). Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI) oraz National Counterterrorism Center (NCTC) odniosły się w nim do zdarzenia, do którego doszło w Stanach Zjednoczonych Ameryki, w Pensylwanii, a które

[5] *Energetyka, dystrybucja, przesył...*, s. 33–49.

[6] Tamże, s. 51–67.

[7] P.W. Parfomak, *Physical Security of the U.S. Power Grid. High-Voltage Transformer Substations*, Congressional Research Service, 17 VI 2014; R. Baldick, B. Chowdhury, I. Dobson, *Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures*, w: *IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

[8] https://www.wsj.com/articles/SB10001424052702304851104579359141941621778 [dostęp: 30 XI 2021].

polegało na próbie ataku na elementy sieci elektroenergetycznej przy użyciu drona z podwieszonym do jego obudowy przewodem elektrycznym. Do ataku najprawdopodobniej użyto bezzałogowego statku powietrznego produkcji firmy DJI Mavic 2[9]. Jest to model powszechnie dostępny w sklepach.

W związku z ujawnieniem informacji o możliwości atakowania sieci elektroenergetycznej za pomocą bezzałogowego statku powietrznego należy zadać pytanie, jak bardzo sieć elektroenergetyczna w Polsce jest podatna na przeprowadzony w ten sposób atak.

Do analizy możliwości uszkodzenia sieci z użyciem bezzałogowego statku powietrznego wybrano urządzenia, których parametry lotu są zbliżone do modeli powszechnie dostępnych na rynku. Należy przyjąć, że niektóre modele przeznaczone są do wykonywania tylko i wyłącznie konkretnych typów misji, np. dla modeli przenoszących kamerę misją taką jest filmowanie obiektu, z kolei inne typy statków powietrznych to platformy uniwersalne, przystosowane przez producenta do podnoszenia dowolnego ładunku użytecznego, którego jedynym ograniczeniem jest rozmiar i masa. Takim ładunkiem użytecznym może być np. urządzenie służące do badania jakości powietrza, system lidarowy, ale także ładunek wybuchowy. Statki powietrzne przeznaczone do wykonania konkretnej misji są konstrukcjami zwartymi, zamkniętymi, a podwieszenie pod nie dodatkowego ładunku jest nieco utrudnione. Statki, które są platformami uniwersalnymi, to konstrukcje otwarte, mające pokłady specjalnie przygotowane do podwieszenia ładunku. Analizując parametry ogólnie dostępnych na rynku platform, można w pewnym przybliżeniu założyć, że najczęściej statek powietrzny może podnieść ładunek dodatkowy o masie stanowiącej ok. 30 proc. masy platformy bez wyposażenia. Do analizy wybrano platformy, które mogą podnieść następujące masy ładunku: 0,25 kg, 0,5 kg, 2,5 kg oraz 4 kg. Wraz ze wzrostem masy ładunku zwiększa się także wielkość statku powietrznego, a więc pojawia się trudność w jego transporcie i ukryciu.

Uszkodzenia instalacji elektrycznej, a tym samym zatrzymania jej pracy, można dokonać na różne sposoby: może to być uszkodzenie mechaniczne na skutek detonacji ładunku wybuchowego, uszkodzenie poprzez spowodowanie zwarcia przewodów z napięciem do ziemi,

[9] https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report [dostęp: 30 XI 2021].

tzw. doziemienie, a także uszkodzenie poprzez spowodowanie zwarcia przewodów z napięciem, przy czym zwarcie to zachodzi między różnymi przewodami fazowymi. W informacji prasowej z listopada 2021 r. opisano próbę ataku polegającego na zwarciu wywołanym w instalacji elektrycznej. Do analizy wybrano dwa scenariusze:

1. Bezzałogowy statek powietrzny z podwieszonym długim, nieizolowanym przewodem elektrycznym podlatuje do nieizolowanego przewodu fazowego i zwiera go do ziemi;
2. Bezzałogowy statek powietrzny z podwieszonym długim nieizolowanym przewodem elektrycznym podlatuje do słupa z nieizolowanymi przewodami elektrycznymi i powoduje zwarcie między przewodami.

Wyznaczenie długości nieizolowanego miedzianego przewodu elektrycznego, który posłuży do powstania zwarcia instalacji elektrycznej

Zwarcie nastąpi pomiędzy jednym z przewodów fazowych a ziemią lub pomiędzy przewodami fazowymi. Długość przewodu elektrycznego, który posłuży do powstania zwarcia instalacji elektrycznej, można wyznaczyć ze wzoru:

$$l = \frac{m}{\sigma \times S}[\mathrm{m}],$$

gdzie:
l – długość przewodu wyrażona w m,
m – masa przewodu wyrażona w kg, którą bezzałogowy statek powietrzny podniesie do góry,
σ – gęstość materiału wyrażona w kg/m^3; gęstość miedzi wynosi 8920 kg/m^3,
S – pole przekroju materiału wyrażone w m^2.

Pola przekroju przewodów elektrycznych są wielkościami znormalizowanymi. Wyliczone długości przewodów stanowiących ładunek dodatkowy o masach: 0,25 kg, 0,5 kg, 2,5 kg, 4 kg, zestawiono w tabeli 1.

Tab. 1. Zestawienie długości przewodów elektrycznych podwieszonych pod bezzałogowy statek powietrzny, o zadanych przekrojach oraz o założonych masach.

Pole przekroju przewodu S [mm^2]	Długość przewodu stanowiącego dodatkowy ładunek statku powietrznego [m] w zależności od masy przewodu podwieszonego pod bezzałogowy statek powietrzny			
	0,25 [kg]	0,50 [kg]	2,50 [kg]	4,00 [kg]
0,50	55,7	111,5	446,3	892,60
0,75	37,1	74,3	297,5	594,80
1,00	28,5	56,9	227,7	455,40
1,50	18,2	36,4	145,7	291,50
2,50	11,0	22,0	88,2	176,30
4,00	7,1	14,2	56,9	113,80
6,00	4,5	9,1	36,4	72,90
10,00	2,7	5,5	22,0	44,02
16,00	1,7	3,5	14,1	28,20
25,00	1,1	2,2	8,9	17,90
35,00	0,8	1,6	6,4	12,90
50,00	0,5	1,1	4,5	8,90

Jak można wyczytać z tabeli 1, dla pól przekroju poprzecznego do 4 mm^2 długość przewodu, który może zostać podwieszony pod bezzałogowy statek powietrzny, jest wystarczająca do spowodowania zwarcia przewodów fazowych na słupie. Dla mniejszych przekrojów przewodu jego długość będzie wystarczająca, by dokonać zwarcia – doziemienia – pomiędzy przewodem fazowym a ziemią. Gdy przewód podwieszony pod bezzałogowy statek powietrzny zostanie zawieszony na przewodzie fazowym instalacji elektrycznej, nastąpi zwarcie, a przez przewód zwierający popłynie prąd zwarcia. Przewód taki może ulec stopieniu, a przybliżony czas jego topienia będzie zależał od jego pola powierzchni przekroju poprzecznego oraz od natężenia prądu zwarcia[10]. Przybliżone wartości natężenia prądów, które spowodują stopienie przewodu w deklarowanym czasie, zostały zestawione w tabeli 2. Przybliżenie to wynika z innych pól przekroju S przewodów stosowanych w Stanach Zjednoczonych.

[10] W.H. Preece, *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, t. 43; W.H. Preece, *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, t. 44; E.R. Stauffacher, *Short-time Current Carrying Capacity of Copper Wire*, „General Electric Review" 1928, t. 31, nr 6.

Tab. 2. Zestawienie przybliżonych natężeń prądu elektrycznego, które dla zadanych przekrojów wywołają stopienie przewodu po deklarowanym czasie.

Pole przekroju przewodu S [mm²]	Orientacyjna wartość natężenia prądu elektrycznego płynącego w deklarowanym czasie do momentu stopienia przewodu [A] w zależności od czasu przepływu prądu elektrycznego		
	10 s	1 s	32 ms
0,50	58,5	158	882
0,75	83,0	250	1 400
1,00	99,0	316	1 800
1,50	140,0	502	2 800
2,50	198,0	798	4 500
4,00	280,0	1 300	7 100
6,00	396,0	2 000	11 000
10,00	561,0	3 200	18 000
16,00	795,0	5 100	28 000
25,00	1 100,0	8 100	45 000
35,00	1 300,0	10 200	57 000
50,00	1 900,0	16 000	91 000

Czasy wyłączenia zwarć zostały opisane w dokumentacji technicznej[11] i wynoszą odpowiednio 120 ms dla sieci 400 kV i 220 kV oraz 150 ms dla sieci 110 kV. Natężenia prądów przepływających przez linie są bardzo różne i zależą między innymi od typu linii. Maksymalne wartości zmierzonych prądów mogą sięgać nawet 1152 A[12]. Oznacza to, że praktycznie każdy ze wskazanych w tabeli przewodów powinien ulec stopieniu przed wyłączeniem zabezpieczeń linii. W przypadku ataku na stacje rozdzielcze napięć wysokich oraz stacje transformatorowe, które są instalacjami skomplikowanymi, niechronionymi od góry, skutki ataku mogą być poważniejsze. Ze względu na skomplikowanie budowy instalacji przedstawionej na rysunku 2 trudno jednak oszacować stopień, w jakim zostaną uszkodzone elementy instalacji.

[11] PSE Operator SA, *Standardowe Specyfikacje Funkcjonalne. Elektroenergetyczna automatyka zabezpieczeniowa, pomiary i układy obwodów wtórnych*, Warszawa 2010 (aktualizacja 2012 r.).

[12] M. Jaworski, M. Szuba, *Analiza obciążeń napowietrznych linii najwyższych napięć w aspekcie wytwarzania pola magnetycznego*, „Przegląd Elektrotechniczny" 2015, nr 5.

Rys. 2. Stacja rozdzielcza wysokich napięć 400/110 kV.

Źródło: https://elbud.katowice.pl/pl,30,3,projekty-rozbudowa-stacji-400_110-kv-dobrzen.html [dostęp: 30 XI 2021].

Konsekwencje uszkodzenia linii przesyłowych lub stacji obsługi mogą być zbliżone do tych, które zaobserwowano w czasie awarii w stacji Rogowiec (przez nią elektrownia w Bełchatowie jest podłączona do krajowego systemu sieci przesyłowych). Jak wskazano w raporcie[13], przyczyną awarii był błąd ludzki, który doprowadził do zwarcia w instalacji elektrycznej. Na skutek awarii wyłączona została większość bloków Elektrowni Bełchatów.

Warto nadmienić, że nie ma zakazu wykonywania lotów ponad liniami przesyłowymi. Przepisy prawa[14] stanowią jedynie, że operacje przeprowadzane z użyciem bezzałogowych statków powietrznych kategorii otwartej oraz kategorii szczególnej nad liniami energetycznymi oraz innymi urządzeniami znajdującymi się w otwartym terenie,

[13] https://businessinsider.com.pl/wiadomosci/awaria-elektrowni-belchatow-pse-podaje-przyczyny/qpp086b [dostęp: 30 XI 2021]; https://www.teraz-srodowisko.pl/aktualnosci/elektrownia-belchatow-awaria-stacja-rozdzielcza-PSE-10340.html [dostęp: 30 XI 2021]; https://www.cire.pl/artykuly/serwis-informacyjny-cire-24/184908-poniedzialkowa-awaria-odlaczyla-od-sieci-niemal-cala-elektrownie-belchatow [dostęp: 30 XI 2021]

[14] *Wytyczne nr 7 Prezesa Urzędu Lotnictwa Cywilnego z dnia 9 czerwca 2021 r. w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.*

których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzkiego oraz środowiska albo spowodować poważne straty materialne, wykonuje się z zachowaniem szczególnej ostrożności.

Metody detekcji bezzałogowych statków powietrznych

Do najczęściej stosowanych metod wykrywania bezzałogowych statków powietrznych należą:

- metody radarowe,
- metody wykrywające komunikację między lecącą platformą bezzałogową a stacją naziemną,
- metody wykrycia sygnału akustycznego emitowanego przez wirujące części lecącej platformy bezzałogowej,
- metody oparte na analizie obrazu zarówno widzialnego, jak i podczerwonego.

Żadna z tych metod użyta oddzielnie nie daje pewności wykrycia lecącego obiektu. Dlatego systemy wykrywające bezzałogowe statki powietrzne zbudowane są z różnych urządzeń detekcyjnych, działających na różnych zasadach. Obecnie wiele firm rozwija systemy antydronowe, należy się więc spodziewać, że ich sprzedaż w związku z rosnącą liczbą statków bezzałogowych również będzie rosła. Wraz ze zwiększeniem się funkcjonalności bezzałogowych statków powietrznych zmienia się też funkcjonalność systemów antydronowych.

Wykrycie statku za pomocą radarów jest metodą znaną z lotnictwa załogowego. Radary służące do wykrywania dronów są jednak inne niż te, które służą do wykrywania załogowych statków powietrznych. Te ostatnie wykrywają obiekty o większej powierzchni odbicia wiązki oraz o większej prędkości postępowej niż statki bezzałogowe[15]. Zaletą tej metody jest możliwość wykrycia ataku, gdy jest on realizowany na dużych wysokościach. Radar skutecznie wykryje statek powietrzny, jeśli między anteną radaru a lecącym statkiem powietrznym nie będzie przeszkód. Wykryje również przelot bezzałogowego statku powietrznego, jeśli będzie on daleko od anteny radarowej. Niestety wadą tego sposobu detekcji jest to, że bezzałogowy statek powietrzny korzystający z lidarowego

[15] https://www.defence24.pl/dlaczego-konflikt-w-gorskim-karabachu-powinien-zmienic-wojsko-polskie [dostęp: 30 XI 2021].

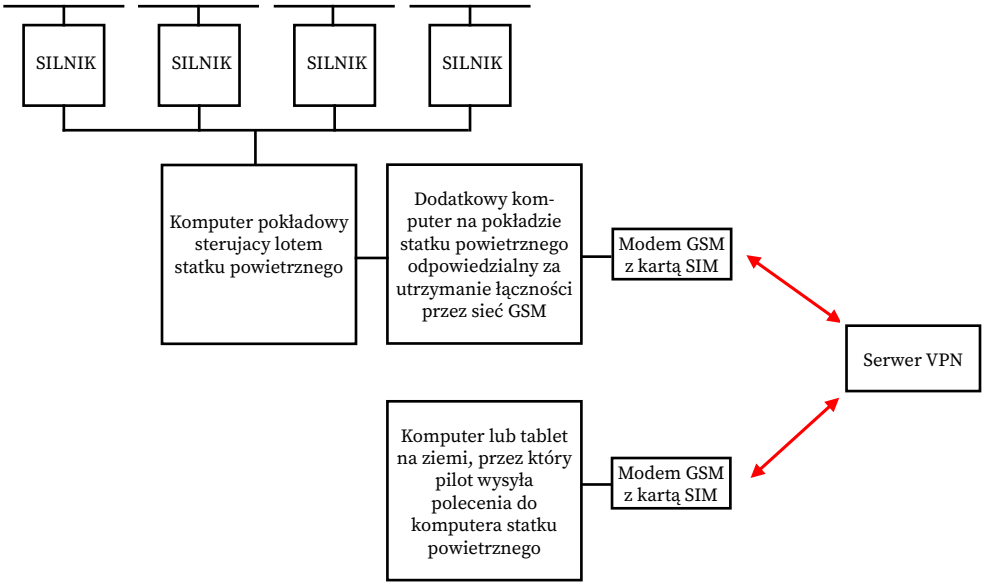
systemu pomiaru odległości, w tym odległości od ziemi, może przemieszczać się tuż nad powierzchnią ziemi. W takiej sytuacji system radarowy nie wykryje lecącego bezzałogowca. Ten sam system lidarowy pozwoli dronowi wykryć i ominiąć przeszkody terenowe. Rynek jest obecnie dość mocno nasycony antydronowymi systemami radarowymi[16]. Wydaje się jednak, że próby wykrycia drona lecącego w terenie gęsto zabudowanym będą w większości przypadków nieskuteczne.

Bezzałogowy statek powietrzny może być także wykryty dzięki monitoringowi komunikacji – sterowania pomiędzy lecącą platformą bezzałogową a stacją naziemną. Do najbardziej popularnych metod sterowania bezzałogowym statkiem powietrznym należy sterowanie z wykorzystaniem aparatury nadawczej, tzw. nadajnika, który znajduje się na ziemi, w ręku pilota. Aparatura taka wyposażona jest w dwa drążki umożliwiające sterowanie platformą w każdym kierunku oraz zestaw przełączników i pokręteł pozwalających na obsługę dodatkowych urządzeń pokładowych. Za pomocą pokręteł można na przykład sterować pracą gimbala z kamerą pokładową, a za pomocą zestawu przełączników innymi urządzeniami, takimi jak np. podnoszone podwozie lub klucz zwalniający podwieszony ładunek, co pozwala na zrzut tego ładunku w wybranym miejscu. Łączność pomiędzy nadajnikiem a komputerem bezzałogowego statku powietrznego może odbywać się na dwóch częstotliwościach: sterowanie platformą na częstotliwości 2,4 GHz, a przesył obrazu z kamery na 5,8 GHz. W typowych rozwiązaniach ten sposób sterowania pozwala na kontrolę nad bezzałogowym statkiem powietrznym na dystansie do 3 lub 4 kilometrów.

Druga metoda sterowania platformą to wysyłanie rozkazów z ziemi do komputera sterującego bezzałogowym statkiem powietrznym za pomocą komputera naziemnego i tableta wykorzystującego tzw. kanał telemetrii. Telemetria to dwukierunkowy kanał łączności odpowiedzialny za przesyłanie z platformy na ziemię parametrów statku powietrznego, w tym takich jak: położenie, wysokość, prędkość postępowa w poziomie, prędkość wznoszenia lub opadania, stan naładowania baterii, a także pochylenie do przodu lub do tyłu i przechylenie w lewo lub w prawo. Telemetria pozwala też na przesłanie do statku powietrznego rozkazu od pilota. Taki rozkaz może zostać zdefiniowany na ziemi przez wyrysowanie w programie obsługującym telemetrię zadanego

[16] https://www.hertzsystems.com/en/antidrone-systems/ [dostęp: 30 XI 2021].

położenia geograficznego platformy, jej wysokości w danym położeniu, prędkości postępowej, którą platforma powinna osiągnąć w drodze do kolejnego położenia, oraz tzw. POI's (ang. *Point of Interest*), czyli punktów, w których stronę w czasie lotu bezzałogowy statek powietrzny powinien skierować obiektyw kamery. Komunikacja pomiędzy statkiem powietrznym a pilotem odbywa się tym kanałem na różnych częstotliwościach, np. 433 MHz lub 868 MHz. Odległość komunikowania się za pomocą telemetrii jest większa niż odległość komunikowania się za pomocą częstotliwości 2,4 GHz lub 5,8 GHz i może wynosić nawet powyżej 20 kilometrów. Bezzałogową platformą latającą można też sterować dzięki wykorzystaniu sieci GSM. Schemat takiego systemu sterującego został pokazany na rysunku 3.



Rys. 3. Schemat komunikacji pomiędzy bezzałogowym statkiem powietrznym a pilotem za pomocą sieci GSM.

Źródło: Opracowanie własne.

Łączność realizowana przez sieć GSM pozwala na sterowanie bezzałogowym statkiem powietrznym bez ograniczeń związanych z odległością. Pilot statku powietrznego może nim sterować, znajdując się w dowolnym miejscu na ziemi. Jedynym warunkiem, jaki musi być spełniony, by realizować takie połączenie, jest dostęp do sieci GSM

zarówno pilota, jak i statku powietrznego. Łączność realizowana jest przez serwer VPN, jest to zatem łączność szyfrowana.

Obecne systemy detekcji lecącego bezzałogowego statku powietrznego kontrolują widmo częstotliwościowe promieniowania elektromagnetycznego w rejonie lokalizacji detektora. Ponieważ standardowe bezzałogowce wykorzystują do komunikacji z pilotem promieniowanie elektromagnetyczne o znanych częstotliwościach, detektor potrafi wykryć pojawienie się źródła emisji takiego promieniowania. Możliwe jest przy tym wykorzystanie technologii sztucznej inteligencji oraz uczenia maszynowego do wskazania detektorowi, które źródła to statki bezzałogowe, a które nimi nie są[17]. Warto zwrócić uwagę, że te systemy mogą wykryć bezzałogowe statki powietrzne, które podczas lotu utrzymują łączność ze stacją naziemną. Zazwyczaj wykrywają one typowe statki powietrzne, powszechnie dostępne na półkach sklepowych. Stają się natomiast nieskuteczne, gdy statek powietrzny został zaprogramowany przed startem i leci, nie komunikując się ze stacją bazową, lub łączność ze stacją bazową utrzymuje na nietypowych częstotliwościach. Dodatkowo elementy elektroniczne, z których zbudowany jest dron, mogą być odseparowane od otoczenia tzw. klatką Faradaya, gdyż uniemożliwia ona przenikanie promieniowania elektromagnetycznego do wnętrza statku powietrznego i z jego wnętrza na zewnątrz. Nie da się wówczas go wykryć, ponieważ klatka Faradaya izoluje go od detektorów promieniowania elektromagnetycznego. Do wykrycia typowych statków powietrznych można stosować monitory kontrolujące pracę wybranych modeli statków powietrznych. Do takich monitorów należy urządzenie AeroScope, które pozwala na wykrycie komunikacji oraz stanu statku powietrznego w czasie rzeczywistym. Urządzenie takie wykrywa jednak tylko drony firmy DJI[18].

Kolejna metoda detekcji bezzałogowych statków powietrznych polega na wykrywaniu hałasu, którego źródłem są ich rotujące elementy. W bezzałogowych statkach powietrznych źródłem hałasu są śmigła i w mniejszym stopniu silniki. Każdy lecący bezzałogowiec emituje dźwięk, przy czym częstotliwość i natężenie fali dźwiękowej zależą od kształtu śmigła i prędkości kątowej, z jaką się to śmigło obraca.

[17] https://www.droneshield.com/ [dostęp: 30 XI 2021]; https://www.dedrone.com/ [dostęp: 30 XI 2021]; https://www.echodyne.com/security/counter-drone-radar/ [dostęp: 30 XI 2021].

[18] https://www.dji.com/pl/aeroscope [dostęp: 30 XI 2021].

Istnieją metody redukcji hałasu emitowanego przez bezzałogowe statki powietrzne[19]. Polegają one m.in. na stosowaniu napędów o niższej prędkości rotacji śmigieł, śmigieł o różnej liczbie łopat, czy też śmigieł o różnym profilu aerodynamicznym. Bezzałogowy statek powietrzny może zatem nie zostać wykryty, jeśli będzie emitował hałas o niskim natężeniu oraz będzie leciał w miejscu, w którym występują inne źródła hałasu, takie jak pojazdy komunikacji miejskiej, samoloty załogowe w czasie startu i lądowania, inne hałasy, których źródłem jest działalność człowieka. Nie należy też zapominać o tym, że statek powietrzny typu samolot może zbliżyć się do chronionego obiektu lotem szybowcowym, zatem nie będzie źródłem hałasu pochodzącego od śmigieł.

Ostatnią istotną metodą identyfikacji bezzałogowych statków powietrznych jest analiza przestrzeni za pomocą kamer pracujących zarówno w obszarze widzialnym, jak i w podczerwieni. Analiza obrazu odbywa się z użyciem systemu komputerowego, który na podstawie obrazu rejestrowanego przez kamerę rozpoznaje, czy lecący obiekt jest dronem czy np. ptakiem. Systemy detekcji wizualnej bazują na nauczaniu maszynowym oraz technologii sztucznej inteligencji. Nauczenie komputera rozpoznawania obiektu jest procesem żmudnym, czasochłonnym, wymagającym dużej mocy obliczeniowej oraz dużej bazy zdjęć źródłowych przedstawiających obiekt, który ma zostać wykryty. Systemy takie wykrywają statki typowe. Gdy statek powietrzny będzie miał kształt nietypowy, jego wykrycie będzie niemożliwe. Bezzałogowe statki powietrzne można budować tak, by kształty były bardzo nietypowe. Głośne było np. zbudowanie przez członków Greenpeace drona w kształcie Supermana i rozbicie go o betonową osłonę reaktora w elektrowni jądrowej Bugey we Francji[20]. Moment ataku przedstawiono na rysunku 4. Samo uderzenie bezzałogowcem o ścianę osłony reaktora nie zagroziło bezpieczeństwu reaktora.

[19] F.B. Metzger, *An Assesment of Propeller Aircraft Noise Reduction Technology*, NASA Contractor Report 198237, 1995; W. Yuliang i in., *Noise Reduction of UAV Using Biomimetic Propellers with Varied Morphologies Leading-edge Serration*, „Journal of Bionic Engineering" 2020, t. 17, s. 767–779.

[20] https://www.reuters.com/article/uk-france-nuclear-greenpeace-idUKKBN1JT17G [dostęp: 30 XI 2021].

Rys. 4. Moment ataku na reaktor jądrowy za pomocą drona w kształcie Supermana.

Źródło: https://www.reuters.com/article/uk-france-nuclear-greenpeace-idUKKBN1JT17G [dostęp: 30 XI 2021].

Ściany takie buduje się tak, aby wytrzymywały uderzenie samolotu załogowego, który lecąc z dużą prędkością i mając dużą masę, uderzałby w cel z dużą energią kinetyczną. Przypadek ten jednak pokazał, jak nieodporne na działania z użyciem dronów są chronione obiekty, zwłaszcza zbudowane w czasach, gdy drony nie były jeszcze tak powszechnie dostępne. Kamery działające w paśmie widzialnym promieniowania elektromagnetycznego nie są w stanie wykryć lecącego statku powietrznego w warunkach słabej widoczności. Analiza przestrzeni za pomocą kamer pracujących w zakresie podczerwieni fal elektromagnetycznych pozwala na wykrycie źródeł ciepła innych niż te, które w przestrzeni znajdują się naturalnie. Kamera podczerwona potrafi wykryć i wyróżnić bezzałogowy statek powietrzny, ponieważ na jego pokładzie wykorzystywane są elementy, które w czasie pracy emitują ciepło. Do takich elementów można zaliczyć silniki elektryczne i spalinowe oraz baterie litowo-polimerowe, które w czasie pracy samoczynnie się podgrzewają. Kamera działająca na podczerwień może wykryć lecący statek powietrzny w nocy. Przy czym również taki sposób detekcji bezzałogowców nie zawsze jest skuteczny. Wiedza na temat

lotnictwa załogowego wskazuje, że można zbudować statek w taki sposób, by energia cieplna była w znacznym stopniu rozpraszana, a tym samym by statek powietrzny nie był wykrywalny.

Wybrane metody neutralizacji bezzałogowych statków powietrznych

Sam proces detekcji bezzałogowego statku powietrznego to tylko pierwszy etap obrony przed jego atakiem. Do neutralizacji wrogich bezzałogowych statków powietrznych stosuje się następujące metody:

- trafienie i splątanie elementów ruchomych bezzałogowego statku powietrznego siatką,
- zakłócenie pozycjonowania systemu satelitarnego, z którego korzysta statek powietrzny,
- zakłócenie komunikacji statek powietrzny–stacja naziemna,
- użycie światła laserowego o dużej mocy,
- uszkodzenie układów elektronicznych za pomocą impulsu elektromagnetycznego o dużej mocy.

Trafienie i splątanie bezzałogowego statku powietrznego jest procesem trudnym. Atakujący statek powietrzny może być statkiem typu multirotor, samolot lub śmigłowiec. Może też łączyć cechy wszystkich wyżej wymienionych typów i wtedy powstaje ich hybryda. Do takich hybryd należą samoloty mające możliwość pionowego startu, tzw. V-tol (od ang. *Vertical Take Off and Landing*). Każde z tych urządzeń ma różne cechy fizyczne, wobec których metoda neutralizacji za pomocą siatki będzie nieskuteczna. Do takich cech należy na pewno prędkość postępowa statku w locie. Samolot porusza się z dużą prędkością, multirotor zaś ze stosunkowo niewielką. Urządzenie miotające może znajdować się w ręku członka personelu ochrony obiektu lub zostać podwieszone pod inny statek powietrzny pilotowany przez członka personelu ochrony obiektu. Systemy siatkowe stosowane do neutralizacji statków powietrznych są skuteczne, gdy atakujący statek porusza się z niewielką prędkością lub pozostaje w tzw. zawisie. Podstawowym problemem podczas stosowania tej metody jest niewielka odległość urządzenia miotającego siatkę od celu. Po skutecznym trafieniu bezzałogowy statek powietrzny splątany siatką opada na ziemię z pomocą systemu spadochronowego. Dzięki niewielkiej prędkości opadania nie rozbije się o ziemię, nie uszkodzi elementów infrastruktury ani nie spowoduje

utraty zdrowia lub życia, gdy upadnie na człowieka. Nieuszkodzony statek powietrzny wraz z komputerem na jego pokładzie może stanowić dowód dla sądu w razie wykrycia sprawcy ataku.

Inną metodą neutralizacji lecącego statku powietrznego jest zakłócenie sygnału systemu pozycjonowania satelitarnego lub podszycie się pod ten system. O zakłóceniach lub podszyciu się pod sygnał satelitarny informują doniesienia prasowe[21]. Zakłócenie polega na tym, że z urządzenia zakłócającego emituje się sygnał o częstotliwościach, na jakich pracuje system pozycjonowania. Sygnał zakłócający ma większą moc niż sygnał satelitarny. W takiej sytuacji służący do nawigacji odbiornik satelitarny, który znajduje się na pokładzie bezzałogowego statku powietrznego, za właściwy uznaje sygnał z urządzenia zakłócającego i korzystając z niego, nie jest w stanie właściwie określić swojego położenia. Podszycie się polega na tym, że urządzenie podszywające się emituje sygnał zawierający zafałszowane położenie. Tym sposobem statek powietrzny zamiast do celu poleci w miejsce wskazane przez urządzenie neutralizujące i atak będzie nieskuteczny. Odpowiedzią na ten sposób obrony może być nawigacja, która pozwala na określenie położenia statku powietrznego przy braku dostępu do sygnału systemu pozycjonowania. Taka nawigacja pozwala także na przelot bezzałogowego statku powietrznego w budynkach lub w kopalniach[22]. Systemy do nawigacji w warunkach braku dostępu do sygnału satelitarnego identyfikują położenie statku powietrznego na podstawie odczytu z lidaru, urządzeń mierzących odległość z użyciem ultradźwięków, systemów kamer działających w obszarze widzialnym lub w podczerwieni[23]. Systemy do nawigacji w warunkach braku dostępu do sygnału satelitarnego będą się rozwijały w sposób gwałtowny ze względu na możliwości uszkodzenia satelitów w razie wojny[24]. Metodą nawigacji bez użycia satelitarnego

[21] https://www.techtarget.com/searchsecurity/definition/GPS-jamming [dostęp: 30 XI 2021]; https://www.militaryaerospace.com/rf-analog/article/14207023/gps-signals-jamming [dostęp: 30 XI 2021]; https://www.c4isrnet.com/newsletters/military-space-report/2020/04/15/natos-new-tool-shows-the-impact-of-gps-jammers/ [dostęp: 30 XI 2021].

[22] https://polskiprzemysl.com.pl/przemysl-energetyczny/gornictwo-urzadzenia-maszyny/drony-w-kopalniach/ [dostęp: 30 XI 2021].

[23] F. He i in., *Automated Aerial Triangulation for UAV-Based Mapping*, „Remote Sensing" 2018, nr 10 (12), 1952.

[24] https://spidersweb.pl/2021/11/rosja-satelita-smieci-kosmiczne.html [dostęp: 30 XI 2021].

systemu pozycjonowania jest również rozstawienie naziemnych stacji emitujących sygnał położenia i nawigacja na podstawie triangulacji[25].

Urządzenia zakłócające sygnał komunikacji między statkiem powietrznym a stacją naziemną emitują promieniowanie elektromagnetyczne o dużej mocy, o różnych częstotliwościach, w których zawarte są częstotliwości używane przez bezzałogowy statek powietrzny. Zakłócenie komunikacji odbywa się poprzez emisję fali elektromagnetycznej o widmie całkowicie płaskim i intensywności szumu równomiernej w całym zagłuszanym paśmie. Jest to tzw. biały szum[26]. Równomierność ta oznacza, że dla każdej częstotliwości szumu elektromagnetycznego moc emitowanej fali jest taka sama. Taki szum zagłusza komunikację pomiędzy statkiem powietrznym a pilotem, uniemożliwiając sterowanie. Systemy zakłócające można ominąć w sposób dość prosty, tzn. przez stosowanie do komunikacji statek–pilot nietypowych częstotliwości nieużywanych w powszechnie dostępnych statkach powietrznych lub przez ukrywanie urządzeń elektronicznych statku powietrznego w klatce Faradaya. Inną metodą uniemożliwiającą neutralizację statku powietrznego jest programowanie misji przed lotem i wykonanie lotu w sposób autonomiczny, tzn. bez udziału pilota, na podstawie poleceń wydanych przed startem.

Użycie impulsu laserowego o dużej mocy jest metodą skuteczną w odpowiednich warunkach. Światło laserowe oświetla lecący statek powietrzny i powoduje jego zapalenie. Metoda ta jest rozwijana obecnie w wielu krajach[27]. Zaletą tego sposobu niszczenia drona jest możliwość jego strącenia ze stosunkowo dużej odległości. Wady systemu zaś to: wymóg zasilania lasera ze źródła dużej mocy, wrażliwość na warunki pogodowe, w tym mgłę lub deszcz. System ten może niszczyć bezzałogowe statki powietrzne pojedynczo. Gdy atak przeprowadzany jest za

[25] R. Kapoor i in., *UAV Navigation Using Signals of Opportunity in Urban Environments. An Overview of Existing Methods*, 1st International Conference on Energy and Power, ICEP 2016, 14–16 grudnia 2016, Melbourne, Australia.

[26] B. Carter, R. Mancini, *Op Amps for Everyone,* Burlington 2009, s. 174–175.

[27] https://www.rafael.co.il/worlds/air-missile-defense/c-uas-counter-unmanned-aircraft-systems/ [dostęp: 30 XI 2021]; https://www.thedefensepost.com/2021/07/09/france-anti-drone-laser/ [dostęp: 30 XI 2021]; https://www.aerospacetestinginternational.com/news/defense/us-air-force-progresses-testing-of-anti-drone-laser-weapons.html [dostęp: 30 XI 2021].

pomocą wielu dronów lub wręcz z użyciem roju, system ten ma ograniczoną skuteczność.

Uszkodzenie układów elektronicznych za pomocą impulsu elektromagnetycznego o dużej mocy jest techniką znaną z zastosowań militarnych. Bezzałogowy statek powietrzny to obiekt techniczny, w którym wykorzystuje się systemy zaawansowanej elektroniki. Do urządzeń elektronicznych stosowanych w dronach należą: komputer sterujący, dodatkowy komputer mogący służyć do wykonywania obliczeń, np. analizy obrazu, elektroniczne sterowniki obrotów silników statku powietrznego, odbiorniki służące do otrzymywania rozkazów od pilota, urządzenia telemetrii służące do wymiany pomiędzy statkiem a stacją naziemną informacji np. o stanie statku powietrznego, urządzenia nawigacji satelitarnej itd. Statki powietrzne mogą być zabezpieczone przed impulsem elektromagnetycznym przez stosowanie wielowarstwowych zasobników ekranujących urządzenia elektroniczne od impulsu.

Wszystkie wyżej wymienione metody charakteryzują się ograniczoną skutecznością, należy zatem poszukiwać innych sposobów ochrony obiektu. Dla bezpieczeństwa lub obronności państwa ważna jest prewencja, zapobieganie rozpoczęciu ataku. Do metod wykorzystywanych w ramach takich działań należą:

- zabezpieczenie chronionego obiektu strefą DRA-P,
- stosowanie urządzeń odcinających możliwość wykonania lotu w chronionej przestrzeni,
- szkolenie funkcjonariuszy Policji z przepisów prawa lotniczego, procedur obowiązujących w lotnictwie bezzałogowym oraz przepisów pozwalających na ukaranie pilotów wykonujących loty niezgodnie z prawem,
- szkolenie pracowników ochrony obiektu z pilotażu statków typu multirotor oraz samolot,
- maskowanie elementów infrastruktury chronionego obiektu,
- osłona elementów infrastruktury przed uderzeniem lub przed skutkami ładunku wybuchowego przenoszonego przez statek powietrzny,
- działania na rzecz lokalnej społeczności.

Zabezpieczenie chronionego obiektu strefą DRA-P

Zgodnie z obecnie obowiązującymi wytycznymi Prezesa Urzędu Lotnictwa Cywilnego[28] Polska Agencja Żeglugi Powietrznej (PAŻP) może wyznaczyć następujące dronowe strefy geograficzne:

a) DRA-T – strefę, w której lot bezzałogowego statku powietrznego jest możliwy po spełnieniu przez ten statek wymogów technicznych wskazanych przez PAŻP. W strefie tej dopuszcza się spełnienie dodatkowych warunków wykonania lotu, w tym na przykład warunku uzyskania zgody na wykonanie lotu;
b) DRA-U – strefę, w której lot bezzałogowego statku powietrznego może się odbyć wyłącznie przy wsparciu wymaganych dla tej strefy usług i na warunkach wykonania lotu wskazanych przez PAŻP;
c) DRA-I – strefę informacyjną, w której zgoda na wykonanie lotu nie jest wymagana, ale dla zapewnienia bezpieczeństwa lotu wymagane jest zapoznanie się z informacjami;
d) DRA-P – strefę zakazaną, w której operacje przy użyciu systemów bezzałogowych statków powietrznych nie mogą być wykonywane;
e) DRA-R – strefę ograniczoną dla systemów bezzałogowych statków powietrznych, w której operacje przy użyciu tych systemów mogą być wykonywane za zgodą i na warunkach określonych przez PAŻP lub podmiot uprawniony, na którego wniosek strefa geograficzna została wyznaczona.

Strefa DRA-R może się składać z dodatkowych podstref oznaczonych jako:

1. DRA-RH – w której prawdopodobieństwo uzyskania zgody na lot przy użyciu bezzałogowego statku powietrznego jest wysokie (ang. *high*);
2. DRA-RM – w której prawdopodobieństwo uzyskania zgody na lot przy użyciu bezzałogowego statku powietrznego jest średnie (ang. *middle*),
3. DRA-RL – w której prawdopodobieństwo uzyskania zgody na lot przy użyciu bezzałogowego statku powietrznego jest niskie (ang. *low*).

[28] Zob. *Wytyczne nr 7 Prezesa Urzędu Lotnictwa Cywilnego z dnia 9 czerwca 2021 r. w sprawie zasobów…*

Ze względu na potrzeby działań albo czynności o szczególnym znaczeniu operacyjnym lub rozpoznawczym dla zapewnienia bezpieczeństwa państwa lub porządku publicznego, prowadzonych w celu realizacji ustawowych działań, strefy geograficzne mogą być wyznaczone na wniosek Dowódcy Operacyjnego Rodzajów Sił Zbrojnych, Komendanta Głównego Żandarmerii Wojskowej, Szefa Szefostwa Służb Ruchu Lotniczego Sił Zbrojnych RP, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Szefa Krajowej Administracji Skarbowej lub Komendanta Służby Ochrony Państwa. Ze względu na potrzeby ochrony obiektów infrastruktury krytycznej, zapobieganie skutkom klęsk żywiołowych lub ich usuwanie, ratowanie zdrowia lub życia ludzkiego strefy geograficzne mogą być wyznaczane na wniosek Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej lub Dyrektora Rządowego Centrum Bezpieczeństwa.

Obecnie na obszarze Unii Europejskiej obowiązują jednolite zasady wykonywania lotów bezzałogowymi statkami powietrznymi[29]. Zgodnie z tymi zasadami loty platform bezzałogowych wykonywane są w trzech różnych kategoriach. Każda kategoria odpowiada pewnemu poziomowi ryzyka związanego z wykonywaną misją. Wyróżnia się trzy poziomy ryzyka: niskie, dla kategorii OPEN (otwartej), średnie, dla kategorii SPECIFIC (szczególnej), oraz wysokie, dla kategorii CERTIFIED (certyfikowanej). Kategoria certyfikowana obejmuje loty, w czasie których przewozi się osoby lub materiały niebezpieczne. Kategoria szczególna to loty, które wymagają z zasady zgody na przeprowadzenie operacji. Zgodę taką, jako dorozumianą, mają piloci z uprawnieniami do lotów zgodnie z tzw. scenariuszami standardowymi. Scenariusze standardowe to zbiór zasad wykonywania lotów, których przestrzeganie gwarantuje, że misja wykonywana jest z ryzykiem akceptowalnym. Obecnie w Polsce obowiązuje osiem scenariuszy standardowych dotyczących lotów w zasięgu (VLOS) i poza zasięgiem wzroku (BVLOS) dla statków powietrznych takich jak samoloty, multirotory i śmigłowce o masie startowej do 4 kg

[29] *Rozporządzenie Wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych*; *Rozporządzenie Wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19* (Dz. Urz. UE L 176/13 z 5 VI 2020 r.).

