TERRORYZM

studia
analizy
prewencja

TERRORISM
PREVENTION
Centre of Excellence

CENTRALNY OŚRODEK
SZKOLENIA I EDUKACJI ABW

Zespół redakcyjny dr Damian Szlachter (redaktor naczelny)
Agnieszka Dębska (sekretarz redakcji, skład)
Aleksandra Dąbała, Aneta Olkowska,
Monika Sikora (redakcja językowa, korekta)

Projekt okładki Aleksandra Bednarczyk

ISSN 2720-4383
e-ISSN 2720-6351

Punkty MEiN: **20**

Artykuły zamieszczone w czasopiśmie są recenzowane

Artykuły wyrażają poglądy autorów

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

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

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

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

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

Numer zamknięto i oddano do druku we wrześniu 2023 r.

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

SPIS TREŚCI

PRACE KONKURSOWE

INNE

Szanowni Państwo!

Dokładamy starań, aby czasopismo „Terroryzm – studia, analizy, prewencja" (T-SAP) odpowiadało oczekiwaniom jego odbiorców – przedstawicieli całej wspólnoty antyterrorystycznej RP oraz środowiska badaczy zjawiska terroryzmu, a także innych osób zainteresowanych jednym z największych wyzwań związanych z bezpieczeństwem krajów Unii Europejskiej i NATO. Zależy nam przede wszystkim na tym, aby poruszane tematy były ważkie i aktualne.

Do takich z pewnością należą zagadnienia dotyczące sztucznej inteligencji. W toczącej się debacie publicznej wiele uwagi poświęca się przede wszystkim zagrożeniom, jakie wiążą się z jej wykorzystaniem. Rzeczywiście są one poważnym problemem. Nie zapominajmy jednak, że dzięki AI zyskaliśmy zupełnie nowe możliwości w zakresie rozwoju wiedzy i wdrażania rozwiązań usprawniających różne dziedziny życia. Sztuczna inteligencja może nam między innymi pomóc lepiej i skuteczniej zadbać o bezpieczeństwo. W jaki sposób? Na przykład, jak wskazują autorzy artykułów, przez wykorzystanie algorytmów AI do zwiększania odporności infrastruktury krytycznej na zagrożenia terrorystyczne lub do predykcji ofiar tego rodzaju ataków.

Współcześnie mamy również do czynienia z dynamicznie rozwijającym się rynkiem walut wirtualnych. W tym numerze mogą Państwo przeczytać o ich wykorzystywaniu do finansowania działalności przestępczej, w tym o charakterze terrorystycznym. Autorzy tekstu analizują to zjawisko od strony uregulowań prawnych i możliwości przeciwdziałania mu przez organy ścigania i ochrony prawa.

Pandemia COVID-19, z którą jeszcze do niedawna musieliśmy się mierzyć, skupiła naszą uwagę na zagadnieniach związanych ze zdrowiem. Na szerszym forum rzadko poruszano temat bezpieczeństwa żywności i agroterroryzmu z wykorzystaniem czynników biologicznych, a ma on ścisły związek z dobrostanem zdrowotnym ludzi. Autor jednego z artykułów analizuje aktualne zagrożenia w obszarze bezpieczeństwa biologicznego i żywnościowego – spotęgowane nie tylko sytuacją epidemiologiczną, lecz także wojną toczącą się w Ukrainie, która jest w ścisłej czołówce światowych producentów żywności.

Niestabilna sytuacja geopolityczna na świecie zwiększa ryzyko ataków o charakterze terrorystycznym, w tym wymierzonych w obiekty dyplomatyczne. O tym, w jaki sposób się je chroni za pomocą zabezpieczeń strefowych, pisze autorka artykułu poświęconego architekturze budynków 22 ambasad znajdujących się w Warszawie, Berlinie i Rzymie.

Od tego numeru T-SAP chcielibyśmy zaproponować Państwu nową, dodatkową formułę. W jej ramach będą się ukazywać teksty niebędące stricte opracowaniami naukowymi. Naszym celem jest stworzenie warunków sprzyjających merytorycznej dyskusji w zakresie przeciwdziałania zagrożeniom o charakterze terrorystycznym, zwalczania ich i zapobiegania im również z punktu widzenia praktyków, z uwzględnieniem ich doświadczeń i opinii. W tym wydaniu publikujemy esej o roli działań kontrwywiadowczych. Jego autor wiele lat poświęcił służbie na rzecz polskiej wspólnoty antyterrorystycznej. Kolejne prezentowane materiały opracowali unijni eksperci ds. terroryzmu. Opisane zostały w nich dwie ważne inicjatywy antyterrorystyczne prowadzone przez Komisję Europejską – EU High Risk Security Network oraz EU Protective Security Advisors. Z myślą o wymianie doświadczeń na poziomie międzynarodowym przeprowadziliśmy wywiad z ekspertem sztokholmskiej policji na temat sposobów budowania w Szwecji odporności na ataki terrorystyczne. W tej części czasopisma publikujemy ponadto komentarz eksperta z amerykańskiego Uniwersytetu Jerzego Waszyngtona, jednego z najbardziej znanych badaczy zagrożeń terrorystycznych, do wyników badań ankietowych poświęconych terroryzmowi

w Polsce i kierunkom jego rozwoju, przeprowadzonych przez ABW w 2022 r.

O nowościach już napisałem. Teraz tradycyjnie chciałbym zachęcić do lektury 4. numeru T-SAP, w tym do zapoznania się z recenzjami dwóch ciekawych pozycji książkowych. Wyrażam przy tym nadzieję, że prezentowane treści spotkają się z Państwa zainteresowaniem i przyczynią się do rozwoju oraz doskonalenia systemu antyterrorystycznego RP na każdym jego poziomie – operacyjnym, taktycznym i strategicznym.

Redaktor naczelny
dr Damian Szlachter

ARTYKUŁY

https://doi.org/10.4467/27204383TER.23.017.18319

https://orcid.org/0000-0002-5288-0324
https://orcid.org/0000-0002-3907-2242
https://orcid.org/0000-0001-6390-1402

TOMASZ P. MICHALAK
MICHAŁ T. GODZISZEWSKI
ANDRZEJ NAGÓRKO

Ochrona infrastruktury krytycznej z wykorzystaniem teorii gier, technik optymalizacji i algorytmów sztucznej inteligencji

Abstrakt

Aktualna sytuacja geopolityczna doprowadziła do wzrostu zagrożeń, z jakimi muszą się mierzyć podmioty odpowiedzialne za bezpieczeństwo w Polsce i Europie. Jednak pomimo zwiększenia czujności, poziomu nakładów i inwestycji zasoby ochrony wciąż pozostają ograniczone w stosunku do dynamicznie rosnących potrzeb. Taka sytuacja sprawia, że stała ochrona każdego potencjalnego celu ataku jest po prostu nieosiągalna. Kluczowe staje się zatem efektywne wykorzystanie już istniejących zasobów ochrony. Przedmiotem niniejszego artykułu jest omówienie zaawansowanych metod, które ułatwiają zautomatyzowane podejmowanie decyzji w zakresie alokacji zasobów bezpieczeństwa. Tego rodzaju metody obejmują wykorzystanie sztucznej inteligencji,

Słowa kluczowe:

optymalizacja,
gry bezpieczeństwa,
sztuczna inteligencja,
infrastruktura krytyczna

teorii gier oraz technik optymalizacji. Wdrożenia podobnych rozwiązań w zakresie ochrony wybranych obiektów infrastruktury krytycznej w Stanach Zjednoczonych Ameryki dowodzą ich skuteczności. W artykule został przedstawiony również skrócony przegląd tego obszaru badań oraz rozwiązania i oprogramowanie opracowane przez zespół „AI dla bezpieczeństwa" utworzony w ramach instytutu badawczego IDEAS NCBR w celu ochrony infrastruktury krytycznej w Polsce i Europie.

Wprowadzenie

Międzynarodowe lotnisko w Los Angeles (ang. Los Angeles International Airport, LAX) jest jednym z największych i najbardziej ruchliwych portów lotniczych na świecie. Stanowi ważny węzeł komunikacyjny dla tej aglomeracji i jej okolic. Pod względem liczby pasażerów jest ok. czterokrotnie większe od Lotniska Chopina w Warszawie – największego polskiego portu lotniczego. Lotnisko LAX zajmuje rozległy obszar i ma cztery równoległe pasy startowe oraz dziewięć terminali, z których każdy obsługuje różne linie lotnicze i miejsca docelowe. Największym z nich jest Tom Bradley International Terminal przeznaczony do obsługi lotów międzynarodowych. Centralny obszar terminalu jest jednocześnie środkowym węzłem ciągów komunikacyjnych łączących wszystkie terminale. Obejmuje on złożoną sieć dróg, parkingów oraz usług transportowych, takich jak transport wahadłowy i taksówki, których celem jest ułatwienie pasażerom poruszania się po lotnisku.

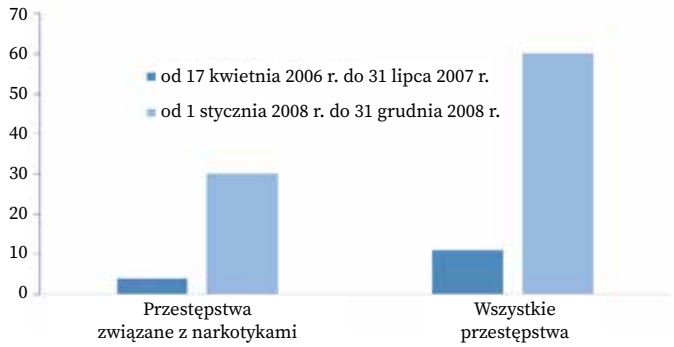
Z uwagi na znaczenie i rozmiar LAX jest jednym z głównych obiektów na Zachodnim Wybrzeżu USA, które są zagrożone potencjalnym atakiem. Ochrona tak złożonego i rozległego obiektu rodzi konieczność zachowania równowagi między środkami bezpieczeństwa a wydajnością operacyjną. Niestety, całodobowa ochrona każdego ważnego obszaru jest niewykonalna ze względu na ograniczone zasoby bezpieczeństwa, którymi dysponuje lotnisko. Jako przykład można wskazać psy służbowe o konkretnej specjalizacji, np. psy mające umiejętność wykrywania materiałów wybuchowych lub narkotyków. Ich liczba jest zawsze za mała w stosunku do potrzeb i stanowczo za mała, aby można było patrolować przez cały czas

wszystkie newralgiczne punkty lotniska. W praktyce oznacza to, że zapewnienie stałej obecności patroli z psami służbowymi na każdym terminalu w LAX jest po prostu niemożliwe. Mimo to patrole z psami szkolonymi do wykrywania narkotyków okazały się w 2008 r. znacznie skuteczniejsze niż w latach poprzednich. Przez 15 miesięcy, tj. od kwietnia 2006 r. do lipca 2007 r., odnotowano tylko cztery przestępstwa związane z narkotykami, a w ciągu 2008 r. – 30 takich czynów.

U źródeł tak dużej poprawy wykrywalności leży system ARMOR (ang. *Assistant for Randomized Monitoring Over Routes*, pol. asystent randomizowanego monitorowania ciągów komunikacyjnych). Jest to innowacyjne narzędzie programistyczne opracowane przez Milinda Tambego i współpracowników z Uniwersytetu Południowej Kalifornii (ang. University of Southern California)[1], w ramach pierwszego Uniwersyteckiego Centrum Doskonałości wspieranego przez Departament Bezpieczeństwa Wewnętrznego (ang. University Center of Excellence at the Department of Homeland Security). Głównym celem systemu ARMOR jest udzielanie pracownikom ochrony wsparcia, aby mogli podejmować lepsze i bardziej efektywne decyzje dzięki zoptymalizowaniu użycia dostępnych zasobów z uwzględnieniem posiadanej oceny ryzyka. W tym celu ARMOR wykorzystuje sztuczną inteligencję (ang. *Artificial Intelligence*, AI), teorię gier oraz techniki optymalizacji. System pozwala siłom bezpieczeństwa na rozmieszczenie ich ograniczonych zasobów w najbardziej efektywny sposób i osiągnięcie maksymalnej skuteczności. Utrudnia to przeciwnikowi takie zaprojektowanie ataku, aby przedostać się przez istniejące systemy bezpieczeństwa.

Wdrożenie systemu ARMOR na lotnisku LAX zaowocowało poprawą poziomu ochrony, zwiększeniem wydajności alokacji zasobów oraz ograniczyło możliwości potencjalnych agresorów. Jego wprowadzenie spowodowało ponadtrzykrotny wzrost liczby wszystkich wykrytych przestępstw (wykres). System ten jest przykładem tego, jak zaawansowana technologia i podejścia oparte na sztucznej inteligencji mogą przyczynić się do zwiększenia poziomu bezpieczeństwa lotnisk oraz przebywających na nich pasażerów.

[1] J. Pita i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57. https://doi.org/10.1609/aimag.v30i1.2173.



Wykres. Liczba wykrytych przestępstw, w tym tych związanych z narkotykami, na lotnisku LAX w Los Angeles w okresie 15 miesięcy przed wprowadzeniem (ciemne słupki) i 12 miesięcy po wprowadzeniu (jasne słupki) systemu ARMOR.

Źródło: opracowanie własne na podstawie: J. Pita i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57.

Sukces, jaki przyniosło zastosowanie ARMOR, wzbudził duże zainteresowanie. Kilka systemów opartych na podobnych zasadach zostało wdrożonych w USA w celu ochrony innych obiektów infrastruktury krytycznej. Są to:

- IRIS[2] – służący do optymalizacji tras i harmonogramu ochrony w ramach programu U.S. Air Marshals (pracownicy służb bezpieczeństwa zatrudnieni na pokładach samolotów);
- PROTECT[3] – służący do optymalizacji bezpieczeństwa portów i wybrzeży w Bostonie i Nowym Jorku;
- TRUSTS[4] – stworzony w celu zapobiegania wyłudzeniom przejazdów i przeznaczony dla systemu transportu kolejowego w Los Angeles.

[2] J. Tsai i in., *Iris – a tool for strategic security allocation in transportation networks*, w: *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2009), s. 37–44 (materiały z poszczególnych konferencji AAMAS są dostępne na: https://dl.acm.org/conference/aamas/proceedings – dop. red.).

[3] E. Shieh i in., *Protect: A deployed game theoretic system to protect the ports of the United States*, w: *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2012), t. 1, s. 13–20.

[4] Z. Yin i in., *Trusts: Scheduling randomized patrols for fare inspection in transit systems*, w: *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence* (AAAI 2012), t. 26, nr 2, s. 2348–2355 (materiały z poszczególnych konferencji i sympozjów AAAI są dostępne na: https://aaai.org/aaai-publications/aaai-conference-proceedings/ – dop. red.).

Wykorzystanie systemu ARMOR jest zalecane również w obszarze cyberbezpieczeństwa[5]. Rośnie także liczba jego zastosowań w sferze cywilnej, np. w ochronie zagrożonych gatunków w parkach narodowych (systemy PAWS[6] i MIDAS[7]). We wszystkich przedstawionych przypadkach znacznie zwiększono poziom bezpieczeństwa, jednak nie przez wprowadzenie dodatkowych środków bezpieczeństwa, a dzięki lepszemu wykorzystaniu już istniejących zasobów.

Jest to ważna lekcja dla Europy, a zwłaszcza dla Polski. Z uwagi na niedawne wydarzenia geopolityczne, przede wszystkim rosyjską pełnoskalową inwazję na Ukrainę w lutym 2022 r., rosną obawy dotyczące bezpieczeństwa infrastruktury. Europa doświadczyła już kilku takich ataków[8]. Z tego względu pytaniem, które należy sobie zadać, nie jest to, czy kolejne ataki nastąpią, lecz to, kiedy do nich dojdzie.

Niestety, problem ochrony przed atakami pogłębia się ze względu na poziom zaawansowania technologicznego infrastruktury krytycznej. Nowoczesne technologie komunikacyjne, obliczeniowe i kontrolne poprawiają wydajność, ale jednocześnie zwiększają poziom skomplikowania istniejących systemów, jak również ich podatność na celowe ataki i przypadkowe awarie. Tego rodzaju ataki mogą przybierać różne formy, mieć różne nasilenie i skalę – od zamachów terrorystycznych wymierzonych w infrastrukturę lokalną po poważne ataki kinetyczne w czasie wojny, takie, do jakich dochodzi podczas trwającej od 2022 r. rosyjskiej inwazji na Ukrainę. Nowe technologie, takie jak drony, również zwiększają możliwości potencjalnych napastników.

W obliczu ewoluującego i rozszerzającego się katalogu zagrożeń, pomimo zwiększonego zainteresowania bezpieczeństwem infrastruktury i nowych inwestycji w tej sferze, zasoby bezpieczeństwa pozostaną ograniczone. To uniemożliwia zapewnienie stałej ochrony wszystkich obiektów.

---

5 Y. Zhang, P. Malacaria, *Bayesian Stackelberg games for cyber-security decision support*, „Decision Support Systems" 2021, t. 148, art. 113599. https://doi.org/10.1016/j.dss.2021.113599.

6 R. Yang i in., *Adaptive resource allocation for wildlife protection against illegal poachers*, w: *Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2014), s. 453–460.

7 W. Haskell i in., *Robust protection of fisheries with COmPASS*, w: *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence* (AAAI 2014), t. 28, nr 2, s. 2978–2983.

8 Na przykład celowe przecięcie 8 października 2022 r. dwóch światłowodów systemu komunikacji Deutsche Bahn, które wstrzymało ruch kolejowy w północnych Niemczech na ok. trzy godziny.

W związku z tym strategiczna alokacja zasobów bezpieczeństwa staje się koniecznością. Przykład lotniska LAX oraz inne wspomniane wcześniej przykłady z USA pokazują, że takie dobrze zaprojektowane, strategiczne podejmowanie decyzji jest niezwykle korzystne, a co najważniejsze – znacznie poprawia bezpieczeństwo.

W niniejszym artykule omówiono podstawy zaawansowanych metod ochrony infrastruktury krytycznej, dokonano krótkiego przeglądu badań prowadzonych w tym obszarze, a następnie przedstawiono rozwiązania i oprogramowanie opracowywane przez zespół „AI dla bezpieczeństwa" z instytutu badawczego IDEAS NCBR.

Gry bezpieczeństwa – obrońca kontra atakujący

Teoria gier bada interakcje pomiędzy inteligentnymi podmiotami, takimi jak jednostki, firmy czy państwa. W rozważanym kontekście te podmioty mogą reprezentować „obrońców", np. siły bezpieczeństwa, policję, wojsko, oraz „napastników", np. przestępców, terrorystów czy aktorów państwowych. Podejścia oparte na teorii gier pomagają zrozumieć, w jaki sposób strony wchodzą w interakcje, przy założeniu, że postępują racjonalnie (co najmniej w pewnym stopniu), mają zdolność przewidywania i mogą reagować na wrogie działania. Dzięki wykorzystaniu teorii gier można opracować strategię efektywnej dystrybucji ograniczonych zasobów bezpieczeństwa w celu ochrony infrastruktury krytycznej, przy czym to podejście pozwala uwzględnić znaczenie różnych celów oraz sposób, w jaki przeciwnicy mogą reagować na określone strategie ochrony.

Gra niekooperacyjna jest definiowana przez zbiór graczy, zbiór strategii dla każdego gracza i funkcję użyteczności, która przypisuje każdemu graczowi wypłatę dla każdej kombinacji strategii. Każdej grze towarzyszą zasady, np. taka, zgodnie z którą gracze poruszają się jednocześnie lub sekwencyjnie.

W tabeli 1 przedstawiono przykładową grę opisaną w publikacji Pity i in.[9] W tym przypadku przedstawiono dwóch graczy, z których każdy ma dwie strategie do wyboru: $\{A,B\}$ oraz odpowiednio $\{C,D\}$. Wartości funkcji użyteczności są określone przez pary liczb wskazane w macierzy, w której każda komórka odpowiada danej kombinacji strategii. Dla przykładu, jeżeli

[9] J. Pita i in., *Using game theory for Los Angeles Airport…*

gracz 1 stosuje strategię *A*, gracz 2 stosuje strategię *C*, gracz 1 otrzymuje wypłatę 2, a gracz 2 otrzymuje wypłatę 1.

W niektórych przypadkach istnieje możliwość określenia, w jaki sposób racjonalni gracze (gdzie racjonalność jest eksplikowana za pomocą ścisłej matematycznej formuły) faktycznie graliby w grę, uwzględniając jej zasady. Tego rodzaju kombinację strategii graczy nazywa się równowagą gry. Niewątpliwie najbardziej rozpowszechnioną koncepcją równowagi jest równowaga Nasha (ang. *Nash equilibrium*). Kombinacja strategii będzie stanowiła równowagę Nasha, w przypadku gdy żaden z graczy nie będzie dążył do zmiany swojej strategii, przy założeniu, że strategie wybrane przez przeciwników pozostaną niezmienione. Na przykład kombinacja strategii przedstawiona w tabeli 1 (*A*,*D*) nie może zostać określona jako równowaga Nasha, gdyż gracz 2 chciałby zmienić swoją strategię z *D* na *C*, przy założeniu, że gracz 1 trzyma się strategii *A*. I odwrotnie, kombinacja strategii (*A*,*C*) będzie traktowana jako równowaga w rozumieniu Nasha, ponieważ dla gracza 1 najlepszą strategią będzie *A*, w przypadku gdy gracz 2 działa na zasadzie *C*, a dla gracza 2 najlepszą strategią będzie *C*, jeśli gracz 1 gra *A*.

Tabela 1. Macierz wypłat dla przykładowej gry.

		Gracz 2	
		C	*D*
Gracz 1	*A*	(2,1)	(4,0)
	B	(1,0)	(3,2)

Źródło: J. Pita i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57.

W ramach gry niekooperacyjnej gracze nie muszą się ograniczać do pojedynczych strategii. Zamiast wybrać jedną strategię z pewnością (tj. z prawdopodobieństwem równym 1), gracz może wybrać jedną strategię z określonym (niezerowym i niestuprocentowym) prawdopodobieństwem lub inną strategię z innym (lub takim samym) prawdopodobieństwem (także niezerowym i niestuprocentowym) itd. Innymi słowy gracze mogą przypisać prawdopodobieństwo każdej dostępnej strategii. Na przykład gracz 1 może wybrać strategię *A* z określonym prawdopodobieństwem, oznaczonym jako *p*, oraz strategię *B* z prawdopodobieństwem 1 – *p*. Analogicznie, gracz 2 może przypisać prawdopodobieństwa do strategii *C* oraz *D*. Stosując powyższe tzw. strategie mieszane, gracze wprowadzają element losowości

do własnego procesu decyzyjnego. Pojęcie równowagi Nasha rozszerza się także do gier w strategiach mieszanych.

Rozważmy grę z macierzą wypłat określoną w tabeli 2.

Tabela 2. Przykład macierzy wypłat dla gry bez zachowania równowagi Nasha w przypadku przyjęcia niezmienionych strategii oraz z zachowaniem równowagi Nasha w przypadku strategii mieszanych.

		Gracz 2	
		C	*D*
Gracz 1	*A*	(2,1)	(1,2)
	B	(1,2)	(3,1)

W niniejszej grze nie istnieje równowaga Nasha w strategiach czystych, ponieważ każdy profil strategii charakteryzuje się tym, że któryś gracz – przy ustaleniu strategii drugiego gracza – osiągałby wyższą wypłatę, gdyby zmienił swoją strategię. Istnieje jednak równowaga Nasha w strategiach mieszanych:

- strategia mieszana gracza 1: *A* z prawdopodobieństwem $\frac{1}{2}$, *B* z prawdopodobieństwem $\frac{1}{2}$;
- strategia mieszana gracza 2: *C* z prawdopodobieństwem $\frac{2}{3}$, *D* z prawdopodobieństwem $\frac{1}{3}$.

Oczekiwana wypłata dla gracza 1 w stanie równowagi wynosi:

$$\frac{1}{2}\times\frac{2}{3}\times 2+\frac{1}{2}\times\frac{1}{3}\times 1+\frac{1}{2}\times\frac{2}{3}\times 1+\frac{1}{2}\times\frac{1}{3}\times 3=\frac{5}{3}$$

Oczekiwana wypłata dla gracza 2 wynosi:

$$\frac{1}{2}\times\frac{2}{3}\times 1+\frac{1}{2}\times\frac{1}{3}\times 2+\frac{1}{2}\times\frac{2}{3}\times 2+\frac{1}{2}\times\frac{1}{3}\times 1=\frac{3}{2}$$

Powyższy model ma uproszczony charakter. Zwłaszcza w przypadku ochrony infrastruktury krytycznej można zakładać, że gracze nie będą poruszali się jednocześnie. Wynika to z tego, że atakujący może mieć możliwość obserwowania taktyki obronnej (strategii) stosowanej przez obrońcę. W celu rozwiązania tego problemu zostanie rozważony model ekonomiczny zaproponowany przez Heinricha Stackelberga[10], w którym gra toczy się pomiędzy dwoma graczami – liderem i śledzącym. To oznacza, że w przeciwieństwie do poprzedniego przykładu gra Stackelberga jest rozgrywana

[10] H. von Stackelberg, *Marktform und Gleichgewicht*, J. Springer 1934.

w trybie ruchów następujących po sobie sekwencyjnie, a nie wykonywanych jednocześnie. W takim przypadku lider najpierw wybiera strategię, a jego wybór jest obserwowany przez śledzącego, który następnie odpowiednio określa swój własny ruch.

Na model Stackelberga zwrócono szczególną uwagę w aspekcie zastosowań w sferze bezpieczeństwa, ze względu na możliwość uchwycenia za jego pomocą dynamiki interakcji na linii obrońca–atakujący. W tym kontekście gry Stackelberga często są nazywane grami bezpieczeństwa.

Należy wyróżnić następujące własności tego modelu:

- obrońca, który w grze Stackelberga przyjmuje rolę lidera, przydziela ograniczone zasoby bezpieczeństwa do ochrony wyznaczonego zestawu celów. Uznając, że przeciwnicy mają zdolność obserwowania strategii obronnych i wykorzystywania zaobserwowanych wzorców, obrońca w sposób naturalny wybiera strategię mieszaną (losową). Na przykład w przypadku lotniska LAX kadra kierownicza odpowiedzialna za psy patrolowe określała częstotliwość oraz rodzaj patrolu prowadzonego w każdym terminalu w danym tygodniu. Innymi słowy ustalała rozkład prawdopodobieństwa dla każdego typu patrolu we wszystkich terminalach;
- atakujący, działając w grze Stackelberga jako śledzący, obserwuje próbkę z wybranej przez obrońcę strategii, tj. próbkę z rozkładów prawdopodobieństwa odpowiadających wybranej strategii mieszanej. Przyjęcie takiego założenia powoduje wdrożenie ostrożnego i realistycznego scenariusza, w którym zakłada się, że napastnik jest inteligentny i przed opracowaniem i przeprowadzeniem ataku bada infrastrukturę krytyczną oraz jej ochronę;
- po uzyskaniu wiedzy o prawdopodobieństwach wybranych przez broniącego napastnik strategicznie wybiera optymalny dla siebie sposób działania, a następnie odpowiednio wykonuje swój ruch.

Należy podkreślić, że atakujący ma możliwość obserwowania rozkładu prawdopodobieństwa wybranego przez obrońcę, nie ma natomiast możliwości prześledzenia faktycznego ruchu. Dla zilustrowania podanego przykładu można wskazać scenariusz z udziałem amerykańskiej straży przybrzeżnej (ang. United States Coast Guard, USCG) odpowiedzialnej za patrolowanie Zatoki Meksykańskiej w celu zwalczania przemytu narkotyków za pomocą łodzi. Przemytnicy mogą obserwować częstotliwość patroli na określonych obszarach morskich oraz to, jak często łodzie patrolowe zmieniają swój kurs. To oznacza, że atakujący znają rozkład

prawdopodobieństwa. Niemniej jednak nie są w stanie przewidzieć, czy łódź patrolowa w danym momencie zmieni kurs czy też nie. W związku z tym nie mogą czekać, aż łódź patrolowa odpłynie, ponieważ istnieje niezerowe prawdopodobieństwo, że może natychmiast powrócić. Trzeba w tym miejscu ponownie wspomnieć o opartym na grze Stackelberga systemie PROTECT, który został wprowadzony przez USCG w celu zwiększenia bezpieczeństwa portów i wybrzeży (jest używany m.in. przez funkcjonariuszy w Nowym Jorku).

Można stwierdzić, że obrońcy infrastruktury krytycznej znajdują się w niekorzystnej sytuacji, ponieważ poruszają się jako pierwsi (decydują o alokacji zasobów obronnych i rozkładach prawdopodobieństwa strategii czystych), a ich ruch jest obserwowany przez atakującego. Jednak dokładniejsza analiza ujawnia, że to właśnie obrońca, wykonując ruch jako pierwszy, może mieć znaczny wpływ na wybory dokonywane przez atakującego. Upraszczając, to obrońca może zmusić atakującego do wybrania danej strategii, a nie innych.

Dla przykładu rozważmy grę o macierzy wypłat określonej w tabeli 3 i załóżmy, że gracz 1 jest liderem w grze Stackelberga.

Tabela 3. Macierz wypłat dla przykładowej gry.

		Gracz 2	
		C	*D*
Gracz 1	*A*	(1,1)	(3,0)
	B	(0,0)	(2,1)

Źródło: D. Korzhyk i in., *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*, „Journal of Artificial Intelligence Research" 2011, t. 41, nr 2, s. 297–327.

Należy zwrócić uwagę, że jeśli gracze poruszają się jednocześnie, to jedyną równowagą Nasha (w strategiach czystych – na mocy definicji – każda równowaga Nasha w strategiach czystych jest również równowagą Nasha w strategiach mieszanych) jest profil strategii (A,C), co daje graczowi 1 oczekiwaną wypłatę równą 1. Natomiast jeśli gracz 1 może poruszyć się jako pierwszy, to może wybrać strategię mieszaną polegającą na grze A i B z prawdopodobieństwami $\frac{1}{2}$ zamiast A z prawdopodobieństwem 1 i B z prawdopodobieństwem 0, jak w przypadku równowagi Nasha dla gry jednoczesnej. Wybór dokonany przez lidera sprawia, że śledzący (gracz 2) wybiera

strategię *D* zamiast *C*[11]. W rezultacie, będąc liderem, gracz 1 może uzyskać oczekiwaną wypłatę w wysokości $\frac{5}{2}$ zamiast 1, co stanowi istotną różnicę.

W załączniku A na końcu artykułu zostało przedstawione bardziej sformalizowane wprowadzenie do gier w obszarze bezpieczeństwa.

Gry bezpieczeństwa – wyzwania i podejścia

Podejście oparte na teorii gier opisane w poprzedniej części artykułu ma ugruntowaną pozycję w literaturze. Jednak dopiero w ciągu ostatnich dwóch dekad koncepcje teoriogrowe zostały skutecznie wdrożone w celu ochrony infrastruktury krytycznej. Powodem opóźnień we wdrożeniu były przede wszystkim wyzwania obliczeniowe związane z grami bezpieczeństwa. W tej części artykułu omówiono te wyzwania oraz opisano sposoby, dzięki którym techniki optymalizacji i sztucznej inteligencji stały się skutecznymi narzędziami do ich pokonywania. Ponadto przedstawiono krótki przegląd istniejących kierunków badań nad grami bezpieczeństwa, aby przybliżyć wyzwania związane z opracowywaniem praktycznych i możliwych do zrealizowania rozwiązań.

Wyzwania obliczeniowe

W rzeczywistych zastosowaniach gry Stackelberga stanowią poważne wyzwanie obliczeniowe ze względu na następujące czynniki:

- przestrzenie decyzyjne w złożonych i wielkoskalowych środowiskach infrastruktury krytycznej są ogromne, co oznacza, że liczba możliwych strategii i działań, które mogą zostać podjęte przez graczy, np. obrońców i napastników, może być bardzo duża. Przykładem takiej złożonej infrastruktury jest system metra w Nowym Jorku, będący jedną z największych i najbardziej ruchliwych sieci transportu publicznego na świecie, obsługującą codziennie miliony osób. Ta sieć składa się z ponad 800 mil (1287 km) torów łączących 472 stacje. Istnieją nie tylko różne metody stosowania środków ochrony (tj. ogromna przestrzeń strategii obrońcy), lecz także bardzo szeroki wachlarz możliwości ataku (tj. ogromna przestrzeń strategii atakującego). Tak rozległe przestrzenie decyzyjne

[11] W grach Stackelberga zakłada się, że jeśli śledzący pozostaje bezczynny, remis jest rozstrzygany na korzyść lidera, ponieważ w przeciwnym razie optymalne rozwiązanie przyjmuje się jako źle zdefiniowane.

wymagają efektywnych algorytmów zarówno do ich eksploracji, jak i optymalizacji;
- niepewność i niekompletność informacji na temat intencji, zdolności i działań przeciwników. Istnieją narzędzia teoriogrowe, tzw. bayesowskie gry bezpieczeństwa (ang. *Bayesian security games,* por. załącznik A), które stanowią narzędzie do modelowania powyższej niepewności przy użyciu narzędzi probabilistycznych. Zwiększa to jednak poziom złożoności obliczeniowej problemu;
- rzeczywiste sytuacje są często dynamiczne i stale ewoluują. Przeciwnicy mogą dostosowywać swoje strategie, a obrońcy muszą odpowiednio reagować. Modelowanie i optymalizacja strategii w takich dynamicznych środowiskach wymagają rozwiązywania powtarzających się (wielorundowych) lub sekwencyjnych gier, co dodatkowo zwiększa wyzwania obliczeniowe.

W literaturze naukowej obserwuje się kilka sposobów radzenia sobie z tego rodzaju wyzwaniami obliczeniowymi. Jednym z podstawowych jest zastosowanie metod optymalizacji matematycznej w celu efektywnego rozwiązywania tych gier. Badacze opracowali liczne algorytmy i techniki optymalizacji, które mogą obsługiwać modele gier na dużą skalę i dostarczać rozwiązań w rozsądnych ramach czasowych. Metody optymalizacji wykorzystują strukturę gry w celu zmniejszenia obciążenia obliczeniowego i poprawy efektywności algorytmów. Posiłkują się one zwłaszcza programowaniem matematycznym, programowaniem liniowym, programowaniem całkowitoliczbowym i innymi metodami optymalizacji w celu znalezienia optymalnych strategii i alokacji zasobów.

Ze względu na inherentną złożoność tych gier znalezienie dokładnych rozwiązań dla scenariuszy na dużą skalę jest często niewykonalne. Dlatego badacze i praktycy często opracowują algorytmy służące do obliczeń przybliżonych, aby sprostać wyzwaniom obliczeniowym przy zachowaniu rozsądnego poziomu dokładności.

Narzędziem mogącym odegrać dużą rolę w poprawie efektywności algorytmów optymalizacyjnych są techniki sztucznej inteligencji. Wykorzystywanie jej do optymalizacji algorytmów w ogóle, a zwłaszcza zagadnień optymalizacyjnych, od wielu lat prowadzi do zwiększania stanu wiedzy w zakresie rozwiązywania trudnych problemów obliczeniowych. Sztuczna inteligencja umożliwia lepsze skalowanie istniejących podejść i może być stosowana w wielu różnych kontekstach, m.in. w kontekście gier

optymalizacyjnych[12]. Ponadto modele sztucznej inteligencji mogą szybko i niezawodnie przybliżać wyniki kosztownych procesów obliczeniowych, pozwalając zrobić więcej przy tej samej ilości zasobów. Na przykład przy podejmowaniu decyzji, jaką interwencję zastosować w celu poprawy odporności i bezpieczeństwa, niektóre alternatywy będą dawały mało satysfakcjonujące wyniki. Modele sztucznej inteligencji mogą pomóc szybko i znacznie mniejszym kosztem zidentyfikować takie gorsze interwencje, nawet jeśli weźmie się pod uwagę niepewność związaną z odnajdywaniem rozwiązań przybliżonych. Ten sam rodzaj technik pozwala systemom takim jak AlphaGO na zbadanie ogromnej przestrzeni możliwych działań w ciągu kilku sekund. W kontekście gier bezpieczeństwa techniki te są wykorzystywane np. w systemach przeznaczonych do odstraszania kłusowników[13].

Inną możliwością jest skorzystanie z technik obliczeń równoległych i rozproszonych. Rozkładając obciążenie obliczeniowe na wiele procesorów lub maszyn, można obsługiwać znacznie większe modele gier. W tym przypadku dużą rolę odgrywają postępy w technologii sprzętowej, które poprawiają możliwości realizacji obliczeń równoległych.

Krótki przegląd literatury

Krótki przegląd na temat gier Stackelberga wraz z obrazowymi przykładami można znaleźć w pracy Sinhy i in.[14] Obszerniejszy przegląd aktualnej literatury dotyczącej gier bezpieczeństwa znajduje się w artykule autorstwa Hunta i Zhuanga[15]. W tym przeglądzie zbadano obecny stan wiedzy w zakresie modelowania teoriogrowego dla scenariuszy atakujący–obrońca oraz przeanalizowano literaturę w kontekście najczęstszych obszarów zastosowań, podejścia do modelowania i metody rozwiązywania gier. Dodatkowo wskazano istotne luki w literaturze przedmiotu. Interesująca jest również zawarta w tym artykule szeroka dyskusja na temat przyszłych kierunków

[12] F. Hutter i in., *Boosting Verification by Automatic Tuning of Decision Procedures*, w: *Proceedings of the 19th International Conference on Computer Aided Verification* (CAV 2007), s. 27–34.

[13] S. Gholami i in., *Adversary models account for imperfect crime data: Forecasting and planning against real-world poachers*, w: *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2018), s. 823–831.

[14] A. Sinha i in., *Stackelberg security games: Looking beyond a decade of success*, w*: Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence* (IJCAI 2018), s. 5494–5501.

[15] K. Hunt, J. Zhuang, *A review of attacker-defender games: Current state and paths forward*, „European Journal of Operational Research" 2023, w druku. https://doi.org/10.1016/j.ejor.2023.04.009.

badań. Inne obszerne badania dotyczące gier bezpieczeństwa zostały opisane w tekście Fang i Nguyen[16], jak również w innym artykule współautorstwa Nguyen[17], gdzie wskazano, że niektóre instytucje zajmujące się bezpieczeństwem regularnie wykorzystują w ramach procesu decyzyjnego narzędzia oparte na teorii gier w celu optymalizacji alokacji ograniczonych zasobów bezpieczeństwa przeciwko strategicznie działającym przeciwnikom, jak również że unikalne cechy tego rodzaju zastosowań wymagają innowacyjnych rozwiązań w postaci systemów sztucznej inteligencji.

Ważnymi punktami odniesienia na granicy teorii gier i bezpieczeństwa stały się dwie klasyczne już monografie. Książka Tambego[18] koncentruje się na postępie dokonanym w dziedzinie projektowania i analizy algorytmów oraz stosowaniu przez organy rządowe oprogramowania opartego na teorii gier. Z kolei w monografii Bier i Azaieza[19] przedstawiono kompilację prac łączących teorię gier i analizę ryzyka w dziedzinie bezpieczeństwa.

Gry Stackelberga są coraz częściej wykorzystywane do badania szerokiego zakresu zagadnień związanych z bezpieczeństwem – od scenariuszy dotyczących systemów obrony przeciwrakietowej[20], terroryzmu[21], bezpieczeństwa publicznego[22], po bezpieczeństwo sieci komputerowych[23].

Przez ostatnie lata gry bezpieczeństwa były przedmiotem szeroko zakrojonych badań i istnieje obszerna literatura poświęcona różnym problemom z nimi związanym. Przykładem może być model alokacji zasobów,

---

[16] F. Fang, T.H. Nguyen, *Green security games: Apply game theory to addressing green security challenges*, „ACM SIGecom Exchanges" 2016, t. 15, nr 1, s. 78–83. https://doi.org/10.1145/2994501.2994507.

[17] T.H. Nguyen i in., *Towards a science of security games*, w: *Mathematical Sciences with Multidisciplinary Applications*, B. Toni (red.), Springer Cham 2016, s. 347–381.

[18] M. Tambe, *Security and game theory: algorithms, deployed systems, lessons learned*, Cambridge 2011.

[19] V.M. Bier, M.N. Azaiez, *Game Theoretic Risk Analysis of Security Threats*, Springer 2008. https://doi.org/10.1007/978-0-387-87767-9.

[20] G. Brown i in., *A Two-Sided Optimization for Theater Ballistic Missile Defense*, „Operations Research" 2005, t. 53, nr 5, s. 745–763. https://doi.org/10.1287/opre.1050.0231.

[21] T. Sandler, *Terrorism & Game Theory*, „Simulation & Gaming" 2003, t. 34, nr 3, s. 319–337. https://doi.org/10.1177/1046878103255492.

[22] N. Gatti i in., *Game Theoretical Insights in Strategic Patrolling: Model and Algorithm in Normal-Form*, w: *Proceedings of the 2008 conference on ECAI 2008: 18th European Conference on Artificial Intelligence* (ECAI 2008), s. 403–407. https://doi.org/10.3233/978-1-58603-891-5-403.

[23] K-w. Lye, J. Wing, *Game Strategies in Network Security*, „International Journal of Information Security" 2005, t. 4, s. 71–86. https://doi.org/10.1007/s10207-004-0060-x.

w ramach którego np. władze rządowe dążą do optymalizacji przydziału zasobów obronnych między określonymi celami (np. lotniska lub dworce kolejowe), a przeciwnik chce zaatakować niektóre z nich. W artykule autorstwa An i in.[24] przedstawiono opis wspomnianego systemu PROTECT, wykorzystywanego przez USCG do planowania patroli w portach w Bostonie i w Nowym Jorku (zdjęcie). Co najważniejsze, system nie zakłada, że przeciwnicy działają w sposób w pełni racjonalny, co pozwala na tworzenie bardziej realistycznych i skuteczniejszych scenariuszy. Istotne jest także to, że pozytywna ocena zastosowania systemu PROTECT w porcie w Bostonie przyczyniła się do jego wdrożenia również w porcie w Nowym Jorku. Podstawą systemu PROTECT jest właśnie model gry atakujący–obrońca opracowany przez Stackelberga. Zaprojektowanie i wdrożenie tego systemu wymagało poniesienia znacznych nakładów, przeznaczonych m.in. na rozwinięcie teoretycznych podstaw takich zastosowań modelu oraz na jego kompleksową ocenę naukową.

Zdjęcie. System PROTECT został wdrożony przez USCG w celu ochrony trasy promowej Staten Island obsługiwanej przez Departament Transportu miasta Nowy Jork. Na zdjęciu jest widoczna łódź USCG chroniąca jeden z promów.

Warto zauważyć, że istnieje wiele stochastycznych gier Stackelberga, w których zdolności decyzyjne przeciwnika są zmniejszone z powodu tzw. ograniczonej racjonalności. Większość systemów opartych na grach Stackelberga co do zasady opiera się na przyjętym założeniu, zgodnie z którym przeciwnicy są doskonale racjonalni, i taki standard jest opisywany

[24] B. An i in., *A Deployed Quantal Response-Based Patrol Planning System for the U.S. Coast Guard*, „Interfaces" 2013, t. 43, nr 5, s. 400–420. https://doi.org/10.1287/inte.2013.0700.

w literaturze. To założenie może jednak niedokładnie odzwierciedlać zachowania rzeczywistych przeciwników, ponieważ ludzie często postępują w sposób nie w pełni racjonalny. Z tego powodu badacze (np. Yang i in.[25]), czerpiąc inspirację z psychologicznych i behawioralnych modeli ekonomicznych, skupili się na badaniu w tych grach sparametryzowanych modeli ograniczonej racjonalności. Modele te oferują wszechstronne podejście do włączania ograniczonej racjonalności do założeń dowolnej gry, dzięki czemu można je zastosować do szerokiej palety gier wykraczających poza te zdefiniowane przez Stackelberga. Przykładem takiego podejścia jest zastosowanie opisane w pracy Nguyen i in.[26], w którym zamiast wybierać pojedynczy cel jako optymalną odpowiedź na indukowane pokrycie celów przez zasoby obronne (to pokrycie jest oznaczone symbolem C, od ang. *cover*), odpowiedź przeciwnika h(C) pociąga za sobą wybór celu *t* na podstawie prawdopodobieństwa q_t związanego z tym celem.

Na zakończenie należy zauważyć, że istnieje wiele innych potencjalnych zastosowań gier Stackelberga w modelowaniu scenariuszy bezpieczeństwa. Obejmują one m.in. następujące koncepcje:

- gry patrolowe (Vorobeychik i in.[27]) – zaprojektowane w celu symulowania sytuacji, w których środowiska muszą być patrolowane, aby odstraszyć intruzów. Tego rodzaju gry czerpią inspirację z powszechnie uznanego modelu pościgu i ucieczki, ale zostały rozszerzone na różne sposoby, w tym przez włączenie systemów alarmowych;
- gry typu „z interwencją w planowanie" (Vorobeychik i Pritchard[28]), w których obrońca ma za zadanie wybrać strategię ograniczania ryzyka, aby uprzedzić potencjalne działania atakującego, podczas gdy ten ostatni w odpowiedzi opracowuje optymalny plan ataku, który próbuje ominąć zaimplementowane środki zaradcze. Model

---

[25] R. Yang i in., *Improving Resource Allocation Strategy Against Human Adversaries in Security Games*, w: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence* (IJCAI 2011), s. 458–464.

[26] T.H. Nguyen i in., *Analyzing the effectiveness of adversary modeling in security games*, w: *Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence* (AAAI 2013), nr 1, s. 718–724.

[27] Y. Vorobeychik, B. An, M. Tambe, *Adversarial Patrolling Games*, w*: Papers from the 2012 AAAI Spring Symposium*, t. 3, s. 91–98.

[28] Y. Vorobeychik, M. Pritchard, *Plan interdiction games*, w: *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia i in. (red.), Springer Cham 2020, s. 159–182. https://doi.org/10.1007/978-3-030-33432-1_8.

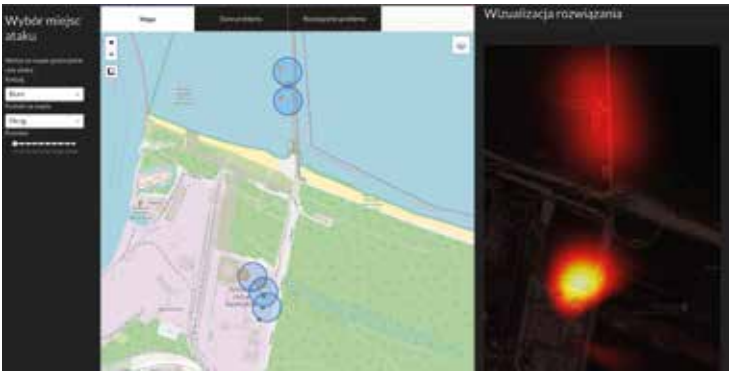
ten znajduje zastosowanie w kontekście przeciwników działających w obszarze cyberbezpieczeństwa;
- gry audytowe (Blocki i in.[29]) – badające aspekty ekonomiczne związane z projektowaniem mechanizmów audytu, ze szczególnym naciskiem na efektywną alokację zasobów i odpowiednie systemy kar. Model gry audytowej rozszerza model gry bezpieczeństwa poprzez wprowadzenie dodatkowego parametru związanego z karą. Modele te znajdują praktyczne zastosowanie w audytach, których celem jest zapewnienie w różnych instytucjach, w tym w szpitalach, zgodności z polityką prywatności;
- koalicyjne gry bezpieczeństwa (Guo i in.[30]) – zajmujące się kwestią optymalizacji zapobiegania koalicjom atakujących, w których atakujący mają możliwość tworzenia sojuszy. Koncepcja ta jest szczególnie ważna w przypadku takich działań, jak zakłócanie sieci terrorystycznych, rozbijanie komórek tych sieci lub zapobieganie zmowie wielu napastników.

Prace zespołu „AI dla bezpieczeństwa"

Zespół „AI dla bezpieczeństwa" w instytucie badawczym IDEAS NCBR buduje modele Stackelberga dla różnych typów infrastruktury krytycznej. Aktualnie zespół koncentruje się na opracowywaniu oprogramowania do ochrony portów, terminali LNG, sieci kolejowych i energetycznych. Rysunek przedstawia podstawowy interfejs tworzonego oprogramowania.

[29] J. Blocki i in., *Audit games with multiple defender resources,* w: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* (AAAI 2015), t. 29, nr 1, s. 791–797.

[30] Q. Guo i in., *Coalitional security games,* w*: Proceedings of the 15th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2016), s. 159–167.



Rysunek. Zrzut z interfejsu oprogramowania do ochrony portów, terminali LNG, sieci kolejowych i energetycznych. Zrzut przedstawia mapę terminalu LNG w Świnoujściu. Czerwone okręgi oznaczają cele (rozmiar okręgu odpowiada znaczeniu celu), niebieskie – rozmieszczenie patroli i ich pole widzenia. Po prawej stronie jest pokazane względne prawdopodobieństwo, określające, które części terenu powinny być patrolowane (optymalna strategia obrońcy). Powyższa wizualizacja służy wyłącznie celom demonstracyjnym.

Celem jest opracowanie systemu mającego następujące cechy:

- ocena ryzyka – system powinien przeprowadzać ciągłą ocenę ryzyka poprzez analizę różnych źródeł danych, bieżących i historycznych oraz raportów wywiadowczych. Aby zoptymalizować alokację zasobów bezpieczeństwa, należy wziąć pod uwagę takie elementy, jak poziomy zagrożenia, pożądane cele i słabe punkty;
- losowość proponowanych strategii – system powinien wykorzystywać losowe strategie w celu określenia optymalnych tras patrolowych dla pracowników ochrony w połączeniu z optymalnym rozmieszczeniem oddziałów ochrony. Losując trasy, system zwiększa trudność potencjalnych przeciwników w przewidywaniu wzorców bezpieczeństwa, co potęguje tym samym element zaskoczenia i odstrasza potencjalnych agresorów;
- dynamiczna adaptacja – system powinien uwzględniać ewoluujące zagrożenia i dostosowywać się do zmieniających się scenariuszy bezpieczeństwa. Powinien mieć zdolność do dynamicznego modyfikowania tras patrolowych i przydzielania zasobów w odpowiedzi na informacje w czasie rzeczywistym, takie jak pojawiające się dane wywiadowcze, które aktualizują wiedzę o zagrożeniach. Ma to na celu zapewnienie optymalnego zasięgu i zwiększenie zdolności reagowania;

- współpraca i koordynacja – system powinien ułatwiać współpracę między różnymi agencjami czy też zespołami bezpieczeństwa działającymi na chronionym obszarze. Powinien on umożliwiać dzielenie się informacjami, koordynację działań oraz wymianę danych wywiadowczych w czasie rzeczywistym w celu zwiększenia świadomości sytuacyjnej i osiągnięcia lepszych wyników w zakresie bezpieczeństwa;
- ocena wydajności i informacje zwrotne – system powinien zawierać mechanizmy oceny wydajności, umożliwiające pracownikom ochrony analizę jego skuteczności i odpowiednie dostosowanie strategii. System powinien oferować informacje zwrotne, identyfikując obszary wymagające poprawy i rozpoznając wzorce, które mogą wymagać uwagi.

W ostatnim czasie członkowie zespołu „AI dla bezpieczeństwa" na jednej z czołowych konferencji informatycznych, tj. 39th Conference on Uncertainty in Artificial Intelligence (UAI 2023, Pittsburgh, USA), zaprezentowali pracę *Two-phase attacks in security games*[31]. Dotyczyła ona ataku, który przebiegał dwuetapowo (dwufazowo). Zazwyczaj atak w grach bezpieczeństwa jest modelowany jako jednorazowy ruch, podczas którego atakujący nie ma szansy na aktualizację swojej strategii, nawet jeśli w trakcie tego procesu są zdobywane nowe i cenne informacje. Jest to oczywiście daleko idące uproszczenie, niepasujące do realiów w wielu sytuacjach. Odejście od niego było celem omawianej pracy. Został w niej zaproponowany model, w którym w pierwszej fazie atakujący wykonuje wstępny ruch, aby uzyskać dodatkowe informacje na temat bieżących działań obrońcy (np. czy dany odcinek granicy jest patrolowany czy nie). Następnie, w drugiej fazie, ta wiedza jest wykorzystywana do wyboru optymalnego ruchu podczas właściwego ataku.

Niedawnym przykładem rzeczywistej sytuacji, która jest bezpośrednio modelowana w opisywanej dwufazowej grze, są działania reżimu Łukaszenki wykorzystującego imigrantów do sondowania granicy Białorusi z Ukrainą[32]. Naraża to życie imigrantów na skrajne niebezpieczeństwo zarówno ze względu na bardzo trudny teren, jak i trwającą wojnę. Zwłaszcza północno-zachodnia granica Ukrainy o długości prawie 900 km to

[31] A. Nagórko, P. Ciosmak, T. Michalak, *Two-phase security games*, w*: Proceedings of the Thirty-Nine Conference on Uncertainty in Artificial Intelligence* (UAI 2023), s. 1489–1498.

[32] V. Romanenko, *Belarus uses migrants for intelligence on border with Ukraine*, Ukrainska Pravda, 6 XII 2022 r., https://www.pravda.com.ua/eng/news/2022/12/6/7379514/ [dostęp: 25 VI 2023].

mocno zalesiony obszar pełen niebezpiecznych mokradeł. Jest tam także Strefa Wykluczenia wokół Czarnobylskiej Elektrowni Jądrowej. Co więcej, granica – która została przekroczona przez armię rosyjską w lutym 2022 r., a następnie przywrócona przez ukraińską kontrofensywę – jest obecnie silnie ufortyfikowana okopami, zasiekami i polami minowymi.

Niestety, nie zważając na te niebezpieczeństwa, białoruska straż graniczna organizuje i koordynuje działania grup imigrantów planujących nielegalne przekroczenie granicy. Celem białoruskich służb jest ujawnienie i zakłócenie ukraińskiej obrony, która jest zmuszona reagować na wszelkie próby przekroczenia granicy ze względu na zagrożenie stwarzane przez rosyjskich dywersantów.

Z uwagi na zastosowanie zaawansowanych, elektronicznych środków bezpieczeństwa większość przekroczeń granicy jest wykrywana. Należy jednak zauważyć, że wykrycie nie gwarantuje obecności patrolu wystarczająco blisko, aby zapobiec nieautoryzowanemu przekroczeniu granicy. To oznacza, że granica nie jest zupełnie nie do przejścia. Niemniej jednak, nawet w przypadkach, gdy określony odcinek granicy jest niestrzeżony w momencie wjazdu, ukraińskie dowództwo niezwłocznie wysyła tam zespół. W związku z tym kolejne próby przekroczenia tego samego odcinka granicy są bardzo mało prawdopodobne, biorąc pod uwagę szybką reakcję odpowiednich służb.

Rozważmy uproszczony model problemu, z czterema odcinkami granicy białorusko-ukraińskiej (S_1, S_2, S_3, i S_4) i dwiema jednostkami patrolowymi. Problem tego rodzaju można modelować jako standardową grę bezpieczeństwa podobną do tej wykorzystywanej na lotnisku w Los Angeles[33]. Zbiór ukraińskich ruchów obejmuje możliwe przydzielenie patroli do odcinków granicy:

$$I = \{S_1S_2, S_1S_3, S_1S_4, S_2S_3, S_2S_4, S_3S_4\}$$

Przyjmijmy założenie, że istnieją dwa możliwe typy napastników: przemytnicy (ludzi) o niskim i wysokim profilu (zaawansowania). Zostaną oni oznaczeni odpowiednio: typ 1 oraz typ 2. Atakujący o wysokim profilu zadają znacznie większe straty obrońcy, ponieważ organizują znacznie większe grupy. Oba typy mają tę samą przestrzeń strategii, tj. atakujący każdego typu może wybrać jedną z czterech sekcji granicy lub wycofać się, tj. $J_1 = J_2 = \{S_1,S_2,S_3,S_4,\varnothing\}$. Wypłaty obu stron, w zależności od typu

[33] J. Pita i in., *Using game theory for Los Angeles Airport…*

atakującego, rosną liniowo wraz z S_i – dla atakującego o wysokim profilu przydzielane punkty wynoszą odpowiednio 50, 100, 150 i 200, a dla atakującego o niskim profilu są przyznawane punkty pięciokrotnie mniejsze. Punkty obrońcy są alokowane przeciwnie, z niewielkim losowym szumem dodawanym równomiernie z przedziału [–5,5].

Zakładając, że prawdopodobieństwo ataków tych dwóch typów wynosi $p_1 = 0{,}8$ dla atakującego o niskim profilu i $p_2 = 0{,}2$ dla napastnika o wysokim profilu, optymalną strategią dla obrońcy jest następująca:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (0\%, 50\%, 0\%, 0\%, 50\%, 0\%)$$

Zgodnie z tą strategią sekcje graniczne S_1 i S_2 nigdy nie są chronione jednocześnie. Taka sytuacja jest typowa dla równowagi Stackelberga (ang. *Stackelberg equilibrium*) w grach jednofazowych i atakujący może to łatwo wykorzystać, przeprowadzając atak dwufazowy.

Omówiona zostanie teraz koncepcja ataku dwufazowego. Załóżmy, że bez wiedzy obrońcy atakujący ma niezbędne zasoby i możliwości przemytnika ludzi zarówno o niskim, jak i wysokim profilu. W związku z tym atakujący może próbować naruszyć dwie sekcje granicy sekwencyjnie, tj. atak będzie miał dwie fazy.

Na podstawie powyżej wyprowadzonej optymalnej strategii dla ataku jednofazowego rozważmy scenariusz, w którym w pierwszej fazie mało znany przemytnik podejmuje próbę przekroczenia granicy na odcinku S_1. Ta początkowa faza zapewnia atakującemu cenne informacje, bez względu na obecne rozmieszczenie obrońcy (tj. czy dany odcinek granicy jest patrolowany w tej chwili czy nie). Wynika to z tego, że po przeprowadzeniu takiego ataku atakujący ma dużo lepszą wiedzę (zna warunkowy rozkład prawdopodobieństwa dotyczący zasobów obrońcy).

Przyjmijmy, że $t \in \{0\%, 17\%, 33\%, 50\%, 67\%, 83\%, 100\%\}$ to prawdopodobieństwa napotkania dwufazowego napastnika, $(1 - t)$ x 80% to prawdopodobieństwo napotkania napastnika o niskim profilu, a $(1 - t)$ x 20% to prawdopodobieństwo napotkania napastnika o wysokim profilu. W przypadku $t = 0\%$ jest to standardowy model jednofazowy, podczas gdy $t = 100\%$ opisuje czysty atak dwufazowy.

W tabeli 4 pokazano, że obecność dwufazowego atakującego znacznie zmienia równowagę Stackelberga w grze. Na przykład dla 33-procentowego prawdopodobieństwa ataku dwufazowego (z 53-procentową szansą na jednofazowy atak o niskim profilu i 13-procentową szansą na jednofazowy

atak o wysokim profilu, utrzymując stosunek 4:1 niskiego profilu do wysokiego profilu) optymalną strategią obrońcy staje się następująca:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (12\%, 15\%, 17\%, 17\%, 18\%, 21\%)$$

Zgodnie z tabelą 4 dwufazowe równowagi Stackelberga są znacznie bardziej odporne na zmiany profili napastników.

Tabela 4. Każdy wiersz przedstawia optymalną mieszaną strategię obrońcy przeciwko grupie atakujących z daną szansą na napotkanie dwufazowego ataku. Zgodnie z ostatnim wierszem bez obecności dwufazowych napastników równowaga Stackelberga jest istotnie niedostosowana do losowego szumu w macierzach punktacji.

S_1S_2	S_1S_3	S_1S_4	S_2S_3	S_2S_4	S_3S_4	Szansa na atak dwufazowy
0,085	0,11	0,12	0,2	0,25	0,23	100%
0,085	0,11	0,12	0,2	0,25	0,23	83%
0,12	0,11	0,12	0,2	0,25	0,23	67%
0,12	0,15	0,17	0,17	0,18	0,21	50%
0,12	0,15	0,17	0,17	0,18	0,21	33%
0,15	0,15	0,17	0,16	0,18	0,18	17%
0	0,5	0	0	0,5	0	0%

Ruchy obrońcy (rozmieszczenie patroli)

W tabeli 5 pokazano, jak zmieniają się wypłaty obrońców w zależności od składu grup atakujących. Na przykład oczekiwana punktacja obrońcy przeciwko atakowi jednofazowemu spada do –175, gdy strategia jednofazowa jest stosowana przeciwko atakującemu dwufazowemu.

Tabela 5. Oczekiwana wypłata obrońcy na etapie gry ze strategią z tabeli 4 przeciwko danej szansie na atak dwufazowy. W ostatniej kolumnie widać, że strata poniesiona w wyniku grania strategią, która ignoruje możliwość ataku dwufazowego, jest o rząd wielkości większa niż zbyt ostrożna ochrona przed takimi atakami.

-16,2	-16,2	-16,2	-20,3	-20,3	-24,9	-175	100%
-14,8	-14,8	-14,8	-17,3	-17,3	-20,9	-146	83%
-13,4	-13,4	-13,4	-14,3	-14,3	-16,9	-116	67%
-12	-12	-12	-11,3	-11,3	-12,8	-87,1	50%
-10,7	-10,7	-10,7	-8,36	-8,36	-8,84	-57,9	33%
-9,27	-9,27	-9,27	-5,38	-5,38	-4,83	-28,6	17%
-7,89	-7,89	-7,89	-2,41	-2,41	-0,816	0,7	0%
100%	83%	67%	50%	33%	17%	0%	

Szansa na atak dwufazowy

Strategia obrońcy

W celu eliminacji przedmiotowej usterki autorzy proponują nowy model, który pozwala na jednoczesne uwzględnienie napastników jedno- i dwufazowych. W tym modelu bezpieczeństwa oczekiwana punktacja przeciwko skoordynowanym atakującym znacznie się zmienia, z –175 do –16,2 (obrońca nadal znajduje się w niekorzystnej sytuacji). Optymalna strategia:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (8{,}5\%, 11\%, 12\%, 20\%, 25\%, 23\%)$$

zmusza atakującego o niskim profilu do zaatakowania S_1, a atakującego o wysokim profilu do wycofania się, jeśli S_1 nie był patrolowany. Należy zauważyć, że wiąże się to z kosztami – w przypadku nieskoordynowanego (jednofazowego) ataku, gdy atakujący o niskim i wysokim profilu działają niezależnie, ta strategia daje obrońcy wypłatę –7,89 (spadek z 0,7).

Podsumowanie

W niniejszym artykule przedstawiono zaawansowane metody poprawiające bezpieczeństwo infrastruktury krytycznej, obejmujące połączenie teorii gier, technik optymalizacji i algorytmów sztucznej inteligencji. Skuteczność tych metod została wykazana poprzez ich wdrożenie w kilku obiektach czy też zastosowaniach w USA. Należy podkreślić, że tego rodzaju ulepszenia zostały osiągnięte nie przez zwiększenie zasobów służb bezpieczeństwa (i kosztów), lecz przez optymalizację wykorzystania dostępnych zasobów. Prace zespołu „AI dla bezpieczeństwa" w instytucie badawczym IDEAS NCBR koncentrują się na rozszerzeniu tych wyników i zastosowaniu ich do różnych rodzajów infrastruktury krytycznej oraz do zagrożeń bezpieczeństwa, które ostatnio pojawiły się ponownie w Europie. Zespół dąży do ich szybkiego wdrożenia, aby zoptymalizować ochronę polskich obiektów i systemów infrastruktury krytycznej.

Załącznik A

Załącznik jest poświęcony formalnemu opisowi gier bezpieczeństwa, który podąża za nowoczesnym podejściem[34]. Następnie została opisana szersza klasa gier Stackelberga, zwana bayesowskimi grami Stackelberga, która stanowi podstawę dla modelu dwufazowego omówionego w poprzedniej części artykułu. Wprowadzono także sformalizowany opis problemu optymalizacyjnego, który można wykorzystać do rozwiązania tych gier.

A.1 Gry bezpieczeństwa

Gry bezpieczeństwa są rozgrywane przez dwóch graczy – obrońcę i atakującego. Obrońca ma ograniczoną liczbę zasobów bezpieczeństwa i dąży do alokacji tych zasobów w celu ochrony n celów ze zbioru $[n] = \{1,2,\ldots,n\}$. Strategia czysta obrońcy to podzbiór celów, które są chronione (pokrywane) w ramach wykonalnej alokacji tych zasobów. Reprezentacją strategii czystej jest wektor binarny $e \in \{0,1\}^n$, gdzie wyrazy o wartości 1 określają cele pokryte ochroną. Symbol $E \subseteq \{0,1\}^n$ oznacza zbiór wszystkich dostępnych strategii czystych obrońcy. Strategia mieszana obrońcy to rozkład prawdopodobieństwa x określony na elementach E. Strategia czysta atakującego jest celem $i \in [n]$. Strategia mieszana atakującego jest oznaczana

[34] H. Xu, *The Mysteries of Security Games: Equilibrium Computation Be-Comes Combinatorial Algorithm Design*, w: *Proceedings of the 2016 ACM Conference on Economics and Computation* (ACM EC 2016), s. 497–514.

przez $y \in \Delta_n$, gdzie Δ_n jest n-wymiarowym sympleksem. W tym przypadku y_i oznacza prawdopodobieństwo ataku na cel i.

W najbardziej ogólnym ujęciu gry bezpieczeństwa są formą gry dwuliniowej. Gra dwuliniowa jest określana przez parę macierzy (A,B) i wielościanów (P,Q). Zakładając, że gracz 1 gra zgodnie z $x \in P$, a gracz 2 gra zgodnie z $y \in Q$, wypłaty dla gracza 1 i 2 wynoszą odpowiednio $x^T Ay$ oraz $x^T By$.

Możemy teraz podać różne pojęcia równowag dla gier bezpieczeństwa. Profil strategii (x,y) jest równowagą Nasha (NE), jeśli:

$$\forall x' \in P \ \forall y' \in Q \ x^T Ay \geq x'^T Ay \ \& \ x^T By \geq x^T By'$$

Zgodnie z twierdzeniem Nasha dla każdej gry dwuliniowej istnieje co najmniej jedna NE w strategiach mieszanych (może ich istnieć więcej niż jedna).

Gdy jeden gracz porusza się przed innym graczem, bardziej odpowiednią koncepcją rozwiązania jest równowaga Stackelberga. Dwuosobowa gra Stackelberga jest rozgrywana pomiędzy liderem i śledzącym. Lider wykonuje ruch jako pierwszy lub, równoważnie, zagrywa zgodnie z pewną strategią mieszaną jako pierwszy. Gracz śledzący obserwuje strategię lidera i reaguje na nią zgodnie z dostępnymi sobie strategiami. Optymalna strategia lidera wraz z najlepszą odpowiedzią śledzącego tworzy równowagę.

Niech

$$y_x = \arg\max_{y' \in Q} x^T By'$$

oznacza najlepszą odpowiedź gracza śledzącego na strategię lidera $x \in P$. Profil strategii (x, y) jest silną równowagą Stackelberga (ang. *strong Stackelberg equilibrium*, SSE), gdy:

$$x = \arg\max_{x' \in P} x'^T Ay_{x'} \quad \text{oraz} \quad y = y_x$$

Gdy $B = -A$, to dwuliniowa gra jest grą o sumie zerowej. W takich grach zarówno NE, jak i SSE są równoważne równowadze minimaksowej (ang. *minimax equilibrium*, ME).

Profil strategii (x, y) stanowi z kolei **równowagę minimaksową**, jeśli

$$\forall x' \in P \forall y' \in Q \ x^T Ay \geq x'^T Ay \ \& \ x^T Ay \leq x^T Ay'$$

W przypadku gdy (x, y) jest równowagą minimaksową, strategia x będzie oznaczała strategię optymalną gracza 1, a strategia y – strategię minimaksową gracza 2.

Wartość gry będzie w takim przypadku następująca:

$$V = x^T Ay = \max_{x' \in \mathcal{P}} \min_{y' \in Q} x'^T Ay'$$

Przejdźmy do opisu struktury wypłat w grze, zakładając, że atakujący atakuje cel i:

- obrońca otrzymuje nagrodę r_i, jeśli cel i zostanie ochroniony, lub ponosi koszt c_i, jeśli i zostanie bez ochrony (odkryty),
- atakujący ponosi koszt ξ_i, jeśli cel i jest pokryty (ochroniony), lub nagrodę ρ_i, jeśli i pozostanie odkryty,
- obaj gracze otrzymują wypłatę 0 na pozostałych $n - 1$ nieatakowanych celów.

Przyjmujemy tu kluczowe założenie: dla wszystkich $i \in [n]$ ustalmy, że:

$$r_i > c_i \quad \text{oraz} \quad \rho_i > \xi_i$$

Oznacza to, że:

- ochrona danego celu jest dla obrońcy bardziej korzystna niż jego odsłanianie,
- atakujący woli zaatakować cel, gdy jest on niepokryty.

Definicja 1 (gra bezpieczeństwa).

Gra bezpieczeństwa G z liczbą celów n to gra (r,c,ρ,ξ,E), która spełnia $r_i > c_i$ oraz $\rho_i > \xi_i$ dla wszystkich $i \in [n]$.

Użyteczność (wypłatę) obrońcy można zdefiniować w następujący sposób:

$$U^d(e,i) = r_i e_i + c_i(1 - e_i)$$

Przy założeniu $p \in \Delta_{|E|}$ oraz $y \in \Delta_n$ oczekiwana wypłata obrońcy wynosi:

$$U^d(p,y) = \sum_{e\in\mathcal{E}} \sum_{i\in[n]} p_e\, y_i U^d(e,i) =$$

$$= \sum_{e\in\mathcal{E}} \sum_{i\in[n]} p_e\, y_i\big(r_i e_i + c_i(1-e_i)\big) =$$

$$= \sum_{i\in[n]} y_i \sum_{e\in\mathcal{E}} p_e\big(r_i e_i + c_i(1-e_i)\big) =$$

$$= \sum_{i\in[n]} y_i \left(r_i \sum_{e\in\mathcal{E}} p_e\, e_i + c_i \left(1 - \sum_{e\in\mathcal{E}} p_e\, e_i \right) \right)$$

Gdy $p \in \Delta_{|\mathcal{E}|}$ i $y \in \Delta_n$, oczekiwana użyteczność obrońcy wynosi:

$$U^d(p,y) = \sum_{i\in[n]} y_i \left(r_i \sum_{e\in\mathcal{E}} p_e\, e_i + c_i \left(1 - \sum_{e\in\mathcal{E}} p_e\, e_i \right) \right)$$

Przyjmując następującą konwencję notacyjną:

$$x_i := \sum_{e\in\mathcal{E}} p_e\, e_i$$

tj. używając symbolu x_i na oznaczenie krańcowego (tzw. marginalnego) prawdopodobieństwa pokrycia celu i, dostajemy równoważne określenie oczekiwanej użyteczności obrońcy jako:

$$U^d(p,y) = \sum_{i\in[n]} y_i\big(r_i x_i + c_i(1-x_i)\big)$$

W przypadku przyjęcia założenia, że $x = (x_1,\ldots,x_n)^T$ oznacza prawdopodobieństwo krańcowe dla wszystkich celów wywołanych przez strategię mieszaną p. Powyższe równanie pokazuje, że oczekiwana użyteczność obrońcy może być zwięźle wyrażona jako postać dwuliniowa:

$$U^d(x,y) = \sum_{i\in[n]} y_i\big(r_i x_i + c_i(1-x_i)\big)$$

Widać, że $U^d(x, y)$ ma postać dwuliniową

$$x^T Ay + ax$$

dla pewnej nieujemnej macierzy diagonalnej A.

Zwróćmy uwagę, że wypukła otoczka zbioru E jest wielościanem wszystkich wykonalnych (tj. możliwych do wdrożenia przez strategię mieszaną obrońcy) prawdopodobieństw krańcowych:

$$\mathcal{P} = \{x = \sum_{e \in \mathcal{E}} p_e \, e : p \in \Delta_{|\mathcal{E}|}\}$$

W tym przypadku można więc zinterpretować punkt $x \in P$ jako strategię mieszaną i – jak wyżej – oznaczyć użyteczność obrońcy poprzez: $U^d(x, y)$.