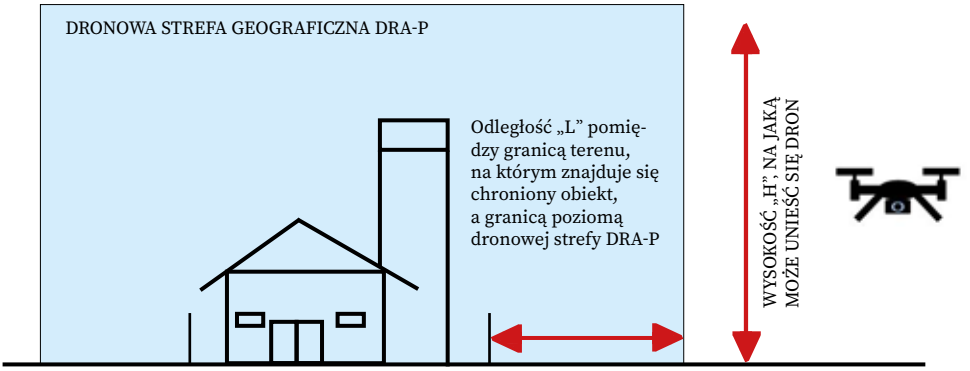
oraz dla statków powietrznych takich jak samoloty, multirotory i śmigłowce o masie startowej nieprzekraczającej 25 kg. Kategoria otwarta to loty obarczone niskim ryzykiem, w związku z czym nie jest wymagana zgoda na lot. Zgodnie z *Wytycznymi nr 7* loty w kategorii otwartej oraz w kategorii szczególnej w dronowej strefie geograficznej DRA-P odbywają się za zgodą zarządzającego daną strefą i na warunkach określonych dla tej strefy. *Wytyczne nr 7* nie obejmują zasad wykonywania lotów w kategorii certyfikowanej. Analiza dokumentacji lotniczej zawartej w komunikatach aplikacji DroneRadar (DroneRadar jest aplikacją na systemy Android oraz iOS, darmową i powszechnie dostępną w sklepach operatorów sieci komórkowych) wskazuje, że w strefach DRA-P wyznaczonych nad chronionymi obiektami dopuszcza się loty bezzałogowymi statkami powietrznymi, ale tylko do wysokości 30 m nad ziemią statkiem powietrznym o masie nie większej niż 0,9 kg oraz w odległości nie mniejszej niż 500 m od granicy chronionego obiektu. Zapisy te wskazują, że można stosować strefy DRA-P do ochrony obiektów, pod warunkiem że są one właściwie zaprojektowane.

Rozważmy dwa przypadki stref DRA-P wyznaczonej jak na rysunku 5.

1. Granice strefy DRA-P znajdują się w odległości „L" mniejszej niż 500 m od granic chronionego obiektu. Poza strefami, zgodnie z ogólnymi zasadami wykonywania lotów, bezzałogowy statek powietrzny może lecieć do wysokości „H" nie większej niż 120 m nad powierzchnią ziemi. Korzystając z twierdzenia Pitagorasa, można obliczyć kąt, pod jakim kamera z platformy bezzałogowej może obserwować chroniony obiekt, gdy lot odbywa się na maksymalnej dopuszczalnej wysokości. Minimalny kąt, pod jakim może obserwować obiekt, to 15 stopni, przy czym im odległość od granicy chronionego obiektu do granicy strefy DRA-P będzie mniejsza, tym kąt obserwacji będzie większy. Na przykład jeśli granice strefy DRA-P zostaną wyznaczone w odległości „L" wynoszącej ok. 120 m, to kąt obserwacji obiektu z platformy będzie równy 45 stopni.
2. Granice strefy DRA-P znajdują się w odległości „L" większej niż 500 m od granic chronionego obiektu. Zgodnie z zasadami platforma bezzałogowa może wykonać lot w przestrzeni pomiędzy 500. metrem liczonym od granic obiektu a granicą strefy DRA-P. Lot może się odbyć do wysokości 30 m ponad powierzchnią ziemi. Korzystając z twierdzenia Pitagorasa, można obliczyć

kąt, pod jakim kamera z platformy bezzałogowej może obserwować chroniony obiekt, gdy lot odbywa się na maksymalnej dopuszczalnej wysokości. Maksymalny kąt, pod jakim może obserwować obiekt, to 15 stopni, przy czym im pozioma odległość lecącej platformy od granicy chronionego obiektu będzie większa, tym kąt obserwacji będzie mniejszy. Jeśli pomiędzy chronionym obiektem a okiem kamery będą jakieś naturalne przeszkody terenowe, np. drzewa, to obserwacja obiektu będzie praktycznie niemożliwa.

Decyzja o wyznaczeniu strefy DRA-P nad obiektem powinna zostać podjęta po gruntownej analizie rzeczywistych zagrożeń i ocenie podatności obiektu na atak z użyciem bezzałogowego statku powietrznego. Dopiero jeśli ocena zagrożeń i podatności na atak wskaże, że ryzyko związane z potencjalnym atakiem na obiekt jest nieakceptowalne, należy wyznaczyć strefę. Wyznaczenie takiej strefy jest jasnym wskaźnikiem, że w danym obiekcie dzieje się coś ważnego z punktu widzenia obronności lub bezpieczeństwa państwa.



Rys. 5. Schemat dronowej strefy geograficznej DRA-P.

Źródło: Opracowanie własne.

Stosowanie urządzeń uniemożliwiających wykonanie lotu w chronionej przestrzeni

Do urządzeń uniemożliwiających wykonanie lotu bezzałogowym statkiem powietrznym należy AeroScope[30]. Oddziałuje ono jednak wyłącznie na statki powietrzne firmy DJI. Nie jest w stanie zabezpieczyć chronionego obiektu przed statkami produkcji innych firm lub zbudowanymi przez niezależnych konstruktorów. AeroScope może zidentyfikować numer seryjny statku powietrznego, jego lokalizację odczytaną z odbiornika sygnału satelitarnego, prędkość i kierunek lotu oraz wysokość, na jakiej jest wykonywany lot. Odczyt tych parametrów odbywa się w czasie rzeczywistym. Polskie przepisy prawa nie wymagają rejestracji statku powietrznego, dlatego identyfikacja takiego statku i przypisanie go do konkretnego pilota są niezwykle trudne. Jedyną możliwością identyfikacji pilota jest deklaracja numeru seryjnego statku powietrznego, jaką każdy pilot musi złożyć, jeśli chce wykonać lot w lotniczej strefie CTR, i rejestracja drona, czyli podanie tego numeru w systemie Pansa_UTM[31]. Bez tej rejestracji nie jest możliwe uzyskanie warunków wykonania lotu w strefach CTR. Jeśli jednak statek powietrzny został wyprodukowany przez producenta innego niż DJI lub przez niezależnego konstruktora, urządzenie Aeroscope go nie zidentyfikuje. AeroScope może także ograniczyć możliwość wykonania lotu przez wyznaczenie strefy, w której lot się nie odbędzie. Funkcja taka nazywa się GeoFencing. Operator AeroScope może wskazać granice poziome oraz pionowe strefy, w której lot się nie może odbyć. Statki powietrzne firmy DJI nie będą zatem mogły wykonać lotu w tej strefie. Wadą urządzenia jest brak możliwości detekcji każdego modelu DJI oraz modeli innych niż produkowanych przez DJI. Dodatkowy problem stwarza przechowywanie danych zebranych przez AeroScope na serwerach chińskiej firmy DJI. Dane te mogą być użyte w celach pozyskania informacji o lokalizacji chronionych obiektów[32].

[30] https://www.dji.com/pl/aeroscope [dostęp: 30 XI 2021].

[31] https://utm.pansa.pl [dostęp: 30 XI 2021].

[32] https://www.911security.com/blog/dji-aeroscope-review-features-specs-and-how-its-used-in-layered-drone-detection [dostęp: 30 XI 2021].

Szkolenie funkcjonariuszy Policji z przepisów prawa lotniczego, procedur obowiązujących w lotnictwie bezzałogowym oraz przepisów pozwalających na ukaranie pilotów wykonujących loty niezgodnie z prawem

Szkolenie takie powinno być standardowym działaniem w jednostkach Policji, w których rejonie działania znajdują się obiekty ważne dla bezpieczeństwa lub obronności państwa. Szkolenie powinno swoim zakresem obejmować przepisy europejskie:

- *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego* (Dz. Urz. UE L 212/1 z 22 VIII 2018 r.);
- *Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich* (Dz. Urz. UE L 152/1 z 11 VI 2019 r.);
- *Rozporządzenie delegowane Komisji (UE) 2020/1058 z dnia 27 kwietnia 2020 r. zmieniające rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych* (Dz. Urz. UE L 232/1 z 20 VII 2020 r.);
- *Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych* (Dz. Urz. UE L 152/45 z 11 VI 2019 r.);
- *Rozporządzenie wykonawcze Komisji (UE) 2020/639 z dnia 12 maja 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do scenariuszy standardowych dla operacji wykonywanych w zasięgu widoczności wzrokowej lub poza zasięgiem widoczności wzrokowej* (Dz. Urz. UE L 150/1 z 13 V 2020 r.).

Szkolenie powinno także obejmować przepisy prawa krajowego, w tym *Ustawę z dnia 3 lipca 2002 r. Prawo lotnicze* (t.j.: DzU z 2020 r. poz. 1970, ze zm.) oraz wytyczne Prezesa ULC:

- *Wytyczne nr 7 Prezesa Urzędu Lotnictwa Cywilnego z dnia 9 czerwca 2021 r. w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych* (Dz. Urz. Urzędu Lotnictwa Cywilnego z 2021 r. poz. 35);

– *Wytyczne nr 24 Prezesa Urzędu Lotnictwa Cywilnego z dnia 30 grudnia 2020 r. w sprawie wyznaczania stref geograficznych dla systemów bezzałogowych statków powietrznych* (Dz. Urz. Urzędu Lotnictwa Cywilnego z 2020 r. poz. 78).

W przypadku obiektów zlokalizowanych w strefach wojskowych MCTR funkcjonariusze Policji powinni się także zapoznać z dokumentem:

– *Wytyczne Szefa Szefostwa Służby Ruchu Lotniczego Sił Zbrojnych Rzeczypospolitej Polskiej nr 6 z dnia 17 września 2018 r. w sprawie uszczegółowienia zasad wykonywania lotów modeli latających oraz bezzałogowych statków powietrznych o MTOW nie większej niż 25 kg w strefach ruchu lotniskowego lotnisk wojskowych (MATZ) oraz strefach kontrolowanych lotnisk wojskowych (MCTR),* (https://ssrlszrp.wp.mil.pl/u/Wytyczne_w_sprawie_wykonywania_lotow_przez_RPAS.pdf).

Dodatkowo funkcjonariusze Policji powinni zapoznać się z zasadami obsługi aplikacji DroneRadar służącej do obrazowania struktury przestrzeni powietrznej, w tym do identyfikacji granic poziomych dronowych stref geograficznych. Aplikacja ta pozwala także na odczytanie zasad wykonywania lotów bezzałogowymi statkami powietrznymi w strefach. Znajomość prawa oraz znajomość zasad wykonywania lotów pozwoli funkcjonariuszom Policji identyfikować pilotów, którzy realizują loty niezgodnie z zasadami wykonywania lotów.

Przepisy umożliwiające ukaranie pilotów wykonujących loty niezgodnie z przepisami zawarte są w różnych aktach prawnych. Wybrane przepisy, które mówią o odpowiedzialności karnej, to:

1. W zakresie ustawy Prawo lotnicze*:*
   a) Art. 211.1. Kto:
      5) wbrew art. 97 ustawy wykonuje lot lub inne czynności lotnicze, nie mając ważnej licencji lub świadectwa kwalifikacji lub niezgodnie z ich treścią i warunkami,
      6) wbrew art. 105 ust. 2 ustawy wykonuje loty lub inne czynności lotnicze mimo utraty wymaganej sprawności psychicznej i fizycznej,
      9a) wbrew art. 123 ust. 2 dokonuje w czasie lotu zrzutu ze statku powietrznego,

podlega karze grzywny, karze ograniczenia wolności lub pozbawienia wolności do roku.

b) Art. 212.1. Kto:
   1) wykonując lot przy użyciu statku powietrznego:
      a) narusza przepisy dotyczące ruchu lotniczego obowiązujące w obszarze, w którym lot się odbywa,
      b) przekracza granicę państwową bez wymaganego zezwolenia lub z naruszeniem warunków zezwolenia,
      c) narusza, wydane na podstawie art. 119 ust. 2 ustawy, zakazy lub ograniczenia lotów w polskiej przestrzeni powietrznej wprowadzone ze względu na konieczność wojskową lub bezpieczeństwo publiczne,

podlega karze pozbawienia wolności do lat 5.

2. W zakresie Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: DzU z 2021 r. poz. 2345, ze zm.):
   a) Art. 267.1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

   b) Art. 267.3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

W czasie szkolenia powinny być także wykładane inne przepisy mające wpływ na wykonywanie lotów, które zawarte są w aktach prawnych: Kodeks wykroczeń, Prawo atomowe, o ochronie osób i mienia, o ochronie przyrody, o prawie autorskim i prawach pokrewnych, o ochronie danych osobowych. Funkcjonariusz Policji znający ww. przepisy powinien mieć wiedzę, w jaki sposób utrudnić lub uniemożliwić lot bezzałogowym statkiem powietrznym w rejonie obiektu chronionego.

Szkolenie pracowników ochrony obiektu z pilotażu statków typu multirotor oraz samolot

Personel ochrony obiektu powinien mieć kompetencje do pilotażu statków powietrznych, umożliwiające im skuteczną ochronę chronionego obiektu. Statki powietrzne typu samolot zdolne są do długotrwałego lotu na duże odległości. Samoloty wyposażone w kamery działające w paśmie widzialnym oraz podczerwonym fali elektromagnetycznej pozwalają na obserwację przedpola chronionego obiektu zarówno w dzień, jak i w nocy. Wyposażenie tych statków w komputer z zainstalowanym oprogramowaniem wykorzystującym algorytmy AI wykrywające nietypową aktywność powinny umożliwić personelowi ochrony przygotowanie się na atak na ochraniany obiekt. Statek powietrzny typu multirotor pozwala na lot na niewielkim dystansie, ale może wykonać zawis w jednym miejscu. Taki zawis pozwala na długotrwałą obserwację miejsca, w którym zaobserwowana została podejrzana aktywność.

Maskowanie elementów infrastruktury chronionego obiektu

Jednym ze sposobów atakowania obiektów ważnych dla bezpieczeństwa i obronności państwa jest atak z użyciem kamer pracujących w paśmie widzialnym i w podczerwonym. Kamera może posłużyć do pozyskania informacji dotyczących wykorzystywanej w obiekcie technologii, urządzeń technicznych, z których wykonany jest system ochrony fizycznej, zwyczajów i procedur, zgodnie z którymi postępuje personel ochrony fizycznej lub inni pracownicy obiektu. Maskowanie elementów infrastruktury powinno zapobiec lub utrudnić pozyskanie z platformy bezzałogowej wrażliwych informacji.

Osłona elementów infrastruktury przed uderzeniem lub przed skutkami ładunku wybuchowego przenoszonego przez statek powietrzny

Bezzałogowy statek powietrzny może być użyteczną platformą służącą do przeniesienia ładunku wybuchowego lub ładunku zawierającego środki chemiczne. Ładunkiem wybuchowym łatwo uszkodzić elementy infrastruktury i spowodować spowolnienie lub wstrzymanie działalności obiektu. Taki sam skutek może wywołać również kontaminacja

obszaru obiektu lub jego przedpola. Konsekwencją takiego ataku będą straty finansowe dla operatora obiektu, straty finansowe dla odbiorców towarów lub usług realizowanych na terenie obiektu. Niewykluczone są także utrata zdrowia lub życia pracowników zaatakowanego obiektu oraz straty związane z zanieczyszczeniem środowiska. Osłonięcie ważnych elementów infrastruktury obiektu przed skutkami eksplozji ładunku wybuchowego lub przed bezpośrednim uderzeniem bezzałogowego statku powietrznego może uchronić obiekt przed skutkami ataku.

Działania na rzecz lokalnej społeczności

Obiekty ważne dla bezpieczeństwa lub obronności państwa bywają zlokalizowane w okolicach zamieszkanych. Właściwa współpraca pomiędzy operatorem obiektu a lokalną ludnością może wspomóc proces ochrony obiektu. Okoliczni mieszkańcy z łatwością rozpoznają osoby obce, zachowujące się w sposób nietypowy. Działania pozwalające na podniesienie stopnia kooperacji pomiędzy operatorem a lokalną ludnością to m.in.: ufundowanie stypendiów dla utalentowanej młodzieży, wsparcie dla lokalnych ośrodków zdrowia i szpitali, wspólne akcje typu „sprzątanie świata", zaproszenie miejscowej ludności do zwiedzania chronionego obiektu w miejscach, w których nie ma urządzeń wrażliwych z punktu widzenia ochrony informacji o technologii ani urządzeń ochrony fizycznej obiektu.

Wnioski

1. Paraliż działania państwa, w tym zakłócenie lub wstrzymanie pracy systemów infrastruktury krytycznej, może nastąpić nie tylko przez zaatakowanie dobrze chronionych obiektów, w których wytwarza się energię elektryczną, lecz także przez atak na niechronioną infrastrukturę służącą do dostarczenia energii do odbiorcy,
2. Sieć elektroenergetyczna w Polsce jest z wyjątkiem linii izolowanych nieodporna na ataki polegające na spowodowaniu zwarcia za pomocą przewodu podwieszonego pod bezzałogowym statkiem powietrznym.

3. Bezzałogowe statki powietrzne, nawet te najmniejsze, bez trudu podniosą niewielki ładunek w postaci przewodu miedzianego, który może zostać użyty do spowodowania zwarcia.
4. Długość linii napowietrznych oraz mnogość stacji obsługujących te linie praktycznie wyklucza szanse na zapobieganie atakom polegającym na zwarciu instalacji.
5. Skutecznie prowadzone ataki mogą spowodować duże straty finansowe zarówno dla wytwórcy energii elektrycznej i operatora sieci, jak i dla odbiorców energii.
6. Projekty budowy nowych linii napowietrznych muszą uwzględniać pojawienie się nowych źródeł zagrożeń, którymi są drony. Linie napowietrzne w miarę możliwości powinny być zatem budowane z użyciem przewodów izolowanych, w taki sposób, aby niemożliwe było ich zwarcie z wykorzystaniem drona. Impulsem do zmiany sposobu projektowania linii może być projekt zwiększenia skablowania sieci średniego napięcia do 2040 r. Skablowanie takie należy prowadzić dopóty, dopóki stopień skablowania sieci w Polsce nie zrówna się ze średnim stopniem skablowania w UE.
7. Właściwie wyznaczona strefa DRA-P umożliwia podniesienie poziomu bezpieczeństwa chronionego obiektu. Ze względu na łatwość ataku należy rozważyć wyznaczenie stref DRA-P dookoła punktów węzłowych, krytycznie ważnych dla przesyłu energii elektrycznej w państwie.
8. Lokalizacja stref DRA-P jest jawna, a informacja o niej dostępna dla każdego, zatem wybór obiektów, dla których wyznaczenie stref DRA-P mogłoby być krytycznie ważne, musi być przeprowadzony z najwyższą ostrożnością.
9. Wobec braku możliwości technicznych i przy ograniczeniach finansowych operatorów sieci warto zastanowić się nad działaniami profilaktycznymi pozwalającymi na zabezpieczenie obiektów, w których wytwarza się energię elektryczną, oraz obiektów i linii wykorzystywanych do przesyłu energii elektrycznej w sposób inny niż za pomocą urządzeń detekcyjnych i systemów neutralizacji bezzałogowych statków powietrznych.

Bibliografia

Baldick R., Chowdhury B., Dobson I., *Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures,* w: *IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

Carter B., Mancini R. , *Op Amps for Everyone*, Burlington 2009.

Jaworski M., Szuba M., *Analiza obciążeń napowietrznych linii najwyższych napięć w aspekcie wytwarzania pola magnetycznego*, „Przegląd Elektrotechniczny" 2015, nr 5, s. 149–154.

Kapoor R. i in., *UAV Navigation Using Signals of Opportunity in Urban Environments. An Overview of Existing Methods, 1st International Conference on Energy and Power*, ICEP2016, 14–16 XII 2016, Melbourne, Australia.

Metzger F.B., *An Assesment of Propeller Aircraft Noise Reduction Technology*, ASA Contractor Report 198237, 1995.

Parfomak P.W., *Physical Security of the U.S. Power Grid. High-Voltage Transformer Substations*, Congressional Research Service, 17 VI 2014.

Preece W.H., *On the Heating Effects of Electric Currents*. No. II, „Proceedings of the Royal Society of London" 1887–1888, t. 43, bez paginacji.

Preece W.H., *On the Heating Effects of Electric Currents*. No. II, „Proceedings of the Royal Society of London" 1887–1888, t. 44, bez paginacji.

Standardowe Specyfikacje Funkcjonalne. Elektroenergetyczna automatyka zabezpieczeniowa, pomiary i układy obwodów wtórnych, Warszawa 2010 (aktualizacja 2012 r.).

Stauffacher E.R., *Short-time Current Carrying Capacity of Copper Wire*, „General Electric Review" 1928 r., t. 31, nr 6, s. 326–327.

Yuliang W. i in., *Noise Reduction of UAV Using Biomimetic Propellers with Varied Morphologies Leading-edge Serration*, „Journal of Bionic Engineering" 2020, t. 17, s. 767–779.

Źródła internetowe

Energetyka, dystrybucja, przesył, PTPiREE, http://ptpiree.pl/raporty/2021/raport_ptpiree_2021.pdf [dostęp: 30 XI 2021].

Akty prawne

Rozporządzenie wykonawcze Komisji (UE) 2020/639 z dnia 12 maja 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do scenariuszy standardowych dla operacji wykonywanych w zasięgu widoczności wzrokowej lub poza zasięgiem widoczności wzrokowej (Dz. Urz. UE L 150/1 z 13 V 2020 r.).

Rozporządzenie delegowane Komisji (UE) 2020/1058 z dnia 27 kwietnia 2020 r. zmieniające rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych (Dz. Urz. UE L 232/1 z 20 VII 2020 r.).

Rozporządzenie wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19 (Dz. Urz. UE L 176/13 z 5 VI 2020 r.).

Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz. Urz. UE L 152/45 z 11 VI 2019 r.).

Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich (Dz. Urz. UE L 152/1 z 11 VI 2019 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (Dz. Urz. UE L 212/1 z 22 VIII 2018 r.).

Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (t.j.: DzU z 2020 r. poz. 1970, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: DzU z 2021 r. poz. 2345, ze zm.).

Wytyczne nr 7 Prezesa Urzędu Lotnictwa Cywilnego z dnia 9 czerwca 2021 r. w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz. Urz. Urzędu Lotnictwa Cywilnego z 2021 r. poz. 35).

Wytyczne nr 24 Prezesa Urzędu Lotnictwa Cywilnego z dnia 30 grudnia 2020 r. w sprawie wyznaczania stref geograficznych dla systemów bezzałogowych statków powietrznych (Dz. Urz. Urzędu Lotnictwa Cywilnego z 2020 r. poz. 78).

Wytyczne Szefa Szefostwa Służby Ruchu Lotniczego Sił Zbrojnych Rzeczypospolitej Polskiej nr 6 z dnia 17 września 2018 r. w sprawie uszczegółowienia zasad wykonywania lotów modeli latających oraz bezzałogowych statków powietrznych o MTOW nie większej niż 25 kg w strefach ruchu lotniskowego lotnisk wojskowych (MATZ) oraz strefach kontrolowanych lotnisk wojskowych (MCTR), https://ssrlszrp.wp.mil.pl/u/Wytyczne_w_sprawie_wykonywania_lotow_przez_RPAS.pdf.

DOI: 10.4467/27204383TER.22.005.15421

ORCID: 0000-0002-3793-5913

ALEKSANDER OLECH

Unikalne rozwiązania Republiki Francuskiej w walce z terroryzmem i radykalizacją

Abstrakt

Doświadczenia i rozwiązania Republiki Francuskiej, gdzie nieustannie są rozwijane struktury antyterrorystyczne, powinny stanowić swego rodzaju drogowskaz dla innych państw. Tworzenie wyjątkowych programów deradykalizacyjnych i prowadzenie polityki reagowania na przypadki ekstremizmu to działania, które można wdrożyć w Polsce. Ponadto wykorzystywanie mediów społecznościowych do walki z treściami o charakterze terrorystycznym oraz do informowania o zagrożeniach ukazuje innowacyjne zastosowanie Internetu. Warto również zwrócić uwagę na zaangażowanie francuskich strażników miejskich oraz służb medycznych w proces reagowania na terroryzm, a także uwydatnić rolę organizacji pozarządowych działających na rzecz wsparcia ofiar. Dekady zmagań Francji z różnymi rodzajami terroryzmu spowodowały, że przez lata usprawniano i weryfikowano tam metody, które byłyby skuteczne w przeciwdziałaniu radykalizacji i zagrożeniom. W ocenie autora należałoby skorzystać z francuskiej eksperiencji i zaimplementować chociaż część rozwiązań w Polsce.

Słowa kluczowe:

antyterroryzm,
Francja,
Polska,
radykalizacja,
deradykalizacja

Zagrożenia terrorystyczne, w tym postępująca radykalizacja, nasilają się w Europie, stanowiąc niebezpieczeństwo dla wszystkich państw na kontynencie. Oprócz działań na poziomie międzynarodowym, m.in. zaangażowania w globalną walkę z terroryzmem, pojawiła się potrzeba reagowania na zagrożenia wewnętrzne. Przyczyn takiego stanu rzeczy należy doszukiwać się w zmianach przekonań religijnych, politycznych i społecznych. W niektórych krajach tworzą się grupy, które chcąc zrealizować swoje cele, podejmują aktywność antypaństwową o charakterze terrorystycznym. Ponadto dążą do budowania przekazu poprzez angażowanie innych osób, także młodych, wzmacniając w nich potrzebę popierania skrajnych poglądów ideologicznych.

Obywatele, którzy stają się agresywni i bezkompromisowi w swoich poglądach oraz sposobach działania, mogą podejmować się organizowania zamachów lub rozwijania komórek ekstremistycznych. Dlatego tak dużą uwagę należy poświęcić terroryzmowi rodzimemu lub domowemu (określanemu także jako *home grown terrorism*[1]). Często, choć nie zawsze, terrorystami stają się osoby wychowane w kulturze państw europejskich, ale będące ortodoksyjnymi wyznawcami islamu lub identyfikujące się z tą religią dopiero w trakcie przygotowywania ataku, jak to się dzieje we Francji[2]. Następuje ich stanowcza radykalizacja (przejmowanie opinii, poglądów i idei, które prowadzą do ekstremizmu), w efekcie czego mogą próbować dokonać zamachów na terytorium państwa, którego obywatelstwo mają od urodzenia, otrzymali je lub w którym uzyskali prawo do pobytu. Ten rodzaj terroryzmu jest określany również jako socjologiczne kuriozum, gdyż religia dominuje nad wartościami republikańskimi promowanymi w kraju zamieszkania.

W Republice Francuskiej stwierdza się, że radykalizacja to rodzaj każdej ideologii lub religii skłaniających jednostkę do wybrania przemocy w imię przekonań, jednocześnie nieuznawania kompromisów i decydowania się na terroryzowanie społeczeństwa.

---

[1] K. Rekawek i in., *Who are the European jihadis? Project Midterm Report*, Bratislava 2018.

[2] We Francji władze od dawna dążą do asymilacji jako modelu integracji społecznej, wierząc, że zminimalizowanie różnic kulturowych i religijnych pozwoli utrzymać Francję jako jednocześnie świecką i multikulturową. W rzeczywistości wiele osób w kraju czuje się wyobcowanych i wykluczonych ze społeczeństwa francuskiego. Ten problem jest widoczny już od ponad dwóch dekad. Za: K. Thachuk, M. Bowman, C. Richardson, *Homegrown Terrorism. The Threat Within*, Washington 2008, s. 5, 15–16.

Radykalizacja to proces stopniowego angażowania się i odrzucania zasad panujących w społeczeństwie. Następuje w trakcie socjalizacji oraz budowania relacji i wpływa na psychikę. Jest to zjawisko mocno powiązane ze wzmacnianiem konfliktów tożsamościowych i słabości przez ideologię lub religię (problemy w pracy lub szkole, rodzinne lub osobiste)[3]. Choć radykalizacja nie dotyczy wyłącznie terrorystów wyznających dżihad, to obecnie przede wszystkim takie osoby stanowią zagrożenie we Francji.

Terroryzm jest zjawiskiem, które nieustannie występuje w środowisku międzynarodowym. Francja stale się zmaga z zagrożeniami o charakterze terrorystycznym i jest to najczęściej atakowane państwo Unii Europejskiej w XXI w. Od lat 50. XX w. doświadcza ona praktycznie wszystkich rodzajów terroryzmu: od prawicowego, przez lewicowy, po separatystyczny i obecnie dżihadystyczny. Polska nie była dotychczas celem ataków terrorystycznych i nie jest krajem, w którym terroryści stale i aktywnie operują, chociaż przemieszczają się na jej terenie tranzytem. Ponadto istnieją przesłanki, które skłaniają do refleksji nad potencjalnym zagrożeniem w Europie Środkowo-Wschodniej oraz rosnącą radykalizacją wśród obywateli tej części kontynentu.

Skorzystanie z rozwiązań stosowanych we Francji stwarza możliwość nie tylko ulepszenia systemów antyterrorystycznych i sposobów działania oddziałów kontrterrorystycznych w Polsce oraz innych państwach, lecz także edukowania i uświadamiania społeczeństwa na temat pojawiających się zagrożeń i wyzwań. Stała współpraca i nadzór wszystkich podmiotów, które mogą być podatne na wpływ zagrożeń terrorystycznych, są niezbędne dla prawidłowego rozwoju struktur bezpieczeństwa w państwie. Wykorzystanie doświadczeń Francji wydaje się także niezwykle ważne w kontekście budowania potencjału antyterrorystycznego we wszystkich krajach członkowskich Unii Europejskiej oraz NATO. Najskuteczniejszym sposobem walki z terroryzmem jest przeciwdziałanie mu, dlatego też państwa członkowskie powinny skorzystać ze sprawdzonych metod, które od dziesięcioleci

[3] Secrétariat général du Comité interministériel de prévention de la délinquance et de la radicalisation, *Une politique publique volontariste et évolutive*, https://www.cipdr.gouv.fr/prevenir-la-radicalisation [dostęp: 4 XI 2021].

są rozwijane we Francji[4], dzięki czemu współcześnie można je określić jako jedyne w swoim rodzaju[5].

Celem artykułu jest usystematyzowanie wiedzy oraz ukierunkowanie działań podmiotów zobowiązanych do zwalczania terroryzmu w Polsce i innych państwach, przy wykorzystaniu profilaktyki antyterrorystycznej stosowanej w Republice Francuskiej. Zdaniem autora niektóre elementy francuskich rozwiązań, przede wszystkim dotyczące deradykalizacji, powinny mieć także zastosowanie w skali europejskiej. Ponadto, na podstawie przeprowadzonych badań, będzie możliwe opracowanie koncepcji organizacji systemu zwalczania zagrożeń terrorystycznych nie tylko we Francji i Polsce, lecz także w innych państwach członkowskich Unii Europejskiej i NATO.

Podjęcie badań skoncentrowanych na systemie zwalczania zagrożeń terrorystycznych wymaga odpowiedniej organizacji, planowania oraz weryfikacji. Elementarna w tych działaniach jest metodologia badań. W prowadzonej kwerendzie oparto się na pytaniach badawczych, hipotezach oraz celu, które sformułowano na podstawie dogłębnej analizy problemu badawczego. Celem badań było doskonalenie poznania naukowego i konfrontacji hipotezy z faktami[6]. Pytania badawcze przyjęły następującą formę:

1. Jak wykorzystać eksperiencję Republiki Francuskiej w walce z terroryzmem, aby nie popełnić tych samych błędów w procesie przeciwdziałania terroryzmowi?
2. Które z metod i działań Francji w zakresie realizacji zadań antyterrorystycznych powinny zostać wykorzystane w Polsce i innych państwach demokratycznych w Europie?
3. Jak profilaktyka antyterrorystyczna w Republice Francuskiej, m.in. w postaci implementacji projektów na rzecz walki z radykalizacją w więzieniach, Internecie oraz w ramach społeczeństwa obywatelskiego, może zminimalizować ryzyko ataku terrorystycznego w państwie?

---

[4] Już w 2005 r. francuskie działania antyterrorystyczne prowadzone od lat 80. XX w. zostały uznane za najskuteczniejsze w Europie. Za: L. Block, *Evaluating the Effectiveness of French Counter-Terrorism*, „Terrorism Monitor Volume" 2005, t. 3, nr 17.

[5] A. Olech, *Walka z terroryzmem. Polskie rozwiązania a francuskie doświadczenia*, Warszawa 2021.

[6] B. Kuc, Z. Ściborek, *Podstawy metodologiczne nauk o bezpieczeństwie*, Warszawa 2013, s. 115–119.

4. Czy rozwiązania stosowane we Francji są wartościowe dla rozwoju polskich struktur antyterrorystycznych i deradykalizacyjnych?
5. W jakim kierunku w sytuacji współczesnych zagrożeń powinny zmierzać zmiany organizacyjne, funkcjonalne i normatywne służące utrzymaniu bezpieczeństwa narodowego RP?

Hipotezy naukowe zostały postawione na podstawie dotychczas przeprowadzonych badań i są powiązane ze stanem wiedzy na temat terroryzmu[7]. Dla uporządkowania rozważań, osiągnięcia przedstawionego powyżej celu oraz wyjaśnienia problemu badawczego przyjęto następujące hipotezy badawcze:

1. Analiza choć części rozwiązań stosowanych we Francji oraz próba ich implementacji w Polsce pozwoli na dopasowanie polskiego systemu antyterrorystycznego do współczesnych zagrożeń międzynarodowych.
2. Wykorzystanie metod stosowanych we Francji może znacznie zwiększyć zdolność oraz skuteczność realizacji czynności antyterrorystycznych i kontrterrorystycznych w Polsce, zwłaszcza w kontekście wprowadzenia programów deradykalizacji w więzieniach oraz wykorzystania mediów społecznościowych.
3. Prowadzenie działań na rzecz zwalczania zagrożeń terrorystycznych jeszcze na poziomie ich rozrostu, zwłaszcza wśród młodych osób, a także wzmacnianie krajowej polityki antyterrorystycznej wśród społeczeństwa znacznie podniosą poziom świadomości na temat zagrożeń.
4. Wyjątkowe rozwiązania wprowadzone we Francji istotnie wpłynęły na liczbę osób ulegających radykalizacji, a w latach 2017––2021 odnotowano mniejszą liczbę ataków terrorystycznych, co oznacza, że podobne metody mogłyby być efektywne w Polsce.
5. Jeśli adekwatnie do terrorystycznych doświadczeń i rozwiązań Republiki Francuskiej, obecnych oraz przyszłych uwarunkowań bezpieczeństwa międzynarodowego, zostaną dokonane stosowne zmiany prawne, organizacyjne i funkcjonalne w działalności antyterrorystycznej Rzeczypospolitej Polskiej, to możliwe będzie sprawne realizowanie działań obronnych oraz podniesienie poziomu bezpieczeństwa narodowego.

[7] J.B. Johnson, H.T. Reynolds, J.D. Mycoff, *Metody badawcze w naukach politycznych*, tłum. A. Kloskowska-Dudzińska, Warszawa 2010, s. 78, 87–90.

Prezentowane w niniejszym artykule rozwiązania są mniej popularne od działań realizowanych przez służby specjalne oraz oddziały kontrterrorystyczne. Jednakże ich znaczenie jest równie ważne w budowaniu potencjału bezpieczeństwa państwa. W Republice Francuskiej najszybciej są rozwijane zdolności do reagowania na zagrożenia oraz stale są one dopasowywane do nowych wyzwań, zarówno tych o charakterze wewnętrznym, jak i zewnętrznym. Oprócz uchwalenia *Ustawy o wzmocnieniu bezpieczeństwa wewnętrznego i walce z terroryzmem*[8] oraz transformacji przeprowadzonych w służbach antyterrorystycznych znaczenie ma także wiele działań pobocznych. Są one podejmowane w celu ograniczenia wpływu terroryzmu na funkcjonowanie państwa. Za ich realizację odpowiadają m.in. policja miejska (straż miejska), administracja więzienna, służba zdrowia czy organizacje pozarządowe. Trzeba podkreślić, że wszystkie działania noszące znamiona antyterroryzmu mają fundamentalne znaczenie dla utrzymywania bezpieczeństwa obywateli i składają się na to zarówno akcje mające na celu eliminację zamachowca, jak i programy deradykalizacji osób zafascynowanych ideologią dżihadu.

W zamierzeniach wynikających z postanowień ustawy określono główne zadania, które mają zostać zrealizowane do końca 2022 r. Są nimi:

- intensyfikacja działań mających na celu zapobieganie radykalizacji,
- większa współpraca służb bezpieczeństwa w zwalczaniu terroryzmu,
- przeciwdziałanie radykalizacji w więzieniach,
- udzielanie wsparcia edukacyjnego zradykalizowanej młodzieży, a także nieletnim powracającym z Bliskiego Wschodu,
- usprawnienie funkcjonowania wymiaru sprawiedliwości w kontekście tłumienia aktów terroryzmu i karania terrorystów,
- uproszczenie i usprawnienie kwestii proceduralnych dla ofiar aktów terroryzmu.

[8] *Loi n° 2017-1510 du 30 octobre 2017 renforçant la securite interieure et la lutte contre le terrorisme*, JORF n°0255 du 31 octobre 2017 texte n° 1.

System walki przeciwko terroryzmowi w Republice Francuskiej

W ramach systemu antyterrorystycznego, który w Republice Francuskiej jest określany jako system walki przeciwko terroryzmowi (fr. *système français de lutte contre le terrorisme*), są realizowane kampanie skierowane przeciw nie tylko terroryzmowi (fr. *le plan d'action contre le terrorisme*, PACT), lecz także radykalizacji (fr. *le plan national de prévention de la radicalisation*, PNPR). Sekretariat Generalny Obrony i Bezpieczeństwa Narodowego (fr. Secrétariat général de la Défense et de la Sécurité nationale, SGDSN) w 2018 r. został upoważniony przez premiera do opracowania, we współpracy z krajowym koordynatorem wywiadu i walki z terroryzmem (fr. *Coordination nationale du renseignement et de la lutte contre le terrorisme*, CNRLT), priorytetów w systemie zwalczania terroryzmu. Nie wyróżniono organów i instytucji oddelegowanych do podejmowania konkretnych działań, ale wysunięto na pierwszy plan podmioty współpracujące z SGDSN, a są to wszystkie służby i ministerstwa w jakikolwiek sposób zapewniające utrzymanie bezpieczeństwa[9]. Uwydatniono również współpracę o charakterze międzynarodowym jako fundament w kampanii przeciw aktom agresji[10]. Całościowo system antyterrorystyczny ma realizować następujące założenia:

- poznawać: lepiej identyfikować i rozumieć zagrożenie terrorystyczne i jego rozwój;
- przeszkadzać: zapobiegać aktom przemocy poprzez obserwację osób niebezpiecznych, powstrzymywanie finansowania terroryzmu oraz rozwiązywanie konfliktów, które powodują powstawanie zagrożeń o charakterze terrorystycznym;
- chronić: dostosować zadania ochrony osób i mienia ze względu na zidentyfikowane zagrożenia (wymaga to w szczególności rozwoju zdolności technologicznych i większego zaangażowania podmiotów publicznych i prywatnych);
- powstrzymywać: karać sprawców przestępstw terrorystycznych, a także stawiać dżihadystów przed sądem;

[9] *Plan d'action contre le terrorisme*, Paris 2018, s. 15–16.

[10] *Rapport: Conférence sur la lutte contre le terrorisme et la prévention de la radicalisation violente*, Paris 2016, s. 35–36.

– zwiększyć współpracę między krajami europejskimi i promować w Unii Europejskiej inicjatywy Francji zmierzające do skuteczniejszego zwalczania terroryzmu[11].

W analizie systemów antyterrorystycznych poszczególnych państw, oprócz określenia centrów, koordynatorów czy gremiów międzyresortowych, zawsze należy rozpoznać poziom, na jakim podejmowane są decyzje i wyznaczane kierunki działań. W strukturę bezpieczeństwa antyterrorystycznego Francji są włączeni formalnie prezydent i premier. Faktyczne kroki podejmowane są jednak na poziomie ministrów odpowiedzialnych za bezpieczeństwo czy funkcjonowanie poszczególnych obszarów gospodarki. Niezmiernie istotną rolę w tym systemie odgrywa właśnie minister spraw wewnętrznych, który nadzoruje pracę Dyrekcji Generalnej Bezpieczeństwa Wewnętrznego (fr. Direction générale de la sécurité intérieure, DGSI). Służba została utworzona w kwietniu 2014 r. w wyniku przekształcenia Centralnej Dyrekcji Wywiadu Wewnętrznego (fr. Direction centrale du renseignement intérieur, DCRI) powstałej 1 lipca 2008 r.[12]. Jest to służba kontrwywiadowcza, której głównym zadaniem jest wykrywanie zagrożeń wewnątrz państwa i neutralizacja niebezpieczeństw ze strony obcych podmiotów[13]. Jej szczególną misją jest uczestniczenie w nadzorze osób i grup zradykalizowanych, które mogą uciekać się do przemocy i zagrażać bezpieczeństwu państwa. Oprócz tego nadrzędną rolą służby specjalnej jest współpraca z Poddyrekcją Antyterrorystyczną (fr. Sous-direction anti-terroriste, SDAT)[14] oraz Sekcją Antyterrorystyczną (fr. Section anti-terroriste, SAT)[15] w zwalczaniu

[11] *Plan d'action…*

[12] *Décret n° 2014-474 du 12 mai de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement 2014 pris pour l'application des assemblées parlementaires et portant désignation des services spécialisés de renseignement*. Article 1.

[13] W Polsce zbliżone zadania ma Agencja Bezpieczeństwa Wewnętrznego.

[14] SDAT ma siedzibę w tym samym budynku co służba specjalna DGSI. Jest to jednocześnie element nowego planu przeciwdziałania terroryzmowi przedstawionego w styczniu 2020 r., w ramach którego służba antyterrorystyczna współpracuje bezpośrednio ze służbą wywiadowczą.

[15] Jest odpowiednikiem SDAT w prefekturze paryskiej policji.

zagrożeń terrorystycznych. Specyfiką DGSI[16] są jej podwójne kompetencje sądowe[17] i wywiadowcze[18].

Można przyjąć, że odpowiednikiem polskiego systemu antyterrorystycznego (który należałoby ponownie opracować, tj. na lata 2022–2026) jest plan Vigipirate[19]. Jego geneza sięga 1978 r., kiedy to Francja i Europa stanęły w obliczu pierwszych fal ataków terrorystycznych przeprowadzanych przez organizacje ekstremistyczne i separatystów. Oficjalnie rządowy plan Vigipirate wdrożono w 1995 r. W obecnym charakterze funkcjonuje od grudnia 2016 r. Dotyczy on trzech etapów analizowania zagrożenia, tj. czujności, zapobiegania i ochrony[20]. Vigipirate, który nadzoruje premier, jest głównym narzędziem francuskiego systemu

[16] DGSI jest systematycznie informowana o wszystkich sprawach powiązanych z terroryzmem we Francji. Jest również koordynatorem śledztw dotyczących czynów popełnionych za granicą przeciwko interesom francuskim (ambasady, francuskie ofiary za granicą itp.). Stale współpracuje z Narodową Prokuraturą Antyterrorystyczną (PNAT).

[17] DGSI jako jedyna ze służb specjalnych w Republice Francuskiej współpracuje bezpośrednio z instytucjami sądowymi (fr. *institution judiciaire*), w tym z Policją Sądową (fr. Police Judiciaire). Ma to na celu ochronę danych wywiadowczych, które zostały zebrane przez służbę, a nie mogą pojawić się w postępowaniu sądowym ze względu na klauzulę tajności. Istotą jest ochrona źródeł, utrzymanie w tajemnicy kooperacji osób trzecich ze służbą, a także sposobu, w jaki są zdobywane informacje. Podmioty zaangażowane we współpracę z DGSI mają pewność, że nie zostaną rozpoznane przed sądem. Zwyczajowo to Policja Sądowa jest odpowiedzialna za współpracę ze służbami i z sądami, pełniąc rolę pośrednika. W tej sytuacji specyfice DGSI ma podwójne kompetencje: w zakresie wywiadu i sądownictwa. W sferze wywiadowczej należy do niej podejmowanie czynności dla dobra interesu narodowego we wszystkich obszarach bezpieczeństwa, a w kompetencji sądowniczej – na potrzeby kontrwywiadu, utrzymywania tajemnicy obrony narodowej oraz współpraca z Policją Sądową (w tym z oddziałami SDAT oraz SAT) w zwalczaniu zagrożeń terrorystycznych. DGSI współdziała również ze specjalistycznymi służbami policji i żandarmerii w zwalczaniu cyberprzestępczości.

[18] *Les services judiciaires anti-terroristes*, https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/police-judiciaire-specialisee/services-judiciaires [dostęp: 24 XI 2021].

[19] Vigipirate jest akronimem od: *vigilance et protection des installations contre les risques d'attentats terroristes à l'explosif* (pol. czujność i ochrona instalacji przed ryzykiem zamachów terrorystycznych).

[20] Plan może zostać rozszerzony o inne rządowe plany zwalczania zagrożeń terrorystycznych, np. *plan Pirate NRBC* (atak nuklearny, radiologiczny, biologiczny lub chemiczny), *plan Piranet* (atak informatyczny, w cyberprzestrzeni), a także plany *Piratair-Intrusair, Pirate Mer, Metropirate* (atak terrorystyczny w przestrzeni powietrznej, na wodzie lub w metrze).

antyterrorystycznego, ponieważ łączy wszystkie krajowe podmioty (władzę państwową, lokalną, publiczną, prywatne podmioty gospodarcze oraz obywateli). Składają one sprawozdania premierowi i wszystkim ministrom. Dominującą rolę w realizowaniu programu odgrywa Ministerstwo Spraw Wewnętrznych[21].

Program przewiduje dwie fazy działania: fazę zwykłą i fazę zagrożenia. Podstawowym założeniem planu jest przeciwdziałanie zamachom terrorystycznym, a także informowanie społeczeństwa o stopniu zagrożenia i sposobach zabezpieczenia się przed ewentualnym zamachem. Wskazuje również policji i służbom bezpieczeństwa konkretne dyspozycje ochronne. Najnowsza wersja planu opiera się na trzech filarach funkcjonowania[22]. Są to:

1. Rozwój kultury bezpieczeństwa indywidualnego i zbiorowego, obejmującej całe społeczeństwo obywatelskie.
2. Zdefiniowanie trzech poziomów zagrożenia i przedstawienie ich na logo widocznym w przestrzeni publicznej:
   a) poziom czujności (fr. *le niveau de «vigilance»*) – wskazuje na potrzebę utrzymania bezpieczeństwa i wdrożenia środków ostrożności poprzez nadzór nad niektórymi środkami transportu i miejscami publicznymi. Ten poziom może obowiązywać w konkretnym regionie;
   b) podwyższony poziom, zaostrzenie środków bezpieczeństwa[23] – istnieje ryzyko ataku (fr. *le niveau «sécurité renforcée – risque attentat»*) – w przypadku jego ogłoszenia należy dostosować możliwą reakcję państwa do wysokiego, a nawet bardzo wysokiego zagrożenia terrorystycznego. Poza ochroną szczególnie wrażliwych punktów (lotniska, stacje kolejowe, miejsca kultu religijnego itp.) można określić dodatkowe miejsca wymagające wzmocnienia kontroli.

[21] *Comprendre le plan Vigipirate*, https://www.gouvernement.fr/risques/comprendre-le-plan-vigipirate [dostęp: 4 XI 2021].

[22] A. Olech, *Counterterrorism Strategies in Poland and France*, https://warsawinstitute.org/counterterrorism-strategies-poland-france [dostęp: 15 XI 2021].

[23] We Francji wprowadza się drugi poziom podczas: ważnych wydarzeń o charakterze międzynarodowym (wydarzenia sportowe, np. Euro 2016, Konferencja Narodów Zjednoczonych w sprawie Zmian Klimatu, COP) itp., ważnych wydarzeń krajowych, takich jak rozpoczęcie roku szkolnego i obchody świąt, po ataku na terytorium Francji lub za granicą, w celu pilnego dostosowania krajowego systemu ochrony.

Ten poziom może obowiązywać na całym terytorium kraju i wiąże się szczególnie z patrolowaniem ulic, a także podejmowaniem działań kontrterrorystycznych, takich jak przeszukiwanie mieszkań i aresztowanie podejrzanych. Nie ma ograniczenia czasowego;

c) poziom alarmowy – bezpośrednie zagrożenie atakiem (fr. *le troisième niveau, intitulé «urgence attentat»*) – może zostać ustanowiony natychmiast po ataku lub w przypadku identyfikacji grupy terrorystycznej i potrzeby lokalizacji zagrożenia. Poziom ten ustanawia się na określony czas: w trakcie ataku. Umożliwia mobilizację wszystkich służb, zamknięcie miejsc publicznych, a także rozpowszechnianie za pośrednictwem stron internetowych, telewizji i radia informacji mogących chronić obywateli w tej szczególnej sytuacji kryzysowej[24].

3. Wdrażanie nowych środków wzmacniających działania rządu w walce z terroryzmem[25]. Oznacza to implementację nowych rozwiązań, które mogą być realizowane przez miesiąc, pół roku lub nawet kilka lat w celu weryfikacji ich skuteczności (np. wprowadzenie wyższego poziomu zagrożenia na terytorium państwa, organizacja stref ochronnych, a także ocena zastosowania nowego prawa – tj. ustawy na rzecz walki z terroryzmem – w celu określenia, czy należy je dalej stosować[26])[27].

W ramach planu Vigipirate służby wywiadowcze oceniają zagrożenie terrorystyczne, a ich analizy pozwalają Sekretariatowi Generalnemu Obrony i Bezpieczeństwa Narodowego na przyjęcie określonego poziomu niebezpieczeństwa. Plan Vigipirate obowiązuje na terytorium

[24] W latach 2003–2013 obowiązywały cztery poziomy: żołty (fr. *jaune*), pomarańczowy (fr. *orange*), czerwony (fr. *rouge*) i szkarłatny (fr. *ecarlate*), a od 2014 r. dwa: poziom czujności (fr. *le niveau de vigilance*) i poziom alarmowy ataku (fr. *le niveau d'alerte attentat*).

[25] L. Wicky, *Le plan Vigipirate et ses trois niveaux d'alerte*, https://www.lemonde.fr/les-decodeurs/article/2016/12/20/en-france-le-plan-vigipirate-et-ses-trois-niveaux-d-alerte_5052094_4355770.html [dostęp: 4 XI 2021].

[26] Ministère de l'Intérieur, *Premier bilan de l'application de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, Communique de Presse, 12 II 2019 r.

[27] J. Sulzer, *Loi Renforçant La Securite Interieure Et La Lutte Contre Le Terrorisme, Analyse juridique critique – Mise en œuvre – Suivi du contentieux constitutionnel, 30 octobre 2017––29 octobre 2018*, H. Decoeur (red.), Paris 2018.

Francji, na morzu, a nawet za granicą. Niektóre środki planu można uruchomić poza granicami, jeśli zostanie udowodnione zagrożenie dla obywateli francuskich lub interesów Francji oraz gdy są one zgodne z suwerennością zainteresowanych krajów. Środki te obejmują na przykład wzmocnienie bezpieczeństwa wokół francuskich przedstawicielstw dyplomatycznych[28].

Co ważne, od 12 stycznia 2015 r. zadania ochronne planu Vigipirate zostały powierzone żołnierzom w ramach misji Opération Sentinelle, która ma na celu zabezpieczenie szczególnie wrażliwych punktów w kraju. Działania są prowadzone ze wszystkimi służbami bezpieczeństwa. Pierwotnie zmobilizowano 10 412 żołnierzy oraz 4700 policjantów i żandarmów, którzy ochraniali 830 lokalizacji we Francji najbardziej narażonych na zamachy, w tym: miejsca kultu, szkoły, przedstawicielstwa dyplomatyczne i konsularne, redakcje prasowe (są monitorowane 24 godziny na dobę). Nie bez znaczenia jest fakt, że odkąd rozpoczęto Opération Sentinelle, regularnie dochodzi do ataków (również o charakterze terrorystycznym) na żołnierzy, którzy przebywają w miejscach szczególnie narażonych[29]. Według ówczesnego ministra sił zbrojnych, Jeana-Yves'a Le Driana, koszt utrzymania operacji wynosi milion euro dziennie[30]. Obecnie rozmieszczonych jest od 7 do 10 tysięcy żołnierzy w pobliżu najważniejszych punktów w kraju (m.in. ochrona infrastruktury krytycznej[31]). Warto zaznaczyć, że podobne systemy działań wprowadziły m.in.:

---

[28] *Plan Vigipirate. Foire aux Questions*, Paris 2016, s. 3.

[29] *Comprendre…*

[30] *Attentats: „L'opération Sentinelle coûte 1 million d'euros par jour"*, http://www.leparisien.fr/faits-divers/le-drian-l-operation-sentinelle-coute-1-million-d-euros-par-jour-08-02-2015-4515903.php [dostęp: 4 XI 2021].

[31] Infrastruktura krytyczna we Francji to obiekty, centra lub instalacje, które dostarczają usługi i towary niezbędne dla życia obywateli. W 2006 r. w celu ochrony infrastruktury krytycznej we Francji zdefiniowano 12 sektorów działalności o największym znaczeniu (fr. *secteurs d'activités d'importance vitale*, SAIV), podzielonych na cztery filary: ludzki, państwowy, ekonomiczny i technologiczny. Zidentyfikowano operatorów o kluczowym znaczeniu (fr. *opérateurs d'importance vitale*, OIV), uznanych za fundamentalnych dla funkcjonowania gospodarki i społeczeństwa, oraz punkty o kluczowym znaczeniu (*points d'importance vitale*, PIV). Ochrona infrastruktury krytycznej we Francji jest definiowana jako: zespół działań, kluczowych i nie do zastąpienia, przyczyniających się do sprawowania władzy w państwie, funkcjonowania gospodarki, zachowania potencjału obronnego oraz zapewnienia bezpieczeństwa narodu, w celu utrzymania produkcji i dystrybucji podstawowych towarów lub usług dla funkcjonowania państwa.

– Belgia – po atakach ze stycznia 2015 r. rozpoczęto tam operację Vigilant Guardian na wzór francuskiego Opération Sentinelle[32];
– Włochy – w lutym 2015 r. rozlokowano na ulicach 4800 żołnierzy, aby chronić ważne miejsca publiczne, w tym Watykan, przed możliwymi atakami terrorystycznymi[33];
– Izrael – w tym kraju od 2015 r. rozmieszcza się funkcjonariuszy w miejscach szczególnie narażonych na ataki, tj. centrum miasta, obiekty infrastruktury krytycznej i świątynie[34];
– Wielka Brytania – po zamachu bombowym w Manchesterze w maju 2017 r. postanowiono rozpocząć operację Temperer, w ramach której postawiono 5100 żołnierzy na ulicach miast[35].

Zaangażowanie armii w ochronę ludności i terytorium kraju ma być sygnałem ostrzegawczym dla terrorystów. W obliczu trwałego zagrożenia terrorystycznego jest ono uzasadnione. Żołnierze wykonują zadania obserwacyjne i nadzorcze[36].

Republika Francuska realizuje wiele misji antyterrorystycznych poza granicami państwa (oprócz utrzymywania stałych baz wojskowych[37], głównie w Afryce Północnej we współpracy z grupą G5 Sahel[38]. Działania mające na celu walkę z terroryzmem są podejmowane już poza terytorium Francji, gdyż rząd w Paryżu ma świadomość zagrożenia w postaci migrujących terrorystów. Ideą jest wzmocnienie potencjału

[32] *Deux ans après: l'image de la Défense améliorée par la présence des militaires en rue*, https://www.rtbf.be/info/dossier/explosions-a-brussels-airport/detail_deux-ans-apres-l--image-de-la-defense-amelioree-par-la-presence-des-militaires-en-rue?id=9505164 [dostęp: 13 XI 2021].

[33] *Rome déploie 4 800 soldats autour de sites sensibles*, https://www.ouest-france.fr/europe/italie/antiterrorisme-rome-deploie-4-800-soldats-autour-de-sites-sensibles-3195080 [dostęp: 13 XI 2021].

[34] M. Bachner, *Hundreds of thousands more Israelis okayed to carry guns under new rules*, https://www.timesofisrael.com/hundreds-of-thousands-more-israelis-okayed-to-carry-guns-under-new-rules [dostęp: 13 XI 2021].

[35] L. Lagneau, *Terrorisme: Engagée dans l'opération «Temperer», la British Army devra faire face à de nouveaux défis*, http://www.opex360.com/2017/05/24/terrorisme-engagee--dans-loperation-temperer-la-british-army-devra-faire-face-un-defi-nouveau [dostęp: 13 XI 2021].

[36] *Plan Vigipirate. Foire...*, s. 3.

[37] A. Olech, *International Military Involvement of the French Republic*, Warsaw 2021.

[38] Czad, Niger, Burkina Faso, Mali i Mauretania stworzyły oficjalne ramy współpracy w celu poprawy bezpieczeństwa i rozwoju działań antyterrorystycznych w regionie ze względu na rozrost organizacji terrorystycznych.

bezpieczeństwa państw w regionie, a także uniemożliwienie terrorystom przedostania się do Europy. Francuscy żołnierze korzystają przy tym z najnowszego uzbrojenia, stosując takie same metody, jak podczas trwającego konfliktu zbrojnego[39]. Kwestią sporną pozostaje jednak, czy decydowanie się na tzw. globalną wojnę z terroryzmem – daleko poza granicami państwa – jest faktycznie skuteczne w zatrzymywaniu zamachowców i czy czasem nie jest to podtrzymywanie na siłę konfliktu, a następnie szybkie wycofanie wszystkich jednostek, jak choćby w przypadku Francji w misji Barkhane czy Amerykanów w Afganistanie.

Polityka publiczna w walce z radykalizacją

Ważnym organem, który należy wyróżnić w systemie francuskim, jest Międzyresortowy Komitet ds. Przeciwdziałania Przestępczości i Radykalizacji (fr. Comité interministériel de prévention de la délinquance et de la radicalisation), który wraz z Sekretarzem Generalnym (stanowiąc SG-CIPDR – fr. Secrétariat général du Comité interministériel de prévention de la délinquance et de la radicalisation) zajmuje się prewencją i walką z radykalizacją oraz ustala wytyczne dla polityki rządu w zakresie określonym w nazwie komitetu. Wspiera działania ministerstw oraz wykorzystanie środków budżetowych przeznaczonych na powstrzymywanie radykalizacji, separatyzmu[40], a także sekciarstwa[41]. Ponadto pomaga w przygotowaniu kampanii informacyjnych oraz prowadzi działania terenowe.

SG-CIPDR odgrywa kluczową rolę we wspieraniu społeczeństwa obywatelskiego, promując dobre praktyki oraz prowadząc szkolenia dla służb państwowych, władz lokalnych, stowarzyszeń i obywateli. Widocznym tego efektem jest organizacja szkoleń i warsztatów dotyczących

[39] J.-D. Merchet, *Mali: une „cinquantaine de terroristes neutralisés" par l'armée française*, „L'Opinion" 3 XI 2020.

[40] *Code de la sécurité intérieure, Version en vigueur au 23 novembre 2021*. Section 1: *Comité interministériel de prévention de la délinquance et de la radicalisation* (art. D132-1 à D132-4).

[41] *Décret n° 2020-867 du 15 juillet 2020 modifiant le décret n° 2002-1392 du 28 novembre 2002 instituant une mission interministérielle de vigilance et de lutte contre les dérives sectaires, NOR : INTX2004492D*, JORF n°0173 du 16 juillet 2020.

m.in. zapobiegania radykalizacji[42], udostępnianie materiałów online dla osób zainteresowanych tą problematyką[43], opracowywanie strategii dla państwa w ramach informowania i edukowania społeczeństwa na temat procesu radykalizacji oraz wykorzystanie mediów społecznościowych do wzmocnienia polityki rządu w zakresie zwalczania przestępczości i terroryzmu.

Publiczna reakcja na zapobieganie przestępczości i radykalizacji ma na celu zaangażowanie jak największej liczby partnerów w celu zapewnienia interdyscyplinarnego podejścia do pojawiających się wyzwań. W ten sposób SG-CIPDR koordynuje sieć podmiotów działających we współpracy ze społeczeństwem obywatelskim, aby promować solidarność w przeciwdziałaniu przestępczości zorganizowanej i radykalizacji. Ponadto instytucja działa w ramach sieci europejskiej kooperacji i uczestniczy w wymianie dobrych praktyk. Reprezentuje Francję w grupie roboczej ds. radykalizacji w Komisji Europejskiej oraz na Forum UE ds. Internetu przy Komisji Europejskiej.

Rozpoznanie osób zradykalizowanych lub będących w trakcie takiego procesu jest niezbędne, aby zapewnić im wsparcie, którego potrzebują, a także zapobiec atakom terrorystycznym. Jednakże identyfikacja zradykalizowanych musi być wystarczająco szczegółowa, aby skoncentrować się na właściwych osobach i nie objąć obserwacją tych, które nie stanowią żadnego zagrożenia. Dlatego konieczne jest oparcie się na ustrukturyzowanym i sprofesjonalizowanym systemie działań na poziomie departamentalnym. CIPDR odpowiada za budowanie prewencyjnej reakcji o charakterze społecznym – publicznym, oferując szczegółowe informacje dotyczące możliwej radykalizacji w przestrzeni

[42] W dniach 4–5 listopada 2021 r. zorganizowano otwartą sesję szkoleniową dot. zapobiegania radykalizacji, na której poruszano takie tematy, jak: reakcja społeczeństwa na zapobieganie i zwalczanie radykalizacji, kluczowe koncepcje islamu, geopolityka ruchu dżihadystycznego, proces radykalizacji: wiedza, kontrowersje i metody badawcze, wsparcie deradykalizacji, walka z radykalizacją i zapobieganie jej w więzieniach, przeciwdziałanie radykalizacji w sporcie, psychiatria i radykalizacja. Celem wydarzeń o charakterze publicznym jest utworzenie sieci podmiotów na poziomie krajowym, co umożliwi wykrycie wszystkich potencjalnie zradykalizowanych osób, aby je obserwować i następnie udzielić niezbędnej opieki.

[43] Materiały wideo udostępnione na portalu YouTube pt.: *E-learning „Znaj, wykrywaj i zgłaszaj zjawiska radykalizacji"*, https://www.youtube.com/playlist?list=PL2VXuAZDO9kb6gI8u4GT0v-J8nrXitELO [dostęp: 22 XI 2021].

publicznej, przedstawiając swego rodzaju wskaźniki radykalizacji opracowane przez ekspertów.

Ponieważ zjawisko radykalizacji zaczyna być coraz bardziej powszechne wśród młodych osób, rząd się do nich zwraca, korzystając z tych samych kanałów co rekrutrzy z grup terrorystycznych, tj. za pośrednictwem Internetu i sieci społecznościowych. Jednym z przykładów takich działań było uruchomienie kampanii #ToujoursLe-Choix[44]. Coraz częściej radykalizacja staje się udziałem młodych osób, bez względu na ich pochodzenie, rolę społeczną i miejsce zamieszkania. Wykorzystują to kampanie w sieci pokazujące, że radykalizacja może nastąpić u każdego i należy się wzajemnie wspierać, aby do niej nie doszło. Innym podejściem do budowania pewności wśród obywateli jest uruchomienie szkoleń e-learningowych na temat pojawiających się zagrożeń terrorystycznych i sposobu reagowania na nie[45]. Ponadto DGSI dokładnie opisuje na swojej stronie, jak rozpoznać oznaki radykalizacji (np. zmiana w ubiorze, nawykach żywieniowych, stopniowe wygaszanie relacji, nowe zainteresowania w sieci dotyczące religii i kultów)[46]. U młodych ludzi mogą one być efektem nieosiągnięcia sukcesu oraz doświadczenia niesprawiedliwości i dyskryminacji[47].

Zaangażowanie w prowadzenie dialogu ze społeczeństwem rządowego podmiotu, który oferuje szkolenia oraz dąży do zapobiegania radykalizacji, jest rozwiązaniem innowacyjnym. Użycie przekazów internetowych (dostęp do Internetu ma 91 proc. Francuzów, a 75,9 proc. ma konto na portalu społecznościowym[48]), przygotowanie planów i strategii rządowych w zakresie deradykalizacji[49], a także organizowanie

---

[44] Pol.: zawsze jest wybór.

[45] *Faire Face Ensemble,* https://vigipirate.gouv.fr [dostęp: 22 XI 2021].

[46] *Reconnaître les signes de la radicalisation violente,* https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/lutte-contre-terrorisme/sinformer/reconnaitre-signes-de-la-radicalisation [dostęp: 22 XI 2021].

[47] Od 2017 r. istnieje specjalna platforma dla nauczycieli, która pomaga zrozumieć zjawisko radykalizacji: CANOPÉ – https://www.reseau-canope.fr/prevenir-la-radicalisation/ressorts-et-etapes.html [dostęp: 22 XI 2021].

[48] A. Patard, *Chiffres clés d'Internet et des réseaux sociaux en France en 2021,* https://www.blogdumoderateur.com/chiffres-internet-reseaux-sociaux-france-2021 [dostęp: 22 XI 2021].

[49] Comité interministériel de prévention de la délinquance et de la radicalisation, «Prévenir Pour Protéger», *Plan national de prévention de la radicalisation*, Communiqué du Premier ministre, vendredi 23 février 2018.

prelekcji i wydarzeń są ważnymi elementami w procesie wzmacniania działań antyterrorystycznych w kraju. To dość nowe podejście do wyzwań jest ważne dla budowania więzi ze społeczeństwem oraz stanowi podwaliny do wspólnego kreowania środowiska, w którym zagrożenia terrorystyczne nie będą miały możliwości rosnąć w siłę. Inne państwa powinny rozważyć uruchomienie podobnych inicjatyw, które pozwolą obywatelom na zrozumienie przyczyn nie tylko radykalizowania, separatyzmu i sekciarstwa, lecz także np. nacjonalizmu. Jednocześnie polityka publiczna na ten temat musi być prowadzona z poszanowaniem wartości oraz ukierunkowaniem na dialog społeczny przy zaangażowaniu teoretyków i praktyków.

Reakcja na radykalizację na poziomie departamentu i kraju

Od 2014 r. na szczeblu departamentu istnieją dwa instrumenty przeciwdziałania radykalizacji. Pierwszym – o profilu bezpieczeństwa – jest utworzona przez prefekta[50] w każdym departamencie specjalna grupa ewaluacyjna ds. radykalizacji islamistycznej (fr. *groupe d'évaluation départemental de la radicalisation islamiste*, GED)[51], której celem jest utrzymanie wymiany informacji między władzami departamentów i kraju. Grupy przede wszystkim są uważane za pierwszy organ operacyjny. Odpowiadają za to, aby każda osoba, która zostanie zgłoszona jako zradykalizowana, została odpowiednio oceniona i monitorowana. GED współpracuje z jednostkami Ministerstwa Spraw Wewnętrznych (DGSI, policją[52], Żandarmerią i policją sądową) oraz w zależności od potrzeby z innymi instytucjami (wywiadem więziennym, służbami celnymi, policją graniczną[53] itp.). Drugim podmiotem – o profilu społecznym –

[50] Jego kompetencje ograniczają się do kontroli wspólnot gmin i departamentów oraz kierowania służbami państwowymi działającymi w departamencie. Więcej: M. Ofiarska, *Francja*, „Annales Universitatis Paedagogicae Cracoviensis. Studia Politologica" 2010, nr 4, s. 88–111.

[51] W jej skład wchodzą przedstawiciele departamentu, Ministerstwa Spraw Wewnętrznych, policji i żandarmerii.

[52] Przede wszystkim ze Służbą Centralną Wywiadu Terytorialnego (fr. Service central du renseignement territorial).

[53] Dyrekcja Centralna Policji Granicznej (fr. Direction Centrale de la Police Aux Frontières).

jest jednostka zapobiegania radykalizacji i wsparcia rodziny (fr. Cellule de prévention de la radicalisation et d'accompagnement des familles, CPRAF)[54]. Jej głównym zadaniem jest udzielanie wsparcia społecznego, edukacyjnego, medycznego i psychologicznego, a nawet psychiatrycznego, jeśli dotyczy radykalizacji. Przedstawiciele CPRAF, na szczeblu departamentów, udzielają obywatelom wyjaśnień w pojmowaniu religii, stanowią uzupełnienie ochrony prawnej młodzieży oraz działań pomocy społecznej dla dzieci czy kuratora. Działania jednostki są też ukierunkowane na rodzinę, aby współpracować z bliskimi osoby zradykalizowanej. Obserwacje prowadzone przez CPRAF opierają się na wskazówkach przekazywanych przez GED[55].

Ponadto na poziomie departamentu utworzono Krajowe Centrum Pomocy i Zapobiegania Radykalizacji (fr. Centre national d'assistance et de prévention de la radicalisation, CNAPR) – mogą się z nim skontaktować osoby[56], które uważają, że ktoś ulega radykalizacji. Przez pierwsze dwa lata, od otwarcia w 2014 r., na infolinię instytucji dzwoniono ponad 5 tys. razy[57]. Informacje uzyskiwane przez centrum są przekazywane do DGSI, a dokładniej do Jednostki Koordynacyjnej ds. Walki z Terroryzmem (fr. Unité de coordination de la lutte antiterroriste, UCLAT). Po potwierdzeniu przez CNAPR, że dana osoba ulega radykalizacji, informacje są przekazywane do departamentu miejsca zamieszkania, aby można było zastosować wsparcie psychologiczno-edukacyjne lub wdrożyć monitorowanie przez jednostki wywiadowcze. Wszystkie służby bezpieczeństwa działające w poszczególnych departamentach pozyskują informacje na temat osoby podejrzanej i przesyłają je do UCLAT.

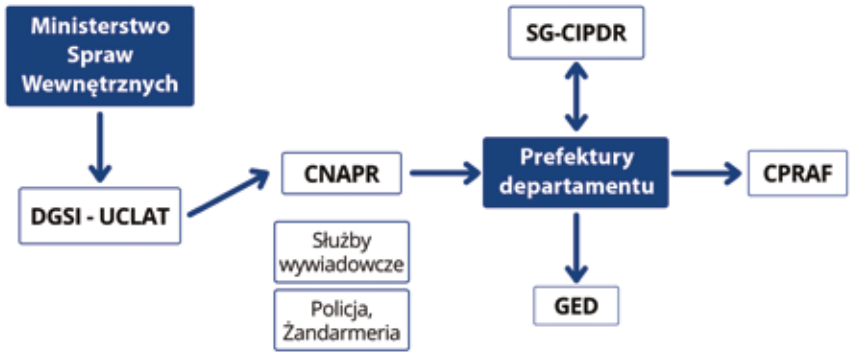
---

[54] Składa się m.in. z przedstawicieli: policji, Ministerstwa Edukacji, sądownictwa (Dyrekcja Sądowej Ochrony Młodzieży – fr. Direction de la protection judiciaire de la jeunesse), służb socjalnych, stowarzyszeń pomocy młodzieży, ale w jej skład mogą wchodzić także przedstawiciele GED.

[55] *Le dispositif territorial de prévention de la radicalisation violente*, https://www.cipdr.gouv.fr/wp-content/uploads/2019/06/Dispositif-territorial-de-pr%C3%A9vention-de-la-radicalisation-violente-1.pdf [dostęp: 22 XI 2021].

[56] Telefonicznie lub przez formularz online.

[57] *Country Reports on Terrorism 2016*, Washington 2017, s. 120.



Schemat. Podmioty zaangażowane w działania realizowane na poziomie krajowym i departamentalnym w celu przeciwdziałania radykalizacji.

Źródło: Opracowanie własne na podstawie https://www.cipdr.gouv.fr/le-cipdr/.

We francuskim ustawodawstwie należy wyróżnić możliwość prowadzenia dochodzeń dotyczących radykalizacji wobec urzędników państwowych. Artykuł 11 ustawy antyterrorystycznej zmienia sposób podejmowania działań zmierzających do zapewnienia bezpieczeństwa wewnętrznego. Nieistniejąca w stanie wyjątkowym walka z radykalizacją jest nowością w ustawie. Urzędnik (funkcjonariusz) wykonujący swoją misję lub zawód związany z bezpieczeństwem i obronnością może zostać przeniesiony lub nawet usunięty, jeżeli w wyniku dochodzenia administracyjnego ujawni skłonności do radykalizacji. Procedura ma również zastosowanie do funkcjonariuszy wojskowych oraz więziennictwa. Nowe prawo pozwala na podjęcie działań w przypadku samych tylko podejrzeń, a nie, jak było wcześniej, w otwartym już śledztwie. Wiąże się to także z cofnięciem podejrzanemu określonych zezwoleń. Wszelkie sprzeczności rozstrzyga specjalnie powoływana komisja (której skład i funkcjonowanie określa dekret Rady Stanu)[58].

Ponadto we francuskim prawie ustawodawca określił nową sankcję – kary dla rodziców, którzy podżegają swoje dzieci do popełnienia aktów terroryzmu lub wyjazdu za granicę w tym celu. Zdefiniowanie nowego przestępstwa oraz nałożenie sankcji w postaci: 15 lat pozbawienia wolności, grzywny w wysokości 225 tys. euro dla rodziców oraz

[58] *LOI n° 2017-1510*... Art. 11.

możliwości utraty praw rodzicielskich[59] – jest precedensem na skalę europejską[60].

Narodowa Prokuratura Antyterrorystyczna

Swego rodzaju novum jest powołanie organu procesowego, który ma dominujący wpływ na funkcjonowanie systemu zwalczania terroryzmu we Francji. Narodowa Prokuratura Antyterrorystyczna (fr. Parquet national antiterroriste, PNAT) została utworzona 1 lipca 2019 r. (projekt pojawił się pod koniec 2017 r.), a jej kompetencje, choć mają charakter krajowy, odnoszą się także do międzynarodowej współpracy w walce z terroryzmem[61]. PNAT jest właściwy do orzekania w takich sprawach, jak: zbrodnie przeciwko ludzkości, zbrodnie wojenne, szczególne przestępstwa, terroryzm, rozprowadzanie broni masowego rażenia i środków jej przenoszenia, tortury i porwania. Prokuratora ma szczególne kompetencje w przypadku najpoważniejszych przestępstw[62], przejmując takie sprawy od prokuratur lokalnych[63]. Ponadto do instytucji są przekazywane informacje o działaniach podejmowanych przez inne podmioty upoważnione (zgodnie z przepisami ustawy o walce z terroryzmem)[64]. W PNAT swoje obowiązki wykonują sędziowie wyspecjalizowani w prowadzeniu dochodzeń dot. terroryzmu i ekstremizmu.

---

[59] W przypadku popełnienia czynu przez osobę sprawującą władzę rodzicielską nad małoletnim sąd pierwszej instancji decyduje o całkowitym lub częściowym cofnięciu władzy rodzicielskiej zgodnie z art. 378 i 379-1 kodeksu cywilnego. Może również orzec o cofnięciu władzy rodzicielskiej w odniesieniu do innych małoletnich dzieci tej osoby.

[60] R. De Massol De Rebetz, M. van der Woude, *Marianne's liberty in jeopardy? A French analysis on recent counterterrorism legal developments*, „Critical Studies on Terrorism" 2020, t. 13, nr 1, s. 1–23.

[61] *Décret n° 2019-628 du 24 juin 2019 portant entrée en vigueur des dispositions relatives au parquet antiterroriste*, JORF n°0145 du 25 juin 2019 texte n° 4, NOR: JUSD1917754D.

[62] *Zoom sur le nouveau Parquet national antiterroriste*, http://www.justice.gouv.fr/justice-penale-11330/zoom-sur-le-nouveau-parquet-national-antiterroriste-32661.html [dostęp: 10 XI 2021].

[63] W praktyce miejscowi prokuratorzy, gdy zostaną zawiadomieni o popełnieniu na swoim terenie aktu potencjalnie terrorystycznego, kontaktują się z Narodową Prokuraturą Antyterrorystyczną, aby ta mogła ocenić, czy zamierza wykorzystać swoje kompetencje w tym zakresie we współpracy z organem lokalnym.

[64] *Code de procédure pénale*: art. 628-1, art. 706-17, art. 706-169. *Code de la sécurité intérieure*: art. L228-2. *Code de l'organisation judiciaire*: art. L217-1, art. L217-5.

Powołanie PNAT to część strategii Emmanuela Macrona dotyczącej scentralizowania walki z terroryzmem poprzez zapewnienie służbom odpowiedniej koordynacji przez prokuratora antyterrorystycznego, co ma umożliwić szybsze i skuteczniejsze działanie w przypadku zagrożenia[65]. Funkcjonowanie prokuratury jest odpowiedzią prawną na zagrożenia terrorystyczne. W świetle francuskiego prawa Narodowa Prokuratura Antyterrorystyczna jest obecnie strukturą autonomiczną, wyspecjalizowaną i przeznaczoną do walki z terroryzmem. Jej utworzenie miało na celu konsolidację działań wymiaru sprawiedliwości, zwłaszcza ze względu na serię procesów terrorystów, którzy dokonali ataków w 2015 r. i 2016 r., a są sądzeni obecnie. Tylko w 2019 r. odbyło się 87 procesów związanych z aktami terroryzmu, które prowadziła Narodowa Prokuratura Antyterrorystyczna[66]. Trzeba podkreślić, że nie wszystkie działania nacechowane terroryzmem mogą być procedowane przez PNAT, jeśli nie ma faktycznych przesłanek, że było to zdarzenie terrorystyczne[67].

Zindywidualizowany program deradykalizacji

W procesie zwalczania radykalizacji należy wyróżnić zindywidualizowany program akceptacji i ponownego przyjęcia społecznego (fr. *le programme d'accueil individualisé et de réaffiliation sociale*, PAIRS). Początkowo prowadzono program badań i interwencji przeciwko ekstremizmowi (fr. *Programme Recherches et Intervention sur les violences extrémistes*, RIVE), funkcjonujący od 2016 r., ale w 2018 r., po pozytywnym ocenieniu działalności, rozszerzono jego działalność i zmieniono

[65] J. Jacquin, *Vers la création d'un parquet national antiterroriste*, „Le Monde", 18 XII 2017 r.

[66] *Le parquet national antiterroriste, une force de frappe judiciaire*, https://france3-regions.francetvinfo.fr/paris-ile-de-france/le-parquet-national-antiterroriste-une-force-de-frappe-judiciaire-1881258.html [dostęp: 22 XI 2021].

[67] Mężczyzna z nożem zaatakował czterech policjantów, ale prokuratura regionalna już na początku śledztwa (sprawdzenie komputera oraz badania psychiatryczne) stwierdziła, że nie ma podstaw do angażowania PNAT. Mężczyznę oskarżono o usiłowanie zabójstwa. Za: K. Blondelle, *Attaque de policiers à Cannes: pas de saisie du parquet national antiterroriste*, francebleu.fr/infos/faits-divers-justice/cannes-pas-de-saisie-du-parquet-national-antiterroriste-apres-l-agression-de-policiers-au-couteau-1636728441 [dostęp: 23 XI 2021].

nazwę[68]. PAIRS organizowany w więzieniach oferuje, pod nadzorem wymiaru sprawiedliwości, system wsparcia dla osadzonych oskarżonych o akty terroryzmu lub skazanych za nie, a także zidentyfikowanych jako zradykalizowani. Oznacza to, że projekt jest realizowany nie tylko w więzieniach, lecz także w domach osadzonych lub punktach wybranych przez sąd. Głównym celem jest stworzenie warunków, w których osadzony odrzuca przemoc i chęć integracji z terrorystami poprzez uczestnictwo w zindywidualizowanym monitoringu zachowania, przy zaangażowaniu grupy wsparcia społecznego (pracownicy socjalni, psychologowie, psychiatrzy, pedagodzy, a także badacze i religioznawcy), a w wyjątkowych przypadkach także rodziny i najbliższych. Każdy uczestnik przechodzi spersonalizowany kurs, na którym poruszane są takie kwestie, jak integracja społeczna, zawodowa i kulturowa, a głównym założeniem jest osiągnięcie przez osadzonego autonomii intelektualnej, a nie całkowite odrzucenie religii. Całość opiera się na trzech filarach: społecznym, psychologicznym oraz ideologicznym. Każda osoba uczestnicząca w procesie deradykalizacji jest oceniana co trzy miesiące, a program może trwać nawet do roku.

Obecnie PAIRS obejmuje nie tylko osoby oskarżone i zradykalizowane, lecz także te, które mogą ulec temu procesowi w przyszłości. Średni czas pracy z podopiecznymi to sześć godzin tygodniowo, a prowadzona terapia może trwać od 3 do 20 godzin tygodniowo. Aktualnie istnieją cztery centra deradykalizacji w kraju, zarządzane przez kierownictwo Administracji Więziennej (fr. Administration pénitentiaire en France[69]), które znajdują się w Paryżu, Lyonie, Marsylii i Lille. W stolicy można przyjąć maksymalnie 50 osób, a łącznie w skali kraju program może objąć 125 zradykalizowanych. W 2019 r. w PAIRS wzięło udział 70 osadzonych, w 2020 r. – 90 osób, a w 2021 r. – ponad 110[70].

---

[68] M. Hecker, *Djihadistes un jour, Djihadistes toujours? Un programme de déradicalisationvu de l'intérieur*, Paris 2021, s. 9–15.

[69] Podlega pod Ministerstwo Sprawiedliwości, odpowiedzialna za wykonanie orzeczeń sądowych w sprawach karnych oraz promowanie reintegracji społecznej osób osadzonych.

[70] Według Institut français des relations internationales żadna z osób w programie po jego ukończeniu nie była sprawcą aktu terrorystycznego (stan na luty 2021 r.). Trzeba jednak podkreślić, że nie brały w nim udziału osoby najbardziej zradykalizowane, choćby te, które dokonały lub próbowały dokonać zabójstwa.

W działaniach na rzecz deradykalizacji wyróżnia się zaangażowanie służby zdrowia. Osoby, które cierpią na zaburzenia psychiczne, będą odnotowywane w raportach, a ich dane przekazywane służbom bezpieczeństwa bez wiedzy pacjentów. Współpraca będzie mieć charakter lokalny, a informacje będą weryfikowane na poziomie departamentów. Dane osób z zaburzeniami psychicznymi są przechowywane w rejestrze HOPSYWEB[71].

PAIRS funkcjonował także w trakcie pełnego zamknięcia, gdy nastąpił kryzys związany z COVID-19. Pracownicy łączyli się z osobami objętymi programem poprzez wideorozmowy oraz pozostawali w kontakcie telefonicznym. Będący pod opieką przyznali, że wsparcie specjalistów było dla nich bardzo ważne, gdy byli samotni podczas ogólnonarodowej kwarantanny[72].

Obecnie największym wyzwaniem w funkcjonowaniu programu jest określenie, czy zradykalizowany nie praktykuje takijji[73]. Jednocześnie w trakcie kilkumiesięcznej obserwacji grupa wsparcia PAIRS oraz specjaliści ze służb specjalnych obserwują osadzonego, co według ekspertów powinno pozwolić im na wychwycenie oznak ekstremizmu[74].

Z uwagi na rozwój PAIRS zarekomendowano zmiany w kodeksie karnym, aby upoważnić sędziego odpowiedzialnego za wymierzanie kary do możliwości objęcia monitoringiem osadzonego już po

---

[71] *Décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement*, NOR: SSAP1811219D, JORF n°0117 du 24 mai 2018.

[72] M. Hecker, *Djihadistes...*, s. 54.

[73] Obowiązujące w islamie przyzwolenie na ukrywanie prawdziwych wierzeń w wypadku prześladowań religijnych (lub osobistego niebezpieczeństwa). *Taqiyyah* oznacza ukrywanie swojej religii lub wiary z powodu strachu, ale w głębi serca osoba musi wyznawać religię, którą ukrywa. Innymi słowy, jest to forma samoobrony, która obejmuje obronę własnego życia, własności, godności i przekonań. Według szariatu, jeśli ktoś jest zagrożony z dwóch stron, a jedno z zagrożeń jest większe, to aby uchronić się przed nim, można zaakceptować niebezpieczeństwo o mniejszej konsekwencji (np. kłamstwo o porzuceniu wiary w porównaniu z długoletnim więzieniem). *Taqiyyah* może być definiowana jako ochrona życia, własności i honoru przed wrogiem. Za: Shia Pen, *Chapter One: Definition of Taqiyyah*, www.shiapen.com/comprehensive/taqiyyah/definition-of-taqiyyah.html [dostęp: 2 XI 2021].