Analogicznie, oczekiwana użyteczność atakującego może być zwięźle przedstawiona w następującej formie:

$$U^a(x, y) = \sum_{i \in [n]} y_i(\rho_i(1 - x_i) + \xi_i x_i)$$

Widać też, że $U^a(x, y)$ ma również postać dwuliniową

$$x^T By + \beta y$$

dla pewnej niedodatniej macierzy diagonalnej B.

W grach o sumie zerowej wszystkie wyżej wymienione standardowe pojęcia równowagi są tym samym co równowaga minimaksowa, a zadaniem polegającym na rozwiązaniu gry jest obliczenie równowagi minimaksowej w czasie wielomianowym.

W przypadku, gdy gra nie ma sumy zerowej, głównym rozwiązaniem jest silna równowaga Stackelberga – obrońca odgrywa rolę lidera i może przyjąć strategię mieszaną, zanim atakujący wykona ruch. Atakujący obserwuje mieszaną strategię obrońcy i stara się reagować na nią w możliwie najlepszy sposób. W tym przypadku zadanie algorytmiczne polega na obliczeniu optymalnej strategii mieszanej dla obrońcy (należy zwrócić uwagę, że atakujący nie jest w stanie obserwować rozmieszczenia obrońcy w czasie rzeczywistym, tj. próbkowanej czystej strategii, ponieważ musi zaplanować atak przed próbkowaniem czystej strategii obrońcy w czasie rzeczywistym).

A.2 Bayesowskie gry bezpieczeństwa

Omówione w artykule rozwiązanie wdrożone na lotnisku LAX opierało się na szerszej klasie gier zwanych Bayesian Security Games (pol. bayesowskie gry bezpieczeństwa) lub Bayesian Stackelberg Games (bayesowskie gry Stackleberga). W opisie tej klasy gier podążamy za układem i notacją z pracy Nagórki i in.[35] oraz używamy omówionego wcześniej problemu ochrony granicy Białoruś–Ukraina jako przykładu ilustrującego działanie tego modelu.

W bayesowskiej grze Stackelberga obrońca gra przeciwko grupie atakujących n różnych typów. W każdej rundzie obrońca gra przeciwko jednemu atakującemu typu $1 \leq t \leq n$ losowo, z prawdopodobieństwem wynoszącym p_t. Atakujący mogą mieć do dyspozycji różne zestawy ruchów, które wyrządzają różne szkody obrońcy. W naszym przykładzie przedstawiamy atakującego o niskim profilu ($t = 1$) i atakującego o wysokim profilu ($t = 2$) wynoszącym

$$p_1 = {}^4\!/_5 \text{ i } p_2 = {}^1\!/_5.$$

Przyjmijmy, że I oznacza zbiór ruchów obrońcy. W omawianym przykładzie patrol graniczny przydziela dwie jednostki patrolujące do czterech segmentów granicy, a zatem $I = \{S_1S_2, S_1S_3, S_1S_4, S_2S_3, S_2S_4, S_3S_4\}$.

W bayesowskiej grze Stackelberga w pierwszej kolejności obrońca wybiera własną strategię mieszaną x. W przykładzie $x = \{x_i\}_{(i \in I)}$ stanowi miarę prawdopodobieństwa na I, oznaczaną przez $x \in Prob(I)$ z

$$Prob(I) = \{x: I \rightarrow R: \sum_{i \in I} x_i = 1 \, , x \geq 0\}$$

Strategia x nie zależy od t, ponieważ obrońca nie zna typu napastnika, którego napotka.

Przez J_t oznaczmy zbiór ruchów atakującego typu t. W tego rodzaju przykładzie $J_1 = J_2 = \{S_1, S_2, S_3, S_4, \varnothing\}$ atakujący mogą zaatakować jeden z segmentów granicznych lub wycofać się. Atakujący wybiera swoją strategię jako drugi, znając strategię obrońcy x. Chociaż na początku może się to wydawać sprzeczne z intuicją, dla obrońcy korzystne będzie ujawnienie atakującemu swojej strategii mieszanej (ale nie swoich aktualnych pozycji obronnych). Ujawnianie informacji w takich scenariuszach jest dość

[35] A. Nagórko, P. Ciosmak, T. Michalak, *Two-phase security games*...

powszechne, aby zmusić przeciwnika do korzystnej reakcji, czego przykładem jest akcja „Znicz" przeprowadzana co roku przez polską Policję[36].

W każdej rundzie gry obaj gracze poruszają się niezależnie, zgodnie ze strategiami x i $y^t(x)$, które wybrali wcześniej. Symbol $r_{i,t,j}$ oznacza wypłatę obrońcy przy zagraniu ruchu $i \in I$ przeciwko atakującemu typu $1 \leq t \leq n$, który zagrał ruch $j \in J_t$. Symbol $c_{i,t,j}$ oznacza wypłatę atakującego (która może różnić się od $-r_{i,t,j}$), ponieważ nie zakładamy, że gry mają sumę zerową.

Użyteczności graczy można zwięźle przedstawić za pomocą macierzy wypłat. W przedmiotowym przykładzie macierze wypłat dla ataku o wysokim profilu są następujące:

	S_1		S_2		S_3		S_4			∅
S_1S_2	51,	-50	102,	-100	-152,	150	-211,	200	0,	0
S_1S_3	55,	-50	-123,	100	175,	-150	-221,	200	0,	0
S_1S_4	59,	-50	-108,	100	-169,	150	206,	-200	0,	0
S_2S_3	-69,	50	101,	-100	168,	-150	-221,	200	0,	0
S_2S_4	-55,	50	113,	-100	-170,	150	212,	-200	0,	0
S_3S_4	-75,	50	-123,	100	166,	-150	211,	-200	0,	0

Pierwsza liczba w wierszu i i kolumnie j to punktacja obrońcy $r_{i,t,j}$ (w tym przypadku 1 oznacza atakującego o wysokim profilu $t = 1$). Druga liczba to $c_{i,1,j}$. Niskoprofilowy atak przynosi następujące wypłaty:

		S_1		S_2		S_3		S_4		∅
S_1S_2	14,	-10	23,	-20	-34,	30	-42,	40	0,	0
S_1S_3	10,	-10	-20,	20	32,	-30	-43,	40	0,	0
S_1S_4	12,	-10	-23,	20	-33,	30	44,	-40	0,	0
S_2S_3	-11,	10	24,	-20	31,	-30	-41,	40	0,	0
S_2S_4	-11,	10	20,	-20	-31,	30	42,	-40	0,	0
S_3S_4	-11,	10	-21,	20	34,	-30	44,	-40	0,	0

Atakujący t wybiera optymalną strategię $\overline{y}^t = \overline{y}^t(x)$, zależącą od znanej strategii obrońcy x, która maksymalizuje również oczekiwaną wypłatę

[36] *Policyjne działania Znicz*, https://policja.pl/pol/aktualnosci/210088,Policyjne-dzialania-ZNICZ.html [dostęp: 25 VI 2023].

$$\bar{c} = \sum_{i \in I} \sum_{j \in J_t} x_i \bar{y}_j^t c_{i,t,j}$$

Wypłata jest maksymalizowana przez zagranie zgodne ze strategią czystą, tj. y^t jest optymalna wtedy i tylko wtedy, gdy

$$\bar{c} \geq \sum_{i \in I} x_i c_{i,t,j}$$

Obrońca działa tak, aby zmaksymalizować swoją oczekiwaną wypłatę w stosunku do optymalnych strategii atakujących, tj. wybiera optymalną strategię *x*, która maksymalizuje jego oczekiwaną punktację:

$$\sum_{i \in I} \sum_{t=1}^{n} \sum_{j \in J_t} p_t x_i \bar{y}_j^t r_{i,t,j}$$

Stąd rozwiązanie bayesowskiej gry Stackelberga jest zadane przez następujący kwadratowy problem optymalizacyjny:

$$\max_{x, y^t} \sum_{i \in I} \sum_{t=1}^{n} \sum_{j \in J_t} p_t x_i y_j^t r_{i,t,j}$$

przy ograniczeniach:

$$\sum_{i \in I} x_i = 1$$

$$\sum_{j \in J_t} y_j^t = 1 \text{ dla każdego } 1 \leq t \leq n,$$

$$\sum_{i \in I} \sum_{j \in J_t} x_i y_j^t c_{i,t,j} \geq \sum_{i \in I} x_i c_{i,t,j} \text{ dla każdego } 1 \leq t \leq n, j \in J_t,$$

$$x \geq 0, y^t \geq 0 \text{ dla każdego } 1 \leq t \leq n$$

Opisana formalizacja w połączeniu z techniką linearyzacji prowadzi do sformułowania mieszanego całkowitoliczbowego programowania liniowego (ang. *mixed integer linear programming*) dla bayesowskich gier Stackelberga, opublikowanego w pracy Paruchuriego i in.[37] jako słynny algorytm DOBSS.

[37] P. Paruchuri i in., *Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games*, w: *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2008), t. 2, s. 895–902.

Bibliografia

An B. i in., *A Deployed Quantal Response-Based Patrol Planning System for the U.S. Coast Guard*, „Interfaces" 2013, t. 43, nr 5, s. 400–420. https://doi.org/10.1287/inte.2013.0700.

Bier V.M., Azaiez M.N., *Game Theoretic Risk Analysis of Security Threats*, Springer 2008, https://doi.org/10.1007/978-0-387-87767-9.

Blocki J. i in., *Audit games with multiple defender resources*, w: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* (AAAI 2015), t. 29, nr 1, s. 791–797.

Brown G. i in., *A Two-Sided Optimization for Theater Ballistic Missile Defense*, „Operations Research" 2005, t. 53, nr 5, s. 745–763. https://doi.org/10.1287/opre.1050.0231.

Fang F., Nguyen T.H., *Green security games: Apply game theory to addressing green security challenges*, „ACM SIGecom Exchanges" 2016, t. 15, nr 1, s. 78–83. https://doi.org/10.1145/2994501.2994507.

Gatti N. i in., *Game Theoretical Insights in Strategic Patrolling: Model and Algorithm in Normal-Form*, w: *Proceedings of the 2008 conference on ECAI 2008: 18th European Conference on Artificial Intelligence* (ECAI 2008), s. 403–407. https://doi.org/10.3233/978-1-58603-891-5-403.

Gholami S. i in., *Adversary models account for imperfect crime data: Forecasting and planning against real-world poachers*, w: *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2018), s. 823–831.

Guo Q. i in., *Coalitional security games*, w: *Proceedings of the 2016 15th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2016), s. 159–167.

Haskell W. i in., *Robust protection of fisheries with COmPASS*, w: *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence* (AAAI 2014), t. 28, nr 2, s. 2978–2983.

Hunt K., Zhuang J., *A review of attacker-defender games: Current state and paths forward*, „European Journal of Operational Research" 2023, w druku. https://doi.org/10.1016/j.ejor.2023.04.009.

Hutter F. i in., *Boosting Verification by Automatic Tuning of Decision Procedures*, w: *Proceedings of the 19th International Conference on Computer Aided Verification* (CAV 2007), s. 27–34.

Korzhyk D. i in., *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*, „Journal of Artificial Intelligence Research" 2011, t. 41, nr 2, s. 297–327.

Lye K-w., Wing J., *Game Strategies in Network Security*, „International Journal of Information Security" 2005, t. 4, s. 71–86. https://doi.org/10.1007/s10207-004-0060-x.

Nagórko A., Ciosmak P., Michalak T., *Two-phase security games*, w: *Proceedings of the Thirty-Nine Conference on Uncertainty in Artificial Intelligence* (UAI 2023), s. 1489–1498.

Nguyen T.H. i in., *Analyzing the effectiveness of adversary modeling in security games*, w: *Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence* (AAAI 2013), nr 1, s. 718–724.

Nguyen T.H. i in., *Towards a science of security games*, w: *Mathematical Sciences with Multidisciplinary Applications*, B. Toni (red.), Springer Cham 2016, s. 347–381.

Paruchuri P. i in., *Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games*, w: *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2008), t. 2, s. 895–902.

Pita J. i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57. https://doi.org/10.1609/aimag.v30i1.2173.

Sandler T., *Terrorism & Game Theory*, „Simulation & Gaming" 2003, t. 34, nr 3, s. 319–337. https://doi.org/10.1177/1046878103255492.

Shieh E. i in., *Protect: A deployed game theoretic system to protect the ports of the United States*, w: *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2012), t. 1, s. 13–20.

Sinha A. i in., *Stackelberg security games: Looking beyond a decade of success*, w: *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence* (IJCAI 2018), s. 5494–5501.

Stackelberg H. von, *Marktform und Gleichgewicht*, J. Springer 1934.

Tambe M., *Security and game theory: algorithms, deployed systems, lessons learned*, Cambridge 2011.

Tsai J. i in., *Iris – a tool for strategic security allocation in transportation networks*, w: *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2009), s. 37–44.

Vorobeychik Y., An B., Tambe M., *Adversarial Patrolling Games*, w: *Papers from the 2012 AAAI Spring Symposium*, t. 3, s. 91–98.

Vorobeychik Y., Pritchard M., *Plan interdiction games*, w: *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia i in. (red.), Springer Cham 2020, s. 159–182. https://doi.org/10.1007/978-3-030-33432-1_8.

Xu H., *The Mysteries of Security Games: Equilibrium Computation Be-Comes Combinatorial Algorithm Design*, w: *Proceedings of the 2016 ACM Conference on Economics and Computation* (ACM EC 2016), s. 497–514.

Yang R. i in., *Adaptive resource allocation for wildlife protection against illegal poachers*, w: *Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2014), s. 453–460.

Yang R. i in., *Improving Resource Allocation Strategy Against Human Adversaries in Security Games*, w: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence* (IJCAI 2011), s. 458–464.

Yang R. i in., *Improving resource allocation strategies against human adversaries in security games: An extended study*, „Artificial Intelligence" 2013, t. 195, s. 440–469. https://doi.org/10.1016/j.artint.2012.11.004.

Yin Z. i in., *Trusts: Scheduling randomized patrols for fare inspection in transit systems*, w: *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence* (AAAI 2012), t. 26, nr 2, s. 2348–2355.

Zhang Y., Malacaria P., *Bayesian Stackelberg games for cyber-security decision support*, „Decision Support Systems" 2021, t. 148, art. 113599. https://doi.org/10.1016/j.dss.2021.113599.

Źródła internetowe

Policyjne działania Znicz, https://policja.pl/pol/aktualnosci/210088,Policyjne-dzialania-ZNICZ.html [dostęp: 25 VI 2023].

Romanenko V., *Belarus uses migrants for intelligence on border with Ukraine*, Ukrainska Pravda, 6 XII 2022 r., https://www.pravda.com.ua/eng/news/2022/12/6/7379514/ [dostęp: 25 VI 2023].

Dr Tomasz P. Michalak

Lider samodzielnego zespołu badawczego w IDEAS NCBR oraz wykładowca na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Absolwent Wydziału Nauk Ekonomicznych Uniwersytetu Warszawskiego. W czasie kariery naukowej prowadził badania na Wydziale Informatyki Uniwersytetu Oksfordzkiego, w Szkole Inżynierii i Informatyki Uniwersytetu w Southampton, na Wydziale Informatyki Uniwersytetu w Liverpoolu oraz Wydziale Ekonomii Stosowanej Uniwersytetu w Antwerpii, na którym otrzymał tytuł doktora ekonomii.

Dr Michał T. Godziszewski

Specjalista w zakresie logiki i jej zastosowań (w matematyce, filozofii i informatyce), sztucznej inteligencji (specjalność – teoria systemów wieloagentowych: algorytmiczna teoria gier, analiza sieciowa, obliczeniowa teoria wyboru społecznego) i informatyki teoretycznej. Obecnie zajmuje się przede wszystkim analizą algorytmiczną sieci społecznych i gier Stackelberga, złożonością obliczeniową w teorii gier oraz ich zastosowaniami do modelowania systemów bezpieczeństwa.

Dr Andrzej Nagórko

Adiunkt na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Były pracownik Instytutu Matematycznego Polskiej Akademii Nauk oraz uniwersytetów w Stanach Zjednoczonych i Izraelu. Od lat stosuje metody optymalizacji matematycznej w różnych dziedzinach – od sztucznej inteligencji poprzez teorię gier po geometryczną teorię grup. W IDEAS NCBR pracuje nad zastosowaniami tych metod do ochrony infrastruktury krytycznej.

https://doi.org/10.4467/27204383TER.23.018.18320

https://orcid.org/0000-0002-4015-5774
https://orcid.org/0000-0002-2761-3144
https://orcid.org/0009-0000-7130-0455

PAWEŁ OPITEK
AGNIESZKA BUTOR-KELER
KAROL KANCLERZ

Wybrane aspekty przestępczości z wykorzystaniem walut wirtualnych

Abstrakt

Artykuł składa się z dwóch części. W pierwszej omówiono zagadnienia związane z funkcjonowaniem rynku kryptoaktywów w Polsce i na świecie oraz planowanymi zmianami w przepisach regulujących ten rynek. Dotyczą one statusu prawnego tokenów cyfrowych i ich wykorzystania w procederze prania pieniędzy i finansowania terroryzmu oraz obowiązków instytucji obowiązanych w systemie przeciwdziałania praniu pieniędzy. W drugiej części skupiono się na kwestiach procesowych i pozaprocesowych związanych z kryptowalutami. Omówiono status cyfrowego artefaktu w postępowaniu karnym, pracę operacyjną oraz prowadzenie śledztwa pod kątem zwalczania przestępczości kryptowalutowej. W podsumowaniu przedstawiono postulaty skierowane do organów ścigania i ochrony prawa. Celem artykułu jest przegląd problematyki dotyczącej wykorzystania walut wirtualnych w popełnianiu przestępstw, zwłaszcza zagadnień z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Słowa kluczowe:

kryptowaluty,
waluty wirtualne,
przestępczość,
pranie pieniędzy,
finansowanie terroryzmu,
śledztwo,
ślady i dowody cyfrowe

Waluty wirtualne stały się nieodłącznym elementem popełniania różnego rodzaju przestępstw – stanowią one przedmiot czynności wykonawczej, gdy sprawca pozbywa osobę uprawnioną władztwa nad bitcoinami, a statuujące je dane binarne stają się obiektem nieuprawnionych manipulacji. Nierzadko kryptowaluty są wykorzystywane do prania pieniędzy, uzyskiwania okupu za ataki oparte na socjotechnice lub oprogramowaniu typu ransomware. Dochodzi także do malwersacji finansowych z wykorzystaniem kryptowalut i crowdfundingu, platform działających podobnie jak tradycyjny rynek Forex czy piramid finansowych, których klienci są kuszeni obietnicą szybkiego i wysokiego zysku po zainwestowaniu w tokeny. Są również emitowane kryptoaktywa stanowiące de facto pochodne instrumenty finansowe z ominięciem przepisów regulujących funkcjonowanie rynku kapitałowego. Zjawisko kryptowalut jest analizowane nie tylko w kontekście modus operandi sprawców czynów zabronionych. Wiążą się z nim także inne ważne zagadnienia, takie jak: status prawny tokenów, analiza kryminalna transferów kryptowalutowych, tymczasowe zajęcie mienia ruchomego i zabezpieczenie majątkowe na bitcoinie lub innych altcoinach, procedury uzyskiwania śladów cyfrowych i międzynarodowa pomoc prawna w tym zakresie czy administracyjne procedury AML/CFT (ang. *Anti-Money Laundering/Counter Financing of Terrorism*). Niniejszy artykuł stanowi ujęcie tych wszystkich zagadnień, jednak z uwagi na jego ograniczoną objętość tylko niektóre z nich mogły zostać omówione bardziej szczegółowo.

Na wstępie warto zadać pytanie: czy polskim organom ścigania przestępstw w ogóle są potrzebne zdolności dotyczące pracy z kryptoaktywami? Odpowiedź na tak postawione pytanie jest z całą pewnością twierdząca, co wynika z kilku powodów. Najogólniej rzecz biorąc, współczesny obraz przestępczości zbyt często jest powiązany z walutami wirtualnymi i technologią tworzącą system rozproszonych rejestrów, aby formacje przeznaczone do ochrony ekonomicznych interesów państwa nie orientowały się w prawnych, ekonomicznych i technicznych aspektach ich funkcjonowania. Ale są też konkretne sprawy, które zobowiązują np. Agencję Bezpieczeństwa Wewnętrznego do zainteresowania się kryptowalutami. Służą one do prania pieniędzy na dużą skalę, a ABW jest zobligowana do rozpoznawania i wykrywania przestępstw godzących w podstawy ekonomiczne państwa oraz zapobiegania im. Bezpieczeństwo to także przestrzeganie przez Polskę zawartych umów międzynarodowych, gdyż ma to bezpośredni wpływ na jej pozycję i renomę na arenie światowej. W tym kontekście warto przypomnieć, że sankcje nałożone na Rosję i Białoruś po agresji Federacji

Rosyjskiej na Ukrainę obejmują także kryptoaktywa i polskie służby nie mogą dopuścić do tego, aby te sankcje były omijane z wykorzystaniem krajowych dostarczycieli usług sieciowych. Anonimowe transfery na blockchainie mogą również stanowić dogodne narzędzie do wspierania organizacji terrorystycznych i agentury wpływu istniejącej w różnych państwach, także w Polsce. Agencja Bezpieczeństwa Wewnętrznego ma za zadanie kontrolować ten segment szeroko pojętego rynku finansowego w celu zapobiegania takim działaniom.

Artykuł opiera się na dwóch celach badawczych: analizie aktualnego statusu prawnego i faktycznej funkcjonalności kryptoaktywów na świecie oraz ustaleniu, czy wiążą się one i na jaką skalę z popełnianiem czynów zabronionych, w tym z praniem pieniędzy oraz finansowaniem terroryzmu. W tym drugim przypadku, oprócz krytycznego spojrzenia na międzynarodowy wymiar omawianej przestępczości, podjęto także bliski autorom opracowania temat działań organów ścigania w zakresie walki z przestępczością kryptowalutową. Analiza omawianej przestępczości w skali mikro (krajowej) i makro (globalnej) doprowadziła do wskazania działań, które wymagają od organów ścigania wiedzy na temat kryptowalut i wykorzystania jej w praktyce.

Zastosowana metodologia badań polegała na obserwacji oraz analizie różnorodnych źródeł internetowych związanych z walutami wirtualnymi i ustaleniu sposobów funkcjonowania tych walut oraz na przemyśleniach autorów artykułu na temat rozpatrywanych zagadnień. Autorzy zapoznali się m.in. z informacjami zawartymi na stronach specjalistycznych firm z branży krypto oraz organizacji rządowych, w tym z raportem z przeprowadzonego w Kongresie Stanów Zjednoczonych wysłuchania przedstawicieli służb walczących z terroryzmem poświęconego aktywności ekstremistów w świecie wirtualnym. Ponadto autorzy – na podstawie własnych kompetencji i doświadczeń zawodowych zdobytych w ramach zajmowania się sprawami karnymi czy też realizacji zadań nadzorczych nad rynkiem kapitałowym – przedstawili wnioski na temat przestępczości kryptowalutowej i działalności polskich służb w tym zakresie. Skonfrontowano je z materiałami źródłowymi w postaci analiz, raportów oraz innych opracowań organizacji i instytucji zajmujących się cyfrowymi tokenami i technologią blockchain. Odwołano się także do obowiązujących lub będących w fazie projektowania aktów prawnych regulujących rynek krypto. Finalnie, na podstawie całości uzyskanych informacji, zastosowano metodę

indukcyjną polegającą na zapisaniu spostrzeżeń poczynionych w odniesieniu do stwierdzonego wcześniej zbioru danych.

W artykule określenia: kryptowaluty, waluty wirtualne i kryptoaktywa (aktywa cyfrowe) są używane zamiennie, gdyż dotyczy on przestępczości i ta dowolność terminologiczna nie ma większego znaczenia dla opisu tematu badań. Należy jednak podkreślić, że określeniem o najszerszym zakresie pojęciowym są kryptoaktywa, chociaż w prawie polskim brakuje ich definicji legalnej. Według *Rozporządzenia wykonawczego Prezydenta Stanów Zjednoczonych z dnia 9 marca 2022 r. w sprawie zapewnienia odpowiedzialnego rozwoju zasobów cyfrowych*[1] pojęcie aktywów cyfrowych odnosi się do pieniędzy cyfrowych emitowanych przez bank centralny (ang. *central bank digital currency*, CBDC) niezależnie od zastosowanej technologii ich emisji oraz do innych reprezentacji wartości, w tym papierów wartościowych, pochodnych instrumentów finansowych oraz innych produktów finansowych, które są wykorzystywane do dokonywania płatności, inwestowania, przesyłania lub wymiany funduszy lub ich ekwiwalentu, emitowane lub reprezentowane w formie cyfrowej przy użyciu technologii rozproszonej księgi rozrachunkowej (ang. *distributed ledger technology*, DLT) niezależnie od nazwy produktu. Pojęcie kryptowalut dotyczy natomiast aktywów cyfrowych, które mogą być środkiem wymiany, generowanych lub obsługiwanych przez technologię DLT. Pośrodku zakresów pojęciowych tych dwóch określeń lokują się waluty wirtualne.

Status prawny tokenów cyfrowych

Waluty wirtualne są różnie traktowane na świecie pod względem regulacji prawnych. Mimo że w niektórych państwach uznano je za prawny środek płatniczy, to są to sytuacje wyjątkowe, gdyż najczęściej odmawia się im pozycji podobnej do tej, jaką ma pieniądz fiducjarny. Wynika to z tego, że rządy poszczególnych państw rygorystycznie strzegą swojego monopolu na emisję pieniądza, gdyż dzięki niemu mogą kształtować politykę monetarną kraju i wpływać na procesy gospodarcze. Badania przeprowadzone przez Międzynarodowy Fundusz Walutowy pokazują, że najmocniejszą pozycję

[1] *Ensuring Responsible Development of Digital Assets*, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [dostęp: 5 IV 2023]. Tłumaczenia w artykule pochodzą od autorów (dop. red.).

waluty wirtualne zyskały w Afryce Subsaharyjskiej, gdzie 25% krajów szczegółowo uregulowało ich status prawny, a ponad połowa z nich zdecydowała się na zniesienie wielu ograniczeń dotyczących funkcjonowania kryptowalut na tradycyjnym rynku finansowym[2]. Dotyczy to jednak regulacji w zakresie tokenów płatniczych, takich jak bitcoin, a więc najprostszych w swoim działaniu. Na przykład w październiku 2021 r. Bank Centralny Nigerii wprowadził wirtualnego tokena o nazwie eNaira jako wsparcie dla tradycyjnego pieniądza fiducjarnego. System opracowała firma Fintech Bitt, a dwie aplikacje do korzystania z eNairy – eNaira Speed Wallet i eNaira Merchant Wallet – są dostępne w sklepach z aplikacjami Google i Apple. W 2022 r. wyemitowano już 500 mln eNair (1,21 mln dolarów), ale nigeryjski rząd jednocześnie zakazał dokonywania transakcji we własnym sektorze bankowym innymi kryptowalutami[3].

W krajach wysoko rozwiniętych podejmuje się natomiast inicjatywy mające na celu usystematyzowanie podejścia do zaawansowanych tokenów cyfrowych emitowanych na podstawie technologii blockchain i podobnych w działaniu do pochodnych instrumentów finansowych. Prace nad tokenizacją takich instrumentów są bardzo zaawansowane w Japonii. W październiku 2021 r. MUFG, największy japoński bank, ogłosił wyniki prac grupy Security Token Research Consortium (przemianowanej w 2022 r. na Digital Asset Co-creation Consortium) zajmującej się budową infrastruktury dla tokenizowanych papierów wartościowych. Zaplanowano ewidencjonowanie obrotu nimi na blockchainie korporacyjnym Corda. Prawo podłączenia się do niego przyznano innym firmom zainteresowanym cyfrowymi instrumentami finansowymi – papierami wartościowymi notowanymi na giełdzie Osaka Digital Exchange, która zintegrowała się z platformą Progmat i umożliwia dokonywanie transakcji P2P (ang. *peer-to-peer*)[4] pomiędzy inwestorami[5]. Platforma cały czas poszerza swoją funkcjonalność

[2] *Living on the Edge*, International Monetary Fund, październik 2022 r., https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [dostęp: 5 IV 2023].

[3] P. Opitek, *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain*, Łódź 2022, s. 214.

[4] Transakcje P2P – transakcje dokonywane między osobami fizycznymi z wyłączeniem pośredników, np. sklepów, oraz fabryk i korporacji (przyp. red.).

[5] *MUFG, SBI share roadmap for Japanese security tokens*, Ledger Insights, 7 X 2021 r., https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [dostęp: 27 III 2023].

(rozrosła się z 80 firm do 163 pod koniec 2022 r.) i obecnie kładzie nacisk na rozwój i obrót stablecoinem, umożliwiającym dokonywanie rozliczeń poza oficjalnym systemem bankowym[6].

Po drugiej stronie plasują się państwa, które całkowicie zakazały posiadania walut wirtualnych, tj. Chiny, Nepal, Bangladesz, Afganistan, Maroko, Algieria i Boliwia[7]. W przypadku Państwa Środka istnieje kilka powodów, dlaczego tak się stało. Chiny mają kilkuletnią przewagę nad resztą rozwiniętych gospodarek globu w rozwoju narodowej waluty cyfrowej Banku Centralnego, a więc tamtejszy rząd mógł postrzegać zdecentralizowane aktywa jako konkurencję zagrażającą projektowi scentralizowanego juana. Ponadto ustrój ekonomiczny Chin preferuje odgórne zarządzanie rynkiem finansowym i zapewne istnienie autonomicznego bitcoina nie jest dla niego korzystne. W rezultacie chińskie władze zaczęły prowadzić politykę antykryptowalutową i medialne akcje marketingowe odradzające korzystanie z bitcoinów i altcoinów. Ostatecznie wprowadzono zakaz wyszukiwania w Internecie haseł związanych z kryptowalutami, jak również zamykanie cyfrowych platform[8].

W Stanach Zjednoczonych oraz w państwach Unii Europejskiej posiadanie walut wirtualnych jest dozwolone, a jedyne obowiązki z tym związane dotyczą jakieś formy rejestracji (zgłoszenia) działalności gospodarczej prowadzonej z wykorzystaniem kryptowalut. Problematyczna jest emisja instrumentów finansowych na blockchainowych protokołach. W Europie takie działania są zasadniczo zabronione, a w Stanach Zjednoczonych obowiązuje zasada neutralności technologicznej i można tokenizować instrumenty finansowe, chociaż w praktyce jest to obwarowane koniecznością spełnienia wielu wymogów i generalnie nieopłacalne. Niedawno Biały Dom opublikował pierwszy raz w historii wytyczne w celu kompleksowego określenia ram odpowiedzialnego rozwoju zasobów cyfrowych w Stanach Zjednoczonych. Zgodnie z zarządzeniem prezydenta Joe Bidena administracja tego kraju sformułowała zalecenia dotyczące ochrony konsumentów, inwestorów, przedsiębiorstw, stabilności finansowej, bezpieczeństwa

---

[6] *MUFG's Progmat security token platform to become digital asset joint venture,* Ledger Insights, 22 XII 2022 r., https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [dostęp: 5 IV 2023].

[7] F. O'Sullivan, *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency,* Cloudwards, 22 II 2023 r., https://www.cloudwards.net/where-is-crypto-illegal/ [dostęp: 5 IV 2023].

[8] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, s. 212.

narodowego i środowiska w kontekście funkcjonowania rynku krypto. Rozporządzenie wykonawcze z 9 marca 2022 r. w sprawie zapewnienia odpowiedzialnego rozwoju zasobów cyfrowych[9] nakreśliło nowatorskie podejście do przeciwdziałania zagrożeniom oraz wykorzystania potencjalnych korzyści płynących z zasobów cyfrowych i leżącej u ich podstaw technologii. Agencje rządowe opracowały ramy i zalecenia wspierające m.in. ochronę konsumentów i inwestorów, promowanie stabilności finansowej i konkurencyjności gospodarczej oraz innowacyjności. Stany Zjednoczone są uznawane także za światowego lidera w stosowaniu procedur przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w środowisku zasobów cyfrowych i ustanawiają w tej sferze globalne standardy. Biały Dom zaznaczył, że popularność kryptoaktywów spowodowała także wzrost liczby cyberprzestępców dokonujących m.in. prania pieniędzy oraz finansowania nielegalnej działalności. W celu przeciwdziałania takim praktykom konieczne są: zwiększenie zakresu regulacji dotyczących rynku kryptowalut i nadzoru nad nim, intensywniejsze zaangażowanie organów ścigania w walkę z omawianą przestępczością oraz zmiana przepisów prawa, w tym najważniejszej amerykańskiej ustawy o tajemnicy bankowej (ang. *The Bank Secrecy Act*, BSA), zaostrzenie kar przewidzianych za anonimowe przesyłanie wartości majątkowych w formie krypto oraz sprawienie, aby dotyczyły one także dostawców usług związanych z giełdami internetowymi i niewymienialnych NFT (ang. *non-fungible token* – niepowtarzalne tokeny utożsamiające zdigitalizowane dzieło sztuki, np. rzeźbę lub obraz malarski). W ramach podjętych działań Biały Dom zobowiązał Departament Sprawiedliwości USA do ścigania poważnych przestępstw związanych z aktywami cyfrowymi dokonywanych w dowolnej jurysdykcji, a Ministerstwo Skarbu do finalizacji w 2023 r. oceny ryzyka nielegalnego finansowania zdecentralizowanych finansów[10].

W UE z kolei brakuje – zdaniem Komisji Europejskiej – jednolitych przepisów mających zastosowanie do usług związanych z kryptoaktywami, co naraża konsumentów i inwestorów instytucjonalnych na znaczne ryzyko strat. Ponadto fakt, że niektóre państwa członkowskie wprowadziły na szczeblu krajowym stosowne regulacje, a inne tego nie zrobiły, prowadzi

[9] *Ensuring Responsible Development*...

[10] *White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, The White House, 16 IX 2022 r., https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [dostęp: 9 IV 2023].

do fragmentacji wspólnego prawa, która zakłóca konkurencję na jednolitym europejskim rynku, utrudnia usługodawcom rozszerzanie ich działalności na skalę transgraniczną i prowadzi do arbitrażu regulacyjnego. Dlatego Parlament Europejski wkrótce przegłosuje przyjęcie rozporządzenia w sprawie rynków kryptaktywów (ang. *Markets in Crypto-assets*, MiCA). Rozporządzenie ustanowiłoby zharmonizowane na szczeblu UE przepisy dotyczące takich wartości majątkowych, zapewniając w ten sposób pewność prawa w odniesieniu do kryptoaktywów nieobjętych obowiązującym prawodawstwem unijnym. Ma to zwiększyć ochronę konsumentów i inwestorów oraz stabilność finansową, promować innowacje i możliwości wykorzystania tokenów opartych na technologii DLT. Rozporządzenie ustanawia trzy rodzaje kryptoaktywów: tokeny powiązane z aktywami (przypominające stablecoiny), tokeny pieniądza elektronicznego oraz kryptoaktywa nieobjęte prawodawstwem UE. Już we wstępnym porozumieniu negocjacyjnym ustalono bardzo istotne kwestie, takie jak chociażby zabezpieczenie płynności i wykupu kryptoaktywów w taki sposób, aby były one zabezpieczone wartością walut referencyjnych (reguła 1:1). Emitent kryptoaktywów będzie zobowiązany zapewnić ich wykup w razie zawirowań na rynku. Ma to na celu zapewnienie wysokiego poziomu ochrony konsumentów i inwestorów oraz integralności ekosystemu krypto, a także minimalizację zagrożeń dla stabilności finansowej i polityki pieniężnej, które mogą wyniknąć z szerokiego wykorzystania kryptoaktywów i technologii DLT w praktyce[11].

Parlament Europejski pracuje także nad nowym rozporządzeniem mającym na celu zaostrzenie polityki dotyczącej walut wirtualnych przez zlikwidowanie luki regulacyjnej. Zaostrzenie to ma polegać na zobowiązaniu zdecentralizowanych organizacji typu DAO[12], platform NFT i DeFi[13]

---

[11] *Proposal for a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [dostęp: 9 IV 2023]; *Markets in crypto-assets (MiCA)*, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221 [dostęp: 9 IV 2023].

[12] DAO (ang. *decentralized autonomous organization*) – zdecentralizowana organizacja, która podejmuje autonomiczne decyzje zarządcze zgodnie z wolą posiadaczy tokenów *governance*, czyli takich, które dają prawo głosowania.

[13] DeFi (ang. *decentralized finance*) – zdecentralizowany system finansowy zaprojektowany dla nieograniczonej liczby inwestorów, przeznaczonych dla nich blockchainowych platform, produktów i usług finansowych oraz ich twórców. DeFi korzysta na różne sposoby z pieniądza fiducjarnego, rachunków bankowych czy bezgotówkowych systemów płatności, jednak najważniejsze są kryptowaluty, innowacyjne protokoły rozproszonego rejestru

do przestrzegania przepisów AML na takich samych zasadach, jakie obowiązują tradycyjne podmioty rynku finansowego. W kwietniu 2023 r. Departament Skarbu Stanów Zjednoczonych opublikował pierwszą na świecie kompleksową ocenę ryzyka związanego z nielegalnym finansowaniem DeFi. Wynika z niej, że przestępcy chętnie wykorzystują usługi rynku „zdecentralizowanych finansów", przede wszystkim do czerpania korzyści z ataków ransomware, kradzieży, oszustw, handlu narkotykami i finansowania proliferacji, a także działań wspierających terroryzm. Najważniejsze czynniki ułatwiające im takie działania wynikają z nieobowiązywania w DeFi procedur AML/CFT i KYC[14], małego stopnia cyberbezpieczeństwa protokołów oraz tego, że ich administratorzy działają często w jurysdykcjach nierespektujących mechanizmów międzynarodowej pomocy prawnej lub w ogóle nie sposób ich powiązać z jakimkolwiek terytorium[15]. Planuje się zatem zobowiązać instytucje kredytowe i finansowe do stosowania wyśrubowanych reguł należytej staranności przy realizacji transakcji krypto o wartości przekraczającej 1000 euro, a relacje biznesowe z komercyjnymi podmiotami nielicencjonowanymi byłyby całkowicie zabronione. Taki sam limit, tj. 1000 euro, dotyczyłby przelewów pochodzących z portfeli hostowanych samodzielnie, kiedy ustalenie personaliów posiadacza takiego portfela jest znacznie utrudnione. Władze UE zaproponowały również ustanowienie nowego organu ds. przeciwdziałania praniu pieniędzy, który będzie nadzorował i egzekwował przepisy AML we wszystkich 27 krajach UE[16].

---

i inteligentne umowy (ang. *smart contracts*) przypominające konta bankowe i lokaty, różne formy kredytów oraz finansowe instrumenty pochodne. Klienci indywidualni oraz instytucjonalni dostarczają kapitał dla funkcjonowania DeFi i oczekują zysku z poczynionych inwestycji, tym bardziej że oferowana stopa zarobku jest często znacznie wyższa niż na tradycyjnym rynku kapitałowym. Z drugiej strony inwestowanie w DeFi wiąże się ze stosunkowo dużym ryzykiem utraty zaangażowanych środków lub brakiem korzyści obiecanych przez tradera. Decentralizacja DeFi oznacza, że nie ma jednej wiodącej organizacji czy instytucji, która odpowiada za cały system bądź jego poszczególne elementy. Zob. P. Opitek, *Funkcjonowanie instrumentów finansowych*..., s. 156.

[14] KYC (ang. *Know Your Customer*) – procedura należytej staranności, którą instytucje finansowe oraz inne prawnie określone podmioty muszą przeprowadzać w celu zidentyfikowania swoich klientów (przyp. red.).

[15] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. Department of the Treasury, kwiecień 2023 r., https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [dostęp: 14 IV 2023].

[16] I. Preiss, *Crypto AML rules passed by MEPs*, The Block, 28 III 2023 r., https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [dostęp: 6 IV 2023].

W polskim prawie jedyna definicja legalna dotycząca tokenów cyfrowych zakotwiczonych w blockchainie znajduje się w *Ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (dalej: u.p.p.p.). Zbudowana jest ona z dwóch elementów: mówi, czym waluta wirtualna nie jest (np. prawnym środkiem płatniczym), oraz wymienia jej pozytywne cechy, takie jak: cyfrowe odwzorowanie wartości, wymienialność w obrocie gospodarczym na prawne środki płatnicze, akceptowalność jako środka wymiany, możliwość elektronicznego przechowywania lub przeniesienia albo możliwość bycia przedmiotem handlu elektronicznego. Chociaż szczegółowa analiza prawna tej definicji[17] wykracza poza ramy niniejszego artykułu, to należy zaznaczyć, że w praktyce jej wykładnia oraz stosowanie sprawia wiele trudności. Nie ulega wątpliwości, że dotyczy ona bitcoina i pozostałych altcoinów, ale można odnieść wrażenie, że organy nadzoru nad rynkiem finansowym nie potrafią jednoznacznie odnieść się do pytania, czy art. 2 ust. 2 pkt 26 u.p.p.p. dotyczy także stablecoinów lub tokenów NFT. Można zaryzykować tezę, że polski ustawodawca nie zamierza podjąć samodzielnych działań w kierunku ściślejszego uregulowania rynku krypto, tylko czeka na zmiany procedowane w Parlamencie Europejskim. Jest to po części uzasadnione tym, że wspólna europejska polityka dotycząca kryptoaktywów jest kształtowana na poziomie unijnym i nie ma sensu wprowadzać specyficznych rozwiązań krajowych w przeddzień wejścia w życie takich regulacji, jak np. MiCA.

Pranie pieniędzy z wykorzystaniem walut wirtualnych

Przestępstwo prania pieniędzy zostało stypizowane w art. 299 Kodeksu karnego[18] i jako przedmiot ochrony zakłada bezpieczeństwo obrotu gospodarczego oraz legalne pochodzenie wartości majątkowych. Spośród opisanych w tym przepisie przedmiotów czynności wykonawczej, jak np. środki płatnicze, instrumenty finansowe, papiery wartościowe, to waluta wirtualna będzie wchodziła w zakres prawa majątkowego. Pojęcie prawa majątkowego odnosi się bowiem do wszelkich praw, które realizują interes

[17] Taka analiza została przeprowadzona w artykule: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Consilium Iuridicum" 2022, nr 3–4, s. 122–139.

[18] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*.

ekonomiczny uprawnionego i składają się na jego majątek[19]. Jak wynika z *Crypto Crime Report*[20] firmy Chainanalysis, w latach 2017–2022 waluty wirtualne wykorzystano w procederze „prania" na kwotę ponad 33 mld dolarów, a transfer znacznej części owej wartości dokonywał się z wykorzystaniem giełd internetowych. Tylko w 2021 r. ten wolumen wyniósł prawie 9 mld dolarów, z czego ponad 750 mln transferowano na platformy DeFi. Obserwowane trendy wskazują, że platformy zdecentralizowanych finansów stają się coraz popularniejszym środowiskiem do inwestowania nielegalnie uzyskanych środków, a rok 2022 był pod tym względem rekordowy[21]. Rezultatem tego są, wspomniane wcześniej, prace Parlamentu Europejskiego i administracji Stanów Zjednoczonych nad ściślejszym objęciem DeFi regulacjami AML.

Doświadczenie zawodowe autorów artykułu także potwierdza, że waluty wirtualne są wykorzystywane do popełniania różnego rodzaju przestępstw, m.in. handlu narkotykami, przemytu broni, oszustw, uchylania się od płacenia podatków, cyberataków, opłacania działań sabotażowo-dywersyjnych, handlu ludźmi i czynów związanych z wykorzystaniem dzieci na tle seksualnym. Od pewnego czasu postrzega się kryptowaluty jako potencjalne źródło finansowania korupcji, ale badania tego zjawiska miały ogólny charakter i opierały się bardziej na przypuszczeniach niż na przekonującej metodologii[22]. Sprawa Sama Bankmana-Frieda pokazała jednak, że taka przestępczość istnieje. Bankman-Fried został oskarżony przez amerykańskiego prokuratora o zdefraudowanie miliardów dolarów wpłaconych przez oszukanych klientów na rzecz jego firmy o nazwie FTX.com operującej kryptowalutami. W śledztwie ustalono, że chcąc zapewnić sobie przychylność polityków, Bankman-Fried wpłacał milionowe darowizny na kampanie wyborcze zarówno Partii Demokratycznej, jak i Partii Republikańskiej[23]. Ponadto w listopadzie 2021 r. miał wręczyć

[19] *Prawo cywilne – część ogólna*, M. Safjan (red.), seria: System Prawa Prywatnego, t. 1, Warszawa 2007, s. 717.

[20] Chainalysis, *The 2022 Crypto Crime Report*, luty 2022 r.

[21] Tamże.

[22] Zob. M. Alnasaa i in., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022 r., https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [dostęp: 4 V 2023].

[23] *United States of America v. Samuel Bankman-Fried*, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [dostęp: 9 IV 2023].

łapówkę w wysokości 40 mln dolarów co najmniej jednemu chińskiemu urzędnikowi w zamian za skłonienie go do odblokowania przez Państwo Środka kryptowalut o wartości miliarda dolarów zajętych przez chińskie organy ochrony prawa[24].

Okazuje się ponadto, że międzynarodowe organizacje przestępcze coraz częściej używają tokenów cyfrowych do przenoszenia i ukrywania zysków z handlu narkotykami. Dotyczy to przede wszystkim krajów Ameryki Łacińskiej, w których nielegalne grupy wykorzystują giełdy działające bez procedur KYC i AML, aby wyprać miliardy dolarów rocznie i tą drogą przenieść część swoich zasobów finansowych do świata wirtualnego w celu uniknięcia wykrycia przez prokuraturę i konfiskaty „owoców przestępstwa". Dotyczy to m.in. meksykańskich karteli Cártel Jalisco Nueva Generación i Sinaloa Cartel, a także Mara Salvatrucha z Ameryki Środkowej oraz Primeiro Comando da Capital z Brazylii. W tych samych obszarach geograficznych rosnąca liczba skorumpowanych rządów specjalnie dereguluje rynek krypto, aby zainwestowane na nim środki uzyskane w wyniku przekupstwa pozostały anonimowe. Takie działania pokrywają się z interesami Rosji, której sojusznicy w Ameryce Południowej, jak np. reżim Maduro w Wenezueli, opracowali własne systemy kryptowalutowe pozwalające uniknąć sankcji nałożonych na Federację Rosyjską przez państwa euroatlantyckie i ominięcie zachodnich rynków walutowych. Wenezuelską kryptowalutę petro wykorzystuje się do transferów wartości między Wenezuelą a Rosją za pośrednictwem rosyjskich banków[25]. Takiej aktywności dotyczył akt oskarżenia wniesiony przez prokuratora w październiku 2022 r. do Sądu Federalnego w Nowym Jorku. Pięciu obywatelom Rosji postawiono w nim zarzuty związane z nielegalnymi zakupami technologii wojskowej dla Federacji Rosyjskiej (m.in. zaawansowanych półprzewodników i mikroprocesorów stosowanych w samolotach myśliwskich, systemach rakietowych i kosmicznych systemach wojskowych), jej przemytu oraz prania pieniędzy z wykorzystaniem kryptowalut. W procederze noszącym znamiona przestępstwa uczestniczyli

[24] M. Sigalos, R. Goswami, *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023 r., https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [dostęp: 9 IV 2023].

[25] D. Farah, M. Richardson, *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023 r., https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [dostęp: 6 IV 2023].

także przedstawiciele Petróleos de Venezuela S.A., wenezuelskiej państwowej firmy naftowej. Złożony schemat przestępczy przewidywał m.in. transfery kryptowalut o wartości milionów dolarów, które posłużyły do zakupów technologii poza oficjalnym rynkiem finansowym, a także „wyprania" wpływów z nielegalnych działań[26]. W tym kontekście można dodać, że 2 marca 2022 r. Prokurator Generalny USA powołał Task Force KleptoCapture jako grupę zadaniową organów ścigania, której zadaniem jest egzekwowanie szeroko zakrojonych sankcji i ograniczeń eksportowych nałożonych na Rosję.

W UE i Stanach Zjednoczonych standardy w zakresie uregulowań o charakterze administracyjnym poświęconych regulacji rynku walut wirtualnych pod kątem przeciwdziałania praniu pieniędzy są kształtowane przez Grupę Specjalną ds. Przeciwdziałania Praniu Pieniędzy (ang. Financial Action Task Force, FATF[27]). W 2021 r. zaktualizowała ona swoje wytyczne dotyczące podejścia opartego na ryzyku w stosunku do obrotu walutami wirtualnymi i usługodawców operujących na tym rynku (ang. Virtual Assets Service Poviders, VASP)[28]. W raporcie FATF pt. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*[29] (wrzesień 2020 r.) wskazano zalety technologiczne kryptoaktywów i blockchaina, ale też zagrożenia, jakie generuje nowa technologia. Nadużyciom sprzyja duża anonimowość transferów, funkcjonowanie serwisów bezpośredniej wymiany wartości typu P2P, „tumblerów" i „mikserów", a także odmienność uregulowań prawnych dotyczących walut wirtualnych istniejących w różnych jurysdykcjach. Samo pojęcie tokena cyfrowego ma bowiem wieloznaczny charakter i poszczególne tokeny mogą różnić się między

[26] *Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme*, United States Attorney's Office, Eastern District of New York, 19 X 2022 r., https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [dostęp: 7 IV 2023].

[27] Financial Action Task Force została utworzona w 1989 r. przez Międzynarodowy Fundusz Walutowy i obecnie skupia 37 krajów członkowskich. Celem FATF jest definiowanie standardów i promowanie środków prawnych służących do zwalczania prania pieniędzy, finansowania terroryzmu i innych poważnych zagrożeń integralności globalnego systemu finansowego. Chociaż FATF nie decyduje wprost o rozwiązaniach w zakresie AML/CFT przyjętych przez poszczególne kraje, to de facto ma zasadniczy wpływ na ich kształt.

[28] Virtual Asset Service Provider to dostarczyciel platformy wirtualnej i innych usług służących do zarządzania walutami wirtualnymi.

[29] *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [dostęp: 7 IV 2023].

sobą pod wieloma względami. Przekłada się to na działanie prokuratora, który staje niekiedy przed trudnym zadaniem ustalenia, czym są kryptoaktywa ujawnione w toku śledztwa.

Podkreśla się rolę poszczególnych państw w zwalczaniu omawianej przestępczości oraz wskazuje, w jaki sposób powinny one monitorować zagrożenia i oceniać ryzyko z nimi związane. Walka z praniem pieniędzy na rynku krypto pozostaje przedmiotem stałego zainteresowania UE, a państwa Starego Kontynentu inkorporowały do swojego ustawodawstwa instytucje przeciwdziałające procederowi prania pieniędzy albo są w trakcie wprowadzania nowych rozwiązań. Chodzi m.in. o zasadę *travel rule*, która dotyczy przekazywania i udostępniania informacji o transakcjach przez dostawców usług działających na rynku aktywów wirtualnych. Takie rozwiązanie zwiększa przejrzystość transferów, a więc możliwości ustalenia osób zaangażowanych w operacje i blokowania podejrzanych środków. Wdrożenie *travel rule* ogranicza także ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu, zwłaszcza w odniesieniu do transferów o charakterze międzynarodowym[30]. Kolejny instrument porządkowania rynku krypto dotyczy obowiązku ustanowienia w każdym państwie UE rejestru dla podmiotów prowadzących działalność w zakresie walut wirtualnych. Na gruncie polskim znalazło to wyraz w art. 129m u.p.p.p. Podmioty zobligowane do wpisu posiadają status instytucji obowiązanej, który zostanie omówiony w dalszej części artykułu. W tym miejscu można zadać pytanie o faktyczne korzyści płynące z funkcjonowania rejestru[31], w którym zgodnie ze stanem na 6 kwietnia 2023 r. było wpisanych 705 podmiotów deklarujących rodzaj świadczonych przez nie usług, tj. wymiany pomiędzy walutami wirtualnymi i środkami pieniężnymi, pomiędzy samymi walutami wirtualnymi, pośrednictwa w takiej wymianie oraz prowadzenia rachunków dla walut wirtualnych. Zdaniem autorów taki wpis, o charakterze deklaratoryjnym, obecnie bardziej służy firmom do uwierzytelnienia swej działalności, jako afirmowanej przez państwo, niż do faktycznej kontroli tych firm przez organy uprawnione na podstawie u.p.p.p.

---

[30] *Anti-money laundering: Provisional agreement reached on transparency of crypto asset tra*nsfers, Council of the EU, 29 VI 2022 r., https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [dostęp: 7 IV 2023].

[31] Zgodnie z ustawą rejestr jest prowadzony przez ministra finansów, a faktycznie zarządza nim Izba Administracji Skarbowej w Katowicach (rejestr znajduje się pod adresem: https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach).

Poszczególne kraje w różny sposób realizują obowiązki polityki AML/CFT, a priorytetem FATF jest to, aby zręby światowego systemu przeciwdziałania praniu pieniędzy były jednolite. W dokumentach FATF zaleca się stosowanie podejścia funkcjonalnego. Zgodnie z nim poszczególne kraje modelują szczegółowe rozwiązania prawne pod kątem ich wewnętrznych, specyficznych uwarunkowań, ale wszędzie implementacja zasadniczych wytycznych powinna być na niezmiennie wysokim poziomie. W UE to zadanie realizuje Komitet Ekspertów ds. Oceny Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (Moneyval), który jest stałym organem monitorującym Rady Europy. Komitetowi powierzono ocenę zgodności norm krajowych z międzynarodowymi standardami AML/CFT, skuteczne wdrażanie tych unormowań, a także formułowanie zaleceń dla władz państwowych w sprawie poprawy przepisów obowiązujących na tym polu. Zalecenia FATF i Moneyval wymagają zatem tworzenia przez kraje sprawnych procedur AML, w tym nałożenia na uczestników rynku kryptoaktywów określonych zobowiązań, chociaż każdy rząd może indywidualnie konkretyzować przyjęte rozwiązania[32]. Determinantami w implementacji dyrektyw unijnych są takie czynniki, jak ustrój polityczny kraju, jego rozwój gospodarczy, otwartość danego społeczeństwa na innowacje i jego zamożność.

Finansowanie terroryzmu za pomocą kryptowalut

Kryptowaluty są powiązane z działalnością organizacji ekstremistycznych – co najmniej od 2015 r. odnotowywano terrorystów starających się wykorzystać bitcoiny do tworzenia zbiórek crowdfundingowych finansujących ich operacje[33]. W większości były one organizowane przez grupy operujące

[32] P. Opitek, *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722 [dostęp: 7 IV 2023].

[33] *Statement of Stephanie Dobitsch, Deputy Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security*, w: *Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives*, 2021 r., https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf, s. 8 [dostęp: 10 V 2023]. Polskie służby ochrony prawa omawiały temat terroryzmu już w 2018 r., m.in. po prelekcji Pawła Opitka pt. *Wykorzystanie kryptowalut w przestępczości zorganizowanej i terroryzmie* przedstawionej podczas szkolenia prokuratorów Departamentu do Spraw Przestępczości

na terenie Bliskiego Wschodu, które cechują silne motywacje ideologiczne, ale do nielegalnych działań dotyczących kryptowalut i terroryzmu doszło także w Stanach Zjednoczonych, Europie Zachodniej, a ostatnio także w Ukrainie i Polsce. W raportach służb amerykańskich potwierdzono, że nowe technologie, takie jak kryptowaluty, umożliwiają terrorystom dalszą ekspansję i wspierają ich wysiłki w gromadzeniu środków finansowych na nielegalną działalność[34].

Do organizowania działań o charakterze terrorystycznym jest potrzebne wsparcie finansowe, a jego beneficjenci mogą otrzymywać pomoc w postaci kryptoaktywów. Finansowanie terroryzmu za pomocą walut wirtualnych wiąże się m.in. z fundamentalizmem islamskim i omijaniem sankcji ekonomicznych przez państwa nierespektujące w pełni reguł rynku finansowego narzucanych przez zachodnie, liberalne demokracje. W kręgach fundamentalistów islamskich toczyła się dyskusja, czy kryptowaluty są dozwolone przez szariat i czy muzułmanie powinni je wykorzystywać. Ostatecznie Al-Ka'ida opublikowała w Internecie latem 2014 r. manifest pt. *Bitcoin wa Sadaqat al-Jihad*[35]. Promowała w nim użycie bitcoina jako dogodnego środka wspierającego walkę z niewiernymi z pominięciem zachodniego systemu bankowego, który ograniczał darowizny na rzecz dżihadu. W manifeście zalecano realizowanie transferów kryptowalutowych z pobudek ideowych i religijnych, jak również opisano techniczne walory walut wirtualnych: odporność na fałszerstwa, anonimowość nadawców i odbiorców, globalny zasięg, trudności w wykryciu płatności przez organy ścigania. Podkreślono wyższość systemu Bitcoina nad takimi metodami, jak PayPal czy eBay, które są zarządzane odgórnie i mają charakter scentralizowany. Twórcom manifestu chodziło o stworzenie całkowicie anonimowego systemu do wysyłania darowizn w bitcoinach ze Stanów Zjednoczonych, Wielkiej Brytanii, Republiki Południowej Afryki, Ghany, Malezji, Sri Lanki lub innego miejsca na świecie na adres portfela DarkWallet zarządzanego przez mudżahedinów. Zapowiedziano opublikowanie takiego narzędzia (pojawiło się ono w 2019 r.). W konkluzji autorzy manifestu stwierdzili,

Zorganizowanej i Korupcji Prokuratury Krajowej oraz funkcjonariuszy Centralnego Biura Śledczego Policji i Agencji Bezpieczeństwa Wewnętrznego i przedstawicieli innych organów w zakresie zwalczania zagrożeń o charakterze terrorystycznym. Szkolenie odbyło się w Waplewie w dniach 5–7 listopada 2018 r.

[34] *Statement of Chairwoman Elissa Slotkin*, w: *Terrorism and Digital Financing*…, s. 3.

[35] *Bitcoin wa Sadaqat al-Jihad,* https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf [dostęp: 20 I 2019].

że chociaż wykorzystanie bitcoinów napotyka różne przeszkody, a większość kafirów wykorzystuje je do nabycia narkotyków, to jednak kryptoaktywo może zostać wykorzystane do realizacji wielu przydatnych celów: od zakupu broni po darowiznę dla mudżahedinów. Takie stanowisko było jedną z przyczyn powstania wielu stron w mediach społecznościowych organizujących zbiórki w kryptowalucie na rzecz terrorystów islamskich z różnych krajów i organizacji. Zbiórki są prowadzone nie tylko przez podmioty bezpośrednio powiązane z przestępcami, lecz także przez ich sympatyków mieszkających w Stanach Zjednoczonych czy Europie.

Al-Ka'ida od początku istnienia korzystała z forów i czatów w otwartym Internecie, jednak po zakrojonej na szeroką skalę akcji służb w 2000 r. i aresztowaniach kilku zwolenników dżihadu wiele platform przeniosło się do Darknetu. Obecnie zaawansowane fora dżihadystów chronią się przed inwigilacją służb szyfrowaniem kryptograficznym, stosują narzędzia typu Sigaint lub TorBox, a dostęp do platformy jest weryfikowany przez administratora. W Internecie powstają fora powiązane z radykalnymi ruchami, np. Shumukh al-Islam oscylujące pomiędzy zwolennikami ISIS i Al-Ka'idy[36]. W 2019 r. militarne skrzydło Hamasu – Brygady Izz ad-Din al-Kassam – zamieściło w mediach społecznościowych i na swoich stronach internetowych (alqassam.net, alqassam.ps, qassam.ps) wezwanie do składki w bitcoinach na „kampanię terroru". Jednocześnie przestępcy uczyli się zasad cyberbezpieczeństwa. Brygady te początkowo zażądały wysyłania kryptowaluty na jeden adres hostowany na amerykańskiej giełdzie, potem jednak opracowały technologię generowania dla każdej wpłaty indywidualnego adresu, aby utrudnić śledzenie pochodzenia i transferów środków. Wprowadzanie przez grupy terrorystyczne nowych rozwiązań wskazuje, że mogą one dostosowywać się do strategii minimalizujących ryzyko i wykorzystywać różne luki w zabezpieczeniach technologicznych[37]. Działalność cyberterrorystów nie ogranicza się tylko do crowdfundingu. Na początku 2021 r. media Al-Ka'idy zaoferowały nagrodę w wysokości 1 bitcoina, wartego wówczas 60 000 dolarów, osobie, która zamorduje policjanta w kraju zachodnim. Dwa lata wcześniej Brenton Tarrant, sprawca ataków na meczety w Christchurch w Nowej

[36] B. Berton, *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 23 VIII 2019].

[37] *Risk Assessment. 2022 National Terrorist Financing*, Department of the Treasury, luty 2022 r., https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf, s. 22 [dostęp: 10 V 2023].

Zelandii, twierdził, że zarabiał na handlu kryptowalutami. W tym samym czasie działający z pobudek rasowych ekstremista, który usiłował dokonać zamachu w synagodze na terenie Niemiec, zeznał, że otrzymywał wsparcie finansowe w bitcoinach[38]. Wiele wskazuje na to, że sprawcy zamachów terrorystycznych przeprowadzonych 13 listopada 2015 r. w Paryżu byli wspierani podczas ich organizowania przekazami kryptowalutowymi[39].

Aktywność internetowych terrorystów została zauważona i rozpracowana przez amerykańskie służby ochrony prawa, które wypracowały najbardziej efektywne i zaawansowane narzędzia oraz metody zwalczania ekstremizmu w Internecie. W Stanach Zjednoczonych jednym z głównych organów publicznych zajmujących się walką z terroryzmem jest Departament Bezpieczeństwa Wewnętrznego (ang. Department of Homeland Security, DHS). Jego przedstawiciel podczas wysłuchania w Kongresie w 2021 r. stwierdził, że DHS wraz z Urzędem Skarbowym (ang. Internal Revenue Service, IRS) i Federalnym Biurem Śledczym (ang. Federal Bureau of Investigation, FBI) przeprowadził globalną operację cybernetyczną i zlikwidował infrastrukturę wirtualną Brygad Izz ad-Din al-Kassam. Począwszy od października 2019 r. działający pod przykryciem agenci Homeland Security Investigations (HSI), służby zajmującej się walką z terroryzmem, dokonywali na rzecz terrorystów darowizn w bitcoinach, aby rozpracować powiązania podmiotów prowadzących internetowe zbiórki na rzecz Hamasu. Te działania umożliwiły śledczym ustalenie zwolenników tej organizacji mieszkających w Stanach Zjednoczonych oraz przeprowadzenie dalszego śledzenia transferowanych środków. Zidentyfikowano 64 unikalne kanały komunikacji (m.in. adresy e-mail), co pozwoliło zabezpieczyć portfele bitcoinowe darczyńców. Operacja ujawniła modus operandi terrorystów w Internecie, w tym sposoby prowadzenia rekrutacji zwolenników w systemie online, metody finansowania, a także użytkowane przez nich domeny oraz infrastrukturę IT, funkcjonującą m.in. w Stanach Zjednoczonych, Kanadzie, Rosji, Niemczech i Arabii Saudyjskiej. W lipcu 2020 r. agenci specjalni HSI i IRS zrealizowali 24 federalne nakazy przeszukania, konfiskaty kryptowaluty i zabezpieczenia danych na licznych giełdach internetowych i u dostawców usług sieciowych – poczty elektronicznej, VPN-ów, płatności online. Zarekwirowano serwery, zamknięto wiele

[38] *Statement of Stephanie Dobitsch…*, s. 8.

[39] Zob. m.in. Y.B. Perez, *Bitcoin, Paris and Terrorism: What the Media Got Wrong*, CoinDesk, 6 III 2023 r., https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [dostęp: 10 V 2023].

domen i skrzynek e-mail powiązanych z działalnością terrorystyczną. Do operacji w cyberprzestrzeni dołączyły zaprzyjaźnione służby na całym świecie, co pozwoliło przejąć terabajty danych kontrolowanych przez terrorystów, setki portfeli bitcoinowych, kryptoaktywa warte kilka milionów dolarów oraz zlikwidować strony przeznaczone do przekazywania datków w bitcoinach. Inne śledztwo z 2020 r., prowadzone przez HSI, IRS i FBI, miało związek z 24 kontami kryptowalutowymi zidentyfikowanymi jako zagraniczne aktywa lub źródła wpływów dla Al-Ka'idy. Cyberoperacja dotyczyła wykorzystania kryptowaluty do wspierania i finansowania terroryzmu, a w jej wyniku zostało przejętych 60 portfeli wirtualnych[40].

Działania ukierunkowane na zwalczanie finansowania terroryzmu z wykorzystaniem walut wirtualnych rząd Stanów Zjednoczonych traktuje jako ważny front walki z międzynarodowym terroryzmem. Potwierdza to dokument pt. *Krajowa strategia walki z terroryzmem i innym nielegalnym finansowaniem* z 2020 r.[41] przygotowany przez Departament Skarbu USA (ang. United States Department of the Treasury). Podniesiono w nim, że po atakach z 11 września 2001 r. tamtejsze władze skupiły się na słabych punktach systemu finansowego. Chodzi o nadużycia dokonywane przez organizacje charytatywne i nielicencjonowane przekazy pieniężne, które pozwoliły Al-Ka'idzie na międzynarodowe transfery pieniędzy w celu finansowania ataków terrorystycznych. Po zamachu na World Trade Center niektóre grupy ekstremistyczne porzuciły działania na skalę globalną

[40] *Statement of John Eisert, Assistant Director, Investigative Programs, Homeland Security Investigations, Immigration and Customs Enforcement, Department of Homeland Security*, w: *Terrorism and Digital Financing*..., s. 14–16. W 2021 r. Departament Sprawiedliwości USA ogłosił likwidację infrastruktury trzech kampanii przeprowadzonych w cyberprzestrzeni i służących finansowaniu terroryzmu, z udziałem Brygad Izz ad-Din al-Kassam będących wojskowym skrzydłem Hamasu, Al-Ka'idy oraz Islamskiego Państwa Iraku i Lewantu (ISIS). W tych kampaniach zostały wykorzystane wyrafinowane narzędzia cybernetyczne, m.in. pozyskano z całego świata darowizny w postaci kryptowalut. Akcja pokazała – jak głosił komunikat rządu USA – jak różne grupy terrorystyczne w podobny sposób dostosowały do ery cybernetycznej swoją działalność związaną z finansowaniem terroryzmu. Amerykańskie władze przejęły miliony dolarów powiązane z nielegalnym procederem, ponad 300 kont kryptowalutowych, cztery strony internetowe i cztery strony na Facebooku. Zob. *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, The United States Department of Justice, 13 VIII 2020 r., https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [dostęp: 9 V 2023].

[41] *National Strategy for Combating Terrorist and Other Illicit Financing 2020*, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [dostęp: 7 VII 2023].

(złożone i rozległe ataki), a skoncentrowały się na działalności pojedynczych terrorystów. Zradykalizowane osoby mogą przeprowadzać stosunkowo tanie i nieskomplikowane, ale skutkujące ofiarami ataki przy użyciu noży, broni palnej i samochodów. Tego rodzaju działaniom sprzyja komunikacja online i transfery kryptowalutowe dokonywane w ukryciu bezpośrednio do portfeli indywidualnych osób, co ogranicza ślad finansowy[42].

Jednak zagadnienie „kryptowaluty a ekstremizm" dotyczy nie tylko terrorystów, lecz także innych organizacji wywrotowych, zagrażających stabilności i bezpieczeństwu państw demokratycznych. Wirtualne zbiórki crowdfundingowe są wykorzystywane również przez organizacje neonazistowskie. Skrajnie prawicowi ekstremiści działający w Internecie używają kryptowalut m.in. dlatego, że są one kojarzone z ideologią głęboko zakorzenionej nieufności wobec instytucji finansowych, jako tych opanowanych i zarządzanych przez „żydowską finansjerę". Przemawiają do nich również libertariańskie początki filozofii związanej z powstaniem bitcoina wiążące się z niechęcią do światowego establishmentu. Nie mniej ważne są czysto praktyczne aspekty funkcjonowania kryptowalut. Amerykańscy neonaziści są rugowani z popularnych platform crowdfundingu typu Patreon, dlatego też tworzą alternatywne serwisy przeznaczone do dokonywania dotacji w formie zdecentralizowanych tokenów. W taki sposób powstał Hatreon. Firmy hostujące odmawiały jego utrzymania, więc zmieniał on domeny na coraz lepiej maskujące administratora platformy[43].

Zbiórkę kryptowalut prowadzi na przykład strona internetowa o nazwie *The Daily Stormer* redagowana przez amerykańskich neonazistów. Znajduje się na niej dokładna instrukcja, jak realizować przelewy bitmonet na podany tam adres, a zalecaną formą wpłat są kryptobankomaty. Andrew Anglin, główny redaktor tej strony, wydający także pismo o takim samym tytule, jest znanym aktywistą realizującym skuteczne akcje crowdfundingowe na cele swojej organizacji. Anglin wielokrotnie zachwalał, m.in. na łamach „The Washington Post", wirtualne waluty jako doskonałe narzędzie do gromadzenia środków na działalność zwalczaną przez władze państwowe oraz potwierdził, że otrzymał znaczne datki od osób wspierających jego projekty i ideologię.

---

[42] Tamże, s. 11–12.

[43] P. Opitek, *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu*, Warszawa 2019, s. 43–44 (praca dyplomowa napisana na studiach podyplomowych w Szkole Głównej Handlowej, niepublikowana, w zasobach autora).

Działania rekrutacyjne prowadzone przez dżihadystów w Internecie są często ściśle powiązane z apelami o pomoc finansową dla terrorystów opartą na crowdfundingu. Łatwość przekazywania funduszy i możliwość dotacji w postaci stosunkowo niewielkich kwot może pomóc materialnie organizacji ekstremistycznej, a aktywność darczyńcy pozostanie niezauważona przez system AML. Przykładem zrealizowanego crowdfundingu kryptowalutowego przeprowadzonego na rzecz bojowników tzw. Państwa Islamskiego była sprawa Alego Shukri Amina. Mężczyzna urodził się w Afryce i w wieku kilku lat wyemigrował z matką do Stanów Zjednoczonych. Zamieszkał w Wirginii i tam uczęszczał na studia. Interesowały go przedmioty ścisłe, tematy dotyczące cyberbezpieczeństwa, szyfrowania i kryptowalut. Jednocześnie Amin radykalizował się i propagował swoje idee w mediach społecznościowych. Założył m.in. konto na Twitterze o nazwie @AmreekiWitness, na którym zamieścił 7000 tweetów pochwalających radykalny islam i propagujących wsparcie finansowe dla ISIS za pomocą anonimowych transferów bitcoinowych. Stworzył ponadto blog Al-Khilafah Aridat, na którym zachęcał do walki z niewiernymi, jak również opracował serię artykułów adresowanych do zwolenników tzw. Państwa Islamskiego. Opisał w nich ze szczegółami, w jaki sposób komunikować się anonimowo w sieci i korzystać z szyfrowania podczas nielegalnej aktywności na rzecz terrorystów. Amin pomógł także znajomemu mężczyźnie dotrzeć przez Turcję do Syrii i przyłączyć się do bojowników islamskich. W 2015 r. prokurator skierował do sądu akt oskarżenia przeciwko niemu[44], w którym zarzucił mu angażowanie się wraz z innymi ustalonymi i nieustalonymi osobami w działalność terrorystyczną polegającą na udzieleniu wsparcia materialnego i fachowych porad zagranicznym terrorystom z ISIS. Mężczyzna został skazany przez sąd na karę 11 lat pozbawienia wolności.