[74] *Programme de suivi des individus radicalisés: „On n'a absolument pas à rougir de ce qu'on fait en France par rapport à ce qui est fait à l'étranger"*, www.ifri.org/fr/espace-media/lifri-medias/programme-de-suivi-individus-radicalises-na-absolument-rougir-de-quon [dostęp: 2 XI 2021].

zwolnieniu. Głównym założeniem jest weryfikacja radykalizacji postaw byłych więźniów[75].

W więzieniach funkcjonują także tzw. jednostki wywiadu więziennego (fr. *renseignement pénitentiaire*) będące częścią Państwowej Służby Wywiadu Więziennego (fr. Service national du renseignement pénitentiaire[76]), których jednym z zadań jest pozyskiwanie informacji dotyczących osób skazanych, m.in. za przestępstwa o charakterze terrorystycznym, oraz podejmowanie działań na rzecz bezpieczeństwa zakładów karnych. Obecnie w terenie operuje około 100 funkcjonariuszy, ale ta liczba ma wzrosnąć o kolejnych 50 do końca 2022 r.

Trzeba zaznaczyć, że we francuskich więzieniach brakowało miejsc do przetrzymywania osób skazanych za terroryzm. Dlatego od 2018 r. stale poszerza się liczbę cel w zakładach penitencjarnych dla terrorystów, także tych szczególnie niebezpiecznych. Specjalne pojedyncze cele zostaną utworzone do końca 2022 r. w 80 zakładach karnych, a docelowo ma ich być 1500[77].

Wcześniej istniały programy oceny i obserwacji więźniów skazanych za terroryzm oraz zradykalizowanych, które były realizowane w wybranych zakładach karnych w wydzielonych i przystosowanych częściach. Pierwszy z nich, prowadzony w wyznaczonych pawilonach, dotyczy oceny radykalizacji postaw (fr. *quartier d'évaluation de la radicalisation*, QER), drugi obejmuje recydywistów terrorystycznych i tych najbardziej zradykalizowanych (fr. *détenus radicalisés les plus prosélytes*, QPR). Co ważne, początkowo kobiety skazane za terroryzm nie były obejmowane żadnym programem oceny radykalizacji[78], ale teraz, właśnie za sprawą PAIRS, we Francji nastąpiła intensyfikacja tego rodzaju działań.

---

[75] Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le contrôle et le suivi de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Rapport d'information n° 348 (2019–2020) de M. Marc-Philippe Daubresse, fait au nom de la commission des lois, déposé le 26 février 2020, s. 49.

[76] *Arrêté du 29 mai 2019 portant création et organisation d'un service à compétence nationale dénommé „Service national du renseignement pénitentiaire"*, NOR: JUST1911857A, JORF n°0125 du 30 mai 2019.

[77] *LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*, NOR: JUST1806695L, JORF n°0071 du 24 mars 2019.

[78] C. Hache, *„Plus prosélytes et violentes": les détenues radicalisées, un défi pour les prisons*, „L'Express", 5 II 2020 r.

Krytycy funkcjonowania programów dla osadzonych podkreślają ich niezindywidualizowaną formę. Osoby skazane za przestępstwa o charakterze terrorystycznym nie mają prawa do uczestnictwa w pogrzebie członka rodziny oraz innych ważnych momentach (np. poważna choroba w rodzinie, uroczystość religijna)[79], pomimo ujęcia ich w kodeksie postępowania karnego[80]. Jest to spowodowane polityką karną prowadzoną przez PNAT, która utrzymuje, że obecne zagrożenie terrorystyczne wymaga utrzymywania wysokiej aktywności antyterrorystycznej w państwie[81].

W połowie 2021 r. administracja więzienna odpowiadała we Francji za niemal 82 tys. osób: 66 591 osadzonych, w tym 19 168 oskarżonych, którzy przebywali w 187 zakładach karnych (obłożenie aż 110 proc.) i 14 701 skazanych pod dozorem elektronicznym. Pod koniec 2021 r. we francuskich więzieniach przebywało 454 skazanych za terroryzm i 648 zradykalizowanych[82]. W 2020 r. było to 558 terrorystów (522 dżihadystów i 36 separatystów baskijskich), a pod obserwacją w więzieniach było łącznie ponad 1400 osadzonych podejrzewanych o radykalizację [83].

We Francji bardzo ważna jest też kwestia monitorowania islamskich terrorystów wychodzących z więzienia. Do 2023 r. 230 z nich opuści zakłady karne: w 2020 r. było to 83 skazanych, w 2021 r. – 70, w 2022 r. ma ich być 50, a w 2023 r. – 30. Co ważne, jedynie 29 proc. skazanych będzie objętych indywidualnymi środkami kontroli administracyjnej i nadzoru[84] (fr. *mesures individuelles de contrôle administratif*

[79] Odpowiednik art. 141a – zezwolenie na opuszczenie zakładu karnego *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy* (DzU z 2021 r. poz. 53).

[80] *Code de procédure pénale*. Version en vigueur au 16 novembre 2021. Art. 723-6.

[81] C. Cottineau, *Justice antiterroriste post-sentencielle: la tentation de la résignation*, https://www.dalloz-actualite.fr/node/justice-antiterroriste-post-sentencielle-tentation-de-resignation#.YaPYadDMI2w [dostęp: 18 XI 2021].

[82] *La France dénombre „648 détenus radicalisés" dans ses prisons, affirme Éric Dupond-Moretti*, https://www.lci.fr/justice-faits-divers/terrorisme-islamisme-la-france-denombre-648-detenus-radicalises-dans-ses-prisons-affirme-eric-dupond-moretti-2195734.html [dostęp: 18 XI 2021].

[83] R. Basra, P.R. Neumann, *Prisons and Terrorism: Extremist Offender Management in 10 European Countries*, London 2020, s. 7.

[84] J. Leclerc, *L'inquiétante défaillance du suivi des terroristes sortant de prison*, https://www.lefigaro.fr/actualite-france/l-inquietante-defaillance-du-suivi-des-terroristes-sortant-de-prison-20201109 [dostęp: 28 XI 2021].

et de surveillance, MICAS) przez okres nie dłuższy niż 12 miesięcy[85]. W związku z tym sprawą priorytetową będzie zweryfikowanie w trakcie odbywania kary, czy osoby skazane za terroryzm nie popełnią tego przestępstwa ponownie.

Programy deradykalizacji oraz kontroli więźniów wydają się efektywne, a Francja od 2017 r. bardzo dynamicznie i mądrze rozwija swoje struktury antyterrorystyczne. Trzeba jednak zaznaczyć, że działania podjęto zdecydowanie za późno i programy powinny funkcjonować już od 2013 lub 2014 r. Jednocześnie implementacja nowych rozwiązań musi być sygnałem dla innych państw w Europie, że wszelkim rodzajom manifestowanych skrajności należy przeciwdziałać wcześniej. Zwłaszcza gdy liczba osób, które muszą zostać objęte kontrolą, nie jest jeszcze duża i nie podjęły one działań o charakterze terrorystycznym.

Po raz kolejny w 2020 r. podkreślono, że należy podwyższyć wymiar kar wobec osób skazanych za przestępstwa terrorystyczne, które ponownie się radykalizują, poprzez zwiększenie wyroku, a także nakaz stałego poddawania się kontroli. Ponadto zarekomendowano kilka działań, które należy stale realizować, a w szczególności: przekazywanie informacji o nadzorze poszczególnych osób do prokuratury krajowej oraz prokuratur terytorialnych, nadanie prefektom możliwości zamykania – nawet kilkakrotnie z tego samego powodu – miejsc kultu, a także obiektów, które należą do osób prawnych lub fizycznych, stała kontrola i monitorowanie osób skazanych za terroryzm w celu weryfikacji ich możliwej radykalizacji, a także ułatwienie służbom dostępu do komputerowych danych podejrzanych. Ostatecznie dotychczasową intensyfikację działań w walce z terroryzmem i radykalizacją realizowanych w państwie oceniono pozytywnie[86].

[85] Rada Konstytucyjna orzekła o zgodności z Konstytucją poszczególnych środków kontroli i nadzoru administracyjnego (MICAS) stworzonych ustawą z 30 października 2017 r. o wzmocnieniu bezpieczeństwa wewnętrznego i walce z terroryzmem. Jest to odpowiednik aresztu domowego. Za: *Loi n° 2017-1510*...; O. Cahn, J. Leblois-Happe, *Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme: perseverare diabolicum*, „Actualité juridique. Pénal" 2017, s. 468; *Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence*; *Décision n° 2017-624 QPC*, 16 mars 2017.

[86] *Rapport d'information fait*...

Wykorzystanie strażników miejskich lub równoważnych służb w innych państwach

Ze względu na zagrożenia terrorystyczne występujące na terytorium Republiki Francuskiej coraz więcej gmin decyduje się na szkolenie funkcjonariuszy. Jest to nowa strategia, którą zaczęto wprowadzać w życie pod koniec 2019 r.[87]. Wynika to z faktu, że policja miejska[88] jest zazwyczaj na pierwszej linii frontu, gdy pojawia się niebezpieczeństwo. Burmistrz gminy Cannes stwierdził, że nawet jeśli reagowanie na terroryzm nie jest częścią uprawnień policjantów miejskich, to wszyscy w tej gminie przejdą trening do końca 2020 r. W listopadzie 2019 r. 200 funkcjonariuszy policji w Cannes zostało przeszkolonych w zakresie reagowania w przypadku ataku terrorystycznego. Kontrterroryści z RAID (fr. Recherche, Assistance, Intervention et Dissuasion) i BRI (fr. Brigade de recherche et d'intervention) przeprowadzili kurs na podstawie scenariusza potencjalnego ataku w Palais des Festivals et des Congrès w Cannes[89]. Jest to bardzo ważny przykład akcji, które angażują w zasadzie każdy z podmiotów do reagowania na zagrożenia o charakterze terrorystycznym. Należy zwrócić uwagę na to, że działania, które zostaną podjęte tuż przed atakiem lub tuż po nim, są decydujące dla stanu bezpieczeństwa w okolicy.

Gdy nastąpił zamach w Nicei w lipcu 2016 r., to m.in. strażnicy miejscy odpowiadali za bezpieczeństwo ruchu drogowego. Ich wiedza na temat zagrożeń terrorystycznych oraz szybkie przekazanie informacji o niebezpieczeństwie do innych służb spowodowały, że ofiar było znacznie mniej[90]. Ponadto dobrze współpracowali w trakcie i po ataku z policją oraz żołnierzami działającymi w ramach operacji Sentinelle.

---

[87] M. Auray, *La place de la police municipale dans la lutte contre le terrorisme*, Lille 2019, s. 1–2.

[88] Która na potrzeby artykułu jest nazywana strażą miejską, a jej kompetencje są podobne do formacji działającej w Polsce, Stadtpolizei w Niemczech, Policia Local w Hiszpanii, městská policie w Czechach, Handhaving w Holandii czy Муніципальна поліція na Ukrainie.

[89] P. Renoir, F. Azur, *Cannes forme ses policiers municipaux à intervenir en cas d'attaque terroriste*, https://www.francebleu.fr/infos/faits-divers-justice/cannes-forme-ses-policiers-a-intervenir-en-cas-d-attaque-terroriste-1574963396 [dostęp: 10 XI 2021].

[90] Warto też dodać, że wówczas funkcjonariusze tej formacji nie dysponowali bronią, jaka jest na wyposażeniu policji, a przez to nie udało im się zatrzymać ciężarówki w pierwszej fazie ataku i mogli tylko przekazać informacje o zagrożeniu do innych podmiotów.

Ich właściwe ruchy były skutkiem przygotowań do organizacji meczów EURO 2016 w Nicei, ponieważ przeszli pięć szkoleń antyterrorystycznych[91].

Strażnikom miejskim nadano uprawnienia do organizowania i utrzymywania stref ochronnych w gminach. Oddzielenie obszarów (w celu utrzymania bezpieczeństwa podczas imprez sportowych, kulturalnych, świątecznych oraz zgromadzeń i demonstracji) ogranicza ryzyko dokonania ataku terrorystycznego poprzez kontrolowanie dostępu i przemieszczania się osób[92]. Jest to przykład na wykorzystanie formacji, której zadaniem nie jest stricte walka z terroryzmem, do konkretnych działań na rzecz wzmocnienia potencjału antyterrorystycznego państwa. Aż 98 proc. gmin we Francji ma straż miejską.

Zaangażowanie strażników miejskich ma służyć wzmocnieniu skuteczności reakcji społecznej na wypadek kryzysów, gdyż to oni znają najlepiej sytuację w poszczególnych gminach. Funkcjonariusze mogliby wspierać policję i żandarmerię, a także być łącznikiem, którego zadaniem byłoby informowanie o potrzebie użycia oddziałów kontrterrorystycznych lub wojsk specjalnych, gdyż już teraz są wykorzystywani podczas zwiększonego zagrożenia w państwie[93] w ramach planu Vigipirate. Co ważne, funkcjonariusze *police municipale* mogą być upoważnieni do noszenia broni (do 2016 r. jej nie posiadali) na wniosek burmistrza gminy[94]. Głównym celem ich angażowania jest podjęcie zintegrowanych działań w walce z terroryzmem, aby wszystkie środki użyte na terytorium kraju były skoordynowane. Obejmuje to również reagowanie na inne zagrożenia w gminie, jak np. przestępczość zorganizowana. We Francji rekomendowane jest dalsze wzmacnianie kompetencji straży miejskiej oraz zacieśnianie współpracy z policją[95].

---

[91] *Déclaration de M. Manuel Valls, Premier ministre, en réponse à diverses questions portant sur la lutte contre le terrorisme depuis 2012, l'attentat de Nice, la prorogation de l'état d'urgence et les opérations extérieures menées par la France contre Daech, à l'Assemblée nationale le 20 juillet 2016*.

[92] *Code de la sécurité intérieure*, Version en vigueur au 18 novembre 2021. Art. L226-1.

[93] *Lutte contre la radicalisation et le séparatisme islamiste: la ville agit pour votre sécurité!*, https://www.vernon27.fr/actualites/lutte-contre-la-radicalisation-et-le-separatisme-islamiste-la-ville-agit-pour-votre-securite [dostęp: 19 XI 2021].

[94] *Code de la sécurité intérieure*, Version en vigueur au 19 novembre 2021. Paragraphe 1: Armes susceptibles d'être autorisées (art. R511-12 à R511-13).

[95] L'ancrage territorial de la sécurité intérieure – Rapport final, n° 323 (2020-2021), Date de remise: 29 janvier 2021.

Działalność organizacji pozarządowych na rzecz ofiar terroryzmu

Oprócz działań podejmowanych przeciwko terroryzmowi lub reagowania na atak równie istotne jest zaangażowanie osób i środków w pomoc obywatelską dla tych, którzy ucierpieli na skutek ataków. W Republice Francuskiej organizacje pozarządowe są uzupełnieniem instytucji państwowych. Specjalnie wyznaczone do tego podmioty mają za zadanie wspomóc funkcjonujący w kraju system zwalczania terroryzmu oraz zapewnić wsparcie potrzebującym. Wybrane instytucje wspierające pokrzywdzonych w zamachach lub z powodu wpływu terroryzmu to m.in.:

- Association française des Victimes du Terrorisme (AfVT, Francuskie Stowarzyszenie Ofiar Terroryzmu) – jest finansowane przez Komisję Europejską, a jego zadaniem jest nawiązanie dialogu między ofiarami zamachów terrorystycznych a ogółem społeczeństwa (szczególnie młodzieżą) w celu zapobiegania radykalizacji oraz promowania poczucia obywatelstwa i koleżeństwa w obliczu terroryzmu. Organizacja ma służyć pomocą ofiarom terroryzmu i ich rodzinom. Pomoc ta może mieć charakter moralny, administracyjny, finansowy, prawny, medyczny lub inny. Prowadzone są trzy rodzaje misji: psychologiczna, prawna lub zapobiegawcza. AfVT nadzoruje i monitoruje działalność Międzynarodowej Federacji Stowarzyszeń Ofiar Terroryzmu (FIAVT). Zapewnia również treści dywersyjne online dla takich wyszukiwarek jak Google, aby wyświetlać je osobom szukającym tematyki ekstremistycznej[96].
- Association IMAD pour la jeunesse et la paix (IMAD, Stowarzyszenie IMAD dla młodości i pokoju) – zostało powołane w celu ustanowienia dialogu międzyreligijnego, aby zapobiec ekscesom o charakterze ekstremistycznym, a także w celu wspierania świeckiej i republikańskiej tradycji[97].
- Fédération nationale des victimes d'attentats et d'accidents collectifs (FENVAC, Krajowa Federacja Ofiar Ataków i Wypadków Zbiorowych) – została założona w 1994 r. Skupia ponad 70 stowarzyszeń we Francji i za granicą (Barcelona, Bardau, Wagadugu,

[96] Association française des Victimes du Terrorisme, https://www.afvt.org/ [dostęp: 8 XI 2021].

[97] Association IMAD pour la jeunesse et la paix, https://association-imad.fr/en/association-for-youth-and-peace/ [dostęp: 8 XI 2021].

Marrakesz itp.). Dzięki swojemu doświadczeniu dzieli się wskazówkami opartymi na relacjach członków i zachęca ofiary do spotkania. Wsparcie to może być również indywidualne i obejmować problemy prawne, administracyjne, psychologiczne, społeczne itp. napotykane przez ofiary[98].

– Association 13 novembre: fraternité et vérité (13onze15, Stowarzyszenie 13 Listopada: Braterstwo i Prawda) – wspiera w sądach i instytucjach pokrzywdzonych w wyniku ataków. Przyczynia się też do upamiętnienia ofiar ataków[99].
– Association Montjoye – oferuje ofiarom wsparcie społeczne, prawne i psychologiczne. Fundacja stanowczo poparła utworzenie strefy informacji dla ofiar zamachu bombowego w Nicei z 14 lipca 2016 r., w którym zginęło 87 osób, a 202 zostały ranne, aby jak najszybciej zapewnić pomoc[100].

We wsparcie finansowe zaangażowały się również organy państwowe. Zgodnie z ustawą w sprawie planowania i reformy wymiaru sprawiedliwości na lata 2018–2022[101] ofiary terroryzmu, tj. obywatele francuscy, a w tym także funkcjonariusze publiczni i żołnierze, otrzymają odszkodowanie. Środki mogą być przyznawane ofiarom aktów terroryzmu popełnionych zarówno w kraju, jak i za granicą, a także osobom pozostającym na utrzymaniu ofiar, niezależnie od ich narodowości. Co ważne, jeśli doszło do niebezpiecznej sytuacji z winy poszkodowanego, można odmówić zadośćuczynienia lub zmniejszyć jego wysokość[102]. Pieniądze będą wypłacane ze specjalnie utworzonego funduszu gwarancyjnego (fr. Fonds de Garantie des Victimes des actes de Terrorisme et d'autres Infractions, FGTI[103]). Obecnie środki przeznaczone przez rząd na pomoc ofiarom terroryzmu to 30 mln euro.

Pomoc finansowa i psychologiczna jest najważniesza, aby wesprzeć obywateli w przypadku ataku terrorystycznego. Dlatego państwa szczególnie narażone na tego rodzaju ataki powinny usprawniać system

[98] Fédération nationale des victimes d'attentats et d'accidents collectifs, https://www.fenvac.com/ [dostęp: 8 XI 2021].

[99] Association 13 novembre: fraternité et vérité, http://13onze15.org/ [dostęp: 8 XI 2021].

[100] Association Montjoye, https://montjoye.org/ [dostęp: 8 XI 2021].

[101] *LOI n° 2019-222…*

[102] *Code des assurances*, Version en vigueur au 17 novembre 2021. Art. L126-1.

[103] *Les statuts du Fonds de Garantie des Victimes des actes de Terrorisme et d'autres Infractions (FGTI)*, https://www.fondsdegarantie.fr/fgti/statuts/ [dostęp: 18 XI 2021].

wsparcia socjalnego. W Niemczech wciąż istnieje problem, aby zapewnić dobre warunki życia ofiarom terroryzmu, i niezbędne są w tej kwestii zmiany legislacyjne. Wiele osób stara się o uzyskanie wystarczającego wsparcia od rządu oraz pieniądze z ubezpieczeń, gdyż nie ma funduszy na życie i rehabilitację[104]. Republika Francuska wykonała zatem właściwy krok na rzecz pomocy poszkodowanym.

Wykorzystanie mediów społecznościowych do informowania obywateli

Przykładem działania mającego na celu przekonanie społeczeństwa do zaalarmowania władz o potencjalnym niebezpieczeństwie jest inicjatywa Ministerstwa Spraw Wewnętrznych Republiki Francuskiej, które nawołuje do przekazywania służbom informacji o tym, że osoba w ich otoczeniu mogła ulec radykalizacji, zamierza dokonać ataku lub wystąpiło zagrożenie terrorystyczne. Utworzono w tym celu specjalną infolinię, aby zgłoszenie zostało skierowane do konkretnego podmiotu.

Innym rozwiązaniem, które należy wysunąć na pierwszy plan, jest wykorzystanie mediów społecznościowych jako formy przekazywania informacji służbom bezpieczeństwa. Takie działania są wprowadzane nie tylko we Francji, lecz także w innych państwach, np. Austrii. Podczas ataku terrorystycznego w Wiedniu 2 listopada 2020 r., gdy policja ścigała terrorystę, o jego ruchach informowały postronne osoby. Austriackie Ministerstwo Spraw Wewnętrznych zdecydowało, żeby osoby widzące terrorystów udostępniły informacje za pomocą specjalnego formularza na stronie, co miało ułatwić służbom lokalizację zagrożenia. Tamtejsze służby prosiły, aby nie umieszczać informacji w mediach społecznościowych – co mogło prowadzić do dezinformacji – tylko aby przekazać dane bezpośrednio do policji, która zweryfikowane informacje o zagrożeniach kolportowała dla obywateli.

Kolejnym istotnym elementem wzmacniania systemu zwalczania zagrożeń terrorystycznych przy wykorzystaniu mediów społecznościowych jest stała komunikacja pomiędzy służbami a społeczeństwem. Posługiwanie się narzędziami cyfrowymi do przekazywania informacji ważnych dla obywateli powinno być podstawą do budowania poczucia

[104] H. Rubinich, *Überlebende von Terroranschlägen. Der schwierige Weg aus dem Trauma*, https://www.deutschlandfunkkultur.de/ueberlebende-von-terroranschlaegen-der-schwierige-weg-aus-100.html [dostęp: 20 XI 2021].

bezpieczeństwa i zatrzymywania rosnącej dezinformacji, np. ze strony fałszywych stron lub grup terrorystycznych[105]. Dlatego też należy sięgnąć do platform, które umożliwią powiadamianie o ryzyku i wskazanie miejsca ataku oraz stref, które są niebezpieczne. Używanie Internetu do komunikacji jest powszechne, a stworzenie oficjalnego profilu służącego wyłącznie do sygnalizowania zagrożeń byłoby bardzo pomocne nie tylko dla obywateli, lecz także dla turystów czy migrantów znajdujących się w danym momencie w zagrożonym regionie[106]. Niezbędny jest do tego oficjalny profil na omawianych portalach (jeden dla całego państwa, aby komunikaty nie były powielane lub modyfikowane na stronach policji, centrum zarządzania kryzysowego lub ministerstwa obrony[107]), który będzie zawsze przedstawiał najważniejsze i oficjalne dane dotyczące zagrożeń dla obywateli. Byłby to profil, który donosiłby o niebezpieczeństwie i dawał konkretne wytyczne, np. nie używać wybranej linii metra lub nie kierować się do centrum miasta. Co więcej, taka strona mogłaby być częścią polityki bezpieczeństwa państwa i być udostępniana przez portale turystyczne oraz na stronie ambasad, aby przyjeżdżający do kraju wiedzieli, że w przypadku np. ataku terrorystycznego mogą sprawdzić oficjalny przekaz w Internecie. Trzeba jednak zaznaczyć, że musi ona funkcjonować w trybie 24 godziny na dobę i być stale aktualizowana.

Szkolenie personelu medycznego

Kolejną bardzo istotną częścią systemu zwalczania zagrożeń terrorystycznych jest odpowiednia reakcja na zamach. Oprócz aktywności służb bezpieczeństwa najważniejsza w przypadku ataku jest właściwa i szybka organizacja służb medycznych. W Republice Francuskiej istnieją specjalne zespoły ratunkowe przygotowane do niesienia pomocy w czasie ataku terrorystycznego, a także udzielenia pomocy dużej

[105] S. Gliwa, A. Olech, *Republika Francuska w obliczu działalności Państwa Islamskiego. Doświadczenia płynące z ataków terrorystycznych i propagandy w mediach społecznościowych w latach 2015–2019*, „Wiedza Obronna" 2020, t. 271, nr 2, s. 109–130.

[106] Ministerstwa spraw wewnętrznych Austrii i Francji podczas ataków terrorystycznych w 2020 r. stale informowały (również w języku polskim) na swoich profilach w mediach społecznościowych o występującym zagrożeniu.

[107] Ministère de l'Intérieur – Alerte, https://twitter.com/Beauvau_Alerte [dostęp: 19 XI 2021].

liczbie poszkodowanych. W reakcji na zamach natychmiastowo są uruchamiane specjalne zespoły medyczne i straży pożarnej oraz grupy rezerwowe (na wypadek kolejnych ataków), a także zespół ds. regulowania kryzysu, który odpowiada za organizowanie przyjęć pacjentów oraz wysyłanie mobilnych jednostek (lekarzy i pielęgniarek). Takie podejście nie powoduje zbyt dużego napływu rannych do jednego szpitala. Ponadto lekarze, pielęgniarki, policja oraz staż pożarna regularnie przechodzą wspólne symulacje i treningi, aby w odpowiedni sposób podjąć czynności ratujące życie w skoordynowanej akcji ratunkowej.

W listopadzie 2015 r. podczas ataków w Paryżu służby medyczne poradziły sobie z sytuacją pomimo brutalności sprawców i przerażającej liczby rannych, ponieważ były dobrze przygotowane. Już od stycznia tego samego roku (po atakach na siedzibę „Charlie Hebdo") istniało niebezpieczeństwo, że może dojść we Francji do kolejnego zamachu. Ponadto w 2013 r. wprowadzono protokoły działań dla zespołów ratowników medycznych (fr. Service d'aide médicale urgente, SAMU), policji i straży pożarnej dotyczące udzielenia pierwszej pomocy oraz transportu poszkodowanych na wypadek ataku terrorystycznego[108]. Odpowiednie przeszkolenie zespołu medycznego skutkuje zmniejszeniem ryzyka zgonu poszkodowanych, a także wysłaniem pacjentów do oddziałów, które udzielą im niezbędnej pomocy (w zależności od specjalizacji szpitala oraz dostępności medyków i sprzętu). Ze wszystkich pacjentów, którzy przyjechali do szpitala po ataku z 13 listopada 2015 r. w Paryżu (łącznie 302 osoby), zmarło czworo, co stanowi mniej niż 1 proc. rannych[109]. Przeprowadzenie bardzo sprawnej akcji ratunkowej było efektem wcześniejszych ćwiczeń dla służb medycznych na wypadek zagrożenia terrorystycznego.

Odnosząc się do powyższych działań, należy podkreślić, że obecnie w wielu państwach w Europie, w tym w Polsce, nie są prowadzone obowiązkowe szkolenia dla ratowników medycznych i lekarzy, które przygotowałyby ich na tego typu sytuacje. Co więcej, nie zostało to ujęte

[108] W dniu zamachu we Francji, 13 listopada 2015 r., SAMU, policja i straż pożarna wzięły udział w ćwiczeniach symulujących organizację zespołów ratowniczych na wypadek strzelaniny w Paryżu. Scenariusz obejmował ataki na wiele lokalizacji. Wieczorem, gdy ci sami lekarze zostali skonfrontowani z tą sytuacją w rzeczywistości, niektórzy z nich uważali, że to kolejne ćwiczenie symulacyjne.

[109] M. Hirsch i in., *The medical response to multisite terrorist attacks in Paris*, „The Lancet" 2015, nr 386 (10012), s. 1–4.

w planowanych kursach doskonalenia zawodowego. Nie ma też uregulowań prawnych ani środków finansowych, aby takie ćwiczenia przeprowadzić. Jednocześnie pojawiają się inicjatywy oddolne, które oferują medykom przejście kursu, aby byli w stanie odpowiednio zareagować w krytycznym momencie[110]. Jest to bardzo ważne, ponieważ zachowanie przedstawicieli służby zdrowia może mieć kluczowe znaczenie, jeśli dojdzie do zamachu. Dlatego też niezbędne jest prawne uregulowanie tej kwestii oraz podjęcie działań na poziomie ministerialnym, aby takie szkolenie przeszła większość ratowników medycznych, a przynajmniej ci, którzy pracują w dużych miastach, gdzie zagrożenie terrorystyczne jest wyższe. Instruktaże przygotowawcze dla ratowników medycznych i szpitali wprowadzono także m.in. w Hiszpanii[111], Wielkiej Brytanii[112] i Turcji[113], czyli krajach już doświadczonych atakami terrorystycznymi. Nie oznacza to, że ratownicy medyczni mają operować przed opanowaniem zagrożenia, ale wykwalifikowana pomoc medyczna powinna mieć wiedzę i schematy do reagowania i minimalizacji strat.

Zakończenie

W ocenie autora proces przeciwdziałania zagrożeniom o charakterze terrorystycznym wymaga współpracy różnych podmiotów i grup

[110] *Czy polscy ratownicy są przygotowani na udzielenie pomocy po ataku terrorystycznym?*, https://www.infosecurity24.pl/czy-polscy-ratownicy-sa-przygotowani-na-udzielenie-pomocy-po-ataku-terrorystycznym?fbclid=IwAR2S8FsK2p2wHhVPrU99lvUJrf9LcLnZf6fmpOhORB1RhV14NT4s3u2eJeU [dostęp: 18 XI 2021].

[111] *Así funcionan los protocolos sanitarios en caso de atentados en España*, https://www.consalud.es/pacientes/asi-funcionan-los-protocolos-sanitarios-en-caso-de-atentados-en-espana_22428_102.html?fbclid=IwAR0fqXimun7oK2vbK7UCiFddJqSYfGbLRc0BKRHQ2ec_ZRuTF8Uw4LQZ41w [dostęp: 21 XI 2021]; *Simulacro antiterrorista*, https://www.diariodesevilla.es/vivirensevilla/Simulacro-antiterrorista_0_1131787221.html [dostęp: 21 XI 2021].

[112] E. Skryabina i in., *UK healthcare staff experiences and perceptions of a mass casualty terrorist incident response: a mixed-methods study*, „Emergency Medicine Journal" 2021, t. 38, nr 10.

[113] G. Tarihi, *Hastanemiz çalışanlarına Adıyaman Emniyet Müdürlüğü Terörle Mücadele Daire Başkanlığı Büro Amirliği tarafından „Terörle Mücadele" eğitimi verildi*, https://besnidh.saglik.gov.tr/TR,36418/hastanemiz-calisanlarina-adiyaman-emniyet-mudurlugu-terorle-mucadele-daire-baskanligi--buro-amirligi-tarafindan-terorle-mucadele-egitimi-verildi.html [dostęp: 21 XI 2021].

na wielu etapach. Współcześnie nie wystarczy tylko utrzymywanie oddziału kontrterrorystycznego. Zwalczanie tego rodzaju agresji wymaga zaangażowania całych społeczeństw i wszystkich środków posiadanych przez państwo. Każdy z elementów nadzorowanych przez administrację publiczną ma ważną rolę do odegrania w procesie weryfikacji i reagowania na niebezpieczeństwa. Antyterroryzm powinien współcześnie obejmować reagowanie na: proces stopniowej radykalizacji, podejmowaną działalność terrorystyczną, a także aktywność osób skazanych za terroryzm (lub inne przestępstwa o znamionach terroryzmu), które już odbyły karę. Ponadto należy wziąć pod uwagę inne wyzwania, jak choćby radykalizację młodych osób, brak dostępu do programów resocjalizacyjnych dla osadzonych, niewystarczające wsparcie ofiar agresji i terroryzmu, niewykorzystanie potencjału Internetu i mediów społecznościowych, nieskuteczność w reagowaniu na terroryzm przez poszczególne formacje mundurowe oraz nieprzygotowanie zespołów medycznych na wypadek ataku. Te wszystkie działania mogą zostać podjęte w krótkim czasie, gdyż wiele państw Unii Europejskiej, w tym przede wszystkim Polska, ma odpowiednie narzędzia oraz zdolność do ich realizacji. Determinantem powinno być to, że we Francji terroryzm ma charakter regularny, a w Polsce zagrożenie wciąż jest niewielkie, można więc uznać, że jest to dobry czas, aby już teraz przygotować się na sytuację krytyczną. Francuska eksperiencja demonstruje zarówno błędy i uchybienia, których nie należy powtarzać, jak i szczególne oraz sprawdzone rozwiązania, z których należy skorzystać.

W procesie deradykalizacji[114] skazanych oraz tych, którzy mogą dopiero rozpocząć działalność terrorystyczną, ważna jest pomoc ze strony wielu grup ludzi. W ramach „zespołu deradykalizacyjnego"[115] wyróżnia się: nauczycieli (mogących zahamować radykalizację młodych osób),

[114] Radykalizacja nie musi przyjmować od razu formy ataku terrorystycznego. Ponadto proces ten dotyczy wszystkich ideologii, w ramach których podejmuje się działania nacechowane przemocą i agresją z intencją wymuszenia zmian w państwie, co prowadzi do destabilizacji, zamieszania oraz wzbudzenia niepokojów. Radykalizować się mogą wyznawcy każdej religii, przedstawiciele konkretnych ideologii, zwolennicy partii politycznych oraz ruchów. Dotyczy to tak samo dżihadu, terroryzmu prawicowego, lewicowego, separatyzmu, nacjonalizmu, a nawet działań prowadzonych przez określone społeczności.

[115] Autor stwierdza, że niezbędna jest nomenklatura dotycząca całego zespołu zaangażowanego we wsparcie osoby mogącej ulegać wpływom szkodliwej ideologii, dlatego też proponuje własną nazwę.

psychologów, strażników (lub opiekunów) w miejscu osadzenia, współpracowników, rodzinę, znajomych i duchownych (albo kogoś postrzeganego jako znawca lub przewodnik w religii lub ideologii, którą dana osoba wyznaje). Wymienione grupy – jeśli będą współpracować – są w stanie pomóc jednostce, która ulega szkodliwym wpływom. Podstawą współpracy jest rozmowa i wymiana poglądów pomiędzy członkami zespołu. Nie musi on mieć oficjalnych ram, ale wystarczy niezbędny kontakt pomiędzy osobami otaczającymi radykalizujących się. Tak jak w systemie zwalczania zagrożeń terrorystycznych ważne jest całe państwo, tak tutaj kluczowy jest zespół, który może odpowiednio wcześnie zareagować, dzięki czemu nie dojdzie do ataku. Ponadto postronni mogą zwrócić uwagę na niepokojące symptomy, które zostaną przeanalizowane przez osoby otaczające radykała. Dlatego tak istotne jest zwracanie uwagi na rosnącą agresję (mającą podstawę w ideologii) czy to w Internecie, czy miejscu pracy (nauki). Każda z osób może stać się sygnalistą zagrożenia. Nie oznacza to, że podejrzany będzie od razu pociągnięty do odpowiedzialności karnej, ale jego zachowanie może być monitorowane przez służby bezpieczeństwa. W Republice Francuskiej ten proces tak właśnie przebiega, co znacznie ułatwia podjęcie działań, jeśli faktycznie dojdzie do silnej radykalizacji. Jest to obecnie tak bardzo specyficzne niebezpieczeństwo, że wymaga stałej czujności i obserwacji wszystkich obywateli.

W walce z terroryzmem i w zapobieganiu gwałtownej radykalizacji rządy państw, a także organizacje regionalne i międzynarodowe stoją w obliczu poważnych wyzwań. Jednak dzięki ponadnarodowej współpracy są one w stanie reagować nie tylko na konwencjonalne, lecz także na asymetryczne zagrożenia, takie jak ekstremizm i zorganizowana przestępczość. Ponadto wobec coraz bardziej niewyraźnego charakteru linii podziału między bezpieczeństwem wewnętrznym i zewnętrznym konieczna jest ponowna analiza dostosowania systemów bezpieczeństwa do sytuacji geopolitycznej, aby uczynić je bardziej skutecznymi. Wykorzystanie nawet części rozwiązań stosowanych we Francji będzie bardzo efektywne na polskim gruncie. Zagrożenie w postaci przeprowadzenia ataku czy radykalizacji jest tak samo możliwe. Zmienia się jedynie sprawca i jego motywacja.

Brak jednolitego postrzegania zjawiska terroryzmu we Francji i w Polsce nie oznacza, że nie można określić skutecznych metod i sposobów przeciwdziałania, które będą właściwe dla obu państw. Podmioty odpowiedzialne za zwalczanie terroryzmu nie mogą być powoływane

dopiero w momencie wykrycia zagrożenia lub nastąpienia ataku. Celem nadrzędnym powinna być prewencja i stworzenie warunków do powstrzymywania radykalizacji poszczególnych grup i jednostek. Jednocześnie w przypadku zamachu, a także w czasie reorganizacji po jego dokonaniu, rząd powinien dysponować zestawem środków do załagodzenia negatywnego wpływu agresji na społeczeństwo. Wiele rozwiązań przedstawionych w niniejszym opracowaniu ma na celu zwrócenie uwagi na mniej popularne metody prowadzenia polityki antyterrorystycznej państwa, ale równie ważne w procesie budowania potencjału bezpieczeństwa. Dodatkowo, opisane francuskie rozwiązania mogą być zaimplementowane i rozszerzone w Polsce dość naturalnie, w ramach rozwoju dotychczas posiadanych narzędzi[116]. Obecnie środowisko, w którym dochodzi do radykalizacji i ataków terrorystycznych, zmienia się. Ze względu na postęp technologiczny dzieje się tak, że terroryzm to nie tylko zamach z użyciem materiałów wybuchowych, lecz także destrukcyjne wykorzystywanie Internetu i mediów społecznościowych. W związku z tym rozpoznanie metod i środków, jakich mogą użyć terroryści, jest niezwykle istotne w procesie weryfikacji zagrożenia, aby móc skutecznie je wyeliminować w pierwszej fazie rozwoju.

Wzmocnienie obecnych struktur do walki z terroryzmem w Polsce będzie bardzo ważne w nadchodzących latach z uwagi na rosnące zjawisko radykalizacji[117]. Ponadto określenie już teraz strategii i metod reagowania na wyzwania, które nie są jeszcze tak powszechne jak we Francji, pozwoli na właściwą ocenę potencjału i umiejętności poszczególnych podmiotów[118]. Przeprowadzona ewaluacja uwydatni również nieprawidłowości, które trzeba naprawić, oraz pozwoli na obranie kierunku zmian i doskonalenia polskiego i europejskiego antyterroryzmu.

Analizując przyszłe rozwiązania dla Polski, na początek warto wznowić prace nad kolejną edycją Narodowego Programu Antyterrorystycznego, aby umieścić w nim obszar radykalizacji w sposób

[116] Między innymi uruchomienie kursów e-learningowych przez Centrum Prewencji Terrorystycznej ABW (za: https://learning.tpcoe.gov.pl/ [dostęp: 27 XI 2021]) oraz utworzenie specjalnej komórki więziennictwa z prawem do inwigilacji (za: infosecurity24.pl/specjalna-komorka-wieziennictwa-z-prawem-do-inwigilacji [dostęp: 27 XI 2021]).

[117] Collegium Civitas, *Społeczny wymiar radykalizacji – czynniki wpływające na proces radykalizacji młodych ludzi. Wnioski z badań w projekcie „DARE"*, Warszawa 2021.

[118] A. Olech, *Walka z terroryzmem…*

adekwatny do wyników ww. badań. Dzięki temu ta problematyka zostałaby kompleksowo rozwinięta w ramach istniejącego systemu AT w RP. Pozwoliłoby to na stworzenie podsystemu wspierającego rozpoznanie zagrożeń terrorystycznych, składającego się z inicjatyw społecznych, projektów naukowo-badawczych oraz rozwiązań instytucjonalnych, które łączyłby potencjał informacji zebranych przez organy administracji lokalnej, Policji, ABW i Służby Więziennej.

Bibliografia

Auray M., *La place de la police municipale dans la lutte contre le terrorisme*, Lille 2019.

Basra R., Neumann P.R., *Prisons and Terrorism. Extremist Offender Management in 10 European Countries*, London 2020.

Block L., *Evaluating the Effectiveness of French Counter-Terrorism*, „Terrorism Monitor" 2005, t. 3, nr 17, bez paginacji.

Cahn O., Leblois-Happe J., *Loi n° 2017–1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme: perseverare diabolicum*, „Actualité juridique. Pénal" 2017, nr 11, s. 468–471.

Collegium Civitas, *Społeczny wymiar radykalizacji – czynniki wpływające na proces radykalizacji młodych ludzi. Wnioski z badań w projekcie „DARE"*, Warszawa 2021.

Country Reports on Terrorism 2016, Washington 2017.

De Massol De Rebetz R., Woude M. van der, *Marianne's liberty in jeopardy? A French analysis on recent counterterrorism legal developments*, „Critical Studies on Terrorism" 2020, t. 13, nr 1, s. 1–23.

Gliwa S., Olech A., *Republika Francuska w obliczu działalności Państwa Islamskiego. Doświadczenia płynące z ataków terrorystycznych i propagandy w mediach społecznościowych w latach 2015–2019*, „Wiedza Obronna" 2020, t. 271, nr 2, s. 109–130.

Hache C., *„Plus prosélytes et violentes": les détenues radicalisées, un défi pour les prisons*, „L'Express", 5 II 2020 r.

Hecker M., *Djihadistes un jour, Djihadistes toujours? Un programme de déradicalisationvu de l'intérieur*, Paris 2021.

Hirsch M. i in., *The medical response to multisite terrorist attacks in Paris*, „The Lancet" 2015, nr 386, s. 1–4.

Jacquin J., *Vers la création d'un parquet national antiterroriste*, „Le Monde", 18 XII 2017 r.

Johnson J.B., Reynolds H.T., Mycoff J.D., *Metody badawcze w naukach politycznych*, tłum. A. Kloskowska-Dudzińska, Warszawa 2010.

Kuc B., Ściborek Z., *Podstawy metodologiczne nauk o bezpieczeństwie*, Warszawa 2013.

Merchet J.D., *Mali: une «cinquantaine de terroristes neutralisés» par l'armée française*, „L'Opinion", 3 XI 2020 r.

Ofiarska M., *Francja*, „Annales Universitatis Paedagogicae Cracoviensis. Studia Politologica" 2010, nr 4, s. 88–111.

Olech A., *International Military Involvement of the French Republic*, Warsaw 2021,

Olech A., *Walka z terroryzmem. Polskie rozwiązania a francuskie doświadczenia*, Warszawa 2021.

Plan d'action contre le terrorisme, Paris 2018.

Plan Vigipirate. Foire aux Questions, Paris 2016.

Rapport: Conference sur la lutte contre le terrorisme et la prevention de la radicalisation violente, Paris 2016.

Rekawek K. i in., *Who are the European jihadis? Project Midterm Report*, Bratislava 2018.

Skryabina E. i in., *UK healthcare staff experiences and perceptions of a mass casualty terrorist incident response: a mixed-methods study*, „Emergency Medicine Journal" 2021, t. 38, nr 10, s. 756–764.

Sulzer L., *Loi Renforçant La Securite Interieure Et La Lutte Contre Le Terrorisme. Analyse juridique critique – Mise en œuvre – Suivi du contentieux constitutionnel, 30 octobre 2017 – 29 octobre 2018*, H. Decoeur (red.), Paris 2018.

Thachuk K., Bowman M., Richardson C., *Homegrown Terrorism. The Threat Within*, Washington 2008.

Źródła internetowe

Así funcionan los protocolos sanitarios en caso de atentados en España, https://www.consalud.es/pacientes/asi-funcionan-los-protocolos-sanitarios-en-caso--de-atentados-en-espana_22428_102.html?fbclid=IwAR0fqXimun7oK2vbK7UCiFddJqSYfGbLRc0BKRHQ2ec_ZRuTF8Uw4LQZ41w [dostęp: 21 XI 2021].

Association 13 novembre: fraternité et vérité, http://13onze15.org/ [dostęp: 8 XI 2021].

Association française des Victimes du Terrorisme, https://www.afvt.org/ [dostęp: 8 XI 2021].

Association IMAD pour la jeunesse et la paix, https://association-imad.fr/en/association-for-youth-and-peace/ [dostęp: 8 XI 2021].

Association Montjoye, https://montjoye.org/ [dostęp: 8 XI 2021].

Attentats: „L'opération Sentinelle coûte 1 million d'euros par jour", http://www.leparisien.fr/faits-divers/le-drian-l-operation-sentinelle-coute-1-million-d-euros-par-jour-08-02-2015-4515903.php [dostęp: 4 XI 2021].

Bachner M., *Hundreds of thousands more Israelis okayed to carry guns under new rules,* https://www.timesofisrael.com/hundreds-of-thousands-more-israelis--okayed-to-carry-guns-under-new-rules [dostęp: 13 XI 2021].

Blondelle K., *Attaque de policiers à Cannes: pas de saisie du parquet national antiterroriste,* francebleu.fr/infos/faits-divers-justice/cannes-pas-de-saisie--du-parquet-national-antiterroriste-apres-l-agression-de-policiers-au-couteau-1636728441 [dostęp: 23 XI 2021].

Comprendre le plan Vigipirate, https://www.gouvernement.fr/risques/comprendre-le-plan-vigipirate [dostęp: 4 XI 2021].

Cottineau C., *Justice antiterroriste post-sentencielle: la tentation de la résignation,* https://www.dalloz-actualite.fr/node/justice-antiterroriste-post-sentencielle-tentation-de-resignation#.YaPYadDMI2w [dostęp: 18 XI 2021].

Czy polscy ratownicy są przygotowani na udzielenie pomocy po ataku terrorystycznym?, https://www.infosecurity24.pl/czy-polscy-ratownicy-sa-przygotowani-na-udzielenie-pomocy-po-ataku-terrorystycznym?fbclid=IwAR2S8FsK2p2wHhVPrU99lvUJrf9LcLnZf6fmpOhORB1RhV14NT4s3u2eJeU [dostęp: 18 XI 2021].

Deux ans après: l'image de la Défense améliorée par la présence des militaires en rue, https://www.rtbf.be/info/dossier/explosions-a-brussels-airport/detail_deux--ans-apres-l-image-de-la-defense-amelioree-par-la-presence-des-militaires--en-rue?id=9505164 [dostęp: 13 XI 2021].

E-learning „Znaj, wykrywaj i zgłaszaj zjawiska radykalizacji"¸ https://www.youtube.com/playlist?list=PL2VXuAZDO9kb6gI8u4GT0v-J8nrXitELO [dostęp: 22 XI 2021].

Faire Face Ensemble, https://vigipirate.gouv.fr [dostęp: 22 XI 2021].

Fédération nationale des victimes d'attentats et d'accidents collectifs, https://www.fenvac.com/ [dostęp: 8 XI 2021].

https://infosecurity24.pl/specjalna-komorka-wieziennictwa-z-prawem-do-inwigilacji [dostęp: 27 XI 2021].

https://learning.tpcoe.gov.pl/ [dostęp: 27 XI 2021].

https://www.reseau-canope.fr/prevenir-la-radicalisation/ressorts-et-etapes.html [dostęp: 22 XI 2021].

La France dénombre „648 détenus radicalisés" dans ses prisons, affirme Éric Dupond-Moretti, https://www.lci.fr/justice-faits-divers/terrorisme-islamisme-la--france-denombre-648-detenus-radicalises-dans-ses-prisons-affirme-eric-dupond-moretti-2195734.html [dostęp: 18 XI 2021].

Lagneau L., *Terrorisme: Engagée dans l'opération «Temperer», la British Army devra faire face à de nouveaux défis*, http://www.opex360.com/2017/05/24/terrorisme-engagee-dans-loperation-temperer-la-british-army-devra-faire-face-un-defi-nouveau [dostęp: 13 XI 2021].

Leclerc J., *L'inquiétante défaillance du suivi des terroristes sortant de prison*, https://www.lefigaro.fr/actualite-france/l-inquietante-defaillance-du-suivi-des--terroristes-sortant-de-prison-20201109 [dostęp: 28 XI 2021].

Le dispositif territorial de prévention de la radicalisation violente, https://www.cipdr.gouv.fr/wp-content/uploads/2019/06/Dispositif-territorial-de--pr%C3%A9vention-de-la-radicalisation-violente-1.pdf [dostęp: 22 XI 2021].

Le parquet national antiterroriste, une force de frappe judiciaire, https://france3-regions.francetvinfo.fr/paris-ile-de-france/le-parquet-national-antiterroriste--une-force-de-frappe-judiciaire-1881258.html [dostęp: 22 XI 2021].

Les services judiciaires anti-terroristes, https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/police-judiciaire-specialisee/services-judiciaires [dostęp: 24 XI 2021].

Les statuts du Fonds de Garantie des Victimes des actes de Terrorisme et d'autres Infractions (FGTI), https://www.fondsdegarantie.fr/fgti/statuts/ [dostęp: 18 XI 2021].

Lutte contre la radicalisation et le séparatisme islamiste: la ville agit pour votre sécurité!, https://www.vernon27.fr/actualites/lutte-contre-la-radicalisation-et-lesseparatisme-islamiste-la-ville-agit-pour-votre-securite [dostęp: 19 XI 2021].

Ministère de l'Intérieur, *Premier bilan de l'application de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme,* Communique de Presse, 12 II 2019.

Ministère de l'Intérieur – Alerte, https://twitter.com/Beauvau_Alerte [dostęp: 19 XI 2021].

Olech A., *Counterterrorism Strategies in Poland and France,* https://warsawinstitute.org/counterterrorism-strategies-poland-france [dostęp: 15 XI 2021].

Patard A., *Chiffres clés d'Internet et des réseaux sociaux en France en 2021,* https://www.blogdumoderateur.com/chiffres-internet-reseaux-sociaux-france-2021 [dostęp: 22 XI 2021].

Programme de suivi des individus radicalisés: „On n'a abolument pas à rougir de ce qu'on fait en France par rapport à ce qui est fait à l'étranger", www.ifri.org/fr/espace-media/lifri-medias/programme-de-suivi-individus-radicalises-na-absolument-rougir-de-quon [dostęp: 2 XI 2021].

Reconnaître les signes de la radicalisation violente, https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/lutte-contre-terrorisme/sinformer/reconnaitre-signes-de-la-radicalisation [dostęp: 22 XI 2021].

Renoir P., Azur F., *Cannes forme ses policiers municipaux à intervenir en cas d'attaque terroriste,* https://www.francebleu.fr/infos/faits-divers-justice/cannes-forme-ses-policiers-a-intervenir-en-cas-d-attaque-terroriste-1574963396 [dostęp: 10 XI 2021].

Rome déploie 4 800 soldats autour de sites sensibles, https://www.ouest-france.fr/europe/italie/antiterrorisme-rome-deploie-4-800-soldats-autour-de-sites-sensibles-3195080 [dostęp: 13 XI 2021].

Rubinich H., *Überlebende von Terroranschlägen. Der schwierige Weg aus dem Trauma,* https://www.deutschlandfunkkultur.de/ueberlebende-von-terroranschlaegen-der-schwierige-weg-aus-100.html [dostęp: 20 XI 2021].

Simulacro antiterrorista, https://www.diariodesevilla.es/vivirensevilla/Simulacro-antiterrorista_0_1131787221.html [dostęp: 21 XI 2021].

Tarihi G., *Hastanemiz çalışanlarına Adıyaman Emniyet Müdürlüğü Terörle Mücadele Daire Başkanlığı Büro Amirliği tarafından „Terörle Mücadele" eğitimi verildi,* https://besnidh.saglik.gov.tr/TR,36418/hastanemiz-calisanlarina-adiyaman--emniyet-mudurlugu-terorle-mucadele-daire-baskanligi--buro-amirligi-tarafindan-terorle-mucadele-egitimi-verildi.html [dostęp: 21 XI 2021].

Wicky L., *Le plan Vigipirate et ses trois niveaux d'alerte,* https://www.lemonde.fr/les-decodeurs/article/2016/12/20/en-france-le-plan-vigipirate-et-ses-trois--niveaux-d-alerte_5052094_4355770.html [dostęp: 4 XI 2021].

Zoom sur le nouveau Parquet national antiterroriste, http://www.justice.gouv.fr/justice-penale-11330/zoom-sur-le-nouveau-parquet-national-antiterroriste-32661.html [dostęp: 10 XI 2021].

Akty prawne

Arrêté du 29 mai 2019 portant création et organisation d'un service à compétence nationale dénommé „Service national du renseignement pénitentiaire", NOR: JUST1911857A, JORF n° 0125 du 30 mai 2019.

Code de la sécurité intérieure.

Code de l'organisation judiciaire.

Code de procédure pénale.

Code des assurances, Version en vigueur au 17 novembre 2021.

Comité interministériel de prévention de la délinquance et de la radicalisation, „Prévenir Pour Protéger", *Plan national de prévention de la radicalisation, Communiqué du Premier ministre,* vendredi 23 février 2018.

Décision n° 2017-624 QPC, 16 mars 2017.

Déclaration de M. Manuel Valls, Premier ministre, en réponse à diverses questions portant sur la lutte contre le terrorisme depuis 2012, l'attentat de Nice, la prorogation de l'état d'urgence et les opérations extérieures menées par la France contre Daech, à l'Assemblée nationale le 20 juillet 2016.

Décret n° 2014-474 du 12 mai de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement 2014 pris pour l'application des assemblées parlementaires et portant désignation des services spécialisés de renseignement.

Décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement, NOR: SSAP1811219D, JORF n°0117 du 24 mai 2018.

Décret n° 2019-628 du 24 juin 2019 portant entrée en vigueur des dispositions relatives au parquet antiterroriste, JORF n°0145 du 25 juin 2019 texte n° 4, NOR: JUSD1917754D.

Décret n° 2020-867 du 15 juillet 2020 modifiant le décret n° 2002-1392 du 28 novembre 2002 instituant une mission interministérielle de vigilance et de lutte contre les dérives sectaires, NOR: INTX2004492D, JORF n° 0173 du 16 juillet 2020.

L'ancrage territorial de la sécurité intérieure – Rapport final, n° 323 (2020––2021), Date de remise: 29 janvier 2021.

Loi n° 2017-1510 du 30 octobre 2017 renforçant la securite interieure et la lutte contre le terrorisme, JORF n°0255 du 31 octobre 2017 texte n° 1.

LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, NOR: JUST1806695L, JORF n°0071 du 24 mars 2019.

Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.

Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le contrôle et le suivi de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Rapport d'information n° 348 (2019–2020) de M. Marc-Philippe Daubresse, fait au nom de la commission des lois, déposé le 26 février 2020.

DOI: 10.4467/27204383TER.22.006.15422

ORCID: 0000-0003-4649-589X

ANNA ROŻEJ

Rola i znaczenie informacji pochodzących ze źródeł otwartych w zwiększaniu podatności na zagrożenia bezpieczeństwa w cyberprzestrzeni, ze szczególnym uwzględnieniem cyberterroryzmu

Abstrakt

Celem artykułu jest przedstawienie, jak w ostatnich latach wzrosły rola i znaczenie informacji pochodzących ze źródeł otwartych w sytuacji przeniesienia znacznej części funkcjonowania społeczeństw do świata Internetu. Niestety, wraz z tym trendem pojawiły się także nowe zagrożenia, w tym o charakterze cyberterrorystycznym, które wymagają podjęcia natychmiastowych działań, aby móc ograniczyć ich oddziaływanie na bezpieczeństwo informacyjne.

Słowa kluczowe:

bezpieczeństwo informacyjne, źródła otwarte, infosfera, zagrożenia, walka informacyjna, infrastruktura krytyczna

W ciągu ostatnich kilkunastu lat dynamicznie zmieniające się otoczenie funkcjonowania człowieka sprawiło, że zaszły radykalne zmiany niemal w każdym środowisku, w tym w środowisku bezpieczeństwa. Pamiętne ataki na World Trade Center w Nowym Jorku oraz Pentagon w Waszyngtonie, od których minęło już ponad 20 lat, należy uznać za wyznacznik zmian w postrzeganiu bezpieczeństwa w skali globalnej. Bezpośrednio po zamachach większość państw należących do NATO, w tym Polska, została zmuszona do wprowadzenia w życie elementów narodowych systemów gotowości obronnej. Tragedia ta stała się też źródłem głębokiej refleksji społeczności międzynarodowej, obejmującej zarówno przyczyny, jak i konsekwencje tego wydarzenia, któremu, mając na uwadze stosunki międzynarodowe, można przypisać charakter przełomowy. Zamachy na World Trade Center i Pentagon były przyczyną gruntownego przeorientowania wszystkich systemów narodowych krajów zachodnich, zwłaszcza pod kątem współpracy z innymi państwami oraz organizacjami międzynarodowymi, w tym również w ramach NATO. Można stwierdzić, że był to pewnego rodzaju przełom od czasów zimnej wojny. Dopiero zamachy z 2001 r. sprawiły, że dostrzeżono potrzebę reformy systemów bezpieczeństwa narodowego, które tkwiły rozwiązaniami w XX w. i były nieprzystosowane do wyzwań świata postmilenijnego.

Zamach na symbole amerykańskiej potęgi w sposób jednoznaczny udowodnił, że „(...) dzisiejsze zagrożenia posiadają inną naturę i skalę niż dotychczas, a współczesna odpowiedź na te zagrożenia jest nieadekwatna. Broń projektowana w celu przeciwstawienia się zagrożeniom w końcu ostatniego tysiąclecia nie będzie w stanie sprostać im w pierwszych dekadach XXI wieku. Nowe, często o asymetrycznym charakterze, zagrożenia dla bezpieczeństwa globalnego wymagają nowego myślenia”[1].

Jednocześnie także legalne organizacje działające w skali ponadpaństwowej zyskują na sile i wpływach, dysponując technicznymi możliwościami dostosowania się do nowego środowiska bezpieczeństwa. Spekulanci giełdowi, handlowcy, korporacje międzynarodowe, firmy świadczące usługi internetowe mają obecnie możliwości znaczącego globalnego wpływu na życie codzienne obywateli wielu państw. Globalizacja oraz rewolucja w technologii informatycznej dały tym instytucjom przewagę. Ich kontrola jest sprawowana bardziej za pośrednictwem

[1] R. Hall, C. Fox, *Ponownie przemyśleć bezpieczeństwo*, „Przegląd NATO” zima 2001/2002, s. 8.

rynków finansowych niż przez struktury globalne, a zakłócenia powstają według takiej samej zasady. Dlatego też nie powinno dziwić, że tradycyjne mechanizmy państwa oparte na idei granic, porządku, władzy, policji, struktur siłowych są zagrożone. Wydają się one także ze swojej natury niezdolne do przeciwstawienia się współczesnym wyzwaniom dla bezpieczeństwa. W miarę jak owa niezdolność staje się coraz bardziej widoczna, narasta rozczarowanie poprzednim systemem i może powstać przekonanie, że wszystko w dziedzinie bezpieczeństwa zmierza ku gorszemu, na co oczywiście nie można pozwolić.

Najczęściej bardzo trudno jest zidentyfikować przywódcę lub region, na których można by skoncentrować zainteresowanie w celu przeciwstawienia się zagrożeniom. Co więcej, skala tych zagrożeń jest tak duża, że staje się to niebezpieczne dla wielu krajów. Zagrożenia te nie znają bowiem granic państwowych i kontynentalnych. Istnieje też zasadnicza trudność we właściwej identyfikacji zjawisk (organizacji, przywódców) w celu podjęcia skutecznego im przeciwdziałania. Zagrożenia te mogą podważać istotę i podwaliny funkcjonowania instytucji narodowych i międzynarodowych, a także zniszczyć gospodarki wielu państw.

Konieczność nowego podejścia do bezpieczeństwa była nagląca, gdyż terroryzm jest tylko jednym z wielu nietradycyjnych wyzwań dla bezpieczeństwa. Stanowią je też: konflikty etniczne i religijne, przemyt narkotyków, masowe migracje, regionalna niestabilność, pranie brudnych pieniędzy, działania różnych grup ekstremistycznych, kradzież informacji, a także sama dezinformacja. Tymczasem pojawiła się właśnie cybersfera, która osiągnęła ogromny dynamizm rozwoju, sprawiając, że wybrane mocarstwa dostrzegły potrzebę zreformowania systemów obronnych. W związku z tym zaczęły powstawać m.in. odrębne rodzaje wojsk – wojska cybernetyczne. Cybersfera wpłynęła na przeorientowanie akcentów w bezpieczeństwie ze zwalczania fizycznego na podejmowanie reakcji i rozwój zasobów do realizacji kontrataków na cyberataki, a także prowadzenie działań wyprzedzających w cyberprzestrzeni.

Uwzględniając rozpatrywaną problematykę, przyjęto, że przedmiotem badań przeprowadzonych w ramach niniejszego artykułu będą informacje pochodzące ze źródeł otwartych przeanalizowane w kontekście potencjalnych zagrożeń. Przedstawiony przedmiot badań jest wyznacznikiem celów procesu badawczego, które są postrzegane w ujęciu teoretycznym oraz praktycznym. Cel teoretyczny ma polegać na rozwinięciu oraz uzupełnieniu treści odnoszących się zarówno do teorii,

jak i praktyki cyberbezpieczeństwa w szczególnym przypadku, jakim jest korzystanie z internetowych źródeł otwartych. Osiągnięcie celu teoretycznego ma przyczynić się do realizacji celu praktycznego, jakim będą użyteczne rozwiązania w zakresie zapewnienia oraz utrzymania bezpieczeństwa informacyjnego. Zaprezentowana sytuacja problemowa, przedmiot badań i ich cel wyraźnie określają główny problem badawczy, który sprowadza się do odpowiedzi na następujące pytanie: czy globalne upublicznienie i ogólna dostępność dla wszystkich użytkowników Internetu w tym samym czasie informacji pochodzących ze źródeł otwartych, a dotyczących bezpieczeństwa państwa wpłynęły na zwiększenie ich podatności na ataki o charakterze cybernetycznym? Rozwiązanie problemu badawczego będzie uwarunkowane rozwiązaniem problemów szczegółowych, sprowadzających się do odpowiedzi na następujące pytania:

1. Jakie zmiany nastąpiły w środowisku bezpieczeństwa?
2. Jak zmieniło się nastawienie do Internetu w ciągu ostatnich kilku lat?
3. Jaka jest istota źródeł otwartych i na czym polega ich specyfika?
4. Jakie są potencjalne zagrożenia wynikające z korzystania z informacji pochodzących ze źródeł otwartych?
5. Jakie działania prewencyjne są możliwe, aby zapobiec zagrożeniom bezpieczeństwa informacyjnego?

Wstępne wnioski z obserwacji oraz analizy dostępnych dokumentów i literatury przedmiotu, a także określony cel badań i problemy badawcze zdeterminowały założoną hipotezę roboczą, dzięki której będzie możliwe przeprowadzenie procesu badawczego: rozwój Internetu oraz zwiększenie zainteresowania źródłami otwartymi są związane ze wzrostem zagrożeń o charakterze cyberterrorystycznym.

Jak mawiał Henry Kissinger – wybitny amerykański polityk i dyplomata, doradca do spraw bezpieczeństwa narodowego prezydenta Richarda Nixona: „Bezpieczeństwo jest fundamentem wszystkiego, co czynimy”[2], i trudno się z tak postawioną tezą nie zgodzić. Jednak w dobie ogromnego rozwoju technologicznego, dostępu do zaawansowanych procesów oraz urządzeń może się wydawać, że troska o bezpieczeństwo schodzi na dalszy plan. Istotne są posiadane narzędzia, możliwości, a nie jedna z najważniejszych wartości, czyli bezpieczeństwo. W związku

[2] H. Kissinger, *Dyplomacja*, Warszawa 2016, s. 23.

z przeniesieniem niemal każdego aspektu życia do świata Internetu jesteśmy narażeni na wiele zagrożeń o charakterze cybernetycznym, a poziom poczucia bezpieczeństwa, zwłaszcza bezpieczeństwa teleinformatycznego, znacznie się obniżył. Istnieje ogromne ryzyko, że zgromadzone przez nas dane, przetwarzane informacje staną się obiektem zainteresowania ze strony cyberprzestępców.

Jeden z pierwszych teoretyków sztuki wojennej, żyjący 25 wieków temu w Chinach Sun Tzu, w swoim traktacie *Sztuka wojny* stwierdza, że „(...) najwyższą umiejętnością w sztuce wojennej jest podporządkowanie sobie nieprzyjaciela bez walki"[3]. Podaje jednocześnie wiele wskazówek, jak ów pożądany stan osiągnąć. Dążąc do uzyskania powodzenia w wojnie, należy m.in. dyskredytować wszystko, co dobre w kraju przeciwnika, wciągać przedstawicieli warstw rządzących przeciwnika w przestępcze przedsięwzięcia, podrywać ich dobre imię i w odpowiednim momencie rzucić ich na pastwę pogardy rodaków. Zasadne jest też dezorganizowanie działalności rządu przeciwnika oraz wywoływanie waśni i niezgody między obywatelami wrogiego kraju. Należy także zwrócić uwagę na indyjski traktat *Arthaśastra* autorstwa Ćanakji Kautilji. Ten indyjski filozof oraz teoretyk wojny poza przypisaniem dużej roli w polityce zagranicznej szpiegom i zdrajcom wprowadził regułę prowadzenia wojny, zgodnie z którą jej rozpoczęcie ma być dopuszczalne jedynie w sytuacji, gdy z analizy porównawczej obu stron wynika pewność zwycięstwa. Gwarantami sukcesu są takie czynniki, jak: mądrość, plan, silna i dobrze wyszkolona armia, wysokie morale oraz ogólny potencjał. Kautilja zaznaczył również, że podbitą ludność należy traktować łagodnie, aby móc nad nią trwale panować.

W środowisku bezpieczeństwa informacyjnego podłoża zmian należy się dopatrywać zwłaszcza w rewolucji informacyjnej, która wprowadziła do obiegu różne technologie pozwalające na pozyskiwanie oraz dystrybucję informacji na masową skalę. To zjawisko miało przełomowy charakter, z uwagi na globalną skalę oddziaływania tych technologii. Powyższe konsekwencje rewolucji informacyjnej powodujące ogrom zmian sprawiły, że infosfera rozumiana jako synonim przestrzeni informacyjnej i środowiska informacyjnego stała się przedmiotem nauk o bezpieczeństwie[4]. W środowisku naukowym infosfera jest rozumiana

[3] Sun Tzu, *Sztuka wojny*, Gliwice 2004, s. 57.

[4] B. Sosińska-Kalata, *Obszary badań współczesnej informatologii (nauki o informacji)*, „Zagadnienia Informacji Naukowej" 2013, nr 2, s. 9–41.

jako całość zasobów informacyjnych, do których dany podmiot ma dostęp. Analiza społeczeństwa informacyjnego w aspekcie systemu cybernetycznego wskazuje zaś, że infosfera dzieli się na warstwę lokalną, która odpowiada lokalnym zasobom informacyjnym powstającym wraz z rozwojem lokalnej społeczności, oraz warstwę globalną złożoną z zasobów globalnych, będącą czymś znacznie większym niż sumą informacyjną zasobów lokalnych[5]. Początków społeczeństwa informacyjnego upatruje się w latach 60. i 70. XX w. Powstało ono w wyniku rewolucji przemysłowej, podczas której wprowadzono do użytku komputer oraz nastąpił rozwój informatyzacji[6]. Po raz pierwszy pojęcia „społeczeństwo informacyjne" (jap. *johoka shakai*) użył Japończyk Tadao Umesao, określając w ten sposób społeczeństwo, które zaczęło używać komputera do komunikacji w epoce rozwoju techniki cyfrowej i mikroelektroniki. Pojęcie to następnie zostało rozwinięte przez Daniela Bella, który uważał, że dla ówczesnego społeczeństwa zasobami strategicznymi były wiedza oraz informacja, a nie – jak do tej pory – praca i kapitał[7].

W ostatnich latach infosfera, poza tym, że jej permanentną cechą stał się globalizm, zyskała ogromnie na znaczeniu poprzez objęcie znacznie większej ilości dostępnych informacji o charakterze powszechnym niż jeszcze kilka lat temu. Wyzwaniem stały się nie tylko masowość i nadmiar informacji, ale przede wszystkim ich cechy, takie jak niewiarygodność, irrelewantność oraz nieprawdziwość. Mnogość kanałów oraz źródeł informacyjnych sprawia, że wskazane cechy obecnie się nasilają.

Ponadto rewolucja informacyjna oraz towarzyszące jej rozwijająca się intensywnie technologia, dynamika życia, a także w ostatnim czasie pandemia wywołana wirusem SARS-CoV-2 sprawiły, że niemal całość życia codziennego została przeniesiona do świata Internetu, co z jednej strony daje ogromne możliwości, z drugiej jednak generuje wiele zagrożeń bezpieczeństwa w skali krajowej i międzynarodowej. „Gdy tylko nowe techniki informacyjne rozprzestrzeniły się i zostały przejęte przez różne kraje, różne kultury, różnorodne organizacje i rozmaite cele, nastąpiła eksplozja różnego rodzaju zachowań i użytków, co zwrotnie

[5] P. Sienkiewicz, *Społeczeństwo informacyjne jako system cybernetyczny*, w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?*, t. 1, L.H. Haber (red.), Kraków 2004, s. 79.

[6] J.S. Nowak, *Społeczeństwo informacyjne – geneza i definicje*, w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, P. Sienkiewicz, J.S. Nowak (red.), Katowice 2008, s. 25.

[7] http://www.bbc.uw.edu.pl/Content/20/08.pdf [dostęp: 25 XI 2021].

przyczyniło się do powstania technologicznych innowacji, przyspieszając tempo i rozszerzając zasięg technologicznej zmiany, a także różnicując jej źródła"[8]. Przytoczone stwierdzenie hiszpańskiego socjologa Manuela Castellsa świadczy o tym, że współczesne społeczeństwo jest rzeczywiście społeczeństwem informacyjnym, które zostało prawie całkowicie zdominowane przez systemy telekomunikacyjne służące do przesyłania, odbierania oraz przetwarzania informacji. Informacja jest aktualnie nieodłącznym elementem życia społecznego, gospodarczego, a także jest obecna w każdym obszarze funkcjonowania człowieka.

Należy zauważyć, że przejawy życia społecznego są najintensywniejsze w dużych przestrzeniach, takich jak na przykład ośrodki miejskie, lotniska czy szlaki komunikacyjne. Współczesne społeczeństwa udowadniają, że miejsca te wcale nie muszą realnie istnieć. Wystarczy, że stanowią one jedynie infrastrukturę czy platformę komunikacyjną, która stwarza warunki, aby organizacje czy różnego rodzaju inne podmioty mogły się ze sobą łączyć w czasie rzeczywistym[9]. Zmiany w społeczeństwie w czasach rewolucji informacyjnej dostrzegał też teoretyk komunikacji Marshall McLuhan. Uważał on, że dzięki bliskim relacjom typu online świat przybiera charakter globalnej wioski, w której ludzie mają możliwość łączenia się i komunikowania w czasie rzeczywistym. Niedługo trzeba było czekać, a nastała era komputerów osobistych, Internetu, smartfonów, bez których już nikt dzisiaj nie wyobraża sobie funkcjonowania. Dzięki powstałym rozwiązaniom technologicznym istnieje możliwość komunikowania się z dowolnymi osobami niezależnie od miejsca pobytu.

Ogromny dynamizm procesów, jakie zaszły w ciągu ostatnich kilkudziesięciu lat, sprawił, że obecnie największym zbiorem informacji jest właśnie Internet, na który składa się część jawna – powszechnie dostępna, oraz ciemna – tzw. Darknet, do którego dostęp jest nieco ograniczony, jednak przy użyciu odpowiednich technologii również możliwy.

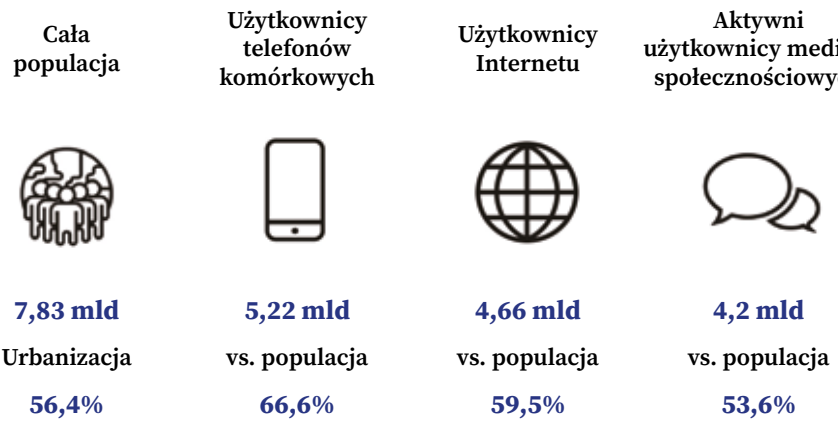
O tym, jak pożądanym źródłem informacji jest Internet, mogą świadczyć dane z raportu opublikowanego w 2018 r. przez ITU (ang. International Telecommunication Union)[10]. Otóż już wówczas ponad

[8] A. Elliott, *M. Castells: Społeczeństwo sieci*, w: A. Elliott, *Współczesna teoria społeczna. Wprowadzenie*, Warszawa 2011, s. 23–24.

[9] Tamże, s. 311–319.

[10] *Measuring the Information Society Report*, t. 1, Geneva 2018.

połowaświatowej populacji miała dostęp do Internetu. Pod koniec 2018 r. korzystało z niego prawie 51,2 proc., czyli 3,9 mld ludzi. Stanowiło to istotny krok w kierunku jeszcze większego rozwoju globalnego społeczeństwa informacyjnego. Szacowano, że w krajach rozwiniętych 4 osoby na 5 miały bezpośredni i nieograniczony dostęp do sieci. W krajach rozwijających się dostęp do Internetu miało ok. 45 proc. społeczeństwa, a w krajach najsłabiej rozwiniętych jedynie 20 proc. Jednak, zgodnie z przewidywaniami ITU, nieustannie obserwuje się tendencję wzrostową w dostępie do sieci. Potwierdzają to dane podane w Global Digital Report[11] dotyczące stanu cyfryzacji społeczeństwa w styczniu 2021 r., które przedstawia rysunek 1.



Rys. 1. Stan cyfryzacji na świecie w styczniu 2021 r.

Źródło: DataReportal, DataReportal – Global Digital Insights.

Charakteryzując dane przedstawione na rysunku 1, należy stwierdzić, że:

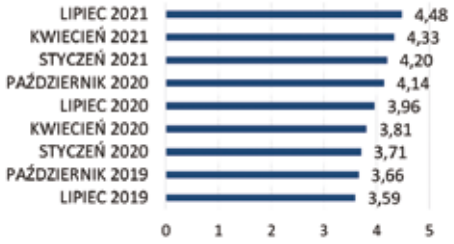
- **Ludność:** liczba ludności na świecie wynosiła 7,83 mld.
- **Telefonia komórkowa:** z telefonu komórkowego korzystało 5,22 mld ludzi, co stanowiło 66,6 proc. populacji na świecie. Liczba użytkowników mobilnych zwiększyła się od stycznia 2020 r. o 1,8 proc. Całkowita liczba połączeń mobilnych wzrosła o 72 mln, osiągając na początku 2021 r. poziom 8,02 mld.

[11] https://datareportal.com/reports/digital-2021-global-overview-report [dostęp: 26 XI 2021].

- **Internet:** z Internetu korzystało 4,66 mld ludzi na świecie , co stanowiło 59,5 proc. światowej populacji. Daje to wzrost o 316 mln w ciągu roku.
- **Media społecznościowe:** na świecie było 4,2 mld użytkowników mediów społecznościowych. Liczba ta wzrosła o 490 mln od stycznia 2020 r. Liczba użytkowników mediów społecznościowych stanowiła ponad 53 proc. światowej populacji.

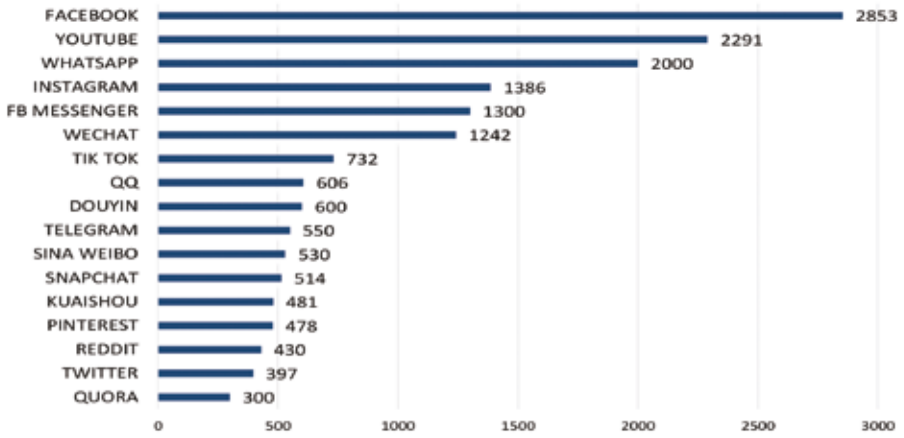
Ponadto o tym, że Internet jest jednym z najbardziej powszechnych źródeł danych, świadczą również poniższe fakty:

1. Liczba użytkowników mediów społecznościowych nieustannie wzrasta. W lipcu 2021 r. wynosiła ok. 4,48 mld (rysunek 2).
2. Platformy należące do rodziny Facebooka (Facebook, WhatsApp, Instagram, Messenger) cieszą się olbrzymim zainteresowaniem (rysunek 3).
3. Wydłuża się czas korzystania z Internetu (rysunek 4).
4. Wydłuża się czas korzystania z mediów społecznościowych (rysunek 5).



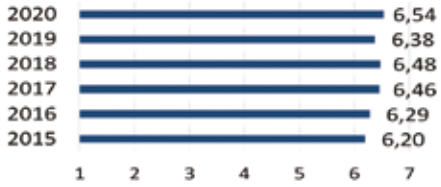
Rys. 2. Wzrost liczby użytkowników (w miliardach) mediów społecznościowych na świecie w latach 2019–2021.

Źródło: DataReportal, DataReportal – Global Digital Insights.



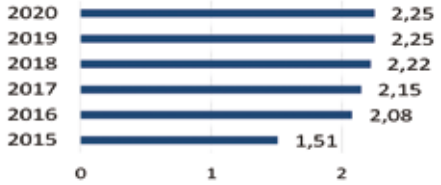
Rys. 3. Liczba użytkowników (w milionach) najpopularniejszych portali społecznościowych na świecie (dane z lipca 2021 r.).

Źródło: DataReportal, DataReportal – Global Digital Insights.



Rys. 4. Wzrost w latach 2015–2020 dziennego czasu (w godzinach) przeznaczanego na korzystanie z Internetu przez użytkowników w wieku 16–64 lat.

Źródło: DataReportal, DataReportal – Global Digital Insights.



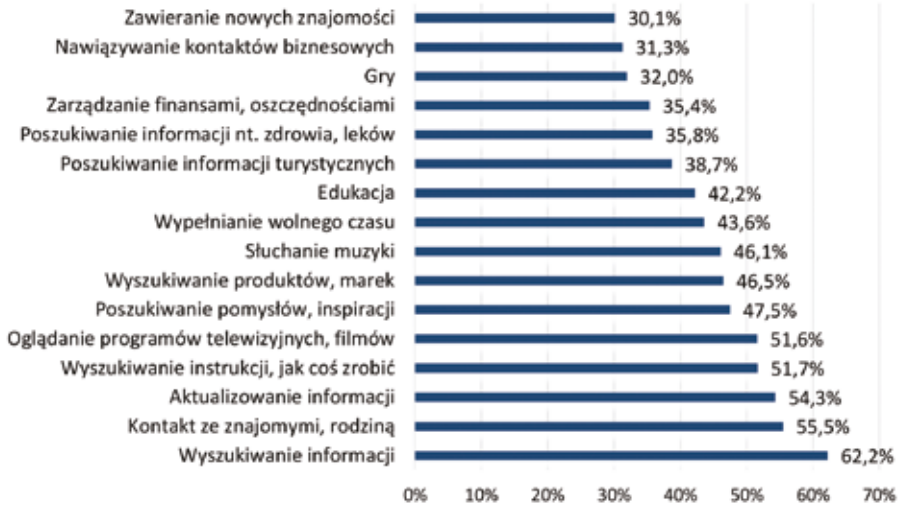
Rys. 5. Wzrost w latach 2015–2020 dziennego czasu (w godzinach) przeznaczanego na korzystanie z mediów społecznościowych przez użytkowników w wieku 16–64 lat.

Źródło: DataReportal, DataReportal – Global Digital Insights.

Do najpopularniejszych powodów, dla których ludzie korzystają z Internetu, zalicza się:

- poszukiwanie informacji;
- chęć bycia w kontakcie ze znajomymi i rodziną;
- chęć posiadania aktualnych danych i informacji;
- poszukiwanie wskazówek co do wykonania określonych czynności;
- oglądanie filmów, telewizji.

Szczegółowe dane zostały przedstawione na rysunku 6.



Rys. 6. Główne powody skłaniające użytkowników w wieku 16–64 lat do korzystania z Internetu.

Źródło: DataReportal, DataReportal – Global Digital Insights.

Na podstawie przedstawionych powyżej danych wskazujących na ogromną aktywność społeczeństwa globalnego w Internecie oraz nieustanny jej wzrost należy stwierdzić, że wspomniana sieć jest największym zbiorem informacji, często o charakterze strategicznym. Nic więc dziwnego, że informacja stała się najważniejszym zasobem decydującym o funkcjonowaniu i powodzeniu niemal każdej organizacji czy przedsiębiorstwa. Jest to zasób, który stanowi podstawę działalności, zapewnia przewagę konkurencyjną, a także daje poczucie

bezpieczeństwa. Powszechność informacji oraz ich niemal nieograniczona dostępność wynikają m.in. stąd, że często ich źródłem pochodzenia są źródła otwarte. Naukowcy oraz eksperci z obszaru działań wywiadowczych definiują źródła otwarte (ang. *open source*) jako podmiot bądź przedmiot cechujący się walorami, które umożliwiają generowanie informacji pozwalającej na ich legalne przetwarzanie, w tym utrwalanie, przesyłanie czy gromadzenie[12]. Informacje pochodzące ze źródeł otwartych mają charakter pierwotny bądź wtórny, co może generować również pewne ograniczenia. Otóż informacja, która pochodzi ze źródła pierwotnego, może mieć ograniczenia związane z możliwościami jej rozpowszechniania, jeśli na przykład będzie informacją niejawną bądź prywatną. Jeżeli jednak informacja pozyskiwana jest ze źródeł wtórnych – ogólnodostępnych, jej jawność nie jest już problemem[13]. Należy zauważyć, że pomimo iż informacje pochodzące ze źródeł otwartych są dostępne, to odbiorca rzadko ma pełną wiedzę o ich źródłach oraz właściwościach. W innej definicji zwraca się uwagę, że źródła otwarte to ogół pisemnych, audiowizualnych bądź informatycznych środków rozpowszechniania informacji[14]. Otwarte źródła informacji można klasyfikować na kilka sposobów, biorąc pod uwagę związek, jaki zachodzi między wagą informacji a wartością źródła. W praktyce jednak najczęściej uwzględniany jest rodzaj medium przekazu informacji, co może wynikać stąd, że media różnią się między sobą jakością, a tytuły są publikowane w różny sposób. Na przykład w Internecie użytkownik może znaleźć informacje, które ukazały się w telewizji bądź w prasie, i odwrotnie. Informacje te mogą występować w artykułach o różnych tytułach.