Obowiązki instytucji obowiązanej w systemie przeciwdziałania praniu pieniędzy

Filarem walki z przestępstwem prania pieniędzy jest polityka AML, którą muszą prowadzić instytucje obowiązane. Są to podmioty uczestniczące

[44] *United States of America v. Ali Shukri Amin*, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [dostęp: 10 V 2023].

w szeroko rozumianym obrocie walutami wirtualnymi i z tego tytułu rządy poszczególnych państw nałożyły na nie określone obowiązki mające przeciwdziałać procederowi prania pieniędzy. Wiele działań AML dotyczących kryptoaktywów jest podobnych do tych, które od dawna są związane z płatnościami pieniądzem lub pieniądzem elektronicznym. Biorąc jednak pod uwagę specyfikę zarządzania ryzykiem transakcji angażujących tokeny cyfrowe, postuluje się konieczność przestrzegania w stosunku do rynku krypto wysokich wymagań dotyczących prowadzonej tam działalności, np. uzyskania zezwolenia na funkcjonowanie firmy, spełnienia wymogów ostrożnościowych w zakresie posiadania kapitału zakładowego gwarantującego płynność, prowadzenia transparentnej rachunkowości i dokonywania okresowych audytów, posiadania aktywów rezerwowych stanowiących równowartość wyemitowanych tokenów. Ten fundusz gwarancyjny, chroniący inwestorów, stanowi zabezpieczenie finansowe, gdyby doszło np. do zhakowania protokołu blockchaina i „kradzieży" bazującej na nim wartości. W związku z takimi cyberzagrożeniami instytucje obowiązane muszą przestrzegać wysokich wymagań chroniących posiadane aktywa, w tym klucze kryptograficzne, oraz stosować, wpisane w ład korporacyjny, profesjonalne systemy kontroli, zarządzania ryzykiem i raportowania. Dochodzą do tego wymagania w zakresie wewnętrznych procesów prowadzenia dokumentacji firmy, przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, bezpiecznego outsourcingu, odporności operacyjnej kluczowych usług (zapewnienie ciągłości funkcjonowania firmy i wysokiej jakości usług w przypadku awarii systemów elektronicznych lub takich zdarzeń fizycznych, jak pożar czy przerwanie dostaw energii elektrycznej). Trzeba również zmierzyć się z takimi wyzwaniami, jak przyjęcie stosownych regulacji dotyczących niewypłacalności i upadłości firmy, która ulokowała swój majątek w kryptoaktywach lub świadczyła usługi i sprzedawała produkty na rynku kryptograficznym[45].

Walka z praniem pieniędzy oraz przeciwdziałanie terroryzmowi, z uwzględnieniem walut wirtualnych, bazuje na wspólnych rozwiązaniach wdrażanych przez UE do porządków prawnych państw Unii. Szczególną rolę odegrała piąta dyrektywa w sprawie przeciwdziałania praniu pieniędzy

[45] *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf, s. 20–21 [dostęp: 9 IV 2023].

(UE) 2018/843[46], która weszła w życie w czerwcu 2018 r. W Polsce przepisy wprowadzające rozwiązania zawarte w tym akcie prawnym obowiązują od maja 2021 r.[47] Dyrektywy AML wydawane wspólnie przez Parlament Europejski i Radę UE kształtują prawa i obowiązki profesjonalnych uczestników rynku, organów administracji publicznej (m.in. jednostek analityki finansowej), a pośrednio oddziałują także na politykę kryminalną państwa. W tym ostatnim przypadku chodzi o możliwości egzekwowania obowiązków wobec instytucji obowiązanych, karania osób odpowiedzialnych za ich niewykonanie, wykorzystania źródeł dowodowych czy zabezpieczania majątku pochodzącego z przestępstwa.

Skorzystanie przez organy ścigania z możliwości, jakie stwarzają w Polsce przepisy u.p.p.p., wymaga znajomości mechanizmów, którymi system AML rządzi się w stosunku do instytucji obowiązanych, w tym podmiotów prowadzących działalność gospodarczą polegającą na świadczeniu usług w zakresie walut wirtualnych (art. 2 ust. 1 pkt 12 u.p.p.p.). Takie podmioty mają obowiązek sporządzenia i stosowania (a także aktualizowania i weryfikowania) wewnętrznej procedury w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, o której mowa w art. 50 u.p.p.p. Wskazany przepis enumeratywnie wymienia, co zawiera taka procedura, z uwzględnieniem charakteru, rodzaju i rozmiaru działalności prowadzonej przez przedsiębiorcę, a całe podejście do bezpieczeństwa finansowego opiera się na szacowaniu ryzyka. Tym ryzykiem jest możliwość zaktualizowana się zagrożenia (łącznie z możliwością popełnienia przestępstwa) w stosunku do konkretnego klienta instytucji obowiązanej w ramach świadczonych przez nią usług. Takie ryzyko może być określone jako minimalne i wtedy nie wymaga się stosowania szczególnych środków ostrożności. W momencie jednak, gdy ryzyko zostanie oszacowane jako wysokie, wdraża się wzmożone środki bezpieczeństwa finansowego (wnikliwe badanie źródła pochodzenia środków, ustalanie beneficjenta rzeczywistego), łącznie z możliwością zerwania przez instytucję obowiązaną relacji gospodarczych z klientem. Już teraz ocena zakresu i częstotliwości

[46] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE,* https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018L0843&from=en.

[47] *Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw.*

stosowania przedmiotowych środków ciąży na firmie kryptowalutowej, a planuje się dalsze zaostrzenie przepisów. W dniu 7 grudnia 2022 r. Rada UE uzgodniła stanowisko, zgodnie z którym w całej Unii będzie obowiązywać maksymalny limit płatności gotówkowych w wysokości 10 000 euro, a dodatkowo anonimowość transferów zostanie ograniczona w przypadku handlu kryptoaktywami, ponieważ wszyscy dostawcy takich usług będą zobowiązani do przeprowadzania badania *due diligence*, tj. szczegółowej oceny aktualnej sytuacji kontrahenta oraz określenia istniejącego i potencjalnego ryzyka związanego z planowaną operacją finansową w przypadku transakcji o wartości co najmniej 1000 euro[48]. Już teraz instytucja obowiązana powinna bliżej zainteresować się swoim klientem, gdy w jego aktywności na platformie pojawiają się typowe symptomy świadczące o możliwości prania pieniędzy przy użyciu kryptowalut. Chodzi m.in. o posługiwanie się wieloma rachunkami zarejestrowanymi na różne osoby, wielokrotne przewalutowanie środków zgromadzonych na rachunkach lub konwersję pomiędzy pieniądzem a walutami wirtualnymi bez sprecyzowanego celu biznesowego, korzystanie przez klienta z bankomatów, wpłatomatów, kryptobankomatów lub innych urządzeń umożliwiających anonimowe wpłaty lub wypłaty gotówki i walut wirtualnych bez racjonalnego uzasadnienia w profilu transakcyjnym danej osoby czy też o wykorzystywanie do transakcji (wejścia lub wyjścia środków) takich niestandardowych metod płatności, jak Mistertango, N26, Revolut, Western Union, Wirex, PayPal, MoneyGram[49]. Identyfikacja i ocena ryzyka AML/CFT powinna uwzględniać wiele czynników, m.in. dotyczących statusu klientów (kraj pochodzenia, wielkość firmy i profil jej działalności), państw lub obszarów geograficznych ich pochodzenia, rodzaju produktów i usług oferowanych przez kontrahentów oraz kanałów dystrybucji dóbr, rodzaju wykonywanych transakcji. Katalog badanych okoliczności nie jest zamknięty i podlega dostosowaniu do zmieniających się wewnętrznych i zewnętrznych uwarunkowań w otoczeniu podmiotu zaangażowanego w działalność kryptowalutową.

Pierwszy wniosek, jaki ABW lub inna służba specjalna prowadząca czynności powinna skierować do instytucji obowiązanej, której działalność pozostaje w zainteresowaniu tej służby, to zwrócenie się o przedłożenie

---

[48] *Fight against money laundering and terrorist financing*, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [dostęp: 9 IV 2023].

[49] E. Przewłoka, *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej*, Bydgoszcz 2023 (metodyka wewnętrzna Policji, w zbiorach autora).

wewnętrznej procedury w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu w celu sprawdzenia, jak ukształtowano tę procedurę, czy dokument spełnia wymogi prawa i odpowiada rzeczywistej działalności instytucji, a następnie zweryfikowania, jak wyglądała realizacja procedury w praktyce. Jeśli dokument jest rzetelny, to na jego podstawie wiadomo, kto za co odpowiadał w polityce AML danego podmiotu, jak szacowano ryzyko, gdzie znajdują się i co zawierają metadane gromadzone w trakcie kontaktów na odległość z kontrahentami. Można ponadto zwrócić się z zapytaniami dotyczącymi konkretnego klienta:

1. Czy w relacjach handlowych ukrywał on prawdziwe dane osobowe?
2. Czy posługiwał się rachunkiem (np. płatniczym, bankowym, walut wirtualnych) założonym na inną osobę lub podawał się za kogoś innego w kontaktach z pracownikami instytucji?
3. Czy przedkładał dokumenty wzbudzające zastrzeżenia co do ich autentyczności lub rzetelności?
4. Czy logował się na konta osób trzecich?
5. Czy odmawiał przedłożenia określonych dokumentów lub podania źródła pochodzenia środków, którymi dysponował?
6. Czy w jeszcze inny sposób utrudniał działanie instytucji obowiązanej w zakresie realizacji obowiązków AML?
7. Czy korzystał z wpłat lub wypłat bankomatowych z zaangażowaniem środków na giełdzie?[50]

Badaniu podlegają także inne dokumenty, które zgodnie z art. 50 ust. 2 u.p.p.p. stanowią obligatoryjne składniki wewnętrznej procedury AML instytucji obowiązanej, tj. zasady dotyczące stosowania środków bezpieczeństwa finansowego, przechowywania dokumentów oraz informacji, wykonywania obowiązków obejmujących przekazywanie Generalnemu Inspektorowi Informacji Finansowej (GIIF) informacji o transakcjach oraz zawiadomieniach, upowszechniania wśród pracowników instytucji obowiązanej wiedzy z zakresu przepisów o przeciwdziałaniu praniu pieniędzy oraz zgłaszania przez pracowników rzeczywistych lub potencjalnych naruszeń tych przepisów, audytu wewnętrznego.

Obowiązki wpisane w politykę AML instytucji obowiązanej dotyczą także analizy samych transakcji dokonywanych przy użyciu walut wirtualnych. Prokurator może zażądać od giełdy przedstawienia w formie analitycznej informacji dotyczących historii zleceń klienta (wejścia i wyjścia środków),

[50] Tamże.

usług i produktów finansowych lub kryptowalutowych (zwłaszcza nietypowych), z jakich korzystał klient, przedłożenia indywidualnej (obowiązującej aktualnie oraz w przeszłości, jeśli ulegała zmianie) oceny ryzyka przypisanego danej osobie lub instytucji, sprawdzenia, czy przelewała ona lub próbowała przelać środki do rajów podatkowych lub krajów objętych sankcjami. W stanie prawnym na dzień 21 marca 2023 r. kryptoaktywa są objęte sankcjami nałożonymi na Rosję, a więc przepisami dotyczącymi zamrożenia majątku określonych osób, zakazu ich udostępniania przez te osoby oraz jakiegokolwiek wykorzystania w celach gospodarczych. Kryptoaktywa nie powinny być także używane do obchodzenia jakichkolwiek sankcji ustanowionych na podstawie rozporządzenia Rady UE nr 833/2014[51]. Podmiotom z Unii zakazuje się ponadto świadczenia usług związanych z prowadzeniem lub dostarczaniem portfeli kryptowalutowych, rachunków lub usług powierniczych związanych z wartościami krypto zarówno obywatelom Rosji, jak i osobom fizycznym zamieszkałym na obszarze Federacji Rosyjskiej, a ponadto osobom prawnym oraz innym podmiotom mającym tam siedzibę. To oznacza, że europejscy dostarczyciele usług powinni zamknąć konta kryptograficzne swoich rosyjskich klientów i zwrócić im cyfrowe aktywa (ewentualnie zamienić je na pieniądze lub inną kategorię aktywów, które nie podlegają sankcjom), a w przypadku osób objętych sankcjami – zamrozić ich majątek. Przepisy sankcyjne należy odczytywać w powiązaniu z limitem depozytów określonym w art. 5b wspomnianego rozporządzenia i w tym zakresie zamiana kryptoaktywów na depozyty fiducjarne byłaby możliwa jedynie do wysokości kwoty dozwolonej dla depozytów[52].

Otwarta pozostaje odpowiedź na pytanie, jak skuteczne w praktyce są sankcje nałożone na Rosję. Według raportu renomowanej firmy analitycznej Inca Digital, wykonanego na podstawie analizy danych zebranych ze 163 platform handlu kryptowalutami na całym świecie, w tym scentralizowanych i zdecentralizowanych giełd i stron P2P oraz dostawców usług pozagiełdowych (ang. *Over the Counter Broker*, OTC[53]), aż 79 z nich umożliwia

---

[51] *Rozporządzenie Rady (UE) NR 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie.*

[52] *Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014*, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 10 IV 2023].

[53] Nazwa oznacza usługi świadczone przez brokerów OTC, którymi są przede wszystkim duże giełdy kryptowalutowe typu Kraken, Binance, Coinbase, Satstreet, ułatwiające bezpośredni handel kryptowalutą pomiędzy dwoma stronami transakcji typu: krypto–krypto

obywatelom Rosji zakup kryptowaluty (zwłaszcza stablecoina Tether w systemie P2P), a 11 z 62 międzynarodowych platform nie ma przed rozpoczęciem handlu żadnych wymagań w stosunku do Rosjan w zakresie spełnienia procedury KYC[54]. Najbardziej przyjazne dla nich oraz najczęściej wykorzystywane są giełdy Huobi i KuCoin z siedzibą na Seszelach. Nie podjęły one żadnych kroków, aby uniemożliwić rosyjskim bankom objętym sankcjami korzystanie ze swoich platform i nieprzerwanie pozwalają na realizację transakcji kartami debetowymi wydanymi przez te banki, w tym Sbierbank. Według Inca Digital także Binance oferuje Rosjanom różne metody konwersji posiadanej przez nich waluty na krypto, m.in. za pomocą systemu OTC i rynku P2P, z pominięciem procedury KYC do równowartości depozytu w wysokości 10 tys. dolarów, ale ten limit jest łatwy do obejścia. Transakcje mogą być ukrywane m.in. poprzez kwalifikowanie płatności na rzecz nierosyjskich przedsiębiorstw użyteczności publicznej. ByBit operujący z Singapuru umożliwia użytkownikom wymianę rosyjskich rubli na kryptowaluty za pomocą rynku P2P i depozytu fiducjarnego. Opisana sytuacja jest bezpośrednim naruszeniem amerykańskich i europejskich sankcji i potwierdza, że analizowany rynek stanowi lukę w systemie ograniczającym możliwości gospodarcze Rosji. Chociaż z powodu nałożonych sankcji wiele giełd oficjalnie ograniczyło swoją działalność w tym kraju oraz deklaruje blokowanie użytkownikom z Rosji dostępu do oferowanych usług, to w rzeczywistości kontynuują one w mniej lub bardziej zawoalowanej formie współpracę z rosyjskimi obywatelami, m.in. umożliwiając im korzystanie z maksymalnych limitów wpłat, handlu i wypłat[55].

(np. wymiana bitcoina na ethereum) lub krypto–pieniądz fiducjarny. Handlowcy dysponujący dużymi wartościami majątkowymi poszukują bowiem bezpiecznych i anonimowych kanałów nieograniczonej limitami wymiany wartości majątkowych, na z góry ustalonych warunkach, które nie są formalnie notowane na scentralizowanych giełdach. Negocjowanie transakcji za pośrednictwem brokerów OTC pomiędzy sprzedającymi i kupującymi może odbywać się przez telefon lub sieć internetową, a nawet przewidywać osobiste spotkanie stron.

[54] *How Russians Use Tether to Evade Global Sanctions*, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [dostęp: 10 IV 2023].

[55] S. Sutton, L. Seligman, *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023 r., https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [dostęp: 10 IV 2023]; *Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned*, Ledger Insights, 28 II 2023 r., https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [dostęp: 10 IV 2023].

Immanentną cechą związaną z obrotem walutami wirtualnymi jest utrudniony dostęp do informacji o podmiotach zaangażowanych w operacje, gdyż zazwyczaj działają one za pośrednictwem Internetu. Dlatego w przepisach prawnych położono nacisk na to, aby kontrolować ślad cyfrowy takiej działalności. Z treści art. 76 u.p.p.p. wynika, że na instytucji obowiązanej ciąży ustawowy nakaz posiadania informacji lub dokumentów dotyczących m.in. adresów IP, z których następowało połączenie klienta z systemem teleinformatycznym instytucji obowiązanej, oraz znaczników czasu połączeń z systemem. Zgromadzenie przez prokuratora historii logów może pozwolić na ustalenie wielu istotnych danych o osobie pozostającej w jego zainteresowaniu, np. geolokalizację urządzeń elektronicznych, z których korzystała, oraz częstotliwość i czas lub okres jej kontaktów z instytucją obowiązaną. Dodatkowa analiza adresów IP w świetle zgromadzonego materiału dowodowego może udowodnić, że:

- transakcje realizowano z IP uprzednio wykorzystanych do nielegalnych działań (np. oszustw, ataków phishingowych, dystrybucji złośliwego oprogramowania typu ransomware);
- transakcji dokonywano z krajów objętych sankcjami, rajów podatkowych lub z innego „egzotycznego" terytorium lub państw wspierających międzynarodowy terroryzm;
- osoba pozostająca w zainteresowaniu organów ścigania używała narzędzi anonimizujących ruch sieciowy (Tor, VPN-y, proxy);
- zachodzą rozbieżności między adresami IP powiązanymi z profilem klienta a tymi, z których inicjowano transakcje (można z tego wnioskować, że osoba objęta śledztwem była tzw. słupem, a jej dane osobowe wykorzystał rzeczywisty beneficjent transakcji)[56].

Transakcje krypto należy zakwalifikować do kategorii podwyższonego ryzyka i szczegółowo analizować. W celu zwiększenia ich przejrzystości 29 czerwca 2022 r. Rada i Parlament UE osiągnęły wstępne porozumienie dotyczące aktualizacji unijnego rozporządzenia w sprawie informacji towarzyszących przekazom pieniężnym. Nowe przepisy wprowadzą obowiązek zbierania i udostępniania określonych informacji o nadawcach i beneficjentach transferów przez dostawców usług w zakresie aktywów kryptograficznych. Ma to zapewnić transparentność transferów kryptowalut, aby

[56] J. Skała, *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, z. 3, s. 92–93. https://doi.org/10.53024/4.3.47.2022.

móc lepiej identyfikować podejrzane operacje i blokować zaangażowane w nie środki[57]. To podwyższone ryzyko związane z anonimowością transakji krypto obejmuje oprócz typowych VASP także innych uczestników rynku finansowego (w tym banki), którzy co prawda nie biorą udziału w obrocie walutami wirtualnymi, ale pośrednio są narażeni na proceder prania pieniędzy z wykorzystaniem kryptoaktywów, gdyż np. prowadzą rachunki bankowe, na których są gromadzone środki pieniężne pochodzące z wymiany cyfrowych tokenów na pieniądz fiducjarny.

Ważną kategorię obowiązków nałożonych na instytucje stanowi powiadamianie właściwych organów państwowych o zdarzeniach mogących stanowić przestępstwo lub próbę jego dokonania oraz powiadamianie o charakterze sprawozdawczym. W ostatnim przypadku chodzi o przekazywanie GIIF informacji o przyjętych wpłatach i wypłatach środków pieniężnych, transakcjach dewizowych i transferach przekraczających próg o określonej wartości pieniężnej, a więc o transakcjach ponadprogowych (art. 72 u.p.p.p.). Instytucje obowiązane zawiadamiają także GIIF o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu (art. 74 u.p.p.p.) oraz przypadkach powzięcia uzasadnionego podejrzenia, że zlecenie przelewu lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu (art. 86 u.p.p.p.). W takiej sytuacji administrator platformy dokonuje blokady środków objętych zawiadomieniem, a dalsze decyzje o losie aktywów podejmuje prokurator zawiadomiony przez GIIF. Ponadto art. 89 u.p.p.p. reguluje obowiązek zawiadomienia właściwego prokuratora o powzięciu uzasadnionego podejrzenia, że wartości majątkowe będące przedmiotem transakcji lub zgromadzone na rachunku pochodzą z przestępstwa innego niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwa skarbowego albo mają związek z przestępstwem innym niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwem skarbowym. Wskazane procedury „blokad" są szczegółowo opisane w wymienionych artykułach, ale warto zwrócić uwagę na brzmienie niektórych instytucji prawnych opisanych w ustawie.

[57] *Fight against money laundering and terrorist financing…*

Określenie statusu cyfrowego artefaktu w postępowaniu karnym

W sytuacji gdy jakieś kryptoaktywo znajdzie się w obszarze zainteresowania organu ścigania, należy ustalić jego status techniczny i prawny. Od tego zależą bowiem ważne kwestie, m.in. możliwość wypełnienia znamion przestępstwa poprzez samo posiadanie lub emisję tokenów (np. zabroniona tokenizacja papierów wartościowych), sposób przejęcia faktycznego władztwa nad mieniem cyfrowym (czy kryptoaktywa są umieszczone na blockchainie publicznym lub prywatnym, a może w ogóle nie mają nic wspólnego z technikami łańcucha bloków), możliwość poszukiwania śladów popełnionego przestępstwa (umiejscowienie serwera). Określenie wspomnianego statusu nie zawsze jest łatwe i chociaż największa liczba spraw dotyczy bitcoinów lub podobnych altcoinów (ethereum czy litecoina), to zdarzają się sytuacje, w których ustalenie wszystkich cech tokena stanowi spore wyzwanie. Działo się tak w przypadku salonów prowadzących nielegalne gry hazardowe, w których gracze nabywali za pieniądze punkty do gry w formie cyfrowego odwzorowania ich wartości w kodzie QR. Badania pokazują, że polscy użytkownicy kryptoaktywów mają w swoich portfelach zaawansowane tokeny, których emisja na krajowym rynku kapitałowym jest obwarowana licznymi wymogami prawnymi, poddana nadzorowi organów regulacyjnych, a często nawet zabroniona. Chodzi m.in. o takie cyfrowe aktywa charakterystyczne dla rynku DeFi, jak PAXGOLD, USDT, COMP[58]. Większość użytkowników zadeklarowała ponadto, że korzystała z tokenów udziałowych podobnych do akcji lub obligacji, pochodnych instrumentów finansowych w formie kryptoaktywów lub inwestowała w takie instrumenty, a prawie połowa posiadała tokeny przypominające opcje, kontrakty terminowe lub swapy[59].

Scentralizowany i zdecentralizowany rynek kryptoaktywów rozrasta się, a organy publiczne, nie tylko w Polsce, lecz także na świecie, mają duże problemy z poruszaniem się po nim i egzekwowaniem obowiązków prawnych nałożonych na uczestników tego rynku. Należy przypuszczać, że czyny zabronione w postaci malwersacji finansowych czy prania pieniędzy dokonywane w środowisku takim jak DeFi zbyt często pozostają poza jakąkolwiek kontrolą państw i rządów. Autorzy artykułu nie znają sprawy, w której polskie organy ścigania lub nadzoru nad rynkiem kapitałowym przeprowadziły zaawansowane czynności związane z nadużyciami na rynku zdecentralizowanych finansów. Efektywne działania na tym polu podejmuje natomiast

[58] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, s. 235.

[59] Tamże.

amerykański organ nadzoru nad rynkiem finansowym – Komisja Nadzoru nad Rynkiem Papierów Wartościowych i Giełd (ang. The Securities and Exchange Commission, SEC). W sierpniu 2021 r. oskarżyła ona przed sądem osoby odpowiedzialne o prowadzenie niezarejestrowanej w SEC sprzedaży papierów wartościowych za kwotę ponad 30 mln dolarów przy użyciu inteligentnych kontraktów i technologii zdecentralizowanych finansów, a także o wprowadzanie inwestorów w błąd w zakresie faktycznej rentowności oferowanych produktów. Oskarżeni działali jako firma Blockchain Credit Partners i emitowali oraz oferowali do sprzedaży na platformie DeFi Money Market dwa rodzaje tokenów o nazwie mTokeny i znacznej stopie zwrotu oraz tokeny DMG dające prawo głosu w wirtualnej spółce (DAO)[60]. Agencja regulująca rynek kontraktów futures (ang. The Commodity Futures Trading Commission, CFTC) w marcu 2023 r. oskarżyła w postępowaniu cywilnym przed sądem federalnym holding Binance, największą na świecie platformę do handlu walutami wirtualnymi, oraz jego dyrektora Changpenga Zhao o to, że bez wymaganej przez prawo rejestracji w CFTC oferował do sprzedaży obywatelom Stanów Zjednoczonych instrumenty pochodne w formie tokenów cyfrowych[61].

Innym przykładem na różnorodność „cyfrowych wartości" występujących w świecie wirtualnym są gry komputerowe, szczególnie te prowadzone w trybie online. Artefakty w grach mogą przedstawiać postacie ludzkie, broń (miecze, pistolety), amunicję, części zbroi, przedmioty ukrywające inne rzeczy (skrzynie, sejfy) lub bardziej abstrakcyjne elementy, których funkcja stanowi jakąś wartość dla użytkowników danej platformy. Znane są sytuacje, gdy artefakty w grach były wykorzystywane do prania pieniędzy[62] czy stanowiły przedmiot zamachu[63] lub działań wspierających terroryzm. W przypadku

[60] *SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings*, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [dostęp: 24 III 2023].

[61] *CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange*, CFTC, 27 III 2023 r., https://www.cftc.gov/PressRoom/PressReleases/8680-23 [dostęp: 5 IV 2023].

[62] P. Opitek, *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*, „Przegląd Policyjny" 2017, nr 2, s. 150. https://doi.org/10.5604/01.3001.0013.6082.

[63] Wyrokiem Sądu Rejonowego dla Krakowa-Krowodrzy II Wydział Karny z 3 VIII 2012 r., sygn. akt II Ka 776/11/K, oskarżony został skazany za to, że w dniu 6 II 2011 r. w K. w celu osiągnięcia korzyści majątkowej, bez upoważnienia wpłynął na przesyłanie informacji poprzez przełamanie elektronicznego zabezpieczenia w ten sposób, że zmienił hasło dostępowe do skrzynki poczty elektronicznej o nazwie '...@poczta.onet.pl' należącej do T. K.,

podejrzenia, że wchodzą one w zakres modus operandi sprawcy przestępstwa, należy dokładnie ustalić status prawny takich „wartości". Przykładem na to, jak duże znaczenie ma właściwa ocena charakteru artefaktu, a pomyłka może dyskredytować prokuratora, jest sprawa dotycząca tzw. skinów, która zawisła przed sądem. Oskarżony został uznany przez Sąd Rejonowy w Przasnyszu[64] winnym popełnienia przestępstwa z art. 107 Kodeksu karnego skarbowego[65] w zw. z art. 29a ust. 1 i w zw. z art. 2 ust. 1 *Ustawy z dnia 19 listopada 2009 r. o grach hazardowych* (w brzmieniu sprzed 1 kwietnia 2017 r.), polegającego na tym, że w latach 2016–2017 organizował na platformach internetowych gry hazardowe o charakterze losowym, w których przedmiotem wygranej były wspomniane skiny. Stanowią one rodzaj funkcji używanej w grze *Counter-Strike: Global Offensive* w postaci różnego rodzaju broni, którą gracz może wypożyczyć i w taki sposób zmienić wygląd artefaktów stosowanych w grze[66]. Osoby, które uczestniczyły w losowaniu urządzanym przez oskarżonego, przekazywały do wirtualnego bębna swoje skiny. Następnie były one mieszane i w zależności od regulaminu obowiązującego na danej platformie wybrany losowo uczestnik otrzymywał największą liczbę skinów, a oskarżony pobierał prowizję z tytułu organizacji gry.

W brzmieniu sprzed 1 kwietnia 2017 r. art. 2 ust. 1 ustawy o grach hazardowych stanowił, że (...) *grami losowymi są gry, w tym urządzane przez sieć Internet, o wygrane pieniężne lub rzeczowe, których wynik w szczególności zależy od przypadku*. Tak więc warunkiem wypełnienia przez sprawcę znamion przestępstwa było uznanie przez sąd, że skin stanowi pieniądz lub rzecz[67]. W apelacji złożonej od wyroku skazującego obrońca oskarżonego podniósł, że skin nie może być traktowany jak pieniądz, gdyż nie jest emitowany przez Narodowy Bank Polski, nie jest także przedmiotem materialnym, a jedynie fragmentem kodu programistycznego, nie spełnia zatem definicji

po czym przejął jego postać w grze Metin 2 o nazwie „Joker 78", czym doprowadził T. K. do niekorzystnego rozporządzenia mieniem w kwocie nie mniejszej niż 500 zł, tj. o czyn z art. 287 § 1 k.k.

64 Akta sprawy Sądu Rejonowego w Przasnyszu II Wydział Karny, sygn. akt II K 608/18.

65 *Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy*.

66 https://counterstrike.fandom.com/wiki/Skins [dostęp: 17 II 2022].

67 W zarzucie znajdującym się w akcie oskarżenia i wyroku sądu I instancji napisano, że „ryzyku poddawane są tzw. skiny – wirtualne klucze posiadające w świecie rzeczywistym realną wartość pieniężną i umożliwiające dostęp do wirtualnej broni o różnej sile rażenia i osprzętów wykorzystywanych w walkach gry zręcznościowej 3D o nazwie Counter-Strike Global Offensive (w skrócie CS: GO) oferowane w ramach platformy społecznościowej STEAM należącej do Valve Corporation z siedzibą w Bellevue, Waszyngton, USA".

rzeczy z art. 45 Kodeksu cywilnego[68]. Sąd Okręgowy w Ostrołęce II Wydział Karny[69] podzielił argumentację zawartą w apelacji i wyrokiem z 27 sierpnia 2020 r. uniewinnił oskarżonego od popełnienia zarzucanego mu czynu. W uzasadnieniu wyroku sąd wskazał, że przepisów art. 2 ust. 1 pkt 1 ustawy nie można interpretować rozszerzająco i przez analogię, a oczywiste jest, że skiny nie mają statusu rzeczy lub przedmiotu, są bowiem wirtualnymi wartościami[70].

W ustaleniu statusu prawnego tokena podstawowe znaczenie ma udzielenie odpowiedzi na pytanie, czy stanowi on walutę wirtualną, której definicja legalna znajduje się w art. 2 ust. 2 pkt 26 u.p.p.p. Przeprowadzenie takiej oceny i udzielenie jednoznacznej odpowiedzi, czy dane aktywo podlega reżimowi ustawy AML, może okazać się bardzo trudne, m.in. dlatego że wspomniana definicja jest bardzo pojemna, a użyte w niej zwroty są nieostre[71]. Zakwalifikowanie tokena do walut wirtualnych powoduje, że organy ścigania mogą egzekwować względem instytucji obowiązanej zajmującej się obrotem taką walutą wiele obowiązków związanych z udzieleniem informacji o podejrzanych osobach i transakcjach. Na żądanie organu ścigania instytucja obowiązana powinna dostarczyć pełnych danych uzyskanych podczas pierwszej i kolejnych weryfikacji klienta (KYC) oraz historie wykonanych przez niego transakcji, wiadomości o ewentualnym raportowaniu do GIIF alertów o podejrzanych operacjach czy bazę numerów IP, które zostały wykorzystane do popełnienia przestępstwa. Podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług w zakresie wymiany pomiędzy walutami wirtualnymi i środkami płatniczymi czy konwersji pomiędzy samymi tokenami mają ponadto obowiązek przedłożenia na żądanie organów ścigania dokumentacji określonej w ustawie AML, m.in. przyjętej procedury szacowania ryzyka i przypisania poziomu ryzyka

[68] *Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny*.

[69] Sygn. akt II Ka 40/20.

[70] W obowiązującym stanie prawnym takie zachowanie stanowiłoby przestępstwo na podstawie art. 2 ust. 5 zmienionego *Ustawą z dnia 15 grudnia 2016 r. o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw* (DzU z 2017 r. poz. 88), który uzyskał brzmienie: „Grami na automatach są także gry na urządzeniach mechanicznych, elektromechanicznych lub elektronicznych, w tym komputerowych, oraz gry odpowiadające zasadom gier na automatach urządzane przez sieć Internet organizowane w celach komercyjnych, w których grający nie ma możliwości uzyskania wygranej pieniężnej lub rzeczowej, ale gra ma charakter losowy".

[71] Szczegółowe omówienie poszczególnych składników definicji terminu „waluty wirtualne" zob. w: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy*..., s. 122–139.

konkretnemu klientowi[72]. Omówienie wszystkich środków i źródeł dowodowych, które można wykorzystać w śledztwie dotyczącym kryptowalut, wykracza poza ramy niniejszego opracowania, ale pewne jest, że u.p.p.p. daje organom ścigania duże możliwości działania. Funkcjonariusze znają je słabo i zbyt rzadko z nich korzystają.

Praca operacyjna w ramach zwalczania przestępczości kryptowalutowej

Doświadczenie nabyte w pracy prokuratora pokazuje, że niejawne działania pozaprocesowe stanowią niezbędny element skutecznej walki z przestępczością kryptowalutową. Dzieje się tak z kilku powodów. Sprawcy popełniający takie czyny zabronione są bardzo ostrożni i funkcjonują zazwyczaj w środowisku osób co najmniej tak hermetycznym jak zorganizowane grupy trudniące się handlem narkotykami czy bojówki pseudokibiców. Wynika to z tego, że zaplecze logistyczne do obrotu kryptowalutami jest dostępne zdalnie, a więc osoby z niego korzystające działają w świecie wirtualnym, do którego akces może być nieodwracalnie utracony wraz z zamknięciem matrycy ich laptopa. To jeden z powodów, dla których w ostatnich latach przewartościowaniu uległa metodyka prowadzenia przeszukania miejsc zajmowanych przez podejrzanych i zabezpieczania należącego do nich sprzętu elektronicznego. Wcześniej niepodważalna zasada głosiła, że funkcjonariusz uczestniczący w przeszukaniu, w trakcie którego ujawniono pracującą jednostkę komputera, nie powinien sam dokonywać przeszukania pamięci urządzenia, gdyż zmieni zapis danych w laptopie, co negatywnie przełoży się na wartość dowodową uzyskanych z niego śladów. Dzisiaj przeszukanie mieszkania lub zatrzymanie osoby nierzadko jest poprzedzone czynnościami operacyjnymi ukierunkowanymi na to, aby w momencie ich realizacji ujawnić i przejąć otwarty komputer sprawcy. Daje to możliwość uzyskania dostępu do wielu cennych informacji i danych zapisanych w pamięci urządzenia lub zasobach chmurowych, z którymi się łączy. W taki sposób można przejąć, tytułem zabezpieczenia majątkowego, cyfrowe mienie, uzyskać hasła dostępu do aplikacji wykorzystywanych do popełniania przestępstw lub do konta na giełdzie

[72] Szczegółowe omówienie źródeł dowodowych, które organy ścigania mogą wykorzystać w działaniach procesowych i operacyjnych związanych z walutami wirtualnymi, jest dostępne w: J. Skała, *Uzyskiwanie przez prokuratora informacji i danych*...

kryptowalutowej, sprawdzić, z jakich stron oraz serwisów internetowych korzystał sprawca, poznać treść rozmów prowadzonych przez niego za pomocą komunikatorów. Jeśli komputer zostanie zamknięty, to jest prawdopodobne, że biegły z zakresu informatyki śledczej nie będzie w stanie przełamać hasła zabezpieczającego dostęp do urządzenia, a nawet jeśli je uruchomi, to i tak zostaną utracone dane zapisane w ulotnej pamięci operacyjnej RAM czy dostęp do artefaktów przechowywanych przez przestępcę na innych serwerach.

Działania podejmowane w celu przejęcia otwartego komputera mogą mieć różny charakter, od podstępu (np. wejście do mieszkania „na listonosza"), przez pułapkę kryminalistyczną (sprowokowanie przestępcy do otworzenia laptopa w miejscu publicznym, co umożliwi jego przejęcie), aż po wykorzystanie zaawansowanych czynności operacyjno-rozpoznawczych. Może je poprzedzać zakamuflowana obserwacja osób i miejsc, wywiad posesyjny czy współpraca z dostawcą usług sieciowych, którego abonentem jest osoba podejrzewana. W grę wchodzi także kontrola operacyjna, zakup kontrolowany i przesyłka niejawnie nadzorowana. Zdarzało się, że organy ścigania nabywały bitcoiny, zakładały własne konta w darkmarkecie i kupowały narkotyki oferowane na platformie po to, aby ustalić kanały przesyłania zabronionych substancji, sposób ich dostawy oraz uzyskać quasi-opinię kryminalistyczną z zakresu badań fizykochemicznych, jak również ustalić, z jakimi środkami mają do czynienia w świetle ustawy o narkomanii[73].

Skuteczność niejawnych operacji w cyberprzestrzeni ukierunkowanych na zwalczanie przestępczości powiązanej z kryptowalutami potwierdzają doświadczenia służb amerykańskich. Chodzi m.in. o wykorzystanie funkcjonariusza operującego w Internecie pod przykryciem czy ustalanie położenia i zamykanie serwerów przechowujących nielegalne treści. Fizyczne przejęcie serwera to duży sukces, gdyż znajdują się na nim ślady będące dla organów ścigania źródłem wielu cennych informacji o setkach osób prowadzących nielegalną działalność z wykorzystaniem infrastruktury IT. Takie przejęcie to jednak niemałe wyzwanie i zazwyczaj jest ono możliwe tylko w ramach współpracy międzynarodowej. W dniu 28 lutego 2023 r. policje niemiecka i ukraińska, przy wsparciu Europolu, policji holenderskiej i FBI, aresztowały członków grupy przestępczej odpowiedzialnej za cyberataki typu ransomware bazujące na oprogramowaniu Doppel-Paymer oraz Dridex i ukierunkowane na infrastrukturę krytyczną firm

[73] *Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii.*

prywatnych. Oprogramowanie ransomware było dystrybuowane różnymi kanałami, w tym metodą phishingu i za pomocą załączonych do spamu dokumentów zawierających złośliwy kod JavaScript lub VBScript. Jednego z najpoważniejszych ataków dokonano na Szpital Uniwersytecki w Düsseldorfie, a w Stanach Zjednoczonych ofiary zapłaciły co najmniej 40 mln euro w kryptowalucie za odszyfrowanie danych[74]. Cechy ransomware są przyrównywane do ataków terrorystycznych, gdyż stanowią poważne zagrożenie bezpieczeństwa narodowego. Podobnie jak terroryzm ransomware koncentruje się na celach miękkich, takich jak cywilna infrastruktura krytyczna, ale w przeciwieństwie do terroryzmu jest motywowany przede wszystkim względami finansowymi[75]. Niekiedy jednak trudno jest postawić wyraźną granicę pomiędzy tymi dwoma cyberzagrożeniami. Na przykład rząd Korei Północnej jest odpowiedzialny za wiele poważnych ataków ransomware na infrastrukturę krytyczną na całym świecie. W 2021 r. Departament Sprawiedliwości Stanów Zjednoczonych ogłosił akt oskarżenia dotyczący trzech urzędników rządu Korei Północnej podejrzanych o przeprowadzenie kilku najniebezpieczniejszych cyberataków, m.in. WannaCry 2.0 (okup za odszyfrowanie danych płacono w kryptowalucie), włamanie do bazy danych Sony Pictures oraz do Banku Bangladeszu. W akcie oskarżenia zarzucono, że hakerzy są członkami koreańskiego wywiadu wojskowego, powiązanego z grupą hakerską o nazwie Lazarus, od lat zaangażowanego w operacje w cyberprzestrzeni[76]. Ślad koreański przypisywano także zaawansowanemu

---

[74] *Germany and Ukraine hit two high-value ransomware targets,* Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [dostęp: 6 IV 2023]. Elissa Slotkin, przewodnicząca ds. Wywiadu i Kontrwywiadu Kongresu USA, w trakcie zeznań przed Kongresem w 2021 r. powiedziała o dokonanych wówczas w Stanach Zjednoczonych atakach terrorystycznych ransomware, „które uderzyły w serce życia codziennego w Ameryce, od gazociągów i przetwórstwa mięsnego i roślin, po funkcjonowanie szkół i szpitali", a na jej spotkaniu z wyborcami „pierwsze pytania rolników dotyczyły cyberataków, kryptowaluty i tego, co rząd zrobił, żeby ich chronić". Zob. *Statement of Chairwoman Elissa Slotkin…*, s. 2.

[75] *Ransomware Attacks on Critical Infrastructure Sectors,* U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf, s. i [dostęp: 11 V 2023].

[76] M. Dugas, *The Latest North Korea Cyber Indictment Should Serve as a Model,* Just Security, 24 II 2021 r., https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [dostęp: 11 V 2023]. W akcie oskarżenia ustalono, że Korea Północna w wyniku cyberterroryzmu, tj. włamań do banków, kradzieży kryptowalut, zarobiła łącznie ponad 1,3 mld dolarów (PKB tego kraju szacuje się na zaledwie 28 mld dolarów). Organizacja Narodów Zjednoczonych oszacowała natomiast, że za pomocą swoich operacji

i zakamuflowanemu cyberatakowi na system teleinformatyczny Komisji Nadzoru Finansowego (KNF) dokonanemu w Polsce w 2021 r. Chociaż wszystkie cele atakujących do dzisiaj nie są jawne, jednym z nich było przedostanie się do zaufanej sieci wewnętrznej systemów bankowych, przejęcie kontroli nad komputerami tam umieszczonymi i ustanowienie komunikacji pomiędzy systemami ofiary a infrastrukturą kontrolowaną przez przestępców[77].

Skuteczne działania przeciwko zorganizowanym grupom przestępczym operującym w Internecie wymagają tworzenia zespołów operacyjnych składających się z przedstawicieli różnych służb ochrony prawa, a nierzadko także podjęcia współpracy międzynarodowej. W Stanach Zjednoczonych powstała specjalna jednostka o nazwie J-CODE (ang. Joint Criminal Opioid and Darknet Enforcement) do walki z cyberprzestępcami, którą tworzy siedem instytucji, m.in. FBI, HSI, Departament Sprawiedliwości oraz Służba Kontroli Pocztowej (ang. The Postal Inspection Service). Wynika z tego, że trudna do przecenienia rola w zwalczaniu wirtualnego handlu substancjami zabronionymi przypada straży granicznej, inspekcji celnej i poczcie, gdyż realizacja usługi transportu towaru zamówionego przez Internet to moment, kiedy wirtualny świat przestępców styka się ze światem materialnym, a powstała w ten sposób sytuacja pozwala nie tylko przejąć nielegalny towar, lecz także podjąć inne działania pod kątem ustalenia i zatrzymania przestępców[78]. Niewskazany jest zatem stan rzeczy zaobserwowany w jednej z krajowych służb, w której odseparowano od siebie pion zajmujący się odzyskiwaniem mienia od komórek realizujących czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze. Efektywne zwalczanie przestępczości kryptowalutowej, w tym realizacja zabezpieczenia majątkowego na tokenach cyfrowych, wymaga stałej współpracy i szybkiego przepływu informacji pomiędzy osobami zajmującymi się różnymi aspektami zwalczania przestępstw, tj. pracą operacyjną, dochodzeniową, odzyskiwaniem mienia. *A contrario* osoba zajmująca się odzyskiwaniem majątku pochodzącego z przestępstwa będzie

cybernetycznych Korea Północna zgromadziła w 2019 r. ponad 2 mld dolarów pochodzących z nielegalnego finansowania w celu sfinansowania programu zbrojeniowego.

[77] Więcej na temat ataku zob. A. Maciąg, I. Tarnowski, *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 11 V 2023].

[78] P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych*, w: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle,* D. Zienkiewicz (red.), Toruń 2021, s. 434.

miała poważne trudności z realizacją tego zadania w stosunku do kryptoaktywów, jeśli w ogóle nie uczestniczy w czynnościach procesowych polegających na przeszukaniu czy przesłuchaniu świadka lub nie ma dostępu do bieżących informacji z ustaleń pozaprocesowych.

Ciekawie rysuje się problem stosowania kontroli operacyjnej w postaci uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych[79], a więc kontroli urządzenia końcowego. Można z całą pewnością stwierdzić, że dzisiaj walka z cyberprzestępczością wymaga stosowania takiej metody pracy operacyjnej, gdyż przestępcy kontaktują się ze sobą głównie za pomocą urządzeń tworzących sieć Internet. Prawo jednoznacznie dopuszcza uzyskiwanie danych zapisanych na dysku urządzenia jako jedną z form kontroli operacyjnej. Obecnie wysiłek Policji, jak również Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego, powinien skupiać się na zwiększaniu zdolności technicznych do kontroli operacyjnej pamięci laptopa, telefonu, modemu czy routera w sposób pasywny, tj. bez modyfikowania śladów cyfrowych znajdujących się w kontrolowanym przedmiocie. Idealnym rozwiązaniem byłoby objęcie kontrolą operacyjną sprzętowego portfela kryptowalutowego, chociaż pod względem technicznym jest to zadanie trudne do realizacji. Umożliwiłoby to m.in. poznanie całej historii transakcji, aktualnej wysokości salda bitcoinów znajdujących się w urządzeniu czy nawet realizację zabezpieczenia majątkowego na ujawnionych kryptowalutach[80]. Podobnych informacji dostarczyłoby objęcie kontrolą w formie uzyskiwania i utrwalania treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej, założonego na giełdzie konta tzw. figuranta, na które są przesyłane dodatkowe dane, jak chociażby kody do wypłat pieniędzy w bankomacie po konwersji krypto na pieniądz fiducjarny. Co prawda na podstawie pisma lub postanowienia prokuratora można żądać od administratora giełdy przedłożenia wspomnianych danych, ale przejęcie kontroli nad kontem pomogłoby w uzyskiwaniu na bieżąco informacji i planowaniu z wyprzedzeniem realizacji zadań. Patrząc szerzej,

[79] Taka metoda kontroli jest przewidziana w ustawach regulujących pracę Policji i 9 służb.

[80] Stwierdzenie, że w portfelu znajdują się jednostki waluty wirtualnej, stanowi skrót myślowy. W rzeczywistości bowiem portfel zawiera dane cyfrowe umożliwiające zarządzanie jednostkami altcoinów w postaci tzw. klucza publicznego i prywatnego, ale same tokeny są odwzorowane w księdze rozrachunkowej nazywanej blockchainem w formie cyfrowego zapisu danych.

zasadne jest wprowadzenie nowej metody kontroli operacyjnej w postaci nieprzerwanego („w locie") śledzenia transferów pieniądza bezgotówkowego, innych środków płatniczych lub kryptoaktywów poprzez ustanowienie nowej, ustawowej formy pracy operacyjnej[81].

W zwalczaniu przestępczości kryptowalutowej znajdują zastosowanie tradycyjne metody i formy pracy operacyjnej. Na przykład funkcjonariusz Policji czy służby specjalnej operujący na platformie internetowej pod legendą jej rzeczywistego użytkownika otrzymuje status FPP, tj. funkcjonariusza działającego pod przykryciem, ze wszystkimi tego konsekwencjami. Dochodzi zatem do realizacji kombinacji operacyjnej w postaci np. zakupu kontrolowanego narkotyków przez agenta, a następnie przesyłki niejawnie nadzorowanej. Ma to na celu rozpracowanie środowiska osób uczestniczących w handlu internetowym nielegalnymi substancjami, ustalenia sposobu przesyłania narkotyków i dostarczania ich klientowi, składu chemicznego tych substancji oraz sposobu komunikowania się pomiędzy kupującym i sprzedającym. Kryptowaluty przeznaczone do płatności za założenie konta czy uiszczenia ceny towaru będą pochodzić z funduszu operacyjnego służby, a operacje nimi dokonywane są szczegółowo dokumentowane aż do pełnego rozliczenia kosztów podjętych działań. Muszą być one odpowiednio dokumentowane w formie notatek z przeprowadzonych czynności na każdym etapie operacji specjalnej wraz z dołączonymi zdjęciami ekranu, a najlepiej nagraniem wideo, dokumentującymi to, co FPP wykonuje w cyberprzestrzeni. Ważne są zrzuty rozmów na komunikatorach prowadzonych przez agenta z osobami łamiącymi prawo, gdyż najczęściej w takiej formie cyberprzestępcy przekazują sobie informacje. Dokumenty z przeprowadzonych czynności, stanowiące materiał dowodowy świadczący o podejrzeniu popełnienia przestępstwa, powinny być w odpowiednim momencie udostępnione przez komendanta Policji lub szefa służby specjalnej do postępowania karnego.

Śledztwo dotyczące przestępczości kryptowalutowej

Rok 2022 był rekordowy pod względem liczby szkoleń i konferencji na temat walut wirtualnych zorganizowanych przez polskie organy ścigania.

[81] Szerzej na ten temat zob. P. Opitek, *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)*, „Prokuratura i Prawo" 2021, nr 2, s. 154–175.

Najwięcej uwagi poświęcono tematowi zabezpieczenia majątkowego na kryptowalutach. Okazuje się jednak, że stricte procesowa realizacja samego zabezpieczenia (tj. wydanie stosownych decyzji przez prokuratora) jest łatwiejsza niż ujawnienie bitcoinów pochodzących z przestępstwa i faktyczne objęcie ich w posiadanie samoistne. Śledztwo dotyczące przestępczości kryptowalutowej w sprawach o dużym ciężarze gatunkowym lub takich, w których istnieje realna możliwość postawienia konkretnych osób w stan oskarżenia, to żmudny proces wykrywczy związany z gromadzeniem obszernego materiału dowodowego. Sukces tego śledztwa zależy od wiedzy i determinacji osób je prowadzących, a niekiedy decyduje o nim również łut szczęścia.

Omawiane postępowania karne wymagają posiadania umiejętności w zakresie gromadzenia śladów cyfrowych oraz dowodów nie tylko od polskich i zagranicznych dostawców usług sieciowych, takich jak giełdy i kantory kryptowalutowe, lecz także od przedsiębiorców dostarczających Internet, operatorów telekomunikacyjnych czy instytucji finansowych, na czele z bankami. Wiadomości cenne dla postępowania przygotowawczego mogą mieć także administratorzy systemów monitoringu przemysłowego (nagrania wypłat bankomatowych), zarządcy dróg krajowych (rejestracja przemieszczania się pojazdów), przewoźnicy w transporcie samolotowym, podmioty obsługujące szybkie płatności typu BLIK czy administratorzy platform handlowych w sieci. Niemniej jednak źródłem największej ilości danych nadal pozostają giełdy kryptowalutowe. Można zażądać od nich wydania informacji dotyczących:

- danych osobowych użytkownika giełdy, które są gromadzone w trakcie realizacji procedury KYC i mogą być zmieniane w trakcie korzystania przez klienta z platformy (imię, nazwisko, data urodzenia, PESEL, numer telefonu, adres zamieszkania itd.);
- skanu dokumentów potwierdzających jego tożsamość (dowód osobisty, prawo jazdy, paszport itp.) oraz innych dokumentów przedłożonych przez klienta w trakcie korzystania z usług oferowanych przez giełdę (np. deklaracji o źródle pochodzenia inwestowanych środków);
- informacji o zrealizowanych transakcjach w walutach wirtualnych i pieniądzu fiducjarnym (wykaz transakcji, ich data, wartość operacji, beneficjent otrzymanych środków);
- daty dostępu do systemu giełdy przez potencjalnego sprawcę (przedłożenie zestawienia logowań do platformy osób pozostających

w zainteresowaniu organów ścigania, wraz z wszelkimi atrybutami w postaci adresów IP portów ze wskazaniem dokładnego czasu logowania, lokalizacji BTS, numerów IMEI/MAC urządzenia inicjującego połączenia internetowe). Należy ponadto sprawdzić, czy dodano nowe urządzenie zaufane do logowań na konto giełdy oraz dane urządzeń, z których następowały logowania (system operacyjny, wersja systemu, rozdzielczość ekranu, wersja przeglądarki);
- historii konta użytkownika giełdy (kody wysłane do przeprowadzenia transakcji bankomatowych, informacje i ostrzeżenia otrzymane od administratora giełdy);
- informacji, czy w trakcie trwania stosunków gospodarczych z klientem wystąpiły anomalie transakcyjne (np. transakcja została niezrealizowana, gdyż środki pochodziły z adresu uznanego za podejrzany, blokowano rachunki bankowe lub adresy walut wirtualnych, wstrzymywano transakcje – jeśli tak, to kiedy i dlaczego);
- zapisów rozmów telefonicznych lub wideokonferencji przeprowadzonych pomiędzy pracownikami giełdy a osobą podejrzewaną;
- dokonywania przez instytucję obowiązaną zgłoszenia do GIIF, prokuratury lub innego organu publicznego w sprawie użytkownika giełdy (kiedy i z jakiego powodu wystosowano zgłoszenie);
- wypłat „skradzionych" środków, zwłaszcza docelowego adresu portfela, na który wypłacono środki, oraz identyfikatora transakcji (*hash* transakcji).

Procedury i zakres danych (np. logi) oraz informacji (historia transakcji) możliwych do uzyskania od giełd zależą od kilku czynników, m.in. siedziby giełdy, rodzaju i ilości danych pozostawionych na platformie przez jej użytkownika czy etapu postępowania karnego. Organy ścigania i dostarczyciele usług sieciowych wypracowali wiele zasad współpracy. Niekiedy otrzymanie żądanych przez prokuratora treści jest realizowane na podstawie pisma procesowego. Wniosek powinien wskazywać funkcjonariusza i jednostkę prowadzącą sprawę, sygnaturę postępowania, zawierać krótki opis sprawy ze wskazaniem, jakie przestępstwo zarzuca się osobie, której dotyczy wniosek. Należy przesłać go drogą elektroniczną na adres oficjalnego punktu kontaktowego giełdy, o którym informację posiadają zazwyczaj organy ochrony prawa. Pismo powinno być sporządzone w języku angielskim lub języku kraju, w którym funkcjonuje giełda. Dokument główny powinien stanowić skan pisma urzędowego, a załącznik ze szczegółowymi danymi należy wysłać w formie edytowalnej po to, aby było możliwe

skopiowanie danych (np. adresów kryptowalutowych) i dalsza praca na nich. Jeśli sprawa ma charakter pilny, to należy to w piśmie wyraźnie zaznaczyć. Co ważne, ponieważ niektóre giełdy informują swoich klientów o prowadzonym w stosunku do nich śledztwie, to we wniosku można zastrzec, aby dostarczyciel usług sieciowych zaniechał takiego poinformowania, oraz uzasadnić to żądanie.

Są jednak jurysdykcje, w których uzyskanie informacji innych niż metadane (ang. *non-content data*) będzie uwarunkowane wydaniem nakazu przez właściwy miejscowo sąd. Wówczas wnioski o międzynarodową pomoc prawną są kierowane na podstawie umów zawieranych między suwerennymi państwami, co w praktyce znacznie wydłuża proces gromadzenia artefaktów. Dotyczy to m.in. Stanów Zjednoczonych, a więc terytorium, na którym funkcjonuje największa liczba firm będących dostarczycielami usług sieciowych. W Europie pomocny okazuje się europejski nakaz dochodzeniowy powszechnie stosowany przez funkcjonariuszy policji i prokuratorów. Osoba zajmująca się przestępczością kryptowalutową musi zatem orientować się zarówno w prawnych, jak i praktycznych aspektach uzyskiwania dowodów, gdyż procedura z tym związana zależy od kilku czynników:

- siedziby firmy oraz usytuowania serwera z danymi;
- rodzaju danych, o które chodzi: *content data* czy *non-content data* (te ostatnie często są udostępniane w sposób odformalizowany);
- zastosowanej procedury: „zamrażania" danych do czasu uzyskania zezwolenia na ich przekazanie, procedury uzyskania właściwych danych czy pilnego uzyskiwania danych w sytuacjach nadzwyczajnych (ang. *emergency cases*);
- polityki wewnętrznej podmiotu zobowiązanego do udostępniania informacji i danych w zakresie zarządzania nimi.

Ostatecznie, jeśli giełda lub inna platforma cyfrowa odmawia realizacji przewidzianej przez prawo procedury wydania danych i informacji lub znacznie ją utrudnia, można rozważyć zajęcie jej serwera w celu ekstrakcji niezbędnych artefaktów lub sprawdzenia, czy nie zostały z niego usunięte. Czasami wizja nieuchronności zajęcia infrastruktury prowadzi do otwarcia się na współpracę ze strony dostawcy usług. Takie działania są niemożliwe w stosunku do podmiotów działających w darkmarkecie, w którym lokalizacja ich infrastruktury jest nieznana, oraz w krajach niewspółpracujących w ramach międzynarodowej pomocy prawnej.

Kolejne ważne informacje dla śledztwa z wątkiem kryptowalutowym są zapisane na sprzęcie elektronicznym wykorzystywanym przez

użytkowników końcowych protokołu Bitcoina, a przede wszystkim w ich telefonach i komputerach. Na zabezpieczonym dowodowym nośniku danych znajdują się artefakty pozwalające ustalić, czy jego użytkownik posługiwał się walutami wirtualnymi, łączył się ze stronami przeznaczonymi do ich obsługi, a w pamięci komputera, w tym operacyjnej RAM, mogą znajdować się ślady lub informacje (hasła, loginy itp.) pozwalające autoryzować dostęp do baz danych, tj. aplikacji, zasobów chmurowych czy portfela kryptowalutowego. Jeśli w jakimkolwiek systemie ujawniono dane statuujące tokeny cyfrowe i należące do podejrzanego, to trzeba je niezwłocznie zabezpieczyć na potrzeby toczącego się śledztwa. W tym celu autorzy postulują, aby utworzyć w jednej z wiodących służb specjalnych w obszarze bezpieczeństwa ekonomicznego RP (np. ABW) lub Policji grupę operacyjno-śledczą składającą się z funkcjonariuszy, którzy będą mieli kompetencje związane z zabezpieczaniem bitcoinów i posiadali zaplecze technologiczne do ich przejmowania we władanie. Chodzi o takie umiejętności, jak oględziny lub przeszukanie systemu informatycznego komputera stanowiącego dowód w miejscu jego ujawnienia, obsługa elektronicznej portmonetki należącej do sprawców czynu zabronionego, ale także o dysponowanie przez formacje zwalczające przestępstwa własnym portfelem sprzętowym do przyjmowania kryptowaluty, rozpoznawania rodzajów cyfrowych aktywów, generowania dla nich adresów. Szczególnie ważna jest instytucja zabezpieczenia majątkowego na kryptowalutach, o której mowa w art. 291 § 1 k.p.k. i nast. W Polsce takie zabezpieczenia są realizowane od kilku już lat (pierwsze wykonano w 2017 r.), a z każdym rokiem ich liczba rośnie. W celu przejęcia bitcoinów funkcjonariusze Policji najczęściej współpracowali z internetowymi giełdami, które najpierw zamrażały środki znajdujące się na podejrzanym koncie, a następnie tworzyły specjalne konto dla prokuratury i na nim składowały przedmiot zabezpieczenia. Znany jest także co najmniej jeden przypadek wygenerowania przez policjantów portfela papierowego, ale najbardziej bezpieczne i praktyczne jest dysponowanie przez służby portfelem sprzętowym typu Ledger lub Trezor. Najtrudniejszym zadaniem w toku czynności operacyjno-rozpoznawczych lub dochodzeniowo-śledczych wydaje się ustalenie, gdzie znajdują się waluty wirtualne pochodzące ze śledztwa, a następnie uzyskanie do nich faktycznego dostępu z możliwością transferu na adres zarządzany przez prowadzącego postępowanie. Znane są bowiem przypadki, w których na podstawie analizy kryminalnej transferów kryptowalutowych ustalono adresy składowania znacznych ilości tokenów pochodzących z przestępstwa,

np. włamań na giełdy, ale nie były one powiązane z żadną z publicznych platform internetowych, brakowało ustaleń w zakresie osób zarządzających tymi adresami i w konsekwencji – możliwości przejęcia władztwa nad środkami wirtualnymi. W takiej sytuacji pozostaje tylko oflagowanie takiego adresu, a więc jego monitorowanie w oczekiwaniu, aż zgromadzone na nim środki zostaną przez kogoś przelane na inny, mniej anonimowy adres.

W przypadku bitcoinów, które zostały już przejęte przez organy ścigania, pojawiają się trudności prawne i faktyczne z ich przechowywaniem. Wynikają one z tego, że cena walut wirtualnych jest bardzo płynna i podlega dużym różnicom kursowym w krótkich odstępach czasu, a każdy z portfeli jest narażony na atak hakerski, uszkodzenie mechaniczne lub informatyczne, a ponadto może zdarzyć się błąd ludzki związany z ich obsługą. Ponadto polskie sądy nie są gotowe na przejmowanie kryptowalut, które zostałyby przekazane wraz z aktem oskarżenia. Praktycznym rozwiązaniem tych problemów jest sprzedaż zabezpieczonego majątku w trakcie śledztwa na podstawie art. 232 § 1 k.p.k. w zw. z art. 236a k.p.k. Stanowią one, że przedmioty, których przechowywanie byłoby połączone z nadmiernymi trudnościami albo powodowałoby znaczne obniżenie wartości rzeczy, można sprzedać według trybu określonego dla właściwych organów postępowania wykonawczego, a ten przepis stosuje się odpowiednio do tokenów cyfrowych stanowiących dane informatyczne. Sprzedaż rzeczy następuje według przepisów o postępowaniu egzekucyjnym w administracji lub zawartych w Kodeksie postępowania cywilnego w zależności od tego, jaka była podstawa zajęcia środków (art. 291 § 1 pkt 1–5 k.p.k.). Inny problem prawny dotyczy treści art. 295 § 1 k.p.k., w którym jest mowa o mieniu ruchomym, a bitcoin nie jest rzeczą w rozumieniu art. 45 k.c. W praktyce jednak instytucja tymczasowego zajęcia mienia ruchomego była już efektywnie stosowana w odniesieniu do walut wirtualnych, a ponadto rozwiązaniem w takim przypadku może okazać się art. 236b k.p.k., a więc uznanie kryptowaluty za środki zgromadzone na rachunku i wydanie postanowienia w przedmiocie dowodów rzeczowych.

Ślady cyfrowe dotyczące walut wirtualnych oraz – ogólniej rzecz biorąc – popełnionego cyberprzestępstwa należy odpowiednio gromadzić, zabezpieczać, a następnie wykorzystywać w śledztwie. Prezentacja w toku postępowania karnego dowodu cyfrowego opiera się na regule, że stanowi on nie tylko to, co widać, lecz także ma metadane. Problem ten zaistniał we wspomnianej już w artykule sprawie rozpatrywanej przed Sądem Rejonowym w Przasnyszu, w której prokurator jako dowód

na wygląd i sposób funkcjonowania stron internetowych poświęconych skinom załączył do aktu oskarżenia wydruki takich stron. W piśmie procesowym obrońca oskarżonego wskazał nieprzydatność dowodu w postaci papierowych wydruków stron internetowych, na których znajdowały się informacje stanowiące – zdaniem oskarżyciela publicznego – dowód popełnienia przestępstwa zarzucanego oskarżonemu. Obrońca oskarżonego podniósł, że:

> (...) w analizowanym stanie faktycznym ewidentnie ma miejsce sytuacja, polegająca na tym, że przeprowadzenie dowodu wskazanego we wniosku dowodowym nie może doprowadzić do stwierdzenia okoliczności w nim wskazanej. Strona internetowa ma charakter interaktywny i sam tylko 'zrzut ekranu' i do tego wydrukowany na kartce papieru nie oddaje jej istoty i sposobu funkcjonowania. Zdaniem obrońcy dowód na okoliczności, których dotyczą zakwestionowane wydruki stron internetowych, powinny zostać przeprowadzone w ten sposób, że oskarżyciel, podczas postępowania dowodowego, odtworzy funkcjonowanie ustalonych stron internetowych. Jest to z całą pewnością technicznie możliwe (chociażby poprzez zapisanie stron na trwały nośnik), ale niewątpliwie wymaga od oskarżyciela nieco więcej wysiłku[82].

Sąd podzielił stanowisko obrony, a to, a także z uwagi na wiele innych błędów popełnionych podczas dochodzenia, skutkowało uniewinnieniem oskarżonego. Wynika z tego, że funkcjonariusze służb powinni mieć wiedzę, umiejętności i należyte oprogramowanie do interaktywnych oględzin lub przeszukiwania stron internetowych[83]. Szczególnie ta druga czynność, tj. przeszukanie w cyberprzestrzeni, mogłaby być częściej wykonywana w toku czynności procesowych, gdyż pozwala uzyskać informacje i zabezpieczyć najważniejsze dowody dla śledztwa, a mimo to referenci spraw karnych albo obawiają się realizacji takich, ich zdaniem, trudnych czynności, albo robią to bez należytej staranności w postaci sporządzenia notatki urzędowej, pomimo że art. 143 § 1 pkt 1 i 6 k.p.k. wymaga w tym przypadku spisania protokołu.

[82] Akta sprawy Sądu Rejonowego w Przasnyszu II Wydział Karny, sygn. akt II K 608/18.

[83] Zob. P. Opitek, *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, „Prokuratura i Prawo" 2022, nr 9, s. 100–128.

Wnioski końcowe

Przeprowadzona analiza wybranych aspektów przestępczości z wykorzystaniem walut wirtualnych prowadzi do kilku podstawowych wniosków. Rola kryptoaktywów w działalności profesjonalnych podmiotów rynku kapitałowego stale rośnie i coraz więcej osób użytkuje tego rodzaju mienie. Kryptoaluty są wykorzystywane także przez przestępców, a liczba spraw karnych związanych przestępczością kryptowalutową z każdym rokiem wzrasta. Raporty instytucji publicznych i doświadczenia autorów pokazują, że nielegalne działania z udziałem infrastruktury krypto mogą dotyczyć poważnych czynów karalnych godzących w podstawy ekonomiczne państwa, służyć do sponsorowania terroryzmu i działań szpiegowskich, korupcji, omijania sankcji, a zatem wpływać na bezpieczeństwo Polski i jej renomę na arenie międzynarodowej. Prowadzi to do prostego wniosku, że organy ścigania, w tym odpowiednie służby specjalne, muszą dysponować wielowymiarowymi zdolnościami (odpowiednio przygotowanymi ludźmi i zapleczem logistycznym) do pracy z kryptowalutami, w kwestiiach zarówno ogólnych (praca z dowodami cyfrowymi, poznanie istoty technologii blockchain), jak i szczegółowych (umiejętność posługiwania się wirtualnymi portfelami, redefinicja pracy funkcjonariusza pod przykryciem w cyberprzestrzeni, a być może stworzenie funduszu operacyjnego w postaci kryptoaktywów). Oczywiste jest, że nie każdy funkcjonariusz takiej instytucji będzie specjalistą w zakresie kryptowalut, niemniej powinien on bezzwłocznie otrzymać profesjonalne wsparcie w momencie, gdy w jego postępowaniu zaistnieją tematy związane z tokenami cyfrowymi. Biorąc ponadto pod uwagę, że nie zawsze jest możliwa współpraca lidera ochrony bezpieczeństwa państwa z innymi organami ochrony prawa wyspecjalizowanymi w zwalczaniu cyberprzestępczości, to tym bardziej tak elitarna formacja powinna mieć własną grupę (strukturę) osób wyspecjalizowanych w realizacji czynności procesowych i pozaprocesowych dotyczących kryptowalut (np. zabezpieczenia majątkowego na bitcoinie).

Patrząc szerzej, należy monitorować polski rynek walut wirtualnych pod kątem ewentualnego prania pieniędzy z wykorzystaniem wartości binarnych czy omijania sankcji nałożonych na Białoruś i Rosję. Instrumenty przydatne do realizacji wspomnianych zadań oferuje u.p.p.p. Wszystkich celów dotyczących minimalizowania zagrożeń bazujących na kryptoaktywach nie sposób osiągnąć bez instytucjonalnej współpracy pomiędzy ABW, prokuraturą, GIIF i KNF, gdyż każda z tych instytucji ma swoiste, tylko jej

przypisane narzędzia prawne i możliwości faktyczne. Dopiero ich synergia daje możliwość budowy skutecznej i wszechstronnej polityki AML/CFT.

Analiza tematu kryptowalut pokazała, że zostały one użyte także do wspierania działań terrorystycznych o różnym charakterze – sponsorowania organizacji terrorystycznych z wykorzystaniem internetowego crowdfundingu, bezpośrednich dotacji na rzecz konkretnej osoby pomagającej w organizacji zamachów lub motywowanej do nich czy też cyberataków ukierunkowanych na infrastrukturę teleinformatyczną obszarów kluczowych dla funkcjonowania państwa. Z informacji podanych przez przedstawiciela HSI wynika, że w Stanach Zjednoczonych liczba postępowań karnych dotyczących kryptowalut wzrosła od jednego w 2011 r. do ponad 604 śledztw w 2021 r. Przez ten czas HSI skonfiskowała bitcoiny i altcoiny o równowartości 79 825 606,65 dolarów. Obrazuje to rosnące zaufanie sprawców czynów nielegalnych o najwyższym ciężarze gatunkowym do kryptoaktywów, a zatem implikuje konieczność zdobywania przez organy ścigania kompetencji do walki z tym rodzajem finansowania terroryzmu[84]. I chociaż główne źródła tego finansowania nadal opierają się na tradycyjnych instytucjach finansowych[85] (szacuje się, że obecnie finansowanie terroryzmu za pomocą kryptowalut generuje tylko 1% takich transakcji[86]), to problem z pewnością będzie narastał. Sposoby działania i podejście sprawców do świata wirtualnego zmieniają się i ewoluują ku najkorzystniejszym dla nich rozwiązaniom. Dzięki opisanym w artykule skutecznym akcjom amerykańskich służb przeciwko platformom internetowym Brygady Izz ad-Din al-Kassam w kwietniu 2023 r. oświadczyło, że zawiesza zbieranie datków z wykorzystaniem bitcoina, powołując się na wzrost „wrogiej" działalności wobec darczyńców. *Wynika to z troski o bezpieczeństwo darczyńców i chęci oszczędzenia im wszelkich szykan* – brzmiał komunikat Hamasu[87]. Jednocześnie wezwano do (...) *kontynuowania darowizn na rzecz Kassama i ruchu oporu wszelkimi dostępnymi środkami*[88].

[84] *Statement of John Eisert...*, s. 14–16.

[85] *Risk Assessment. 2022 National Terrorist Financing...*

[86] *Statement of Ranking Member August Pfluger*, w: *Terrorism and Digital Financing...*, s. 3.

[87] N. Al-Mughrabi, *Hamas armed wing announces suspension of bitcoin fundraising*, Reuters, 28 IV 2023 r., https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [dostęp: 9 V 2023]; *Hamas armed wing to stop crypto fundraising over 'hostility' against donors*, i24NEWS, 30 IV 2023 r., https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [dostęp: 9 V 2023].

[88] Tamże.

Polska jest podmiotem działań terrorystycznych wykorzystujących infrastrukturę Internetu i kryptowaluty. Są to m.in. wymierzone w RP ataki ransomware czy zamieszczone w Darknecie, operującym bitcoinem, ogłoszenia zachęcające do zabójstw najważniejszych, wymienionych z imienia i nazwiska, polskich polityków. Zagadnienia dotyczące kryptowalut są powiązane także z działalnością wrogich organizacji wywiadowczych ukierunkowaną na bezpieczeństwo Polski. Konieczne jest zatem, aby najważniejsze służby ochrony państwa zwiększały swoje kompetencje w zakresie aktywności w świecie wirtualnym, realizacji cyberoperacji i przeciwdziałania wrogim atakom IT. Dotyczy to m.in. umiejętności badania transferów kryptowalutowych, zabezpieczania takich wartości majątkowych, ale także ich wykorzystywania do realizacji własnych celów.

Bibliografia

Chainalysis, *The 2022 Crypto Crime Report*, luty 2022 r.

Ocieczek G., Opitek P., *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Consilium Iuridicum" 2022, nr 3–4, s. 122–139.

Opitek P., *Biegły z zakresu kryptowalut w sprawach karnych*, w: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, D. Zienkiewicz (red.), Toruń 2021, s. 413–447.

Opitek P., *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain*, Łódź 2022.

Opitek P., *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)*, „Prokuratura i Prawo" 2021, nr 2, s. 154–175.

Opitek P., *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*, „Przegląd Policyjny" 2017, nr 2, s. 138–158. https://doi.org/10.5604/01.3001.0013.6082.

Opitek P., *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722.

Opitek P., *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, „Prokuratura i Prawo" 2022, nr 9, s. 100–128.

Opitek P., *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu*, Warszawa 2019 (praca dyplomowa napisana na studiach podyplomowych w Szkole Głównej Handlowej, niepublikowana, w zasobach autora).

Prawo cywilne – część ogólna, M. Safjan (red.), seria: System Prawa Prywatnego, t. 1, Warszawa 2007.

Przewłoka E., *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej*, Bydgoszcz 2023 (metodyka wewnętrzna Policji, w zbiorach autora).

Skała J., *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, z. 3, s. 83–100. https://doi.org/10.53024/4.3.47.2022.