Rozwój technologiczny, a także wzrost dostępu do Internetu sprawiły, że ewoluowały także otwarte źródła informacji. Przykłady takich źródeł zostały przedstawione w tabeli.

[12] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 22–23.

[13] Ch. West, *Competitive intelligence,* New York 2001, s. 50.

[14] J. Oleński, *Ekonomika informacji*, Warszawa 2001, s. 49.

Tabela. Przykłady otwartych źródeł informacji.

ŹRÓDŁA OTWARTE			
Domeny (np. rejestry, listy, WHOIS)	Mapy (np. Wojewódzkie Systemy Informacji Przestrzennej)	Osoby (np. nazwiska – nazwiska-polskie.pl, Biuletyn Informacji Publicznej)	Użytkownicy/loginy (np. Albicla, Allegro, Fotka)
Serwisy społecznościowe (np. Facebook, Albicla, Fotka)	Serwisy randkowe (np. Sympatia, eDarling)	Firmy/organizacje (np. CEIDG, eKRS, Rejestr.io)	Społeczeństwo (np. Bank Danych Lokalnych – GUS, Baza Demografia – GUS)
Biznes/gospodarka (np. Allegro, GPW)	Archiwa (np. Inwentarz Archiwalny IPN, Narodowe Archiwum Cyfrowe)	Tłumaczenia (np. Elektroniczny Słownik Języka Polskiego)	Rejestry publiczne (np. Bank Danych, Biuletyn Zamówień Publicznych)
Prawo (np. Dzienniki Urzędowe, Internetowy System Aktów Prawnych)	Uczelnie (np. POL-on, RAD-on)	Transport (np. CEPiK API, EPKT Spotters)	Dark web (Aktywne strony TOR)
Dokumenty (np. chomikuj.pl)	Wideo (np. Kamery.edu.pl)	Zdjęcia (np. Fotosik.pl)	Numery telefonów
Książki telefoniczne (np. Dostawca usług, Kto dzwonił)	SIGNIT (np. WebSDR)	OpSec (np. Generatory IT, GenApps)	Baza Wiedzy (np. blogi, kursy, prezentacje)

Źródło: Opracowanie własne.

Każde z powyższych źródeł możemy podzielić na poszczególne podkategorie, a elementem łączącym je wszystkie jest Internet. Do informacji wyszukiwanych w sieci należy jednak podchodzić z dużą ostrożnością i nie zapominać o innych źródłach – tych z kategorii drukowanych, takich jak chociażby książki, dzienniki czy czasopisma. Ponadto warto zauważyć, że Internet to nie tylko serwisy informacyjne, lecz także bardzo popularne portale społecznościowe, które zapewniają funkcjonowanie różnych środowisk tematycznych, grup zainteresowań, a także słowniki, encyklopedie, fora czy blogi. Wszystkie te źródła zawierają wiele różnych informacji. Ponadto źródła otwarte pozwalają dotrzeć do zdjęć prywatnych, zdjęć satelitarnych, a także danych geolokalizacyjnych. Pomimo że wskazane źródła cechują się przede wszystkim otwartością,

dostępnością oraz jawnością, to ostrożność nakazuje podchodzić do nich z racjonalnym dystansem oraz je weryfikować.

Warto mieć świadomość, że usługi przeszukiwania Internetu (ang. *search service*), czyli jedna z najpopularniejszych funkcjonalności użytkowania sieci, bazują na wykorzystaniu wyspecjalizowanych oprogramowań, które odpowiadają za eksplorację baz internetowych. Do najbardziej popularnych mechanizmów zalicza się:

- mechaniczne indeksowanie wyrazów i fraz – AltaVista/Yahoo, Google, HotBot;
- arbitralne katalogowanie dokumentów zgodnie z przyjętą klasyfikacją tematyczną – Yahoo;
- usługi przeszukujące dokumenty z grup dyskusyjnych – AltaVista Usenet;
- metasearch – narzędzie wykorzystujące pojedyncze wyszukiwarki – MetaCrawler, MetaFIND;
- wyszukiwanie korzystające ze specjalistycznych baz danych – Alphasearch;
- inne.

Pomimo istnienia tak specjalistycznej technologii przy przeglądaniu źródeł otwartych, w tym stron internetowych, należy za każdym razem ocenić je pod względem ich wiarygodności. W tym celu warto zadać sobie pięć podstawowych pytań: kto?, co?, gdzie?, kiedy?, dlaczego?

Chcąc znaleźć odpowiedź na pytanie: kto? – można dokonać analizy strony pod kątem wyszukiwania autorów, konkretnych nazwisk czy szczegółowych informacji. Dobrą praktyką jest też sprawdzenie typów domen – .com/.org/.gov/kod kraju, a także ocena, czy dany typ jest odpowiedni dla przedstawionych treści. Jeśli strona, z której są pobierane informacje, to strona osobista albo strona użytkownika portalu społecznościowego, należałoby zidentyfikować, kto jest odpowiedzialny za wprowadzenie danych treści, a także, jeśli jest taka możliwość, przeanalizować kod źródłowy strony, gdzie często jest zapisane nazwisko autora. W następnej kolejności, aby zweryfikować wiarygodność informacji, należałoby sprawdzić, do kogo należy serwer, na którym jest umieszczona dana strona, oraz czy zebrane informacje są ze sobą spójne. Dobrą metodą na sprawdzenie wiarygodności danych treści jest poszukiwanie opinii innych użytkowników, a także prześledzenie rozpowszechniania danej informacji, chociażby przez weryfikację liczby udostępnień.

Sprawdzając daną stronę, należy zwrócić uwagę na zawarte w niej treści, czyli spróbować odpowiedzieć na pytanie: co? Aby móc ocenić prawdziwość zamieszczonych treści, trzeba zweryfikować źródła, daty oraz czy treści nie są zmienione w odniesieniu na przykład do cytowanych źródeł. Bardzo istotną cechą informacji jest jej aktualność, czyli odpowiedź na pytanie: kiedy? W związku z tym powinno się sprawdzić, kiedy dana informacja została zamieszczona, kiedy była aktualizowana bądź jak często jest aktualizowana. Zebranie odpowiedzi na powyższe pytania pozwoli ocenić, czy informacje pochodzące ze źródeł otwartych są przede wszystkim prawdziwe, wiarygodne i aktualne.

Z danych statystycznych przedstawionych w pierwszej części artykułu wynika, że wobec rosnącej liczby populacji z dostępem do Internetu jest on narzędziem służącym do zamieszczania, poszukiwania oraz wymiany informacji. Co więcej, zasoby internetowe są w łatwy i szybki sposób uzupełniane przez użytkowników Internetu. W związku z tym każdy może być zarówno odbiorcą informacji, jak i ich autorem. Chcąc zidentyfikować atrybuty źródeł otwartych, należy wskazać:

- dostępność,
- niski koszt pozyskania,
- niepewną wiarygodność,
- brak zależności,
- niskie ryzyko,
- jawność.

Powyższe cechy poniekąd odpowiadają na pytania dotyczące liczby źródeł otwartych, a przede wszystkim liczby gromadzonych i przetwarzanych w nich informacji. Przykładem może być chociażby portal społecznościowy Facebook.com, który obecnie ma ok. 2,8 mld aktywnych użytkowników miesięcznie, a dziennie odwiedza go ok. 1,84 mld osób. Od początku 2021 r. liczba użytkowników Facebooka wzrosła o ok. 12 proc. Skala ta obrazuje, jak wiele informacji jednocześnie pojawia się na portalu.

Przedstawione dotychczas informacje wskazują, że zasięg oraz dostępność źródeł otwartych są ogromne. Obecnie ponad połowa ludności na całym świecie ma dostęp do Internetu za pomocą komputerów, smartfonów czy innych urządzeń. Rewolucja technologiczna, jaka nastąpiła w tym zakresie, bez wątpienia podniosła jakość życia, a przez to również kompetencje cyfrowe społeczności międzynarodowej. Trudno już wyobrazić sobie życie zawodowe czy prywatne bez dostępu do sieci. Gdy spojrzy się przez pryzmat rozwoju w obszarze gospodarczym

i społecznym, obecna sytuacja powinna być powodem jedynie do zadowolenia i dumy. Dostęp do tak wielu informacji to podstawa dalszego rozwoju, nowych możliwości oraz szans.

Niestety, rozwój cyberprzestrzeni, w której dochodzi do przetwarzania ogromnej ilości informacji, niesie za sobą także rozwój cyberterroryzmu. Tak jak cyberprzestrzeń pozbawiona jest wszelkich granic, podobnie terroryzm ma nieograniczony zasięg, co pozwala cyberprzestępcom podejmować i skutecznie przeprowadzać w sieci Internet działania o charakterze cyberterrorystycznym. Permanentną cechą cyberterroryzmu jest niewidoczność jego działania, a także poniekąd skutków, czego nie da się powiedzieć o terroryzmie w formie konwencjonalnej. Najczęściej użytkownik Internetu nie dostrzega cyberataku i nie zdaje sobie z niego sprawy. Atak ujawnia się w przypadku zablokowania na przykład systemów teleinformatycznych obiektów strategicznych odpowiadających chociażby za infrastrukturę krytyczną. Te zagrożenia są niestety bardzo słabo mierzalne albo wręcz niemierzalne. Problem polega również na tym, że cyberterrorysta jest to przeciwnik, wobec którego trudno zastosować jakiekolwiek konwencje międzynarodowe o działaniach zbrojnych państw, gdyż tak naprawdę nie wiadomo, kto jest przeciwnikiem. Potrzeba powstania legislacji w tym obszarze jest na pewno priorytetem każdego państwa, jak i organizacji międzynarodowych. Rozwój cyberprzestrzeni spowodował, że państwa straciły możliwość walki z tym niewidocznym przeciwnikiem, nie ma także podstaw prawnych, aby uruchomić współpracę międzynarodową w celu identyfikacji wroga i jego statusu.

Jeszcze zaledwie kilkanaście lat temu byliśmy jako społeczeństwo pod wielkim wrażeniem rozwoju teleinformatycznego i cyfryzacji wielu obszarów. Jednak nowe zagrożenia bezpieczeństwa XXI w., takie jak m.in. cyberprzestępczość, a także cyberterroryzm, doprowadziły do zweryfikowania takiego entuzjastycznego podejścia. Pod pojęciem „cyberprzestępczości" należy rozumieć każde nielegalne zachowanie realizowane za pomocą działań elektronicznych nakierowanych na bezpieczeństwo systemów komputerowych i danych w nich przetwarzanych. To także nielegalne działania podejmowane za pomocą lub względem systemu komputerowego czy sieci, w tym takie przestępstwa, jak nielegalne posiadanie, oferowanie lub rozpowszechnianie informacji za pomocą systemu komputerowego lub sieci. Do tego typu przestępstw można zaliczyć m.in. oszustwa, fałszerstwa, szpiegostwo przemysłowe, sabotaż i wymuszenia poprzez piractwo komputerowe i inne przestępstwa przeciwko własności

intelektualnej. Cyberterroryzm zaś obejmuje ataki na bezpieczeństwo publiczne, życie oraz walkę elektroniczną skierowaną przeciwko infrastrukturze krytycznej. Cyberterroryzm wykorzystuje nowe technologie informacyjne lub cyberprzestrzeń również do działań tradycyjnych[15].

Wcześniej cyberterroryzm bardziej był kojarzony z systemami bankowymi, kradzieżą tożsamości czy zawirusowaniem systemów komputerowych. Przykładem skali ówczesnego cyberterroryzmu mogą być wydarzenia, do jakich doszło w Estonii w 2007 r. Przy okazji próby przeniesienia pomnika tzw. Brązowego Żołnierza, który upamiętniał radzieckich wojskowych, rozegrała się zimna wojna o charakterze cybernetycznym. Wówczas to nie konflikty na ulicach były poważnym zagrożeniem, ale masowe ataki na rządowe oraz prywatne serwery. Spowodowały one powszechny paraliż poprzez blokady systemów bankowych, serwisów informacyjnych, stron rządowych. Skalę tych wydarzeń oddają słowa byłego prezydenta Estonii Toomasa Hendrika Ilvesa, który stwierdził, że: „W obecnych czasach nie potrzeba pocisków, żeby niszczyć infrastrukturę. Można to zrobić on-line". Społeczeństwo estońskie przekonało się wtedy, że Internet daje wiele możliwości, ale może też odebrać zdolność do prawidłowego funkcjonowania. Przeniesienie życia do świata Internetu powoduje, że cyberterroryzm nieustannie się rozwija i swoim zasięgiem obejmuje kolejne obszary działania. Według literatury przedmiotu „cyberterroryzm" „(...) to zjawisko o politycznie motywowanym ataku bądź też groźba ataku wycelowana w system informatyczny, określone dane. Cel ataku może być różny: od zniszczenia informacji po np. ich udostępnienie dla osiągnięcia wyznaczonych celów politycznych czy społecznych. Obecnie cyberterroryzm to nie tylko typowe ataki terrorystyczne w cyberprzestrzeni, współcześnie to działania również takie, jak propaganda, dezinformacja, szpiegostwo, inwigilacja w sieci, manipulacja informacją, nazywana miękkim cyberterroryzmem"[16].

Należy zauważyć, że w cyberprzestrzeni występują wszystkie negatywne zjawiska, z jakimi można spotkać się na co dzień w „prawdziwym życiu". Kradzież, oszustwo, manipulacja, szpiegostwo to przykłady zagrożeń, z jakimi można mieć do czynienia w cyberprzestrzeni. Przykładem może być również fizyczne zniszczenie serwerów, przyczyniające się do

[15] http://unicjin.org/documents/congr10/10e.pdf [dostęp: 27 XI 2021].

[16] M. Grzelak, *Szpiegostwo i inwigilacja w Internecie*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, s. 164–181.

powstania zakłóceń w pracy systemów. Podobny cel hakerzy mogą osiągnąć przez wprowadzenie złośliwego oprogramowania typu malware. Tym złośliwym oprogramowaniem może być wirus, koń trojański, ransomware, exploit, rootkit, keylogger czy backdoor. Wszystkie te przykłady malware'u są w stanie doprowadzić do blokady systemów teleinformatycznych i pozbawić użytkowników dostępu do informacji. Ich sposób działania jest przy tym utajniony, przez co są bardzo trudne, a w pewnych sytuacjach wręcz niemożliwe do wykrycia.

Warto zwrócić uwagę, że udostępniane często na masową skalę informacje, dane w źródłach otwartych zostają w cyberprzestrzeni już na zawsze, nie ma możliwości ich trwałego usunięcia. Dotyczy to również danych umieszczanych o nas samych na różnego rodzaju portalach społecznościowych, urzędów, które udostępniają dane publiczne, czy wszystkich innych organizacji. Ten zbiór danych jest później powszechnie dostępny, łatwy do pozyskania bez pozostawiania praktycznie żadnych śladów. To powoduje, że pozyskanie informacji do przeprowadzenia ataków może przestępcom zająć dosłownie chwilę. Ludzie poniekąd przyzwyczaili się już do bezrefleksyjnego zamieszczania informacji w Internecie, bez zastanowienia się, jaki ma to wpływ chociażby na ich prywatne bezpieczeństwo. Ponadto portale społecznościowe, ale także już witryny internetowe, przyzwyczaiły użytkowników sieci do wyrażania reakcji i swoich emocji pod zamieszczanymi postami bądź artykułami. Jednak niewiele osób sprawdza, czy polubiony przez nie post nie został później zamieniony w post nacechowany treściami negatywnymi, przestępczymi i czy nie jest wykorzystywany do popełnienia czynów zabronionych. Do takich scenariuszy są wykorzystywane np. akcje charytatywne przekonujące użytkownika, że za każdego „lajka" jest wpłacana określona kwota na leczenie danej osoby. W ten sposób dochodzi do masowych oszustw, a uzyskane pieniądze są przeznaczane na zupełnie inne cele.

Kolejnym zagrożeniem informacji jest ich przepływ generowany przez poszczególne portale społecznościowe czy narzędzia służące do pozyskiwania informacji ze źródeł otwartych. Dostępna dokumentacja niektórych portali wskazuje, że wysyłane żądania nie są kierowane do docelowych źródeł danych, a do serwerów pośredniczących. Bardzo często lokalizacje tych serwerów znajdują się na terenie Stanów Zjednoczonych, co ze względu na legislację może mieć negatywny wpływ na atrybut bezpieczeństwa informacji, jakim jest poufność. Ponadto wysyłanie żądań do serwerów pośredniczących budzi wątpliwości, czy

nie są one przypadkiem kierowane do niepożądanych lokalizacji. Ze względu na możliwość istnienia serwerów pośredniczących użytkownik nie ma żadnej pewności, czy zwracane wyniki nie są modyfikowane bądź częściowo odfiltrowywane. Przesyłanie informacji w postaci tekstowej stwarza też zagrożenie łatwego przejęcia ich w wyniku działań hakerskich. Jest to niebezpieczne zwłaszcza wtedy, gdy wyciek dotyczy informacji strategicznych bądź informacji przetwarzanych przez jednostki odpowiedzialne za zapewnienie bezpieczeństwa kraju[17].

Portale społecznościowe stały się jednym z podstawowych kanałów wymiany informacji. Często jesteśmy nawet zapewniani o komunikacji szyfrowej, inaczej zwanej bezpieczną. Należy jednak zwrócić uwagę, że nie jest to najbezpieczniejszy sposób wymiany informacji. Nie jest tajemnicą, że administracja serwisów internetowych, społecznościowych przegląda je i wykorzystuje w zależności od potrzeb. Przykładem może być portal Facebook, który wykorzystał dane ok. 87 mln użytkowników Cambridge Analytica. Działanie to polegało na przekazaniu zdjęć oraz prywatnych rozmów do działu, który zajmuje się analizą osobowości i strategiami wpływania na masowe zachowania ludności.

Niestety, ujawnienie prywatnych wiadomości nawet przez bliżej nam nieznaną administrację stron internetowych czy portali społecznościowych to nie jest optymistyczna perspektywa. Dodatkowym zagrożeniem pozostaje możliwość przekazywania informacji, wiadomości różnego rodzaju instytucjom, w tym także rządowym, bądź służbom zagranicznym.

Warto mieć świadomość, że w przypadku działań cyberprzestępców bądź co gorsza cyberterrorystów mogą oni mieć dostęp do poniższych danych:

- numerów telefonów;
- numerów kont bankowych;
- loginów i haseł do komputerów, kont bankowych, domen;
- informacji prywatnych;
- informacji o prawach własności przemysłowej i intelektualnej;
- wiedzy o planowanych projektach.

W najmniej szkodliwym przypadku pozyskane dane, pochodzące z prywatnych rozmów na platformach komunikacyjnych, informacji z portali społecznościowych czy różnych innych witryn internetowych,

[17] Przegląd dokumentacji przeprowadzony przez analityków Inseqr sp. z o.o.

są wykorzystywane do przygotowania, a następnie przedstawienia najrozmaitszych produktów w postaci reklam pojawiających się na przeglądanych stronach internetowych. Te działania mają na celu oczywiście pobudzenie zainteresowania użytkownika, a w konsekwencji nakłonienie go do zakupu. Mechanizmy sztucznej inteligencji pozwalają obecnie różnym asystentom internetowym na podsłuchiwanie naszych rozmów w celu np. dopasowania reklamy produktu mogącego nas zainteresować. Dlatego też warto zwracać uwagę na poufność prowadzonych rozmów oraz rozważyć zabezpieczenie smartfonów podczas ważnych spotkań. Przykładem produktu, który może zapewnić naszym rozmowom poufność, są dostępne już na rynku tzw. szumiki. Są to skrzynki akustyczne, które pełnią funkcję bezpiecznego depozytu urządzeń mogących przechwytywać lub przesyłać dźwięk. Rozwiązania takie bardzo często uniemożliwiają podsłuch za pomocą elektronicznych urządzeń zaopatrzonych w funkcję dyktafonu. Dodatkowo zapobiegają nasłuchowi, jaki może być prowadzony przez asystentów wbudowanych w systemy mobilne.

Poważnym zagrożeniem dla odbiorców informacji pochodzących ze źródeł otwartych jest dezinformacja, przede wszystkim ze względu na zakres jej oddziaływania. Kiedy pojawiają się terminy „dezinformacja", „fake news", ludzie zwykle myślą o postach w mediach społecznościowych z nieco fantastycznymi, nieprawdopodobnymi historiami. Jednak fałszywe wiadomości to o wiele więcej niż przesadzone tytuły artykułów w mediach społecznościowych. Dezinformacja może wydawać się nowym zjawiskiem, ale jedynymi nowościami są wykorzystywana platforma i środowisko, w którym jest ona rozprzestrzeniana. Tak naprawdę to zjawisko istnieje od wieków, a Internet jest tylko nowszym środkiem komunikacji, który może być wykorzystywany do rozpowszechniania kłamstw i dezinformacji.

Istotą dezinformacji jest taki sposób przekazania informacji – prawdziwej lub fałszywej, aby wprowadzić w błąd przeciwnika lub konkurenta i skłonić go do zachowania zgodnego z naszymi oczekiwaniami i korzystnego dla nas. Dezinformacja nie jest prostym kłamstwem, czyli przekazaniem fałszywej informacji, ale prawdziwym podstępem. Zazwyczaj akcja szerzenia dezinformacji polega na przekazywaniu wielu informacji, z których większość jest prawdziwa, a tylko jedna – kluczowa dla wywołania zakładanego efektu – jest informacją fałszywą. Zdarza się też, że akcja dezinformacyjna jest przeprowadzana na podstawie informacji

prawdziwych, lecz podanych w taki sposób, że konkurent uznaje je za fałszywe. Dodatkowo w celu zwiększenia skuteczności podczas stosowania dezinformacji wykorzystuje się kilka niezależnych od siebie źródeł i kanałów informacyjnych. Pomimo że, jak wspomniano już wcześniej, dezinformacja nie jest nowym zjawiskiem, to bez wątpienia jej znaczenie wzrosło wraz z pojawieniem się mediów masowych. Jak słusznie zauważył Tomasz Aleksandrowicz, nastąpiła weaponizacja informacji, co przyczyniło się do powstania broni masowej manipulacji[18]. Doskonałym przykładem użycia tej broni był wyciek poufnych informacji za pośrednictwem portalu WikiLeaks. Ten przypadek doskonale pokazuje, że zachowanie bezpieczeństwa danych w sieci to duże wyzwanie.

Analogicznie do trójkąta ognia, który zakłada, że niezbędne są trzy czynniki – tlen, paliwo i energia, aby doszło do rozprzestrzeniania się ognia w budynku, dezinformacja również wymaga trzech różnych elementów, aby odnieść sukces. Wspólnie tworzą one trójkąt fałszywych wiadomości, a brak chociaż jednego z nich spowoduje, że fałszywe wiadomości nie będą w stanie się rozprzestrzeniać i docierać do docelowych odbiorców.

Rys. 7. Trójkąt fałszywych wiadomości.

Źródło: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media [dostęp: 26 XI 2021].

Pierwszym elementem są narzędzia i usługi służące do manipulowania i rozpowszechniania wiadomości w odpowiednich sieciach społecznościowych. Na świecie jest dostępna szeroka gama narzędzi

[18] T.R. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*, Warszawa 2021, s. 32–49.

i usług, część z nich jest stosunkowo prosta (płatne polubienia/obserwatorzy itp.), inne są bardziej skomplikowane — niektóre usługi obiecują przekazanie ankiet online, kolejne zmuszają właścicieli witryn do usuwania historii.

Oczywiście aby te narzędzia były przydatne, muszą istnieć sieci społecznościowe jako platforma do szerzenia propagandy. Ponieważ ludzie spędzają w nich dużo czasu, aby uzyskać najnowsze informacje, nie można nie docenić ich znaczenia w rozpowszechnianiu fałszywych wiadomości. Istnieje jednak różnica między zwykłym publikowaniem propagandy a przekształcaniem jej w coś, co konsumuje docelowa publiczność. Badanie mediów społecznościowych stwarza również możliwość spojrzenia na relacje między botami a odbiorcami promocji w mediach społecznościowych, np. w serwisie Twitter, a dzięki temu daje wyobrażenie o zakresie i organizacji kampanii próbujących manipulować opinią publiczną.

Kampania propagandowa zawsze niesie ze sobą pytanie: dlaczego? Motywy, którymi kierują się osoby rozpowszechniające fake newsy, są różne. Czasami jest to po prostu chęć zdobycia pieniędzy poprzez reklamę, ale może chodzić również o cele kryminalne czy polityczne. Niezależnie od motywu, sukces każdej kampanii propagandowej ostatecznie mierzy się tym, jak bardzo wpływa ona na rzeczywisty świat.

Reasumując, o dezinformacji można mówić, gdy rozpowszechniane informacje:

- są całkowicie lub częściowo fałszywe, zmanipulowane lub wprowadzające w błąd;
- dotyczą kwestii ważnej z punktu widzenia interesu publicznego;
- mają wywołać niepewność lub wrogość, doprowadzić do polaryzacji społeczeństwa albo zakłócenia procesów demokratycznych;
- są rozpowszechniane lub wzmacniane za pomocą zautomatyzowanych i agresywnych technik, takich jak boty społeczne, sztuczna inteligencja (ang. *artificial intelligence*, AI), mikrotargeting lub trollowanie.

Dezinformacja może destabilizować sytuację w państwie, wywierać destrukcyjny wpływ na jego struktury administracyjne i decyzyjne, a także podważać podstawy społeczne, ekonomiczne oraz kulturowe. Według raportu *Freedom on the Net 2017: Manipulating Social Media to*

Undermine Democracy[19] coraz więcej krajów na świecie wykorzystuje media społecznościowe do działań dezinformacyjnych – zarówno do kształtowania swojej polityki wewnętrznej, jak i do wpływania na inne państwa. Przeciwdziałanie dezinformacji staje się wyzwaniem, przed jakim stoją nie tylko pojedyncze państwa, lecz także instytucje i organizacje międzynarodowe. Konieczność przeciwdziałania kampaniom dezinformacyjnym w Europie podkreśliła po raz pierwszy Rada Europejska w marcu 2015 r. Od tego czasu w strukturach Europejskiej Służby Działań Zewnętrznych (ang. European External Action Service) powstało kilka zespołów zajmujących się analizowaniem dezinformacji w Unii Europejskiej oraz krajach sąsiadujących ze wspólnotą.

Problem dezinformacji – na szczeblu ogólnopaństwowym i strategicznym – był poruszany w Biurze Bezpieczeństwa Narodowego podczas prac nad rekomendacjami do nowej Strategii Bezpieczeństwa Narodowego. Omawiano go również na forum międzynarodowym oraz w trakcie licznych spotkań eksperckich organizowanych w BBN. Z dyskusji wynika, że największymi wyzwaniami w środowisku informacyjnym są obecnie:

- brak zrozumienia wagi i charakteru problemu;
- brak sprawnego systemu komunikacji strategicznej i koordynacji działań w zakresie zwalczania dezinformacji na szczeblu krajowym;
- niski poziom umiejętności korzystania z mediów wśród wybranych grup społecznych;
- wypracowanie równowagi między wolnością słowa a przeciwdziałaniem dezinformacji;
- zbudowanie pozytywnej narracji oraz promocja państwa na zewnątrz.

Wszystkie te wyzwania mają charakter uniwersalny i w dużej mierze dotyczą także Polski jako państwa należącego do wspólnoty cywilizacji zachodniej podzielającej wartości demokratyczne. W ujęciu międzynarodowym dezinformacja jest najczęściej wymierzona właśnie w procedury demokratyczne i ma podważyć zaufanie obywateli do państwa. Takie działanie zagraża także bezpieczeństwu narodowemu. Działania dezinformacyjne wprowadzają obywateli w błąd i często wzbudzają

[19] https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [dostęp: 28 XI 2021].

w nich niepewność. Uniemożliwia im to m.in. podejmowanie suwerennych, opartych na wiarygodnych informacjach, decyzji wyborczych.

Przeciwdziałanie dezinformacji wymaga przede wszystkim:

- podnoszenia świadomości obywateli na temat zagrożeń dezinformacyjnych;
- budowania zdolności instytucjonalnych;
- podjęcia współpracy różnych instytucji z komórkami ds. komunikacji strategicznej w krajach i instytucjach UE i NATO;
- projektowania i wdrażania działań aktywnych, tj. prowadzenia projektów i kampanii informacyjnych;
- wsparcia polskich organizacji pozarządowych i podjęcia z nimi współpracy.

Aby rozpoznać dezinformację, należy:

1. Poznać źródło informacji (zrozumieć jego cele i intencje), dowiedzieć się, kto odpowiada za to źródło, kto jest jego właścicielem itp.
2. Czytać całość artykułu, a nie tylko nagłówek (aby zrozumieć cały materiał).
3. Sprawdzić autorów, aby zweryfikować, czy są oni wiarygodni. Nie zawsze jest to możliwe, ponieważ nie wszystkie artykuły są podpisane z nazwiska oraz nie wszyscy autorzy – nawet w wiarygodnych treściach – są podpisani. Jeśli jest taka możliwość, dobrze jest wyszukać nazwisko autorki czy autora i zobaczyć inne treści, które ta osoba tworzy.
4. Sprawdzić tę informację w innych źródłach (upewnić się, że podają te same dane).
5. Znaleźć datę publikacji (aby sprawdzić, czy informacje są aktualne).
6. Przemyśleć własne uprzedzenia (aby zobaczyć, czy nie wpływają one na nasz osąd).
7. Zapytać ekspertów (uzyskać potwierdzenie od niezależnych ludzi dysponujących wiedzą na dany temat).

W obliczu ogromnej liczby informacji, które na co dzień są przetwarzane w źródłach otwartych, powstaje problem w odróżnieniu prawdy od kłamstwa. Bardzo często mamy do czynienia z kreowaniem pewnych wizji, zwłaszcza przez media, zamiast z przedstawianiem wiarygodnych informacji. Ponadto dynamiczne tempo życia sprawia, że cykl życia informacji jest bardzo krótki. Informację, która pojawiła się

dzisiaj i poruszyła opinię publiczną, kolejnego dnia zastąpi inna, równie ważna. Dodatkowo przesyt różnych informacji sprawia, że procesy decyzyjne bywają niezwykle skomplikowane, a ludzie kierują się nie stanem rzeczywistym, a raczej społecznym postrzeganiem danych faktów. Do tego dochodzi jeszcze manipulowanie informacjami w celu osiągnięcia określonych korzyści. Za przykład może posłużyć szerzenie dezinformacji przez Rosję podczas wyborów prezydenckich w Stanach Zjednoczonych w 2016 r. Taki stan rzeczy to ogromny problem współczesnych społeczeństw. Obecnie bardzo trudno jest kontrolować obieg informacji publicznych, istnieje bowiem wiele narzędzi manipulacyjnych podważających w dużym stopniu wiarygodność przedstawianych informacji. Dodatkowo bardzo niepokojąca jest sytuacja, w której ataki informacyjne stają się rozpoznawalne dopiero w momencie osiągnięcia celu przez atakującego bądź nie są rozpoznawane wcale. Zasadne wydają się zatem słowa Sławomira Zalewskiego, który powiedział: „(...) stwierdzenie braku występowania zagrożeń nie eliminuje ich w przyszłości, ale też nie wyklucza, że działania stanowiące zagrożenie podejmowane są tu i teraz, tyle że zostały jeszcze nierozpoznane”[20].

Biorąc pod uwagę liczne zagrożenia informacji w cyberprzestrzeni, należy zauważyć, że największe państwa na świecie wprowadziły specjalne regulacje prawne mające na celu ochronę zasobów teleinformatycznych oraz przeciwdziałanie zagrożeniom w tym zakresie. Między innymi Rosja w ustawie o ochronie danych osobowych wraz z jej późniejszymi uzupełnieniami wprowadziła nakaz przechowywania danych osobowych Rosjan wyłącznie na terenie ich państwa[21]. Stany Zjednoczone ustanowiły CLOUD Act[22], który zobowiązuje amerykańskich dostawców usług o charakterze elektronicznym do ujawnienia na żądanie amerykańskiego sądu informacji dotyczących użytkowników tych usług, niezależnie od tego, czy są one przetwarzane w Stanach, czy w dowolnym innym państwie na świecie. Warto również zwrócić uwagę na ustawę o cyberbezpieczeństwie wprowadzoną w Chinach i ustawę wyznaczającą Narodowy Standard Bezpieczeństwa Informacyjnego. Otóż dokumenty te sankcjonują zasadę, że każdy sprzęt oraz oprogramowanie dostarczane na potrzeby

[20] S. Zalewski, *Bezpieczeństwo polityczne. Zarys problematyki*, Siedlce 2013, s. 148.

[21] https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [dostęp: 28 XI 2021].

[22] https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [dostęp: 28 XI 2021].

podmiotów rządowych bądź podmiotów z obszaru infrastruktury krytycznej muszą być audytowane przez wyznaczone i przygotowane do tego jednostki. Sprawdzeniu podlega też kod źródłowy oprogramowania kupowanego na potrzeby powyższych jednostek.

W 2014 r. proces skutecznego tworzenia systemu cyberbezpieczeństwa rozpoczęto na Ukrainie. Najważniejszym impulsem do podjęcia takich działań były cyberataki na sieć elektroenergetyczną, które doprowadziły do tymczasowych przerw w dostawie energii elektrycznej. W 2016 r. została zatwierdzona Strategia Cyberbezpieczeństwa Ukrainy w której podkreślono potrzebę prac legislacyjnych w zakresie krajowego systemu cyberbezpieczeństwa[23]. Uznano, że powyższe działania są podstawą bezpieczeństwa narodowego. Ponadto skupiono się na interakcji pomiędzy działaniami podejmowanymi przez organy państwowe, samorządowe, formacje wojskowe, instytucje naukowe, a także podmioty komercyjne. Pomimo wprowadzenia dokumentów legislacyjnych na Ukrainie istnieją ogromne problemy z rozwojem strategii cyberbezpieczeństwa. Wynikają one m.in. z braku skutecznej realizacji polityki cyberbezpieczeństwa, braku świadomości z zakresu cyberzagrożeń oraz niewystarczającego potencjału ludzkiego. Problemy stwarza również: brak prawnych i organizacyjnych ram ochrony infrastruktury krytycznej, brak aktualnych standardów cyberbezpieczeństwa oraz słabe ustawodawstwo krajowe dotyczące cyberprzestępczości[24].

Na uwagę zasługują działania podejmowane w Estonii, które mogą być wzorem dla innych państw. Estonię należy uznać za pioniera cyfryzacji w Europie, co potwierdza wprowadzenie już w 2008 r. strategii cyberbezpieczeństwa[25]. Był to pierwszy tego typu dokument na świecie. Estonia nieustannie pracuje nad zwiększeniem poziomu cyberbezpieczeństwa. Wynika to przede wszystkim z wysoce rozwiniętych e-usług, a działania prewencyjne mają przeciwdziałać przestępczości w sieci. Estonia jest zwolennikiem jednolitego rynku cyfrowego na obszarze Unii Europejskiej, co ma przełożyć się na wymierne zyski w perspektywie

[23] J. Semeniy, S. Glushchenko, O. Makarevich, *Ukraine*, w: *Cybersecurity 2018*, B.A. Powell, J.C. Chipman (red.), Law Business Research, London, s. 99.

[24] V. Boiko, *Comparison of the Polish and Ukrainian cybersecurity system*, „Teka of Political Science and International Relations" 2019, t. 14, nr 2, s. 119–137.

[25] Narodowa Strategia Cyberprzestrzeni Estonii, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia [dostęp: 28 XI 2021].

rozwoju e-gospodarki. Ponadto usilnie mobilizuje państwa członkowskie do wspólnych działań na rzecz cyfryzacji i bezpieczeństwa w cyberprzestrzeni. Przedmiotem zainteresowania są m.in.: ochrona danych osobowych w sieciach komórkowych i na stronach internetowych, swobodny przepływ danych nieosobowych, a także opodatkowanie usług internetowych. Estonia realizując politykę cyberbezpieczeństwa, stara się przede wszystkim uporządkować istniejące regulacje, a także adaptować je do dynamicznie zmieniających się uwarunkowań. W dalszym ciągu dąży też do doskonalenia technologii wspomagającej reagowanie na incydenty w cyberprzestrzeni poprzez m.in. poprawę infrastruktury sieci, skoordynowanie administrowania systemami informatycznymi oraz wzmocnienie działu IT w administracji[26].

Wymiernym działaniem na terenie Unii Europejskiej w zakresie cyberbezpieczeństwa było przyjęcie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*[27], tzw. RODO, wiążącego wszystkich przetwarzających dane osobowe w związku z prowadzoną działalnością gospodarczą. Za pomocą powyższego rozporządzenia wprowadzono wiele zmian oraz zwiększono zakres obowiązków administratorów i podmiotów przetwarzających dane.

W związku z tym, że cyberbezpieczeństwo stanowi obecnie jedno z największych wyzwań, jakie stoją przed administratorami i użytkownikami sieci teleinformatycznych, unijną odpowiedzią na nie jest również *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*[28]. Na terenie Polski dyrektywa ta została zaimplementowana *Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[29]. Ustawa nałożyła nowe obowiązki na podmioty mające wpływ na bezpieczeństwo państwa. Między innymi wymogiem stały się audyty wewnętrzne systemów

[26] K. Raś, *Estonia jako lider w zwiększeniu cyberbezpieczeństwa*, „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, nr 68, s. 20–22.

[27] Dz. Urz. UE L 119/1 z 27 IV 2016 r.

[28] Dz. Urz. UE L 194/1 z 6 VII 2016 r.

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

teleinformatycznych, opracowywanie stosownej dokumentacji, wdrażanie systemów zarządzania bezpieczeństwem, a także przeprowadzanie czynności pozwalających na wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów. W Polsce została też uchwalona *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[30]. Na mocy tego dokumentu do zadań Agencji Bezpieczeństwa Wewnętrznego włączono m.in.: rozpoznawanie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, oraz zapobieganie tym zagrożeniom. Szef ABW jest odpowiedzialny za prowadzenie centralnego rejestru zdarzeń o charakterze terrorystycznym naruszających bezpieczeństwo systemów teleinformatycznych o szczególnym znaczeniu dla bezpieczeństwa państwa albo sieci teleinformatycznych. Ponadto w celu zapobiegania i przeciwdziałania zdarzeniom o charakterze terrorystycznym w cyberprzestrzeni oraz ich zwalczania ABW może dokonywać oceny bezpieczeństwa systemów teleinformatycznych polegającej na przeprowadzeniu testów bezpieczeństwa w celu identyfikacji podatności. Przez podatność rozumie się słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana i zagrozić integralności, poufności, rozliczalności i dostępności tego systemu.

Przedstawione przykłady pokazują, jak istotna jest ochrona zasobów informacyjnych na arenie międzynarodowej oraz jakie środki bezpieczeństwa pozwolą przeciwdziałać wszelkim zagrożeniom związanym z przepływem informacji.

Warto również zaznaczyć, że działania cyberprzestępców wywierają duży wpływ na obiekty należące do infrastruktury krytycznej. Ich celem jest przede wszystkim podważenie zaufania publicznego wobec społeczeństwa obywatelskiego i fundamentów demokracji. Jest to także zagrożenie suwerenności, które daje organizacjom terrorystycznym i kryminalistom możliwość anonimowego działania przy wykorzystaniu technik oraz skutecznych metod wpływania na politykę i strategię

[30] Tekst jednolity: DzU z 2021 r. poz. 2234.

innych państw. Przykładem mogą być działania Rosji, która jest jednym z najaktywniejszych sprawców cyberataków, podczas bezprawnej aneksji Krymu w 2014 r. Kolejnym przykładem są Chiny, które aktywnie zaangażowały się w przeprowadzanie cyberataków i kampanie dezinformacyjne skierowane przeciwko członkom sojuszu NATO i stanowią bardzo poważne zagrożenie krytycznych elementów infrastruktury energetycznej, co zostało podkreślone w ekspertyzie NATO 2030[31].

Cyberataki przeprowadzone w ciągu ostatnich 15 lat są dowodem na to, że mają one wpływ zarówno na tych, którzy je przeprowadzają – cyberprzestępców, jak i na środowiska, które próbują bronić sieci. Obecnie środowisko związane z cyberbezpieczeństwem wymaga wielu narzędzi i rozwiązań, które zazwyczaj są bardzo kosztowne. Ataki prowadzone naźmniejszą skalę to jedynie przyczółek do większych ataków, a idąc dalej – do rozwoju cyberbroni. Rozwój cyberataków sprawił, że specjaliści w dziedzinie bezpieczeństwa cybernetycznego zaczęli uważać je za nagminne zjawisko i skoncentrowali swoje działania na obronie sieci. Metody zapewnienia cyberbezpieczeństwa, jak i sposób reakcji na ataki muszą ewoluować adekwatnie do sposobów działania cyberprzestępców. W związku z tym, że za środowisko internetowe w większości odpowiada sektor komercyjny, organizacje państwowe i podmioty prywatne powinny rozważyć współpracę w zakresie bezpieczeństwa sieci. Wymaga to jednak szerokich zmian legislacyjnych dotyczących działań proaktywnych i reaktywnych podejmowanych w odpowiedzi na zagrożenia cybernetyczne.

Zasadny wydaje się rozwój doktryny operacyjnej realizowanej przez krajowe siły cybernetyczne, które powinny być rozwijane, testowane oraz modyfikowane w zależności od zagrożeń. Organizacja ćwiczeń bilateralnych wydaje się dobrym wstępem do dalszej kooperacji. W dłuższej perspektywie w ćwiczeniach powinni brać udział również przedstawiciele sektora komercyjnego odpowiedzialni za działania ochronne. Przedstawiciele organów i instytucji państwowych nie powinni obawiać się współpracy z ekspertami do spraw cybernetyki reprezentującymi ten sektor, gdyż przejęli oni już inicjatywę i prowadzą działania wyprzedzające. Ponadto globalny charakter Internetu wymaga współpracy międzynarodowej. Indywidualne rozwiązania stosowane w poszczególnych państwach nie będą efektywne w obliczu zagrożeń cybernetycznych, gdyż walka z tymi zagrożeniami wymaga spójnego

[31] https://nato.int [dostęp: 29 XI 2021].

i elastycznego podejścia. NATO jako organizacja międzynarodowa ma wieloletnie doświadczenie w kreowaniu polityki i przeprowadzaniu operacji skierowanych przeciwko zagrożeniom o charakterze konwencjonalnym. Jednak teraz nastąpił czas, aby zdobyte doświadczenie i wiedzę specjalistyczną wykorzystać w celu zapewnienia i utrzymania cyberbezpieczeństwa[32].

Reasumując, należy stwierdzić, że założona hipoteza została zweryfikowana. W ciągu ostatnich kilkudziesięciu lat nastąpił ogromny postęp technologiczny związany z rozwojem nowoczesnych technologii, a przede wszystkim powstaniem zaawansowanego społeczeństwa informacyjnego. Obecnie nikt już nie wyobraża sobie życia bez dostępu do Internetu, a tym samym do informacji pochodzących ze źródeł otwartych. Ich powszechność, dostępność, niski koszt pozyskania sprawiają, że są one pierwszym źródłem, z którego się korzysta. Jednakże wraz z ich rozwojem powstały także nowe zagrożenia, często o charakterze cyberterrorystycznym, które stanowią ogromne niebezpieczeństwo dla człowieka jako jednostki, jak również organizacji oraz struktur państwowych. Bezpieczeństwo informacyjne to obszar, który wymaga podjęcia radykalnych i natychmiastowych działań, gdyż cyberprzestępcy w sposób utajniony są w stanie dotrzeć do wszelkich systemów, aby zrealizować zaplanowany cel. Sytuacji nie sprzyja dynamicznie zmieniające się środowisko, pandemia koronawirusa i przeniesienie życia do świata Internetu, a także konflikty między państwami mające na celu zdobycie przewagi na arenie międzynarodowej. Implementowane regulacje prawne wydają się niewystarczające do ochrony informacji. Trzeba stworzyć efekt synergii poprzez połączenie działań międzynarodowych, a także działań na poziomie poszczególnych państw, aby na stałe zapewnić bezpieczeństwo sieci, na poziomie zarówno krajowym, jak i międzynarodowym. Należy mieć świadomość, że ataki cyberterrorystyczne będą występować, a nawet się nasilać. Ich skala może być bardzo różna, od manipulacji informacjami i szerzenia dezinformacji po ataki na systemy teleinformatyczne infrastruktury krytycznej. Pomimo że całkowite wyeliminowanie cyberterroryzmu nie jest realne, należy podejmować działania prewencyjne, a także mające na celu jak najszybsze wykrywanie ataków o charakterze cyberterrorystycznym i minimalizowanie powodowanych przez nie strat.

[32] W.E. Leigher, *Cyber conflict in a hybrid threat environment: Death by a thousand cuts*, Helsinki 2021.

Bibliografia

Aleksandrowicz T.R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze,* Warszawa 2021.

Boiko V., *Comparison of the polish and Ukrainian cybersecurity system,* „Teka of Political Science and International Relations" 2019, t. 14, nr 2, s. 119–137.

Elliott A., *Castells M.: Społeczeństwo sieci,* w: Elliott A., *Współczesna teoria społeczna. Wprowadzenie,* Warszawa 2011.

Grzelak M., *Szpiegostwo i inwigilacja w Internecie,* w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, s. 164–181.

Hall R., Fox C., *Ponownie przemyśleć bezpieczeństwo,* „Przegląd NATO" zima 2001/2002.

Kissinger H., *Dyplomacja,* Warszawa 2016.

Leigher W.E., *Cyber conflict in a hybrid threat environment: Death by a thousand cuts,* Helsinki 2021.

Measuring the Information Society Report, t. 1, Geneva 2018.

Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje,* w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz,* P. Sienkiewicz, J.S. Nowak (red.), Katowice 2008.

Oleński J., *Ekonomika informacji,* Warszawa 2001.

Raś K., *Estonia jako lider w zwiększeniu cyberbezpieczeństwa,* „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, nr 68, s. 20–22.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy,* Warszawa 2015.

Sienkiewicz P., *Społeczeństwo informacyjne jako system cybernetyczny,* w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?,* t. 1, L.H. Haber (red.), Kraków 2004.

Semeniy J., Glushchenko S., Makarevich O., *Ukraine,* w: *Cybersecurity* 2018, B.A. Powell, J.C. Chipman (red.), Law Business Research, London.

Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)*, „Zagadnienia Informacji Naukowej" 2013, nr 2, s. 9–41.

Sun Tzu, *Sztuka wojny*, Gliwice 2004.

West Ch., *Competitive intelligence*, New York 2001.

Zalewski S., *Bezpieczeństwo polityczne. Zarys problematyki*, Siedlce 2013.

Źródła internetowe

https://datareportal.com/reports/digital-2021-global-overview-report [dostęp: 26 XI 2021].

https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [dostęp: 28 XI 2021].

https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [dostęp: 28 XI 2021].

https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [dostęp: 28 XI 2021].

https://nato.int [dostęp: 29 XI 2021].

http://unicjin.org/documents/congr10/10e.pdf [dostęp: 27 XI 2021].

http://www.bbc.uw.edu.pl/Content/20/08.pdf [dostęp: 25 XI 2021].

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia [dostęp: 28 XI 2021].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 27 IV 2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 6 VII 2016 r.).

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

Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych (DzU z 2021 r. poz. 2234.).

DOI: 10.4467/27204383TER.22.007.15423

ORCID: 0000-0002-2174-6966

ARTUR SYBICKI

Problematyka ochrony antyterrorystycznej miejsc kultu religijnego

Abstrakt

Ataki terrorystyczne w Europie na obiekty sakralne wymusiły w polityce bezpieczeństwa państw członkowskich UE, na których terenie do nich doszło, opracowanie i wdrożenie rozwiązań (prawnych, merytorycznych, technicznych i fizycznych) proporcjonalnych do charakteru i rodzaju danego obiektu. Celem ich wprowadzenia jest wzmocnienie poziomu ochrony antyterrorystycznej zarówno samego miejsca kultu religijnego, jak i osób mających z nim bezpośredni kontakt (duchownych oraz uczestników zgromadzeń liturgicznych). Czynniki świadczące o atrakcyjności obiektów sakralnych jako celów zamachów terrorystycznych, w tym główne zagrożenia ich bezpieczeństwa, oraz wymagane elementy systemu ich ochrony antyterrorystycznej w wielu państwach pozostają tożsame. Istotnym zagadnieniem jest również to, że polskie miejsca kultu religijnego mają wiele cech, które umiejscawiają je w gronie obiektów użyteczności publicznej zagrożonych ewentualnymi zdarzeniami o charakterze terrorystycznym. Można odnieść jednak wrażenie, że kwestie dotyczące ich ochrony antyterrorystycznej nie są traktowane na terytorium RP systemowo. Dużo dyskutuje się na temat bezpieczeństwa obiektów użyteczności publicznej, jednak polscy naukowcy i eksperci praktycy w zakresie bezpieczeństwa terrorystycznego nie skupili na nich swojej uwagi w sposób kompleksowy.

Słowa kluczowe:

obiekty sakralne, miejsca kultu religijnego, system ochrony antyterrorystycznej obiektów sakralnych, bezpieczeństwo terrorystyczne miejsc kultu religijnego

Przełomowy w opracowaniu i budowaniu systemów bezpieczeństwa antyterrorystycznego miejsc kultu, zarówno w wymiarze europejskim, jak i polskim, jest rok 2021. Komisja Europejska finansuje bowiem w tym zakresie sześć projektów (jeden pod przewodnictwem Uniwersytetu Łódzkiego jest realizowany na terytorium RP), których celem jest usystematyzowanie problematyki ochrony antyterrorystycznej obiektów sakralnych, a w przyszłości zwiększenie poziomu ich ochrony przed niebezpieczeństwami. Intencją autora artykułu jest przedstawienie rozwiązań w tym zakresie procedowanych przez Komisję Europejską i uzyskanie odpowiedzi na pytanie, w jakim stopniu polskie obiekty sakralne są przygotowane na niebezpieczne incydenty, zwłaszcza te o charakterze terrorystycznym.

Modus operandi sprawców zdarzeń o charakterze terrorystycznym na terenie Europy ewoluuje. Zauważalna jest tendencja do wycofywania się przez organizacje terrorystyczne z koncepcji zamachów na wielką skalę i przyjęcie rozproszonej formuły aktywności. Grupy terrorystyczne odchodzą od skomplikowanej i wyrafinowanej metodyki działania i skupiają się na aktywności jednostek (ang. *lone wolf*, *solo terrorist*) lub małej liczby osób stosujących proste środki działania, łatwo dostępne i niewymagające znacznych przygotowań logistycznych[1]. Niejednokrotnie sprawcy zamachów terrorystycznych sięgają po rozwiązania używane przez kryminalne środowiska przestępcze, wykorzystując podczas ataków tożsame metody i narzędzia. Pomimo różnorodności działania główne cele ich aktywności pozostają niezmienne. Nadal najczęściej atakują niewinne i bezbronne osoby oraz miejsca ich pobytu, w tym obiekty użyteczności publicznej, stanowiące tzw. miękkie cele, o niskim poziomie zabezpieczeń przed zagrożeniami oraz mające symboliczną, określoną wartość dla danego społeczeństwa. Taka metodyka działania powoduje pojawianie się nowych, dotąd nieznanych lub zdarzających się incydentalnie sposobów mobilizacji zamachowców i stwarza dużo większe zagrożenie bezpieczeństwa powszechnego. Eksperci ds. bezpieczeństwa

[1] T. Aleksandrowicz, *Bieżące zagrożenia, terrorystyczne, cz. 1. – Doświadczenia ostatniego dziesięciolecia*, „Przegląd Policyjny" 2017, nr 4 (128), s. 38.

terrorystycznego zgodnie podkreślają, że wobec nieprzewidywalności zachowań napastników organy władzy publicznej, w kompetencji których jest zwalczanie terroryzmu i zapobieganie mu, są zmuszone stawiać czoło przeciwnikowi znacznie trudniejszemu i o wiele bardziej niebezpiecznemu (koncepcja nazywana tzw. nowym terroryzmem)[2].

Jednym z celów ataków są miejsca kultu religijnego – obiekty sakralne związane z chrześcijaństwem, islamem, buddyzmem i judaizmem – oraz uczęszczający do nich wyznawcy. Na terenie Europy co roku dochodzi do wielu celowych ataków na te miejsca, wskutek których duchowni oraz uczestnicy zgromadzeń liturgicznych tracą życie i zdrowie. Niejednokrotnie te ataki są kwalifikowane jako zdarzenia o charakterze terrorystycznym lub ekstremistycznym i są m.in. wynikiem działań motywowanych nienawiścią na tle religijnym.

Ze względu na cykliczny wzrost ataków na miejsca kultu religijnego na terenie Europy członkowie Unii Europejskiej coraz częściej zastanawiają się nad tym, jak powinien wyglądać ich system ochrony antyterrorystycznej. W wielu państwach Wspólnoty, zwłaszcza tych o wysokim poziomie ryzyka wystąpienia zdarzenia o charakterze terrorystycznym, którego celem były, są lub mogą być m.in. miejsca kultu religijnego, są opracowywane rozwiązania służące ich skutecznej ochronie. Wszystkie tego typu systemy, przez lata systematycznie rozwijane i udoskonalane, mają być odpowiedzią na ewentualne zdarzenia zarówno o charakterze terrorystycznym, jak i ekstremistycznym. Z perspektywy Unii Europejskiej uznano, że tematyka bezpieczeństwa terrorystycznego obiektów użyteczności publicznej, w tym miejsc kultu religijnego, jest bardzo istotna, w związku z czym zapisano ją w strategii bezpieczeństwa UE na lata 2020–2025 jako jeden ze strategicznych priorytetów unii bezpieczeństwa[3].

Biorąc po uwagę powyższe informacje, autor skupił się w artykule na charakterystyce procedowanych przez Komisję Europejską rozwiązań służących bezpieczeństwu terrorystycznemu europejskich miejsc kultu

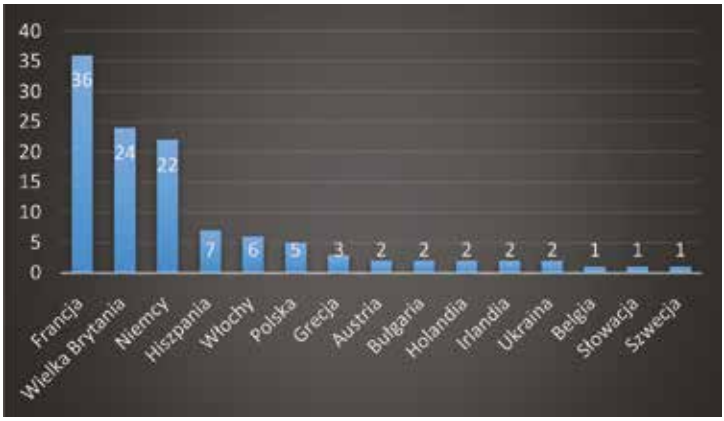
---

[2] T. Aleksandrowicz, K. Jałoszyński, *Cechy charakterystyczne organizacji terrorystycznych w XXI wieku*, w: *Bezpieczeństwo państwa a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, K. Jałoszyński, T. Aleksandrowicz, K. Wiciak (red.), Szczytno 2016, s. 47.

[3] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa,* Bruksela 2020, s. 11–13, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605&cookies=disabled [dostęp: 30 XI 2021].

religijnego. Ważnym elementem artykułu jest również próba oceny systemu ochrony antyterrorystycznej polskich obiektów sakralnych i uzyskanie odpowiedzi na pytanie, w jakim stopniu są one przygotowane na niebezpieczne incydenty, zwłaszcza te o charakterze terrorystycznym.

Z informacji zawartych w biuletynach opublikowanych na oficjalnej stronie internetowej projektu SOAR – *Protecting Places of Worship in Europe* finansowanego przez Komisję Europejską wynika, że tylko od 2 lipca do 22 października 2021 r. na terenie Europy doszło do wielu niebezpiecznych zdarzeń, których celem były miejsca kultu religijnego lub związane z nimi osoby[4]. Na podstawie opracowania własnego autora artykułu, wykonanego na bazie danych znajdujących się w treści wymienionych publikacji, ustalono, że spośród 116 incydentów najwięcej z nich wydarzyło się na terenie Francji, Niemiec i Wielkiej Brytanii (łącznie 82). Służby pozostałych 12 państw, gdzie również doszło do takich zdarzeń (wśród nich również na terytorium Polski), odnotowały po kilka tego typu wydarzeń. We wskazanym okresie na terenie RP popełniono pięć przestępstw, które polskie organy ścigania – w większości przypadków – zakwalifikowały jako czyny zabronione popełnione z nienawiści na tle religijnym. Zestawienie liczbowe tych zdarzeń z podziałem na państwa europejskie prezentuje wykres nr 1.

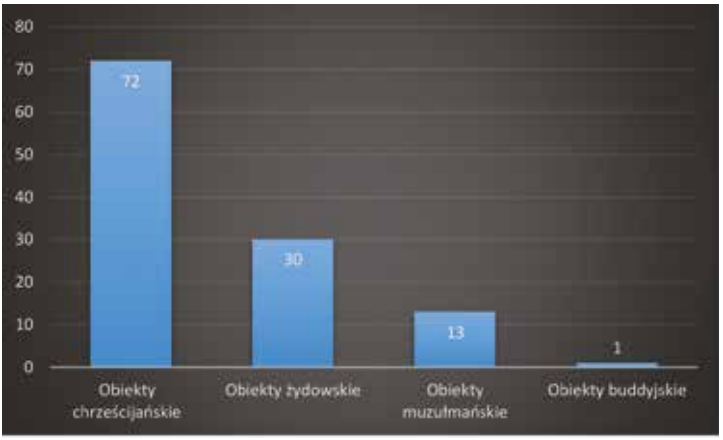


Wykres 1. Liczba ataków na miejsca kultu religijnego w Europie w okresie od 2 lipca do 22 października 2021 r.

Źródło: Opracowanie własne na podstawie biuletynów informacyjnych zamieszczonych na oficjalnej stronie projektu SOAR, https://soarproject.eu/resources/ [dostęp: 11 XII 2021].

[4] https://soarproject.eu/newsletter/ [dostęp: 11 XII 2021].

W tożsamy sposób autor artykułu przeanalizował, które grupy wspólnot wyznaniowych były najczęściej atakowane na terenie Europy. Z uzyskanych informacji wynika, że w prezentowanym okresie najczęstszym celem sprawców były miejsca i osoby związane z religią chrześcijańską. Łącznie zidentyfikowano 72 przypadki agresji, co stanowi 62,07 proc. wszystkich ataków na europejskie miejsca kultu religijnego. Ataki na miejsca i osoby związane z pozostałymi wspólnotami wyznaniowymi to odpowiednio: 30 incydentów związanych ze wspólnotą żydowską (co stanowi 25,86 proc. wszystkich zdarzeń na terenie Europy), 13 czynów zabronionych dotyczących miejsc związanych z islamem (co stanowi 11,21 proc. wszystkich zdarzeń na terenie Europy) oraz jeden atak, którego celem był obiekt buddyjski (co stanowi 0,86 proc. wszystkich zdarzeń)[5]. Zestawienie liczbowe z podziałem na religie prezentuje wykres nr 2.



Wykres 2. Liczba ataków na osoby i miejsca związane z daną religią, mające miejsce w Europie od 2 lipca do 22 października 2021 r.

Źródło: Opracowanie własne na podstawie biuletynów informacyjnych zamieszczonych na oficjalnej stronie projektu SOAR, https://soarproject.eu/resources/ [dostęp: 11 XII 2021].

[5] Do ataku na obiekt związany z buddyzmem doszło we wrześniu 2021 r. na terytorium Wielkiej Brytanii, www.swindonadvertiser.co.uk/news/19590833.hundreds-march-town-centre-solidarity-hindu-community-temple-break-ins/ [dostęp: 12 XII 2021].

Czyny zabronione, które osoby zatrzymane popełniały wobec miejsc związanych z chrześcijaństwem, były w większości aktami wandalizmu i polegały m.in. na uszkadzaniu mienia znajdującego się w budynkach, dewastacji i kradzieży symboli religijnych, wykorzystaniu pojazdu jako narzędzia ataku (Francja, Sarthe)[6], ostrzelaniu budynku kościoła z broni palnej (Słowacja, Bratysława)[7], usiłowaniu wykorzystania samolotu do ataku na obiekt (Francja, Paryż)[8]. W dwóch przypadkach doszło do zabójstw, które służby antyterrorystyczne oceniły jako akty przemocy motywowane religijnie. Jedno z nich popełniono w sierpniu 2021 r. na terenie Francji. Sprawca będący osobą zaburzoną psychicznie – w przeszłości został zatrzymany przez służby policyjne pod zarzutem podpalenia obiektu sakralnego – dokonał zabójstwa duchownego katolickiego, wykorzystując w tym celu niebezpieczny przedmiot z ostrzem[9]. Drugie zabójstwo miało miejsce w październiku 2021 r. na terenie Wielkiej Brytanii. Dotyczyło konserwatywnego brytyjskiego polityka ściśle związanego z religią katolicką[10]. Służby brytyjskie zakwalifikowały to przestępstwo jako zdarzenie o charakterze terrorystycznym, a samego sprawcę jako radykała islamskiego.

Z opracowania własnego autora artykułu wynika ponadto, że państwami, na których terenie doszło do największej liczby ataków na miejsca kultu i osoby związane z religią chrześcijańską, były Francja, Wielka Brytania, Niemcy, Hiszpania i Włochy. Incydenty te stanowiły 87,5 proc. wszystkich zdarzeń na terenie Europy, których celem były obiekty chrześcijańskie. W tej grupie znalazło się również terytorium RP, gdzie doszło do trzech aktów agresji. Zestawienie liczbowe w przedmiotowym zakresie prezentuje wykres nr 3.

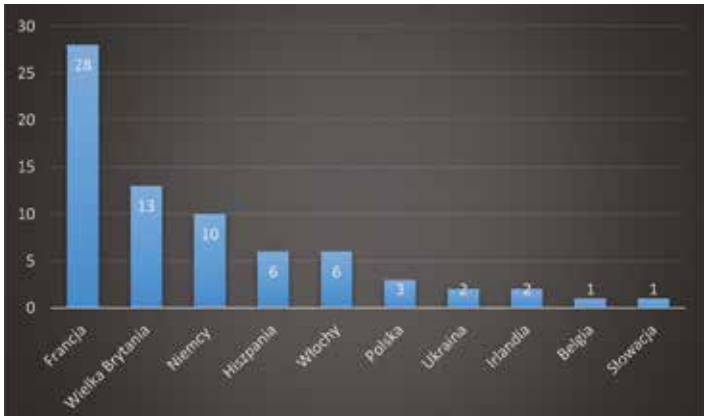
[6] https://actu.fr/pays-de-la-loire/beille_72031/sarthe-un-camion-fonce-dans-l-eglise-son-chauffeur-s-enfuit-le-maire-lance-un-appel-a-temoins_45259304.html [dostęp: 11 XII 2021].

[7] https://www.kath.net/news/76584 [dostęp: 11 XII 2021].

[8] https://www.leprogres.fr/faits-divers-justice/2021/10/10/il-projetait-de-percuter-la-cathedrale-notre-dame-en-avion-un-homme-interpelle [dostęp: 11 XII 2021].

[9] https://www.europe1.fr/faits-divers/un-pretre-assassine-en-vendee-annonce-darmanin-4061489 [dostęp: 11 XII 2021].

[10] https://www.bbc.com/news/uk-58935372 [dostęp: 11 XII 2021].



Wykres 3. Liczba ataków na obiekty chrześcijańskie w Europie w okresie od 2 lipca do 22 października 2021 r.

Źródło: Opracowanie własne na podstawie biuletynów informacyjnych zamieszczonych na oficjalnej stronie projektu SOAR, https://soarproject.eu/resources/ [dostęp: 11 XII 2021].

Czyny zabronione, które sprawcy popełnili wobec miejsc związanych z judaizmem, islamem i buddyzmem – podobnie jak w obiektach chrześcijańskich – miały podłoże ekstremistyczne oraz kryminalne motywowane nienawiścią na tle religijnym. Były to m.in. akty wandalizmu polegające na niszczeniu i dewastacji mienia, w tym: podpalenia, umieszczanie obraźliwych napisów na symbolach religijnych (Wielka Brytania, Essex)[11], groźby karalne kierowane z powodów rasistowskich i przynależności religijnej (Francja, Strasburg)[12], groźby użycia niebezpiecznych przedmiotów z ostrzem (Francja, Villeurbanne)[13].

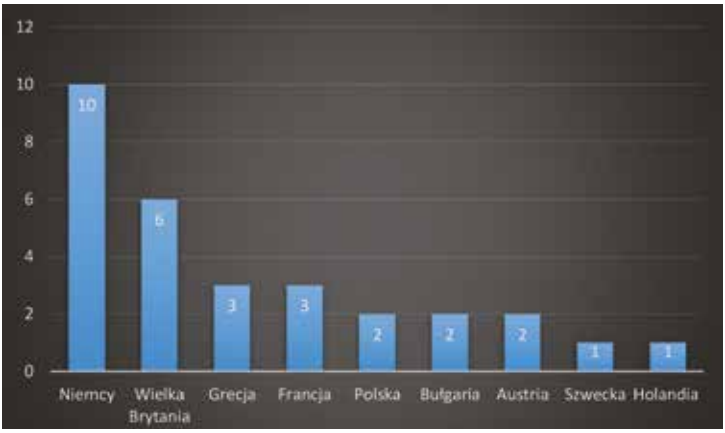
Z opracowania własnego autora artykułu wynika, że państwami, na których terenie doszło do największej liczby ataków na miejsca kultu i osoby związane z judaizmem i islamem, były Niemcy, Wielka Brytania i Francja. Ataki na obiekty żydowskie przeprowadzone w tych trzech krajach stanowiły 63,33 proc. tego rodzaju zdarzeń, które miały miejsce w całej Europie. W przypadku ataków na obiekty muzułmańskie ten

[11] https://muslimnews.co.uk/news/islamophobia/france-3-mosques-face-islamophobic-attack/ [dostęp: 11 XII 2021].

[12] https://actu.fr/grand-est/strasbourg_67482/mosquee-a-strasbourg-l-association-derriere-le-projet-menacee-d-attentats_45450694.html [dostęp: 11 XII 2021].

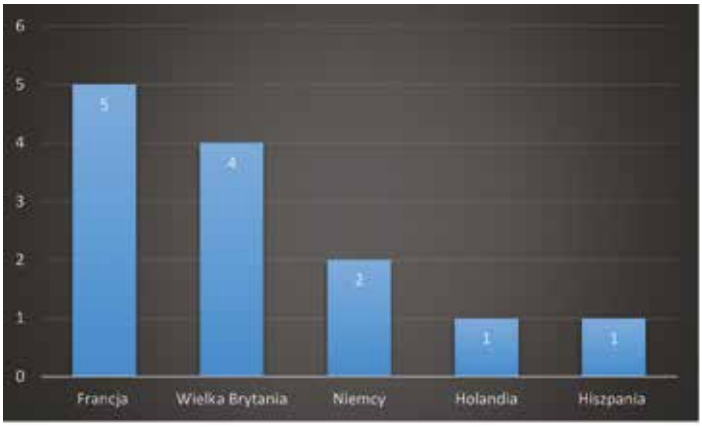
[13] https://www.jpost.com/diaspora/antisemitism/teenager-arrested-after-waving-knife-in-front-of-french-jewish-school-684430 [dostęp: 11 XII 2021].

odsetek wynosi 84,61 proc. Zestawienie liczbowe w przedmiotowym zakresie prezentują wykresy nr 4 i 5.



Wykres 4. Liczba ataków na obiekty żydowskie w Europie w okresie od 2 lipca do 22 października 2021 r.

Źródło: Opracowanie własne na podstawie biuletynów informacyjnych zamieszczonych na oficjalnej stronie projektu SOAR, https://soarproject.eu/resources/ [dostęp: 11 XII 2021].



Wykres 5. Liczba ataków na obiekty muzułmańskie w Europie od 2 lipca do 22 października 2021 r.

Źródło: Opracowanie własne na podstawie biuletynów informacyjnych zamieszczonych na oficjalnej stronie projektu SOAR, https://soarproject.eu/resources/ [dostęp: 11 XII 2021].

Wsparciem dla projektów podejmowanych w zakresie ochrony miejsc kultu religijnego jest działalność Dyrekcji Generalnej Komisji Europejskiej ds. Migracji i Spraw Wewnętrznych (ang. DG for Migration and Home Affairs, DG HOME), realizującej szereg inicjatyw służących zwiększaniu poziomu bezpieczeństwa w obszarze zagrożeń terrorystycznych dla miejsc użyteczności publicznej, w tym dla miejsc kultu religijnego. W 2017 r. Komisja Europejska przyjęła plan działania, którego celem jest wspieranie państw członkowskich UE w zakresie ochrony tych miejsc. Po zakończonych konsultacjach w 2019 r. wydano dokument pt. *Good practices to support the protection of public spaces*. W obszarze zabezpieczenia obiektów publicznych określono szereg praktyk o charakterze ogólnym, stanowiących punkt wyjścia do budowania systemów ich zabezpieczenia przez osoby odpowiedzialne za ten proces w poszczególnych podmiotach[14]. Dodatkowo w maju 2021 r. przedstawiciele zespołu doradczego UE ds. zapewnienia bezpieczeństwa przy DG HOME, przy udziale przedstawicieli formacji policyjnych zrzeszonych od 2018 r. w ramach unijnej sieci ds. bezpieczeństwa w miejscach wysokiego ryzyka (ang. EU High Risk Security Network), opracowali publikację pt. *Krótki podręcznik UE służący wsparciu ochrony miejsc kultu* (*EU Quick Guide to support the protection of places of worship*). Wskazuje ona dodatkowe dobre praktyki w zakresie ochrony tych miejsc kultu religijnego, które można uznać za obiekty o niskim ryzyku zagrożenia zdarzeniami o charakterze terrorystycznym[15].

Autorzy podręcznika podkreślają, że stanowi on wsparcie merytoryczne dla członków wszystkich religijnych wspólnot wyznaniowych, i zachęcają do jego wykorzystywania w procesie oceny stopnia zagrożenia terrorystycznego miejsc kultu. Zdaniem ekspertów DG HOME przywołana publikacja jest mniej przydatna w ocenie rodzajów zdarzeń, których charakter wskazuje, że były one elementem działań uprzednio zaplanowanych przez sprawców zamachów. W tym kontekście nie znajduje

[14] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Bruksela 2019, s. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6--11e9-8ed-01aa75ed71a1/language-en [dostęp: 16 XI 2021].

[15] European Commission, DG HOME, *EU Quick Guide to support the protection of places of worship, 2021*, s. 4–5, https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [dostęp: 27 XI 2021].

ona szerokiego zastosowania wobec miejsc kultu charakteryzujących się wysokim poziomem podatności na zagrożenia, wynikającym m.in. z ich lokalizacji (często o charakterze symbolicznym), ważnych wydarzeń religijnych odbywających się na ich terenie czy obecności w ich trakcie osób o statusie VIP. Szczególnego podkreślenia wymaga fakt, że *EU Quick Guide to support the protection of places of worship* służy podnoszeniu świadomości i ocenie odporności obiektów na ograniczoną liczbę rodzajów zdarzeń o charakterze terrorystycznym, tzn. takich, podczas których sprawca bądź sprawcy wykorzystują jako narzędzie ataku: pojazdy, broń palną, przedmioty niebezpieczne z ostrzem oraz materiały wybuchowe (nazywane przez autora instrumentarium sprawcy)[16]. Najistotniejszą część przewodnika stanowią zasady służące ocenie poziomu ewentualnych niebezpieczeństw, oparte na poszukiwaniu odpowiedzi na zamieszczone w treści dokumentu pytania pomocnicze, w obszarach istotnych z punktu widzenia bezpieczeństwa miejsc kultu[17].

W czerwcu 2020 r. Komisja Europejska, w ramach Funduszu Bezpieczeństwa Wewnętrznego – Policja (ang. Internal Security Fund – Police), skierowała do członków UE zaproszenie do składania wniosków o dofinansowanie projektów służących podniesieniu poziomu bezpieczeństwa miejsc kultu religijnego. Zakładane działania w ramach projektu miały polegać m.in. na:

- nawiązywaniu lub zacieśnianiu współpracy pomiędzy podmiotami publicznymi a przywódcami religijnymi danego wyznania;
- tworzeniu kanałów wymiany informacji pomiędzy tymi podmiotami na temat ewentualnych zagrożeń o charakterze terrorystycznym i kryminalnym (przestępstwa z nienawiści);
- opracowywaniu i realizacji kampanii społecznych na rzecz podnoszenia świadomości antyterrorystycznej obywateli UE;
- dzieleniu się wiedzą, dobrymi praktykami w zakresie rozwiązań stosowanych przez różne państwa członkowskie;
- opracowywaniu, wdrażaniu i realizacji koncepcji, programów bezpieczeństwa i szkoleń[18].

[16] Tamże, s. 5.

[17] Tamże, s. 7–22.

[18] ISF Police, 2020 Call for proposals: ISFP-2020-AG-PROTECT, https://ec.europa.eu/research/participants/data/ref/other_eu_prog/home/wp/call-fiche_isfp-2020-ag-protect_en.pdf [dostęp: 28 XI 2021].

Na tej podstawie w 2021 r. Komisja Europejska wsparła finansowo sześć niezależnych projektów służących poprawie bezpieczeństwa terrorystycznego miejsc kultu religijnego, tj.:

- ProSPeReS – *Protection System for large gatherings of People in Religious Sites* – w chwili obecnej jedyny projekt służący ochronie antyterrorystycznej miejsc kultu religijnego realizowany na terytorium RP[19];
- SASCE – *Safer and Stronger Communities in Europe*;
- SHIELD – *Solutions to Enhance Interfaith Protection of Places of Worship from Terrorist Danger*;
- PROTECTOR – *Protecting Places of Worship*;
- PROSECUW – *Protection and Security for Places of Worship*;
- SOAR Project – *Protecting Places of Worship in Europe*[20].

Celem wspomnianych inicjatyw jest podniesienie poziomu ochrony antyterrorystycznej miejsc kultu religijnego poprzez opracowanie ich systemu/systemów bezpieczeństwa terrorystycznego, przeciwdziałanie ewentualnym zagrożeniom o charakterze terrorystycznym i reagowanie na nie, w tym m.in. z użyciem środków CBRN[21] (projekt ProSPeReS). Powyższe założenia mają być realizowane na bazie współpracy pomiędzy europejskimi naukowcami, ekspertami i praktykami w dziedzinie bezpieczeństwa miejsc użyteczności publicznej, tj. przedstawicielami organów administracji państwowej i wyznaniowych instytucji religijnych[22]. Projekty zakładają dokonanie analizy pilotażowych studiów przypadków, do jakich doszło w wymienionych obiektach na terenie państw europejskich, identyfikację luk w ich systemach

[19] Wśród beneficjentów projektu znalazły się następujące polskie podmioty: Szkoła Główna Służby Pożarniczej, Komenda Stołeczna Policji, Komenda Wojewódzka Policji w Łodzi, Komenda Wojewódzka Policji we Wrocławiu, Akademia WSB, Fundacja Obserwatorium Społeczne, Centrum Badań Kosmicznych PAN, Gmina Wyznaniowa Żydowska w Warszawie, Archidiecezja Łódzka, Dynamic Safety Corporation Sp. z o.o. oraz europejscy partnerzy z Finlandii, Grecji, Cypru, Holandii i Słowacji.

[20] TOPIC ID: ISFP-2020-AG-PROTECT, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/isfp-2020-ag-protect [dostęp: 11 XII 2021].

[21] Symbol oznaczający zagrożenia z użyciem czynników chemicznych, biologicznych, radiacyjnych i nuklearnych.

[22] *Funding & tender opportunities*, http://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034230/ISFP [dostęp: 11 XII 2021].

ochrony i na tej podstawie opracowanie zaleceń zwiększających bezpieczeństwo terrorystyczne tych obiektów. Rezultatem wyników ma być opracowanie profilowanych szkoleń, materiałów instruktażowych i informacji na temat najlepszych praktyk w zakresie bezpieczeństwa terrorystycznego miejsc kultu oraz realizacja kampanii społecznych o szerokim zasięgu oddziaływania.

Sygnatariusze projektów podkreślają, że najważniejszym elementem ich działań będzie również zwiększanie ochrony miejsc kultu poprzez wdrażanie koncepcji bezpieczeństwa nazywanej *security by design*. Model ten wpisuje się w ogólne założenia wskazywane przez ekspertów Komisji Europejskiej, którzy stoją na stanowisku, że minimalizację skutków działania sprawców zdarzeń o charakterze terrorystycznym można osiągać już na etapie projektowania i budowy danego obiektu, tworząc takie jego części lub przestrzenie funkcjonowania, które w chwili ataku zapewnią powstanie w nim jak najmniejszej liczby szkód i będą efektywnie zapobiegać jego znacznemu uszkodzeniu[23].

Eksperci DG HOME oraz przedstawiciele Departamentu Bezpieczeństwa Krajowego (ang. Department of Homeland Security), resortu rządu Stanów Zjednoczonych Ameryki odpowiedzialnego za bezpieczeństwo m.in. miejsc kultu religijnego, wskazują na czynniki, które zwiększają prawdopodobieństwo ataku terrorystycznego na obiekty sakralne[24].

Pierwszym wymienionym elementem jest otwarty dostęp i swobodny udział w nabożeństwach religijnych duchownych oraz uczestników zgromadzeń liturgicznych (często o statusie VIP). Fakt ten sprawia, że w związku z odbywającymi się wydarzeniami i rytuałami o znaczeniu religijnym w dowolnym miejscu, o ustalonej godzinie, może zgromadzić się we wnętrzu lub na zewnątrz obiektu przewidywalna liczba uczestników. Na tej podstawie zarówno samo miejsce, jak i znajdujący się w nim ludzie stają się gotowym i łatwym celem dla przeciwnika mającego swobodny i nieograniczony dostęp do niemalże każdego kościoła, meczetu lub synagogi[25].

[23] European Commission, Commission Staff Working Document, *Good practices to support…*, s. 4–5.

[24] U.S. Department of Homeland Security, *Houses of Worship Security Practice Guide*, May 2013, s. 6, https://www2.illinois.gov/ready/plan/documents/dhs_houses_of_worship_security_practices_guide.pdf [dostęp: 20 XI 2021].

[25] European Commission, *Protection of Places of Worship,* 2020, https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=696367&utm_source=pps_newsroom&utm_

Obiekty sakralne mają dla wielu społeczności wyznaniowych znaczenie religijne, historyczne, kulturowe lub społeczne. Symboliczna wartość danego miejsca jest kolejnym z elementów zwiększających prawdopodobieństwo wystąpienia zdarzenia o charakterze terrorystycznym lub ekstremistycznym na jego terenie[26]. Dla fundamentalistycznych ideologów religijnych zaatakowanie symbolu staje się podstawą do osiągania celów politycznych, a poprzez propagowanie nienawiści i strachu wśród przeciwników religijnych zachętą do przejmowania kontroli nad wybraną społecznością, do jej pokonania i zdobycia nad nią władzy[27]. Dla sprawców przestępstw kryminalnych z nienawiści czynnikiem, który definiuje ich zachowania, jest najczęściej tzw. motywacja uprzedzeniowa względem osób i ich szeroko rozumianych odmienności[28].

Kolejny wskazywany czynnik zwiększający prawdopodobieństwo ataku na obiekt sakralny to nieograniczony dostęp zarówno osób, jak i pojazdów do jego obszarów peryferyjnych. Przez mnogość obiektów przyległych do budynków kultu religijnego (nieruchomości miejskie, szczególnie instytucje i ważne miejsca publiczne) oraz ich lokalizację (centrum, peryferie miasta) zwiększa się liczba mogących przebywać tam osób, a wśród nich potencjalnych agresorów[29]. Swoboda parkowania pojazdów bez kontroli w dowolnym miejscu tej strefy, np. na parkingach, pobliskich ulicach, wjazdach na teren obiektu, i wielokrotnie wiążący się z tym brak fizycznych barier ograniczających ruch aut zwiększa ryzyko wykorzystania pojazdu jako narzędzia ataku (np. poprzez detonację ukrytych w pojeździe materiałów wybuchowych, wykorzystanie pojazdu do taranowania osób poruszających się w ciągach komunikacyjnych)[30].

Ograniczenia i trudności finansowe miejsc kultu religijnego to także czynniki zwiększające ich atrakcyjność jako obiektów ataku. Głównym bowiem celem ich funkcjonowania jest aktywność religijna

---

medium=Website&utm_campaign=pps&utm_content=Protection%20of%20Places%20of%20Worship&lang=en [dostęp: 27 XI 2021].

[26] U.S. Department of Homeland Security, *Houses of Worship Security*..., s. 6.

[27] K. Izak, *Nie tylko islam. Ekstremizm i terroryzm religijny*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 209.

[28] A. Mazurczak, *Przestępstwa motywowane uprzedzeniami. Analiza i zalecenia*, „Biuletyn Rzecznika Praw Obywatelskich" 2017, nr 6, s. 10.

[29] European Commission, *Protection of Places of Worship*...

[30] U.S. Department of Homeland Security, *Houses of Worship Security* ..., s. 6.

na rzecz poszczególnych wspólnot wyznaniowych i zaspokajanie ich potrzeb duchowych. Dysponowanie niskimi dochodami znacznie ogranicza osobom odpowiadającym za ich administrowanie dostęp do rozwiązań wpływających na zwiększenie poziomu bezpieczeństwa tych miejsc, w tym np. zakupu sprzętu ochrony fizycznej czy też zatrudnienia ekspertów do budowania odpowiednich systemów bezpieczeństwa[31].

W polityce bezpieczeństwa terrorystycznego miejsc kultu religijnego najważniejszym elementem jest osiągnięcie i utrzymanie wysokiego poziomu świadomości sytuacyjnej osób związanych z danym obiektem i zrozumienia przez nie tego, co dzieje się zarówno w jego środowisku wewnętrznym, jak i wokół niego. Stan ten osiąga się przez kształtowanie kultury bezpieczeństwa zarówno wśród osób odpowiedzialnych za kierowanie danym miejscem (duchownych), jak i pracowników i pozostałych uczestników zgromadzeń liturgicznych. Każdy z nich musi zrozumieć, że zagrożenia terrorystyczne istnieją, a ich ignorowanie znacznie obniża szansę ich szybkiego rozpoznania. Istotnym czynnikiem w sytuacji kryzysu jest wzięcie przez wszystkich wymienionych odpowiedzialności za bezpieczeństwo swoje, bezpieczeństwo otoczenia (obiekt i ludzie), a w sytuacji zagrożenia – podjęcie odpowiednich działań ochronnych i obronnych[32]. Działania takie wspierać powinna edukacja antyterrorystyczna realizowana poprzez opracowywanie programów edukacyjnych podnoszących świadomość antyterrorystyczną wśród wymienionych osób. Tylko łącząc teorię z praktyką można przygotować ludzi na ewentualne zagrożenia i odpowiedzieć na pytania, jak mają identyfikować niebezpieczeństwa, jak się przed nimi bronić i jak zachować w sytuacji kryzysowej[33].

Eksperci Komisji Europejskiej w podręczniku pt. *EU Quick Guide to support the protection of places of worship* podkreślają, że na poziomie projektowania systemu ochrony antyterrorystycznej miejsc kultu

[31] Tamże.

[32] K. Liedel, P. Piasecka, *Bezpieczeństwo w czasach terroryzmu. Jak przeżyć zamach terrorystyczny*, Warszawa 2018, s. 42.

[33] B. Wiśniewska-Paź, J. Stelmach, *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, t. 4 – *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (red.), Toruń 2019, s. 8.

religijnego należy wziąć pod uwagę wiele istotnych elementów i na podstawie informacji na temat identyfikowanych, podstawowych zagrożeń przeprowadzić proces oceny ryzyka ich wystąpienia. Ważnym zagadnieniem jest również uzyskanie odpowiedzi na pytanie, jaki rodzaj ryzyka wystąpienia danego zagrożenia można uznać za akceptowalny i jaki rodzaj działań można podjąć w obiekcie w celu minimalizacji prawdopodobieństwa wystąpienia zagrożenia[34].