Źródła internetowe

Al-Mughrabi N., *Hamas armed wing announces suspension of bitcoin fundraising*, Reuters, 28 IV 2023 r., https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [dostęp: 9 V 2023]

Alnasaa M. i in., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022 r., https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [dostęp: 4 V 2023].

Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers, Council of the EU, 29 VI 2022 r., https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [dostęp: 7 IV 2023].

Berton B., *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 23 VIII 2019].

Bitcoin wa Sadaqat al-Jihad, https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf [dostęp: 20 I 2019].

CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange, CFTC, 27 III 2023 r., https://www.cftc.gov/PressRoom/PressReleases/8680-23 [dostęp: 9 IV 2023].

Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 10 IV 2023].

Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned, Ledger Insights, 28 II 2023 r., https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [dostęp: 10 IV 2023].

Dugas M., *The Latest North Korea Cyber Indictment Should Serve as a Model*, Just Security, 24 II 2021 r., https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [dostęp: 11 V 2023].

Farah D., Richardson M., *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023 r., https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [dostęp: 6 IV 2023].

Fight against money laundering and terrorist financing, European Council, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [dostęp: 9 IV 2023].

Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme, United States Attorney's Office, Eastern District of New York, 19 X 2022 r., https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [dostęp: 7 IV 2023].

Germany and Ukraine hit two high-value ransomware targets, Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [dostęp: 6 IV 2023].

Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, The United States Department of Justice, 13 VIII 2020 r., https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [dostęp: 9 V 2023].

Hamas armed wing to stop crypto fundraising over 'hostility' against donors, i24NEWS, 30 IV 2023 r., https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [dostęp: 9 V 2023].

How Russians Use Tether to Evade Global Sanctions, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [dostęp: 10 IV 2023].

https://counterstrike.fandom.com/wiki/Skins [dostęp: 17 II 2022].

Illicit Finance Risk Assessment of Decentralized Finance, U.S. Department of the Treasury, kwiecień 2023 r., https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [dostęp: 14 IV 2023].

Living on the Edge, International Monetary Fund, październik 2022 r., https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [dostęp: 5 IV 2023].

Maciąg A., Tarnowski I., *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 11 V 2023].

MUFG's Progmat security token platform to become digital asset joint venture, Ledger Insights, 7 X 2021 r., https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [dostęp: 5 IV 2023].

MUFG, SBI share roadmap for Japanese security tokens, Ledger Insights, 7 X 2021 r., https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [dostęp: 27 III 2023].

National Strategy for Combating Terrorist and Other Illicit Financing 2020, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [dostęp: 7 VII 2023].

O'Sullivan F., *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency*, Cloudwards, 22 II 2023 r., https://www.cloudwards.net/where-is-crypto-illegal/ [dostęp: 5 IV 2023].

Perez Y.B., *Bitcoin, Paris and Terrorism: What the Media Got Wrong*, CoinDesk, 6 III 2023 r., https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [dostęp: 10 V 2023].

Preiss I., *Crypto AML rules passed by MEPs*, The Block, 28 III 2023 r., https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [dostęp: 6 IV 2023].

Ransomware Attacks on Critical Infrastructure Sectors, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf [dostęp: 11 V 2023].

Risk Assessment. 2022 National Terrorist Financing, Department of the Treasury, luty 2022 r., https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf [dostęp: 10 V 2023].

SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [dostęp: 24 III 2023].

Sigalos M., Goswami R., *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023 r., https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [dostęp: 9 IV 2023].

Sutton S., Seligman L., *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023 r., https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [dostęp: 10 IV 2023].

Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives, https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf [dostęp: 10 V 2023].

UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf [dostęp: 9 IV 2023].

United States of America v. Samuel Bankman-Fried, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [dostęp: 7 IV 2023].

United States of America v. Ali Shukri Amin, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [dostęp: 10 V 2023].

Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [dostęp: 7 IV 2023].

White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, The White House, 16 IX 2022 r., https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [dostęp: 9 IV 2023].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156/43 z 19 VI 2018 r.).

Rozporządzenie Rady (UE) NR 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 229/1 z 31 VII 2014 r.).

Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (DzU z 2021 r. poz. 815, ze zm.).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. DzU z 2023 r. poz. 1124, ze zm.).

Ustawa z dnia 19 listopada 2009 r. o grach hazardowych (t.j. DzU z 2023 r. poz. 227).

Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. DzU z 2023 r. poz. 172, z 2022 r. poz. 2600).

Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (t.j. DzU z 2023 r. poz. 654, ze zm.).

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

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. DzU z 2022 r. poz. 1360, ze zm.).

Ensuring Responsible Development of Digital Assets, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [dostęp: 5 IV 2023].

Orzecznictwo

Akta sprawy Sądu Rejonowego w Przasnyszu II Wydział Karny, sygn. akt II K 608/18.

Wyrok Sądu Okręgowego w Ostrołęce z 27 VIII 2020 r., sygn. akt II Ka 40/20.

Wyrok Sądu Rejonowego dla Krakowa-Krowodrzy II Wydział Karny z 3 VIII 2012 r., sygn. akt II Ka 776/11/K.

Inne dokumenty

Markets in crypto-assets (MiCA), https://www.europarl.europa.eu [dostęp: 9 IV 2023].
Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [dostęp: 9 IV 2023].

Poglądy zawarte w artykule są osobistymi poglądami autorów i nie wyrażają oficjalnego stanowiska instytucji, w której są zatrudnieni.

Dr Paweł Opitek

Doktor nauk prawnych, prokurator Prokuratury Okręgowej w Krakowie delegowany do Prokuratury Krajowej.

Dr Agnieszka Butor-Keler

Doktor w dziedzinie nauk społecznych w dyscyplinie ekonomia i finanse, adiunkt w Katedrze Rachunkowości Menedżerskiej w Szkole Głównej Handlowej w Warszawie.

Karol Kanclerz

Aplikant radcowski, główny specjalista w Departamencie Prawnym Urzędu Komisji Nadzoru Finansowego.

https://doi.org/10.4467/27204383TER.23.019.18321

https://orcid.org/0000-0003-0385-3650

AGNIESZKA DOBRZYŃSKA-JAROSZ

Zabezpieczenia strefowe współczesnych obiektów dyplomatycznych na przykładzie budynków ambasad w Europie powstałych bądź zmodernizowanych na przełomie XX i XXI wieku

Abstrakt

Obiekty dyplomatyczne to budynki z wyjątkową strukturą i o dużym znaczeniu międzynarodowym. Jednym z czynników istotnych przy ich projektowaniu jest bezpieczeństwo, a co za tym idzie – zastosowanie możliwych sposobów zabezpieczeń (aktywnych i pasywnych), by zapobiec potencjalnym zagrożeniom. Celem artykułu jest przedstawienie stosowanych środków bezpieczeństwa w zakresie architektury obiektów dyplomatycznych na przykładzie budynków ambasad w Europie. Pod tym kątem zanalizowano 22 ambasady znajdujące się w Warszawie, Berlinie i Rzymie. W artykule scharakteryzowano elementy zastosowane przy ich projektowaniu, realizacji i modernizacji na przełomie XX i XXI w.

Słowa kluczowe:

architektura ambasad, bezpieczeństwo, obiekty dyplomatyczne, zabezpieczenia

Budowy obiektów dyplomatycznych w porównaniu z innymi obiektami użyteczności publicznej zdarzają się stosunkowo rzadko, a realizacje bądź modernizacje są podejmowane z określonych przyczyn przez państwa wysyłające. Z uwagi na lokalizację – przeważnie w stolicach państw – w ich bezpośrednim otoczeniu znajdują się inne budynki dyplomatyczne lub obiekty o różnym przeznaczeniu, tj. obiekty rządowe, budynki użyteczności publicznej, budynki usługowe i zabudowa mieszkaniowa. Placówki dyplomatyczne tworzą swoiste strefy w zabudowie miejskiej i – jak inne obiekty budowlane – są jej częścią przez wiele lat. Dlatego niezmiernie istotne jest ich odpowiednie projektowanie. Projektanci obiektów dyplomatycznych muszą wziąć pod uwagę m.in. uwarunkowania prawne, ekonomiczne, użytkowe, techniczne, przestrzenne i potrzebę zapewnienia właściwego poziomu bezpieczeństwa.

Celem badawczym artykułu jest zebranie, opisanie, uporządkowanie i usystematyzowanie informacji na temat architektury budynków ambasad powstałych bądź zmodernizowanych w Europie na przełomie XX i XXI w. w odniesieniu do współcześnie stosowanych środków bezpieczeństwa i wykorzystywanych w tym zakresie rozwiązań architektonicznych.

Przy rozpatrywaniu zagadnienia architektury ambasad oprócz analizy projektów architektoniczno-budowlanych ważne są także pozycje literaturowe poświęcone prawu międzynarodowemu i dziedzinie szeroko pojętej dyplomacji, w tym publikacje na temat prawa dyplomatycznego, konsularnego, polityki zagranicznej, a także genezy stosunków międzynarodowych, w których często pomija się aspekty architektoniczne. W literaturze przedmiotu są dostępne przede wszystkim zagraniczne publikacje z zakresu zabezpieczeń w przestrzeni publicznej miast wydawane przez organizacje rządowe (głównie brytyjskie i amerykańskie) i organy wykonawcze Unii Europejskiej. Z polskich publikacji do najważniejszych należy zaliczyć prace m.in. architekta Artura Jasińskiego poświęcone bezpieczeństwu i ochronie antyterrorystycznej przestrzeni i obiektów budowlanych, w których autor przybliża współczesne zasady formowania wymagań urbanistycznych i architektonicznych nieruchomości. Opisuje regulacje prawne dotyczące budowy, zabezpieczeń budynków i terenów otwartych. W swoich analizach uwzględnia normy brytyjskie i amerykańskie, odnosi się także do zabezpieczeń antyterrorystycznych architektury współczesnych ambasad amerykańskich.

Do najnowszych europejskich opracowań z zakresu projektowania bezpiecznych przestrzeni publicznych należą publikacje Komisji Europejskiej, m.in. komunikat z 9 grudnia 2020 r. *Program zwalczania terroryzmu dla UE: przewidywanie, zapobieganie, ochrona, reagowanie*[1] i opracowanie z końca 2022 r. pt. *Security by Design: Protection of public spaces from terrorist attacks* (pol. Bezpieczeństwo od samego początku. Ochrona przestrzeni publicznej przed atakami terrorystycznymi)[2].

Warto podkreślić, że ambasady w architekturze były traktowane przede wszystkim jako budynki reprezentacyjne. Dopiero w ostatnich 30 latach jest zauważalny wzrost zainteresowania ich rozwiązaniami architektonicznymi[3]. Potwierdza to m.in. zwiększająca się liczba publikacji na ich temat, chociaż w Polsce są to wciąż głównie nieliczne artykuły dotyczące konkretnych realizacji publikowane m.in. w miesięcznikach branżowych[4].

---

1 *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0795&from=PL [dostęp: 5 VII 2023].

2 Komisja Europejska, *Security by Design: Protection of public spaces from terrorist attacks*, https://www.urbanagenda.urban-initiative.eu/news/security-design-protection-public-spaces-terrorist-attacks [dostęp: 20 IV 2023]. (Tłumaczenia w tekście pochodzą od autorki – dop. red.).

3 Wzrost zainteresowania wiąże się z upadkiem ery komunizmu w państwach Europy Środkowo-Wschodniej i zburzeniem muru berlińskiego w 1989 r., kiedy to nastąpiła wielopłaszczyznowa współpraca międzynarodowa. Niedługo później powstała Unia Europejska, a państwa wysyłające zdecydowały się zaprezentować swoje siedziby (głównie w Niemczech) na nowo.

4 Są to m.in.: A. Jasiński, *Wpływ zabezpieczeń antyterrorystycznych na architekturę współczesnych ambasad amerykańskich*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 97–114; T. Fretton, G. Stiasny, *Ambasada Wielkiej Brytanii w Warszawie*, „Architektura–Murator" 2009, nr 12, s. 56–63; B. Gadomska, *Ambasada Izraela w Berlinie*, „Architektura–Murator" 2002, nr 2, s. 16–19; W. Gorczyński, *Ambasada Kanady w Warszawie*, „Architektura–Murator" 2002, nr 2, s. 9–15; H. Jootsen, A. Stępniowska, *Ambasada Niemiec w Warszawie*, „Architektura–Murator" 2009, nr 12, s. 48–55; M. Leśniakowska, *Architektura polskich ambasad*, „Architektura–Murator" 2004, nr 2, s. 60–62; K. Majewski, M. Sroka-Strzeszyńska, *Ambasada Korei Południowej*, „Architektura–Murator" 2004, nr 2, s. 38–41; J.P. Pagarde, G. Stiasny, *Ambasada Francji w Warszawie*, „Architektura–Murator" 2005, nr 2, s. 30; A. Sitko, S. Szafarczyk, *Technologie architektury – Ambasada Królestwa Niderlandów w Warszawie*, „Architektura–Murator" 2004, nr 2, s. 90–97; E. van Egeraat, G. Stiasny, *Ambasada Królestwa Niderlandów*, „Architektura–Murator" 2004, nr 2, s. 25–37; G. Stiasny, *Konkursy na nowe budynki ambasad w Warszawie*, „Architektura–Murator" 2004, nr 2, s. 44–59.

Potencjalne zagrożenia dla ambasad

Działania terrorystyczne obserwowane w ostatnich ponad 20 latach przyczyniają się do wprowadzania zmian w strukturach urbanistycznych i architektonicznych miast. Najbardziej zagrożone są stolice państw i metropolie[5]. W wyniku działalności terrorystycznej zaostrzają się restrykcje związane z minimalizacją skutków ataków i zapobieganiem im. W XXI w. terroryzm nabrał nowego wymiaru. Za sprawą rozwoju technologii, komunikacji, mediów społecznościowych informacje mogą być przekazywane w coraz szybszym tempie. Możliwa jest zatem sprawna rekrutacja potencjalnych zamachowców, którzy obierając za cel również ludność cywilną i miejsca publiczne[6], chcą doprowadzić do ataku z jak największą liczbą rannych i ofiar śmiertelnych[7]. Jak już wspomniano, ambasady znajdują się przeważnie w centrach stolic, w pobliżu budynków rządowych i innych ważnych obiektów użyteczności publicznej, w miejscach tłumnie uczęszczanych w ciągu dnia. Tym samym mogą one stać się bezpośrednim lub pośrednim celem ataków terrorystycznych. Dlatego tak istotne jest odpowiednie przeciwdziałanie potencjalnym działaniom zagrażającym – już na etapie projektowania i wykonawstwa – mające na celu pełne zabezpieczenie obiektów lub zminimalizowanie skutków ewentualnego ataku terrorystycznego.

Warto podkreślić, że projektowanie placówek zagranicznych nie jest w żaden sposób zunifikowane. Dobór projektów koncepcyjnych, budowlanych bądź realizacyjnych w przypadku budynków ambasad zależy od wewnętrznych regulacji prawnych zarówno w państwie wysyłającym, jak i państwie przyjmującym, z uwzględnieniem w pierwszej kolejności norm prawnych kraju macierzystego placówki. Liczbę modernizacji, zakupów obiektów bądź projektów nowych budynków warunkuje budżet przeznaczony na te cele. Wiele pomieszczeń i obiektów jest wynajmowanych.

---

[5] A. Jasiński, *Architektura w czasach terroryzmu. Miasto–przestrzeń publiczna–budynek*, Warszawa 2013, s. 9.

[6] Przykładami opisywanych ataków terrorystycznych są zamachy przeprowadzone m.in. na bliźniacze wieże World Trade Center w Nowym Jorku z użyciem uprowadzonych samolotów pasażerskich (11 IX 2001 r.) oraz zamach bombowy w metrze i autobusie w Londynie (lipiec 2005 r.).

[7] Współczesny terroryzm jest rozumiany jako działalność ugrupowań ekstremistycznych, które swoimi atakami, zamachami, porwaniami itp. usiłują zwrócić uwagę opinii publicznej na propagowane idee lub starają się wymusić w ten sposób na rządach poszczególnych krajów określone ustępstwa bądź korzyści. Za: *Encyklopedia*, t. 9, Warszawa 2001, s. 141.

W 2004 r. naczelnik Wydziału Inwestycji i Remontów polskiego Ministerstwa Spraw Zagranicznych stwierdził, że zakup nowego obiektu jest rentowny, gdy wskaźnik kosztów najmu w stosunku do kosztów zakupu zwróci się w ciągu dziesięciu lat[8].

Ataki terrorystyczne, będące największym zagrożeniem bezpieczeństwa placówek dyplomatycznych, mogą polegać na pojedynczych akcjach (z wykorzystaniem broni palnej, materiałów wybuchowych) bądź masowych atakach (z użyciem materiałów wybuchowych, broni chemicznej, biologicznej lub jądrowej, ang. *chemical, biological, and radiological*, CBR)[9]. Z największym ryzykiem wiąże się jednak atak przeprowadzony za pomocą ładunku wybuchowego umieszczonego w pojeździe, tzw. samochodów pułapek (ang. *vehicle borne improvised explosive device*). Siła rażenia wybuchu często ma katastrofalne skutki, dlatego zaleca się lokalizowanie miejsc parkingowych dla pojazdów stanowiących potencjalne zagrożenie w miarę możliwości daleko od budynków, aby w ten sposób zmniejszyć ryzyko szkód[10]. Zwraca się przy tym uwagę na możliwą prędkość i masę pojazdów[11].

W latach 80. XX w. doszło do wielu ataków terrorystycznych na amerykańskie placówki dyplomatyczne na Bliskim Wschodzie. W kwietniu 1983 r. w Bejrucie w wyniku najazdu na ambasadę Stanów Zjednoczonych i eksplozji samochodu wypełnionego materiałami wybuchowymi prowadzonego przez islamskiego zamachowca samobójcę śmierć poniosły 63 osoby, a 120 osób zostało rannych. Rok później miał miejsce kolejny wybuch przy ambasadzie, w wyniku którego zginęły 24 osoby, a 21 zostało rannych. W dniu 23 października 1983 r. w zamachu na koszary US Marines na terenie

[8] K. Rzechowski, *Polskie placówki dyplomatyczne*, „Architektura–Murator" 2004, nr 2, s. 63–70.

[9] Najczęstszym zagrożeniem są także ataki z użyciem materiałów wybuchowych (bomb). Można spośród nich wyróżnić: wybuch zaparkowanego samochodu załadowanego materiałami wybuchowymi w pobliżu placówki lub na jej terenie, staranowanie wjazdu lub wejścia, lub fasady ambasady samochodem załadowanym materiałami wybuchowymi, umieszczenie ładunku wybuchowego w przesyłce lub towarze podlegającym dostawie, podrzucenie lub umieszczenie ładunku na terenie budynku, atak zamachowca samobójcy. Zob. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, seria: Buildings and Infrastructure Protection Series, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, s. 1/15 [dostęp: 16 V 2016].

[10] *Embassy Perimeter Improvement Concepts & Design Guidelines*, Department of State Bureau of Overseas Buildings Operations, 2011 r., https://www.scribd.com/document/261408078/Embassy-Perimeter-Improvement-Concepts-Design-Guidelines, s. 56; *Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks*, seria: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [dostęp: 13 V 2023].

[11] *Embassy Perimeter Improvement Concepts...*, s. 56–72.

lotniska zginęło 241 żołnierzy. W dniu 12 grudnia 1983 r. przeprowadzono w Kuwejcie ataki na ambasady Stanów Zjednoczonych i Republiki Francuskiej[12]. W sierpniu 1998 r. zaatakowano amerykańskie ambasady w Kenii i Tanzanii (zdjęcie 1). Te zdarzenia wykazały ogrom niedoskonałości w systemie ich ochrony i obrony. Od tego czasu rząd USA pracuje nad poprawą wytycznych i standardów ochrony i kształtowania swoich zagranicznych placówek dyplomatycznych[13].

A

B

Zdjęcie 1. Stan budynków ambasad USA po atakach terrorystycznych w sierpniu 1998 r. – ambasada w Nairobi w Kenii (A), ambasada w Dar es Salaam w Tanzanii (B).

Źródło: *Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks*, seria: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, s. 1/29, 1/31 [dostęp: 13 V 2023].

Budynki ambasad mogą także zostać uszkodzone w wyniku ataku terrorystycznego przeprowadzonego w sąsiedztwie obiektu. Stało się tak np. w Atenach w listopadzie 2015 r., kiedy ambasada Republiki Cypryjskiej została poważnie zniszczona wskutek eksplozji bomby (zdjęcie 2). Najprawdopodobniej celem ataku terrorystów był budynek Federation of Greek Industries (pol. Grecka Federacja Biznesu) mieszczący się naprzeciwko ambasady. Jednak siła eksplozji i podmuchu była tak duża, że zostały uszkodzone: strefa wejściowa budynku, fasada frontowa i szklenie ściany zewnętrznej od parteru do szóstej kondygnacji. Konstrukcja budynku ambasady znacznie ucierpiała, mimo że nie to było zamierzeniem zamachowców.

[12] *Site and Urban Design for Security...*, s. 1/29–1/31.

[13] Zob. szerzej: A. Jasiński, *Wpływ zabezpieczeń...*, s. 97–114.


A


B

Zdjęcie 2. Strefa wejściowa do Ambasady Republiki Cypryjskiej w Atenach – stan przed wybuchem (A), stan po eksplozji bomby (B).

Źródło: zdjęcie 2A – własność autorki; 2B – A. Kades, *Cypriot embassy severely damaged in Athens bomb blast*, http://cyprus-mail.com/2015/11/24/cypriot-embassns-bomb-attack/ [dostęp: 24 XI 2015].

Warto podkreślić, że politykę antyterrorystyczną, z rygorystycznymi warunkami dotyczącymi m.in. własnych placówek zagranicznych, najdokładniej opracowano w USA i Wielkiej Brytanii. Indywidualne regulacje prawne obejmujące zagadnienie terroryzmu zawierają istotne wytyczne co do kształtowania architektury ambasad i należących do nich przestrzeni. W świetle prowadzonych na szeroką skalę badań nad zabezpieczeniami budynków, obiektów dyplomatycznych oraz przestrzeni publicznej przed zagrożeniami terrorystycznymi oba podejścia – odpowiednie stosowanie zabezpieczeń oraz formowanie obiektów – są istotne już na etapie projektowania.

Sposoby zabezpieczeń obiektów dyplomatycznych

Przy analizie zagadnień dotyczących bezpieczeństwa budynków ambasad najważniejszym, wiążącym aktem prawnym jest konwencja wiedeńska o stosunkach dyplomatycznych, na której podstawie ambasady, ich tereny i pracownicy są chronieni. Określa ona, że pomieszczenia misji mają zapewnioną nietykalność[14]. Analogicznie ochronie przez państwo przyjmujące podlega rezydencja ambasadora, niezależnie od tego, czy znajduje się ona w obrębie budynku ambasady czy poza nim[15]. Państwo przyjmujące jest natomiast zobowiązane m.in. do przedsięwzięcia wszelkich

[14] *Konwencja wiedeńska o stosunkach dyplomatycznych, sporządzona w Wiedniu dnia 18 kwietnia 1961 r.*, art. 22, 29 i 30.

[15] Tamże, art. 30. Rezydencja prywatna przedstawiciela dyplomatycznego korzysta z takiej samej nietykalności i ochrony jak pomieszczenia misji.

stosownych kroków w celu ochrony ambasady przed wtargnięciem osób niepożądanych lub szkodą, przed zakłóceniem spokoju misji i uchybieniem jej godności. Co istotne, państwo przyjmujące odpowiada za bezpieczeństwo, ochronę i poszanowanie placówki zagranicznej nawet w sytuacji konfliktu zbrojnego, zerwania stosunków dyplomatycznych czy odwołania misji. Nietykalność ambasad obowiązuje także w przypadku zgromadzeń publicznych, manifestacji itp.[16] Państwa przyjmujące są zobowiązane również do zapobiegania próbom dokonania napaści na ambasady. Pomimo wszystkich wspomnianych regulacji i obowiązków można zaobserwować sytuacje naruszające bezpieczeństwo ambasad i ich pracowników.

Jak wspomniano, najważniejsze polskie opracowania poświęcone kształtowaniu architektury i przestrzeni urbanistycznej w kontekście terroryzmu opublikował architekt Artur Jasiński. Określa on dwie możliwości zapewnienia odpowiedniego poziomu bezpieczeństwa w razie ataku terrorystycznego przeprowadzonego z użyciem materiałów wybuchowych. Pierwsze rozwiązanie to zabezpieczenie strefowe, tj. odpowiednio duża, wyposażona w przeszkody pośrednie strefa bezpieczeństwa, dzięki której można zachować należytą odległość obiektu od miejsca możliwej eksplozji, tak by budynek nie został uszkodzony. Drugi sposób to wzmocnienie jego konstrukcji i elementów. Jasiński podkreśla, że pierwszy wariant jest bardziej skuteczny, ekonomiczny i szybszy w realizacji, ponieważ nie we wszystkich istniejących już obiektach można dokonać zmian technicznych[17].

W swoich opracowaniach Jasiński opisuje i charakteryzuje dokumenty, akty prawne i publikacje naukowe – powstałe głównie w Stanach Zjednoczonych i Wielkiej Brytanii – poświęcone problematyce terroryzmu i odpowiedniej ochrony przestrzeni publicznej oraz budynków o różnym przeznaczeniu[18]. Jednocześnie zwraca uwagę, że w polskiej literaturze brakuje opracowań na ten temat i wymienia jedynie własne badania i publikacje.

Preferowane zabezpieczenia strefowe polegają na rozlokowaniu barier ochronnych wokół chronionego obiektu i wykorzystaniu środków

[16] W przypadku organizacji zgromadzeń w pobliżu siedzib przedstawicielstw dyplomatycznych gmina winna jest niezwłocznie powiadomić ministra spraw zagranicznych o miejscu, terminie i potencjalnej liczbie uczestników. Zob. *Ustawa z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach*.

[17] A. Jasiński, *Architektura w czasach terroryzmu…*, s. 177.

[18] Zob. szerzej: tamże, s. 13–30.

znajdujących się pomiędzy granicami działki a budynkiem, które mogą znacznie obniżyć skuteczność ataku[19]. Istotne są takie elementy, jak ogrodzenia, wjazdy bramne, wjazdy techniczne, wejścia, parkingi, kontrole dostępu i bezpieczeństwa (nadzór wizyjny, bramki obrotowe, sensoryczne, wykrywania metali, skanery RTG do kontroli bagażu i paczek). Do elementów zabezpieczeń strefowych zalicza się m.in. formę ukształtowania terenu, jego nierówności, występujące cieki wodne i elementy wprowadzone przez człowieka, np. bariery w postaci murów, ogrodzeń, ścian oporowych, a także obiekty małej architektury[20]. W literaturze przedmiotu rozróżnia się dwie grupy zabezpieczeń strefowych obiektów: pasywne i aktywne[21].

Pasywne sposoby zabezpieczeń strefowych obiektów dyplomatycznych

Do elementów pasywnych służących ochronie ambasad możemy zaliczyć[22]:

- **wzmocnione stalowe lub żelbetowe meble miejskie**, np. ławki, siedziska, słupki, kwiatony, donice, stojaki na rowery, latarnie, tablice informacyjne, wiaty przystankowe, wiaty osłaniające – dostosowane do miejsca tak, aby odległość pomiędzy nimi nie wynosiła więcej niż 1,2 m;
- **mury oporowe lub wolnostojące ściany** (punktowe lub obwodowe), których zadaniem jest ochrona przed staranowaniem i niepożądanym wjazdem na teren, np. poprzez uzupełnienie i wzmocnienie naturalnie występującego ukształtowania terenu, obiektu czy ogrodzenia. W przypadku ich lokalizacji w strefie dostępnej publicznie (tj. plac, chodnik itp.) mogą to być murki wyposażone w siedziska lub nasadzenia roślinne bądź obłożone specjalnymi okładzinami wykończeniowymi. Dodatkowo można wprowadzić zintegrowane systemy obwodowe z elementami roślinności, miejscami odpoczynku

[19] *Reference Manual to Mitigate...*, s. 2/2.

[20] A. Jasiński, *Architektura w czasach terroryzmu...*, s. 177.

[21] Zabezpieczenia przestrzeni publicznej i stref wokół budynku zostały zarekomendowane oraz opisane m.in. w: *Reference Manual to Mitigate...*, s. 2/18–2/77; *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*, seria: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema427.pdf, s. 6/1–6/7 [dostęp: 30 V 2023]; A. Jasiński, *Architektura w czasach terroryzmu...*, s. 177–198.

[22] Opracowane na podstawie amerykańskich standardów dotyczących projektowania ambasad i zaleceń przygotowanych przez Amerykańskie Federalne Centrum Zarządzania Kryzysowego (ang. US Federal Emergency Management Agency). Zob. także: D. Cormie, G. Mays, P. Smith, *Blast effects on buildings*, London 2009, s. 250–273; *Embassy Perimeter Improvement Concepts...*, s. 56–72; *Site and Urban Design for Security...*

i punktami informacyjnymi, zawierające przerwy na przejścia piesze (zalecana szerokość wynosi 1 m). Stosuje się również rozwiązania w postaci zbrojonych, prefabrykowanych, betonowych barier drogowych (ang. *jersey barriers*), możliwych do sprawnego przemieszczania, mogące skutecznie oddzielić określone strefy;
– **statyczne, wolnostojące słupy**, które zapobiegają nieuprawnionym wjazdom i parkowaniu samochodów oraz wyznaczają strefy wyłączone z ruchu kołowego. Mogą one występować pojedynczo lub w grupach i przyjmować różne formy, np. proste – pełniące wyłącznie funkcję ochronną, architektoniczno-dekoracyjne (np. zintegrowane z oświetleniem), widoczne bądź ukryte (zintegrowane z innymi elementami, np. kwiatonami, ławkami lub donicami) – (zdjęcie 3);


A


B

Zdjęcie 3. Statyczne słupki będące elementem ochrony strefowej przed Ambasadą Królestwa Niderlandów w Berlinie (A), wolnostojące słupki ochronne i donice będące elementem pasywnego zabezpieczenia strefowego przed Ambasadą Izraela w Atenach (B).

Źródło: własność autorki.

– **rzeźby** (określane jako *NoGo barriers)* zaprojektowane specjalnie dla obszaru Wall Street w Nowym Jorku[23], będące oryginalną formą statycznych wolnostojących słupków (zdjęcie 4). Formy typu *NoGo barriers* są wymyślane i wykonywane w taki sposób, aby wyglądały estetycznie, były atrakcyjne wizualnie i mogły – oprócz nadrzędnej roli ochronnej – pełnić funkcje użytkowe jako siedziska czy stoliki.

[23] Artystyczne formy mające zapewnić odpowiedni poziom bezpieczeństwa w strefie Wall Street zostały zaprojektowane przez amerykańskie biuro projektowe Rogers Marvel Architects. Zob. http://www.rogersmarvel.com/projects/NYSE/ [dostęp: 28 V 2023].

Elementami ochronnymi mogą być też inne rzeźby i instalacje artystyczne;


A


B

Zdjęcie 4. *NoGo barriers* w obrębie strefy Wall Street – formy rzeźbione wykonane z brązu zintegrowane z oświetleniem (A), siedziska zintegrowane z pneumatycznie opuszczanymi słupkami przejazdowymi (B).

Źródło: http://www.rogersmarvel.com/projects/NYSE/ [dostęp: 15 VI 2016].

– **naturalne formy ochrony**, tj. elementy przyrody mogące pełnić funkcję bariery ochronnej przy jednoczesnym integralnym uzupełnieniu kompozycji otoczenia (zdjęcie 5). Można do nich zaliczyć m.in. głazy, masywnie i odpowiednio głęboko posadowione, stanowiące skuteczne zabezpieczenie strefowe; naturalne bądź wtórnie stworzone cieki wodne (strumyki, sadzawki, oczka wodne, fosy, wodospady, fontanny, rzeki itp.); formy ogrodowe *aha*[24] (fr. *ha-ha*), tj. ukryte elementy uniemożliwiające wkroczenie na teren ogrodu, np. ukryty rów, uskok albo ciek wodny; masywne nasadzenia, których system korzeniowy nie może uszkodzić innych elementów zabezpieczeń strefowych (np. ogrodzenia), rozmieszczone w odpowiedniej odległości od osłon obwodowych w celu zapewnienia pełnego oglądu i kontroli poprzez system kamer i system ochrony fizycznej, uniemożliwiający wspięcie się i przejście osób niepożądanych;

[24] Za: *Encyklopedia humanistyczna*, http://encenc.pl/aha/ [dostęp: 14 V 2023].


A


B

Zdjęcie 5. Drzewa, donice i gazony będące elementami pasywnego zabezpieczenia strefy – przed Ambasadą Republiki Francuskiej w Warszawie (A), przed Ambasadą Kanady w Warszawie (B).

Źródło: własność autorki.

– **ogrodzenia** z materiałów różnych pod względem faktury i przejrzystości (np. kamień, cegła, stał, szkło, perforowany metal, siatka) wykonane w sposób uniemożliwiający wspinanie się (zdjęcie 6). Zaleca się stosowanie pionowych przepierzeń, które pozwalają użytkownikom przestrzeni miejskiej na wgląd na teren ambasady, dzięki czemu miejsce zyskuje przyjazny i otwarty charakter.


A


B

Zdjęcie 6. Fasada i ogrodzenie frontowe Ambasady Królestwa Niderlandów w Warszawie (A), widok ogrodzenia i fasady od strony północno-zachodniej Ambasady Królestwa Wielkiej Brytanii w Warszawie (B).

Źródło: własność autorki.

Aktywne sposoby zabezpieczeń strefowych obiektów dyplomatycznych

Aktywne środki zabezpieczeń strefowych znajdują się przede wszystkim w miejscach wjazdów, przejazdów, punktów dostępu, wjazdów technicznych, wjazdów i wyjazdów awaryjnych. Wśród nich możemy wyróżnić dwa typy rozwiązań: sterowane mechanicznie lub ręcznie:

– **wolnostojące słupki** umieszczane w obrębie przejazdu, opuszczane hydraulicznie, pneumatycznie, elektrycznie bądź ręcznie, zrobione

z aluminium, stali, włókna szklanego, często uzupełnione o dodatkowe elementy (oświetlenie, tablice informacyjne)[25] – (zdjęcie 7);

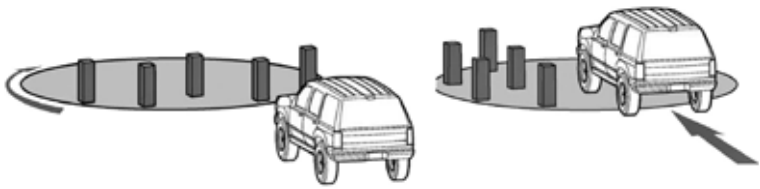
A

B

Zdjęcie 7. Wolnostojące opuszczane słupki – przed bramą wjazdową do parkingu Ambasady Stanów Zjednoczonych w Berlinie (A), w obrębie przejazdu na dziedziniec wewnętrzny Ambasady Królestwa Niderlandów w Berlinie (B).

Źródło: własność autorki.

– **obrotowe platformy przejazdowe**[26], które jako rozwiązanie hybrydowe składają się z dwóch elementów: panelu obrotowego i słupków (rysunek 1).



Rysunek 1. Obrotowe platformy przejazdowe. Po lewej – zamknięty przejazd, po prawej – otwarty przejazd.

Źródło: *Site and Urban Design for Security. Guidance Against Potential Terrorist Attack*, seria: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, s. 4/48 [dostęp: 13 V 2016].

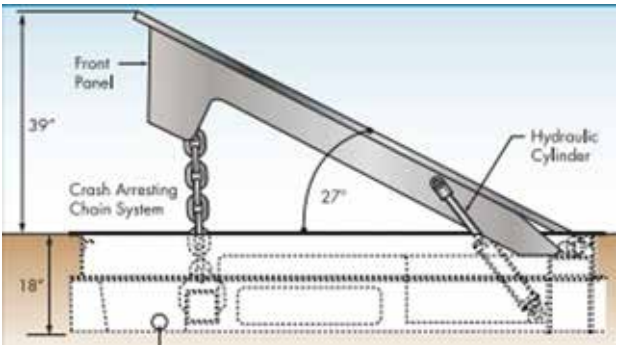
[25] Zob. szerzej: *High Security Bollards*, Delta Scientific Corporation, http://deltascientific.com/high-security/bollards/ [dostęp: 28 V 2023].

[26] Ch.G. Oakes, *The Bollard: Crash- and Attack-Resistant Models*, Whole Building Design Guide, 9 II 2016 r., https://www.wbdg.org/resources/bollard-non-crash-and-non-attack-resistant-models [dostęp: 9 I 2023].

– **tarcze lub zapory przejazdowo-drogowe**[27] służące do zablokowania wjazdu pojazdom nieuprawnionym. Po odebraniu sygnału z panelu sterującego mogą one zostać wysunięte, a po ustąpieniu zagrożenia – schowane. W zależności od formy ruchomego elementu wyróżnia się dwa rodzaje zapór drogowych. Pierwszy to zapory z wznoszącym się klinem (ang. *rising wedge*) – (zdjęcie 8 i rysunek 2).

Zdjęcie 8. Zapora drogowa typu wznoszącego się klina przed bramą wjazdową na teren Ambasady Stanów Zjednoczonych w Baku.

Źródło: *U.S. Embassy security upgrades in Baku*, https://www.pernixgroup.com/project/baku-design-build-isat-security-upgrades/ [dostęp: 10 I 2023].



Rysunek 2. Przekrój zapory drogowej typu wznoszącego się klina.

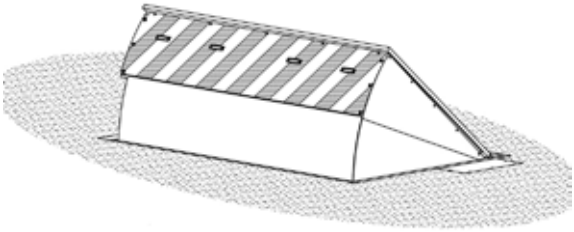
Źródło: *Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks*, seria: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, s. 4/40 [dostęp: 13 V 2023].

[27] *Reference Manual to Mitigate…*, s. 2/57–2/61.

Drugi rodzaj jest wyposażony w panel obrotowy (ang. *rotating wedge system*) – (zdjęcie 9 i rysunek 3).

Zdjęcie 9. Zapora drogowa z panelem obrotowym w strefie wjazdowej przed wjazdem na teren Ambasady i Rezydencji Japonii w Warszawie.

Źródło: http://www.google.pl/maps/ [dostęp: 10 III 2015].



Rysunek 3. Zapora drogowa.

Źródło: https://deltascientific.com/wp-content/uploads/2021/01/90140-Rev-B-DSC207S-General--Arrangement.pdf [dostęp: 9 I 2023].

Dostępne są również **przenośne zapory drogowe**, które są opuszczane i podnoszone hydraulicznie, automatycznie bądź ręcznie (zdjęcie 10)[28].

[28] Element przenośny chroni przed wjazdem i staranowaniem przez pojazdy niepożądane w miejscu, w którym nie można wykonać zapory na stałe. Zaletą takiego rozwiązania jest brak specjalnego fundamentowania lub kotwienia. Blokada składa się z dwóch bocznych stalowych komponentów o masie nieprzekraczającej 318 kg, które wcześniej bądź na miejscu należy wypełnić betonem. Zapora jest wyposażona w panel radiowy i czytnik kart. Szerzej na ten temat zob. *DSC1100 K8 Portable Barriers*, Delta Scientific Corporation, https://deltascientific.com/product/portable-barrier-dsc1100/ [dostęp: 28 V 2023].

Zdjęcie 10. Przenośna zapora drogowa typu DSC1100 przed Ambasadą Wielkiej Brytanii w Budapeszcie.

Źródło: *DSC1100 K8 Portable Barriers*, Delta Scientific Corporation, https://deltascientific.com/product/portable-barrier-dsc1100/ [dostęp: 28 V 2023].

– **bramy wjazdowe** (przesuwne, rozwierne lub otwierane zawiasowo z prześwitem ponad poziomem gruntu albo bez niego) dla pieszych i pojazdów (zdjęcie 11)[29]. W celu zwiększenia poziomu bezpieczeństwa bramy wjazdowe mogą być zintegrowane z innymi elementami ochrony obiektów i przestrzeni ambasad. W praktyce są one łączone z tarczami lub zaporami drogowymi bądź słupkami wolnostojącymi opuszczanymi hydraulicznie lub pneumatycznie.

Zdjęcie 11. Ażurowa brama wjazdowa przed zjazdem do garażu w Ambasadzie Republiki Turcji w Berlinie, za bramą są widoczne ruchome słupki zabezpieczające.

Źródło: własność autorki.

[29] Występują systemy obsługiwane ręcznie lub mechanicznie. Wielkości i formy bram zależą od producentów. Oferują oni różne rodzaje bram o rozpiętościach od 3,6 m do 9,15 m. W celu poprawy estetyki masywnych obramowań są proponowane następujące wykończenia: szkło, szkło pokryte sitodrukiem, kamień, stal, beton, drewno i malowanie określoną gamą kolorów. Szerzej na ten temat zob. *Sliding High Security Crash Rated Gates*, Delta Scientific Corporation, https://deltascientific.com/high-security/sliding-gates/ [dostęp: 28 V 2023].

– **opuszczane szlabany**, montowane na stałe bądź czasowo, jako np. przenośne instalacje, które mogą zmieniać swoją lokalizację[30].

Środki bezpieczeństwa zastosowane w ambasadach wybudowanych bądź zmodernizowanych w Europie na przełomie XX i XXI wieku

Na potrzeby badań aspektu bezpieczeństwa budynków ambasad przeprowadzono analizę materiałów źródłowych i badania terenowe oraz fotograficzne 22 wybranych obiektów zlokalizowanych w Warszawie, Berlinie i Rzymie.

W pobliżu realizacji oprócz wzmocnionej ochrony terenu i masywnych, statycznych zapór drogowych można zauważyć patrole oraz stałe budki obserwacyjne, zgodne z regulacjami prawnymi konwencji wiedeńskiej dotyczącymi zapewnienia odpowiedniego poziomu ochrony i bezpieczeństwa placówkom dyplomatycznym oraz konsularnym. Przykładem jest Ambasada Stanów Zjednoczonych w Atenach (zdjęcie 12).

Zdjęcie 12. Zabezpieczenia strefowe w postaci statycznych zapór drogowych, wysokiego ogrodzenia, stałej budki strażniczej dla służb porządkowych i patrolu drogowego przed Ambasadą Stanów Zjednoczonych w Atenach.

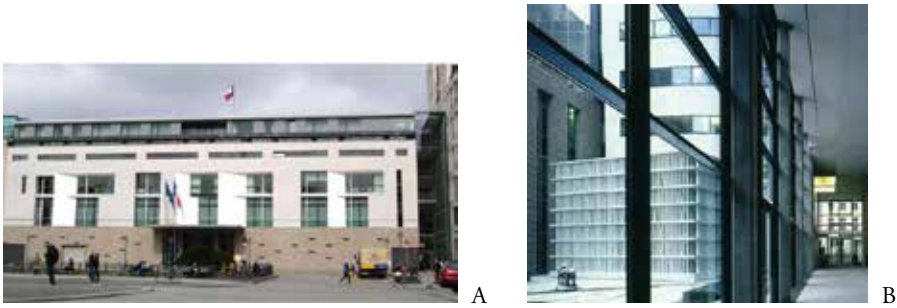
Źródło: własność autorki.

[30] Sterowanie urządzeniem występuje w dwóch wersjach: ręcznej i hydraulicznej. Urządzenie nie wymaga ani kotwienia, ani fundamentowania, dzięki czemu jest możliwe jego szybkie i sprawne przeniesienie. Zob. szerzej: *P500 High Security Portable Barriers*, Delta Scientific Corporation, http://www.deltascientific.com/high-security/portable-barriers/ip500 [dostęp: 28 V 2023].

Skutkiem ataku z 11 września 2001 r. na bliźniacze wieże WTC w Nowym Jorku było zaniechanie prób pełnej integracji ambasad z przestrzeniami miejskimi stolic państw przyjmujących[31]. Przykładem rezygnacji ze wstępnych założeń otwartości jest Ambasada Republiki Francuskiej w Berlinie, zlokalizowana przy Pariser Platz 5 (zdjęcie 13). Jest to zwarty obiekt usytuowany w pierzei placu i ulicy, z wewnętrznymi dziedzińcami, bez ogrodzenia. W zachodniej części głównej fasady, bezpośrednio przy ścianie budynku sąsiadującego z placówką, znajduje się Rue publice – dwukondygnacyjny wewnętrzny pasaż pieszy, szeroki na 5 m, przeszklony i wybrukowany. Ma on kształt litery L i łączy przestrzenie publiczne od stron Wilhelmstraße i Pariser Platz. Pasaż, z założenia otwarty i ogólnodostępny, miał być formą zaproszenia przechodniów do środka ambasady, ale w wyniku wzmożonych ataków terrorystycznych w pierwszych latach XXI w. pasaż już na etapie realizacji zamknięto dla ogółu ze względów bezpieczeństwa[32].

[31] Z wyłączeniem amerykańskich realizacji, których relokacja i modyfikacja kształtowania została zdefiniowana w latach 80. i 90. XX w. Świadczą o tym raporty Inmana i Cowe'a.
Inman Report (pol. Raport Inmana) – raport z 1985 r. przedstawiający zakres i wymiar problemów związanych z bezpieczeństwem amerykańskich zagranicznych misji dyplomatycznych i wskazujący elementy pozwalające zapewnić odpowiedni poziom bezpieczeństwa oraz ochrony osób pracujących w tych placówkach lub odwiedzających je. Raport jest dostępny na stronie internetowej Federation of American Scientists (pol. Federacja Naukowców Amerykańskich), zajmującej sie analizą naukową i poszukiwaniem rozwiązań dotyczących m.in. ochrony przed zagrożeniami dla bezpieczeństwa krajowego i międzynarodowego. Zob. *Report of the Secretary of State's. Advisory Panel on Overseas Security,* http://www.fas.org/irp/threat/inman/ [dostęp: 5 VII 2023]; J.C. Barker, *The Protection of Diplomatic Personnel,* University of Sussex 2006, s. 9–10.
The Crowe Report on embassy security (pol. Raport Crowe'a dotyczący bezpieczeństwa ambasad amerykańskich) – raport Departamentu Rządowego sporządzony pod przewodnictwem admirała Wiliama J. Crowe'a. Raport zakładał wprowadzenie 10-letniego rządowego programu budowy obiektów dyplomatycznych, zabezpieczenia misji i pracowników w amerykańskich ambasadach na całym świecie. Prognozowany roczny koszt przedsięwzięcia wynosił 1,4 bln dolarów amerykańskich. Zob. J.C. Loeffler, *Embassy design: security vs. openness,* „Foreign Service Journal", September 2005, s. 44–51.

[32] K. Englert, J. Tietz, *Botschaften in Berlin*, Berlin 2004, s. 130–131; S. Redecke, *Der Weg zum Licht – Französische Botschaft am Pariser Platz in Berlin*, „Bauwelt" 2003, nr 10, s. 12–19; P. Ulrich, *Die franzoesische Vertretung am Pariser Platz will trotz hoher Sicherheitsanforderungen ein offenes Haus sein: Bald bietet die Botschaft Fuehrungen durch das neue Gebaeude,* „Berliner Zeitung", 24 I 2003 r.



A B

Zdjęcie 13. Fasada frontowa Ambasady Republiki Francuskiej w Berlinie od strony Pariser Platz (A), wnętrze pasażu Rue publice i dziedziniec z widoczną rzeźbą (B).

Źródło: zdjęcie 13A – własność autorki; 13B – S. Redecke, *Der Weg zum Licht – Französische Botschaft am Pariser Platz in Berlin*, „Bauwelt" 2003, nr 10, s. 14.

Niektóre realizacje ambasad w swoim programie nie uwzględniają rozwiniętej struktury zabezpieczeń. Przykładem może być wolnostojąca Ambasada Republiki Włoskiej w Berlinie (zdjęcie 14). Budynek powstawał w latach 1938–1942, a w latach 1999–2003 zabytkowy obiekt przebudowano. Ambasada jest zlokalizowana na działce o kształcie trapezu. Budynek trzyskrzydłowy, rozwiązany na planie litery U, od zachodu został domknięty dwukondygnacyjnym portykiem. Frontowa część budynku nie jest w żaden sposób odseparowana od przestrzeni publicznej, podobnie jak zachodnia i wschodnia elewacja. Jedyny widoczny element zabezpieczenia to monitoring.

Zdjęcie 14. Fasada frontowa Ambasady Republiki Włoskiej w Berlinie.

Źródło: własność autorki.

Projektowanie budynków pod kątem zapewnienia odpowiedniego poziomu bezpieczeństwa powinno pozostawać w równowadze z pozostałymi istotnymi aspektami, m.in. z estetyką, prestiżem, dostępnością, funkcjonalnością, zużyciem technicznym, oddziaływaniem obiektu na środowisko czy wykorzystaniem odnawialnych źródeł energii. Stosowane w projektach i realizacjach środki zaradcze powinny być zintegrowane z innymi elementami założenia, tak aby stworzyły przyjazne środowisko pracy i były pozytywnie odbierane przez użytkowników obiektów dyplomatycznych i mieszkańców stolicy. Odpowiednie ukształtowanie zarówno działek, na których są zlokalizowane ambasady, jak i przyległego do nich otoczenia może zapobiec zbliżeniu się zagrożenia do ścian budynku. Nie wszystkie działki budowlane i obiekty można zabezpieczyć w obrębie zajmowanego przez nie terenu. Dostępne publikacje poświęcone zabezpieczeniom budynków rekomendują zachowanie stref bezpieczeństwa pomiędzy budynkiem a ogrodzeniem lub granicą działki. Jeżeli rozpatrywany jest obszar poza miastem lub na jego obrzeżach, wymóg dotyczący utrzymania dystansu zazwyczaj nie stwarza trudności. Inaczej wygląda to w przypadku zabudowy śródmiejskiej, w której – ze względu na intensywną zabudowę – są stosowane rozwiązania zamienne, np. wyłączanie fragmentów ulic lub chodników użytkowanych jako przestrzenie publiczne, czego przykładem jest Ambasada Wielkiej Brytanii w Berlinie (zdjęcie 15), gdzie fragmentarycznie, za pomocą barier drogowych, wyłączono z ruchu kołowego odcinek Wilhelmstraße i zapewniono tym samym dostęp do budynku wyłącznie pojazdom uprawnionym.

Zdjęcie 15. Wyłączenie za pomocą barier strefowych fragmentu Wilhelmstraße przed Ambasadą Wielkiej Brytanii w Berlinie. Widok od Behrenstraße.

Źródło: własność autorki.

W tabeli przedstawiono wyniki analizy zabezpieczeń strefowych 22 ambasad znajdujących się w Warszawie, Berlinie i Rzymie. We wszystkich badanych obiektach występują pasywne zabezpieczenia strefowe nieruchomości w postaci kontroli dostępu do obiektu, monitoringu wewnętrznego i zewnętrznego. W przypadku 68% placówek w obrębie ogrodzenia bądź bezpośrednio przy strefie wejściowej do budynku znajdują się dodatkowe strażnice z punktem ochrony. Połowa rozpatrywanych stałych misji dyplomatycznych w swoim zagospodarowaniu terenu lub obszarów przyległych do ich działek wykorzystuje elementy stałych zapór drogowych w postaci pachołków bądź słupków. Ponad 3/4 badanych ambasad (77%) jest całkowicie lub fragmentarycznie odizolowanych od przestrzeni i działek sąsiednich za pomocą ogrodzenia.

Aktywne elementy zabezpieczeń strefowych zapór drogowych służących zablokowaniu wjazdu pojazdom nieuprawnionym (tarcze) zostały wykorzystane tylko w 9% przypadków. W 27% obiektów zastosowano ruchome zapory w postaci słupków lub pachołków, w 54% wykorzystano masywne, wzmocnione bramy wjazdowe, a podwójne bariery drogowe wystąpiły w trzech realizacjach (14%). W przypadku 27% placówek zostały podwojone zarówno strefy wejściowe w obrębie ogrodzenia, jak i bramy wjazdowe na teren ambasady. W ten sposób powstały śluzy zapewniające kontrolę wejść i wjazdów, ponieważ w razie przekroczenia przez osoby lub pojazdy niepożądane pierwszej strefy z elementami zabezpieczającymi służby mają możliwość blokady tego odcinka i uniemożliwienia dalszego dostępu.

Tabela. Charakterystyka zabezpieczeń w ambasadach – zabezpieczenia strefowe: pasywne i aktywne.

Lp.	Ambasada	Miasto	Zabezpieczenia budynku/zespołu budynków ambasady										
			Pasywne elementy zabezpieczeń strefowych						Aktywne elementy zabezpieczeń strefowych				
			Kontrola dostępu	Strażnica/-e z punktem ochrony	Monitoring zewnętrzny	Monitoring wewnętrzny	Zapory drogowe (stałe słupki)	Ogrodzenie	Hydrauliczne zapory drogowe (tarcze)	Hydrauliczne zapory drogowe (słupki)	Podwójne bariery drogowe	Masywne, wzmocnione bramy wjazdowe	Podwójne strefy wejściowe i wjazdowe (śluzy)
1.	Republiki Francuskiej	Warszawa	•	•	•	•	•	•	–	–	–	•	–
2.		Berlin	•	–	•	•	–	–	–	–	–	–	–

3.	Królestwa Niderlandów	Warszawa	•	•	•	•	–	•	–	–	–	–	–
4.		Berlin	•	•	•	•	•	–	–	•	–	–	–
5.		Rzym	•	•	•	•	–	•	–	–	–	•	–
6.	Wielkiej Brytanii	Warszawa	•	•	•	•	•	•	–	•	–	•	•
7.		Berlin	•	•	•	•	•	–	–	•	•	•	•
8.	Ambasady krajów skandynawskich	Berlin	•	–	•	•	•	•	–	–	–	–	–
9.	Japonii	Warszawa	•	•	•	•	–	•	•	–	–	•	•
10.		Berlin	•	•	•	•	–	•	•	–	–	•	•
11.	Korei Południowej	Warszawa	•	•	•	•	–	•	–	–	–	•	–
12.	Stanów Zjednoczonych	Berlin	•	–	•	•	•	•*	–	•	•	–	•
13.	Konfederacji Szwajcarskiej	Berlin	•	•	•	•	–	•	–	–	–	–	–
14.	Kanady	Warszawa	•	•	•	•	•	•	–	–	–	•	–
15.		Berlin	•	–	•	•	•	–	–	•	–	–	–
16.	Republiki Federalnej Niemiec	Warszawa	•	•	•	•	•	•	–	–	–	•	•
17.	Królestwa Hiszpanii	Warszawa	•	•	•	•	•	•	–	–	–	•	–
18.	Meksykańskich Stanów Zjednoczonych	Berlin	•	–	•	•	–	•*	–	–	–	–	–
19.	Republiki Indii	Berlin	•	•	•	•	–	•	–	–	–	•	–
20.	Republiki Turcji	Berlin	•	•	•	•	•	•	–	•	•	•	–
21.	Republiki Południowej Afryki	Berlin	•	–	•	•	–	•	–	–	–	–	–
22.	Królestwa Belgii	Berlin	•	–	•	•	–	–	–	–	–	–	–
Stosunek procentowy			100%	68%	100%	100%	50%	77%	9%	27%	14%	54%	27%
Legenda: • element występuje, •* element występuje fragmentarycznie, – brak													

Źródło: opracowanie własne.

Ze względu na zwiększone prawdopodobieństwo ataku na ambasady nie można pominąć także konieczności zapewnienia bezpieczeństwa na terenie placówki. Osoby fizyczne mogą wnieść niebezpieczny element bezpośrednio do obiektu. Aby umożliwić szybką reakcję na potencjalne niebezpieczeństwo, w wielu placówkach zabrania się wnoszenia plecaków, toreb, urządzeń elektronicznych, tj. komputerów, aparatów fotograficznych czy

telefonów komórkowych. Muszą one zostać zdeponowane w punkcie kontroli i po wizycie są oddawane interesantowi.

Ochrona stałych misji dyplomatycznych jest niezmiernie istotna i często skomplikowana. Proces wprowadzania zabezpieczeń musi przebiegać równolegle z następującymi po sobie etapami projektowania. Zastosowanie dostępnych metod pozwala na spójną realizację inwestycji i zagospodarowanie przyległego do niej otoczenia. Producenci barier izolacyjnych są w stanie dopasować katalogowe rozwiązania do skonkretyzowanych, indywidualnych zamówień. Zastosowanie elementów asekuracyjnych w postaci wzmocnionych elementów małej architektury i odpowiednio ukształtowanej rzeźby terenu oprócz tego, że poprawia estetykę, stanowi także utrudnienie dla potencjalnych napastników.

Podsumowanie

We współczesnych opracowaniach dotyczących *security by design* i ochrony przestrzeni publicznej jest podkreślana konieczność stosowania koncepcji bezpieczeństwa już na początkowym etapie projektowania czy też modernizowania przestrzeni miejskich, z uwzględnieniem np. reorganizacji rozwiązań urbanistyczno-komunikacyjnych w sąsiedztwie obszarów lub obiektów narażonych na potencjalne ataki terrorystyczne. Należy także skupić się na projektowaniu zintegrowanym, w myśl zrównoważonego rozwoju i w zgodzie z założeniami Nowego Europejskiego Bauhausu, czyli projektowaniu z naciskiem na bezpieczeństwo, inkluzywność, jakość i łatwość życia, dostępność dla użytkowników oraz wprowadzaniu atrakcyjnych i funkcjonalnych rozwiązań[33]. Trzeba pamiętać także o wykorzystywaniu elementów mogących pozytywnie wpłynąć na minimalizację zmian klimatycznych. Te warunki powinny być spełnione w każdej z sześciu kategorii przestrzeni publicznych sklasyfikowanych przez KE. Misje dyplomatyczne należą do przestrzeni rządowej[34].

Do czterech najważniejszych aspektów koncepcji projektowania bezpiecznych przestrzeni publicznych należy zaliczyć: wielofunkcyjność, proporcjonalność, estetykę i współpracę ze stronami, które mogą mieć wpływ

[33] Zob. szerzej: https://new-european-bauhaus.europa.eu/index_en [dostęp: 5 VII 2023].

[34] Zgodnie z klasyfikacją stosowaną przez KE wyróżnia się następujące kategorie przestrzeni publicznej: rekreacyjną, komercyjną, publiczną, religijną, komunikacyjną, rządową. Zob. *Security by Design: Protection...*, s. 19–29, 38–39.

na proponowane rozwiązania lub na które będą one oddziaływać. Komisja Europejska podkreśla konieczność stosowania niezbędnych środków ochrony, przy czym zgodnie z założeniami koncepcji „niewidzialnego bezpieczeństwa" formy ochrony powinny stanowić elementy małej architektury i inżynierii miejskiej, które są zintegrowane z otoczeniem i nie sprawiają wrażenia fortyfikacji[35]. Uwzględnienie powyższych aspektów oraz zaangażowanie interdyscyplinarnego zespołu projektowego składającego się ze specjalistów i zainteresowanych stron włączonych w proces projektowy pozwolą na wdrożenie w odpowiednim czasie właściwych, skutecznych i estetycznych rozwiązań realizacyjnych.

Zapewnieniu odpowiedniego poziomu bezpieczeństwa ambasad służy szeroka gama środków. W obrębie budynku są wykorzystywane najnowocześniejsza technologia, systemy zintegrowanego monitoringu i alarmu antywłamaniowego, urządzenia kontroli dostępu, czujniki ruchu, folie ochronne na szkło, wzmocnienia konstrukcji budynku, zabezpieczenia wentylacji (zabezpieczenie wszystkich wlotów i wylotów z budynku, tj. wyrzutnie i czerpnie, w celu uniknięcia umieszczenia w nich elementów stanowiących zagrożenie), a także fizyczne aktywne i pasywne elementy ochrony strefowej oraz widoki z satelit. Wszystkie te środki mają na celu ochronę przed potencjalnymi atakami terrorystycznymi i zapobieganie im[36]. Jednak coraz większa pomysłowość grup przestępczych i istniejąca obecnie intensyfikacja zamachów dokonywanych przy użyciu różnego rodzaju przedmiotów, maszyn bądź urządzeń wymuszają ciągły rozwój rozwiązań służących zwiększaniu poziomu bezpieczeństwa.

Bezpieczeństwo na terenie działki i ambasady jest zapewniane przede wszystkim przez ogrodzenie, odseparowujące przestrzeń placówki od sąsiednich terenów, oraz punkty kontroli, gdzie petenci i goście są legitymowani, a ich rzeczy oraz pojazdy – sprawdzane (prześwietlane). W zależności od potrzeb inwestorów punkty kontroli mogą znajdować się w linii ogrodzenia zewnętrznego, w budynku lub w obu tych miejscach. Punkty kontroli w obrębie ogrodzenia mogą być wspólne dla kilku miejsc (np. osobne punkty kontroli do części konsularnej, rezydencji i kancelarii) lub indywidualne dla każdego z nich. Pierwsze rozwiązanie wiąże się z potrzebą oszczędności, a co za tym idzie – ograniczeniem liczby budynków strażniczych

[35] A. Jasiński, *Koncepcja „niewidzialnego bezpieczeństwa" stosowana w zabezpieczeniu antyterrorystycznym amerykańskich miast metropolitalnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 5, s. 99–115.

[36] *Reference Manual to Mitigate*..., s. viii–ix.

i strażników. We współczesnych realizacjach bądź modernizacjach ambasad zdarzają się przypadki, gdy w ich rozwiązaniach nie występuje ani ogrodzenie, ani zewnętrzny punkt kontroli dostępu. Uzupełnieniem kontroli bezpieczeństwa są zarówno monitoring działki, jak i elementy małej architektury, nasadzenia roślinne oraz inne elementy krajobrazu (cieki wodne, głazy, pagórki). W pobliżu europejskich realizacji oprócz wzmocnionej ochrony terenu i masywnych, statycznych zapór drogowych można zaobserwować patrole oraz stałe budki obserwacyjne, zgodne z regulacjami prawnymi konwencji wiedeńskiej dotyczącymi zapewnienia odpowiedniego poziomu ochrony i bezpieczeństwa placówkom dyplomatycznym oraz konsularnym. Przy ważnych inwestycjach coraz częściej rezygnuje się z lokalizacji parkingów czy garaży w obrębie budynków, ponieważ stanowią one łatwe miejsca detonacji ładunku wybuchowego. Zaleca się lokalizowanie miejsc postojowych poza obrysem budynku. Jeśli nie jest to możliwe, miejsca w jego obrębie powinny być przeznaczone wyłącznie dla określonej grupy pojazdów (należących do pracowników i osób uprzywilejowanych).

Przy omawianiu sposobów zabezpieczeń nie można pominąć konieczności zapewnienia bezpieczeństwa na terenie placówki, gdzie może dojść do wniesienia niebezpiecznego elementu bezpośrednio do obiektu przez osoby fizyczne (broń, ładunek). Punkty kontroli dostępu najczęściej znajdują się przed strefami wejściowymi. W ich obrębie następuje monitorowanie, kontrolowanie, sprawdzanie i legitymowanie osób, pojazdów oraz przesyłek przed wejściem lub wjazdem na teren placówki. Nadzór i zasady dostępu są regulowane przede wszystkim przez wewnątrzpaństwowe procedury i współczesne wymagania dotyczące bezpieczeństwa. Zazwyczaj stosuje się mechaniczne i elektroniczne systemy kontroli dostępu, tj. nadzór wizyjny – kamery (system CCTV, z ang. *Closed-Circuit TeleVision*), kołowroty wejściowe, niskie bramki obrotowe (tripody) lub sensoryczne, bramki do wykrywania metali, przejścia z zamkami wymagającymi kodów numerycznych (PIN) lub kart dostępu (zbliżeniowych, chipowych, magnetycznych) i skanery RTG do kontroli bagażu i paczek.

Zróżnicowanie przeznaczenia nieruchomości sąsiadujących z budynkami dyplomatycznymi w Europie pozwoliło na integrację terenów o różnych funkcjach, a w niektórych przypadkach wzmogło zainteresowanie nimi zarówno ze strony lokalnej społeczności, jak i turystów. Dlatego też stosowane umocnienia form przestrzennych budynków i terenów przyległych do ambasad nie powinny w istotny sposób wpływać na estetykę

obiektów. Wykorzystanie elementów małej architektury i odpowiednio ukształtowanej rzeźby terenu nie tylko poprawia wygląd, lecz także stanowi dodatkową trudność dla potencjalnych napastników. Należy oczywiście przypomnieć, że środki bezpieczeństwa stosowane zarówno na terenie, jak i w budynkach ambasad mogą znacznie się różnić w zależności od kraju wysyłającego, wzajemnych stosunków z państwem przyjmującym oraz ich wewnętrznych regulacji, zasobów finansowych inwestora i lokalizacji obiektu. Współcześnie występują realizacje ambasad zlokalizowane w obrębie fragmentu, pięter lub piętra budynku o innym przeznaczeniu, co znacznie utrudnia wprowadzenie przedstawionych zabezpieczeń i zapewnienie odpowiedniego poziomu bezpieczeństwa.

Bibliografia

Barker J.C., *The Protection of Diplomatic Personnel*, University of Sussex 2006.

Cormie D., Mays G., Smith P., *Blast effects on buildings*, London 2009.

van Egeraat E., Stiasny G., *Ambasada Królestwa Niderlandów*, „Architektura–Murator" 2004, nr 2, s. 25–37.

Encyklopedia, t. 9, Warszawa 2001.

Englert K., Tietz J., *Botschaften in Berlin*, Berlin 2004.

Fretton T., Stiasny G., *Ambasada Wielkiej Brytanii w Warszawie*, „Architektura–Murator" 2009, nr 12, s. 56–63.

Gadomska B., *Ambasada Izraela w Berlinie*, „Architektura–Murator" 2002, nr 2, s. 16–19.

Gorczyński W., *Ambasada Kanady w Warszawie*, „Architektura–Murator" 2002, nr 2, s. 9–15.

Jasiński A., *Architektura w czasach terroryzmu. Miasto–przestrzeń publiczna–budynek*, Warszawa 2013.

Jasiński A., *Koncepcja „niewidzialnego bezpieczeństwa" stosowana w zabezpieczeniu antyterrorystycznym amerykańskich miast metropolitalnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 5, s. 99–115.

Jasiński A., *Wpływ zabezpieczeń antyterrorystycznych na architekturę współczesnych ambasad amerykańskich*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 97–114.

Jootsen H., Stępniowska A., *Ambasada Niemiec w Warszawie*, „Architektura–Murator" 2009, nr 12, s. 48–55.

Leśniakowska M., *Architektura polskich ambasad*, „Architektura–Murator" 2004, nr 2, s. 60–62.

Loeffler J.C., *Embassy design: security vs. openness*, „Foreign Service Journal", September 2005, s. 44–51.

Majewski K., Sroka-Strzeszyńska M., *Ambasada Korei Południowej*, „Architektura–Murator" 2004, nr 2, s. 38–41.

Pagarde J.P., Stiasny G., *Ambasada Francji w Warszawie*, „Architektura–Murator" 2005, nr 2, s. 30.

Redecke S., *Der Weg zum Licht – Französische Botschaft am Pariser Platz in Berlin*, „Bauwelt" 2003, nr 10, s. 12–19.

Rzechowski K., *Polskie placówki dyplomatyczne*, „Architektura–Murator" 2004, nr 2, s. 63–70.

Sitko A., Szafarczyk S., *Technologie architektury – Ambasada Królestwa Niderlandów w Warszawie*, „Architektura–Murator" 2004, nr 2, s. 90–97.

Stiasny G., *Konkursy na nowe budynki ambasad w Warszawie*, „Architektura–Murator" 2004, nr 2, s. 44–59.

Ulrich P., *Die franzoesische Vertretung am Pariser Platz will trotz hoher Sicherheitsanforderungen ein offenes Haus sein: Bald bietet die Botschaft Fuehrungen durch das neue Gebaeude*, „Berliner Zeitung", 24 I 2003 r.

Źródła internetowe

DSC1100 K8 Portable Barriers, Delta Scientific Corporation, https://deltascientific.com/product/portable-barrier-dsc1100/ [dostęp: 28 V 2023].

Embassy Perimeter Improvement Concepts & Design Guidelines, Department of State Bureau of Overseas Buildings Operations, czerwiec 2011 r., https://www.scribd.com/document/261408078/Embassy-Perimeter-Improvement-Concepts-Design-Guidelines [dostęp: 12 V 2023].

Encyklopedia humanistyczna, http://encenc.pl/aha/ [dostęp: 14 V 2023].

High Security Bollards, Delta Scientific Corporation, http://deltascientific.com/high-security/bollards/ [dostęp: 28 V 2023].

https://deltascientific.com/wp-content/uploads/2021/01/90140-Rev-B-DSC207S-General-Arrangement.pdf [dostęp: 9 I 2023].

https://new-european-bauhaus.europa.eu/index_en [dostęp: 5 VII 2023].

http://www.google.pl/maps/ [dostęp: 10 III 2015].

http://www.rogersmarvel.com/projects/NYSE/ [dostęp: 28 V 2023].

IP500 High Security Portable Barriers, Delta Scientific Corporation, http://www.deltascientific.com/high-security/portable-barriers/ip500 [dostęp: 28 V 2023].

Kades A., *Cypriot embassy severely damaged in Athens bomb blast*, CyprusMail, 24 XI 2015 r., http://cyprus-mail.com/2015/11/24/cypriot-embassns-bomb-attack/ [dostęp: 24 XI 2015].

Komisja Europejska, *Security by Design: Protection of public spaces from terrorist attacks*, https://www.urbanagenda.urban-initiative.eu/news/security-design-protection-public-spaces-terrorist-attacks [dostęp: 20 IV 2023].

Oakes Ch.G., *The Bollard: Crash- and Attack-Resistant Models*, Whole Building Design Guide, 9 II 2016 r., https://www.wbdg.org/resources/bollard-non-crash-and-non-attack-resistant-models [dostęp: 9 I 2023].

Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, seria: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema427.pdf [dostęp: 30 V 2023].

Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, seria: Buil dings and Infrastructure Protection Series, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [dostęp: 16 V 2023].

Report of the Secretary of State's. Advisory Panel on Overseas Security, http://www.fas.org/irp/threat/inman/ [dostęp: 5 VII 2023].

Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks, seria: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [dostęp: 13 V 2023].

Sliding High Security Crash Rated Gates, Delta Scientific Corporation, https://deltascientific.com/high-security/sliding-gates/ [dostęp: 28 V 2023].

U.S. Embassy security upgrades in Baku, Pernix Group, https://www.pernixgroup.com/project/baku-design-build-isat-security-upgrades/ [dostęp: 10 I 2023].

Akty prawne

Konwencja wiedeńska o stosunkach dyplomatycznych, sporządzona w Wiedniu dnia 18 kwietnia 1961 r. (DzU z 1965 r. nr 37 poz. 232).

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0795&from=PL [dostęp: 5 VII 2023].

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

Dr inż. Agnieszka Dobrzyńska-Jarosz

Architekt, adiunkt w Katedrze Architektury Użyteczności Publicznej, Podstaw Projektowania i Kształtowania Środowiska Wydziału Architektury Politechniki Wrocławskiej, członek Dolnośląskiej Okręgowej Izby Architektów RP.

https://doi.org/10.4467/27204383TER.23.020.18322
https://orcid.org/0000-0003-0949-6674

ANDRZEJ JARYNOWSKI

Agroterroryzm z wykorzystaniem czynników biologicznych i zagrożenia z nim związane w Polsce i Europie w kontekście pandemii COVID-19 i wojny w Ukrainie

Abstrakt

W związku z rosnącym zagrożeniem agroterrorystycznym i najwyższym poziomem jego ryzyka w Polsce oraz regionie europejskim od czasu wejścia w życie konwencji o zakazie broni biologicznej i toksycznej (1972 r.), a także protokołów dodatkowych do konwencji genewskich (1977 r.) istotne znaczenie ma analiza wyzwań w obszarze bezpieczeństwa biologicznego i żywnościowego oraz przedstawianie rekomendacji. Analiza przeprowadzona przez autora artykułu wskazuje, że pandemia COVID-19 przyczyniła się do upowszechnienia wiedzy na temat podstaw mikrobiologii i epidemiologii oraz do zwiększenia dostępności do taniej, przenośnej diagnostyki mikrobiologicznej, co może mieć również skutki negatywne. W analizie została uwzględniona możliwość wpływu obcego wywiadu na produkcję żywności w Polsce, np. za pomocą dezinformacji prowadzonej w mediach społecznościowych. Wnioski płynące z tej analizy obejmują: rozszerzenie monitorowania środowisk specjalistów oraz mediów społecznościowych, wzmocnienie czujności producentów żywności i ekspertów rolniczych, przeprowadzenie symulacji scenariuszy introdukcji, badanie procesów radykalizacji oraz wykorzystanie narzędzi oceny epidemiologicznej w przypadku wystąpienia niepokojących zdarzeń.

Słowa kluczowe:

agroterroryzm, bioterroryzm, bezpieczeństwo żywnościowe, biopolityka, INFOOPS

Żadne z wydarzeń w XXI w. nie zmieniło życia społecznego w Europie tak bardzo jak pandemia COVID-19[1] oraz wojna w Ukrainie[2]. Rozprzestrzenienie się wirusa SARS-CoV-2 sprawiło, że mikrobiologia i epidemiologia stały się na pewien czas jednym z dominujących tematów interesujących dużą część społeczeństwa. W trakcie pandemii COVID-19 dyskurs publiczny dotyczył głównie wirusów ludzkich, ale pozyskana wiedza może być ekstrapolowana na zakażenia wywoływane przez inne drobnoustroje chorobotwórcze.

Wojna Rosji przeciwko Ukrainie oraz rosnące ceny nawozów powodują, że pogłębia się światowy kryzys żywnościowy[3]. Rosja, dążąc m.in. do osłabienia zdolności Ukrainy do eksportu produktów rolno-spożywczych, zaatakowała tamtejszą infrastrukturę transportową i de facto zablokowała porty na Morzu Czarnym od końca lutego do końca lipca 2022 r. (od sierpnia 2022 r. na podstawie umów krzyżowych za pośrednictwem ONZ i Turcji wywóz produktów zbożowych z ukraińskich portów został wznowiony[4]).

Osią artykułu są następujące pytania[5]:

1. Jaki wpływ na zjawisko agroterrozymu miały pandemia COVID-19 i wojna w Ukrainie?
2. Jakie korzyści mogą osiągnąć potencjalni terroryści za pomocą bio- i agroterroryzmu w warunkach wojny hybrydowej?
3. Na ile dotychczasowa bariera w postaci posiadania wiedzy na temat mikrobiologii i epidemiologii, epizootii, roślin epifitycznych oraz dysponowania sprzętem laboratoryjnym i określonymi umiejętnościami, ograniczająca w pewnym stopniu możliwości

---

1 A. Jarynowski, M. Stochmal, J. Maciejewski, *Przegląd i charakterystyka prowadzonych w Polsce badań na temat społecznych uwarunkowań epidemii COVID-19 w jej początkowej fazie*, „Bezpieczeństwo. Obronność. Socjologia" 2020, t. 13, s. 38–87.

2 J. Maciejewski, *Grupy dyspozycyjne w systemie bezpieczeństwa państwa*, XXIII Międzynarodowe Seminarium z cyklu „Metodologia badań systemów społecznych", Wrocław, 7 IV 2022 r.

3 B. Radziejewski, *Widmo krąży po świecie. Widmo głodu*, Nowa Konfederacja, 25 V 2022 r., https://nowakonfederacja.pl/widmo-krazy-po-swiecie-widmo-glodu/ [dostęp: 12 VIII 2022].

4 *Black Sea Grain Initiative*, Wikipedia, https://en.wikipedia.org/wiki/Black_Sea_Grain_Initiative [dostęp: 12 VIII 2022].

5 Artykuł stanowi kontynuację tez zawartych w referacie pt. *(Re-)Emergence of agroterrorism during the food crisis*, zaprezentowanym przez autora 20 VII 2022 r. dla NATO Centre of Excellence for Military Medicine, oraz prezentacji pt. *Agro/bio-terrorism in Europe? Analysis of selected suspicious biological events (significant from the One Health perspective) after 24.02.2022*, wygłoszonej 25 X 2022 r. podczas NATO BioMed Panel.

podejmowania działań bio- i agroterrorystycznych, została obniżona dla potencjalnych terrorystów, takich jak samotne wilki i małe organizacje?
4. Kto (przez kogo inspirowany), w jaki sposób i kiedy mógłby dokonać aktu agroterroryzmu w Polsce i w regionie europejskim oraz jakie byłyby tego skutki?
5. W jaki sposób dezinformacja dotycząca broni biologicznej, bezpieczeństwa żywnościowego i pandemii COVID-19 może wpływać na społeczeństwo?
6. Jakie obszary zainteresowania związane z bronią biologiczną i bezpieczeństwem biologicznym są najważniejsze w obliczu współczesnych zagrożeń?

Agroterroryzm a bioterroryzm

Pojęcie agroterroryzmu[6] oznacza nie tylko atak biologiczny na produkcję zwierzęcą i roślinną (ten wymiar zawiera się w szeroko pojętym bioterroryzmie), lecz także atak na środki transportu i przewozu, infrastrukturę, środki produkcji rolnej, jak również wywieranie negatywnego wpływu na społeczne uwarunkowania produkcji (inne działanie kryminalne lub terrorystyczne typu żywnościowego). Agroterroryzm może obejmować użycie środków biologicznych, mechanicznych, chemicznych czy informatycznych, ale na potrzeby niniejszego artykułu zostaną omówione jedynie czynniki biologiczne (wraz z działaniami pomocniczymi).

Działania o charakterze agroterrorystycznym mogą być prowadzone przez różne podmioty. Ze względu na możliwość wykrycia można je podzielić na:

- działania na małą skalę prowadzone przez niewielkie organizacje terrorystyczne (np. organizacje ekologiczne czy religijne), które nie muszą się liczyć z wykryciem;
- działania hybrydowe poniżej progu (czyli działania, w których mechanizmy ochronne nie zostaną skutecznie wdrożone) konwencji o zakazie broni biologicznej i toksycznej z 1972 r. (ang. *Biological*

[6] H. Keremidis i in., *Historical Perspective on Agroterrorism: Lessons Learned from 1945 to 2012*, „Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science" 2013, t. 11, s. 17–24. https://doi.org/10.1089/bsp.2012.0080.

and Toxin Weapons Convention, BTWC[7]) i protokołów dodatkowych z 1977 r. do konwencji genewskich (o ochronie ofiar międzynarodowych konfliktów zbrojnych[8]) podejmowane przez państwa (np. ataki na łańcuchy dostaw lub polaryzowanie producentów żywności) lub utrudnianie przez agresorów udowodnienia aktu terroryzmu. W tych przypadkach dużo większą wagę przykłada się do ukrycia rzeczywistego mocodawcy.

Wspomniane akty prawne są obecnie dwoma podstawowymi unormowaniami międzynarodowymi odnoszącymi się do zjawiska agroterroryzmu. Zgodnie z art. 1 konwencji o zakazie broni biologicznej: *Każde Państwo-Strona* (...) *zobowiązuje się, że nigdy, w żadnych okolicznościach nie będzie prowadzić badań, produkować, gromadzić, nabywać w jakikolwiek inny sposób lub przechowywać: 1) mikrobiologicznych lub innych biologicznych środków czy toksyn, bez względu na pochodzenie lub sposób produkcji, takich rodzajów i w takich ilościach, które nie są przeznaczone do wykorzystania w celach profilaktycznych, ochronnych lub w innych celach pokojowych*. Warto wspomnieć, że 8 lipca 2022 r. państwa-strony konwencji o zakazie broni biologicznej zostały powiadomione, że Rosja uruchomiła art. 5 tej konwencji, zobowiązujący strony do współpracy ze sobą w rozstrzyganiu trudności, które mogą pojawić się w związku z celem lub stosowaniem konwencji, i wezwała do formalnego spotkania konsultacyjnego[9]. Odbyło się ono w dniach 1–5 września 2022 r. (był to drugi raz w historii, po sprawie Kuba vs USA z 1997 r.).

Artykuł 54 Protokołu I oraz art. 14 Protokołu II do konwencji genewskich dotyczą ochrony dóbr niezbędnych do przetrwania ludności cywilnej. Zgodnie z art. 14: *Zabrania się stosowania wobec ludności cywilnej głodu jako środka walki. Z tego powodu zabronione jest atakowanie, niszczenie, zabieranie lub czynienie niezdatnymi do użytku dóbr niezbędnych dla przetrwania ludności cywilnej, takich jak zapasy żywności, obszary rolnicze, które ją*

[7] *Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu, sporządzona w Moskwie, Londynie i Waszyngtonie dnia 10 kwietnia 1972 r.*

[8] *Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r.*

[9] F. Lentzow, J. Littlewood, *Russia finds another stage for the Ukraine "biolabs" disinformation show*, Bulletin of the Atomic Scientists, 8 VII 2022 r., https://thebulletin.org/2022/07/russia-finds-another-stage-for-the-ukraine-biolabs-disinformation-show/ [dostęp: 12 VIII 2022].

wytwarzają, zbiory, bydło, urządzenia dostarczające wody do picia i jej zapasy oraz urządzenia nawadniające.

Wiadomo, że patogeny wykorzystywane do działań z zakresu agroterroryzmu znajdowały się w arsenale wojsk radzieckich[10] i amerykańskich oraz innych państw[11]. Były używane przed 1972 r., a zatem przed wejściem w życie konwencji o zakazie broni biologicznej (protokół genewski z 1925 r. dotyczył jedynie czynników biologicznych, pośród innych środków oddziałujących w czasie wojny na ludzi[12]), w tym przez państwa, które później przystąpiły do NATO (taka opinia panuje w środowisku epizootiologów i epifitiologów). Na przykład w 1971 r. Stany Zjednoczone najprawdopodobniej celowo wprowadziły na Kubę wirus afrykańskiego pomoru świń (ang. *African Swine Fever Virus*, ASFV)[13], co potwierdzają m.in. ukraińscy uczestnicy radzieckiej epizootiologicznej misji na Kubę[14].

Niepokojące jest to, że pomimo istnienia konwencji o zakazie broni biologicznej nadal co najmniej 18 krajów i terytoriów (Chiny, Francja, Irak, Iran, Izrael, Japonia, Kanada, Korea Północna, Kuba, Libia, Niemcy, Republika Południowej Afryki, Rosja, Stany Zjednoczone, Syria, Tajwan, Wielka Brytania oraz organizacja terrorystyczna tzw. Państwo Islamskie) prawie na pewno posiada taką broń oraz z dużym prawdopodobieństwem, zdaniem Stanisława Maksymowicza, eksperta ds. zdrowia, prowadzi prace nad jej nowymi typami[15]. Nie są do tego potrzebne najdroższe laboratoria o 3 i 4 klasie bezpieczeństwa biologicznego (ang. *Biological Safety Level*, BSL).

---

[10] M. Leitenberg, R.A. Zilinskas, *The Soviet biological weapons program: A history*, Cambridge 2012.

[11] Л.П. Жиганова, *Биотерроризм и агротерроризм – реальная угроза биобезопасности общества*, „США и Канада: экономика, политика, культура" 2004, t. 417, nr 9, s. 3–25. (analiza źródeł rosyjskich wymaga ostrożności z uwagi na obecność propagandy, zwłaszcza w dziedzinie militarnej).

[12] *Protokół dotyczący zakazu używania na wojnie gazów duszących, trujących lub podobnych oraz środków bakterjologicznych.*

[13] Б. Стегній, А. Герилович, А. Бузун, *Африканська чума свиней: історія, сьогодення та перспективи*, Київ 2015.

[14] Komunikacja prywatna autora artykułu z aktualnymi i emerytowanymi pracownikami Instytutu Eksperymentalnej Wirusologii Weterynaryjnej w Charkowie.

[15] S. Maksymowicz, *Atak biologiczny i agroterrorystyczny na Polskę. Jakie scenariusze są prawdopodobne?*, Nowa Konfederacja, 31 V 2022 r., https://nowakonfederacja.pl/atak-biologiczny-i-agroterrorystyczny-na-polske-jakie-scenariusze-sa-prawdopodobne/ [dostęp: 7 XI 2022].

Między bioterroryzmem w wąskim rozumieniu a agroterroryzmem istnieją pewne istotne różnice. Choroby zakaźne można sklasyfikować w zależności od typu gospodarza. W Polsce jest stosowany m.in. podział na[16]:

- żywicieli ludzkich (choroby z tej grupy budzą największe zainteresowanie populacji ogólnej, służb specjalnych oraz środowiska medycznego);
- żywicieli zwierzęcych stanowiących jednocześnie wektory chorób przenoszonych na ludzi (np. wścieklizna, borelioza, ogniska wysoce zjadliwej grypy ptaków występującej u ssaków, ogniska SARS-CoV-2 wśród norek; wzbudzają one umiarkowane zainteresowanie populacji ogólnej, z pewnymi szczytami o lokalnym charakterze; uwagę poświęcają im służby specjalne, środowiska medyczne i weterynaryjne);
- żywicieli zwierzęcych lub roślinnych (choroby dotyczące tych grup żywicieli praktycznie nie wzbudzają zainteresowania populacji ogólnej, a jedynie niewielkie zainteresowanie służb specjalnych; zajmują się nimi głównie służby weterynaryjne i fitosanitarne oraz interesariusze – rolnicy i hodowcy, leśnicy, myśliwi, ekolodzy).

W niektórych państwach, takich jak Wielka Brytania, Irlandia, Australia czy Nowa Zelandia, świadomość na temat bezpieczeństwa epidemiologicznego i żywnościowego wydaje się bardzo duża (co może manifestować się np. liczbą powstających tam artykułów naukowych dotyczących tych zagadnień[17]). Wynika to również z określonych czynników geograficznych i Polska raczej nie dorówna takiemu poziomowi wiedzy i wzorcowemu nadzorowi. Widoczne jest jednak dążenie do standardów północnoamerykańskich i zachodnioeuropejskich w budowaniu wiedzy o bezpieczeństwie żywności czy bioterroryzmie (np. jest ona przekazywana na studiach rolniczych, biochemicznych[18]). W polskim społeczeństwie

[16] A. Jarynowski, A. Semenov, V. Belik, *Perception of infectious diseases with animal and humans hosts on the Polish internet*, 20th Congress of the International Society for Animal Hygiene, Berlin, 5–7 X 2022 r., http://interdisciplinary-research.eu/wp-content/uploads/2022/08/Abstract-form-ISAH_jarynowski_corr.pdf [dostęp: 7 XI 2022].

[17] Ponad połowa (768 spośród 1336, tj. 57%) prac naukowych wyszukanych w bazie Scopus za pomocą fraz kluczowych 'invasive species' and 'infectious' pochodzi z przynajmniej jednego z tych państw.

[18] P. Cwynar, *Bioterroryzm – syllabus*, Uniwersytet Przyrodniczy we Wrocławiu, 2021 r., https://sylabus.upwr.edu.pl/pl/document/7562fe08-5a02-4db5-8d31-d7144fdd99bb.pdf [dostęp: 1 XI 2022].

wiedza na te tematy i zainteresowanie nimi nadal są jednak niewielkie, pomimo prowadzenia kampanii informacyjnych[19].

W przypadku ataku biologicznego zamachowcy mogą postrzegać następujące czynniki jako dające agroterroryzmowi przewagę nad bioterroryzmem[20]:

- materiał zakaźny można pobrać, przetwarzać i transportować z minimalnym narażaniem własnego zdrowia;
- ryzyko wykrycia w czasie przygotowań do ataku jest niewielkie (relatywnie słabo rozbudowany nadzór agencji wywiadu, inspekcji weterynaryjnej czy fitosanitarnej nad środkami biologicznymi (ang. *biological agent*[21]) niestanowiącymi zagrożenia dla ludzi);
- niski koszt a jednocześnie duży wpływ na gospodarkę i bezpieczeństwo żywnościowe (działanie wysoce efektywne pod względem kosztów[22]);
- ideologiczne i utylitarne motywacje potencjalnych agroterrorystów[23] (np. unijny program Zielony Ład – podłożem ataków mogą być napięcia społeczne spowodowane kryzysem klimatycznym i związaną z nim koniecznością redukcji emisji gazów cieplarnianych przez ograniczenie produkcji zwierzęcej; prawa zwierząt i ich dobrostan[24] – np. ataki na ubojnie czy fermy przemysłowe; zwierzęta nieczyste w islamie).

---

[19] A. Jarynowski, A. Semenov, V. Belik, *Perception of infectious diseases*...

[20] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-covid era in context of massive scale dissemination of microbiology/epidemiology knowledge*, „DiMiMED – International Conference on Disaster and Military Medicine", Düsseldorf, 15–16 XI 2021 r., https://events.military-medicine.com/media/landingpage/25/attachment-1639063402.pdf [dostęp: 12 VIII 2022].

[21] Szkodliwe czynniki biologiczne, takie jak wirus, bakteria, pierwotniak, grzyb czy toksyna (przyp. red.).

[22] J. Monke, *Agroterrorism: Threats and preparedness*, https://sgp.fas.org/crs/terror/RL32521.pdf, s. 1 [dostęp: 7 VIII 2022].

[23] *Debata Bezpieczeństwo żywnościowe Europy w świetle nadchodzących wyzwań*, Instytut Gospodarki Rolnej, 2022 r., https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/ [dostęp: 2 XI 2022 r.]. Materiał został przeniesiony do archiwum: https://web.archive.org/web/20221104152532/https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/.

[24] *Jedno zdrowie. Ludzie i inne gatunki*, H. Mamzer, P. Białas (red. nauk.), Wrocław 2022, s. 11.

Wadami ataku biologicznego w porównaniu z bioterroryzmem są natomiast (z perspektywy zamachowców)[25]:

- brak efektu paniki oraz niewielkie zainteresowanie chorobami zwierząt lub roślin wśród ogółu społeczeństwa[26] (w związku z tym pozyskanie terrorysty niezwiązanego z rolnictwem czy zwierzętami może być trudne);
- dysonans etyczny[27] dla potencjalnego agroterrorysty zachęconego do działania z pobudek ideologicznych.

W kontekście zjawiska agroterroryzmu warto wspomnieć o idei One Health (pol. Jedno zdrowie), zgodnie z którą pojęcie zdrowia nie powinno być postrzegane wyłącznie w kategoriach ludzkich, ale obejmować również dobrostan zwierząt i całego środowiska[28]. To koncepcja postrzegająca zdrowie ludzi, zwierząt, roślin i środowiska przyrodniczego jako elementy jednego i współzależnego układu, w którym zdrowie ludzkie jest nierozerwalnie związane z dobrostanem zwierząt i środowiska naturalnego, a choroby przenoszone pomiędzy ludźmi, zwierzętami i środowiskiem są silnie ze sobą powiązane. Takie holistyczne podejście jest potrzebne, gdyż między zdrowiem ludzi, stanem zwierząt hodowlanych i dzikiej zwierzyny oraz m.in. fitopatologią roślin istnieje ścisły związek, a różnice między tymi grupami zostały wprowadzone przez ludzi i są w dużej mierze sztuczne. Uwarunkowania społeczne czy metody kontroli zakażeń co do zasady są takie same, jednak wiedzę na ten temat buduje się w sposób silosowy (osobno dla takich dziedzin, jak medycyna, weterynaria i ochrona roślin). Zdaniem autora artykułu tę silosowość podtrzymują urzędnicy[29] (osobne ustawy o zapobieganiu oraz zwalczaniu

---

[25] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era*...

[26] A. Jarynowski, A. Semenov, V. Belik, *Perception of infectious diseases*...

[27] H. Mamzer, *Choroba jako zjawisko społeczne. Analiza walki z afrykańskim pomorem świń*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2020, t. 82, nr 2, s. 281–297. https://doi.org/10.14746/rpeis.2020.82.2.19.

[28] S.Y. Essack, *Environment: the neglected component of the One Health triad*, „The Lancet Planetary Health" 2018, t. 2, nr 6, e238-e239. https://doi.org/10.1016/S2542-5196(18)30124-4.

[29] Jest to opinia sformułowana na podstawie doświadczeń autora w zwalczaniu ASF, HPAI u drobiu oraz u ssaków, COVID-19, pracy związanej z próbą wyjaśnienia i ograniczenia skutków katastrofy ekologicznej na Odrze, jak również zminimalizowania zagrożeń wynikających z biologicznego zanieczyszczenia zboża z Ukrainy. W celu pełnego zrozumienia zagadnienia należy zapoznać się z obowiązującym prawem sanitarnym, weterynaryjnym i żywnościowym w postaci: rozporządzeń UE o zwalczaniu chorób zakaźnych ludzi, zwierząt i roślin; ustaw dotyczących działań administracji rządowej i jednostek samorządu

zakażeń i chorób zakaźnych u ludzi; o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt; o ochronie roślin przed agrofagami), a procedury administracyjne mające na celu ponowne scalenie przez służbę cywilną (zwłaszcza administrację zespoloną) wiedzy z różnych dziedzin są realizowane w oderwaniu od paradygmatów biologicznych[30]. Idea Jednego zdrowia coraz bardziej zyskuje na znaczeniu i popularności. Po wejściu Polski do NATO struktura organizacyjna wojskowych ośrodków medycyny prewencyjnej została dostosowana do paradygmatu zwalczania zagrożeń wypracowanego w ramach tego podejścia (zgodnie z wzorcami NATO dostosowanymi do polskich warunków m.in. przez Jarosława Foremnego)[31].

Wpływ pandemii COVID-19 na zjawisko agroterroryzmu

W trakcie pandemii wiele osób mogło zdobyć wiedzę związaną z transmisyjnością chorób zakaźnych, zarezerwowaną do tej pory dla wąskiego grona specjalistów. Jednym ze środków przeciwepidemicznych było bowiem zapoznanie z nią społeczeństwa, aby ograniczyć zapadalność na COVID-19 (np. przez stosowanie środków ochrony osobistej czy samotestowanie). Ta wiedza może zostać wykorzystana w różny sposób. Pandemia wymusiła również postęp w wybranych dziedzinach nauki, odsłoniła globalne podatności na zagrożenia biologiczne i ponownie skupiła uwagę na możliwości celowych ataków z wykorzystaniem czynników biologicznych, co eksperci NATO wskazali jako możliwy czynnik ryzyka[32]. Powszechniejsze, i przez to

terytorialnego oraz funkcjonowania odpowiednich inspekcji; aktów wykonawczych (w formie rozporządzeń odpowiednich ministrów oraz Prezesa Rady Ministrów) w sprawie współpracy krajowych inspekcji.

30 M. Kędzierski, *Integracja czy połączenie. Analiza możliwości zwiększenia efektywności działania inspekcji weterynaryjnej oraz ochrony roślin i nasiennictwa*, Europejski Fundusz Rozwoju Wsi Polskiej, https://efrwp.pl/publikacje/integracja-czy-polaczenie-analiza-mozliwosci-zwiekszenia-efektywnosci-dzialania-inspekcji-weterynaryjnej-oraz-ochrony-roslin-i-nasiennictwa/ [dostęp: 7 VI 2023].

31 Lista tych ośrodków jest dostępna na stronie: https://www.gov.pl/web/obrona-narodowa/wojskowe-osrodki-medycyny-prewencyjnej [dostęp: 2 III 2023].

32 S. Clement, *Biological Threats: Technological Progress and the Spectre of Bioterrorism in the Post-Covid-19 Era*, https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-01/024%20STCTTS%2021%20E%20rev.%201%20fin%20-%20%20BIOLOGICAL%20THREATS.pdf [dostęp: 8 VIII 2022].

dostępniejsze, stały się niektóre techniki diagnostyczne, np. typu POI/POC (ang. *point of interest* lub *point of care*), czyli diagnostyki przenośnej. Ponadto mamy do czynienia z postępem wielu dziedzin nauk biologicznych, inżynieryjnych i wojskowych, które także mają potencjał podwójnego zastosowania (ang. *dual use research of concern*, DURC) i mogą być wykorzystane do planowania i przeprowadzenia ataków terrorystycznych bądź sabotażu z użyciem czynników biologicznych. Generalnie od dziesięcioleci jest widoczny postęp naukowo-technologiczny w obszarze medycyny, biologii i techniki (o czym dyskutowano m.in. na dziewięciu konferencjach przeglądowych konwencji BTWC), jednak zdaniem autora niniejszego artykułu w ostatnich kilku latach zmiany mają charakter skokowy. Pozostaje pytanie o motywacje do działań sprzecznych z dobrem ogółu[33] i procesy prowadzące do radykalizacji.

Podsumowując, pandemia COVID-19 przyczyniła się do[34]:

- zwiększenia łatwości pozyskania materiału zakaźnego (znajomość podstaw mikrobiologii i patogenezy). Składa się na to praktyka w zbieraniu i przygotowywaniu próbek (powszechne samotestowanie na COVID-19), wiedza o procesach immunologicznych, dynamice wiremii, serokonwersji, podatności poszczególnych organów i układów. Ponadto przyczyniła się do rozwoju biologii syntetycznej z wykorzystaniem obliczeniowych modeli uczenia maszynowego[35] do przewidywania toksyczności lub wirulencji i zakaźliwości w różnych obszarach czy docelowo do modyfikacji genetycznej bioagentów;
- uproszczenia weryfikacji czynnika zakaźnego (dostęp do diagnostyki). Gwałtowny postęp nauki, skutkujący masową dostępnością do taniej, przenośnej diagnostyki mikrobiologicznej, np. w postaci testów kasetowych (zwłaszcza upowszechnienie wśród szerszej grupy odbiorców praktycznych umiejętności korzystania z tych narzędzi), mimo że służył przede wszystkim do zwalczania pandemii COVID-19, ma również skutki uboczne;
- zwiększenia łatwości introdukcji (znajomość podstaw epidemiologii, w tym dróg transmisji) – zrozumienie zasad triady epidemiologicznej

[33] A. Jarynowski, M. Stochmal, J. Maciejewski, *Przegląd i charakterystyka prowadzonych w Polsce badań…*, s. 73.

[34] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era…*

[35] S. Clement, *Biological Threats: Technological Progress…*

(czynnik zakaźny, gospodarz i środowisko, w którym występują warunki do przeniesienia czynnika zakaźnego), transmisyjności materiału zakaźnego, sezonowości, a także poznanie, jak działają systemy nadzoru epidemiologicznego.

Postęp można zilustrować na przykładzie potencjalnych scenariuszy intencjonalnego wprowadzenia wirusa ASF w warunkach pre-[36] i postcovidowych[37] w Polsce i Europie. Należy podkreślić, że ze względu na wady techniczne użycia broni biologicznej wobec ludzi (polityczne konsekwencje jej użycia wobec agresora, np. Rosji, mogą być bardzo poważne) jej zastosowanie wydaje się mało prawdopodobne[38]. Realnym zagrożeniem jest natomiast agroterroryzm, tym bardziej że takie działania nie muszą mieć spektakularnego charakteru i mogą zostać przeprowadzone poniżej progu wykrycia. Możliwe są mniejsze lokalne działania z wykorzystaniem agentów uśpionych. Skala agroterroryzmu może być trudna do oszacowania, a repertuar działań jest naprawdę szeroki. Jego skutkiem może okazać się osłabienie produkcji żywności i polaryzacja społeczna w Polsce oraz w regionie europejskim[39].

Analiza epidemiologiczna, epizootyczna, epifityczna w kontekście bezpieczeństwa żywnościowego

Czynniki biologiczne zagrażające ludziom są dosyć dobrze zbadane przez polskie środowisko naukowe. Z kwerendy przeprowadzonej przez Akademię Wojsk Lądowych wynika, że latach 2009–2018 w polskim piśmiennictwie ukazywało się średnio 10 prac naukowych rocznie poświęconych

[36] A. Jarynowski i in., *ASF jako zagrożenie biologiczne w Polsce i na świecie*, w: *Bezpieczeństwo regionalne. Węzłowe problemy i procesy*, P. Bajor (red.), Kraków 2021, s. 239–254. https://doi.org/10.12797/9788381383899.14.

[37] A. Jarynowski, Ł. Krzowski, V. Belik, *Afrykański pomór świń: epizootiologia, ekonomia i zarządzanie kryzysowe w kontekście naturalnego bądź intencjonalnego wprowadzenia*, „Studia Administracji i Bezpieczeństwa" 2021, t. 11, nr 11, s. 129–153. https://doi.org/10.5604/01.3001.0015.6752.

[38] G. Kessler, *How the right embraced Russian disinformation about 'U.S. bioweapons labs' in Ukraine*, „The Washington Post", 11 III 2022 r., https://www.washingtonpost.com/politics/2022/03/11/how-right-embraced-russian-disinformation-about-us-bioweapons-labs-ukraine/ [dostęp: 7 VIII 2022].

[39] A. Jarynowski i in., *African Swine Fever – potential biological warfare threat*, preprint, https://easychair.org/publications/preprint/vjFf [dostęp: 7 VIII 2022].

tym czynnikom[40]. Głównym obszarem badawczym pozostają odzwierzęce czynniki chorobotwórcze (powodujące zoonozy), gdyż mają one znaczenie dla medycyny. W dużym stopniu jest natomiast pomijany problem zakażeń niedotyczących populacji ludzi. Popularnością cieszy się również tematyka bezpieczeństwa żywnościowego (w latach 2009–2021 było to ok. 15 prac tematycznych rocznie polskich autorów[41]). Z kolei czynniki agroterroryzmu biologicznego są rzadko omawiane poza środowiskiem specjalistów z dziedziny nauk rolniczych. W opinii krajowych ekspertów Polska do tej pory nie wydawała się bezpośrednio zagrożona agroterroryzmem, zwłaszcza wobec roślin[42], o czym może świadczyć niefrasobliwe postępowanie Polaków z gatunkami inwazyjnymi czy z nasionami nieznanego pochodzenia. Niewielkie zainteresowanie zagrożeniami związanymi z agroterroryzmem dotyczącym roślin (w przeciwieństwie do działań wobec zwierząt[43]), spowodowane m.in. brakiem dokumentowania takich przypadków, może prowadzić do uśpienia czujności.

Potencjalnie wrogie organizacje terrorystyczne (finansowane przez reżimy, takie jak Federacja Rosyjska czy Chiny, lub twory parapaństwowe, jak np. Państwo Islamskie) mogą skorzystać z szerokiego repertuaru narzędzi i możliwości, np. z modelowania matematycznego[44] i sztucznej inteligencji, w celu zoptymalizowania efektów działania agroterrorystycznego. Warto zwrócić uwagę przede wszystkim na tzw. samotne wilki (terrorystów działających w pojedynkę, niebędących częścią większej siatki

---

[40] *Broń masowego rażenia, broń biologiczna, broń chemiczna, broń jądrowa. Cz. 2,* K. Mordzak (oprac.), Wrocław 2019, https://www.wojsko-polskie.pl/awl/u/96/0c/960cad22-5698-4356-b-8f5-38117fb19499/bron_cbn.pdf [dostęp: 7 VIII 2022].

[41] *Bezpieczeństwo żywnościowe,* K. Mordzak (oprac.), Wrocław 2021, https://www.wojsko-polskie.pl/awl/u/50/d4/50d46baf-332b-4acb-aeb3-8f5b17777590/bezpieczenstwo_zywnosciowe.pdf [dostęp: 7 VIII 2022].

[42] J. Lipa, *Agroterroryzm – wyzwaniem dla kwarantanny i ochrony roślin,* „Progress in Plant Protection" 2006, t. 46, nr 1, s. 167; M. Lenda i in., *Misinformation, internet honey trading and beekeepers drive a plant invasion,* „Ecology Letters" 2021, t. 24, nr 2, s. 165–169. https://doi.org/10.1111/ele.13645; M. Lenda i in., *Effect of the Internet Commerce on Dispersal Modes of Invasive Alien Species,* „PLoS ONE" 2014, t. 9, nr 6, p.e99786. https://doi.org/10.1371/journal.pone.0099786.

[43] M. Wiśniewska, *The food terrorism – the essence and the methods of systemic defense,* „Journal of Modern Science" 2023, t. 50, nr 1, s. 331–349. https://doi.org/10.13166/jms/161535.

[44] A. Jarynowski, A. Grabowski, *Modelowanie epidemiologiczne dedykowane Polsce,* Portal CZM, 2015 r., http://www.czm.mif.pg.gda.pl/wp-content/uploads/fam/publ/jarynowski2.pdf [dostęp: 7 VIII 2022].

terrorystycznej)[45], których działania cechują się niskobudżetowością i tzw. mikrobiologią kuchenną (ang. *kitchen microbiology* lub *do-it-yourself microbiology*). Zwiększenie wiedzy i rozwój technologii spowodowane pandemią COVID-19 mogą sprzyjać ich aktywności o charakterze agroterrorystycznym. Są pewne grupy zawodów medycznych, weterynaryjnych, rolniczych czy związanych z ochroną środowiska i biologią, które mogą predysponować od strony technicznej do agroterroryzmu z uwagi na posiadane umiejętności. Warto jednak podkreślić, że wzorce przenoszenia chorób zakaźnych zwierząt i roślin są stosunkowo dobrze znane (ze względu na możliwość przeprowadzania eksperymentów w przeciwieństwie do eksperymentów z udziałem ludzi), w związku z tym specjalista weterynaryjny czy ochrony roślin łatwiej opracuje skuteczny plan introdukcji niż lekarz czy reprezentant innego zawodu medycznego. W przypadku chorób dotyczących ludzi wiedza epidemiologiczna jest mniejsza i pomimo miliardów dolarów wydanych na badania naukowe do tej pory nie są znane podstawowe charakterystyki SARS-CoV-2[46], np. ID50 (ang. *median infective dose*)[47].

Użycie najgroźniejszych patogenów zwierzęcych i roślinnych, takich jak ASFV czy *Xylella fastidiosa* (gram-ujemna bakteria zasiedlająca tkankę przewodzącą roślin), na obszarach wolnych od choroby może mieć poważne skutki. Może zostać wydany zakaz eksportu produktów na terenach zapowietrzonych lub występowania agrofagów kwarantannowych, co mogłoby spowodować straty liczone nawet w milionach euro miesięcznie.

Produkcja zwierzęca

W skali światowej główne działania mające na celu nadzorowanie ryzyka agroterroryzmu prowadzi Organizacja Narodów Zjednoczonych ds. Wyżywienia i Rolnictwa (ang. Food and Agriculture Organization of the United Nations, FAO), a na poziomie Unii Europejskiej – Europejski Urząd ds. Bezpieczeństwa Żywności (ang. European Food Safety Authority, EFSA).

[45] C.R. MacIntyre i in., *Converging and emerging threats to health security*, „Environment Systems and Decisions" 2018, t. 38, nr 2, s. 198–207. https://doi.org/10.1007/s10669-017-9667-0.

[46] S. Karimzadeh, R. Bhopal, H. Nguyen Tien, *Review of infective dose, routes of transmission and outcome of COVID-19 caused by the SARS-COV-2: comparison with other respiratory viruses*, „Epidemiology and Infection" 2021, t. 149, e96. https://doi.org/10.1017/S0950268821000790.

[47] ID50 – średnia dawka zakaźna w warunkach naturalnych, która powoduje rozwój choroby u 50% eksponowanych.

W Polsce za bezpieczeństwo biologiczne zwierząt odpowiada Inspekcja Weterynaryjna[48]. Rozwój epizootii zależy od wielu czynników, takich jak gęstość i wielkość gospodarstw, poziom bioasekuracji, interakcje ze środowiskiem naturalnym[49]. Epizootie cechują się średnim tempem rozwoju, ale zazwyczaj jest to kilkanaście lub kilkadziesiąt kilometrów rocznie (nie biorąc pod uwagę dalekozasięgowych skoków poza obszar funkcjonalny, które się dokonują za pośrednictwem człowieka[50]). Za pomocą introdukcji patogenu można średnioterminowo uzyskać istotną dezorganizację produkcji zwierzęcej (np. przecięcie łańcuchów dostaw).

Światowa Organizacja Zdrowia Zwierząt (ang. World Organisation for Animal Health, WOAH, wcześniej Office International des Epizooties, OiE) wykorzystała do klasyfikacji z 2018 r. choroby zwierząt gospodarskich (obecnie ta klasyfikacja nie jest stosowana). Podobnie klasyfikuje czynniki wywołujące choroby u zwierząt Centrum Kontroli i Prewencji Chorób Stanów Zjednoczonych (ang. Centers for Disease Control and Prevention, CDC), dzieląc je na dwie grupy pod względem poziomu ryzyka[51]:

- grupa A to najwyższe ryzyko – powodują ciężkie choroby, szybko się rozprzestrzeniają, łatwo pozyskać materiał zakaźny, np. ASF, FMD (ang. *Foot and Mouth Disease*, pol. pryszczyca), CSF (ang. *Classical Swine Fever*, pol. klasyczny pomór świń), HPAI (ang. *Highly Pathogenic Avian Influenza*, pol. wysoce zjadliwa grypa ptaków);
- grupa B to średnie ryzyko – powodują umiarkowanie groźne choroby o niskim wskaźniku śmiertelności, rozprzestrzeniają się umiarkowanie łatwo, np. bruceloza, salmonelloza.

Światowej klasy epidemiolog weterynaryjny Dirk Pfeifer stwierdził, że ASF (...) *to prawdopodobnie najpoważniejsza choroba zwierząt, jaką świat ma*

[48] Na stronie: https://bip.wetgiw.gov.pl/asf/mapa/ można obserwować mapy zagrożeń biologicznych na poziomie krajowym, a na stronie: https://empres-i.apps.fao.org – światowym.

[49] A. Jarynowski, V. Belik, *African Swine Fever (ASF) Virus propagation in Poland (Spatio-temporal analysis)*, preprint, https://www.researchgate.net/publication/338436134_African_Swine_Fever_ASF_Virus_propagation_in_Poland_Spatio-temporal_analysis [dostęp: 7 VIII 2022]. https://doi.org/10.13140/RG.2.2.29807.6167.

[50] A. Jarynowski, V. Belik, *Spatio-temporal analysis of African Swine Fever Spread in Poland with network perspective*, preprint, https://www.academia.edu/43262326/Multilayer_network_approach_to_African_Swine_Fever_Spread_in_Poland [dostęp: 12 VIII 2022].

[51] OiE, *Classification of diseases notifiable*, https://www.oie.int/en/animal-health-in-the-world/the-world-animal-health-information-system/old-classification-of-diseases-notifiable-to-the-oie-list-a/ [dostęp: 29 VII 2022].

od dawna, jeśli nie od zawsze[52]. Niedobór wieprzowiny w Chinach spowodowany ASF mógł przyczynić się do przeniesienia SARS-CoV-2 ze zwierząt na ludzi, gdyż wymusił poszukiwanie alternatywnych źródeł białek w dziczyźnie[53]. Pewne organizacje lub osoby, działające z różnych pobudek, ideologicznych, politycznych czy ekonomicznych, mogą czerpać korzyści z wprowadzenia ASF. Potencjalny agroterrorysta (wywodzący się z grona specjalistów przyrodników lub w ogóle niemający wykształcenia kierunkowego, ale przez dwa lata pandemii zgłębiający wiedzę na temat mechanizmów biologicznych rządzących chorobami zakaźnymi) będzie obecnie w stanie pobrać materiał i zweryfikować jego zakaźność oraz optymalnie wprowadzić patogen na wybrany obszar. Scenariusze introdukcji wirusa ASF, m.in. do Europy Zachodniej i zachodniej Polski, autor artykułu przedstawił we wrześniu 2019 r. podczas III Jagiellońskiej Konferencji Bezpieczeństwa[54] oraz w październiku 2019 r. na 44. spotkaniu BIOMED-EP, za pośrednictwem polskiej delegacji, w siedzibie NATO w Brukseli[55], czyli przed „przeskokiem" wirusa do zachodniej Polski i Niemiec[56]. Należy odróżniać doniesienia oparte na teoriach spiskowych, np. o zrzucaniu przez helikoptery zamrożonych ciał dzików[57], od realnych celowych działań potencjalnych terrorystów.

Dla przykładu warto przedstawić w skrócie kazus analizy wykonalności dla różnych potencjalnych ścieżek introdukcji, mającej następujące etapy[58]:

– pobranie materiału zakaźnego (z tusz dzików, produktów wieprzowych, dostarczenie przez służby lub hodowla);

---

[52] D. Normile, *African swine fever keeps spreading in Asia, threatening food security*, „Science", 2019 r., https://www.science.org/content/article/african-swine-fever-keeps-spreading-asia-threatening-food-security [dostęp: 12 VIII 2022]. Tłumaczenia w artykule pochodzą od autora (dop. red.).

[53] Wei Xia i in., *How One Pandemic Led To Another: Asfv, the Disruption Contributing To Sars-Cov-2 Emergence in Wuhan*, preprint, https://www.researchgate.net/publication/349628301_How_One_Pandemic_Led_To_Another_Asfv_the_Disruption_Contributing_To_Sars-Cov-2_Emergence_in_Wuhan [dostęp: 7 VIII 2022]. https://doi.org/10.20944/preprints202102.0590.v1.

[54] A. Jarynowski i in., *ASF jako zagrożenie biologiczne w Polsce*...

[55] A. Jarynowski i in., *African Swine Fever – potential biological*...

[56] A. Jarynowski, Ł. Krzowski, V. Belik, *Afrykański pomór świń*...

[57] *Zarażone ASF dziki spadają z nieba? Mające być dowodem zdjęcie budzi poważne wątpliwości*, Lublin112.pl, 22 VII 2018 r., https://www.lublin112.pl/zarazone-asf-dziki-spadaja-nieba-majace-byc-dowodem-zdjecie-budzi-powazne-watpliwosci/ [dostęp: 7 VIII 2022].

[58] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era*...; A. Jarynowski i in., *ASF jako zagrożenie biologiczne w Polsce*...

– procesowanie materiału i przygotowanie do optymalnego transportu (przygotowanie krwi, tkanek, kawałków ciała, inokulum[59]);
– introdukcję zakażenia materiałem zakaźnym (wybranie czasu oraz celów, a potem wstrzykiwanie dzikom czy świniom lub skarmianie ich bądź pojenie).

Brak sukcesów w zwalczaniu chorób zakaźnych zwierząt stał się jedną z przyczyn napięć na linii przedstawiciele branży spożywczej – rząd – ekolodzy, do których doszło w styczniu 2019 r. (protesty przeciw odstrzałom sanitarnym dzików[60]), w październiku 2020 r. (projekty takie, jak dobrostan zwierząt, Piątka dla zwierząt, zwalczanie ASF[61] i HPAI[62]) czy w lipcu 2022 r. (m.in. kwestia importu produktów spożywczych z Ukrainy, solidarność polskich rolników z rolnikami holenderskimi). Skala protestów rolniczych, pomimo pandemii COVID-19 i wojny, jest wyraźna. W Polsce są one organizowane na mniejszą skalę, ale w innych państwach UE mają większy zasięg i gwałtowniejszy przebieg. Już w czasie trwania pełnej rosyjskiej inwazji na Ukrainę (od lutego 2022 r.) aktywiści na rzecz praw zwierząt dokonali aktów dywersji. W dniach 19–20 czerwca 2022 r. w chlewniach i rzeźniach w Bocholt oraz Schermbeck w Niemczech spowodowali śmierć 130 zwierząt i duże straty materialne[63].

Kolejnym czynnikiem, który intensyfikuje ruchy ekologiczne, są zmiany klimatu (i ich postrzeganie). Padają między innymi żądania dotyczące zmniejszenia produkcji zwierzęcej odpowiadającej za emisję gazów cieplarnianych poprzez ograniczanie popytu i podaży. Prowadzi to do powstania nowej podkategorii ekologów – potencjalnych uczestników aktów

---

[59] *Inokulum* (łac.) – zawiesina cząstek wirusa, komórek bakterii lub zarodników grzyba (czasem fragmentów strzępek) patogenicznych dla rośliny, przygotowana przez człowieka w celu dokonania sztucznego zakażenia rośliny (inokulacja). Za: Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/inokulum;3914841.html [dostęp: 10 V 2023] – przyp. red.

[60] A. Jarynowski i in., *African Swine Fever Awareness in the Internet Media in Poland – exploratory review*, „E-methodology" 2019, t. 6, nr 6, s. 100–115. https://doi.org/10.15503/emet2019.100.115.

[61] H. Mamzer, *Choroba jako zjawisko społeczne*..., s. 293–294.

[62] A. Jarynowski i in., *Animal breeders protests in Polish Twitter - preliminary research*, preprint, http://interdisciplinary-research.eu/wp-content/uploads/2022/04/animal_related_protests_in_twitter_preprint_pdf.pdf [dostęp: 12 VIII 2022].

[63] A. Deter, *50 vermummte Aktivisten blockieren Bocholter Schlachthof*, Topagrar, 20 VI 2022 r., https://www.topagrar.com/schwein/news/aktivisten-blockieren-bocholter-schlachthof-13131573.html [dostęp: 7 VIII 2022].

agroterroryzmu, gdyż do tej pory obrońcy praw zwierząt stanowili główną kategorię sprawców[64].

Produkcja roślinna

Na poziomie unijnym agrofagi podlegające monitorowaniu lub kwarantannowaniu, czyli najgroźniejsze patogeny, szkodniki i chwasty obniżające plony roślin uprawnych, są wskazywane przez Międzynarodową Konwencję Ochrony Roślin (ang. International Plant Protection Convention, IPPC) we współpracy z FAO oraz EFSA. W Polsce organem nadzorującym jest Państwowa Inspekcja Ochrony Roślin i Nasiennictwa (PIORiN)[65]. Szczególną uwagę należy zwrócić na agrofagi: *Xylella fastidiosa* (bakteryjny agrofag m.in. drzew oliwnych stanowiący według EFSA największy problem w UE[66]), *Candidatus Liberibacter solanacearum* (bakteria wywołująca chorobę ziemniaka zwaną zebrowatością chipsów), *Ralstonia solanacearum* (bakteria wywołująca chorobę ziemniaka zwaną śluzakiem) oraz *Colletotrichum fructicola* (grzyb wywołujący chorobę owoców, np. jabłek). Ze względu na specyficzne cykle epidemiologiczne w agrofagach patogennych roślin (np. siewstwo z cyklem nasiennym) tempo rozprzestrzeniania się epifitozy zależy od wielu czynników, takich jak struktura upraw, warunki pogodowe i klimat. Tempo to jest zazwyczaj wolne – rzadko przekracza kilka kilometrów na rok (czasami zdarzają się skoki dalekozasięgowe spowodowane działalnością człowieka). W związku z powyższym za pomocą agrofagów trudno jest osiągnąć efekty w krótkim czasie (wyjątkiem jest ukierunkowane wykorzystanie szarańczy). Wprowadzenie inwazyjnego agrofaga może mieć jednak daleko idące skutki dla ekosystemu, trudne do zamodelowania czy przewidzenia[67].

[64] *Bridging the expertise of the animal health and law enforcement sectors*, https://www.woah.org/app/uploads/2023/02/building-resilience-against-agro-crime-and-agro-terrorism.pdf [dostęp: 4 III 2023].

[65] Na stronie: https://www.sygnalizacja.agrofagi.com.pl można obserwować mapy zagrożeń agrofagami na poziomie krajowym, a na stronie: https://gd.eppo.int – światowym.

[66] European Food Safety Authority (EFSA), *Update of the Xylella spp. host plant database – systematic literature search up to 31 December 2021*, „EFSA Journal" 2022, t. 20, nr 6, e07356. https://doi.org/10.2903/j.efsa.2022.7356.

[67] A. Jarynowski, F. Lopez-Nunez, H. Fan, *How network temporal dynamics shape a mutualistic system with invasive species?*, preprint, https://arxiv.org/ftp/arxiv/papers/1407/1407.4334.pdf [dostęp: 7 VIII 2022]. https://doi.org/10.48550/arXiv.1407.4334.

Warto przyjrzeć się bliżej *Colletotrichum fructicola*[68]. Patogen ten rozprzestrzenia się wolno. Zainfekowanie może nastąpić przez bezpośredni kontakt z grzybnią oraz drogą powietrzną – zarodniki mogą być niesione na niewielkie odległości wiatrem oraz przez wektory mechaniczne w postaci insektów. W latach 2019–2021 odnotowano dwa ogniska zakażeń we Włoszech i jedno we Francji. W Polsce, której przypada jedna trzecia produkcji jabłek w UE, jest duży potencjał żywiciela. Jednakże *Colletotrichum fructicola* to patogen zależny od klimatu (raczej nie przeżyje zimy w Polsce poza systemem przechowywania owoców), więc intencjonalne wprowadzenie go ze względów naturalnych i działań fitosanitarnych będzie z dużym prawdopodobieństwem jedynie jednosezonowe.

Dezinformacja dotycząca broni biologicznej i żywności – przyczynek teoretyczny

Broń biologiczna ma ogromny potencjał zastraszania. Pokazali to Rosjanie, gdy tematem rzekomych tajnych amerykańskich laboratoriów na terenie Ukrainy rozpoczęli cykl publicznych wrzutek Ministerstwa Obrony FR[69] w postaci serii prezentacji w 2022 r. (10 i 17 marca, 14 kwietnia, 27 maja, 17 czerwca, 7 lipca, 4 sierpnia, 3 i 19 września). Należy podkreślić, że w każdej z nich przewijał się wątek chorób zakaźnych zwierząt, głównie ASF i grypy ptaków. Igor Kiriłłow, dowódca wojsk obrony radiologicznej, chemicznej i biologicznej Rosji, wielokrotnie podkreślał, że Rosjanie „zdobyli" dowody na przeprowadzanie na terenie Ukrainy eksperymentów biologicznych na ludziach, jak również na świniach, dzikach, ptakach czy insektach[70]. Na posiedzeniu sesji Rady Bezpieczeństwa ONZ 11 marca 2022 r. doszło do konfrontacji między USA a Rosją[71]. Ponadto 8 lipca 2022 r. Rosja uruchomiła, o czym już wspomniano, art. 5 konwencji o zakazie broni biologicznej i wezwała do formalnego spotkania

[68] EFSA Panel on Plant Health (PLH), *Pest categorisation of Colletotrichum fructicola*, „EFSA Journal" 2021, t. 19, nr 8, e06803.

[69] И. Кириллов, *Тезисы брифинги начальника войск радиационной, химической и биологической защиты ВС РФ генерал-лейтенанта И.А. Кириллова* (materiał Ministerstwa Obrony Federacji Rosyjskiej zebrany przez autora z kanału Telegram, dostępny u autora na prośbę e-mailową).

[70] Tamże.

[71] S. Maksymowicz, *Atak biologiczny i agroterrorystyczny na Polskę*...

konsultacyjnego. W sierpniu i wrześniu 2022 r. odbyło się postępowanie kontrolne wobec USA i Ukrainy (mogły tam paść zarzuty czy insynuacje dotyczące Polski, dlatego obserwacja formalnego spotkania państw-stron konwencji o zakazie broni biologicznej była bardzo ważna, gdyż Polska jest po USA, Ukrainie, Niemczech następnym celem rosyjskiej propagandy na temat broni biologicznej[72]). W związku z tym warto, aby Polska zawczasu się do tego przygotowała (9 września 2022 r. w Genewie na posiedzeniu formalnym państw-stron konwencji o zakazie broni biologicznej reprezentant Polski przedstawił stanowisko zbieżne ze stanowiskiem UE). Według amerykańskich analityków Rosja być może próbuje w ten sposób maskować użycie środków biologicznych jako części zainscenizowanego incydentu lub ich wykorzystanie do wsparcia taktycznych operacji wojskowych[73]. We wrześniu 2022 r. Kiriłłow zmienił front, wskazując na zagrożenie nuklearne. Przyczyną mogła być porażka kampanii dotyczącej broni biologicznej.

W wewnętrznej narracji prowadzonej w Rosji[74] już od dawna przewija się wątek rozwijania przez Polskę broni biologicznej. Zarówno w mediach, jak i w opracowaniach „naukowych" pojawiają się na ten temat anegdoty, z których część sięga czasów wojen polsko-moskiewskich. Najwięcej zarzutów opiera się na mitycznym polskim programie biologicznym z okresu międzywojennego rozwijanym w trakcie wojny polsko-bolszewickiej[75] i po jej zakończeniu oraz w ramach działalności Polskiego Państwa Podziemnego. W zewnętrznej narracji Rosji są stosowane wobec Polski (głównie poprzez polskojęzyczne kanały propagandy lub kanały rezonujące

[72] A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet as a possible Kremlin warfare* (wersja robocza), https://zenodo.org/record/8081493 [dostęp: 26 VI 2023].

[73] Tamże.

[74] I. Kiriya, *From "Troll Factories" to "Littering the Information Space": Control Strategies Over the Russian Internet*, „Media and Communication" 2021, t. 9, nr 4, s. 16–24. https://doi.org/10.17645/mac.v9i4.4177.

[75] Rzeczywiście był taki program, ale dotyczył on badań w zakresie ochrony przed bronią biologiczną i toksynową, a wroga propaganda wykorzystywała i wykorzystuje jego istnienie do własnych celów.

z propagandą rosyjską[76]) przede wszystkim techniki służące wywołaniu niepokoju[77].

Aby zbadać zaangażowanie społeczeństwa w tematy związane z biopolityką, warto wykorzystać monitoring mediów[78]. Wiadomo, że potencjalnie prokremlowskie konta biorące udział w dyskursie na temat wojny pojawiają się również (ponad 50-krotnie większa szansa zaangażowania) w dyskursie dotyczącym protestu antycovidowego i szczepionkowego[79]. W związku z tym z dynamiki dyskursu w mediach społecznościowych, nawet w obszarach niekoniecznie na pierwszy rzut oka związanych z wojną (jak kwestie biopolityczne), można dosyć dużo wywnioskować na temat nastrojów społecznych. Warto podkreślić, że nietypowa dynamika zainteresowania w Niemczech szczepieniami przeciw COVID-19 szczepionką firmy Oxford/AstraZeneca[80] (a zwłaszcza niepożądanymi odczynami poszczepiennymi[81]) nosi znamiona ingerencji obcych wywiadów (potencjalnie rosyjskiego[82],

---

[76] *Analiza i dekonstrukcja rosyjskich przekazów dezinformacyjnych oraz propagandowych na temat Polski i Polaków*, https://infowarfare.pl/realizowane-projekty/ [dostęp: 25 VI 2023]; M. Marek, *Rosyjska dezinformacja w Polsce – cele i przekazy*, Centrum Badań nad Współczesnym Środowiskiem Bezpieczeństwa, 30 III 2022 r., https://infowarfare.pl/2022/03/30/rosyjska-dezinformacja-w-polsce-cele-i-przekazy/ [dostęp: 25 VI 2023].

[77] T. Helmus i in., *Russian social media influence: Understanding Russian propaganda in Eastern Europe*, Santa Monica 2018.

[78] A. Jarynowski, *Infodemiologia oraz infonadzór – doświadczenia doby pandemii*, w: *Epidemiologia i bezpieczeństwo CBRN. Nauka, innowacje, implikacje praktyczne*, A. Mróz-Jagiełło, J. Walczak (red.), seria: Epimilitaris, Zielonka 2022, s. 235–248.

[79] Gdy wylosuje się 50 kont na niemieckojęzycznym Twitterze zaangażowanych w czasie pandemii COVID-19 jednocześnie w dyskurs antyszczepionkowy i antysanitarny oraz porówna ich zaangażowanie w dyskurs wojenny na początku inwazji rosyjskiej w 2022 r., to okaże się, że średnio 49 kont będzie można sklasyfikować jako prokremlowskie, a tylko jedno jako proukraińskie. Zob. A. Jarynowski, *Pro-Kremlin German Twitter users are more likely to be involved in both anti-lockdown and anti-vaccine discourse than Anti-Kremlin users*, preprint, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4079045 [dostęp: 7 VIII 2022]. https://dx.doi.org/10.2139/ssrn.4079045.

[80] D. Jemielniak, Y. Krempovych, *An analysis of AstraZeneca COVID-19 vaccine misinformation and fear mongering on Twitter*, „Public Health" 2021, t. 200, s. 4–6. https://doi.org/10.1016/j.puhe.2021.08.019.

[81] V. Belik, A. Jarynowski, *Elucidating the interplay of COVID-19 epidemic and social dynamics via Internet media in Germany*, konferencja on-line „Preparedness for future pandemics from a global perspective", 15 XI 2021 r., https://zenodo.org/record/6400773#.ZGRny3ZByUk [dostęp: 7 VIII 2022].

[82] EEAS, *Short assessments of narratives and disinformation around the Covid-19 pandemic (update December 2020 - April 2021)*, EUvsDisinfo, 28 IV 2021 r., https://euvsdisinfo.eu/eeas-

ale niektórzy analitycy wskazują również na chiński[83] w ramach jawnej i niejawnej dyplomacji szczepionkowej[84]).

W Polsce odróżnienie narracji proklemlowskiej od antykremlowskiej nie jest tak łatwe jak w Niemczech, gdzie inwazję popiera się w sposób bardziej jawny. W Polsce jest to mniej jednoznaczne[85] i wymaga intensywniejszej pracy służb, takich jak Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, a także Biura Bezpieczeństwa Narodowego. Warto podkreślić, że sposób, w jaki jest prowadzona rosyjska propaganda, różni się w zależności od kraju czy medium, więc co do zasady polskie służby w większym stopniu powinny się skupić na własnych analizach empirycznych[86] niż na literaturze światowej (zwłaszcza amerykańskiej[87]). Jarynowski i współautorzy zauważyli, że pewne konta występowały we wszystkich dyskursach i to często w nietypowych dla siebie pozycjach (np. w dyskursach dotyczących koronawirusa[88] czy lockdownów[89] pojawiających się na prawicy, ale akurat w kontekście zwalczania ASF klastrowały się one z ideologiczną lewicą[90]. Jedyny łączący te postawy wzorzec to działanie na szkodę Jednego zdrowia poprzez negacjonizm biologiczny[91]).

---

special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021/ [dostęp: 7 VIII 2022].

83 A. Lipińska, *Chińskie operacje w dobie COVID-19. Dezinformacja – metody, dziedziny i ewolucja*, „Cyber Security and Law" 2022, t. 7, nr 1, s. 61–71.

84 *What next for vaccine diplomacy?*, „The Economist", 3 V 2021 r., https://www.economist.com/podcasts/2021/05/03/whats-next-for-vaccine-diplomacy [dostęp: 7 VIII 2022].

85 *W okresie ostatnich 48 godzin dynamicznie rośnie zagrożenie dezinformacyjne w tematyce wydarzeń #Ukraina #Rosja w polskiej przestrzeni internetowej*, IBIMS, https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ [dostęp: 7 VIII 2022].

86 A. Jarynowski, *Pro-Kremlin German Twitter*...

87 D. Broniatowski i in., *Vaccine Communication as Weaponized Identity Politics*, „American Journal of Public Health" 2020, t. 110, nr 5, s. 1378–1384.

88 A. Jarynowski i in., *Attempt to understand public health relevant social dimensions of COVID-19 outbreak in Poland*, „Society Register" 2020, t. 4, nr 3, s. 20. https://doi.org/10.14746/sr.2020.4.3.01.

89 A. Jarynowski, D. Płatek, *Sentiment analysis: Topic modelling and social network analysis. COVID-19, protest movements and the Polish Tweetosphere*, w: *The Covid-19 Pandemic as a Challenge for Media and Communication Studies*, London 2022, s. 210–224. https://doi.org/10.4324/9781003232049-21.

90 A. Jarynowski i in., *African Swine Fever – potential biological*...

91 M. Duplaga, *Znaczenie kompetencji zdrowotnych w świecie infodemii*, Instytut Zdrowia Publicznego, https://izp.wnz.cm.uj.edu.pl/pl/blog/projekt-znaczenie-kompetencji-zdrowotnych-w-swiecie-infodemii/ [dostęp: 7 VIII 2022].

W związku z powyższym na problematykę kryzysu żywnościowego, laboratoriów biologicznych i pandemii COVID-19 można spojrzeć również jak na przedmiot operacji informacyjnych (ang. *information operations*, INFOOPS) oraz operacji psychologicznych (ang. *psychological operations*, PSYOPS)[92]. W kontekście istnienia zjawiska infodemii[93] (o czym można było się przekonać w czasie pandemii COVID-19[94]) dużą rolę odgrywa zaangażowanie obcego wywiadu, za pośrednictwem tzw. armii botów, farm trolli, agentów wpływu czy pożytecznych idiotów, w dyskurs dotyczący chorób zakaźnych[95]. Niestety w tej wojnie informacyjnej[96] mamy do czynienia z bardzo dobrze przygotowanym i doświadczonym przeciwnikiem, który będzie wykorzystywał żywność i czynniki biologiczne w celach propagandowych, gdyż ułatwia mu to wywieranie wpływu na polskie społeczeństwo. Warto jednak podkreślić, że to nie Polska, a głównie kraje Globalnego Południa, które są uzależnione od importu taniej żywności z Rosji i Ukrainy, są najważniejszym teatrem działań informacyjnych. Dlatego należy bacznie obserwować, jakie nastroje są tam wzbudzane i czy braki w dostawach zboża mogą wywołać niepokoje, a w konsekwencji falę migracji.

Dezinformacja dotycząca broni biologicznej i żywności – przyczynek empiryczny[97]

W celu dokonania pomocniczej analizy zawartości mediów pod kątem tematów biopolitycznych wykorzystano narzędzia przeznaczone do monitoringu mediów (zgodnie z wewnętrznymi definicjami tych narzędzi dotyczącymi wyszukiwania, filtrowania i klasyfikowania materiałów

[92] *Analiza i dekonstrukcja rosyjskich przekazów dezinformacyjnych…*

[93] Według definicji WHO infodemia to nadmiar informacji, w tym informacji nieprawdziwych lub wprowadzających w błąd, podczas epidemii (przyp. red.).

[94] G. Eysenbach, *How to fight an infodemic: the four pillars of infodemic management*, „Journal of Medical Internet Research" 2020, t. 22, nr 6, e21820.

[95] R. Kasprzyk, *Modelowanie i analiza procesu złośliwego sterowania ludźmi*, w: *CyberExpert 2021 – Metody i narzędzia w procesie tworzenia cyberzdolności Sił Zbrojnych RP – wyzwania i perspektywy*, Warszawa 2022, s. 9–28.

[96] J. Richards i in., *Introduction to the Special Issue section: Challenges for the state and international security – the current state and prognosis for the future*, „Security and Defence Quarterly" 2022, t. 37, nr 1, s. 1–3. https://doi.org/10.35467/sdq/147537.

[97] A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet…*

internetowych). Za pomocą BuzzSumo otrzymano zbiór materiałów opublikowanych w mediach o dużym zasięgu (zgodnie z definicją tego narzędzia) w postaci pasywnych stron internetowych nadawców tradycyjnych i portali internetowych (forma tekstowa) oraz materiałów wideo (forma audiowizualna), tj. opublikowanych w tzw. mediach kontentowych, bez rozróżniania typu medium. Za pomocą Brand24 otrzymano wzmianki z podziałem na media społecznościowo-kontentowe i media niespołecznościowe. Dzięki akademickiemu kontu do API zebrano posty z Twittera. Za pomocą narzędzia Google Trends otrzymano relatywne dzienne zliczenia wyszukiwań poszczególnych fraz w Google. Po przeanalizowaniu kontentu w języku polskim opublikowanego między 24 lutego a 1 sierpnia 2022 r. pod kątem występowania w treści haseł „biolab", „broń biologiczna" i ich wariantów znaleziono 65 artykułów i multimediów zamieszczonych na stronach internetowych mediów tradycyjnych, tj. radia, telewizji, prasy, i w pasywnych portalach internetowych o największym zasięgu oraz 396 tweetów. Aż 41% wzmianek w mediach społecznościowo-kontentowych miało wydźwięk negatywny (głównie wyrażały one złość użytkowników sieci na Stany Zjednoczone i Ukrainę za prowadzenie „nielegalnych" badań czy lęk przed atakiem biologicznym na Polskę), co świadczy o silnym nacechowaniu emocjonalnym dyskursu. Warto podkreślić, że zainteresowanie polskiego społeczeństwa tematyką laboratoriów biologicznych oraz broni biologicznej (na podstawie zapytań w Google) było 2,6 razy większe niż w Rosji i dwa razy większe niż w Niemczech. Fale zainteresowania ściśle korelują z wrzutkami rosyjskiej propagandy (co było najbardziej widoczne w marcu 2022 r.). Szczyt tej aktywności w polskich mediach przypadł pomiędzy 9 a 24 marca 2022 r. (co stanowi mniej niż 10% całego przedziału czasowego). W tym okresie odnotowano aż 72% zapytań w Google, 49% artykułów na pasywnych stronach internetowych i w mediach kontentowych oraz 43% tweetów. Wynika z tego, że oddziaływanie Kremla na polskie społeczeństwo odniosło skutek w tym sensie, że wywołało falę zainteresowania.

W okresie pomiędzy 24 lutego a 1 sierpnia 2022 r. został przeprowadzony za pomocą tych samych narzędzi i w odniesieniu do tych samych mediów również monitoring kontentu w języku polskim pod kątem występowania w treści takich fraz, jak „głód", „bezpieczeństwo żywnościowe", wraz z ich wariantami. Znaleziono 958 artykułów i multimediów oraz 59 453 tweety. Jedynie 33% wzmianek w mediach niespołecznościowych i społecznościowych było nacechowane negatywnie. Może to wynikać

z tego, że dyskusja prowadzona za pośrednictwem tych mediów była wielowątkowa, a jeden z wątków dotyczył wsparcia udzielonego latem 2022 r. holenderskim rolnikom przez polskich rolników (efekt jedności[98]) i wydźwięk tych materiałów był pozytywny. W przypadku głodu występował w miarę równy poziom zainteresowania. Ciekawe jest to, że cyfrowe media tradycyjne lekko wzmożone zainteresowanie tematem zanotowały między 24 kwietnia a 23 maja 2022 r. (np. dyskusje o wywozie produktów żywnościowych z Ukrainy). Najwięcej wyszukiwań (o 13% więcej niż średnia) w Google miało miejsce między 24 lutego a 14 kwietnia 2022 r. (objaw lęku związanego z początkiem wojny), ponadprzeciętne zainteresowanie na pasywnych stronach internetowych i na portalach internetowych oraz w mediach kontentowych odnotowano pomiędzy 23 maja a 24 czerwca 2022 r. (dyskusja na temat ukraińskiego zboża i roli Polski w transporcie), a wzmożoną aktywność na Twitterze między 4 a 14 lipca 2022 r. (duża część tweetów odnosiła się do protestów rolniczych w Holandii i negocjacji dotyczących dostępu do ukraińskiego zboża w Polsce lub poprzez odblokowanie portów w Odessie), co świadczy o zróżnicowanej dynamice zainteresowania w targetach różnych mediów. Warto podkreślić, że powszechny lęk przed kryzysem żywnościowym i drożyzną produktów spożywczych w Polsce wygasł już w kwietniu 2022 r.[99] W związku z tym wydaje się, że kremlowska propaganda w pierwszej fazie konfliktu w Ukrainie podsycała lęk przed drożyzną żywności, a później przeniosła akcent na potencjalne zagrożenie polskiego rolnictwa z powodu napływu taniej żywności z Ukrainy. Przyczyną znacznego wzrostu zainteresowania w mediach społecznościowych w lipcu 2022 r. były w dużym stopniu tematy związane z pojawieniem się w Polsce ukraińskiego zboża oraz z protestami solidarnościowymi z holenderskimi rolnikami przeciwko unijnym programom, takim jak Zielony Ład czy Od pola do stołu[100], prowadzonymi np. za pośrednictwem kont związanych z Agrounią.

---

98 A. Jarynowski i in., *Animal breeders protests in Polish Twitter*…

99 A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet*…

100 J. Barreiro Hurle i in., *Modelling environmental and climate ambition in the agricultural sector with the CAPRI model*, JRC Publications Repository, https://publications.jrc.ec.europa.eu/repository/handle/JRC121368 [dostęp: 7 VIII 2022].

Perspektywa krótkoterminowa (2022–2023)

W trakcie pisania artykułu (sierpień–październik 2022 r.) w Polsce obowiązywał stopień alarmowy zagrożenia terrorystycznego BRAVO i wydaje się, że zostanie on utrzymany do końca 2023 r., a być może nawet podniesiony. W związku z powyższym jest zalecane wzmożenie monitoringu, np. przez wywiady państw NATO, w środowiskach specjalistów (w tym personelu medycznego, weterynaryjnego, rolniczego) w kierunku radykalizacji bądź działań agenturalnych w Polsce i regionie europejskim[101]. Tym bardziej powinny być kontynuowane badania, z uwzględnieniem wymiaru bezpieczeństwa, nad społecznymi uwarunkowaniami pandemii i wojny, zwłaszcza pod kątem osób z zaangażowaniem śledzących aktualną sytuację. Można się spodziewać następujących zjawisk (wymieniono je w kolejności od najbardziej do najmniej prawdopodobnego):

- polaryzacji producentów żywności wobec reszty społeczeństwa. Warto podkreślić, że protesty rolników w Holandii (których bezpośrednim powodem było zobowiązanie do redukcji pogłowia bydła mięsnego i mlecznego będące elementem szerszego procesu związanego z wprowadzeniem programu Zielony Ład[102]) mogą być wykorzystywane przez ośrodki propagandy rosyjskiej do wzmacniania polaryzacji społecznej w ramach już istniejących linii konfliktu[103];
- dezinformacji na temat amerykańskich (z udziałem Polski[104]) laboratoriów biologicznych (np. wykorzystanie forum ONZ w celu zmniejszenia wiarygodności rządu amerykańskiego oraz sojuszników wśród ich własnych obywateli[105], a także uzyskanie wsparcia państw trzecich). To właśnie walka z obcą propagandą (zwłaszcza ze strony

[101] A. Jarynowski i in., *African Swine Fever – potential biological*...

[102] Redukowanie pogłowia bydła i trzody chlewnej jest jednym z celów międzynarodowej polityki w zakresie ograniczenia emisji gazów cieplarnianych. Działania na rzecz przeciwdziałania zmianom klimatu czy obrony praw zwierząt mają potencjał podwójnego zastosowania i mogą, choć nie muszą, zostać wykorzystane również we wrogich celach.

[103] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 71–92. https://doi.org/10.4467/27204383TER.22.019.16339.

[104] A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet*...

[105] G. Kessler, *How the right embraced Russian disinformation*...

Federacji Rosyjskiej i ISIS) została uznana za jeden z priorytetów badań nad terroryzmem w Polsce[106];
- nasilenia działań przeciwko infrastrukturze i łańcuchowi dostaw rolniczych (np. z wykorzystaniem organizacji proekologicznych);
- zawleczeń patogenów roślin lub zwierząt na obszary wolne od choroby (np. możliwy jest przeskok ASF do Holandii, co może jeszcze bardziej nasilić protesty).

W związku z tym, że narzędzie destabilizacyjne w postaci agroterroryzmu jest stosunkowo łatwo dostępne, przede wszystkim należy zadać pytanie o to, jakie cele taktyczne lub operacyjne, mogące być elementem działań na poziomie strategicznym, wrogi kraj, np. Rosja, może za jego pomocą osiągnąć. Wachlarz działań agroterrorystycznych jest bardzo szeroki i nie ogranicza się tylko do czynników biologicznych[107]. Możliwe jest wykorzystanie na przykład wirusa komputerowego, aby doprowadzić do rozmrożenia strategicznych rezerw mięsa lub skażenia wody w rzekach nawadniających pola[108], czy też rozpylenie na pola w delcie Wisły substancji chemicznych za pomocą dronów wysłanych z Obwodu Kaliningradzkiego[109]. W krajach o silnej pozycji rolnictwa, ale geostrategicznie postępujących bardzo ostrożnie wobec Rosji, takich jak Holandia, Francja, Włochy, Niemcy i Hiszpania, agroterroryzm wspierany dez- i misinformacją może być wykorzystany do wywołania niepokojów społecznych nakłaniających rządy tych krajów do wywierania nacisku, aby Ukraina zakończyła wojnę. Niestety, w związku z potencjalną eskalacją sytuacji na Bliskim Wschodzie i zagrożeniem związanym z fundamentalizmem islamskim w Europie Zachodniej możliwe są zamachy z wykorzystaniem tzw. mikrobiologii kuchennej (czynniki agroterrotystyczne wydają się w tym przypadku najlepszym środkiem dla małych organizacji i samotnych wilków). Za to w krajach otwarcie wspierających Ukrainę, takich jak Polska, kraje bałtyckie i nordyckie, Czechy,

---

[106] D. Szlachter, *Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych (skrócony raport)*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 153–168. https://doi.org/10.4467/27204383TER.22.022.16342.