Proces oceny ryzyka wystąpienia zdarzenia o charakterze terrorystycznym w miejscach kultu religijnego jest częścią wieloskładnikowego procesu zarządzania ryzykiem, będącego najważniejszą składową systemu zabezpieczenia antyterrorystycznego zarówno obiektu, jak i przebywających w nim ludzi. Według ekspertów National Counter Terrorism Security Office (NaCTSO) w zarządzaniu ryzykiem w obiekcie należy uwzględnić wiele ważnych elementów, które m.in. w marcu 2019 r. Komisja Europejska wskazała jako dobre praktyki wzmacniające ochronę antyterrorystyczną miejsc użyteczności publicznej[35]. W tym zakresie istotnym wsparciem dla osób dokonujących takiej oceny jest również wymieniany powyżej *EU Quick Guide to support the protection of places of worship*, zwłaszcza w kontekście zagrożeń związanych ze wspomnianym powyżej instrumentarium sprawców wykorzystywanym podczas ataków[36].

Bazowym czynnikiem systemu jest zidentyfikowanie i określenie poziomu ryzyka terrorystycznego w obiekcie, polegające m.in. na zrozumieniu intencji i możliwości napastnika bądź napastników oraz tego, czego mogą dokonać i przy wykorzystaniu jakiej metodyki ataku. Eksperci brytyjscy wskazują, że w tym obszarze pomocne jest uzyskanie odpowiedzi na następujące pytania:

- Jakiego rodzaju informacje na temat zagrożeń terrorystycznych wobec danego obiektu mogących wystąpić na poziomie lokalnym i krajowym osoba odpowiedzialna za jego bezpieczeństwo może uzyskać od instytucji państwowych, np. Policji?
- Czy istnieją takie elementy funkcjonowania obiektu, które mogą przyciągnąć uwagę sprawców zdarzeń o charakterze terrorystycznym?

---

[34] European Commission, DG HOME, *EU Quick Guide to support the protection…*, s. 13.

[35] European Commission, Commission Staff Working Document, *Good practices to support…*, s. 4–5.

[36] European Commission, DG HOME, *EU Quick Guide to support the protection…*, s. 5.

- Czy istnieje związek pomiędzy obiektem a osobami lub organizacjami o statusie VIP, które mogą być celem ataków terrorystycznych? Czy istnieją procedury bezpieczeństwa regulujące udział ww. podmiotów w wydarzeniach odbywających się na terenie obiektu? Jak często są one weryfikowane?
- Czy w bezpośredniej lokalizacji obiektu znajdują się budynki, które poprzez specyfikę funkcjonowania są miejscami wysokiego ryzyka terrorystycznego i mogą pośrednio sprowadzać niebezpieczeństwo na sam obiekt?
- Czy istnieją obszary działalności obiektu lub jego personelu, które napastnicy mogliby wykorzystać podczas ataku, np. dostępne dla osób trzecich plany architektoniczne budynków, wiedza techniczna, nieograniczony dostęp do stref zastrzeżonych obiektu?[37].

Kolejnym elementem jest zidentyfikowanie podmiotów, które należy poddać ochronie, ocena ich podatności na zagrożenia oraz określenie słabych punktów danego obiektu. Każdorazowo w kontekście bezpieczeństwa miejsca kultu religijnego priorytetem są ludzie (duchowni, pracownicy, uczestnicy zgromadzeń liturgicznych), dalej zasoby materialne (np. budynki, ich wyposażenie, plany), a na końcu informacje (zarówno dane elektroniczne, jak i papierowe). Wytypowanie słabych punktów systemu, w odniesieniu do zagrożeń zarówno zewnętrznych, jak i wewnętrznych, pozwala na uzyskanie odpowiedzi, jakiego rodzaju rozwiązania należy opracować, by go ulepszać. Usprawnianie systemu może odbywać się m.in. poprzez ścisłą współpracę pomiędzy osobami zarządzającymi obiektem a państwowymi jednostkami organizacyjnymi odpowiedzialnymi za zwalczanie terroryzmu. Wskazane podmioty powinny regularnie dokonywać oceny podatności osób na zagrożenia terrorystyczne pochodzące z zewnątrz i wewnątrz danego miejsca. Istotne w tej sytuacji jest uzyskanie odpowiedzi na pytania, dlaczego i na jakie rodzaje zagrożeń podatne są ochraniane obiekty[38].

W systemie ochrony antyterrorystycznej miejsca kultu religijnego ważne jest zidentyfikowanie środków zmniejszających lub łagodzących ryzyko wystąpienia w nim zdarzenia o charakterze terrorystycznym.

[37] National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020 r., https://www.gov.uk/government/publications/crowded-places-guidance/managing-risk-business-continuity [dostęp: 20 XI 2021].

[38] European Commission, Commission Staff Working Document, *Good practices to support…*, s. 4–5.

Po identyfikacji pozwalającej na stwierdzenie, że niebezpieczeństwo dla ludzi i obiektu jest realne, powinna nastąpić identyfikacja i ocena skuteczności istniejących już środków bezpieczeństwa, a w dalszej kolejności wdrożenie nowych, dodatkowych i proporcjonalnych rozwiązań ochronnych dostosowanych do różnych środowisk. Celem jest osiągnięcie możliwie najniższego poziomu wszelkich zagrożeń[39]. Eksperci Komisji Europejskiej podkreślają, że wybranym i dostosowanym do potrzeb środkom ochrony każdorazowo muszą towarzyszyć odpowiednie rozwiązania techniczne, opracowywane przez specjalistów ds. bezpieczeństwa, zarówno w ramach danego miejsca, jak i na zasadzie outsourcingu[40]. Często okazuje się, że inwestowanie w kosztowne środki ochrony służące funkcjonowaniu obiektu nie ma większego sensu, a najbardziej efektywnymi rozwiązaniami okazują się te najprostsze. Tym bardziej stają się one skuteczne, gdy ludzi związanych z obiektem cechuje wysoka kultura bezpieczeństwa. Na takich podstawach, po ocenie, że zagrożenie jest realne, można budować kolejne elementy systemu bezpieczeństwa w obiekcie[41].

Opracowanie, regularne przeglądanie i aktualizowanie planów ochrony obiektu to kolejne ogniwo systemu. Skuteczny plan bezpieczeństwa powinien być prosty i jasno sformułowany. Jego zasadniczym celem ma być powstrzymanie ewentualnego zagrożenia wynikającego z czynników zewnętrznych i wewnętrznych (np. ze strony osób zatrudnionych w obiekcie), a w sytuacji jego wystąpienia złagodzenie potencjalnych skutków działania sprawcy lub sprawców. W takiej sytuacji konieczne staje się stworzenie kompleksowej strategii, która połączyć powinna działania zapobiegawcze, ochronne i przygotowawcze, opierając wszystkie jej elementy na analizie ryzyka, w powiązaniu z działaniami zwiększającymi odporność obiektu na ewentualne zagrożenia, w szczególności te najpoważniejsze[42]. W procedurach ochrony zaleca się systematyczne sprawdzanie planów ochrony, m.in. pod kątem oceny ich dokładności, wykonalności i aktualności, a po wykonanym audycie

[39] National Counter Terrorism Security Office, *Crowded Places Guidance*...

[40] European Commission, Commission Staff Working Document, *Good practices to support*..., s. 4–5.

[41] National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020 r., https://www.gov.uk/government/publications/crowded-places-guidance/introduction [dostęp: 20 XI 2021].

[42] National Counter Terrorism Security Office, *Crowded Places Guidance*...

wyciąganie wniosków, zalecanie koniecznych rekomendacji i wdrażanie ich w życie.

Według brytyjskiej koncepcji bezpieczeństwa terrorystycznego obiektów sakralnych odpowiedzialność za przygotowanie planów ochrony w miejscach kultu religijnego powinna spoczywać na tzw. liderach bezpieczeństwa. Osoby te na terenie danego obiektu sakralnego m.in. przewodniczą specjalnie utworzonym w tym celu zespołom ds. oceny zagrożeń terrorystycznych (ang. *threat assessment team*)[43]. Co do zasady, w ich skład powinni wchodzić specjaliści mający nie tylko formalne uprawnienia do wykonania zadań ochronnych, ale przede wszystkim wiedzę i doświadczenie w zakresie projektowania całościowego systemu ochrony[44]. Rolą członków zespołu jest zarówno ochrona fizyczna obiektu, jak i zbieranie informacji o rodzaju zagrożeń jego bezpieczeństwa, próba ich identyfikacji oraz ocena ich charakteru. Funkcjonując w ramach miejsc kultu religijnego, osoby te włączają się również w proces edukacji antyterrorystycznej, której program obejmuje m.in. identyfikację możliwych zagrożeń ludzi i obiektu, wskazanie, w jaki sposób reagować i jak bronić się w momencie zaistnienia niebezpieczeństwa.

Ważnym obszarem działalności zespołu są stałe kontakty z przedstawicielami instytucji państwowych odpowiedzialnych za bezpieczeństwo terrorystyczne zarówno na szczeblu lokalnym, regionalnym, krajowym (np. Policja, inne służby ratunkowe), jak i międzynarodowym. Utrzymywanie relacji z formacjami państwowymi daje przede wszystkim możliwość niezwłocznego przekazywania ustalonym kanałem komunikacyjnym informacji o zidentyfikowanym zagrożeniu, korzystania z wiedzy eksperckiej, dzielenia się informacjami wykorzystywanymi w procesie dokonywania analizy ryzyka oraz pomocy w typowaniu i rozpoznawaniu wewnętrznych i zewnętrznych zagrożeń dla danej społeczności religijnej[45].

---

[43] U.S. Department of Homeland Security, *Houses of Worship Security…*, s. 6.

[44] J. Stelmach, M. Kożuszek, *Założenia i rekomendacje do wykonywania planów ochrony w obiektach podlegających obowiązkowej ochronie*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, t. 4 – *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (red.), Toruń 2019, s. 25.

[45] National Counter Terrorism Security Office, *Counter Terrorism Protective Security Advice for Places of Worship,* ACPO 2009, s. 42, https://www.welhat.gov.uk/

System ochrony antyterrorystycznej miejsc kultu religijnego to również ich ochrona fizyczna, która – przez wykorzystanie proporcjonalnych środków ochrony – służyć ma m.in. ograniczeniom w swobodnym dostępie do miejsc będących strefami ograniczonego dostępu. Z tym ściśle wiąże się również wykorzystanie technicznych środków detekcji, np. do wykrywania materiałów wybuchowych, broni palnej, niebezpiecznych przedmiotów z ostrzem. Specjaliści Komisji Europejskiej uzależniają jednak zastosowanie tego typu rozwiązań od oceny podatności danego obiektu na ewentualne zagrożenia[46].

Ostatnim elementem systemu ochrony antyterrorystycznej obiektów sakralnych jest stałe i cykliczne szkolenie personelu. Standardem stają się regularne szkolenia stacjonarne przeznaczone dla personelu obiektu (duchownych, pracowników, uczestników zgromadzeń liturgicznych) w celu podnoszenia ich poziomu świadomości antyterrorystycznej, upewnienia się, że rozumieją swoje obowiązki i akceptują potrzebę wdrażania środków bezpieczeństwa terrorystycznego zawartych w planie ochrony. Istotnym elementem systemu szkoleń są również ćwiczenia praktyczne. Ich realizacja służyć ma ujawnianiu ewentualnych błędów i luk w istniejących procedurach bezpieczeństwa, określaniu wątpliwości lub uwag do planów ochrony, wykorzystaniu przez osoby związane z danym miejscem zdobytej wiedzy teoretycznej do dalszego doskonalenia rozwiązań służących bezpieczeństwu danego obiektu. Ćwiczenia to również nieustanna weryfikacja tego, czy opracowane plany ochrony są wykonalne i spełniają oczekiwania. Działania praktyczne powinny angażować wszystkie zainteresowane strony systemu ochrony, zwłaszcza administratorów obiektu, jego personel, uczestników zgromadzeń liturgicznych, ale również służby ratownicze (np. straż pożarną, Policję, siły specjalne) i inne właściwe podmioty odpowiedzialne za bezpieczeństwo oraz zapewniać wielorakość scenariuszy, zgodnie z zasadą „planuj-wykonaj-sprawdź-działaj”[47].

Podsumowując wybrane zagadnienia rozwiązań proponowanych przez Unię Europejską w zakresie zwiększenia poziomu ochrony

media/16407/Crowded-Places-Guidance/pdf/Crowded_Places_Guidance.pdf?m=637242863669130000 [dostęp: 20 XI 2021].

[46] European Commission, Commission Staff Working Document, *Good practices to support...*, s. 4–5.

[47] National Counter Terrorism Security Office, *Counter Terrorism Protective Security Advice...*, s. 37.

miejsc kultu religijnego przed zagrożeniami o charakterze terrorystycznym, należy zwrócić uwagę na dwie dodatkowe, nierzadko trudne do pogodzenia, kwestie. Z jednej strony – jak wspomniano powyżej – przez otwarty charakter obiektów sakralnych, swobodny i w przewidywalnym czasie udział w wydarzeniach i uroczystościach religijnych dużej liczby osób oraz częsty brak wystarczających procedur bezpieczeństwa miejsca te stają się łatwym celem ataku. Z drugiej strony nie należy zapominać, że dla zachowania ich rzeczywistej roli i przeznaczenia nie jest możliwe stworzenie z nich typowej fortecy zapewniającej im bezwzględne bezpieczeństwo. Stan, który można osiągnąć, to stworzenie systemu ochrony pozwalającego na minimalizację ryzyka wystąpienia ataku i zredukowanie do pewnego poziomu ewentualnych niepożądanych skutków działania sprawcy lub sprawców[48]. W tej sytuacji nie można zapominać, że nie w każdym miejscu kultu religijnego znajdą zastosowanie tożsame proponowane rozwiązania. Poszczególne obiekty różnią się między sobą wieloma wskaźnikami, takimi jak wielkość, lokalizacja, przeznaczenie, mniej lub bardziej rozwinięta kultura bezpieczeństwa ludzi itp. Dlatego też rozwiązania służące podnoszeniu poziomu ich ochrony powinny być opracowywane indywidualnie i odpowiadać rzeczywistemu przeznaczeniu i charakterystyce funkcjonowania danego miejsca[49].

Poddając pod rozwagę problem ochrony antyterrorystycznej miejsc kultu religijnego na terenie UE, nie sposób nie zadać sobie pytania, czy polskie obiekty sakralne spotykają się z podobnymi problemami, czy były lub są celem ataków sprawców zdarzeń o charakterze terrorystycznym lub ekstremistycznym i w związku z tym jak wygląda system ich zabezpieczenia przed tego typu zdarzeniami.

Odpowiadając na powyższe, należy stwierdzić, że w Polsce nie odnotowano incydentów o stricte terrorystycznym podłożu. Do chwili obecnej wszystkie incydenty, których celem były polskie miejsca kultu religijnego, były kwalifikowane przez polskie służby jako kryminalne, w tym motywowane nienawiścią na tle religijnym. Sprawcy tych przestępstw (zarówno pojedynczy, jak i działający wspólnie i w porozumieniu z innymi) podczas usiłowania lub dokonania fizycznego ata-

[48] Tamże, s. 6.

[49] European Commission, Commission Staff Working Document, *Good practices to support…*, s. 4–5.

ku na osoby i miejsca związane z daną wspólnotą wyznaniową używali jako instrumentarium niebezpiecznych przedmiotów z ostrzem, broni pneumatycznej, stosowali siłę fizyczną (pobicia) oraz groźby karalne wobec osób. Źródłem czynów napastników były choroby psychiczne, agresja na tle różnic religijnych lub wpływ środków odurzających. W jednym przypadku atak agresora zakończył się śmiercią ofiary i zranieniem duchownego udzielającego ofierze pomocy medycznej. W pozostałych przypadkach obrażenia ciała odniesione przez poszkodowanych nie stanowiły zagrożenia ich życia i zdrowia. Większość sprawców została zatrzymana przez organy ścigania w krótkim czasie od momentu zdarzenia. Do chwili obecnej nie zarejestrowano ataków na polskie obiekty sakralne z wykorzystaniem materiałów wybuchowych, broni palnej, substancji chemicznych lub biologicznych, nie były też one celem cyberprzestępców.

Podobnie jak obiekty sakralne na świecie, również polskie miejsca kultu religijnego charakteryzują się cechami zwiększającymi ich atrakcyjność jako celów ewentualnego ataku terrorystycznego. W dużej mierze są one tożsame, wręcz identyczne z tymi, które przedstawiciele brytyjskiego NaCTSO opisali w swojej publikacji. W literaturze przedmiotu polscy eksperci ds. bezpieczeństwa uzupełniają ten katalog o dodatkowe elementy i wskazują oprócz wymienionych powyżej np. niski stopień zabezpieczenia antyterrorystycznego danego miejsca, możliwość zwiększania oddziaływania powybuchowego w przypadku zamachów bombowych zagrażających stabilności konstrukcji budynków, ograniczone możliwości działania służb ratowniczych ze względu na trudności wynikające z przepustowości dróg ewakuacyjnych oraz zwartej infrastruktury wokół budynków[50].

W rozważaniach dotyczących zabezpieczenia miejsc kultu religijnego w Polsce należy zwrócić uwagę na jeszcze jeden istotny problem. Pomimo identyfikacji ewentualnych czynników ryzyka dla obiektów sakralnych w kontekście wystąpienia zamachu terrorystycznego nadal mieszczą się one w kategorii obiektów użyteczności publicznej, w których ochrona nie jest obligatoryjna. W związku z tym nie istnieje żaden

[50] J. Stelmach, B. Wiśniewska-Paź, *Wprowadzenie – rozważania na temat zagrożenia terroryzmem dla obiektów użyteczności publicznej*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, t. 2 – *Metody i narzędzia zamachów vs działania antyterrorystyczne i kontrterrorystyczne*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (red.), Toruń 2018, s. 9–10.

prawny obowiązek opracowywania w nich kompleksowej dokumentacji dotyczącej systemu ochrony antyterrorystycznej. O posiadaniu np. fizycznych lub technicznych środków bezpieczeństwa, przygotowania i wdrażania planu ochrony, prowadzenia działań profilaktycznych, realizacji szkoleń i ćwiczeń praktycznych decyduje wyłącznie zarządzający (administrujący) budynkiem, a jego decyzja jest najczęściej wynikiem analizy ryzyka oraz możliwości finansowych danego miejsca[51].

Obecnie kwestie związane z postępowaniem na terenie miejsca kultu religijnego podczas wystąpienia konfliktu zbrojnego i sytuacji kryzysowej, w tym również zdarzeń o charakterze terrorystycznym, uregulowano w rozdziale 8 *Ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami*[52]. Swoją właściwością rzeczową obejmuje on jednak wyłącznie te obiekty, które zgodnie z definicją mają status zabytku i ich zachowanie w niezmiennym stanie (jako nieruchomość, jej część lub zespół), z uwagi na wartość historyczną, artystyczną i naukową, stanowi interes społeczny. Na tej podstawie zgodnie z treścią aktu wykonawczego do ustawy, tj. *Rozporządzenia Ministra Kultury z dnia 25 sierpnia 2004 r. w sprawie organizacji i sposobu ochrony zabytków na wypadek konfliktu zbrojnego i sytuacji kryzysowych*[53], są ustalane organizacja i sposób ochrony tych miejsc w jednostkach organizacyjnych mających zabytki, opisywany jest stan zasobów podlegających ochronie, potencjalne zagrożenia i środki służące ich zapobieganiu. W planie ochrony zabytków poszczególnych jednostek organizacyjnych administracji państwowej i samorządowej organy odpowiedzialne za jego tworzenie, opierając się na przewidywalnych i realnych zagrożeniach, określają potrzebne siły i środki oraz czas i koszty na wypadek wystąpienia takiego incydentu. Ponadto umieszczają w treści dokumentu informacje dotyczące procesu realizacji prac przygotowawczych oraz sprawnego koordynowania i zarządzania ochroną podczas wystąpienia takiego zdarzenia[54].

[51] J. Stelmach, *Kategorie obiektów użyteczności publicznej i stopnie ich ochrony w kontekście zagrożenia współczesnym terroryzmem*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Analiza – Diagnoza – Case study*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (red.), Toruń 2018, s. 31.

[52] Tekst jednolity: DzU z 2021 r. poz. 710.

[53] DzU z 2004 r. nr 212 poz. 2153.

[54] A. Ginter, A. Michalak, *Komentarz do art. 88*, w: *Ustawa o ochronie zabytków i opiece nad zabytkami. Komentarz*, A. Ginter, A. Michalak (red.), Warszawa 2016, LEX Omega nr 500623.

Liczba ataków terrorystycznych na miejsca użyteczności publicznej, w tym miejsca kultu religijnego, na terenie Unii Europejskiej systematycznie wzrasta. Tylko w ciągu ostatniej dekady w wyniku zamachów terrorystycznych w Europie śmierć poniosło wielu duchownych oraz uczestników uroczystości liturgicznych. Częstotliwość i charakter wydarzeń spowodowały, że budowanie systemu ochrony antyterrorystycznej tych obiektów stało się koniecznością i znormalizowanym elementem polityki bezpieczeństwa wielu państw. W proces tworzenia poziomu bezpieczeństwa miejsc i ludzi włączyła się Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej. Od wielu lat jej eksperci – poprzez opracowywanie i wdrażanie szeregu inicjatyw legislacyjnych, proponowanie rozwiązań w zakresie tzw. dobrych praktyk, finansowanie projektów itp. – zachęcają państwa członkowskie UE do włączania się w proces budowania i wdrażania systemu antyterrorystycznego miejsc kultu religijnego. O ważności zagadnienia świadczy również umieszczenie kwestii ochrony antyterrorystycznej miejsc kultu w strategii bezpieczeństwa UE w latach 2020–2025 jako jednego z priorytetowych zadań. Rezultatem wspomnianych założeń są projekty finansowane przez Komisję Europejską, które – należy mieć nadzieję – usystematyzują kwestie zabezpieczenia europejskich miejsc kultu religijnego. Jak wspomniano na wstępie artykułu, rok 2021 ma wymiar symboliczny, ponieważ właśnie wtedy zapoczątkowane zostały wszelkie działania służące poprawie poziomu bezpieczeństwa terrorystycznego miejsc kultu religijnego, również na obszarze Polski.

Nie pozostając obojętnym na trudne doświadczenia państw UE, na których terytorium doszło do zdarzeń o charakterze terrorystycznym wobec miejsc kultu religijnego, należy kontynuować w naszym kraju dyskusję na temat problematyki związanej z ochroną antyterrorystyczną polskich obiektów sakralnych. Warto zastanowić się nad potrzebą uregulowania w jednym akcie prawnym kwestii bezpieczeństwa terrorystycznego wszystkich polskich miejsc kultu religijnego. Rozstrzygnięcia legislacyjne zawarte w ustawie o ochronie zabytków i opiece nad zabytkami są pewnym rozwiązaniem, jednak ograniczanie ich wyłącznie do obiektów będących zabytkami nie rozwiązuje wspomnianego problemu w sposób kompleksowy. Warto zatem rozważyć powrót do koncepcji proponowanych w 2016 r., kiedy podczas prac nad projektem ustawy o działaniach antyterrorystycznych Ministerstwo Spraw Wewnętrznych postulowało, by w procedowanym dokumencie znalazł

się zapis dotyczący objęcia miejsc kultu religijnego obowiązkowymi planami ochrony. Po krytyce ze strony ekspertów ds. bezpieczeństwa ustawodawca wycofał się z realizacji przedmiotowego założenia. W negatywnych komentarzach podkreślano znaczne – mogące się pojawić – obciążenia finansowe dla administratorów tych miejsc, trudności w implementacji fizycznych i technicznych środków ochrony, w tym przede wszystkim brak podstaw merytorycznych do działania, wynikających z braku rzeczywistych zagrożeń o charakterze terrorystycznym na terytorium RP[55].

Na szczególną uwagę zasługuje również realizacja przez Uniwersytet Łódzki i zaproszonych konsorcjantów pierwszego w naszym kraju projektu służącego ochronie antyterrorystycznej miejsc kultu religijnego finansowanego ze środków Komisji Europejskiej. Należy mieć nadzieję, że dobre praktyki i doświadczenia zebrane w ramach jego realizacji będą służyć poprawie poziomu bezpieczeństwa terrorystycznego tych obiektów. Ponadto dobrym posunięciem byłoby zaproszenie do Polski w 2022 r. ekspertów z Komisji Europejskiej (DG HOME), którzy przygotowują w trakcie autorskich szkoleń (bazując na ww. unijnym podręczniku ds. wsparcia ochrony miejsc kultu religijnego) trenerów ds. zabezpieczenia obiektów sakralnych. Tak przygotowane osoby mogłyby szkolić kaskadowo kolejnych krajowych specjalistów w tym zakresie. W kontekście powyższych wniosków istotne wydaje się również uzyskanie odpowiedzi na pytanie, czy i ewentualnie które z proponowanych lub już istniejących rozwiązań w systemie ochrony antyterrorystycznej miejsc kultu religijnego w Europie można zaimplementować, ulepszyć, zmodyfikować lub dostosować w RP. Przewidywanie zagrożeń, wdrożenie odpowiednio wcześniej właściwych środków służących przeciwdziałaniu im, minimalizowanie ryzyka ich wystąpienia oraz skutków ewentualnego ataku terrorystycznego mogą ocalić ludzkie życie i zdrowie oraz zabezpieczyć obiekt przed ewentualnym uszkodzeniem. Osoby bezpośrednio związane z miejscami kultu religijnego mają prawo czuć się w nich komfortowo i bezpiecznie, a obowiązkiem osób odpowiedzialnych za bezpieczeństwo obiektów sakralnych, zarówno na poziomie narodowym, jak i lokalnym, jest zapewnienie tym osobom i miejscom oczekiwanego komfortu i bezpieczeństwa.

[55] www.pch24.pl/plan-ochrony-dla-kazdego--mswia-stawia-na-profilaktyke-antyterrorystyczna,42810,i.html [dostęp: 14 XII 2021].

Bibliografia

Aleksandrowicz T., *Bieżące zagrożenia, terrorystyczne*, cz. 1 – *Doświadczenia ostatniego dziesięciolecia*, „Przegląd Policyjny" 2017, nr 4, s. 27–47.

Aleksandrowicz T., Jałoszyński K., *Cechy charakterystyczne organizacji terrorystycznych w XXI wieku*, w: *Bezpieczeństwo państwa a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, K. Jałoszyński, T. Aleksandrowicz, K. Wiciak (red.), Szczytno 2016, s. 46–51.

Ginter A., Michalak A., *Komentarz do art. 88*, w: *Ustawa o ochronie zabytków i opiece nad zabytkami. Komentarz*, A. Ginter, A. Michalak (red.), Warszawa 2016, LEX Omega nr 500623.

Izak K., *Nie tylko islam. Ekstremizm i terroryzm religijny*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 183–210.

Liedel K., Piasecka P., *Bezpieczeństwo w czasach terroryzmu. Jak przeżyć zamach terrorystyczny*, Warszawa 2018.

Mazurczak A., *Ochrona przed przestępstwami motywowanymi uprzedzeniami w przepisach prawa polskiego i międzynarodowego*, w: *Przestępstwa motywowane uprzedzeniami. Analiza i zalecenia*, „Biuletyn Rzecznika Praw Obywatelskich" 2017, nr 6, s. 9–13.

Stelmach J., *Kategorie obiektów użyteczności publicznej i stopnie ich ochrony w kontekście zagrożenia współczesnym terroryzmem*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Analiza – Diagnoza – Case study*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (red.), Toruń 2018.

Stelmach J., Kożuszek M., *Założenia i rekomendacje do wykonywania planów ochrony w obiektach podlegających obowiązkowej ochronie*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, t. 4 – *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (red.), Toruń 2019.

Stelmach J., Wiśniewska-Paź B., *Wprowadzenie – rozważania na temat zagrożenia terroryzmem dla obiektów użyteczności publicznej*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, t. 2 – *Metody i narzędzia zamachów vs działania antyterrorystyczne i kontrterrorystyczne*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (red.), Toruń 2018.

Wiśniewska-Paź B., Stelmach J., *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, w: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, t. 4 – *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (red.), Toruń 2019.

Źródła internetowe

European Commission, DG HOME, *EU Quick Guide to support the protection of places of worship*, 2021 r., https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [dostęp: 27 XI 2021].

European Commission, *Protection of Places of Worship*, 2020, https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=696367&utm_source=pps_newsroom&utm_medium=Website&utm_campaign=pps&utm_content=Protection%20of%20Places%20of%20Worship&lang=en [dostęp: 27 XI 2021].

https://actu.fr/grand-est/strasbourg_67482/mosquee-a-strasbourg-l-association-derriere-le-projet-menacee-d-attentats_45450694.html [dostęp: 11 XII 2021].

https://actu.fr/pays-de-la-loire/beille_72031/sarthe-un-camion-fonce-dans-l-eglise-son-chauffeur-s-enfuit-le-maire-lance-un-appel-a-temoins_45259304.html [dostęp: 11 XII 2021].

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034230/ISFP [dostęp: 11 XII 2021].

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/isfp-2020-ag-protect [dostęp: 11 XII 2021].

https://ec.europa.eu/newsroom/pps/newsletter-archives/35274 [dostęp: 11 XII 2021].

https://muslimnews.co.uk/news/islamophobia/france-3-mosques-face-islamophobic-attack/ [dostęp: 11 XII 2021].

https://soarproject.eu/newsletter/ [dostęp: 11 XII 2021].

https://www.bbc.com/news/uk-58935372 [dostęp: 11 XII 2021].

https://www.europe1.fr/faits-divers/un-pretre-assassine-en-vendee-annonce--darmanin-4061489 [dostęp: 11 XII 2021].

https://www.jpost.com/diaspora/antisemitism/teenager-arrested-after-waving--knife-in-front-of-french-jewish-school-684430 [dostęp: 11 XII 2021].

https://www.kath.net/news/76584 [dostęp: 11 XII 2021].

https://www.leprogres.fr/faits-divers-justice/2021/10/10/il-projetait-de-percuter--la-cathedrale-notre-dame-en-avion-un-homme-interpelle [dostęp: 11 XII 2021].

ISF Police, 2020 Call for proposals: ISFP-2020-AG-PROTECT, https://ec.europa.eu/research/participants/data/ref/other_eu_prog/home/wp/call-fiche_isfp--2020-ag-protect_en.pdf [dostęp: 28 XI 2021].

National Counter Terrorism Security Office, *Counter Terrorism Protective Security Advice for Places of Worship,* ACPO 2009, https://www.welhat.gov.uk/media/16407/Crowded-Places-Guidance/pdf/Crowded_Places_Guidance.pdf?m=637242863669130000 [dostęp: 20 XI 2021].

National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/introduction [dostęp: 20 XI 2021].

National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/managing-risk-business-continuity [dostęp: 20 XI 2021].

U.S. Department of Homeland Security, *Houses of Worship Security Practice Guide*, maj 2013, https://www2.illinois.gov/ready/plan/documents/dhs_houses_of_worship_security_practices_guide.pdf [dostęp: 20 XI 2021].

www.pch24.pl/plan-ochrony-dla-kazdego--mswia-stawia-na-profilaktyke-antyterrorystyczna,42810,i.html [dostęp: 14 XII 2021].

Akty prawne

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa,* Bruksela 2020, s. 11–13, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 &cookies=disabled [dostęp: 30 XI 2021].

European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Bruksela 2019, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [dostęp: 16 XI 2021].

Ustawa z 23 lipca 2003 r. o ochronie zabytków i opiece na zabytkami (t.j.: DzU z 2021 r. poz. 710).

Rozporządzenie Ministra Kultury z 25 sierpnia 2004 r. w sprawie organizacji i sposobu ochrony zabytków na wypadek konfliktu zbrojnego i sytuacji kryzysowej (DzU z 2004 r. nr 212 poz. 2153).

DOI: 10.4467/27204383TER.22.008.15424

CENTRUM PREWENCJI TERRORYSTYCZNEJ

nowa jednostka pionu antyterrorystycznego Agencji Bezpieczeństwa Wewnętrznego

Centrum Prewencji Terrorystycznej (CPT) ABW jest jednostką typowo szkoleniową. Jej aktywność jest oparta na zapisach ustawy o działaniach antyterrorystycznych z 2016 r. i skoncentrowana na pozostających poza sferą działania Centrum Antyterrorystycznego ABW forach współpracy krajowej i międzynarodowej, które służą do pozyskiwania i wymiany wiedzy oraz dobrych praktyk w zakresie szkoleń zwiększających świadomość antyterrorystyczną instytucji i obywateli RP w kraju i za granicą.

Jawna działalność CPT ABW związana z inicjatywami szkoleniowymi dla społeczeństwa ułatwia uczestniczenie w krajowych i międzynarodowych konferencjach, warsztatach i innych formach wymiany informacji, które łączą środowiska akademickie oraz praktyków z różnych krajów, oraz pozwala na swobodne operowanie w celu uzyskania jak najlepszych rezultatów aktywności dydaktycznej.

W 2021 r. CPT ABW kontynuowało prowadzenie szkoleń antyterrorystycznych z zakresu profilaktyki i prewencji terrorystycznej na trzech płaszczyznach: bezpośrednio przez trenerów Centrum, online z udziałem ekspertów zewnętrznych oraz przez platformę e-learningową. Szkolenia te opierały się na koncepcji wypracowanej w wyniku współpracy zagranicznych i krajowych przedstawicieli sektora akademickiego, służb specjalnych oraz instytucji unijnych. Odbiorcami tych szkoleń były inne służby, ministerstwa, urzędy centralne, instytucje i agencje rządowe, uczelnie wyższe oraz podmioty gospodarcze mające kluczowe znaczenie z punktu widzenia bezpieczeństwa Polski. W ramach bezpośrednich spotkań przeszkolono ponad 3 tys. osób.

Z uwagi na bardzo duże zainteresowanie podmiotów polskiej administracji publicznej oraz sektora prywatnego, które w ciągu ubiegłego roku licznie zwracały się z prośbą o przeszkolenie swoich pracowników, jak również ze względu na brak możliwości bezpośredniego spotkania z tymi osobami, CPT ABW przeszkoliło w 2021 r. ponad 50 tys. osób w ramach kursu e-learningowego z zakresu prewencji terrorystycznej. Kurs ten jest dostępny na stronie internetowej przeznaczonej dla pracowników administracji państwowej oraz funkcjonariuszy publicznych.

Równolegle CPT ABW prowadziło aktywną współpracę na poziomie krajowym, uczestnicząc w konferencjach i seminariach tematycznych zorganizowanych w porozumieniu m.in. z Uniwersytetem Wrocławskim (Centrum Studiów i Edukacji na Rzecz Bezpieczeństwa) oraz Urzędem Lotnictwa Cywilnego, jak również podejmowało własne inicjatywy, m.in. związane z podnoszeniem poziomu wiedzy w zakresie reagowania na zagrożenia o charakterze terrorystycznym w obiektach mających status infrastruktury krytycznej.

Wnioski płynące ze wspomnianych działań będą służyć efektywniejszemu pozyskiwaniu i wydatkowaniu finansowania zewnętrznego projektów oraz przedsięwzięć dotyczących bezpieczeństwa CBRN i IED promowanych na szczeblu europejskim, a także wspierać nawiązywanie i rozwijanie kontaktów z potencjalnymi parterami zainteresowanymi współpracą projektową z ABW.

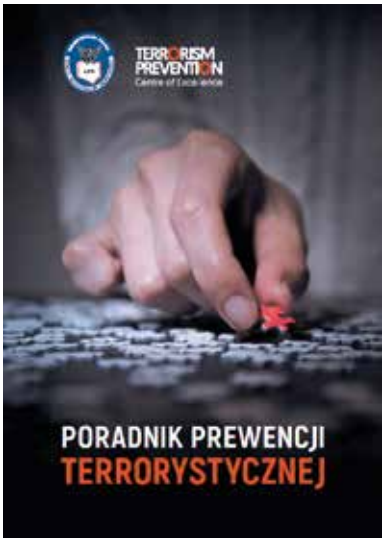
Ponadto, na bazie pozytywnego odbioru Kampanii Społecznej 4U! (Uważaj!, Uciekaj!, Ukryj się!, Udaremnij atak!) zainaugurowanej w 2019 r., CPT ABW we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji zaprezentowało w listopadzie 2021 r. ujednoliconą procedurę informowania w sytuacji zaistnienia zdarzenia o charakterze terrorystycznym z udziałem uzbrojonego sprawcy. Rekomendowany tryb udzielania informacji operatorom wojewódzkich centrów powiadamiania ratunkowego jest istotnym krokiem w kierunku wypracowania jednolitej kultury bezpieczeństwa w systemie zgłaszania alarmowego związanego z ewentualnym incydentem terrorystycznym (obejmującym całe terytorium RP).

Wspomniane inicjatywy realizowane na poziomie krajowym bazowały na aktywności CPT ABW za granicą, zwłaszcza w ramach gremiów Unii Europejskiej (Grupy Roboczej UE ds. Terroryzmu, Komitetu Sterującego ds. Radykalizacji, Sieci ekspertów skupiającej decydentów w zakresie przepisów prawnych dot. radykalizacji, Sieci praktyków uświadamiających na temat radykalizacji, Europejskiego Forum Internetowego) oraz innych form współpracy pomiędzy państwami członkowskimi UE opartej na wspólnych celach projektowej kooperacji, m.in. w obszarach przeciwdziałania radykalizacji w placówkach penitencjarnych oraz szkołach.

Dzięki aktywności CPT ABW 27 października 2021 r. zostało podpisane przez Szefa Agencji Bezpieczeństwa Wewnętrznego płk. Krzysztofa Wacławka oraz Dyrektora Generalnego Służby Więziennej gen. Jacka Kitlińskiego porozumienie o współpracy naukowo-dydaktycznej w zakresie przeciwdziałania radykalizacji i zagrożeniom terrorystycznym. CPT ABW aktywnie uczestniczyło również w pracach Organizacji Bezpieczeństwa i Współpracy w Europie oraz Komitetu Sterującego OBWE ds. Przeciwdziałania Terroryzmowi. Z kolei podejmowane w Polsce działania dotyczące bezpieczeństwa lotniczego nie byłyby możliwe bez współpracy z Europejską Komisją Lotnictwa Cywilnego (ECAC) oraz Organizacją Międzynarodowego Lotnictwa Cywilnego (ICAO).

Jednocześnie CPT ABW prowadziło współpracę bilateralną z partnerami z krajów UE oraz pozaeuropejskich, jak również uczestniczyło w projektach współfinansowanych z funduszy zewnętrznych, takich jak: „EU-HYBNET – Wzmocnienie ogólnoeuropejskiej sieci przeciwdziałania zagrożeniom hybrydowym", „PREVENT PCP – Przedkomercyjne zamówienia innowacyjnych i zaawansowanych systemów wspierających bezpieczeństwo w transporcie publicznym", „INDEED – Model oparty na dowodach do oceny zapobiegania radykalizacji", „Sprawniejsze rozpoznawanie zagrożeń asymetrycznych – tendencje, wskaźniki,

Działalność CPT ABW w 2021 r. w liczbach	
Szkolenia bezpośrednie	103
Osoby przeszkolone bezpośrednio	3 150
Osoby przeszkolone online	53 405
Spotkania z partnerami zagranicznymi w Polsce	4
Spotkania z partnerami zagranicznymi za granicą	3
Spotkania międzynarodowe online	51



zależności" oraz „Podnoszenie kompetencji służb bezpieczeństwa państwa, pracowników administracji publicznej i ośrodków naukowo-badawczych oraz rozwój ich współpracy w obszarze bezpieczeństwa narodowego". W ramach tego ostatniego projektu powstał *Poradnik prewencji terrorystycznej* (w wersji papierowej oraz elektronicznej), przekazywany wybranym przedstawicielom administracji publicznej oraz podmiotom współpracującym z CPT ABW. Opracowanie jest dostępne w polskiej oraz angielskiej wersji językowej i stanowi kompendialne podsumowanie pięciomodułowego programu szkoleniowego, który został przygotowany przez ekspertów zewnętrznych w 2020 r. w ramach projektu unijnego PO WER („Program Operacyjny Wiedza Edukacja Rozwój").

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.

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 inż. Jędrzej Łukasiewicz – adiunkt w Zakładzie Lotnictwa Wydziału Inżynierii Lądowej i Transportu Politechniki Poznańskiej oraz instruktor pilotażu bezzałogowych statków powietrznych w ośrodku szkolenia Politechniki Poznańskiej. Uczestnik gremiów eksperckich na poziomie unijnym (DG MOVE, DG HOME) i krajowym, międzyresortowym

ds. bezpieczeństwa infrastruktury krytycznej oraz budowania odporności na zagrożenia ze strony bezzałogowych statków powietrznych.

Dr Aleksander Olech – dyrektor Programu Bezpieczeństwa Europejskiego w Instytucie Nowej Europy. Absolwent Europejskiej Akademii Dyplomacji. Doświadczenie badawcze zdobywał m.in. na Université Jean Moulin Lyon 3, w Instytucie Stosunków Międzynarodowych w Pradze, Instytucie Wspierania Pokoju i Zarządzania Konfliktami w Wiedniu, NATO Energy Security Centre of Excellence w Wilnie oraz Baltic Defence College w Tartu. Stypendysta OSCE & UNODA Peace and Security, NATO 2030 Global Fellowship oraz Fundacji im. Kazimierza Pułaskiego.

Dr Anna Rożej – 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.

Ppłk Artur Sybicki – funkcjonariusz Centrum Prewencji Terrorystycznej ABW odpowiedzialny za organizację i prowadzenie szkoleń antyterrorystycznych dla przedstawicieli polskiej administracji państwowej. Od 2005 r. zajmuje się zagadnieniami związanymi z przeciwdziałaniem zdarzeniom o charakterze terrorystycznym na terytorium RP.