[107] S. Maksymowicz, *Atak biologiczny i agroterrorystyczny na Polskę*...

[108] A. Jarynowski, *Katastrofa na Odrze ukazała dysfunkcjonalność działania instytucji państwa*, Nowa Konfederacja, 22 VIII 2022 r., https://nowakonfederacja.pl/katastrofa-na-odrze-ukazala-dysfunkcjonalnosc-dzialania-instytucji-panstwa/ [dostęp: 7 VIII 2022].

[109] A. Jarynowski, *Disconnecting the Kaliningrad oblast and new threats from Polish perspective*, „Bre Reviews" 2022, nr 3, https://sites.utu.fi/bre/disconnecting-the-kaliningrad-oblast-and-new-threats-from-polish-perspective/ [dostęp: 7 VIII 2022].

Słowacja, Mołdawia, Rumunia oraz Wielka Brytania, ważniejszym celem mogłoby być zachwianie bezpieczeństwa żywnościowego i długofalowe ograniczenie zdolności produkcyjnych w tym zakresie. Należy również uważnie przyglądać się zdolnościom i celom Chin w ramach wojny hybrydowej z USA i ich sojusznikami, gdyż w ostatnich latach wzrosło tam tempo rozwoju w dziedzinie biotechnologii, a w sposób jeszcze bardziej zdecydowany – w dziedzinie bioinformatyki (dzięki uczeniu maszynowemu i sztucznej inteligencji[110]). Postęp biotechnologiczny został poniekąd wymuszony wcześniejszymi ogniskami epidemicznymi, jakich doświadczały Chiny (m.in. SARS-CoV-1 w latach 2002–2003, grypa A/H5N1 w latach 2003–2006).

Perspektywa średnioterminowa (kilka najbliższych lat)

Pandemia COVID-19 przyczyniła się do dużego wzrostu wiedzy i rozwoju technologii przeznaczonych do zwalczania chorób zakaźnych, ale jednocześnie ta sama wiedza i te same technologie mogą zostać wykorzystane do celowej introdukcji patogenów. Do tej pory bioterroryzm był domeną organizacji mających odpowiednie zasoby finansowe, a przede wszystkim specjalistów i laboratoria, jak również jednostek o dużej inteligencji, potrafiących skonstruować domowe laboratorium[111]. Obecnie próg jest zdecydowanie niższy, gdyż nastąpiła rewolucja w dostępności do informacji i technologii. Czynniki biologiczne uzyskały status „broni masowego rażenia dla ubogich", ze względu na łatwość pozyskania (znajomość podstaw mikrobiologii i patogenezy), weryfikacji czynnika zakaźnego (dostęp do diagnostyki) i introdukcji (znajomość podstaw epidemiologii, takich jak drogi transmisji).

Ciekawy jest paradoks Polski jako państwa, w którym zatrudnienie w przemyśle rolno-spożywczym (15%) i usługach żywieniowych lub handlu żywnością (10%) sięga łącznie 25%[112], a poziom zainteresowania chorobami zakaźnymi zwierząt czy roślin i wiedzy o nich jest wśród mieszkańców

[110] V. Bergengruen, *Tech Leaders Warn the U.S. Military Is Falling Behind China on AI*, Time, 18 VII 2023 r., https://time.com/6295586/military-ai-warfare-alexandr-wang/ [dostęp: 15 VIII 2023].

[111] M. Dąbrowski, *Koronawirus, broń biologiczna a wojsko (opinia)*, Defence 24, 15 III 2020 r., https://defence24.pl/sily-zbrojne/koronawirus-bron-biologiczna-a-wojsko-opinia [dostęp: 8 VIII 2022].

[112] M. Kędzierski, *Integracja czy połączenie*...

miast w Polsce jednym z najniższych w UE (np. w konkretnym przypadku, dla którego są zebrane dane międzynarodowe, czyli wiedzy o antybiotykach[113]). To oznacza, że z jednej strony jest budowana specjalistyczna wiedza osobno o bioterroryzmie i o bezpieczeństwie żywnościowym, jednak brakuje interdyscyplinarnego podejścia do agroterroryzmu w szerokim jego rozumieniu – biologicznym, rolniczym, społecznym, ekonomicznym czy politycznym. Sytuacja z katastrofą ekologiczną na Odrze latem 2022 r. pokazała służbom innych krajów, jakie są słabe punkty bezpieczeństwa Jednego zdrowia w Polsce[114], pozwalając na stworzenie scenariuszy ataków wykazujących nieefektywność działania polskich służb[115]. W walce z rozprzestrzenianiem się chorób zagrażających Jednemu zdrowiu najważniejsze są wczesna identyfikacja i natychmiastowe alarmowanie o każdym nietypowym zdarzeniu. Katastrofa na Odrze unaoczniła, że szybka diagnoza i reakcja adekwatna do zagrożenia mogą stanowić słaby punkt regionalnych inspekcji Jednego zdrowia (tj. Państwowej Inspekcji Sanitarnej, Inspekcji Weterynaryjnej, Inspekcji Ochrony Roślin i Nasiennictwa, Inspekcji Farmaceutycznej, Inspekcji Ochrony Środowiska).

Stawia to zupełnie nowe wyzwania przed grupami dyspozycyjnymi[116], gdyż do tej pory bioterroryzm mógł zostać wybrany tylko przez niewielki odsetek radykalistów, a obecnie liczba osób, które zdobyły odpowiednie kompetencje, może być nawet o rząd wielkości większa. Właściwie nie kompetencje stanowią teraz barierę, lecz motywacje. W związku z tym zalecany monitoring środowisk specjalistów (w tym personelu biomedycznego jak do tej pory), prowadzony np. przez wywiady państw NATO, wydaje się już niewystarczający i konieczne jest rozszerzenie tej grupy o środowiska weterynaryjne, rolnicze i inne (zwłaszcza że nie wiadomo, w jaki sposób zakończy się wojna w Ukrainie), gdyż zupełnie nowi nieprofesjonalni aktorzy uzyskali potencjał wystarczający do przeprowadzenia skutecznej introdukcji zakażenia na nowy obszar. W przypadku zagrożeń hybrydowych ze strony takich państw jak Rosja mogą zostać wybrane cele

[113] Na przykład seria pytań Q5 w: *Special Eurobarometer: Antimicrobial resistance (in the EU)*, Directorate General for Communication, European Union, 2018 r., https://data.europa.eu/data/datasets/s2190_90_1_478_eng?locale=en [dostęp: 26 VI 2023].

[114] A. Jarynowski, *Katastrofa na Odrze*...

[115] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych*..., s. 80.

[116] A. Kołodziejczyk, J. Maciejewski, P. Pieńkowski, *Grupy dyspozycyjne w dobie pandemii Covid-19*, XVIII Zjazd Socjologiczny, Warszawa, 2022 r., https://zjazdpts.pl/grupy/grupy-dyspozycyjne-w-dobie-pandemii-covid-19/ [dostęp: 2 XI 2022].

miękkie (jak to zazwyczaj czyniły organizacje islamskie), a nie jak do tej pory obiekty infrastruktury krytycznej czy wojskowej[117].

Wciąż jednak pozostają zagadnienia oraz czynniki warunkujące oblicza agroterroryzmu w Polsce i regionie europejskim, o których w tym artykule nie napisano. W odniesieniu do zjawiska agroterroryzmu są podejmowane działania kompensacyjne (np. działania operacyjne służb wobec mediów jawnie prokremlowskich propagujących negacjonizm biologiczny czy rozpracowywanie środowisk radykalnych) i zachodzą procesy konkurencyjne (np. z upływem czasu wiedza nabyta w trakcie pandemii ulega zapominaniu, a w związku z tym kapitał kompetencyjny może się zmniejszać). Państwa i organizacje postawiły na nabycie odporności i będą bardziej przygotowane na zwalczanie chorób zakaźnych (oraz mogącego im towarzyszyć zjawiska infodemii)[118]. Z jednej strony rozwój wiedzy i technologii sprzyja zjawisku bioterroryzmu, z drugiej jednak pozwala lepiej się przed nim chronić. Przyszłość pokaże, które procesy będą zachodzić szybciej.

Podsumowanie i rekomendacje

W zależności od zastosowanej metody za pomocą agroterroryzmu można osiągnąć cel taktyczny (np. wywołać protesty) lub operacyjny (np. spowodować duże straty w gospodarce). Z tej „broni masowego rażenia dla biednych" może korzystać mała grupa terrorystów, a nawet jedna zdeterminowana osoba, która ma wykształcenie rolnicze, weterynaryjne czy biomedyczne bądź w czasie pandemii nabyła podstawową wiedzę mikrobiologiczno-epidemiologiczną oraz jest zdolna do zrozumienia artykułów naukowych i informacji opublikowanych w internecie, a także do zastosowania tej wiedzy w praktyce[119]. Bronią jest dopiero połączenie czynnika biologicznego ze środkiem jego przenoszenia czy transportu, a w przypadku działań samotnych wilków mieszkających na obszarze, na którym chcą dokonać zamachu, często zaawansowana wiedza

[117] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych...*, s. 84.

[118] *Germany open Hub for Pandemic and Epidemic Intelligence in Berlin*, World Health Organisation, 1 IX 2021 r., https://www.who.int/news/item/01-09-2021-who-germany-open-hub-for-pandemic-and-epidemic-intelligence-in-berlin [dostęp: 12 VIII 2022].

[119] A. Jarynowski i in., *ASF jako zagrożenie biologiczne w Polsce*...

inżynieryjna i techniczna nie jest potrzebna. Ze względu na znaczenie bezpieczeństwa biologicznego (co udowodniła m.in. pandemia COVID-19) oraz bezpieczeństwa żywnościowego (zwłaszcza że eksport żywności stanowi znaczny wkład w PKB Polski) sensu largo (wraz z PSYOPS i INFOOPS), to zagadnienia te powinny być wzięte pod uwagę podczas prac przy kolejnych edycjach Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[120].

Najważniejsze wnioski i rekomendacje płynące z przeprowadzonej analizy to:

1. Celowe wprowadzenie patogenów zwierzęcych lub roślinnych na teren wolny od choroby było stosunkowo proste, a obecnie stało się jeszcze prostsze[121].
2. Ze względu na kryzys żywnościowy i wojnę w Ukrainie zagrożenie agroterroryzmem jest obecnie największe od czasu podpisania konwencji o zakazie broni biologicznej. Po odblokowaniu portów w Odessie zagrożenie to zmalało, ale w przypadku ich ponownego zablokowania problem może powrócić – zarówno w wymiarze rzeczywistym, jak i medialnym.
3. Polska, kraje nordyckie, kraje bałtyckie i Wielka Brytania wydają się najbardziej narażone na działania ze strony Kremla, a Niemcy i Francja na działania ISIS (w związku z tym mogą zostać zastosowane inne scenariusze introdukcji).
4. Należy wzmóc (zwłaszcza w nadchodzących latach) czujność producentów żywności i lekarzy weterynarii czy specjalistów ochrony roślin i ich zainteresowanie potencjalnymi zagrożeniami agroterrorystycznymi.
5. Warto przeprowadzić ćwiczenia i symulacje na podstawie prawdopodobnych scenariuszy introdukcji (np. wprowadzenie ASF w Holandii, FMD w Wielkopolsce czy agrofagów jabłek na Lubelszczyźnie) w paradygmacie działania hybrydowego[122], z wykorzystaniem gotowych scenariuszy introdukcji[123].

---

[120] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 13 III 2023].

[121] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era*...

[122] A. Jarynowski, Ł. Krzowski, V. Belik, *Afrykański pomór świń*...

[123] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych*..., s. 80.

6. Należy rozwinąć system stałej obserwacji mediów tradycyjnych i społecznościowych w celu monitorowania potencjalnego oddziaływania propagandy kremlowskiej oraz wykrycia w czasie rzeczywistym (ang. *real-time*) aktorów z nią rezonujących[124].
7. Należy stworzyć system monitorowania ryzyka radykalizacji w zawodach weterynaryjnych i rolniczych oraz wśród nowej kategorii profesjonalistów postpandemicznych.
8. Należy upowszechnić wykorzystanie wiarygodnych, tj. opartych na dowodach naukowych[125], narzędzi do oceny ryzyka, np. Grunow & Finke (ang. *The Grunow-Finke tool*, GFT)[126] czy Indeks rolniczy (ang. *Agricultural Index*)[127].

Bibliografia

Bertrandt J., *Bioterroryzm żywnościowy – realne zagrożenia użycia patogenów biologicznych w działaniach terrorystycznych*, „Lekarz Wojskowy" 2007, t. 8, nr 1, s. 33–35.

Broniatowski D. i in., *Vaccine Communication as Weaponized Identity Politics*, „American Journal of Public Health" 2020, t. 110, nr 5, s. 1378–1384. https://doi.org/10.2105/ajph.2020.305616.

Chen X., Chughtai A.A., MacIntyre C.R., *Recalibration of the Grunow–Finke assessment tool to improve performance in detecting unnatural epidemics*, „Risk Analysis" 2019, t. 39, nr 7, s. 1465–1475.

EFSA Panel on Plant Health (PLH), *Pest categorisation of Colletotrichum fructicola*, „EFSA Journal" 2021, t. 19, nr 8, e06803. https://doi.org/10.2903/j.efsa.2021.6803.

[124] A. Jarynowski, *Dyskurs antyszczepionkowy i koronasceptyczny a prokremlowska propaganda w niemieckim Twitterze*, Blog Zdrowia Publicznego, 22 V 2022 r., https://izp.wnz.cm.uj.edu.pl/pl/blog/publikacja-dyskurs-antyszczepionkowy-i-koronascpetyczny-a-prokremlowska-propaganda-w-niemieckim-twitterze/ [dostęp: 7 VIII 2022].

[125] A. Jarynowski, *Agro/bio-terrorism in Europe?*...

[126] X. Chen, A.A. Chughtai, C.R. MacIntyre, *Recalibration of the Grunow–Finke assessment tool to improve performance in detecting unnatural epidemics*, „Risk Analysis" 2019, t. 39, nr 7, s. 1465–1475.

[127] R. Sequeira, *Safeguarding production agriculture and natural ecosystems against biological terrorism: A U.S. Department of Agriculture emergency response framework*, „Annals of the New York Academy of Sciences" 1999, t. 894, nr 1, s. 48–69. https://doi.org/10.1111/j.1749-6632.1999.tb08043.x.

Essack S.Y., *Environment: the neglected component of the One Health triad*, „The Lancet Planetary Health" 2018, t. 2, nr 6, e238–e239. https://doi.org/10.1016/S2542-5196(18)30124-4.

European Food Safety Authority (EFSA), *Update of the Xylella spp. host plant database – systematic literature search up to 31 December 2021*, „EFSA Journal" 2022, t. 20, nr 6, e07356. https://doi.org/10.2903/j.efsa.2022.7356.

Eysenbach G., *How to fight an infodemic: the four pillars of infodemic management*, „Journal of Medical Internet Research" 2020, t. 22, nr 6, e21820. https://doi.org/10.2196/21820.

Helmus T. i in., *Russian social media influence: Understanding Russian propaganda in Eastern Europe*, Santa Monica 2018.

Jarynowski A., *Infodemiologia oraz infonadzór – doświadczenia doby pandemii*, w: *Epidemiologia i bezpieczeństwo CBRN. Nauka, innowacje, implikacje praktyczne*, A. Mróz-Jagiełło, J. Walczak (red.), seria: Epimilitaris, Zielonka 2022, s. 235–248.

Jarynowski A. i in., *African Swine Fever Awareness in the Internet Media in Poland – exploratory review*, „E-methodology" 2019, t. 6, nr 6, s. 100–115. https://doi.org/10.15503/emet2019.100.115.

Jarynowski A. i in., *ASF jako zagrożenie biologiczne w Polsce i na świecie*, w: *Bezpieczeństwo regionalne. Węzłowe problemy i procesy*, P. Bajor (red.), Kraków 2021, s. 239–254. https://doi.org/10.12797/9788381383899.14.

Jarynowski A., Krzowski Ł., Belik V., *Afrykański pomór świń: epizootiologia, ekonomia i zarządzanie kryzysowe w kontekście naturalnego bądź intencjonalnego wprowadzenia*, „Studia Administracji i Bezpieczeństwa" 2021, t. 11, nr 11, s. 129–153. http://dx.doi.org/10.5604/01.3001.0015.6752.

Jarynowski A., Płatek D., *Sentiment analysis, topic modelling and social network analysis. COVID-19, protest movements and the Polish Tweetosphere*, w: *The Covid-19 Pandemic as a Challenge for Media and Communication Studies*, London 2022. https://doi.org/10.4324/9781003232049-21.

Jarynowski A., Stochmal M., Maciejewski J., *Przegląd i charakterystyka prowadzonych w Polsce badań na temat społecznych uwarunkowań epidemii COVID-19 w jej początkowej fazie*, „Bezpieczeństwo. Obronność. Socjologia" 2020, t. 13, s. 38–87.

Jarynowski A., Wójta-Kempa M., Płatek D., Czopek K., *Attempt to understand public health relevant social dimensions of COVID-19 outbreak in Poland*, „Society Register" 2020, t. 4, nr 3, s. 7–44. https://doi.org/10.14746/sr.2020.4.3.01.

Jedno zdrowie. Ludzie i inne gatunki, H. Mamzer, P. Białas (red. nauk.), Wrocław 2022.

Jemielniak D., Krempovych Y., *An analysis of AstraZeneca COVID-19 vaccine misinformation and fear mongering on Twitter*, „Public Health" 2021, t. 200, s. 4–6. https://doi.org/10.1016/j.puhe.2021.08.019.

Karimzadeh S., Bhopal R., Nguyen Tien H., *Review of infective dose, routes of transmission and outcome of COVID-19 caused by the SARS-COV-2: comparison with other respiratory viruses*, „Epidemiology and Infection" 2021, t. 149, e96. https://doi.org/10.1017/S0950268821000790.

Kasprzyk R., *Modelowanie i analiza procesu złośliwego sterowania ludźmi*, w: *CyberExpert 2021 – Metody i narzędzia w procesie tworzenia cyberzdolności Sił Zbrojnych RP – wyzwania i perspektywy*, Warszawa 2022, s. 9–28.

Keremidis H. i in., *Historical Perspective on Agroterrorism: Lessons Learned from 1945 to 2012*, „Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science" 2013, t. 11, s. 17–24. https://doi.org/10.1089/bsp.2012.0080.

Kiriya I., *From "Troll Factories" to "Littering the Information Space": Control Strategies Over the Russian Internet*, „Media and Communication" 2021, t. 9, nr 4, s. 16–24. https://doi.org/10.17645/mac.v9i4.4177.

Leitenberg M., Zilinskas R.A., *The Soviet biological weapons program: A history*, Cambridge 2012.

Lenda M. i in., *Effect of the internet commerce on dispersal modes of invasive alien species*, „PLoS ONE" 2014, t. 9, nr 6, p.e99786. https://doi.org/10.1371/journal.pone.0099786.

Lenda M. i in., *Misinformation, internet honey trading and beekeepers drive a plant invasion*, „Ecology Letters" 2021, t. 24, nr 2, s. 165–169. https://doi.org/10.1111/ele.13645.

Lipa J., *Agroterroryzm – wyzwaniem dla kwarantanny i ochrony roślin*, „Progress in Plant Protection" 2006, t. 46, nr 1, s. 162–168.

Lipińska A., *Chińskie operacje w dobie COVID-19. Dezinformacja – metody, dziedziny i ewolucja*, „Cyber Security and Law" 2022, t. 7, nr 1, s. 61–71.

Maciejewski J., *Grupy dyspozycyjne w systemie bezpieczeństwa państwa*, XXIII Międzynarodowe Seminarium z cyklu „Metodologia badań systemów społecznych", Wrocław, 7 IV 2022 r.

MacIntyre R.C. i in., *Converging and emerging threats to health security*, „Environment Systems and Decisions" 2018, t. 38, nr 2, s. 198–207. https://doi.org/10.1007/s10669-017-9667-0.

Mamzer H., *Choroba jako zjawisko społeczne. Analiza walki z afrykańskim pomorem świń*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2020, t. 82, nr 2, s. 281–297. https://doi.org/10.14746/rpeis.2020.82.2.19.

Piekarski M., *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 71–92. https://doi.org/10.4467/27204383TER.22.019.16339.

Richards J., Świeboda H., Gębska M., *Introduction to the Special Issue section: Challenges for the state and international security – the current state and prognosis for the future*, „Security and Defence Quarterly" 2022, t. 37, nr 1, s. 1–3. https://doi.org/10.35467/sdq/147537.

Sequeira R., *Safeguarding production agriculture and natural ecosystems against biological terrorism: A U.S. Department of Agriculture emergency response framework*, „Annals of the New York Academy of Sciences" 1999, t. 894, nr 1, s. 48–69. https://doi.org/10.1111/j.1749-6632.1999.tb08043.x.

Szlachter D., *Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych (skrócony raport)*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 148–176. https://doi.org/10.4467/27204383TER.22.022.16342.

Wiśniewska M., *The food terrorism – the essence and the methods of systemic defense*, „Journal of Modern Science" 2023, t. 50, nr 1, s. 331–349. https://doi.org/10.13166/jms/161535.

Literatura rosyjska i ukraińska

Кириллов И., *Тезисы брифинги начальника войск радиационной, химической и биологической защиты ВС РФ генерал-лейтенанта Игоря Кириллова* (materiał Ministerstwa Obrony Federacji Rosyjskiej zebrany przez autora z kanału Telegram, dostępny na prośbę e-mailową).

Стегній Б., Герилович А., Бузун А., *Африканська чума свиней: історія, сьогоденна та перспективи*, Київ 2015.

Жиганова Л.П., *Биотерроризм и агротерроризм – реальная угроза биобезопасности общества*, „США и Канада: экономика, политика, культура" 2004, t. 417, nr 9, s. 3–25.

Źródła internetowe

Analiza i dekonstrukcja rosyjskich przekazów dezinformacyjnych oraz propagandowych na temat Polski i Polaków, 2022 r., https://infowarfare.pl/realizowane-projekty/ [dostęp: 25 VI 2023].

Barreiro Hurle J. i in., *Modelling environmental and climate ambition in the agricultural sector with the CAPRI model*, JRC Publications Repository, https://publications.jrc.ec.europa.eu/repository/handle/JRC121368 [dostęp: 7 VIII 2022].

Belik V., Jarynowski A., *Elucidating the interplay of COVID-19 epidemic and social dynamics via Internet media in Germany*, konferencja on-line „Preparedness for future pandemics from a global perspective", 15 XI 2021 r., https://zenodo.org/record/6400773#.ZGRny3ZByUk [dostęp: 7 VIII 2022].

Bergengruen V., *Tech Leaders Warn the U.S. Military Is Falling Behind China on AI*, Time, 18 VII 2023 r., https://time.com/6295586/military-ai-warfare-alexandr-wang/ [dostęp: 15 VIII 2023].

Bezpieczeństwo żywnościowe, K. Mordzak (oprac.), Wrocław 2021, https://www.wojsko-polskie.pl/awl/u/50/d4/50d46baf-332b-4acb-aeb3-8f5b17777590/bezpieczenstwo_zywnosciowe.pdf [dostęp: 7 VIII 2022].

Black Sea Grain Initiative, Wikipedia, https://en.wikipedia.org/wiki/Black_Sea_Grain_Initiative [dostęp: 7 VIII 2022].

Broń masowego rażenia, broń biologiczna, broń chemiczna, broń jądrowa. Cz. 2, K. Mordzak (oprac.), Wrocław 2019, https://www.wojsko-polskie.pl/awl/u/96/0c/960cad22-5698-4356-b8f5-38117fb19499/bron_cbn.pdf [dostęp: 7 VIII 2022].

Building resilience against agro-crime and agro-terrorism, World Organisation for Animal Health, https://www.woah.org/en/document/building-resilience-against-agro-crime-and-agro-terrorism/ [dostęp: 5 III 2023].

Clement S., *Biological Threats: Technological Progress and the Spectre of Bioterrorism in the Post-Covid-19 Era*, https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-01/024%20STCTTS%2021%20E%20rev.%201%20fin%20-%20%20BIOLOGICAL%20THREATS.pdf [dostęp: 8 VIII 2022].

Cwynar P., *Bioterroryzm – syllabus*, Uniwersytet Przyrodniczy we Wrocławiu, 2021 r., https://sylabus.upwr.edu.pl/pl/document/7562fe08-5a02-4db5-8d31-d7144fdd99bb.pdf [dostęp: 1 XI 2022].

Debata Bezpieczeństwo żywnościowe Europy w świetle nadchodzących wyzwań, https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/ [dostęp: 2 XI 2022]. Materiał został przeniesiony do archiwum: https://web.archive.org/web/20221104152532/https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/.

EEAS, *Short assessments of narratives and disinformation around the Covid-19 pandemic (update December 2020 - April 2021)*, EUvsDisinfo, 28 IV 2021 r., https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021 [dostęp: 7 VIII 2022].

Dąbrowski M., *Koronawirus, broń biologiczna a wojsko*, Defence 24, 15 III 2020 r., https://defence24.pl/sily-zbrojne/koronawirus-bron-biologiczna-a-wojsko-opinia [dostęp: 7 VIII 2022].

Deter A., *50 vermummte Aktivisten blockieren Bocholter Schlachthof*, Topagrar, 20 VI 2022 r., https://www.topagrar.com/schwein/news/aktivisten-blockieren-bocholter-schlachthof-13131573.html [dostęp: 7 VIII 2022].

Duplaga M., *Znaczenie kompetencji zdrowotnych w świecie infodemii*, Instytut Zdrowia Publicznego, https://izp.wnz.cm.uj.edu.pl/pl/blog/projekt-znaczenie-kompetencji-zdrowotnych-w-swiecie-infodemii/ [dostęp: 7 VIII 2022].

Germany open Hub for Pandemic and Epidemic Intelligence in Berlin, World Health Organisation, 1 IX 2021 r., https://www.who.int/news/item/01-09-2021-who-germany-open-hub-for-pandemic-and-epidemic-intelligence-in-berlin [dostęp: 12 VIII 2022].

Jarynowski A., *Agro/bio-terrorism in Europe? Analysis of selected suspicious biological events (significant from the One Health perspective) after 24.02.2022*, prezentacja, NATO BioMed Panel, 25 X 2022 r., http://interdisciplinary-research.eu/wp-content/uploads/2022/10/agro_BIOTERRORISM_aj_warsaw_2022.pdf [dostęp: 2 XI 2022].

Jarynowski A., *Disconnecting the Kaliningrad oblast and new threats from Polish perspective*, „Bre Reviews" 2022, nr 3, https://sites.utu.fi/bre/disconnecting-the-kaliningrad-oblast-and-new-threats-from-polish-perspective/ [dostęp: 7 VIII 2022].

Jarynowski A., *Dyskurs antyszczepionkowy i koronascpetyczny a prokremlowska propaganda w niemieckim Twitterze*, Blog Zdrowia Publicznego, 22 V 2022 r., https://izp.wnz.cm.uj.edu.pl/pl/blog/publikacja-dyskurs-antyszczepionkowy-i-koronascpetyczny-a-prokremlowska-propaganda-w-niemieckim-twitterze/ [dostęp: 7 VIII 2022].

Jarynowski A., *Katastrofa na Odrze ukazała dysfunkcjonalność działania instytucji państwa,* „Nowa Konfederacja", 22 VIII 2022 r., https://nowakonfederacja.pl/katastrofa-na-odrze-ukazala-dysfunkcjonalnosc-dzialania-instytucji-panstwa/ [dostęp: 2 XI 2022].

Jarynowski A., *Pro-Kremlin German Twitter users are more likely to be involved in both anti-lockdown and anti-vaccine discourse than Anti-Kremlin users,* preprint, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4079045 [dostęp: 7 VIII 2022]. https://dx.doi.org/10.2139/ssrn.4079045.

Jarynowski A., *(Re-)Emergence of agroterrorism during the food crisis,* prezentacja, NATO Centre of Excellence for Military Medicine, 20 VII 2022 r., https://zenodo.org/record/6969341 [dostęp: 2 XI 2022].

Jarynowski A., Belik V., *African Swine Fever (ASF) Virus propagation in Poland (Spatio-temporal analysis),* preprint, https://www.researchgate.net/publication/338436134_African_Swine_Fever_ASF_Virus_propagation_in_Poland_Spatio-temporal_analysis [dostęp: 7 VIII 2022]. https://doi.org/10.13140/RG.2.2.29807.6167.

Jarynowski A., Belik V., *Spatio-temporal analysis of African Swine Fever Spread in Poland with network perspective,* preprint, https://www.academia.edu/43262326/Multilayer_network_approach_to_African_Swine_Fever_Spread_in_Poland [dostęp: 12 VIII 2022].

Jarynowski A., Grabowski A., *Modelowanie epidemiologiczne dedykowane Polsce,* Portal CZM, 2015 r., http://www.czm.mif.pg.gda.pl/wp-content/uploads/fam/publ/jarynowski2.pdf [dostęp: 7 VIII 2022].

Jarynowski A. i in., *African Swine Fever – potential biological warfare threat,* preprint, https://easychair.org/publications/preprint/vjFf [dostęp: 7 VIII 2022].

Jarynowski A. i in., *Animal breeders protests in Polish Twitter - preliminary research,* preprint, http://interdisciplinary-research.eu/wp-content/uploads/2022/04/animal_related_protests_in_twitter_preprint_pdf.pdf [dostęp: 7 VIII 2022].

Jarynowski A., Krzowski Ł., *BIO (AGRO) Terrorism/Crime in post-covid era in context of massive scale dissemination of microbiology/epidemiology knowledge,* „DiMiMED – International Conference on Disaster and Military Medicine", Düsseldorf, 15–16 XI 2021 r., https://events.military-medicine.com/media/landingpage/25/attachment-1639063402.pdf [dostęp: 7 VIII 2022].

Jarynowski A., Krzowski Ł., Maksymowicz S., *Biological mis(dis)-information in the Internet as a possible Kremlin warfare* (wersja robocza), https://zenodo.org/record/8081493 [dostęp: 26 VI 2023].

Jarynowski A., Lopez-Nunez F., Fan H., *How network temporal dynamics shape a mutualistic system with invasive species?*, preprint, https://arxiv.org/ftp/arxiv/papers/1407/1407.4334.pdf [dostęp: 7 VIII 2022]. https://doi.org/10.48550/arXiv.1407.4334.

Jarynowski A., Semenov A., Belik V., *Perception of infectious diseases with animal and humans hosts on the Polish internet*, Proceedings of 20th Congress of the International Society for Animal Hygiene, Berlin, 5–7 X 2022 r., http://interdisciplinary-research.eu/wp-content/uploads/2022/08/Abstract-form-ISAH_jarynowski_corr.pdf [dostęp: 7 XI 2022].

Kessler G., *How the right embraced Russian disinformation about 'U.S. bioweapons labs' in Ukraine*, „The Washington Post", 11 III 2022 r., https://www.washingtonpost.com/politics/2022/03/11/how-right-embraced-russian-disinformation-about-us-bioweapons-labs-ukraine/ [dostęp: 7 VIII 2022].

Kędzierski M., *Integracja czy połączenie. Analiza możliwości zwiększenia efektywności działania inspekcji weterynaryjnej oraz ochrony roślin i nasiennictwa*, Europejski Fundusz Rozwoju Wsi Polskiej, https://efrwp.pl/publikacje/integracja-czy-polaczenie-analiza-mozliwosci-zwiekszenia-efektywnosci-dzialania-inspekcji-weterynaryjnej-oraz-ochrony-roslin-i-nasiennictwa/ [dostęp: 7 VIII 2022].

Kołodziejczyk A., Maciejewski J., Pieńkowski P., *Grupy dyspozycyjne w dobie pandemii Covid-19*, XVIII Zjazd Socjologiczny, Warszawa, 2022 r., https://zjazdpts.pl/grupy/grupy-dyspozycyjne-w-dobie-pandemii-covid-19/ [dostęp: 2 XI 2022].

Lentzow F., Littlewood J., *Russia finds another stage for the Ukraine "biolabs" disinformation show*, Bulletin of the Atomic Scientists, 8 VII 2022 r., https://thebulletin.org/2022/07/russia-finds-another-stage-for-the-ukraine-biolabs-disinformation-show/ [dostęp: 12 VIII 2022].

Maksymowicz S., *Atak biologiczny i agroterrorystyczny na Polskę. Jakie scenariusze są prawdopodobne?*, Nowa Konfederacja, 31 V 2022 r., https://nowakonfederacja.pl/atak-biologiczny-i-agroterrorystyczny-na-polske-jakie-scenariusze-sa-prawdopodobne/ [dostęp: 7 XI 2022].

Marek M., *Rosyjska dezinformacja w Polsce – cele i przekazy*, Centrum Badań nad Współczesnym Środowiskiem Bezpieczeństwa, 30 III 2022 r., https://infowarfare.pl/2022/03/30/rosyjska-dezinformacja-w-polsce-cele-i-przekazy/ [dostęp: 7 VIII 2022].

Monke J., *Agroterrorism: Threats and preparedness*, https://sgp.fas.org/crs/terror/RL32521.pdf [dostęp: 7 VIII 2022].

Normile D., *African swine fever keeps spreading in Asia, threatening food security*, „Science", 2019 r., https://www.science.org/content/article/african-swine-fever-keeps-spreading-asia-threatening-food-security [dostęp: 7 VIII 2022].

OiE, *Classification of diseases notifiable*, https://www.oie.int/en/animal-health-in-the-world/the-world-animal-health-information-system/old-classification-of-diseases-notifiable-to-the-oie-list-a/ [dostęp: 29 VII 2022].

Radziejewski B., *Widmo krąży po świecie. Widmo głodu*, Nowa Konfederacja, 25 V 2022 r., https://nowakonfederacja.pl/widmo-krazy-po-swiecie-widmo-glodu/ [dostęp: 7 VIII 2022].

Special Eurobarometer: Antimicrobial resistance (in the EU), Directorate General for Communication, European Union, 2018 r., https://data.europa.eu/data/datasets/s2190_90_1_478_eng?locale=en [dostęp: 26 VI 2023].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 13 III 2023].

Tajemnicze nasiona w paczkach z Chin, Polsat News, 5 VIII 2020 r., https://www.polsatnews.pl/wiadomosc/2020-08-05/tajemnicze-nasiona-w-paczkach-z-chin-zidentyfikowano-14-gatunkow-roslin/ [dostęp: 7 VIII 2022].

What next for vaccine diplomacy?, „The Economist", 3 V 2021 r., https://www.eiu.com/n/campaigns/q2-global-forecast-2021/ [dostęp: 7 VIII 2022].

Wojskowe Ośrodki Medycyny Prewencyjnej, https://www.gov.pl/web/obrona-narodowa/wojskowe-osrodki-medycyny-prewencyjnej [dostęp: 2 III 2023].

W okresie ostatnich 48 godzin dynamicznie rośnie zagrożenie dezinformacyjne w tematyce wydarzeń #Ukraina #Rosja w polskiej przestrzeni internetowej, IBIMS, https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ [dostęp: 7 VIII 2022].

Xia Wei i in., *How One Pandemic Led To Another: Asfv, the Disruption Contributing To Sars-Cov-2 Emergence in Wuhan*, preprint, https://www.researchgate.net/publication/349628301_How_One_Pandemic_Led_To_Another_Asfv_the_Disruption_Contributing_To_Sars-Cov-2_Emergence_in_Wuhan [dostęp: 7 VIII 2022]. https://doi.org/10.20944/preprints202102.0590.v1.

Zarażone ASF dziki spadają z nieba? Mające być dowodem zdjęcie budzi poważne wątpliwości, Lublin112.pl, https://www.lublin112.pl/zarazone-asf-dziki-spadaja-nieba-majace-byc-dowodem-zdjecie-budzi-powazne-watpliwosci/ [dostęp: 7 VIII 2022].

Akty prawne

Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu, sporządzona w Moskwie, Londynie i Waszyngtonie dnia 10 kwietnia 1972 r. (DzU z 1976 r. nr 1 poz. 1).

Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r. (DzU z 1992 r. nr 41 poz. 175).

Protokół dotyczący zakazu używania na wojnie gazów duszących, trujących lub podobnych oraz środków bakterjologicznych (DzU z 1929 r. nr 28 poz. 278).

Dr Andrzej Jarynowski

Specjalista w zakresie modelowania rozprzestrzeniania się chorób zakaźnych. Interesuje się między innymi tematyką sieci kontaktów, Jednego zdrowia, telemedycyną, infodemiologią i bioterroryzmem. Współpracuje jako konsultant epidemiologiczny dla Europy Wschodniej z agencją Bloomberg, „The Washington Post", „Nową Konfederacją".

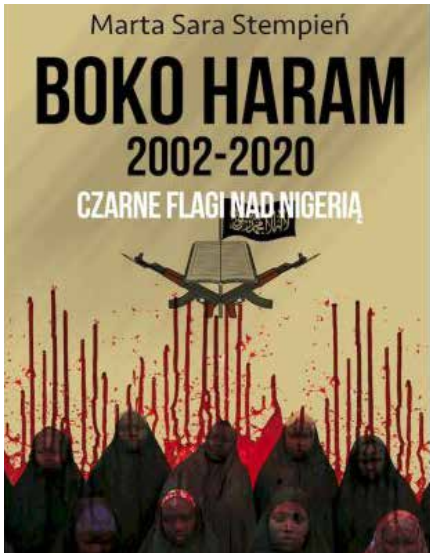
Kontakt: ajarynowski@gmail.com

RECENZJE

https://doi.org/10.4467/27204383TER.23.021.18323
https://orcid.org/0000-0001-9815-6035

KRZYSZTOF IZAK

Recenzja książki: Marta Sara Stempień, Boko Haram 2002–2020. Czarne flagi nad Nigerią[1]



W maju 2021 r. zginął Abu Bakr Szekau, charyzmatyczny przywódca Boko Haram (pol. Zachodnia Cywilizacja Jest Zakazana), jednej z najbardziej krwawych organizacji terrorystycznych, która pod względem liczby zabitych ludzi w drugiej dekadzie XXI w. ustępowała tylko Państwu Islamskiemu. Szekau zginął – zgodnie z jedną wersją – w wyniku ran odniesionych w walce z rywalizującą grupą Islamic State in West Africa Province, ISWAP (pol. Państwo Islamskie w Prowincji Afryka Zachodnia), znaną również

[1] M.S. Stempień, *Boko Haram 2002–2020. Czarne flagi nad Nigerią*, Warszawa–Siedlce 2020, Rytm, 206 s.

jako Wilajet Gharb Ifriqijja (pol. Prowincja Sudanu Zachodniego). Według innej wersji wysadził się w powietrze przy użyciu pasa szahida, dlatego też nie znaleziono jego zwłok. Potwierdziły się wówczas opinie, że członkowie Boko Haram przejdą do ISWAP, z którym organizacja połączyła się w 2015 r. Później jednak przez różnice ideologiczne ich drogi się rozeszły, a następnie doszło do konfliktu zakończonego śmiercią przywódcy Boko Haram. Właściwa nazwa tej organizacji to: Stowarzyszenie Ludności Sunnickiej na rzecz Działalności Misyjnej i Dżihadu (Dżama'atu Ahlis Sunna Lidda'Awati wal-Dżihad w języku hausa zapisywanym alfabetem arabskim lub Dżama'at Ahl al-Sunna li ad-Dawa wa al-Dżihad w języku arabskim). Wydaje się, że jej aktywność ustała, gdyż brakuje nowych informacji na temat jej zbrodniczej działalności. Organizacja otwarcie się do niej przyznawała, co stanowiło część jej strategii propagandowej. Znacznie zmniejszyła się również skala działań ISWAP, co nie oznacza, że w Nigerii jest bezpieczniej. Aktywność różnych grup i organizacji przesunęła się z północnego wschodu Nigerii (stany Borno, Yobe, Adamawa), matecznika obu ugrupowań, na zachód i południe kraju. Statystycznie sytuacja przedstawia się następująco: w 2021 r. na północy Nigerii w zamachach przeprowadzonych przez inne grupy niż Boko Haram i ISWAP zginęło ponad 2600 cywilów, a więc znacznie więcej niż w tym samym czasie zabiły te dwie organizacje i trzykrotnie więcej niż w 2020 r. Natomiast w pierwszym kwartale 2022 r. w Nigerii zostało zabitych 2968 osób. Aż 86% tych zgonów odnotowano w północnej części kraju.

Ta dygresja niech posłuży za wstęp do recenzji publikacji Marty Sary Stempień, będącej monografią poświęconą najbardziej zbrodniczej organizacji ekstremistów islamskich w historii Nigerii. Autorka, jak można przeczytać w notce biograficznej, jest adiunktem w Instytucie Nauk o Bezpieczeństwie Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach i zastępcą redaktor naczelnej czasopisma naukowego „Die Securitate et Defensione. O Bezpieczeństwie i Obronności". Oprócz recenzowanej monografii opublikowała książki *Państwo Islamskie: nowe oblicze terroryzmu* (2018 r.) i *Bliski Wschód: ciągle w ogniu* (2019 r., wspólnie z Maliną Kaszubą).

Monografia *Boko Haram*... składa się z pięciu rozdziałów, które mają różną wartość merytoryczną. Spełniają one postawiony cel, określają problem i hipotezę badawczą (sformułowane we wstępie), jednak zdaniem recenzenta należałoby tu raczej mówić o tezach opartych na dobrze

udokumentowanych faktach[2] niż hipotezie badawczej. W wielu miejscach brakuje równomiernego rozłożenia akcentów. Poważne problemy są bagatelizowane, a sprawom mniej istotnym poświęca się więcej uwagi. Ponadto skróty myślowe sprawiają, że czytelnikowi umykają najważniejsze kwestie. Te krytyczne uwagi odnoszą się przede wszystkim do rozdziału 1. zatytułowanego *Nigeria*, w którym w osobnych podrozdziałach zostały zawarte informacje na temat uwarunkowań historycznych i geopolitycznych, populacji kraju, rozwoju salafizmu w północnej Nigerii, idei liberalnej demokracji oraz sytuacji politycznej i ekonomicznej. Rozdział ten liczy 33 strony. Autorka nieproporcjonalnie i wybiórczo potraktowała poruszaną w nim problematykę. Najważniejszemu zagadnieniu, czyli islamowi, poświęciła niespełna 6 stron (s. 26–31), podczas gdy sytuacji ekonomicznej – 8 stron (s. 43–51). Zabrakło niestety informacji o kalifacie Sokoto, który wywarł olbrzymi wpływ na kształtowanie się islamu w Nigerii na początku XIX w., oraz o współczesnych wpływach Hezbollahu. O tym pierwszym autorka wspomina dopiero na stronach 56, 84 i 143–144. Na s. 144 pisze: *Od czasów Usmana dan Fodio do brytyjskiego podboju na początku XX wieku władzę sprawowało dwudziestu kalifów*. Nie jest to zgodne z historią i współczesnością Nigerii, ponieważ dwudziesty kalif i sułtan Sokoto, Muhammad Saad Abubakar, sprawuje te funkcje (wyłącznie reprezentacyjne, cieszy się jednak dużym szacunkiem) od 2006 r. do dziś. Pisząc w rozdziale 1. o wojnie biafrańskiej (1967–1970), autorka wspomniała między innymi o państwach biorących udział w tym konflikcie: *W wojnę zaangażowane były ówczesne potęgi światowe. Wielka Brytania i Związek Radziecki wspierały rząd Nigerii. Z kolei Biafra uzyskała wsparcie ze strony Francji i Izraela* (s. 22). Jest to niepełna informacja, ponieważ siły rządowe były także wspierane przez Stany Zjednoczone, a Biafra przez Portugalię i Watykan. Warto dodać, że lotnictwem biafrańskim dowodził Jan Zumbach, były dowódca dywizjonu 303. Zabrakło również ważnej informacji, że separatyzm biafrański jest aktywny do tej pory w południowo-wschodniej Nigerii. Reprezentuje go przede wszystkim organizacja Indigenous People of Biafra (pol. Rdzenna Ludność Biafry), oskarżana przez władze o działalność terrorystyczną. Walczy ona przede wszystkim o interesy ludu Ibo (Igbo). Autorka używa zarówno tych

[2] Jak wskazała autorka, celem monografii jest próba określenia ewolucji struktury terrorystycznej Boko Haram. Główny problem badawczy został zawarty w odpowiedzi na pytanie: jakie skutki dla Nigerii, w tym bezpieczeństwa, niesie aktywność Boko Haram? Stempień przyjęła też następującą hipotezę badawczą: Boko Haram w ostatnich latach stała się ważną grupą przedstawicielską salafickiej społeczności i znaczącą siłą militarną w Nigerii.

dwóch nazw, jak i niepoprawnego określenia Ikbo, nie wyjaśnia jednak, że chodzi o tę samą grupę etniczną. Może to wytworzyć u czytelnika mylne przekonanie, że mowa o dwóch różnych społecznościach. Podobny problem dotyczy Fulanów, pasterskiego muzułmańskiego ludu koczowniczego zamieszkującego całą strefę Sahelu. Są oni znani również pod nazwami: Fulbeje, Peul czy Bororo.

Przy opisie sytuacji politycznej Nigerii po uzyskaniu przez ten kraj niepodległości autorka wspomina, że gen. Olusẹgun Ọbasanjọ, prezydent i jeden z przywódców pierwszej junty wojskowej, w 1979 r. przekazał władzę w ręce cywilne. Zabrakło jednak istotnej uwagi, że tej zmianie władzy towarzyszyła poważna redukcja sił zbrojnych. Armię opuściły wówczas tysiące żołnierzy, którym pozostawiono broń. Stało się to przyczyną niebywałego wzrostu bandytyzmu i terroru w Nigerii, szczególnie na ulicach Lagos, byłej stolicy.

W pracy bardzo widoczne jest pobieżne potraktowanie przez autorkę zagadnienia rozwoju islamu w Nigerii. Pozostawia to uczucie sporego niedosytu. Pamięć o wydarzeniach w Afryce Zachodniej w XIX w., kiedy różni przywódcy religijni ogłaszali dżihad, wciąż jest żywa w tradycji i religii islamu wielu krajów Afryki, także w Nigerii.

W pracy bardzo rażący jest brak odwołań do znakomitej monografii Stanisława Piłaszewicza pt. *Potęga Księgi i Miecza Prawdy*[3]. Autorka najprawdopodobniej z niej nie korzystała, ponieważ nie wymieniła tego tytułu w bibliografii. Niewiele miejsca poświęciła również problemowi salafizmu w północnej Nigerii i radykalizmu muzułmańskiego, ale zwróciła uwagę na działalność krwawej sekty Maitatsine i wspomniała o kulcie Ombatse. W przypadku tego ostatniego warto byłoby poświęcić kilka zdań, aby przybliżyć czytelnikowi to zagadnienie, choćby ze względu na jego krwawy charakter związany z tradycyjnymi wierzeniami społeczności Eggon w środkowej Nigerii.

Na s. 31 pojawia się stwierdzenie: *W ostatnich latach wzrosła również rola szerzej nieznanej na świecie grupy tzw. bojowników Fulani*. Nie można się z tym zgodzić. W Afryce nie istnieje taka grupa zbrojna, autorka ma na myśli bojowników wyżej wspomnianego ludu Fulanów. Na jej usprawiedliwienie należy zaznaczyć, że opisując działalność tej „grupy", opierała się na informacjach opublikowanych przez Institute for Economics and Peace

[3] S. Piłaszewicz, *Potęga Księgi i Miecza Prawdy. Religia, cywilizacja i kultura islamu w Afryce Zachodniej*, Warszawa 1994.

w Global Terrorism Index (GTI) za 2014 r. Według GTI bojownicy Fulani stanowili wówczas czwartą najgroźniejszą grupę terrorystyczną za Boko Haram, Państwem Islamskim i talibami. W raporcie GTI potraktowano więc Fulanów jako organizację, a nie jako lud, w którym mężczyźni, jak w większości ludów pasterskich, w razie konieczności stają się wojownikami, co jednak nie oznacza, że są terrorystami. Populacja Fulanów i spokrewnionych z nimi Tukulerów liczy łącznie ponad 40 mln ludzi mieszkających od wybrzeża Atlantyku po Sudan i Republikę Środkowej Afryki. Posługują się oni językiem fulfulde i słyną z purytanizmu, neofickiej gorliwości oraz przekonania o wyższości etnicznej i językowej. Utworzone przez nich organizacje są dobrze znane. To chociażby Ansar al-Islam w Burkina Faso, ściśle związana z Dżama'at Nasr al-Islam wa al-Muslimin (pol. Grupa Wsparcia Islamu i Muzułmanów)[4], Al-Dżabhat li Tahrir al-Macina (pol. Front Wyzwolenia Maciny), zwana również Katiba Macina (pol. Batalion Maciny) lub Retour, Reclamation et Réhabilitation, 3R (pol. Powrót, Reklamacja, Naprawa), ruch kontrolujący obszar w Republice Środkowej Afryki wzdłuż granicy z Kamerunem. Fulanie byli i są także obecni w Dżama'at at-Tawhid wa al-Dżihad fi Gharbi Ifrikija (pol. Grupa Jedności i Dżihadu w Afryce Zachodniej) czy Ad-Dawla al-Islamijja fi as-Sahra al-Kabira (pol. Państwo Islamskie na Wielkiej Saharze). W raporcie GTI brakuje informacji o tych organizacjach, zwłaszcza Ansar al-Islam i Katiba Macina, co wynika być może z przeoczenia. Ta pierwsza odpowiada za masakry ludności w północnej i wschodniej części Burkina Faso oraz ucieczkę z domów 1,9 mln ludzi. Jej przywódcy, bracia Ibrahim Malam Dicko i Dżafar Dicko, od początku istnienia organizacji w 2016 r. odwoływali się do emiratu Dżelgudżi, historycznego królestwa Fulanów w północnej części Burkina Faso. Front Wyzwolenia Maciny został założony w 2015 r. przez fulańskiego charyzmatycznego kaznodzieję Amadu Kuffę, znanego z krytyki władz Mali. Taka retoryka z kolei nawiązywała do emiratu Maciny. Ugrupowanie słynie z napadów na wioski rolników ludów Bambara i Dogon w regionie Mopti w Mali. Ci drudzy dla obrony mieszkańców utworzyli zbrojną milicję Dan Na Ambassagu (pol. Myśliwi, którzy ufają Bogu). W marcu 2019 r., w odwecie za liczne napady, jej członkowie najechali na zamieszkałą przez Fulanów wieś Ogossogu i zabili 160 osób, w tym przywódcę wsi oraz jego wnuki.

[4] Organizacja utworzona w marcu 2017 r. przez: Tanzim al-Kaida bi Bilad al-Maghrib al-Islami (Organizację Al-Ka'idy w Krajach Islamskiego Maghrebu) działającą w strefie Sahelu, Ansar Dine (pol. Zwolennicy/Obrońcy Religii), Al-Murabitun (pol. Strażnicy) i Al-Dżabhat li Tahrir al-Macina (pol. Front Wyzwolenia Maciny).

Masakra wywołała szok w całym państwie i w kwietniu 2019 r. zmusiła rząd do dymisji.

W ostatnim podrozdziale pt. *Sytuacja ekonomiczna* panuje chaos w przywoływanych datach i wydarzeniach, zwłaszcza na stronach 46–47. W tej części autorka poruszyła również kwestię przejęcia przez dżihadystów kontroli nad produkcją żywności w północno-wschodniej Nigerii i pobierania opłat od produktów spożywczych. Wydaje się, że omówienie tego tematu powinno znaleźć się w podrozdziale czwartym *Finansowanie działalności* rozdziału 2. zatytułowanego *Struktura organizacyjna Boko Haram*. Rozdział ten zawiera wiele interesujących informacji i prezentuje duży zasób wiedzy autorki, lecz i w nim zauważa się błędnie zapisane nazwy organizacji lub mało trafne określenia. W leadzie do tego rozdziału Stempień informuje: *W 2012 r. od Boko Haram oderwała się grupa o nazwie Front Obrony Muzułmanów w Czarnej Afryce, znana jako Ansaru i rzadziej nazywana Al-Kaidą na Ziemiach poza Sahelem* (s. 52). Wymieniona organizacja nosiła nazwę Dżama'atu Ansarul Muslimina fi Biladis Sudan (pol. Stowarzyszenie Obrońców Muzułmanów w Krainie Czarnych). Pełną nazwę podano dopiero na s. 59, ale zamiast rzeczownika „Ansarul" błędnie użyto „Ansaril", podobnie „Ahlus" zamiast „Ahlis" czy „Afriqiya" zamiast „Ifriqija". Konstrukcja samego rozdziału również nie została dobrze przemyślana. Kolejne podrozdziały: *Geneza i ewolucja Boko Haram*, *Co oznacza Boko Haram* oraz *Struktura organizacyjna i władza* zostały wypełnione treścią w taki sposób, że wiele zdarzeń powtarza się, a porządek chronologiczny i faktograficzny został w dużej mierze zakłócony, co wywołuje wrażenie chaosu. Trudno uporządkować sobie następstwo wydarzeń oraz to, jak w danych okresach układały się stosunki łączące głównych aktorów. Autorka w ewolucji Boko Haram wyróżniła pięć cezur: lata 1970–1990, 2001–2009, 2010–2013, 2013–2015 oraz okres po 2015 r. Inne fazy rozwoju Boko Haram wymieniła natomiast w rozdziale 4. na s. 119: faza Kanama (2003–2005), faza dawah (2005–2009), faza reorganizacji (od 2009 r.). Wydaje się, że poprawniej byłoby połączyć te dwa rozdziały, tym bardziej że właśnie w rozdziale 2. Stempień pisze o Kanamie w stanie Yobe, gdzie założono pierwszy obóz islamskich ekstremistów nazwany „Afganistanem", a członków tej grupy określano mianem nigeryjskich talibów.

Autorka wiele miejsca poświęca koncepcji takfiru, czyli wykluczenia z ummy. Za jej twórcę uznawany jest Muhammad al-Maghili (1440–1505). Jego nauki wykorzystał Usman dan Fodio, założyciel sułtanatu Sokoto w 1809 r. Obecnie wiele muzułmańskich organizacji terrorystycznych używa tej koncepcji w celu wykluczenia z ummy tych muzułmanów, którzy nie

podzielają ich poglądów i nie chcą do nich dołączyć. Wśród nich były Boko Haram i Państwo Islamskie. Główną ideą głoszoną przez Ustaza Mohammada Jusufa, założyciela tej pierwszej, było obalenie rządu Nigerii i narzucenie dosłownej interpretacji Koranu. Od jego nazwiska ruch nazywano Jusufiją. Ważnym wydarzeniem w historii Boko Haram było odrzucenie zachodniego systemu szkolnictwa jako niszczącego wiarę w jednego Boga i przyjęcie jedynej słusznej prawdy, że sprawcą wszystkich zjawisk i rzeczy jest Bóg. W 2009 r. członkowie organizacji wzniecili powstanie w mieście Maiduguri, stolicy stanu Borno, w celu obalenia rządu i ogłoszenia stanu kalifatem. Uliczne walki przeniosły się z Maiduguri nie tylko na cały stan, lecz także na sąsiedni Yobe i dalsze – Bauchi i Kano. Za początek niepokojów należy uznać lipiec 2009 r., gdy bojówka Boko Haram zaatakowała posterunek policji w mieście Bauchi. Następnie islamscy ekstremiści dokonali brutalnych ataków w innych miastach północnej Nigerii. Celem napaści były komisariaty policji, więzienia, budynki rządowe, obiekty należące do administracji lokalnej oraz kościoły. We wrześniu 2009 r. podczas ataku na więzienie federalne w Bauchi uwolniono ponad 700 więźniów. Nastąpiła eskalacja konfliktu pomiędzy muzułmanami i chrześcijanami. W wyniku ataków Boko Haram zginęło ponad 700 osób, a wiele rodzin porzuciło swój dobytek i uciekło z domów. Rząd skierował siły wojskowe do pacyfikacji ekstremistów i ochrony ludności. W Maiduguri w wyniku walk zginęło ok. 500 osób. Policja zburzyła meczet Boko Haram, w którym ekstremiści stawiali opór. Aresztowano setki wyznawców, w tym Jusufa. Kilka dni później jego zwłoki znaleziono na jednej z ulic w Maiduguri. Policja stwierdziła, że zginął podczas próby ucieczki. Władze ogłosiły, że ruch Boko Haram został zniszczony raz na zawsze, co okazało się nieprawdą.

Po śmierci Jusufa przywództwo nad organizacją objął Szekau. Od 2010 r. obserwuje się postępującą aktywność zbrojnej działalności i eskalację przemocy ze strony Boko Haram. Organizacja rekrutuje coraz więcej wykluczonych młodych ludzi żyjących na marginesie społeczeństwa. W dniu 6 czerwca 2011 r. bojownik Boko Haram przeprowadził atak na kwaterę główną policji w Abudży. Był to pierwszy zamach samobójczy w Nigerii, w którym użyto samochodu pułapki. Atak był reakcją na pobyt szefa nigeryjskiej policji w Maiduguri, który nawoływał do likwidacji ugrupowania. W 2012 r. od Boko Haram odeszła część jego członków na czele z Khalidem al-Barnawim alias Abu Ussamata al-Ansary (aresztowany na początku kwietnia 2016 r.). Przyczyną rozpadu był sprzeciw secesjonistów wobec mordowania muzułmanów. Ci ostatni, uznawani, zgodnie z koncepcją

takfiru za niewiernych i odstępców od wiary, zasługiwali według Szekaua wyłącznie na śmierć. Masowe mordy były więc na porządku dziennym. Organizacja Al-Barnawiego przyjęła wspomnianą wcześniej nazwę: Dżama'atu Ansarul Muslimina fi Biladis Sudan, relokowała bazę do sąsiedniego Kamerunu i nawiązała współpracę z Tanzim al-Kaida bi Bilad al-Maghrib al-Islami (pol. Organizacja Al-Ka'idy w Krajach Islamskiego Maghrebu). Na s. 60 autorka informuje o kolejnym rozłamie w Boko Haram, do którego doszło w połowie 2015 r. Wówczas (...) *Mamman Nur i Abu Musab al-Barnawi, syn Mohammeda Yusufa, odłączyli się od Boko Haram i złożyli przysięgę wierności Państwu Islamskiemu, proklamując Prowincję Afryki Zachodniej (Wilayat Gharb Afriqiya – WGA)*. Tę tezę rozwija na s. 74. Jednak to Szekau na początku 2015 r. przyjął zwierzchność Państwa Islamskiego, oficjalnie zmieniając nazwę swej organizacji na Prowincja Afryki Zachodniej Państwa Islamskiego. Nie można zapominać, że centrala w Iraku chciała przejąć kontrolę nad Boko Haram i dążyła do osłabienia pozycji Szekaua. Wynikało to z jego sprzeciwu wobec planów kalifa Abu Bakra al-Bagdadiego co do rozszerzenia działalności Boko Haram poza obszar Nigru i Kamerunu w ramach idei globalnego dżihadu oraz powierzenia przywództwa nad grupą organowi kolegialnemu (arab. *medżlis asz-szura*). W jej skład mieliby wejść m.in. Mamman Nur i Abubakar Adam Kambara, wyznaczeni przez samozwańczego kalifa, co pozbawiłoby Szekaua jednoosobowego dowództwa nad Boko Haram. Zmniejszeniu jego wpływów służył także zarządzony przez Al-Bagdadiego podział bojowników Boko Haram na trzy zgrupowania, które zostały dyslokowane do północnego Kamerunu, w okolice jeziora Czad, oraz do wschodniego Nigru. Zadaniem Szekaua byłoby koordynowanie tych działań, głównie w północnej Nigerii. Spory między liderami dotyczące zakresu terytorialnego działania i kompetencji doprowadziły do odmowy pełnego podporządkowania się Szekaua centralnemu dowództwu Państwa Islamskiego, które w sierpniu 2016 r. usunęło go ze stanowiska przywódcy Prowincji Afryki Zachodniej. Szekau zerwał z podległością wobec centrali w Iraku, zachowując przywództwo nad wiernymi mu bojownikami Boko Haram. Natomiast liderem Prowincji Afryki Zachodniej został Abu Musab al-Barnawi (zginął w sierpniu 2021 r.). Spór pomiędzy obiema organizacjami przerodził się w zbrojną konfrontację. W jej wyniku w maju 2021 r. zginął Szekau.

W podrozdziale czwartym Stempień pisze o finansowaniu działalności Boko Haram, a w piątym o podstawach ideologicznych tej organizacji. Zdaniem recenzenta lepiej byłoby zamienić je miejscami, a w podrozdział

piąty wpleść fragmenty tekstu z podrozdziału trzeciego (*Struktura organizacyjna i władza*), którego duża część również została poświęcona założeniom ideologicznym organizacji. Ostatni podrozdział dotyczy natomiast aparatu medialnego i propagandy Boko Haram.

Dużo lepiej niż pierwsze dwa rozdziały prezentuje się część 3. monografii pt. *Ofiary Boko Haram*. Jest ona napisana w sposób przejrzysty i uporządkowany, a poszczególne podrozdziały zostały wypełnione interesującą treścią. Na uwagę zasługuje m.in. zawarcie informacji, że w 2014 r. Boko Haram i Państwo Islamskie odpowiadały za ponad połowę ofiar śmiertelnych ataków terrorystycznych. W tym samym roku nigeryjska organizacja wyprzedziła jednak Państwo Islamskie pod względem liczby ofiar śmiertelnych. Stosunek ten wynosił 6644 do 6073 zabitych. Szacuje się, że od początku istnienia do końca 2020 r. Boko Haram odpowiada za śmierć ok. 40 000 ludzi, w większości cywilów. Z przemocą seksualną członków organizacji, której autorka poświęciła osobny podrozdział, były związane porwania uczennic ze szkół i internatów. Kobiety i dziewczynki zmuszano do małżeństw. Stanowiły one również nagrodę dla nowych bojowników wstępujących w szeregi organizacji. O zjawisku tym, tak powszechnym w Państwie Islamskim na terenie Iraku, stało się głośno w kwietniu 2014 r., gdy Boko Haram uprowadziła 276 uczennic w wieku od 12 do 17 lat ze szkoły w mieście Chibok w stanie Borno, co zostało opisane w oddzielnym podrozdziale. To zdarzenie wywołało międzynarodową reakcję, ale nie stanowiło wyjątku. Kilka miesięcy później dżihadyści porwali 300 uczniów i kolejnych 100 kobiet i dzieci w miejscowości Damasak, o czym media już milczały. Faktem jest, że porwanie dziewcząt w Chibok sprawiło, że oczy świata z niepokojem zwróciły się na Nigerię. Przez media społecznościowe przeszła kampania „Zwróćcie nasze dziewczynki", do której przyłączyła się nawet pierwsza dama USA Michelle Obama. Miało to wywrzeć presję na nigeryjskie siły. Jednak mimo obietnic afrykańskich polityków i upływu ośmiu lat od tamtego zdarzenia los ponad 100 dziewcząt, obecnie już kobiet, nie jest znany. Wolność odzyskały te, które zdołały same uciec. Jedną z nich, z dzieckiem, 14 czerwca 2022 r. znalazł oddział nigeryjskich sił zbrojnych patrolujący okolice wioski Ngoshe w stanie Borno. Stempień informuje, że całkowita liczba porwań podczas konfliktu nie jest znana, ale ocenia się, że od 2012 r. uprowadzono od 500 do 2000 kobiet i dzieci. Te szacunki są jednak bardzo zaniżone, ponieważ według Amnesty International tylko od początku 2014 r. do kwietnia 2015 r. Boko Haram porwała co najmniej 2000 kobiet i dzieci. Kobiety są wykorzystywane jako niewolnice seksualne, pomoce kuchenne,

jako karta przetargowa w negocjacjach mających doprowadzić do zwolnienia więźniów oraz do zamachów terrorystycznych. Należy zaznaczyć, że proceder porwań uczniów ze szkół i internatów prowadzą do tej pory inne bandyckie ugrupowania działające w północnych stanach Nigerii, poza obszarem aktywności Boko Haram. Dnia 6 kwietnia 2022 r. władze Nigerii nazwały te gangi grupami terrorystycznymi, które zasługują na takie samo traktowanie jak Boko Haram. Prezydent Muhammadu Buhari wymienił dwie organizacje: Yan Bindiga (pol. Członkowie Bindigi) i Yan Ta'adda (pol. Członkowie Ta'adda). Porywają one ludzi dla okupu.

W pięciu kolejnych podrozdziałach zostały scharakteryzowane największe zamachy terrorystyczne od 2016 r. do 2020 r. Uzupełnieniem informacji na temat każdego roku są przejrzyste tabele zawierające listę ataków terrorystycznych, w wyniku których zginęło ponad 20 osób, z wyszczególnieniem daty, miejsca i sposobu przeprowadzenia ataku oraz liczbą ofiar śmiertelnych. Ostatni podrozdział dotyczy aktywności Boko Haram w 2020 r. oraz wpływu pandemii koronawirusa na działalność organizacji.

Rozdział 4. jest zatytułowany *Ewolucja militarna*. Jego wyodrębnienie jako oddzielną część skutkuje powieleniem informacji zawartych w poprzednich rozdziałach. Uniknięcie tych powtórzeń spowodowałoby wiele niejasności i fragmentaryzację struktury narracji. Obniżają one jednak walor naukowy książki, choć z pewnością przyczyniają się do utrwalenia wiedzy przez czytelnika. Uwaga ta dotyczy przede wszystkim podrozdziału pierwszego pt. *Strategia polityczno-militarna*. W opinii recenzenta bardziej korzystne byłoby omówienie zawartej w nim problematyki w podrozdziale pierwszym rozdziału 2. pt. *Geneza i ewolucja Boko Haram*. Ta sama uwaga dotyczy podrozdziału drugiego pt. *Metody i narzędzia działania* i w części także pozostałych. Tym samym można stwierdzić, że konstrukcja książki nie została dobrze przemyślana. Należy jednak zwrócić uwagę, że informacje zawarte w tej części mają dużą wartość poznawczą. Ukazują w pełni taktykę i metody działania Boko Haram, które w wielu przypadkach mogły zaskakiwać innowacyjnością względem strategii Państwa Islamskiego.

Olbrzymią rolę w przeprowadzaniu ataków terrorystycznych przez Boko Haram odgrywały kobiety i dzieci. Mimo że wykorzystywanie kobiet-samobójczyń przez nigeryjską organizację nie było żadną nowością, to skala tego procederu jest nieporównywalna z żadnym innym ugrupowaniem terrorystycznym. Obrazuje to wykres na s. 130, z którego wynika, że kobiety w Boko Haram były odpowiedzialne aż za 48% samobójczych ataków terrorystycznych na świecie od 1985 r. do 2018 r. Ta skala jeszcze

bardziej przemawia do wyobraźni, gdy weźmie się pod uwagę, że pierwszego zamachu samobójczego Boko Haram dokonała w 2011 r.

Znacznie więcej kontrowersji budzi wykorzystywanie dzieci do zamachów samobójczych. W 2015 r. w Nigerii, Kamerunie i Czadzie zmuszono do tego 44 dzieci, podczas gdy rok wcześniej było ich „tylko" czworo. Łączna liczba zamachów samobójczych w tych trzech krajach oraz w Nigrze przeprowadzonych przez Boko Haram oraz Stowarzyszenie Obrońców Muzułmanów w Krainie Czarnych wzrosła z 32 w 2014 r. do 151 w 2015 r. Aby uzupełnić tę porażającą statystykę, należy wspomnieć, że tylko od 1 stycznia 2017 r. do 16 sierpnia 2017 r. wysadzono w powietrze 83 dzieci, w tym 55 dziewczynek. Większość z nich miała mniej niż 15 lat. Do jednej z nich dodatkowo przyklejono za pomocą taśmy niemowlę, aby odwrócić uwagę policji. Terroryści zwykle przymocowywali do dziecka ładunek wybuchowy, a następnie pozostawiali je w jakimś zatłoczonym miejscu publicznym. Następnie bomba była zdalnie detonowana. W kilku przypadkach dzieciom udało się uciec do patroli policyjnych, które zdjęły z nich ładunki wybuchowe i zabezpieczyły je. W marcu 2015 r. nastolatka, której udało się udaremnić zamach, powiedziała, że jest jedną z uczennic porwanych ze szkoły w Chibok. Boko Haram jest pierwszą organizacją na świecie, w której większy odsetek zamachowców stanowią dzieci i kobiety. Działalność tej organizacji, jak żadnej innej, miała też katastrofalne skutki dla oświaty. Boko Haram całkowicie zniszczyła ponad 900 szkół i doprowadziła do zamknięcia dwukrotnie większej ich liczby. Ponad 600 nauczycieli i pracowników szkolnych zostało zabitych, a 19 000 zmuszono do ucieczki.

W podrozdziale czwartym monografii autorka omówiła powiązania Boko Haram z innymi ugrupowaniami, w tym relacje z Organizacją Al-Ka'idy w Krajach Islamskiego Maghrebu, a także z Ruchem na rzecz Jedności i Dżihadu w Afryce Zachodniej (arab. Dżama'at at-Tawhid wa al-Dżihad fi Gharbi Ifrikija, znaną jako MUJAO od francuskiej nazwy Mouvement pour l'Unicité et le Jihad en Afrique de l'Ouest), który powstał w Mali w październiku 2011 r. w wyniku secesji części bojowników z Al-Ka'idy. Dowodził nimi Muhammad Kheiru alias Abu Kumkum. W sierpniu 2013 r. MUJAO połączył się z organizacją Katibat al-Mulassamin (pol. Zamaskowany Batalion), zwaną również Muwakaun bi ad-Dima (pol. Podpisani Krwią), kierowaną przez słynnego Mokhtara Belmokhtara, tworząc organizację Al-Murabitun (pol. Strażnicy).

W piątym podrozdziale pt. *Powiązania z Państwem Islamskim i utworzenie afrykańskiego kalifatu* autorka powraca do zagadnienia powstania

Prowincji Afryki Zachodniej Państwa Islamskiego, wymieniając m.in. czynniki, które mogą prowadzić do podziałów w ruchu dżihadystycznym, co się zdarzyło w przypadku Boko Haram. Od 2016 r. Boko Haram i Prowincja Afryki Zachodniej prowadziły krwawą, terrorystyczną rywalizację, popełniały coraz bardziej okrutne i bezsensowne mordy. Ofiarami byli zwykli mieszkańcy miasteczek i wsi. Wydaje się, że religijnie zradykalizowani oprawcy zabijali ich dla rozrywki, ponieważ uważali, że działają w imię Boga. To Allah w ich mniemaniu wymierza sprawiedliwość na Ziemi. Na przykład 9 czerwca 2016 r. Boko Haram zamordowała 81 osób w Gubio. Tego samego dnia miejscowy odłam Państwa Islamskiego zabił 69 mieszkańców wioski Felo, w odwecie za wcześniejsze udaremnienie przez wojsko kradzieży bydła z tej wsi. Obie miejscowości są położone w stanie Borno w północno-wschodniej Nigerii. Podobnych przykładów można znaleźć znacznie więcej. Jednak z upływem czasu rywalizacja zmieniła się w otwarty konflikt między tymi organizacjami, w którym zwycięstwo odniosło Państwo Islamskie. Lektura tego podrozdziału skłania do stwierdzenia, że można byłoby połączyć część zawartej w nim treści z podrozdziałem drugim, zatytułowanym *Metody i narzędzia działania*. Taka uwaga jest tym bardziej uzasadniona, że dopiero w tym miejscu autorka definiuje zjawisko dżihadyzmu i pisze o dżihadzie prowadzonym na początku XIX w. przez Usmana dan Fodio i sułtanacie Sokoto.

W ostatnim podrozdziale scharakteryzowano działalność Boko Haram w Kamerunie, Nigrze i Czadzie. Warto zaznaczyć, że granice tych państw oraz Nigerii zbiegają się na jeziorze Czad. Na jego brzegu atakowano wioski rybackie, palono zabudowania, zabijano i uprowadzano ludzi. Według autorki w Czadzie nie doszło do żadnego ataku przeprowadzonego przez Boko Haram, w którym zginęło co najmniej 20 osób (s. 147). Tymczasem w tabeli 12 (s. 115) zawierającej listę ataków terrorystycznych dokonanych przez tę organizację w pierwszej połowie 2020 r. z liczbą ofiar śmiertelnych wynoszącą ponad 20 osób pod datą 23 marca wymienia ona atak na bazę wojskową w Czadzie, w którym śmierć poniosło 98 żołnierzy. Na s. 114 autorka wspomina o tym zdarzeniu w zaledwie dwóch zdaniach. Zasługuje ono na nieco szerszy opis, także dlatego, że przy omawianiu łamania praw człowieka i zbrodni wojennych na s. 170 nieco więcej miejsca poświęca śmierci 44 osób, które zmarły w więzieniu. Zostały one aresztowane w marcu 2020 r. po operacji „Gniew Bomy". Autorka jednak nie rozwija tego zagadnienia, dlatego czytelnik pozostaje w niewiedzy, jaką operację Stempień miała na myśli. Recenzent czuje się zobowiązany uzupełnić ten wątek.

W nocy z 22 na 23 marca 2020 r. dżihadyści zaatakowali bazę wojsk czadyjskich w Boma położoną na wyspie na jeziorze Czad. Oblężenie trwało ok. siedmiu godzin. Zginęło 98 żołnierzy armii czadyjskiej, uznawanej za najbardziej bitną w strefie Sahelu, a 47 zostało rannych. Napastnicy zaatakowali również przybywające posiłki. Zniszczyli 24 pojazdy, w tym samochody pancerne, i zdobyli duże ilości uzbrojenia, które załadowali na łodzie motorowe i zbiegli do Nigerii. Był to jeden z najbardziej spektakularnych ataków Boko Haram, w którym zadano jednorazowo największe straty armii Czadu w XXI w. Na miejsce zdarzenia przybył prezydent Czadu Idriss Déby, który zapowiedział operację odwetową pod kryptonimem „Gniew Bomy". Trwała ona od 31 marca do 8 kwietnia. Żołnierze czadyjscy wyparli wówczas bojowników Boko Haram z wysp na jeziorze Czad, zniszczyli jej liczne bunkry i wkroczyli do nigeryjskiej prowincji Borno, gdzie w miejscowości Magumeri uwolnili kilku nigeryjskich żołnierzy przetrzymywanych przez terrorystów. Poinformowano, że zginęło ok. 1000 islamskich ekstremistów. Aresztowano 58 dżihadystów, których przewieziono do więzienia w stolicy kraju – Ndżamenie. Tam umieszczono ich w jednej celi. Przez trzy dni odmawiano im jedzenia i wody. W dniu 18 kwietnia ujawniono, że 44 więźniów znaleziono martwych. Była to pozasądowa egzekucja dokonana przez czadyjskie służby bezpieczeństwa.

Na końcu rozdziału autorka wysuwa wniosek, że biorąc pod uwagę obszary aktywności Państwa Islamskiego, ataki w Nigrze, Burkina Faso lub Mali należy przypisać Państwu Islamskiemu na Wielkiej Saharze, podczas gdy te w regionie jeziora Czad – Państwu Islamskiemu w Prowincji Afryka Zachodnia. Jest to jednak duże uproszczenie, ponieważ część jeziora Czad należy do Nigru. W niektórych z tych państw działają również inne organizacje terrorystyczne, a w północno-zachodniej Nigerii zorganizowano ponadto grupy bandyckie. Region Diffa w południowo-wschodnim Nigrze, przy granicy z Nigerią, był atakowany przez nigeryjskie uzbrojone grupy, których nie udało się zidentyfikować. Ataki w tym regionie przypisywano Boko Haram lub Państwu Islamskiemu. Sprawdziła się natomiast prognoza autorki dotycząca intensyfikacji działalności i militaryzacji frakcji Boko Haram podległej centrali Państwa Islamskiego. W 2021 r. Prowincja Afryki Zachodniej pokonała „macierzysty" odłam Boko Haram i przejęła główną rolę w ruchu dżihadystycznym w Nigerii.

Na ostatni rozdział zatytułowany *Przeciwdziałanie ekspansji Boko Haram* składają się cztery podrozdziały. Dwa pierwsze dotyczą działań kontrterrorystycznych prowadzonych przez siły zbrojne Nigerii i sojuszników.

Autorka zwraca uwagę na początkowe bagatelizowanie działalności Boko Haram przez rząd federalny Nigerii, co doprowadziło do utraty kontroli nad trzema prowincjami – Borno, Jobe i Adamawa – oraz zdolności do pełnienia funkcji gwaranta bezpieczeństwa. Podstawą prawną walki z terroryzmem miała być ustawa o zapobieganiu terroryzmowi z 2011 r., jednak dopiero dwa lata później w wymienionych stanach ogłoszono stan wyjątkowy, a prezydent Goodluck Jonathan powiadomił o ofensywie przeciwko Boko Haram. Była ona prowadzona w sposób mało zdecydowany. Sukcesom w jednym miejscu towarzyszyły spektakularne porażki w innym. Mimo że udało się wypchnąć bojowników z niektórych miast, to obszary wiejskie znajdowały się pod ich kontrolą, nie wspominając już o lesie Sambisa oraz górzystym regionie Gwoza i masywie Mandara, w których organizacja rozlokowała stałe bazy funkcjonujące praktycznie do dziś. W 2021 r. zostały one przejęte przez Prowincję Afryki Zachodniej. Atakami terrorystycznymi były zagrożone środkowe stany Nigerii, nie wyłączając stolicy – Abudży, gdzie przeprowadzono atak na kwaterę główną policji. Siły zbrojne oskarżano o łamanie praw człowieka, w tym liczne aresztowania niewinnych osób, tortury i pozasądowe egzekucje prawdziwych i rzekomych członków Boko Haram. Na porządku dziennym były pacyfikacje całych wiosek podejrzanych o sprzyjanie organizacji. Wielu mieszkańców uciekło przed dżihadystami i armią.

Stempień podaje dane liczbowe dotyczące aresztowań i zbrodni dokonanych przez siły zbrojne. Skompromitowały się one także w związku ze wspomnianym wcześniej porwaniem 276 uczennic ze szkoły w Chibok. Samo zdarzenie nie stanowiło podważenia autorytetu sił bezpieczeństwa, ale niemożność odnalezienia i odbicia uprowadzonych dziewcząt już tak. Kolejny prezydent Muhammadu Buhari, generał w stanie spoczynku, który do wyborów w 2015 r. szedł z hasłem zlikwidowania w ciągu jednego roku dżihadystycznej rebelii na północnym wschodzie kraju, nie dotrzymał obietnicy. Instytucje cywilne nawiązały natomiast współpracę z armią, tworząc Civilian Joint Task Force (pol. Cywilna Wspólna Grupa Zadaniowa). Ochotnicy wyszkoleni i uzbrojeni przez armię ponosili jednak duże straty w starciach z bojownikami, mimo że zdarzały się zwycięskie bitwy antydżihadystycznych milicji. Autorka pisze o inicjatywach społeczności międzynarodowej w zwalczaniu Boko Haram, w tym działaniach Multinational Joint Task Force (pol. Wielonarodowa Wspólna Grupa Zadaniowa), która połączyła siły militarne Nigerii, Nigru, Kamerunu i Czadu, wspierane przez USA, Francję i Wielką Brytanię. Nie wspomniała

natomiast o najemnikach zwerbowanych przez firmę ochroniarską Pilgrim Africa z RPA. Właściciele „Pielgrzyma" zaoferowali rządowi Nigerii, że na początku 2015 r. przyjadą z własnym wojskiem, bronią, południowoafrykańskimi wozami pancernymi i poradzieckimi śmigłowcami Mi-24, pilotowanymi przez doświadczone załogi z Ukrainy. Według nigeryjskiej prasy najemnicy, zatrudnieni oficjalnie do szkolenia rządowego wojska, wyręczali je w wojnie z dżihadystami. Walczyli nocą, wyposażeni w najnowocześniejszy sprzęt noktowizyjny. Nad ranem wycofywali się do baz, pozwalając się zastępować w roli wyzwolicieli nigeryjskim żołnierzom. Władze Nigerii ogłosiły, że odbiły z rąk Boko Haram ok. 40 miejscowości, nie wspomniały natomiast o pomocy najemników.

W podrozdziale trzecim został poruszony między innymi problem deradykalizacji bojowników. Władze Nigerii od wielu lat korzystają z możliwości amnestii, łagodzenia kar i porozumień z różnymi grupami rebelianckimi. W 2015 r. stworzono kontrowersyjny program dla „skruszonych" niższej rangi dezerterów z Boko Haram. Uruchomiono również plan reintegracji pod nazwą „Operation Safe Corridor" (pol. „Operacja Bezpieczny Korytarz"), zainicjowany przez armię i ułatwiający dezercję. Przystąpiono także do realizacji innych projektów dotyczących rehabilitacji i reintegracji „skruszonych" bojowników oraz dziewcząt i kobiet porwanych przez Boko Haram, które odzyskały wolność, ale przez posiadanie dzieci z bojownikami zostały wykluczone przez rodzinę lub wiejską społeczność.

Działalność Boko Haram doprowadziła w Nigerii do kryzysu humanitarnego, któremu poświęcony jest ostatni podrozdział. Na ten kryzys złożyły się m.in. łamanie praw człowieka i zbrodnie wojenne. Autorka podaje dane statystyczne z badań Amnesty International i informacji zawartych w Globalnym Indeksie Pokoju. W kontekście udokumentowanych zbrodni wojennych wymienia śmierć 44 tymczasowo aresztowanych osób w więzieniu w Ndżamenie. Byli to bojownicy Boko Haram schwytani przez siły zbrojne Czadu podczas wspomnianej wcześniej operacji „Gniew Bomy". Aktywność terrorystyczna Boko Haram, Państwa Islamskiego i operacje kontrterrorystyczne spowodowały ucieczkę z domów i przesiedlenie kilku milionów ludzi w północno-wschodniej Nigerii i państwach sąsiednich. W wielu obozach przesiedleńcy doświadczyli głodu, nie mieli dostępu do środków higieny i podstawowej opieki medycznej. Skala zniszczeń dokonanych przez Boko Haram okazała się wprost niewyobrażalna, co pokazały zdjęcia satelitarne, na których widać, że wiele miejscowości doszczętnie spalono. Ich mieszkańcy zostali zabici, a ci, którzy przeżyli, uciekli lub

zostali wcześniej przesiedleni. Kryzys związany z działalnością Boko Haram pogłębiły siły bezpieczeństwa. Ich operacje mające na celu rozbicie dżihadystów prowadziły często do pozasądowych egzekucji. Ofiarami byli schwytani bojownicy lub osoby podejrzewane o przynależność do organizacji. Wojsko niszczyło też wioski, które pod przymusem lub dobrowolnie wspierały ekstremistów.

W podsumowaniu autorka dokonała krótkiego streszczenia problematyki poruszonej w książce oraz przedstawiła wnioski. Potwierdziła przyjętą we wstępie hipotezę, że ekspansja Boko Haram znacznie przyczyniła się do pogłębienia destabilizacji Nigerii. Warto jednak zauważyć, że dzieje się tak w każdym kraju, w którym działają duże organizacje terrorystyczne. Z krajów afrykańskich dla przykładu można wymienić: Somalię, Mozambik, Kongo, Mali czy Burkina Faso. Stempień stwierdziła m.in., że w ramach procesu badawczego udało się jej ukazać ewolucję Boko Haram oraz wskazać możliwe kierunki dalszej działalności tej organizacji. Jak słusznie wcześniej zauważyła, została ona zdominowana przez Państwo Islamskie w Afryce Zachodniej. Nie można natomiast zgodzić się z wnioskiem, że walka zbrojna z dżihadystami jest istotna, ale ma drugorzędne znaczenie, ponieważ (...) *priorytetem powinno być „inwestowanie" w pozamilitarne aspekty walki z dżihadystami, tj. programy deradykalizacji, rehabilitacji i reintegracji. Jednym z głównych wyzwań będzie przekonanie Nigeryjczyków do zaufania tego typu inicjatywom*. Zdaniem recenzenta działania zbrojne przeciwko organizacjom terrorystycznym i fizyczna eliminacja przywódców powinny być priorytetem, a nie „wypchnięcie dżihadystów z okupowanych obszarów", jak stwierdza autorka. Doświadczenia wielu państw wskazują, że deradykalizacja islamskich bojowników przynosi słabe rezultaty. Bardzo trudno jest zweryfikować, czy dana osoba rzeczywiście złagodziła swoje poglądy i czy jej skrucha jest szczera. Niełatwo także prognozować dalsze zachowanie takich ludzi. Bardzo często pozorują oni jedynie zmianę postępowania, by odwrócić uwagę służb bezpieczeństwa.

Francuzi otwarcie przyznali, że są bezradni w obliczu radykalizacji młodzieży muzułmańskiej. W 2017 r. francuski senat opublikował raport dotyczący rządowych programów deradykalizacji muzułmanów. Jednoznacznie stwierdzono w nim, że zakończyły się one całkowitym fiaskiem. Z opinii przedstawionej przez francuską prokuraturę przy okazji ogłoszenia wyroków za zamachy w Paryżu 13 listopada 2015 r. również wynika, że nie można mieć złudzeń co do możliwości resocjalizacji i deradykalizacji

islamskich ekstremistów. Podczas pobytu w więzieniach fanatycy rzadko porzucają swoją ideologię. Kara pozbawienia wolności to jednak jedyny akceptowalny sposób, by chronić społeczeństwo przed tymi, którzy tzw. sprawiedliwość boską przeciwstawiają wymiarowi sprawiedliwości, i mordując, wymierzają słuszne – w ich mniemaniu – kary.

Recenzowana publikacja została zaopatrzona w fotografie, mapy, wykresy i tabele. Na końcu książki zamieszczono bogatą bibliografię podzieloną na: słowniki i encyklopedie, opracowania zwarte, artykuły, akty prawne, netografię. Monografię uzupełnia wykaz ilustracji i tabel oraz indeksy: nazwisk i nazw geograficznych. Opracowanie Marty Sary Stempień stanowi wartościowe studium Boko Haram. W tekście autor recenzji wymienił m.in. nieścisłości w tłumaczeniu niektórych pojęć. Nie mają one jednak wpływu na treść pracy. Większym mankamentem jest natomiast rozpoczęcie danego wątku w jednej części, by kontynuować go w następnym rozdziale. Zmusza to czytelnika do powrotu do przeczytanego już materiału w celu całościowego spojrzenia na poruszany problem, np. historię islamu w Nigerii czy też ewolucję Boko Haram. Mimo to recenzent gorąco zachęca do przeczytania tej publikacji, ważnej z punktu widzenia zagrożenia terrorystycznego w Afryce oraz obrazującej trudności i niepowodzenia w prowadzeniu działań kontrterrorystycznych.

Krzysztof Izak

Emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewętrznego.

https://doi.org/10.4467/27204383TER.23.022.18324
https://orcid.org/0000-0001-6716-3224

MARCIN WIELEC

Recenzja książki: **Legal aspects of the European intelligence services' activities** pod red. dr. Piotra Burczaniuka[1]

Pod koniec 2022 r. nakładem wydawnictwa Agencji Bezpieczeństwa Wewnętrznego ukazała się anglojęzyczna monografia wieloautorska pt. *Legal aspects of the European intelligence services' activities* (pol. Prawne aspekty działalności europejskich służb specjalnych[2]) pod redakcją naukową dr. Piotra Burczaniuka. Jej tematem przewodnim jest funkcjonowanie służb specjalnych w ramach systemów prawnych 19 państw europejskich, tj. Austrii, Belgii, Bułgarii, Chorwacji, Czech, Estonii, Francji, Niemiec, Grecji, Węgier, Włoch, Łotwy, Litwy, Holandii, Polski,

[1] *Legal aspects of the European intelligence services' activities,* P. Burczaniuk (red. nauk.), Warszawa 2022, Agencja Bezpieczeństwa Wewnętrznego.

[2] Tłumaczenia w tekście pochodzą od autora (przyp. red.).

Rumunii, Słowacji, Hiszpanii i Szwecji. W książce zostały omówione modele organizacyjne, struktura i zakres kompetencji służb specjalnych w wymienionych państwach, jak również wybrane problemy związane z ich działalnością.

Monografia ma 302 strony i składa się z 20 rozdziałów oraz bogatej bibliografii. Rozpoczyna ją przedmowa szefa Agencji Bezpieczeństwa Wewnętrznego płk. Krzysztofa Wacławka oraz wstęp dr. Burczaniuka. Następnie w ramach 19 rozdziałów poświęconych poszczególnym państwom zostały zaprezentowane analizy dotyczące wskazanej w tytule problematyki, przeprowadzone na podstawie czytelnego schematu zaproponowanego przez redaktora naukowego publikacji. Zgodnie z nim rozdziały składają się z dwóch zasadniczych części. W pierwszej z nich autorzy omawiają: miejsce danej służby w krajowym systemie prawnym, definicję legalną służb specjalnych, ich pozycję i rolę w systemie administracji publicznej, realizowane przez nie czynności, kontrolę i nadzór nad służbami, status prawny funkcjonariuszy i pracowników służb. Druga część jest poświęcona wybranym przez autorów zagadnieniom związanym z działalnością tego rodzaju podmiotów, m.in.: zadaniom i mandatowi służb, zwłaszcza ich uprawnieniom dochodzeniowo-śledczym, roli służb w postępowaniu karnym, zbieraniu informacji, ochronie informacji niejawnych i danych osobowych oraz współpracy międzynarodowej. Z uwagi na wielość omawianych państw, zróżnicowanie ich systemów prawnych oraz zagadnień poddawanych analizie wprowadzenie wspólnego wzorca konstrukcyjnego należy ocenić pozytywnie.

Jedynym rozdziałem odbiegającym od opisanego schematu i stanowiącym cenne dopełnienie wcześniejszych rozważań jest rozdział dwudziesty, zatytułowany *National Security Clause in the EU Law and Its Implications for Intelligence and Security Services* (pol. Klauzula bezpieczeństwa narodowego w prawie Unii Europejskiej i jej skutki dla służb specjalnych). Zaprezentowano w nim wybrane zagadnienia związane z polityką państw Unii Europejskiej i ich służb specjalnych w kontekście bezpieczeństwa narodowego, a sama jego koncepcja została przedstawiona w szerszej perspektywie, uwzględniającej najnowsze orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej.

Wydaje się, że systemy prawne państw opisanych w publikacji mają, pomimo różnic dotyczących modeli i umiejscowienia służb specjalnych, wiele cech wspólnych. Do zagadnień uniwersalnych, a zarazem budzących

największe kontrowersje, należą nadzór i kontrola nad tego rodzaju strukturami państwowymi oraz status ich funkcjonariuszy.

Omawianą pozycję należy ocenić bardzo wysoko. Na uznanie zasługuje nie tylko zebranie w jednym miejscu kompleksowych analiz dotyczących służb specjalnych tak wielu państw, lecz także dobór autorów. Są to osoby będące ekspertami w swoich dziedzinach, a przede wszystkim bezpośrednio związane z działalnością służb specjalnych w poszczególnych państwach i wykorzystujące w praktyce akty prawne opisywane w książce. Dzięki temu prezentowane analizy są wiarygodne, rzetelne i konkretne, a poruszane zagadnienia – aktualne. Dotyczą one również kwestii tak żywotnych, jak cyberbezpieczeństwo, *big data* czy dezinformacja.

W literaturze z zakresu nauk prawnych, nauk politycznych i dotyczących bezpieczeństwa narodowego monografia *Legal aspects of the European intelligence services' activities* jest pozycją wyjątkową. Może ona być bardzo przydatna osobom zajmującym się zawodowo problematyką służb specjalnych oraz środowiskom akademickim z uwagi na zebranie w niej i omówienie wielu istotnych zagadnień związanych z funkcjonowaniem służb specjalnych w aż 19 krajach europejskich.

Dr hab. Marcin Wielec

Prodziekan Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, kierownik Katedry Postępowania Karnego Wydziału Prawa i Administracji UKSW, dyrektor Instytutu Wymiaru Sprawiedliwości. Autor i współautor kilku pozycji książkowych oraz wielu artykułów naukowych z zakresu postępowania karnego. Członek Rady Programowo-Naukowej kwartalnika „Probacja". Absolwent IESE Business School i Krajowej Szkoły Administracji Publicznej.

PRACE KONKURSOWE

https://doi.org/10.4467/27204383TER.23.023.18325
https://orcid.org/0009-0009-3421-6399

JAKUB TUSZYŃSKI

Skuteczność wybranych modeli AI w predykcji ofiar ataków terrorystycznych[1]

Abstrakt

W artykule porównano skuteczność wybranych algorytmów uczenia maszynowego w predykcji ofiar ataków terrorystycznych. Celem autora było udzielenie odpowiedzi na pytanie, czy mogą one posłużyć jako jedno z narzędzi antyterrorystycznych. Dokonano eksploracyjnej analizy danych, omówiono wybrane trendy i charakterystykę zamachów terrorystycznych. Przedstawiono niektóre miary oceny algorytmów klasyfikacyjnych użytych w badaniu oraz wskazano potencjalne kierunki dalszych badań.

Słowa kluczowe:

AI,
uczenie maszynowe,
terroryzm,
ofiary,
klasyfikacja

[1] Artykuł powstał na podstawie pracy magisterskiej pt. *Skuteczność wybranych modeli AI w predykcji ofiar ataków terrorystycznych,* obronionej na Wydziale Dziennikarstwa, Informacji i Bibliologii Uniwersytetu Warszawskiego. Autor wykorzystał fragmenty rozdziałów 3. i 6. Praca została nagrodzona w XII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Badanie ataków terrorystycznych

Ze względu na spory definicyjne na potrzeby niniejszego artykułu przyjmuje się, że zamach terrorystyczny to (...) *zamierzony akt przemocy lub groźba jej użycia ze strony podmiotu niepaństwowego*[2]. W ramach tego artykułu przeprowadzono badanie mające na celu porównanie skuteczności różnych algorytmów sztucznej inteligencji w przewidywaniu ofiar ataków terrorystycznych. Do przeprowadzenia badania wykorzystano bazę danych Global Terrorism Database (dalej: GTD) utrzymywaną przez badaczy z konsorcjum START[3], zawierającą informacje na temat zamachów terrorystycznych.

W ramach GTD przyjęto trzy kryteria, z których co najmniej dwa muszą być spełnione, żeby dane zdarzenie zostało uznane za atak terrorystyczny. Te kryteria to:

- akt przemocy miał na celu osiągnięcie celu politycznego, ekonomicznego, religijnego lub społecznego;
- akt przemocy zawierał dowody na zamiar wymuszenia, zastraszenia lub przekazania innego przesłania szerszej publiczności, innej niż bezpośrednie ofiary;
- akt przemocy wykraczał poza zakres międzynarodowego prawa humanitarnego[4].

Oznaczono również te zdarzenia, w których liczba informacji okazała się niewystarczająca do jednoznacznego określenia, czy dane wydarzenie było atakiem terrorystycznym czy też nie, i są one możliwe do odfiltrowania przez użytkownika.

Założenia

W celu możliwie jak najdokładniejszego wyeliminowania przypadków błędnego zaklasyfikowania danego zdarzenia jako ataku terrorystycznego wykluczono te obserwacje, które nie spełniają wszystkich trzech kryteriów opisanych powyżej, oraz te, co do których autorzy bazy mieli wątpliwości.

---

[2] *Data Collection Methodology*, Global Terrorism Database, http://www.start-dev.umd.edu/gtd/using-gtd/ [dostęp: 21 V 2022].

[3] *History of the GTD*, Global Terrorism Database, https://start.umd.edu/gtd/about/History.aspx [dostęp: 11 V 2022].

[4] *Data Collection Methodology*... Tłumaczenia w artykule pochodzą od autora (dop. red.).

Za ofiary ataku uznaje się wszelkie osoby niebędące terrorystami, które w wyniku zdarzenia zostały ranne lub zabite. Zbudowano kilka modeli uczenia maszynowego i porównano je za pomocą odpowiednich metryk.

Eksploracyjna analiza danych

Podczas eksploracyjnej analizy danych nacisk został położony na zrozumienie badanego zbioru danych. W pierwszej kolejności przeprowadzono analizę strukturalną.

Na rysunku 1 wyróżnia się następujące cechy zbioru:

- ponad 200 000 wierszy zarejestrowanych zamachów;
- 135 kolumn zawierających cechy opisujące dane zdarzenie;
- *dtypes* opisuje typy danych poszczególnych kolumn. Są to dane kategoryczne, mające skończoną liczbę kategorii – 9, kolumny zawierające liczby zmiennoprzecinkowe – 53, liczby całkowite występujące w 24 kolumnach i 49 kolumn zawierających dane mogące być zarówno ciągami znaków, jak i liczbami. Typ danych *object* jest przypisywany wówczas, kiedy nie można jednoznacznie przypisać żadnego innego typu danych;
- zbiór zajmuje ok. 200 megabajtów pamięci.

```
Int64Index: 201183 entries, 0 to 201182
Columns: 135 entries, eventid to related
dtypes: category(9), float64(53), int64(24), object(49)
memory usage: 197.1+ MB
```

Rysunek 1. Podstawowe statystyki opisujące zbiór danych.

Źródło: opracowanie własne.

W następnej kolejności odfiltrowano dane niespełniające wszystkich trzech kryteriów zamachu terrorystycznego oraz te, co do których autorzy bazy mieli wątpliwości. Usunięto również te kolumny, w których 50% lub więcej wierszy było pustych. Celem zredukowania zbioru danych było przyspieszenie wykonywanych na nim operacji. Ponadto większość algorytmów uczenia maszynowego zastosowanych w badaniu wymaga, żeby zbiór danych nie miał wartości pustych. Ich uzupełnienie za pomocą średniej,

mediany czy najczęściej występującej wartości przy tak dużej liczbie pustych obserwacji powodowałoby nieuprawnioną generalizację na podstawie niewielkiej ilości danych. Ta operacja zmniejszyła zbiór danych do 154 260 wierszy i 60 kolumn, a rozmiar pliku wyniósł niecałe 70 megabajtów.

W kolejnym kroku sprawdzono podstawowe wartości poszczególnych kolumn. Na osi x są widoczne nazwy kolumn, a na osi y są wyliczone statystyki: liczba obserwacji, średnia, odchylenie standardowe, wartość minimalna, pierwszy kwartyl, mediana, trzeci kwartyl oraz wartość maksymalna.

Na rysunku 2 widać, że zmienne *latitude* i *longitude* zawierają braki, które odpowiednio przeprocesowano poprzez usunięcie wierszy z brakującymi wartościami w tych zmiennych, dzięki czemu zostały użyte podczas modelowania. Warto również zwrócić uwagę na minimalną wartość zmiennej *vicinity*, która wynosi -9 (jest to widoczne w ostatnim wierszu kolumny *min*). Autorzy bazy w ten sposób oznaczają przypadki braku danych. Zostało to opisane w tzw. *Codebooku*[5].

	count	mean	std	min	25%	50%	75%	max
eventid	154260.0	2.005463e+11	1.294940e+09	1.970000e+11	1.995042e+11	2.012022e+11	2.015091e+11	2.019123e+11
iyear	154260.0	2.005397e+03	1.294946e+01	1.970000e+03	1.995000e+03	2.012000e+03	2.015000e+03	2.019000e+03
imonth	154260.0	6.443965e+00	3.392222e+00	0.000000e+00	4.000000e+00	6.000000e+00	9.000000e+00	1.200000e+01
iday	154260.0	1.553523e+01	8.803117e+00	0.000000e+00	8.000000e+00	1.500000e+01	2.300000e+01	3.100000e+01
extended	154260.0	5.527032e-02	2.285079e-01	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	1.000000e+00
country	154260.0	1.297654e+02	1.116024e+02	4.000000e+00	7.800000e+01	9.700000e+01	1.600000e+02	1.004000e+03
region	154260.0	7.321360e+00	2.838782e+00	1.000000e+00	6.000000e+00	8.000000e+00	1.000000e+01	1.200000e+01
latitude	151329.0	2.369732e+01	1.798608e+01	-5.315461e+01	1.184079e+01	3.153024e+01	3.451689e+01	7.463355e+01
longitude	151329.0	3.227138e+01	5.485520e+01	-1.578583e+02	9.735686e+00	4.414823e+01	6.914701e+01	1.793667e+02
specificity	154259.0	1.447591e+00	9.567426e-01	1.000000e+00	1.000000e+00	1.000000e+00	1.000000e+00	5.000000e+00
vicinity	154260.0	6.333463e-02	2.803160e-01	-9.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	1.000000e+00

Rysunek 2. Fragment statystyk zmiennych liczbowych.

Źródło: opracowanie własne.

Na rysunku 3 przedstawiono statystyki dla zmiennych tekstowych: liczba obserwacji, liczba unikalnych wartości, najczęściej występująca wartość oraz jej częstotliwość.

W zbiorze danych część zmiennych występuje pod postacią liczbową i tekstową. Jest to np. zmienna *region_txt* (rysunek 3) i zmienna *region* (rysunek 2). Uwzględniono to przed modelowaniem ze względu na możliwą korelację pomiędzy tymi samymi zmiennymi i niepotrzebnym

[5] *Codebook: Inclusion Criteria and Variables*, Global Terrorism Database, sierpień 2018 r., https://www.start.umd.edu/gtd/downloads/Codebook.pdf [dostęp: 30 V 2022].

skomplikowaniu zbioru danych, co przekłada się na spowolnienie procesu treningu modeli.

	count	unique	top	freq
country_txt	154260	202	Iraq	23407
region_txt	154260	12	Middle East & North Africa	43858
provstate	154260	2380	Baghdad	7563
city	153874	34443	Unknown	7594
summary	112205	109189	09/00/2016: Sometime between September ...	100
attacktype1_txt	154260	9	Bombing/Explosion	79879
targtype1_txt	154260	22	Private Citizens & Property	43145
targsubtype1_txt	144441	112	Unnamed Civilian/Unspecified	11599
corp1	123010	32224	Unknown	18458
target1	153807	73022	Civilians	7489
natlty1_txt	152648	209	Iraq	23077

Rysunek 3. Fragment statystyk zmiennych kategorycznych.

Źródło: opracowanie własne.

Widoczny jest również problem w postaci wysokiej liczby unikalnych wartości niektórych zmiennych, jak np. *city*, co mogło wpłynąć na wydajność budowanych modeli. Ten problem został rozwiązany podczas przetwarzania danych poprzez usunięcie takich zmiennych ze zbioru danych.

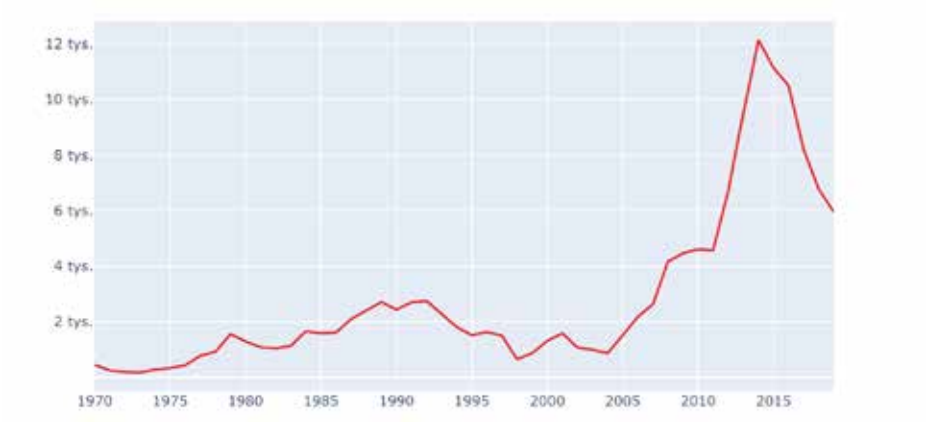
W kolejnym etapie usunięto puste wartości ze zmiennych mających wpływ na liczbę rannych i zabitych. Następnie rozwiązano problem podawania łącznie liczby ofiar zabitych i rannych w wyniku zdarzenia z liczbą zabitych i rannych terrorystów. Odjęto liczbę terrorystów od ogólnej liczby zabitych i rannych w celu uzyskania liczby poszkodowanych niebędących terrorystami.

Po tej operacji utworzono nowe zmienne: *ncasualites* będącą sumą zabitych i rannych oraz *cas_class*, gdzie zerem oznaczono przypadki, w których nie było ofiar, a jedynką te zdarzenia, w których wystąpiły ofiary. Następnie zapisano wstępnie przeprocesowane dane do nowego pliku.

Trendy w liczbie ataków terrorystycznych i liczbie ofiar

Sporządzono wizualizacje części zmiennych, co pozwoliło na ich dogłębniejszą analizę. Na wykresach przedstawiono liczbę ataków terrorystycznych przeprowadzonych w latach 1970–2019 i ich ofiar.

Od drugiej połowy lat 70. do początku lat 90. XX w. wzrastała liczba ataków (wykres 1), jak również ich ofiar (wykres 2). Wyraźny wzrost w liczbie ofiar w 2001 r. jest spowodowany atakiem na World Trade Center (WTC) z 11 września. Kolejny zauważalny trend wzrostowy w obu przypadkach nastąpił w 2005 r. i utrzymywał się do 2014–2015 r. Przy czym, jak już wspomniano, wzrost ok. 2012 r. jest częściowo spowodowany zmianą metodyki zbierania danych[6], jednakże ten wzrost rozpoczął się jeszcze przed rokiem 2005. Od 2015 r. widać trend spadkowy w liczbie zarówno ataków, jak i ofiar. Na dzień 4 czerwca 2022 r.[7] badacze z konsorcjum START nie opublikowali danych z lat 2020–2021, więc nie jest znany wpływ pandemii COVID-19 na dynamikę występowania ataków terrorystycznych.

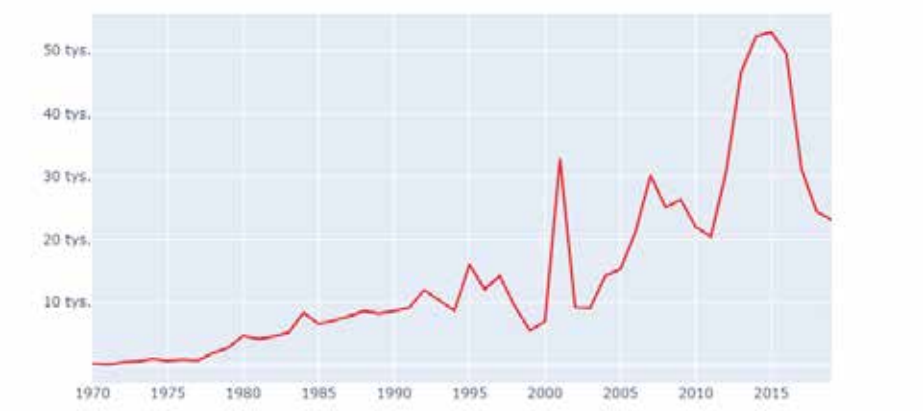


Wykres 1. Liczba ataków terrorystycznych w latach 1970–2019.

Źródło: opracowanie własne.

[6] Identyfikacja incydentów terrorystycznych do GTD przed 2012 r. wymagała użycia ok. 300 unikalnych źródeł wiadomości, a po aktualizacji z 2012 r. – ponad 1500. Były to międzynarodowe agencje informacyjne oraz angielskie tłumaczenia lokalnych gazet publikowanych w różnych językach.

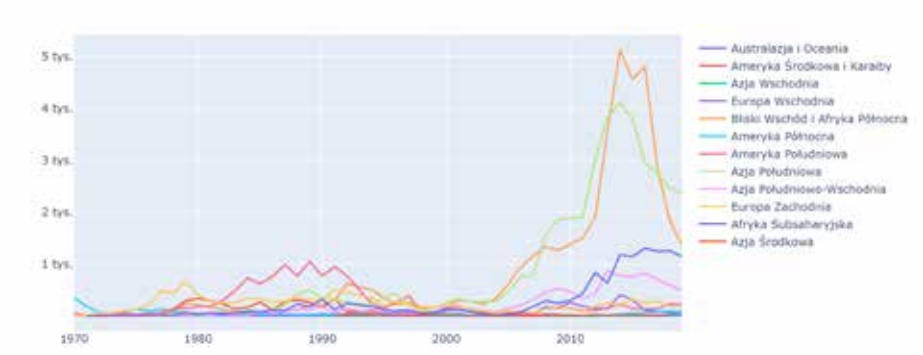
[7] Aktualizacja – na dzień 15 lipca 2023 r. są dostępne dane z pierwszej połowy 2021 r.



Wykres 2. Liczba ofiar ataków terrorystycznych w latach 1970–2019.

Źródło: opracowanie własne.

Następnie dokonano wizualizacji liczby zamachów terrorystycznych i ich ofiar z podziałem na regiony (wykresy 3 i 4).



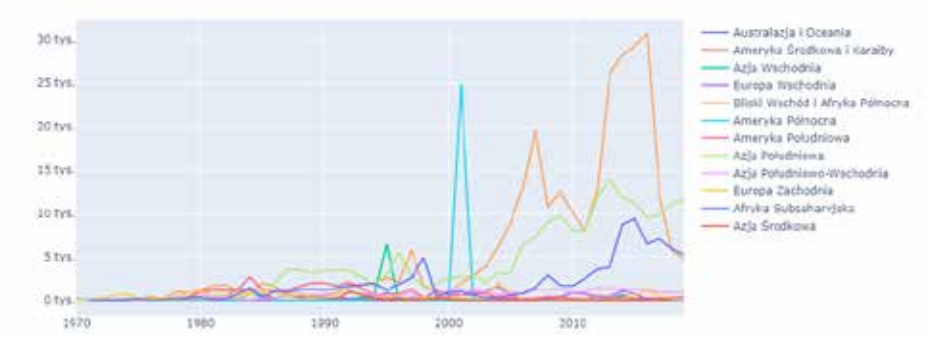
Wykres 3. Liczba ataków terrorystycznych w latach 1970–2019 z podziałem na regiony.

Źródło: opracowanie własne.

W Europie Zachodniej najwięcej zamachów przeprowadzono w drugiej połowie lat 70., co nie przełożyło się na wzrost liczby ofiar. Podobną sytuację można zaobserwować w Ameryce Południowej w latach 1980–1995, kiedy to dynamicznie wzrosła liczba ataków (co również nie miało przełożenia na liczbę ofiar). W latach 90. nastąpił spadek liczby ataków we wszystkich regionach. Mimo to w Afryce Subsaharyjskiej, na Bliskim

Wschodzie i w Afryce Północnej oraz Azji Południowej i Azji Wschodniej zaobserwowano wzrost liczby ofiar. Widoczny gwałtowny wzrost liczby ofiar w 2001 r. w Ameryce Północnej nie jest efektem błędu we wprowadzaniu danych – wtedy miał miejsce zamach na WTC.

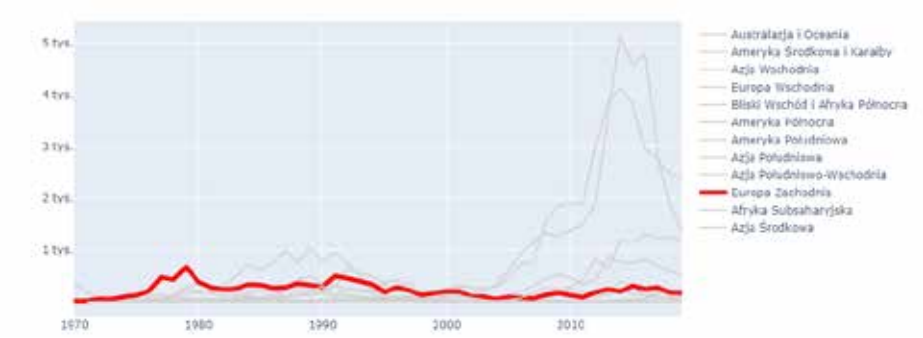
W regionie Bliskiego Wschodu i Afryki Północnej, Azji Południowej oraz w Afryce Subsaharyjskiej zaobserwowano również wzrost liczby ataków i ofiar na początku 2000 r. Szczególnie wyróżnia się krzywa wzrostu na Bliskim Wschodzie, która jest bardziej stroma od krzywych dwóch wcześniej wymienionych regionów. Może to mieć związek z interwencją Stanów Zjednoczonych w Afganistanie oraz Iraku. Na Bliskim Wschodzie w 2000 r. liczba ofiar wyniosła ok. 900, a w 2005 r. było to już prawie 9000. Od 2015 r. jest widoczny trend spadkowy liczby zarówno ataków terrorystycznych, jak i ofiar (wyjątkiem jest Azja Południowa, w której obserwuje się trend wzrostowy pod względem liczby ofiar).



Wykres 4. Liczba ofiar ataków terrorystycznych w latach 1970–2019 z podziałem na regiony.

Źródło: opracowanie własne.

Warto zwrócić uwagę na obszar Europy Zachodniej w tym okresie, ponieważ pomimo kryzysu migracyjnego z 2015 r. nie odnotowano tam wyraźnego wzrostu liczby ataków terrorystycznych (wykres 5).



Wykres 5. Liczba ataków terrorystycznych w Europie Zachodniej latach 1970–2019.

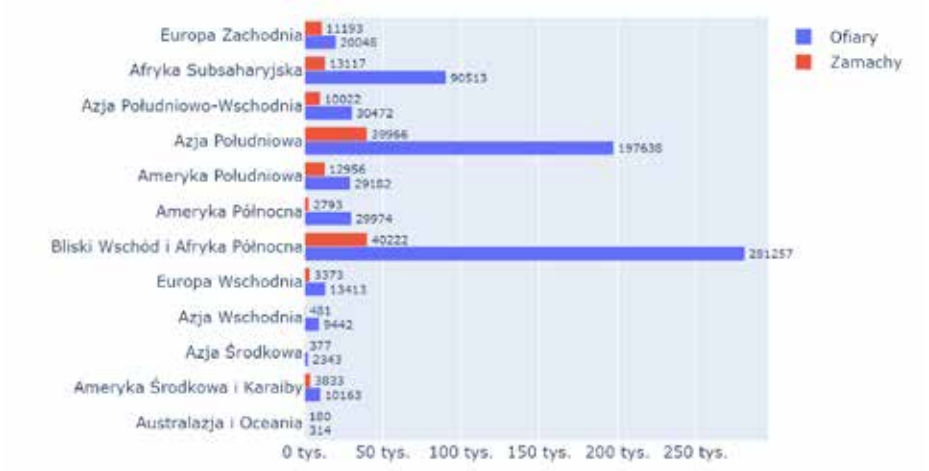
Źródło: opracowanie własne.

W tabeli 1 i na wykresie 6 zawarto informacje na temat stosunku liczby ofiar do liczby zamachów nazywanego dalej współczynnikiem ofiar, co jest bardziej miarodajnym wskaźnikiem niż bezpośrednie porównywanie danych.

Tabela 1. Porównanie współczynnika ofiar ataków terrorystycznych dla poszczególnych regionów.

Region	Współczynnik ofiar
Azja Wschodnia	19,6:1
Ameryka Północna	10,7:1
Bliski Wschód i Afryka Północna	7,0:1
Afryka Subsaharyjska	6,9:1
Azja Środkowa	6,2:1
Azja Południowa	5,0:1
Europa Wschodnia	4,0:1
Azja Południowo-Wschodnia	3,0:1
Ameryka Środkowa i Karaiby	2,7:1
Ameryka Południowa	2,3:1
Europa Zachodnia	1,8:1
Australazja i Oceania	1,7:1

Źródło: opracowanie własne.



Wykres 6. Liczba ataków terrorystycznych oraz liczba ofiar z podziałem na regiony.

Źródło: opracowanie własne.

Zamachy w regionie Bliskiego Wschodu i Afryki Północnej oraz Azji Południowej – pomimo największych liczb bezwzględnych – nie są najbardziej śmiercionośne. Najwyższy współczynnik ofiar występuje w Azji Wschodniej i prawie dwukrotnie przewyższa znajdującą się na drugim miejscu Amerykę Północną. Na trzecim miejscu znalazła się Afryka Subsaharyjska. Średnio najniższy współczynnik ofiar mają zamachy przeprowadzone w Australazji i Oceanii oraz w Europie Zachodniej. Z tych statystyk wynika, że w przypadku terroryzmu podział na bogatą północ i biedne południe nie znajduje bezpośredniego przełożenia. Część biedniejszych regionów, takich jak Ameryka Południowa, Azja Południowo-Wschodnia czy też Ameryka Środkowa i Karaiby, nie odnotowuje wyraźnie wyższego współczynnika ofiar niż bogatsze regiony. Może to wskazywać na czynniki pozaekonomiczne, które wpływają na skuteczność działań terrorystów.

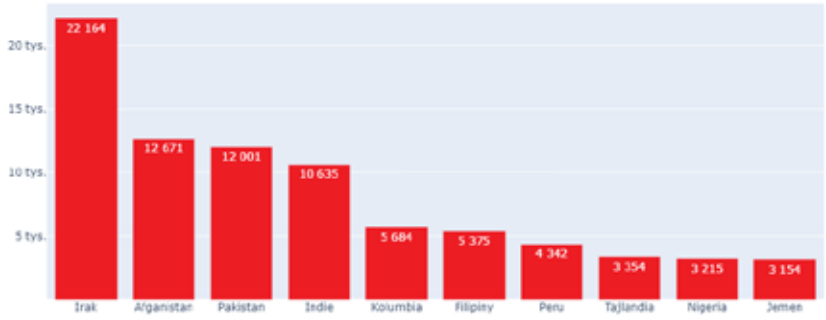
Po przeanalizowaniu danych wskazano kolejno dziesięć krajów z największą liczbą ataków terrorystycznych przeprowadzonych w latach 1970–2019 (wykres 7) oraz dziesięć krajów z największą liczbą ofiar tych ataków (wykres 8).

Kraje te (z podziałem na regiony[8]) to:

- Bliski Wschód i Afryka Północna: Irak, Jemen, Syria;
- Azja Południowa: Afganistan, Pakistan, Indie, Sri Lanka;

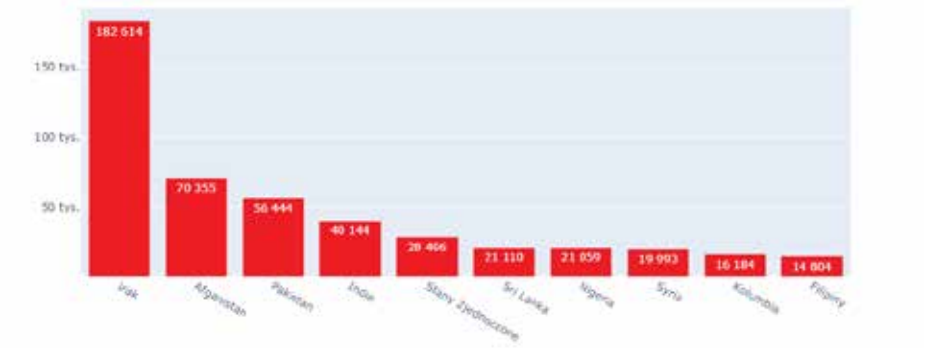
[8] Kraje przypisano do regionów zgodnie z *Codebookiem*.

- Azja Południowo-Wschodnia: Filipiny, Tajlandia;
- Ameryka Południowa: Kolumbia, Peru;
- Ameryka Północna: Stany Zjednoczone;
- Afryka Subsaharyjska: Nigeria.



Wykres 7. Liczba ataków terrorystycznych w krajach zajmujących dziesięć pierwszych miejsc pod względem liczby tych ataków.

Źródło: opracowanie własne.



Wykres 8. Liczba ofiar ataków terrorystycznych w krajach zajmujących dziesięć pierwszych miejsc pod względem liczby tych ofiar.

Źródło: opracowanie własne.

Ze względu na relatywnie niewielką liczbę ataków i ofiar w porównaniu z innymi państwami na liście nie ma żadnego kraju z Azji Wschodniej (pomimo wysokiego współczynnika ofiar). Najbardziej dotknięty tym problemem jest Irak, w którym prawie dwa razy częściej niż w Afganistanie

przeprowadzano ataki terrorystyczne, co przekłada się na ponaddwukrotnie większą liczbę ofiar. Pozostałe kraje ujęte w zestawieniu mają już bardziej zbliżone do siebie wartości zarówno pod względem liczby ataków terrorystycznych, jak i ofiar tych zdarzeń.

W tabeli 2 wskazano współczynnik ofiar dla krajów, w których było ich najwięcej. Najwyższe współczynniki mają: Syria (12,8), Stany Zjednoczone (12,0) i Sri Lanka (11,2). Średnio najmniej ofiar zamachu było w Kolumbii i na Filipinach.

Tabela 2. Porównanie współczynnika ofiar ataków terrorystycznych dla dziesięciu krajów z największą liczbą tych ofiar.

Kraj	Współczynnik ofiar
Syria	12,8:1
Stany Zjednoczone	12,0:1
Sri Lanka	11,2:1
Irak	8,2:1
Nigeria	6,6:1
Afganistan	5,6:1
Pakistan	4,7:1
Indie	3,8:1
Kolumbia	2,8:1
Filipiny	2,8:1

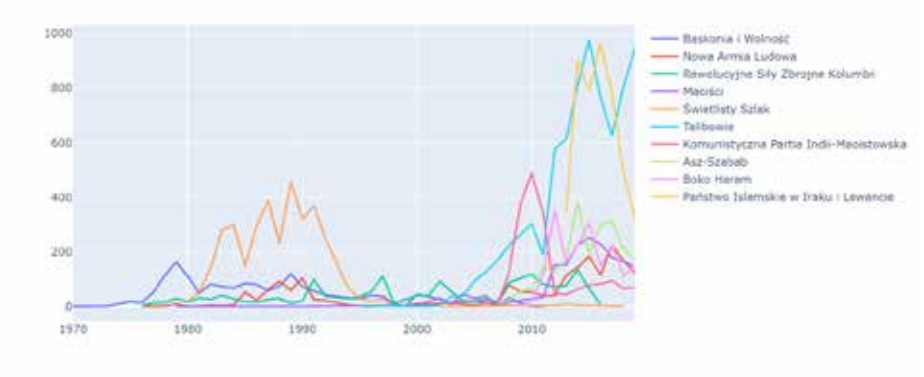
Źródło: opracowanie własne.

Można więc wysunąć wniosek, że czynniki geograficzne mają związek z tym, czy atak terrorystyczny zakończy się ofiarami, czy też nie. Wzięto je więc pod uwagę w trakcie modelowania i został przeanalizowany ich wpływ na wynik predykcji.

Aktywność wybranych grup terrorystycznych

Następnie dokonano analizy aktywności grup odpowiedzialnych za zamachy terrorystyczne. Na wykresie 9 przedstawiono najaktywniejsze grupy terrorystyczne w latach 1970–2019. Dziesięć pierwszych miejsc zajmują grupy powiązane z terroryzmem islamskim: Talibowie (ang. *Taliban*),

Asz-Szabab (ang. *Al-Shabaab*), Boko Haram, Państwo Islamskie (ang. *Islamic State*, ISIS) znane też jako Państwo Islamskie w Iraku i Lewancie (ang. *Islamic State of Iraq and the Levant*, ISIL) oraz z terroryzmem o charakterze skrajnie lewicowym: Baskonia i Wolność (ang. *Basque Fatherland and Freedom*, ETA), Nowa Armia Ludowa (ang. *New People's Army*, NPA), Rewolucyjne Siły Zbrojne Kolumbii (ang. *Revolutionary Armed Forces of Colombia*, FARC), Maoiści (ang. *Maoists*), Świetlisty Szlak (ang. *Shining Path*, hiszp. Sendero Luminoso, SL), Komunistyczna Partia Indii (Maoistowska), ang. *Communist Party of India-Maoist* (CPI-Maoist). Może to wskazywać na pewną korelację pomiędzy motywacją grupy do przeprowadzenia ataku a jej wysoką aktywnością, jednakże w GTD poszczególne grupy nie mają przypisanych charakterystyk. Może to być wskazówka dla badaczy z konsorcjum START, żeby uaktualnić GTD w tym zakresie.



Wykres 9. Liczba ataków terrorystycznych przeprowadzonych w latach 1970–2019 przez dziesięć najbardziej aktywnych grup terrorystycznych.

Źródło: opracowanie własne.

Najstarszą grupą ze wszystkich wyżej wymienionych jest ETA, która w badanym okresie najaktywniej działała w latach 1970–1980, a od początku lat 90. była coraz mniej aktywna. Ostatni odnotowany w GTD zamach został przeprowadzony przez tę grupę w 2011 r. Najprawdopodobniej wiąże się to

z zakończeniem działań zbrojnych tej organizacji w październiku tego samego roku[9]. ETA ostatecznie dokonała samorozwiązania w 2018 r.[10]

Aktywny w dosyć wysokim stopniu był również Świetlisty Szlak, którego działalność przypadła przede wszystkim na lata 1980–1990. Później nastąpił wyraźny spadek liczby zamachów przeprowadzanych przez tę grupę. Prawdopodobnie wynikało to z zatrzymania jej kolejnych przywódców w latach 90. oraz w 2012 r.[11] Aktywna pozostała jedna z frakcji Świetlistego Szlaku, czyli Zmilitaryzowana Komunistyczna Partia Peru (ang. *Militarized Communist Party of Peru*), która w 2018 r. odżegnała się od SL[12].

Kolejną grupą, której wzmożona działalność przypadła na lata 80., jest NPA operująca na Filipinach. Powstała ona w 1969 r. jako zbrojne ramię Komunistycznej Partii Filipin[13]. Spadek aktywności tej grupy po 1990 r. może wynikać z aresztowania postaci kluczowych dla tej organizacji oraz z czystek wewnętrznych[14]. Ponadto NPA zrywała, m.in. w 1986 r. i 2010 r., różnego rodzaju zawieszenia broni oraz negocjacje[15]. Kolejny wzrost aktywności tej grupy odnotowuje się od 2013 r. NPA, w odróżnieniu od SL i ETA, pozostaje aktywna.

Rewolucyjne Siły Zbrojne Kolumbii powstały w 1964 r. Pierwotnie celem tej organizacji było obalenie rządu Kolumbii[16]. W latach 2008–2015 nastąpił wzrost aktywności terrorystycznej tej grupy. Pomimo że od 2012 r. rząd podejmował próby negocjacji z FARC, w tym zawierano zawieszania broni, to grupa regularnie je łamała[17]. W 2016 r. doszło do porozumienia między rządem a FARC, które przekształciły się w partię polityczną

---

[9] *Basque group Eta says armed campaign is over*, BBC News, 20 X 2011 r., https://www.bbc.com/news/world-europe-15393014 [dostęp: 6 VI 2022].

[10] I. Binnie, *Basque separatist group ETA says it has „completely dissolved"*, Reuters, 2 V 2018 r., https://www.reuters.com/article/us-spain-eta-idUSKBN1I31TP [dostęp: 6 VI 2022].

[11] S. Saffón, *Peru in Familiar Stalemate With Shining Path Rebels*, InSight Crime, 4 IX 2020 r., https://insightcrime.org/news/brief/peru-stalemate-shining-path/ [dostęp: 8 VI 2022].

[12] Tamże.

[13] *Communist Part of the Philippines – New People's Army*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/communist-party-philippines-new-peoples-army [dostęp: 11 VI 2022].

[14] Tamże.

[15] Tamże.

[16] *Revolutionary Armed Forces of Colombia (FARC)*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/revolutionary-armed-forces-colombia-farc [dostęp: 8 VI 2022].

[17] Tamże.

i zaprzestały działalności zbrojnej[18]. Według danych GTD od 2016 r. ta organizacja nie przeprowadziła ani jednego zamachu.

Komunistyczna Partia Indii (Maoistowska) to grupa zdelegalizowana przez indyjski rząd[19]. Wzrost aktywności CPI-Maoist w 2009 r. oraz jej późniejszy spadek może być związany z operacją kontrterrorystyczną „Green Hunt" wymierzoną w tę organizację[20]. Pomimo podjętych wysiłków nie udało się jej rozbić. Maoiści z kolei to zbiorcza nazwa terrorystycznych grup skrajnie lewicowych niewchodzących w skład CPI-Maoist[21].

Talibowie powstali jako organizacja w 1994 r. i w latach 1996–2001 rządzili w Afganistanie[22]. Gwałtowny wzrost ich aktywności jest zauważalny po 2001 r., kiedy pokonano ich militarnie, jednak organizacja nie została rozbita. Talibowie powrócili do władzy w 2021 r.

Asz-Szabab jest organizacją wywodzącą się z Somalii, działającą na obszarze wschodniej Afryki oraz Jemenu. Szczyt aktywności grupy przypadł na rok 2014. Rok później odnotowano jednak spadek, który mógł być spowodowany uśmierceniem w 2014 r. przez Stany Zjednoczone jednego z liderów organizacji, co okazało się dla niej dużą stratą[23]. Pomimo wysiłków podejmowanych przez rząd somalijski oraz Stany Zjednoczone w celu zwalczenia tej organizacji jest ona nadal aktywna.

Boko Haram powstała w Nigerii w 2002 r.[24] i rozpoczęła swoją działalność jako organizacja terrorystyczna w 2009 r., kiedy doszło do strzelaniny

---

[18] Tamże.

[19] *Left Wing Extremism Division*, Ministry of Home Affairs, https://web.archive.org/web/20220707070953/https://www.mha.gov.in/division_of_mha/left-wing-extremism-division [dostęp: 8 VI 2022].

[20] A. Sethi, *Green Hunt: the anatomy of an operation*, The Hindu, 6 II 2010 r., https://www.thehindu.com/opinion/op-ed/Green-Hunt-the-anatomy-of-an-operation/article16812797.ece. [dostęp: 8 VI 2022].

[21] *Deaths in Maoist attacks down by 21%: Shah at CMs' meeting*, The Times of India, 27 IX 2021 r., https://timesofindia.indiatimes.com/india/deaths-in-naxal-attacks-down-by-21-shah-at-cms-meeting/articleshow/86543018.cms [dostęp: 8 VI 2022].

[22] *The Afghan Taliban*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/afghan-taliban [dostęp: 8 VI 2022].

[23] *Pentagon confirms death of Somalia terror leader*, The Washington Times, 5 IX 2014 r., https://www.washingtontimes.com/news/2014/sep/5/pentagon-confirms-death-of-somalia-terror-leader/ [dostęp: 10 VI 2022].

[24] H. Matfess, *Boko Haram: History and Context*, w: *Oxford Research Encyclopedia of African History*, Oxford University Press 2017, s. 1.

pomiędzy jej członkami a policją[25]. Trudno przewidzieć trendy w aktywności tej grupy, gdyż wpływ na to mają działania władz w postaci np. użycia sił zbrojnych, a także odporność Boko Haram na te działania[26].

Ostatnią omawianą grupą jest Państwo Islamskie. Organizacja powstała w 1999 r. pod nazwą Dżama'at at-Tauhid wa al-Dżihad (arab. *Jama'at al-Tawhid wal-Jihad*), a po interwencji Stanów Zjednoczonych w Iraku przemianowano ją na Al-Ka'idę w Iraku (ang. *Al Qaeda in Iraq*)[27]. Grupa wzmocniła się po wycofaniu się Amerykanów z Iraku. Wykorzystując ten fakt oraz wybuch wojny domowej w Syrii, zaczęła sukcesywnie przejmować tereny obu państw w 2013 r. i 2014 r.[28] W tym okresie organizacja zmieniła nazwę najpierw na Państwo Islamskie w Iraku i Syrii, następnie w czerwcu 2014 r. ogłosiła utworzenie kalifatu i ostatecznie przyjęła nazwę Państwo Islamskie[29]. Dynamika zmian w działaniach grupy jest wyraźnie związana z jej postępami w przejmowaniu terytoriów wyżej wymienionych państw. Szczyt osiągnęła w 2014 r. i do 2017 r. była wysoce aktywna, wyprzedzając niekiedy Talibów. Widoczny spadek aktywności w 2018 r. i 2019 r. wynika najpewniej z utraty przez tę grupę większości terytoriów. W 2017 r. ISIS zostało wyparte z kontrolowanych przez siebie ośrodków miejskich, a dwa lata później organizacja utraciła kontrolę nad ostatnimi terytoriami w prowincji Baghuz w Syrii[30]. Wraz z utratą terytoriów, a co za tym idzie – również środków na prowadzenie operacji, aktywność ISIS sukcesywnie malała. Wyraźny trend spadkowy jest widoczny nadal, jednak pomimo starań sił kurdyjskich, irackich, syryjskich czy też zaangażowania armii Stanów Zjednoczonych grupa pozostaje aktywna.

Warto zwrócić uwagę, że wszystkie najaktywniejsze grupy, pomimo podjęcia różnych działań i środków, w dalszym ciągu prowadzą działalność. Nie dotyczy to tych, które dokonały samorozwiązania na skutek negocjacji podjętych z nimi przez rządy poszczególnych państw.

Dla najbardziej aktywnych grup terrorystycznych obliczono współczynnik ofiar. Jest on przedstawiony w tabeli 3.

---

[25] Tamże, s. 7.

[26] Tamże, s. 15.

[27] *The Islamic State*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state [dostęp: 11 VI 2022].

[28] Tamże.

[29] Tamże.

[30] Tamże.

Tabela 3. Współczynnik ofiar dla najaktywniejszych grup terrorystycznych.

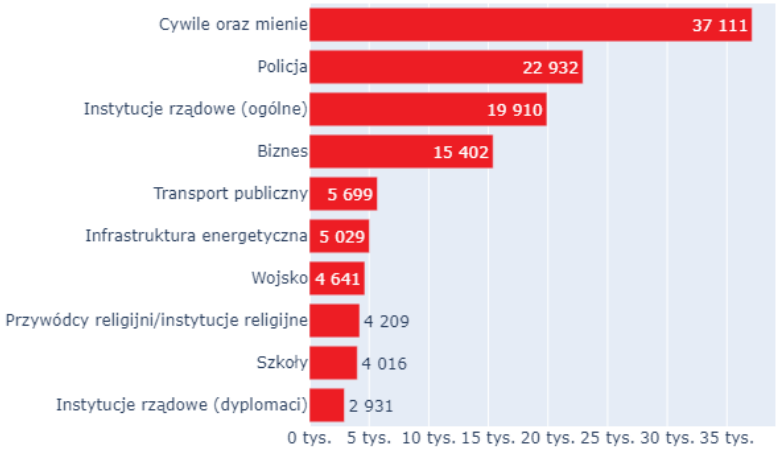
Grupa terrorystyczna	Współczynnik ofiar
Państwo Islamskie	11,0:1
Boko Haram	10,0:1
Al-Szabab	5,8:1
Talibowie	5,8:1
Rewolucyjne Siły Zbrojne Kolumbii	3,6:1
Świetlisty Szlak	2,7:1
Komunistyczna Partia Indii (Maoistowska)	1,9:1
Nowa Armia Ludowa	1,8:1
Baskonia i Wolność	1,6:1
Maoiści	1,4:1

Źródło: opracowanie własne.

Można zauważyć, że współczynnik ofiar dla grup islamistycznych jest znacznie wyższy niż dla grup skrajnie lewicowych. Może to stanowić kolejny argument za dodaniem nowej cechy do zbioru danych – wskazującej na przynależność religijną lub polityczną danej grupy i dalsze eksplorowanie tego zagadnienia. Mogłoby to pozytywnie wpłynąć na doskonalenie modeli uczenia maszynowego w zakresie predykcji ofiar zamachów terrorystycznych.

Najczęstsze cele ataków terrorystycznych

Następnie dokonano wizualizacji charakterystyki ataków terrorystycznych w tym ich celów i typów. Na wykresie 10 przedstawiono w kolejności najczęstsze cele ataków terrorystycznych przeprowadzonych w latach 1970–2019. Były to: cywile oraz mienie, policja, instytucje rządowe (ogólne), biznes, transport publiczny, infrastruktura energetyczna, wojsko, przywódcy religijni lub instytucje religijne, szkoły, instytucje rządowe (dyplomaci).



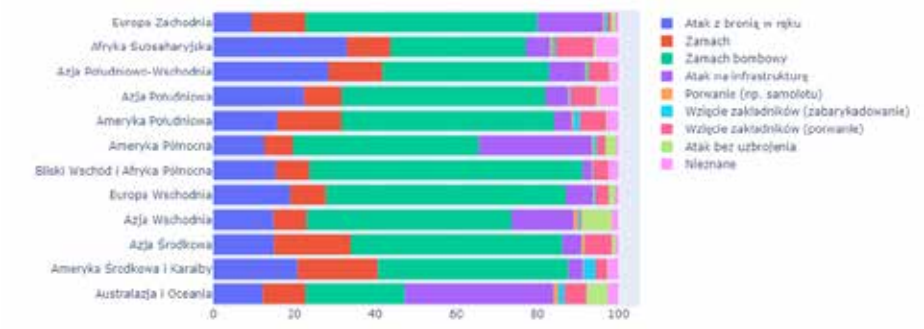
Wykres 10. Najczęstsze cele ataków terrorystycznych z uwzględnieniem liczby przeprowadzonych na nie ataków.

Źródło: opracowanie własne.

Duża liczba ataków skierowanych w cywili oraz mienie może świadczyć o chęci zastraszenia opinii publicznej w danym państwie, a tym samym wpłynięcia na działania jego rządu. Z kolei ataki na policję, wojsko czy też instytucje rządowe mogą sygnalizować motywację polityczną grup terrorystycznych, często uważających władze państw za wroga, którego należy zwalczyć. Ataki na szeroko pojęty sektor prywatny, przeprowadzane np. przez FARC, mogą wskazywać na skrajnie lewicowe motywacje takich grup. Ich celem w dalszej perspektywie może być doprowadzenie do zniesienia własności prywatnej.

Typy ataków terrorystycznych

Sprawdzono również, jaki typ ataku terrorystycznego był przeprowadzany najczęściej (wykres 11). Uwzględniono podział na regiony, co pozwoliło na lepsze uwidocznienie specyfiki ataków dokonywanych w różnych częściach świata.



Wykres 11. Procentowy udział różnych typów ataków terrorystycznych z uwzględnieniem podziału na regiony.

Źródło: opracowanie własne.

Największy odsetek we wszystkich badanych regionach, z wyłączeniem Australazji i Oceanii, stanowiły ataki przeprowadzone przy użyciu materiałów wybuchowych. Ponadto częste były napaść z bronią w ręku i zabójstwo oraz – w niektórych regionach – ataki na infrastrukturę. Może to stanowić wskazówkę dla rządów państw, na jaki typ ataku instytucje państwowe powinny być przygotowane. Wówczas mogą one dokonywać oceny, czy służby właściwe w zakresie zwalczania zagrożenia terrorystycznego mają wypracowane odpowiednie procedury na wypadek danego typu zdarzenia oraz czy służba zdrowia będzie na tyle wydolna, żeby skutecznie zaopiekować się rannymi (mogłoby to zmniejszyć liczbę ofiar śmiertelnych). Taka ewaluacja obecnych możliwości instytucji państwowych wskazałaby pewne luki w odporności (ang. *resilience*) na tego typu zdarzenia.

Przetwarzanie danych

W kolejnym etapie dokonano przetworzenia danych. W pierwszej kolejności wyselekcjonowano ostateczne zmienne użyte do modelowania. Przedstawiono je w tabeli 4.

Tabela 4. Opis zmiennych użytych do przeprowadzenia badania.

Nazwa zmiennej	Opis zmiennej
Extended	określa, czy czas trwania zdarzenia przekroczył 24 godziny

Country_txt	określa kraj, w którym wystąpiło zdarzenie
Region	określa region, w którym wystąpiło zdarzenie
Latitude	określa szerokość geograficzną miejsca, w którym wystąpiło zdarzenie
Longitude	określa długość geograficzną miejsca, w którym wystąpiło zdarzenie
Specificity	określa rozdzielczość geoprzestrzeni pól szerokości i długości geograficznej. Najbardziej szczegółowa rozdzielczość dostępna w całym zbiorze danych to środek miasta, wsi lub miejscowości, w której nastąpił atak. Współrzędne o większej rozdzielczości, chociaż możliwe, nie są systematycznie umieszczane w bazie danych
Vicinity	określa, czy zdarzenie wystąpiło w bezpośrednim sąsiedztwie danego miasta
Multiple	określa, czy dany atak terrorystyczny jest powiązany z innymi zamachami
Success	sukces zamachu terrorystycznego definiuje się na podstawie jego namacalnych skutków. Sukcesu nie ocenia się w kategoriach szerszych celów sprawców. Na przykład bomba, która eksplodowała w budynku, zostałaby uznana za sukces, nawet gdyby nie udało się zniszczyć budynku ani wywołać represji rządowych
Suicide	określa, czy dany atak był zamachem samobójczym
Attack type1	określa typ ataku terrorystycznego
Targ type1	określa typ celu ataku terrorystycznego
Targ subtype1	określa bardziej szczegółowo kategorię celu
Natlty1	jest to narodowość zaatakowanego celu, niekoniecznie tożsama z krajem, w którym doszło do zdarzenia, choć zazwyczaj tak właśnie jest. W przypadku porwania samolotu rejestruje się jego przynależność państwową, a nie narodowość pasażerów
Gname	zawiera nazwę grupy, która przeprowadziła atak

Guncertain1	określa, czy informacje podawane przez źródła na temat grupy odpowiedzialnej za atak są oparte na spekulacjach lub wątpliwych roszczeniach dotyczących odpowiedzialności
Individual	określa, czy atak został przeprowadzony przez osobę lub kilka osób, o których nie wiadomo, czy są powiązane z grupą lub organizacją terrorystyczną
Nperps	określa łączną liczbę terrorystów uczestniczących w zdarzeniu
Claimed	służy do wskazania, czy grupa lub osoba (-y) przyznała się do ataku
Weaptype1	określa rodzaj użytej broni
Weapsubtype1	określa bardziej szczegółowo kategorię broni
Property	określa, czy w wyniku zdarzenia zostało uszkodzone mienie
Ishostkid	określa, czy podczas zdarzenia ofiary zostały pojmane jako zakładnicy lub porwane
Int_log	wskazuje, czy w celu przeprowadzenia ataku grupa sprawców przekroczyła granicę
Int_misc	wskazuje, czy grupa sprawców zaatakowała cel innej narodowości
Int_any	określa, czy zostały spełnione wszystkie warunki zmiennych z przedrostkiem *int*
Cas_class	określa, czy zdarzenie spowodowało ofiary

Źródło: opracowanie własne na podstawie: *Codebook: Inclusion Criteria and Variables*, Global Terrorism Database, sierpień 2018 r., http://www.start-dev.umd.edu/gtd/downloads/Codebook.pdf [dostęp: 30 V 2022].

Ten zabieg spowodował zmniejszenie liczby kolumn z 60 do 28. Ograniczenie liczby cech przyspieszy modelom uczenia maszynowego proces treningu. Ze względu na to, że część kolumn występuje w formie liczbowej lub tekstowej, jak np. *region* i *region_txt,* zdecydowano się w takim przypadku na wybór tylko jednej kolumny w celu uproszczenia zbioru danych. Zostały usunięte również kolumny zawierające takie metadane, jak unikalny identyfikator zdarzenia czy też pierwotne źródło danych. Nie wzięto pod uwagę zmiennych określających warunki włączenia danego zdarzenia do GTD, ponieważ – jak już wspomniano – zostały odfiltrowane te ataki, które nie

spełniały wszystkich warunków, oraz te, co do których istniały wątpliwości. Tym samym te zmienne nie dostarczają modelom uczenia maszynowego istotnych informacji wpływających na predykcję, a tylko wydłużałyby proces treningu. Ostatnią grupą usuniętych cech są zmienne określające liczbę ofiar lub rannych. Wyeliminowanie ich miało na celu uniknięcie wycieku danych (ang. *data leakage*), przez co wyniki badania byłyby niemiarodajne.

Następnie sprawdzono, jak wiele ataków terrorystycznych zakończyło się ofiarami. W ok. 59% przypadków doszło do zabicia lub ranienia co najmniej jednej osoby niebędącej terrorystą. To oznacza, że występuje niezbalansowanie klas w przewidywanej zmiennej, co może negatywnie wpłynąć na wynik predykcji. Ten problem został rozwiązany podczas budowania modeli uczenia maszynowego poprzez ustawienie parametru *class weight* na wartość *balanced*. Dzięki temu modele zwracają większą uwagę na klasę mniej liczną, co pomaga zrównoważyć wpływ każdej klasy na model, zwiększając tym samym ogólną skuteczność predykcji.

W dalszej kolejności dokonano podziału na zbiór treningowy (80% danych) oraz testowy (pozostałe 20%). Zastosowano przy tym próbkowanie warstwowe (ang. *stratified sampling*), żeby zapewnić podobne rozłożenie klas przewidywanej zmiennej jak w całym zbiorze danych.

W kolejnym kroku utworzono potok (ang. *pipeline*) dokonujący ostatecznych przekształceń na zbiorze danych.

Pierwszym etapem jest transformacja zmiennych *country_txt* oraz *gname* z formy tekstowej na liczbową, ponieważ zbudowane modele uczenia maszynowego mogą pracować wyłącznie na danych w takiej postaci. Z powodu dużej liczby unikalnych wartości w obu kolumnach zdecydowano się na zakodowanie ich na podstawie liczebności występowania. Ta metoda – w przeciwieństwie do metody kodowania 1 z n (ang. *one-hot encoding*), której efektem jest powstanie takiej liczby kolumn, ile jest unikalnych wartości – nie ma efektów ubocznych w postaci zwiększenia wymiarowości danych.

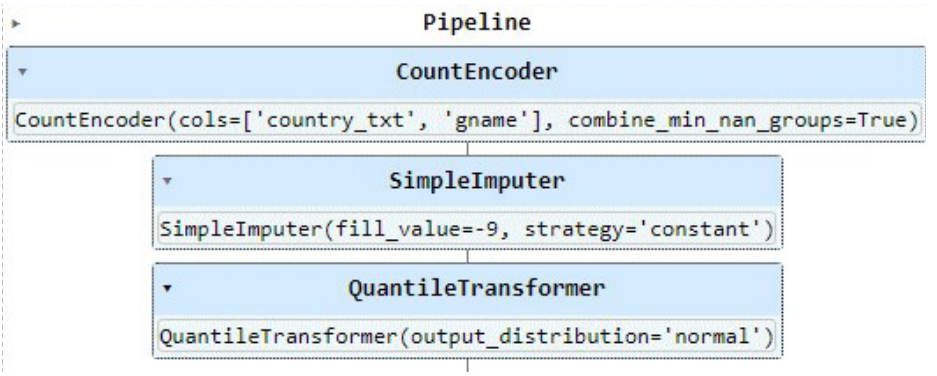
Następnie zamieniono wartości puste na -9. W ten sposób w GTD koduje się wartości, co do których badacze nie mieli wystarczających informacji, aby w sposób jednoznaczny przypisać konkretną wartość do danej cechy zdarzenia[31].

W ostatnim etapie dokonano normalizacji danych ze względu na to, że część zbudowanych modeli, takich jak np. regresja logistyczna czy maszyny

[31] *History of the GTD…*

wektorów nośnych, jest wrażliwa na skrajnie różne skale wartości. Ta metoda rozwiązuje problem i może przełożyć się na lepsze wyniki tych modeli oraz przyspieszyć proces uczenia.

Warto wskazać, że obliczanie liczebności występowania danych wartości powinno się odbywać wyłącznie na zbiorze treningowym. Na zbiorze testowym zaś dokonuje się transformacji na podstawie wyliczeń ze zbioru treningowego. Jest to istotne, ponieważ inna procedura prowadzi do wycieku danych, a co za tym idzie – rzutuje na wyniki badania. Z tego też powodu zdecydowano się na zastosowanie potoku dostępnego w bibliotece Scikit-learn, dzięki któremu w prosty sposób można kontrolować etapy przekształceń i zredukować tym samym ryzyko pomyłki (rysunek 4).



Rysunek 4. Potok przeprowadzający przekształcenia na zbiorze danych.

Źródło: opracowanie własne.

Na koniec etapu przetwarzania danych zapisano zbiór treningowy oraz testowy do osobnych plików, żeby zachować przeprowadzone przekształcenia i móc po ich późniejszym wczytaniu przejść bezpośrednio do modelowania.

Proces trenowania modeli uczenia maszynowego

Wszystkie modele były trenowane na komputerze stacjonarnym o parametrach: 16 GB RAM, procesor AMD Ryzen 5 3600. Każdy model trenowano w analogiczny sposób: hiperparametry były wyszukiwane za pomocą frameworka Optuna, a metryki zapisywano za pomocą biblioteki

MLFlow. Aby uniknąć niepotrzebnych powtórzeń, proces trenowania zostanie pokazany tylko na przykładzie drzewa decyzyjnego (rysunek 5).

Rysunek 5. Fragment kodu odpowiedzialny za wyszukiwanie hiperparametrów.

Źródło: opracowanie własne.

W pierwszej linijce zdefiniowano funkcję, której nazwa oraz przyjmowane argumenty są zgodne z konwencją przyjętą w Optunie. W linijkach 2–7 określono przestrzeń hiperparametrów. W późniejszym etapie została ona przeszukana w celu znalezienia jak najlepszej ich kombinacji. Dla linijek 2–3 oznaczono przedział, w którym wartości tych hiperparametrów mają zostać wyszukiwane, i w tym wypadku będzie to liczba całkowita. Na szczególną uwagę zasługuje linijka 5. Zaznaczono w niej, że waga klas (ang. *class weight*) powinna być zbalansowana (ang. *balanced*). Jest to jedna z metod rozwiązania wcześniej wspomnianego problemu niezbalansowania klas. W dalszej kolejności dokonano inicjalizacji modelu w linijce 9, a następnie określono metryki użyte do oceny modeli, czyli kolejno: dokładność (ang. *accuracy*), precyzję (ang. *precision*), czułość (ang. *recall*) oraz F1. Zostaną one szczegółowo omówione w dalszej części artykułu. W linijce 13 następuje trening modelu na zbiorze treningowym za pomocą walidacji krzyżowej (ang. *cross validation*), a następnie są obliczane wyniki dla poszczególnych zmiennych, które na końcu są zwracane przez tę funkcję.

W kolejnym kroku utworzono tzw. *study*, w którym określa się jego nazwę oraz kierunek optymalizacji metryk. Ze względu na to, że zastosowane metryki dotyczą problemu klasyfikacyjnego, to zostały one

zmaksymalizowane. Następnie dokonuje się przeszukiwania hiperparametrów (rysunek 6), które są zapisywane za pomocą MLFlow (rysunek 7).

```
study = optuna.create_study(study_name="decision_tree",
                            directions=["maximize", "maximize", "maximize", "maximize"])
study.optimize(objective, n_trials=100, callbacks=[mlflow_callback])
```

Rysunek 6. Inicjalizacja wyszukiwania hiperparametrów przez Optunę.

Źródło: opracowanie własne.

	Metrics				Parameters				
	accuracy	f1	precision	recall	criterion	max_depth	max_features	min_samples_lea	min_samples_sp
	0.849	0.868	0.892	0.845	entropy	21	-	38	-
	0.848	0.868	0.887	0.849	entropy	37	-	15	-
	0.848	0.868	0.89	0.846	entropy	33	None	20	82
	0.848	0.867	0.888	0.848	entropy	25	-	17	-
	0.848	0.867	0.89	0.846	entropy	18	None	34	31
	0.848	0.867	0.89	0.846	entropy	18	None	34	31

Rysunek 7. Fragment dashboardu z MLFlow z zapisanymi metrykami i parametrami drzewa decyzyjnego.

Źródło: opracowanie własne.

Dla każdego modelu wykonano kilkaset iteracji w celu wyszukania optymalnych hiperparametrów. Następnie wszystkie modele z optymalnymi dla nich hiperparametrami wytrenowano na całym zbiorze treningowym i dokonano walidacji na zbiorze testowym. Do treningu zostały wybrane te modele, które osiągnęły najwyższe wartości metryki F1. Parametry tych modeli oraz ich wyniki zostaną przedstawione później. Wcześniej opisano poszczególne metryki jakości modeli klasyfikacyjnych użytych podczas badania.

Wybrane miary jakości modeli klasyfikacyjnych

Ze względu na wielość różnych miar jakości znajdujących zastosowanie w ocenie modeli klasyfikacyjnych zostały opisane tylko te miary, których użyto podczas badania.

Dokładność klasyfikatora jest miarą określającą, jak wiele przypadków zostało sklasyfikowanych poprawnie[32]. Można ją przedstawić następującym wzorem:

$$\text{dokładność} = \frac{PP + PN}{FP + FN + PP + PN}$$

gdzie:

- PP, czyli prawdziwie pozytywne (ang. *true positive*, TP) przypadki, kiedy model poprawnie sklasyfikował dane zdarzenie jako powodujące ofiary;
- PN, czyli prawdziwie negatywne (ang. *true negative*, TN) przypadki, kiedy model poprawnie sklasyfikował dane zdarzenie jako niepowodujące ofiar;
- FP, czyli fałszywie pozytywnie (ang. *false positive*, FP) przypadki, kiedy model niepoprawnie sklasyfikował dane zdarzenie jako powodujące ofiary;
- FN, czyli fałszywie negatywne (ang. *false negative*, FN) przypadki, kiedy model niepoprawnie sklasyfikował dane zdarzenie jako niepowodujące ofiar[33].

Dwie kolejne miary, czyli precyzja oraz czułość, są ze sobą bezpośrednio związane. Precyzja promuje sytuację, w której klasyfikator jest pewien swoich decyzji i popełnia jak najmniej błędów rodzaju fałszywie pozytywnego, jednakże kosztem tego jest zwiększenie przewidywań fałszywie negatywnych[34]. Odwrotnie jest w przypadku czułości, ponieważ promuje się tę sytuację, w której klasyfikator dokonuje jak najmniej błędów rodzaju fałszywie negatywnego, jednak kosztem zwiększenia przypadków fałszywie pozytywnych[35]. Jeśli więc zoptymalizujemy klasyfikator w taki sposób, aby minimalizował szanse niepoprawnego sklasyfikowania danego zdarzenia

[32] S. Raschka i in., *Machine Learning with PyTorch and Scikit-Learn: Develop machine learning and deep learning models with Python*, Birmingham 2022, s. 13.

[33] Tamże, s. 195.

[34] Tamże, s. 196.

[35] Tamże.

jako niepowodującego ofiar, to będzie się on cechował wysoką czułością. Wzór na obliczenie czułości jest następujący:

$$\text{czułość} = \frac{PP}{FN + PP}$$

Odbędzie się to jednak kosztem precyzji, wyrażonej wzorem:

$$\text{precyzja} = \frac{PP}{PP + FP}$$

W celu zrównoważenia precyzji i czułości stosuje się miarę F1, która jest średnią harmoniczną precyzji i czułości[36]. Oznacza to, że aby osiągnąć wysoką wartość miary F1, klasyfikator musi mieć wysokie wyniki zarówno w precyzji, jak i czułości, ponieważ średnia harmoniczna przywiązuje większą wagę do niskich wartości[37]. Wartość miary F1 oblicza się następująco:

$$F1 = 2\,\frac{\text{precyzja} \times \text{czułość}}{\text{precyzja} + \text{czułość}}$$

Wyniki badania dla poszczególnych modeli

W tabelach 5–8 zaprezentowano hiperparametry dla poszczególnych modeli uczenia maszynowego, a w tabeli 9 – wyniki ich walidacji na zbiorze testowym. Należy zaznaczyć, że przedstawiono tylko te wartości hiperparametrów, które były wcześniej wyszukiwane. Jeśli jakiś hiperparametr nie znajduje się w tabeli, to oznacza, że przyjmuje wartość domyślną zgodną z dokumentacją właściwej biblioteki. Ze względu na to, że klasyfikator

[36] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, Sebastopol 2019, s. 140.

[37] Tamże.

głosujący oraz klasyfikator oparty na nakładaniu składają się z innych zbudowanych modeli, to ich hiperparametry są identyczne z tymi przedstawionymi w tabelach.

Tabela 5. Wartości hiperparametrów dla regresji logistycznej.

Nazwa hiperparametru	Wartość
C	9,58649376280703
class_weight	balanced
max_iter	500

Źródło: opracowanie własne.

Tabela 6. Wartości hiperparametrów dla liniowej maszyny wektorów nośnych.

Nazwa hiperparametru	Wartość
C	0,0036775852394361204
class_weight	balanced
dual	false
penalty	L1

Źródło: opracowanie własne.

Tabela 7. Wartości hiperparametrów dla drzewa decyzyjnego.

Nazwa hiperparametru	Wartość
criterion	entropy
class_weight	balanced
max_depth	21
min_samples_leaf	38

Źródło: opracowanie własne.

Tabela 8. Wartości hiperparametrów dla lasu losowego.

Nazwa hiperparametru	Wartość
criterion	entropy
class_weight	balanced

max_depth	42
min_samples_split	6
n_estimators	551
max_features	sqrt

Źródło: opracowanie własne.

Tabela 9. Wartości hiperparametrów dla modelu XGBoost.

Nazwa hiperparametru	**Wartość**
colsample_bylevel	0,6783261477402747
colsample_bytree	0,23127225599162296
gamma	0,4906870500968865
learning_rate	0,0675784773135259
max_delta_step	5
max_depth	22
min_child_weight	1
n_estimators	1475
reg_alpha	0,12263684424466229
reg_lambda	1,9559489540115411
scale_pos_weight	0,9676022078596858
subsample	0,976706655475712

Źródło: opracowanie własne.

W tabeli 10 znajdują się wyniki poszczególnych modeli wraz z ich czasem treningu. Najlepsze wyniki z danej kategorii zostały wytłuszczone.

Tabela 10. Wyniki poszczególnych modeli uczenia maszynowego.

Nazwa modelu	**Czas trwania treningu**	**Dokładność**	**Precyzja**	**Czułość**	**F1**
Regresja logistyczna	2,8 s	0,765	0,823	0,762	0,792
Maszyny wektorów nośnych	10,4 s	0,765	0,824	0,763	0,792

Drzewo decyzyjne	**1,0 s**	0,845	0,894	0,835	0,864
Las losowy	1,3 min	0,876	0,891	0,898	0,895
XGBoost	1,4 min	**0,879**	0,890	**0,905**	**0,898**
Klasyfikator głosujący	3,6 min	0,870	0,888	0,891	0,889
Klasyfikator oparty na nakładaniu	7,8 min	**0,879**	**0,904**	0,889	0,896

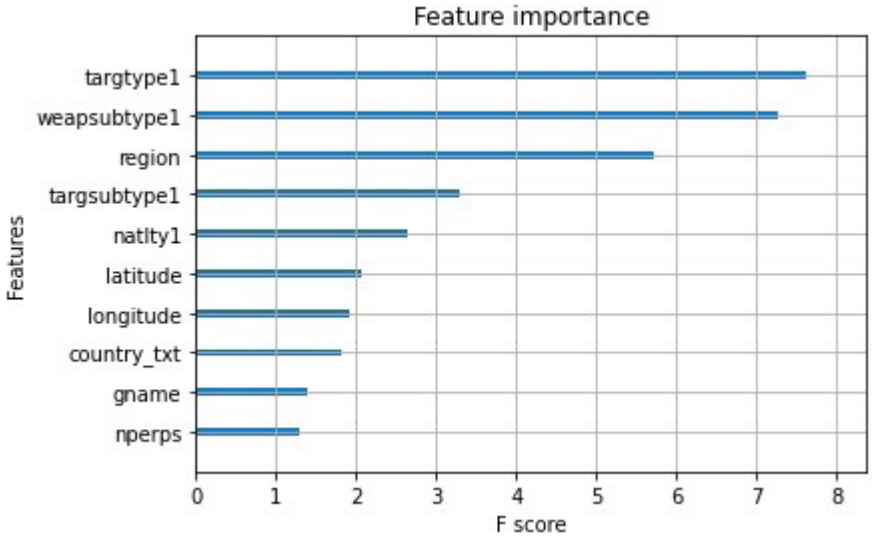
Źródło: opracowanie własne.

Najlepszym modelem pod względem wartości miar jakości jest XGBoost. Ewidentnie gorsze wyniki osiągnęły modele liniowe, czyli regresja logistyczna oraz maszyny wektorów nośnych. W związku z tym w dalszych badaniach prawdopodobnie lepiej będzie się skupić na modelach drzewiastych. Warto zwrócić uwagę na to, że różnica w wynikach pomiędzy XGBoost a klasyfikatorem opartym na nakładaniu jest niewielka, jednakże czas treningu XGBoosta jest ponadpięciokrotnie krótszy. Takie wyniki sugerują, że w dalszych badaniach należy skoncentrować się na modelach drzewiastych opartych na wzmacnianiu gradientowym.

Żadnemu modelowi nie udało się przekroczyć progu 90-procentowej skuteczności w metryce F1 pomimo wielu iteracji przy poszukiwaniu hiperparametrów. Prawdopodobnie do osiągnięcia wyników rzędu ok. 95% potrzebne byłoby rozbudowanie zbioru danych o nowe zmienne, takie jak np. przynależność polityczna/religijna danej grupy terrorystycznej, występowanie w danym kraju napięć na tle etnicznym/politycznym/religijnym, odległość miejsca zdarzenia od najbliższego szpitala.

Zdecydowano się również na obliczenie istotności cech (ang. *feature importance*) dla modelu opartego na bibliotece XGBoost, w celu ustalenia, które cechy były najistotniejsze dla tego modelu podczas dokonywania predykcji. Zostało to zaprezentowane na wykresie 12. Na osi y znajdują się opisane wcześniej cechy, a na osi x ukazano wartość danej cechy dla predykcji. Najważniejsze były cele oraz podtyp broni. Podczas ewaluacji planów kryzysowych na wypadek ataku terrorystycznego te dwa czynniki powinny być szczególnie uważnie przeanalizowane. Zbiór czynników geograficznych, takich jak np. region czy długość i szerokość geograficzna, wskazuje

na to, że terroryzm stanowi problem dla niektórych obszarów świata i ma różną charakterystykę.



Wykres 12. Najistotniejsze cechy dla modelu XGBoost.

Źródło: opracowanie własne.

Wnioski

Przeprowadzono badanie zamachów terrorystycznych występujących w latach 1970–2019, w tym dogłębnie przeanalizowano trendy w aktywności wybranych grup terrorystycznych. Zbudowane modele zespołowe osiągnęły zdecydowanie lepsze wyniki od modeli liniowych.

Uzyskane rezultaty wskazują, że w przyszłości należałoby się skupić na modelach opartych na uczeniu zespołowym, ponieważ modele liniowe, takie jak chociażby regresja logistyczna, poradziły sobie wyraźnie gorzej. W szczególności należy się przyjrzeć modelom drzewiastym opartym na wzmacnianiu gradientowym, gdyż XGBoost uzyskał lepsze wyniki przy krótszym czasie treningu w porównaniu z klasyfikatorem głosującym i klasyfikatorem opartym na nakładaniu. W dalszych badaniach można również sprawdzić skuteczność modeli podobnych do XGBoost, jak np. CatBoost,

LightGBM, lub sprawdzić, jak z takim zadaniem poradziłyby sobie głębokie sieci neuronowe.

Po opublikowaniu przez badaczy z konsorcjum START pełnych danych za lata 2020–2021 warto byłoby dokonać analizy, czy zmieniła się aktywność terrorystów, oraz scharakteryzować ich działania podczas pandemii COVID-19. Również uzupełnienie GTD o nowe zmienne, takie jak np. informacje na temat napięć etnicznych czy religijnych, kondycji ekonomicznej danego państwa czy też przynależności religijnej lub politycznej danej grupy terrorystycznej, mogłoby pozytywnie wpłynąć na wyniki klasyfikacji, w tym pomóc przekroczyć barierę 90%.

Niniejszy artykuł wskazuje, że jest możliwe skuteczne wykorzystanie uczenia maszynowego w zakresie bezpieczeństwa. Może to wspomóc odpowiednie organy przy tworzeniu planów zarządzania kryzysowego w przypadku zaistnienia zdarzenia o charakterze terrorystycznym. Państwo może również podjąć działania edukacyjne w postaci kampanii informacyjnych czy też uczenia w szkołach, jak należy się zachowywać podczas zamachu terrorystycznego w zależności od jego rodzaju. Jak wykazano za pomocą wartości istotności zmiennych, to właśnie cel ataku był najważniejszym czynnikiem dla modelu XGBoost, a jak wskazano wcześniej, najczęściej atakowani są cywile. Dzięki działaniom edukacyjnym prawdopodobnie możliwe byłoby zmniejszenie do pewnego stopnia liczby ofiar zamachów terrorystycznych. Drugim ważnym czynnikiem okazał się podtyp broni, zatem po dogłębnym przeanalizowaniu przez odpowiednie służby środków stosowanych przez grupy terrorystyczne na danym terenie można byłoby opracować nowe regulacje prawne utrudniające terrorystom pozyskiwanie broni.

Bibliografia

Géron A., *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, Sebastopol 2019.

Matfess H., *Boko Haram: History and Context*, w: *Oxford Research Encyclopedia of African History*, Oxford University Press 2017.

Raschka S. i in., *Machine Learning with PyTorch and Scikit-Learn: Develop machine learning and deep learning models with Python*, Birmingham 2022.

Źródła internetowe

Basque group Eta says armed campaign is over, BBC News, 20 X 2011 r., https://www.bbc.com/news/world-europe-15393014 [dostęp: 6 VI 2022].

Binnie I., *Basque separatist group ETA says it has „completely dissolved"*, Reuters, 2 V 2018 r., https://www.reuters.com/article/us-spain-eta-idUSKBN1I31TP [dostęp: 6 VI 2022].

Codebook: Inclusion Criteria and Variables, Global Terrorism Database, sierpień 2018 r., https://www.start.umd.edu/gtd/downloads/Codebook.pdf/ [dostęp: 30 V 2022].

Communist Part of the Philippines – New People's Army, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/communist-party-philippines-new-peoples-army [dostęp: 11 VI 2022].

Data Collection Methodology, Global Terrorism Database, http://www.start-dev.umd.edu/gtd/using-gtd/ [dostęp: 21 V 2022].

Deaths in Maoist attacks down by 21%: Shah at CMs' meeting, The Times of India, 27 IX 2021 r., https://timesofindia.indiatimes.com/india/deaths-in-naxal-attacks-down-by-21-shah-at-cms-meeting/articleshow/86543018.cms [dostęp: 8 VI 2022].

History of the GTD, Global Terrorism Database, https://start.umd.edu/gtd/about/History.aspx [dostęp: 11 V 2022].

Left Wing Extremism Division, Ministry of Home Affairs, https://web.archive.org/web/20220707070953/https://www.mha.gov.in/division_of_mha/left-wing-extremism-division [dostęp: 8 VI 2022].

Pentagon confirms death of Somalia terror leader, The Washington Times, 5 IX 2014 r., https://www.washingtontimes.com/news/2014/sep/5/pentagon-confirms-death-of-somalia-terror-leader/ [dostęp: 10 VI 2022].

Revolutionary Armed Forces of Colombia (FARC), Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/revolutionary-armed-forces-colombia-farc [dostęp: 8 VI 2022].

Saffón S., *Peru in Familiar Stalemate With Shining Path Rebels*, InSight Crime, 4 IX 2020 r., https://insightcrime.org/news/brief/peru-stalemate-shining-path/ [dostęp: 8 VI 2022].

Sethi A., *Green Hunt: the anatomy of an operation,* The Hindu, 6 II 2010 r., https://www.thehindu.com/opinion/op-ed/Green-Hunt-the-anatomy-of-an-operation/article16812797.ece [dostęp: 8 VI 2022].

The Afghan Taliban, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/afghan-taliban [dostęp: 8 VI 2022].

The Islamic State, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state [dostęp: 11 VI 2022].

Jakub Tuszyński

Absolwent studiów magisterskich na Uniwersytecie Warszawskim na kierunku zarządzanie big data.

INNE

https://doi.org/10.4467/27204383TER.23.024.18326
https://orcid.org/0009-0005-0658-0901

Kontrwywiad w działaniach antyterrorystycznych

Esej o relacjach

Tomasz Białek

Gra

Wiele lat temu podczas wykładu o socjologii bezpieczeństwa wewnętrznego zostałem zapytany przez studentów: co to są służby specjalne? Ta oczywista próba usystematyzowania wiedzy przez adeptów socjologii wywołała żywiołową dyskusję. Poprosiłem, aby sami spróbowali udzielić odpowiedzi. Wszystkie definicje okazały się mniej lub bardziej trafne. Niemal za każdym razem pojawiało się słowo „tajne" lub jego synonim – „niejawne". Najwięcej trudności sprawiły próby zdefiniowania działań operacyjnych (które, w przeciwieństwie do służb specjalnych, są przecież szczegółowo opisane w ustawodawstwie), gdyż już sama liczba służb mających uprawnienia do nich jest imponująca. Zapamiętałem ciekawe stwierdzenie, że „specjalne" są takie służby, jak Centralne Biuro Antykorupcyjne czy Służba Ochrony Państwa, dlatego że (uwaga!) „specjalizują się" w zwalczaniu korupcji czy też ochronie władz. W innej definicji nie wymieniono służb mających uprawnienia śledcze (CBA, Agencja Bezpieczeństwa Wewnętrznego). Argument? *Bo są to po prostu służby policyjne*. Najciekawsze jednak okazało

się w jednej z definicji wyłączenie z katalogu służb specjalnych Agencji Wywiadu, Służby Wywiadu Wojskowego i Służby Kontrwywiadu Wojskowego. Argumentowano, że nie są to służby specjalne, lecz wywiadowcze (również w literaturze fachowej przewija się ten punkt widzenia[1]).

Kiedy już się wydawało, że grupa osiąga porozumienie co do definicji, ktoś podawał w wątpliwość jeden z elementów omawianej propozycji. Bardziej dociekliwi doszukiwali się innych znaczeń słów tworzących definicję, a ci z lepszym warsztatem naukowym zastanawiali się, czy nie można by zastosować jej również do innych elementów systemu bezpieczeństwa państwa i nie tylko. Jeden ze studentów zapytał: *Dlaczego tylko państwa? A czy organizacja przestępcza lub duża korporacja nie mogą mieć swoich służb specjalnych?* Końcowy efekt prac nie zadowolił wszystkich w pełni, ale za to wszyscy dowiedzieli się i zrozumieli, czym są służby specjalne.

Przez wiele lat zachęcałem do tej gry zarówno studentów na uczelniach, jak i funkcjonariuszy na szkoleniach. Dyskusja zawsze przebiegała tak samo i kończyła się tymi samymi konstatacjami. Na szczęście bowiem w mądrych podręcznikach są równie mądre definicje mądrych specjalistów, których mądrzy wykładowcy wymagają od mądrych (!) słuchaczy i słuchaczek.

Szyld

Historia tajnych, specjalnych, wywiadowczych i tym podobnych służb jest tak stara, jak historia organizowania się ludzi w zwarte grupy społeczne. Historykom trudno jednak odtworzyć proces powstawania i działania takich służb w starożytnym Egipcie, w Imperium Rzymskim czy Macedońskim albo w Polsce czasów Piastów lub Jagiellonów. Zapewne dlatego, że np. zacny kanclerz Mikołaj Trąba, prawa ręka króla Władysława Jagiełły, kiedy tworzył służby wywiadowcze, nie nadawał im takich nazw, jak Koronna Agencja Wywiadu, Świetna Królewska Służba Kontrwywiadu albo Biuro Wyjątkowych i Specjalnych Zadań Monarszych. Za to w XX w. różnego rodzaju służby weszły w fazę rozkwitu szyldów. Agencje, służby, biura. Wywiadu, kontrwywiadu, bezpieczeństwa. Specjalne, wyjątkowe,

[1] Zob. R. Faligot, R. Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie*, Warszawa 2006; Z. Siemiątkowski, A. Zięba, *Służby specjalne we współczesnym państwie*, Warszawa 2016.

ekstraordynaryjne. W dzisiejszych czasach dłużej trwa wymyślanie dobrej nazwy i logotypu niż opracowanie aktu prawnego tworzącego służbę. A służb jest co niemiara.

W wielu krajach powołuje się kolegia służb – niczym parlamenty zawodowe – z marszałkami w roli koordynatorów w bardzo wysokiej randze. Doszło do sytuacji, w której szefowie służb odbywają wizyty zagraniczne i prowadzą rozmowy z pominięciem niekiedy ministrów spraw zagranicznych. Zmiana szefa służby jest wydarzeniem medialnym i zanim wejdzie on po raz pierwszy do swojego gabinetu, z jego CV można już się zapoznać w mediach. Tajne służby już nie są tajne, lecz mainstreamowe. Minęły czasy, gdy np. „kierownik magazynu materiałów biurowych" wchodził tylnymi drzwiami na dyskretne spotkanie z głową państwa i dostarczał rzetelnych informacji wywiadowczych.

Podstawy działania

Przyczynkiem (absolutnie nie o charakterze definicyjnym!) do dalszych rozważań niech będzie stwierdzenie, że istota służb specjalnych to działania specjalistyczne lub operacyjne, skoncentrowane na określonym zjawisku (np. CBA, SOP), a istota służb wywiadowczych to pozyskiwanie informacji i wywieranie wpływu w sposób niejawny (np. AW, SWW, ABW, SKW). Należy zatem zadać sobie pytanie, gdzie w tym systemie umieścić działania antyterrorystyczne? Niestety nie ma na nie jednoznacznej odpowiedzi, a wiąże się to z dwoma elementami. Pierwszy to cel strategiczny, który stawia sobie państwo w związku z działaniami antyterrorystycznymi, drugi to główne ulokowanie pionu antyterrorystycznego. W sytuacji gdy celem strategicznym państwa będzie aresztowanie członków grupy terrorystycznej, a działania zostaną skoncentrowane w policji, to oczywiście pion antyterrorystyczny będzie służbą policyjną. Jeżeli państwo obierze za cel przejęcie kontroli nad grupą terrorystyczną, a czynności zostaną skupione w kontrwywiadzie, to pion antyterrorystyczny będzie służbą wywiadowczą. Jeżeli natomiast celem strategicznym będzie likwidacja grupy terrorystycznej, a działania zostaną skoncentrowane w osobnej służbie przeznaczonej do tego zadania, to pion antyterrorystyczny będzie służbą specjalną.

Czy takie przyporządkowanie ma znaczenie? Z perspektywy opracowań naukowych i publicystycznych[2] na pewno, ale pod względem bezpośredniej realizacji zadań nie jest to zagadnienie, które zaprzątałoby myśli funkcjonariuszy i żołnierzy pionów antyterrorystycznych.

Relacje

Piony antyterrorystyczne często mają swoje korzenie w pionach kontrwywiadowczych, a w niektórych państwach nadal są właśnie tam ulokowane. W innych modelach ciężar wykonywania zadań w tym zakresie spoczywa głównie na barkach służb policyjnych. W obu przypadkach każda ze służb ma coś do powiedzenia na temat zagrożeń terrorystycznych. W związku z tym przez lata powstawały punkty koordynacyjne, takie jak Centrum Antyterrorystyczne ABW. Analizując przyjęte rozwiązania (tu przydatne mogą być obszerne analizy dostępne m.in. w czasopiśmie „Terroryzm – studia, analizy, prewencja"), można pokusić się o banalne, ale słuszne stwierdzenie, że miarą określającą najlepsze rozwiązanie jest jego skuteczność. Próby implementacji na własnym podwórku któregoś z zewnętrznych modeli mogą okazać się wadliwe, gdyż przede wszystkim adekwatność rozwiązań do funkcjonującego systemu może przynieść efekty.

Wróćmy do relacji pionu antyterrorystycznego z pionem kontrwywiadu. Należy zauważyć, że formy i metody działań wypracowane w kontrwywiadzie w pionie antyterrorystycznym musiały zostać zmodyfikowane. Mimo że mają elementy wspólne, ich działania są determinowane przez charakter zagrożeń, z jakimi każdy z pionów musi się mierzyć, a przede wszystkim przez przyświecający im cel. Na przykład działania terrorystyczne zawsze dążą do kulminacji w postaci zamachu, tymczasem działania szpiegowskie na ogół nie mają punktu kulminacyjnego. Dlatego w pionie kontrwywiadowczym tzw. wyścig z czasem zdarza się sporadycznie, za to jest stałym elementem pracy w pionie antyterrorystycznym. Ten będzie zmierzał do likwidacji grupy w celu zapobieżenia zamachowi, podczas gdy pionowi kontrwywiadu będzie zależało na jak najdłuższym wykorzystywaniu rozpoznanej grupy do prowadzenia dezinformacji. Takie przykłady można oczywiście mnożyć, ale ten jest szczególnie obrazowy.

[2] Zob. S. Sabataj, *Byłem szefem Mosadu*, Wrocław 2020; *Dwie dekady walki z terroryzmem*, P. Piasecka, K. Maniszewska, R. Borkowski (red.), Warszawa 2022.

Współpraca pomiędzy pionami wydaje się nieodzowna. Ale czy jest częsta? Pion kontrwywiadowczy zwalcza przede wszystkim próby wywierania wpływu, a pion antyterrorystyczny – próby obalenia. Mają więc różne motywy, działają w różnych środowiskach, co sprawia, że wcale ku sobie nie ciążą. Chyba że zachodzi sytuacja, w której obce służby wywiadowcze wspierają lub nawet tworzą grupę terrorystyczną. Wtedy bez wątpienia tworzy się pole do współpracy między pionami, choć może być ona trudna ze względu na rozbieżność celów.

Z założenia przeciwnikiem pionu kontrwywiadu jest inne państwo, przeciwnikiem pionu antyterrorystycznego – grupa terrorystyczna. Ma to olbrzymi wpływ na zasięg konsekwencji ich działań. Skutki postępowania pionu kontrwywiadowczego zawsze mają charakter międzynarodowy, podczas gdy konsekwencje działań pionu antyterrorystycznego wiążą się głównie z bezpieczeństwem wewnętrznym państwa.

Kolejne zagadnienie to zapoczątkowanie procesu wykrywczego. Pion kontrwywiadowczy skupia się na punktach dostępu do informacji i ośrodkach decyzyjnych, czyli miejscach szczególnie narażonych na działalność szpiegowską. Dotyczy to osób z dostępem do informacji, osób podejmujących kluczowe decyzje, instytucji istotnych w procesie decyzyjnym, rządu, parlamentu, ministerstw, osób związanych z biznesem. Pion antyterrorystyczny natomiast koncentruje się na bezpośrednim dostępie do obiektów o istotnym znaczeniu. Problem tkwi w tym, że sporadycznie będzie to dotyczyć infrastruktury krytycznej, rzadko obiektów państwowych, najczęściej zaś celów miękkich, publicznych. W przeciwieństwie do pionu antyterrorystycznego kontrwywiad zawsze wie, gdzie szukać.

Niezbędnym elementem pracy obu pionów jest analityka, jednak w przypadku każdego z nich ma ona inny charakter. Pion kontrwywiadowczy skupia się na analizie tego, co już się wydarzyło i dlaczego się wydarzyło, podczas gdy pion antyterrorystyczny koncentruje się na tym, co, gdzie i jak może się stać. O ile w pierwszym przypadku najważniejsza jest analiza konsekwencji zdarzeń i możliwości ich wykorzystania, o tyle w drugim analiza dotyczy potencjalnych zniszczeń, którym należy zapobiec.

Casus I – Niemcy

W 2020 r. w Hesji ujawniono, że autorami listów z pogróżkami do polityków popierających liberalne podejście do kwestii uchodźców były osoby mające

dostęp do policyjnych archiwów. Listy podpisywano „NSU 2.0", co nawiązywało do działającej w latach 2000–2011 niemieckiej, skrajnie prawicowej grupy terrorystycznej o nazwie Nationalsozialistischer Untergrund (NSU). Grupa dokonała dziesięciu morderstw na tle rasowym oraz licznych ataków bombowych, w wyniku których wiele osób zostało poważnie rannych. Ofiarami byli mieszkający w Niemczech imigranci.

W tym samym okresie, na skutek wewnętrznych działań policji w Nadrenii Północnej-Westfalii, zdemaskowano grupę ok. 30 policjantów aktywnych na nazistowskich forach internetowych, u których ponadto znaleziono wiele przedmiotów związanych z tą symboliką. Podobne sytuacje miały miejsce w Meklemburgii-Pomorzu Przednim, Saksonii-Anhalt i Saksonii[3].

W 2020 r. została także rozwiązana cała kompania w elitarnej jednostce antyterrorystycznej Bundeswehry o nazwie Kommando Spezialkräfte (KSK) m.in. za prezentowanie faszystowskich pozdrowień. Liczba przypadków osób pozostających pod wpływem ideologii w tej jednostce była kilkakrotnie większa niż w innych jednostkach armii niemieckiej[4].

Szacowano, że w 2020 r. w Bundeswehrze działało ok. 600 żołnierzy będących zwolennikami organizacji Obywatele Rzeszy (niem. Reichsbürger), która negowała istnienie Republiki Federalnej Niemiec i jej organów. Otwarcie grozili oni aktami terroru. Ich poglądy opierały się na prawicowym ekstremizmie, rasizmie oraz antysemityzmie[5]. Ruch miał ok. 20 000. zwolenników na terenie Niemiec (!). W 2020 r. jego działalność została zdelegalizowana. W latach 2016–2021 byłym i obecnym członkom organizacji cofnięto ponad 1000 pozwoleń na posiadanie broni. Około 1200 z nich sklasyfikowano jako prawicowych ekstremistów.

Temat organizacji Obywatele Rzeszy powrócił, gdy 7 grudnia 2022 r. w Niemczech, w ramach szeroko zakrojonej operacji antyterrorystycznej, aresztowano ponad 25 osób. Większość z nich była powiązana z organizacją. Zatrzymani planowali obalenie istniejącego porządku państwowego i przejęcie władzy drogą zamachu stanu. Na początek zamierzali opanować ośrodki parlamentarne Reichstag i Bundestag oraz dokonać sabotażu sieci energetycznych. Na czele nowych władz miał stanąć książę Heinrich XIII Reuss.

---

[3] *Ein Beamter machte stehend auf zwei Dienstwagen den Hitlergruß*, „Die Welt", 30 XII 2020 r.

[4] *Hitlergruß und fliegende Schweineköpfe*, „Die Zeit", 17 VI 2017 r.

[5] K. Benhold, *Germany Disbands Special Forces Group Tainted by Far-Right Extremists*, „The New York Times", 1 VII 2020 r.

W spisek byli zaangażowani przedstawiciele różnych środowisk, także ze świata polityki, mediów oraz biznesu[6]. Również w tym przypadku zatrzymano kilku żołnierzy Bundeswehry, w tym ponownie komandosów z jednostki specjalnej KSK[7]. Aresztowań dokonano na terenie Badenii-Wirtembergii, Bawarii, Hesji, Dolnej Saksonii, Saksonii, Turyngii i Berlina. Przeszukano także obiekty w Brandenburgii, Nadrenii Północnej-Westfalii, Nadrenii-Palatynacie i Kraju Saary. Było to ponad 140 mieszkań, biur, magazynów oraz koszary dowództwa sił specjalnych w Calw w Badenii-Wirtembergii. Podejrzani zgromadzili broń, materiały wybuchowe i spore zasoby pieniężne.

Komentarz

Każdy obywatel ma prawo do własnych poglądów. Nie może on jednak w związku z nimi łamać prawa, zwłaszcza funkcjonariusz i żołnierz. Oczywiste! Służba także w tym zakresie stawia znacznie wyższe wymagania. W tej swobodzie myślenia istnieje granica, której przekroczenie trudno zaakceptować, a jest nią propagowanie faszyzmu. Ta ideologia nie tylko całkowicie się skompromitowała, lecz także została zabroniona z mocy prawa, co nie zdarza się często w przypadku ideologii jako takich. W związku z tym sytuacja (zwłaszcza że dotyczy Niemiec) budzi spory niepokój i daje do myślenia w kontekście podobnych zagrożeń, które mogą pojawiać się również w służbach innych krajów i przez długi czas pozostawać niewykryte. To, co wydarzyło się i dzieje w tym względzie w Niemczech, winno być ostrzeżeniem, z którego powinny skorzystać inne służby, także w Polsce. Oczywiście, nie ograniczając się do faszyzmu. Tak samo niebezpieczne mogą być np. rasizm, komunizm, radykalne ruchy religijne czy też homofobia lub zwykłe partyjniactwo. W „zdrowej" służbie jest miejsce tylko dla państwa, prawa i uczciwości. Oczywiste! Tylko tyle i aż tyle.

Żadna służba nie funkcjonuje poza społeczeństwem. Napięcia społeczne, polityczne, ekonomiczne i ideologiczne zawsze mają mniejsze lub większe odzwierciedlenie wewnątrz systemu bezpieczeństwa, a raczej wśród ludzi go tworzących. Oczywiście, im mniejsza skala tego zjawiska, tym lepiej, ale źle by się stało, gdyby w ogóle ono nie zachodziło. Ludzie

[6] *Gefährliche Mischung*, „Tagesschau", 8 XII 2022 r.

[7] Tamże.

tworzący system – funkcjonariusze, żołnierze, urzędnicy – nie mogą w związku ze swoimi poglądami podejmować działań mających na celu nielegalną ingerencję w ustrój państwa, na którego straży stoją. Nie mają też prawa służyć żadnej partii czy wyznawać ideologie.

Rozwiązanie przez Niemców części elitarnej jednostki specjalnej to za mało. Każda służba, w której pojawiają się wpływy ideologii, powinna zostać całkowicie zlikwidowana, bo to oznacza, że przez lata nikt nie rozpoznał zagrożenia lub, co gorsza, zidentyfikował je, ale nie zareagował. W obu przypadkach jest to kompromitujące dla służby. Jednostka taka jak KSK traci na zawsze swój niepisany status „elitarności" natychmiast po takim zdarzeniu.

Co jednak zrobić, gdy ten problem dotyczy struktur policyjnych? Policji ani wojska nie da się rozwiązać w żadnym państwie. Trzeba jednak budować ich struktury i zasoby osobowe z największą uwagą. Obecnie łatwiej jest np. ukarać policjanta za złamanie przepisów ruchu drogowego niż za propagowanie skompromitowanej ideologii lub homofobiczne czy rasistowskie zachowania. To nie rokuje dobrze.

Ochrona informacji niejawnych

Bezpieczeństwo wewnętrzne służb i związane z tym działania kontrwywiadowcze często budzą kontrowersje i są negatywnie odbierane także przez samych funkcjonariuszy. Niewiele osób lubi, gdy ktoś patrzy im na ręce podczas pracy. To jednak nie może mieć żadnego wpływu na realizację zadań – wewnętrzne działania kontrwywiadowcze są koniecznością i niezbędnym elementem profilaktyki zagrożeń. Pojawienie się wśród funkcjonariuszy osób podatnych na niebezpieczne ideologie, skorumpowanych, skłonnych do łamania prawa, dyspozycyjnych wobec partii politycznych zawsze będzie działać destrukcyjnie na służbę, i to na wielu poziomach.

W tym kontekście należy wspomnieć o relacji pionu kontrwywiadu z pionem ochrony informacji niejawnych. Współdziałanie tychże jest koniecznością, gdyż to pion OIN dokonuje najszerzej zakrojonych sprawdzeń osobowych i dysponuje największą wiedzą na temat funkcjonariuszy i żołnierzy. To on wydaje dokument decydujący o tym, że funkcjonariusz i żołnierz mogą wejść do grupy podwyższonego ryzyka, czyli poświadczenie bezpieczeństwa. Każda osoba otrzymująca dostęp do informacji niejawnych automatycznie musi być poddana większemu nadzorowi i weryfikacji.

Błędem jest myślenie, że poświadczenie bezpieczeństwa to świadectwo uczciwości i praworządności. To dokument zwiększający zagrożenie dla systemu, gdyż dopuszcza się do niego kolejną osobę. Sama nazwa dokumentu wydaje się zatem niewłaściwa.

Praca pionu OIN nie może kończyć się na wydaniu poświadczenia, ale dopiero od niego powinna się zaczynać. Właśnie w tym zakresie niezbędne jest współdziałanie z pionem kontrwywiadu, któremu wraz z wydaniem każdego poświadczenia przybywa zagrożeń do weryfikacji. W obrębie bezpieczeństwa służby funkcjonalne rozwiązania organizacyjne i relacje pionów OIN, kontrwywiadu i bezpieczeństwa wewnętrznego stanowią najważniejszy element właściwie działającego systemu.

Specyfika funkcjonowania, a szczególnie konsekwencje błędu (zamach), generują konieczność działań wewnętrznych także w pionie antyterrorystycznym. W związku z tym, że on również będzie poddawany weryfikacji przez system, jest potrzebne odpowiednie wypracowanie jej wewnętrznych mechanizmów.

Rozwiązania systemowe

„Rozwiązania systemowe stanowią fundament sprawnego funkcjonowania aparatu bezpieczeństwa państwa. Precyzyjne określenie zakresu odpowiedzialności pomiędzy elementami systemu jest niezbędnym warunkiem skutecznego działania". W ilu opracowaniach można znaleźć tego typu frazy. Są one tak oczywiste, że ich uzasadnianie mogłoby urazić wielu specjalistów, czego pragnę uniknąć. Warto jednak mówić także o dysproporcjach systemowych. Spójrzmy pod tym kątem na zaangażowanie służb w poszczególnych obszarach systemu bezpieczeństwa państwa:

a) ochrona władz – SOP,
b) ochrona granic – SG,
c) przestępczość zorganizowana – Policja,
d) wywiad – AW, SWW,
e) kontrwywiad – ABW, SKW,
f) korupcja – CBA, SKW, Policja, SG, ABW, ŻW,
g) terroryzm – ABW, SKW, AW, SWW, SOP, Policja, SG, KAS, ŻW.

To jedynie pobieżny przegląd, pokazuje on jednak, gdzie według polskiego systemu leżą największe zagrożenia państwa. Można pokusić się o stwierdzenie, że skoro terroryzm jest tak wielkim zagrożeniem (jak korupcja),

to już dawno powinna powstać specjalistyczna służba antyterrorystyczna (np. taka jak CBA w obszarze korupcji). Czy rzeczywiście?

W połowie 2022 r. Norweska Policja Bezpieczeństwa (norw. Politiets Sikkerhetstjeneste, PST) zdecydowała o przesunięciach kadrowych wewnątrz służby. Grupę funkcjonariuszy z pionu antyterrorystycznego przeniesiono do pionu kontrwywiadowczego. Wiele wskazuje, że i w innych służbach podjęto działania mające na celu przesunięcie głównego ciężaru zaangażowania, co wynika z analizy materiałów prasowych i rozmów ze specjalistami z innych krajów. Nie znaczy to jednak, że zmniejszyła się potrzeba sprawnego funkcjonowania pionów antyterrorystycznych, gdyż terroryzm niezmiennie ma się dobrze. Jeszcze „lepiej" natomiast mają się zagrożenia kontrwywiadowcze, dlatego właśnie trzeba reagować. Naturalna fluktuacja kadr pomiędzy tymi pionami okazuje się koniecznością, ale może być też czynnikiem spajającym wewnętrzne struktury służb oraz elementem doskonalenia zawodowego.

W październiku 2022 r. senacka komisja w USA stwierdziła, że Narodowe Centrum Kontrwywiadu i Bezpieczeństwa (ang. National Counterintelligence and Security Center, NCSC), będące częścią Biura Dyrektora Wywiadu Krajowego (ang. Office of the Director of National Intelligence, ODNI), powinno stać się wyodrębnioną z dotychczasowej struktury jednostką kontrwywiadu krajowego. Przejęłoby tym samym rolę FBI w zakresie kontrwywiadu. W Stanach Zjednoczonych mnogość służb jest na porządku dziennym.

Casus II – Afganistan

Humam Chalil al-Balawi był jordańskim lekarzem urodzonym w Kuwejcie. Związał się ze skrajnie islamistycznymi ugrupowaniami działającymi w Turcji, gdzie prowadził praktykę i mieszkał z żoną i dziećmi. W 2007 r. został zatrzymany przez jordańskie służby specjalne, które postanowiły „odwrócić" terrorystę i wysłać go do Afganistanu. Jordańczycy blisko współdziałali z amerykańską CIA. Celem Al-Balawiego była pomoc w infiltracji Al-Ka'idy. W 2009 r. został zaproszony na spotkanie do bazy CIA w Camp Chapman w prowincji Khost. Po przybyciu na miejsce zdetonował ładunki wybuchowe, które miał na sobie, zabijając wiele osób. Było to jedno z najgorszych „odwróceń" agentów w historii.

Komentarz

Wydarzenia związane z Chalilem al-Balawim doskonale unaoczniły, że nawet najbardziej rozbudowane systemy weryfikacji nie dają pewności. W działaniu pionu zarówno antyterrorystycznego, jak i kontrwywiadowczego fundamentalne znaczenie ma praca z osobowymi źródłami informacji. To właśnie ten typ działań przynosi pozytywne efekty, ale jednocześnie wiąże się z największymi zagrożeniami. Mimo wielopoziomowych sprawdzeń źródła, czyli człowieka, z którym przyjdzie pracować, nie da się uniknąć ryzyka dekonspiracji, dezinformacji lub po prostu porażki. W pracy ze źródłami, jaką prowadzą piony antyterrorystyczne, jest konieczne korzystanie z doświadczeń „starszego brata", czyli kontrwywiadu, mimo różnej specyfiki pracy w tych dwóch pionach.

Przenikanie

Należy się zastanowić, w jakim stopniu piony kontrwywiadu i antyterrorystyczny powinny działać równolegle, a w jakim wzajemnie się przenikać. Ten problem można omówić na przykładzie trzech obszarów aktywności służb. Pierwszy to działania kontrwywiadowcze skupiające się na przeciwdziałaniu ingerencji podmiotów zewnętrznych (państwowych – obce służby, oraz prywatnych – korporacje lub grupy przestępcze) w strukturę państwa (polityczną, ekonomiczną, bezpieczeństwa). Drugi obszar, ściśle związany z pierwszym, to aktywności mające na celu przeciwdziałanie ingerencji w same służby. Jest jeszcze trzecia sfera, która wydaje się nieco zaniedbywana – przeciwdziałanie powstawaniu wewnątrz służb szkodliwych zjawisk. Zalicza się do nich tworzenie grup, których poglądy i cele są sprzeczne z porządkiem prawnym lub mogą mieć negatywny wpływ na funkcjonowanie demokratycznego państwa.

O ile udział pionu kontrwywiadu w dwóch pierwszych aktywnościach nie budzi wątpliwości, o tyle wydaje się, że w wielu strukturach działania z trzeciego obszaru scedowano na komórki bezpieczeństwa wewnętrznego. Ten model, można powiedzieć: klasyczny, nie jest oczywiście złym rozwiązaniem. Pozostaje jednak kwestia nasycenia działaniami oraz celu ich realizacji. W większości przypadków komórki bezpieczeństwa wewnętrznego opierają się na postępowaniu typu policyjnego – podejrzenie popełnienia przestępstwa, zebranie materiału dowodowego, penalizacja. Warto jednak pamiętać,

że więcej korzyści niż szybkie zamknięcie sprawy przynoszą odpowiednio przeprowadzone działania kontrwywiadowcze oraz aktywna profilaktyka.

W przypadku pionu antyterrorystycznego sytuacja wygląda zupełnie inaczej. Nigdy nie ukierunkowuje on swoich działań na własną strukturę i pozostawia te kwestie komórkom bezpieczeństwa wewnętrznego. Zaniedbywanie tego elementu może wiązać się z bardzo negatywnymi konsekwencjami i poważnym zagrożeniem bezpieczeństwa państwa.

Casus III – Szwecja

W listopadzie 2022 r. rozpoczął się w Szwecji proces pochodzących z Iranu braci, 42-letniego Peymana Kia i 25-letniego Payama Kia, którzy przez wiele lat pracowali dla rosyjskiego wywiadu wojskowego GRU. Bracia trafili do Szwecji jako dzieci w latach 80. XX stulecia. Obywatelstwo uzyskali w 1994 r. Payam studiował w akademii policyjnej, porzucił ją jednak po pierwszym semestrze. Starszy brat Peyman studiował na Uniwersytecie w Uppsali, po czym rozpoczął pracę w służbach celnych. Następnie ponad trzy lata pracował w szwedzkiej Policji Bezpieczeństwa (szwedz. Säkerhetspolisen, SÄPO). W 2011 r. przeniósł się do wywiadu wojskowego MUST (szwedz. Militära underrättelse- och säkerhetstjänsten). Wykonywał zadania w ściśle tajnym Urzędzie Wywiadu Specjalnego (szwedz. Kontoret för särskild inhämtning, KSI), który rekrutuje szpiegów poza Szwecją. Następnie wrócił do SÄPO. Kolejnym etapem jego kariery było pełnienie funkcji naczelnika wydziału bezpieczeństwa w Szwedzkiej Agencji ds. Żywności. Dla GRU szpiegował prawdopodobnie od 2011 r. i zaangażował w to Payama, który został łącznikiem. Braci aresztowano w 2021 r. po blisko sześcioletnim śledztwie.

W przeszłości szwedzkie służby nie zatrudniały osób urodzonych we „wrogich" krajach, z obawy, że mogą być podatne na rekrutację przez ich rodzime władze lub ich sojuszników. Kilka innych państw w regionie nadal stosuje tę politykę, Szwecja jednak w ostatnich latach złagodziła podejście do tego problemu.

Komentarz

Szwedzki przypadek wywołał dyskusję na temat procesu naboru do służb. Szczególną uwagę zwróciły głosy, że nie powinno się do nich przyjmować

obcokrajowców. Warto w tym miejscu podkreślić dwie rzeczy. Po pierwsze, bracia Kia byli obywatelami Szwecji , a nie obcokrajowcami. Po drugie, analiza pracy szwedzkich służb pokazuje, że w tym samym czasie dla Rosjan pracowało wielu Szwedów urodzonych w Szwecji. Zatem to nie irańskie korzenie braci Kia stały się problemem, lecz ich cechy indywidualne i decyzje, które tylko oni podejmowali. Jednak najważniejszym wnioskiem nasuwającym się po analizie tej sprawy jest zdiagnozowana słabość bezpieczeństwa wewnętrznego szwedzkich służb, co przyznają sami zainteresowani. Wyciągnęli oni wnioski z tego zdarzenia, bynajmniej nie ograniczając dostępu do służby Szwedom urodzonym w innych krajach. Wzmocnili system bezpieczeństwa wewnętrznego i kontrwywiad. Między innymi dlatego są to jedne z najlepszych służb w Europie, które na kierunku rosyjskim pozostają bez wątpienia w gronie liderów działań kontrwywiadowczych. A z liderami warto współdziałać.

Nabór

Nie system, nie sprzęt, nie zaplecze, ale człowiek. Każda dobra służba, zarówno pion antyterrorystyczny, jak i kontrwywiad, musi stawiać na dobór jak najlepszych kadr. W dobie postępującej cyfryzacji życia i włączania w pracę służb nowoczesnych rozwiązań technicznych może umknąć oczywista zasada, że o sile i sprawności służby decyduje zespół ludzi, których udało się do niej pozyskać i odpowiednio przygotować.

W zakresie naboru i szkolenia w świecie służb istnieje absolutna dowolność i autonomia. Co więcej, co kilka lat modyfikują one systemy naboru i reformują programy szkoleń. To oczywiście słuszny kierunek, pod warunkiem że wynika z analizy doświadczeń i potrzeb danej służby. Jeżeli natomiast jest rezultatem swego rodzaju mody lub kopiowania zagranicznych rozwiązań, wówczas powoduje obniżenie wartości kadr. W tej dowolności nie ma nic złego także pod warunkiem, że osiągane rezultaty są jak najlepsze. Dlatego właśnie procesy naboru i szkolenia są tak ważnymi i zarazem wrażliwymi etapami. Ewaluacja przychodzi wraz z efektami, a na te trzeba czekać. Chyba że modyfikacje i reformy są wprowadzane za często. Trudno wówczas zweryfikować, co miało decydujący wpływ na ostateczne wyniki.

Biorąc pod uwagę współczesne uwarunkowania pracy służb, warto poddać analizie dwa elementy. Pierwszy to badania psychologiczne, drugi – aktywny nabór. Badania psychologiczne bez wątpienia są piętą achillesową

procesu naboru. O ile inne jego elementy mają wyraźne wskaźniki określające przydatność lub nieprzydatność do służby (np. wykształcenie, zdrowie, karalność, znajomość języków, sprawność), o tyle wyniki badań psychologicznych i wyciągane na ich podstawie wnioski zależą od psychologa prowadzącego badania. Psychologia nie jest nauką ścisłą, a umiejętności oceny kandydatów bywają tak różne, jak różni bywają psychologowie. Nie ma służby, która ani razu nie odrzuciła na badaniach świetnego kandydata lub nigdy nie przyjęła takiego, który okazał się totalną porażką. A wszystko to tylko na podstawie opinii psychologa.

Aktywny nabór to działania, w których służba otwarcie poszukuje kandydatów. Obecnie służby reklamują się plakatami na przystankach, pogadankami na uczelniach, stoiskami na targach pracy. Podobno „takie czasy". Jakie wyzwanie stanowi ten sposób naboru dla kontrwywiadu! Szanująca się służba wywiadowcza z radością zainstaluje się przy takim stoisku lub na uczelnianej pogawędce, by typować osoby do rozpracowania, np. te najdłużej rozmawiające z rekrutującym lub samego rekrutującego. Ten sposób naboru bez wątpienia zwiększył zaangażowanie pionu kontrwywiadu. Pion antyterrorystyczny jest z takiego zaangażowania zwolniony. Gdzie się podziały czasy, kiedy to służba szukała kandydata i dopiero po weryfikacji podejmowała z nim rozmowę oraz ewentualnie dalsze kroki, czasy, kiedy kandydat aplikował do służby, mając cichą nadzieję, że „może zadzwonią"... Rynek pracy (bo teraz tak się nazywa obszar pozyskiwania kandydatów) wymusza działania kojarzące się raczej z naborem do boys bandu. Jaką tworzy się przez to jakość w służbie? Adekwatną do jakości naboru. Pewnie dlatego zdarzają się np. przypadki rezygnacji ze służby już po kursie podstawowym. Tacy kandydaci okazują się szczególnie uciążliwi dla pionu kontrwywiadu. Zdobywają oni wiedzę, poznają ludzi wewnątrz służby i... opuszczają ją szybko, wychodząc z tą wiedzą na zewnątrz.

Szkolenie jest nierozerwalnie związane z naborem. Żeby to zobrazować, można powiedzieć, że przyjęcie świetnego matematyka na studia do akademii sztuk pięknych byłoby równie chybione, jak przyjęcie znakomitego malarza na wydział fizyki i astronomii. Trafiony nabór jest fundamentem efektywnego szkolenia. Warto zadać sobie w takim razie pytanie, gdzie powinno kończyć się tzw. szkolenie podstawowe, a gdzie piony kontrwywiadu i antyterrorystyczny powinny rozpoczynać proces kształtowania funkcjonariusza lub żołnierza do wykonywania zadań. Ponadto istnieją formy i metody działań, które są tożsame w pracy różnych pionów. Biorąc pod uwagę opisaną wcześniej specyfikę, można zaryzykować stwierdzenie, że proces

szkolenia powinien być wspólny, poszerzony o fakultatywne zajęcia dla kandydatów do służby w poszczególnych pionach. To możliwe i konieczne, gdyż delegowanie do zadań ma wynikać z aktualnych potrzeb służby, a te, jak pokazuje wcześniej opisany przypadek Norwegii, mogą się zmieniać.

Przeciwnicy

I na koniec, żeby zrozumieć, z kim przychodzi mierzyć się pionom, o których mowa, należy krótko scharakteryzować ich przeciwników. Pion kontrwywiadowczy będzie miał za przeciwnika obcy wywiad, czyli grupę przestępczą z potężnym zapleczem. Dlaczego przestępczą? Bo skoro wywiad ma prowadzić działania niejawne poza granicami swojego kraju, to w świetle prawa innych państw będzie tam działał nielegalnie. Taka grupa ma za sobą państwo z całym jego aparatem i zasobami, co czyni z niej poważnego przeciwnika.

Pion antyterrorystyczny będzie zwalczał grupę terrorystyczną, czyli grupę działającą poza prawem, bez takiego zaplecza jak wywiad. Sytuacja jednak tylko pozornie wygląda nieco lepiej, kierunek przeciwdziałania będzie bowiem znacznie bardziej rozproszony. Pozostaje jeszcze ten najgroźniejszy wariant, w którym grupa terrorystyczna jest wspierana przez wywiad, z wszystkimi jego zasobami, co stanowi kolejny element wymuszający bliską współpracę obu pionów.

Podsumowanie

Po zamachu w Madrycie wysłano mnie do Madrytu – po wnioski. Po zamachu w Londynie wysłano mnie do Londynu – po wnioski. Po zamachu w Bagdadzie wysłano mnie do Bagdadu – po wnioski. Po zamachu w Kabulu wysłano mnie do Kabulu – po wnioski. Zawsze warto wiedzieć więcej lub więcej słuchać tych, którzy wiedzą. Mam nadzieję, że będziemy nadal wyciągać wnioski ze zdarzeń spoza Polski, po to, by w Polsce nigdy do podobnych nie doszło.

Bibliografia

Benhold K., *Germany Disbands Special Forces Group Tainted by Far-Right Extremists*, „The New York Times", 1 VII 2020 r.

Dwie dekady walki z terroryzmem, P. Piasecka, K. Maniszewska, R. Borkowski (red. nauk.), Warszawa 2022.

Działania kontrwykrywcze zorganizowanych grup przestępczych i organizacji terrorystycznych, P. Chlebowicz, T. Safjański, P. Łabuz (red. nauk.), Warszawa 2021.

Ein Beamter machte stehend auf zwei Dienstwagen den Hitlergruß, „Die Welt", 30 XII 2020 r.

Faligot R., Kauffer R., *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie*, Warszawa 2006.

Gefährliche Mischung, „Tagesschau", 8 XII 2022 r.

Hitlergruß und fliegende Schweineköpfe, „Die Zeit", 17 VI 2017 r.

Kahneman D., *Pułapki myślenia*, Poznań 2012.

Marshall T., *Potęga geografii, czyli jak będzie wyglądał w przyszłości nasz świat*, Poznań 2021.

Piasecki B., *Kontrwywiad. Atak i obrona*, Łomianki 2021.

Sabataj S., *Byłem szefem Mosadu*, Wrocław 2020.

Schuman Tomas D. (wł. Jurij Bezmienow), *Agentura wpływu. Tajniki działalności wywrotowej KGB*, Kraków 2021.

Siemiątkowski Z., Zięba A., *Służby specjalne we współczesnym państwie*, Warszawa 2016.

Staniuk W., *Współczesny wywiad. Humint*, Warszawa 2023.

Szlachter D., *Walka z terroryzmem w Unii Europejskiej. Nowy impuls*, Toruń 2006.

Terroryzm i antyterroryzm w opiniach ekspertów w XX rocznicę zamachów na WTC i Pentagon, J. Stelmach (red. nauk.), Warszawa 2021.

„Terroryzm – studia, analizy, prewencja" 2022, nr 1, nr 2.

„Terroryzm – studia, analizy, prewencja" 2023, nr 3.

Treści zawarte w eseju są wynikiem doświadczenia autora w służbie na rzecz polskiej wspólnoty antyterrorystycznej i stanowią jego osobiste poglądy.

Ppłk rez. dr inż. Tomasz Białek

Były dowódca pododdziałów specjalnych Wojska Polskiego, były dyrektor Zarządu Profilaktyki Ochronnej i Bezpieczeństwa Wewnętrznego Biura Ochrony Rządu oraz Departamentu Ochrony Centralnego Biura Antykorupcyjnego. Audytor i ekspert z zakresu systemów bezpieczeństwa, ze szczególnym uwzględnieniem bezpieczeństwa informacji oraz osób i obiektów o podwyższonym poziomie zagrożenia. Wykładowca akademicki specjalizujący się w socjologii bezpieczeństwa. Rzeczoznawca Polskiej Izby Ochrony.

https://doi.org/10.4467/27204383TER.23.025.18327

Badania ankietowe poświęcone terroryzmowi w Polsce i kierunkom jego rozwoju

Komentarz ekspercki

Lorenzo Vidino

Badanie przeprowadzone wśród 94 polskich ekspertów i praktyków w dziedzinie terroryzmu dostarcza ważnych informacji o postrzeganiu przez nich tej problematyki[1]. Niektóre otrzymane wyniki są prawdopodobnie zbieżne z tymi, które uzyskano by, gdyby wywiady przeprowadzono wśród partnerów w innych krajach europejskich. Dotyczy to na przykład wskazania Daesh i Al-Ka'idy – w tej konkretnej kolejności – jako dwóch organizacji stanowiących największe zagrożenie bezpieczeństwa zarówno UE, jak i Polski, prawdopodobnych celów terrorystycznych, a także obaw związanych z wykorzystaniem różnych technologii do działań terrorystycznych.

Jednocześnie kilka wyników tego badania się wyróżnia. Najprawdopodobniej odzwierciedlają one specyficzną polską perspektywę. Pierwszym z nich jest obawa dotycząca działań rosyjskich służb specjalnych (oraz, jak można przypuszczać, rosyjskiej inwazji na Ukrainę). Jest to element, który w Europie Zachodniej prawdopodobnie nie będzie przedmiotem takiej

[1] Wyniki badania zostały opublikowane w: „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 148–176.

samej uwagi, ale który ze zrozumiałych względów niepokoi znaczną część przedstawicieli polskiego sektora bezpieczeństwa.

Drugim wyróżniającym się wynikiem jest nieco mniejsza obawa przed terroryzmem o skrajnie prawicowym charakterze. Otrzymane odpowiedzi mogłyby być inne, gdyby w badaniu poproszono o wytypowanie nie pojedynczej organizacji, lecz ruchu ideologicznego. To, że jako główne zagrożenie została wskazana tylko jedna prawicowa organizacja ekstremistyczna (Atomwaffen) i w dodatku przez znacznie mniejszą liczbę respondentów w porównaniu z tymi, którzy wskazali na Daesh i Al-Ka'idę, świadczy o pewnej odmienności w stosunku do Europy Zachodniej. Mimo że dynamika zmienia się w zależności od kraju, to w ostatnich trzech, czterech latach instytucje bezpieczeństwa większości państw Europy Zachodniej coraz częściej traktowały prawicowy ekstremizm jako tak samo, jeśli nie bardziej, niebezpieczny jak dżihadyzm.

Uderzające jest to, że zdaniem dużego odsetka respondentów Polska może stać się krajem atrakcyjnym dla terrorystów. Wprawdzie w ostatnich latach niewiele na to wskazywało, jednak przekonanie, że w najbliższej przyszłości sytuacja ulegnie pogorszeniu, wydaje się dość powszechne. Niektóre spośród odpowiedzi mogą świadczyć o tym, że te obawy są przynajmniej częściowo związane z zagrożeniami płynącymi z Rosji.

Uzyskane wyniki są bardzo interesujące i pozwalają dobrze wyczuć „puls" polskiego środowiska antyterrorystycznego, a omawiane badanie jest warte uwagi i powinno zostać powtórzone w innych krajach.

Prof. Lorenzo Vidino

Ekspert w dziedzinie islamizmu w Europie i Ameryce Północnej, dyrektor Programu ds. Ekstremizmu na Uniwersytecie Jerzego Waszyngtona w Waszyngtonie. Od 20 lat zajmuje się badaniami poświęconymi dynamice mobilizacji sieci dżihadystów na Zachodzie, rządowej polityce przeciwdziałania radykalizacji oraz działalności organizacji inspirowanych przez Bractwo Muzułmańskie na Zachodzie.

https://doi.org/10.4467/27204383TER.23.026.18328

Hiszpańska prezydencja w EU High Risk Security Network

sprawowana przez Guardia Civil za pośrednictwem Grupo de Acción Rápida

Gregorio Salazar

Chodzi nie tyle o potrzebę wiedzy, ile o chęć dzielenia się nią.
Martin Schieffer, szef jednostki DG HOME-D2

W ostatnich latach celem radykalnego terroryzmu było dokonywanie niezwykle brutalnych ataków wymierzonych w infrastrukturę krytyczną (cywilną), cele wrażliwe i węzły transportowe w całej Europie. Aby uniknąć tego rodzaju aktów przemocy lub przynajmniej zapobiec wzrostowi ich liczby, państwa członkowskie Unii Europejskiej podejmują coraz więcej działań prewencyjnych, zdając sobie sprawę z potrzeby wdrożenia solidniejszych środków bezpieczeństwa i zapewnienia lepszego przygotowania. Osiągnięcie wyższego poziomu gotowości i bezpieczeństwa wymaga wypracowania wspólnej, transgranicznej strategii oraz wspólnych działań i zaangażowania w nie władz państwowych, stowarzyszeń zawodowych i podmiotów prywatnych. Istotne jest, aby tą współpracą objąć jak największą liczbę krajów – zarówno europejskich, jak i tych spoza Starego Kontynentu.

W odpowiedzi na te potrzeby i cele w ramach realizacji unijnego planu działania pod nazwą *Unia bezpieczeństwa: Ochrona przestrzeni publicznych*

(ogłoszonego w październiku 2017 r.) powstała EU High Risk Security Network (EU-HRSN) – unijna sieć mundurowych formacji specjalnych ds. działań wysokiego ryzyka.

Rysunek 1. Logo EU High Risk Security Network.

Źródło: materiały własne Grupo de Acción Rápida.

Przy ogłaszaniu tego planu padły słowa:

W ciągu ostatnich trzech lat Unia Europejska i jej państwa członkowskie podjęły zdecydowane kroki w celu zapobiegania atakom terrorystycznym, wymiany informacji między państwami członkowskimi, przeciwdziałania radykalizacji postaw i lepszego zarządzania naszymi granicami. Jednak, jak pokazują ataki terrorystyczne przeprowadzone w Europie, konieczne jest zintensyfikowanie działań zapobiegawczych, aby uniemożliwić przeprowadzenie w przyszłości ataków takich jak te, które miały miejsce na ulicach Barcelony, Berlina, Londynu, Manchesteru, Nicei, Paryża czy Sztokholmu. Wspólnym mianownikiem tych ataków było dokonanie ich w przestrzeni publicznej. Chociaż ryzyka takich ataków nigdy nie da się całkowicie wyeliminować, istnieją konkretne rozwiązania operacyjne, które państwa członkowskie mogą podjąć przy wsparciu UE, aby lepiej chronić przestrzeń publiczną przed zagrożeniem terrorystycznym. Komisja zobowiązała się do zapewnienia specjalnego finansowania w wysokości ponad 118 mln euro, 11 mln euro w przyszłym roku, w celu zwiększenia wymiany najlepszych praktyk, opublikowania materiałów zawierających wytyczne dla państw członkowskich oraz wspierania współpracy między podmiotami lokalnymi i sektorem prywatnym (...). Komisja utworzy Forum Profesjonalistów, na którym specjaliści w zakresie egzekwowania prawa oraz istniejące sieci organów ścigania będą mogli dzielić się wiedzą

dotyczącą ochrony przestrzeni publicznej. Komisja ustanowi również sieć bezpieczeństwa na rzecz ochrony miejsc wysokiego ryzyka w celu organizowania wspólnych szkoleń i ćwiczeń dla organów ścigania, aby poprawić ich gotowość i zwiększyć zdolności reagowania[1].

Koncepcja EU-HRSN

Oficjalna inauguracja działalności sieci EU-HRSN nastąpiła 1 listopada 2018 r. Jej zadaniem jest integracja przedstawicieli europejskich mundurowych formacji specjalnych ds. działań wysokiego ryzyka (cywilnych i wojskowych), będących częścią organów ścigania lub jednostek wykonujących zadania wspierające działania operacyjne lub ochronne, w celu zapewnienia ochrony miejsc publicznych, celów miękkich oraz infrastruktury krytycznej przed aktami o charakterze terrorystycznym oraz wykrywania i ścigania ich sprawców. Powstanie sieci ma służyć usprawnieniu procesu wymiany wypracowanych taktyk, technik i procedur (*tactics, techniques, and procedures*, TTP) oraz budowaniu lepszej odporności na ataki. Wymiana ma obejmować dobre praktyki w zakresie zapobiegania atakowi terrorystycznemu, wykrywania i reagowania na jego pierwszą fazę, ale niekoniecznie dotyczyć zorganizowanej interwencji, zwykle przeprowadzanej przez rząd podczas rozmieszczania – w odpowiedzi na atak terrorystyczny – zasobów wykorzystywanych priorytetowo.

Prezydencja w EU-HRSN pozwala krajowi przewodniczącemu na wykorzystanie nie tylko zasobów zapewnionych przez Komisję Europejską, lecz także środków krajowych przeznaczonych na realizację wspomnianych wyżej celów. Pierwszą prezydencję sprawowała holenderska jednostka Koninklijke Marechaussee za pośrednictwem brygady Hoog Risico Beveiliging (HRB) i przy wsparciu Hiszpanii, która pełniła funkcję wiceprzewodniczącej. W dniu 1 lipca 2021 r. przewodnictwo objęła na kolejne 24 miesiące, zgodnie z postanowieniami Karty EU-HRSN, hiszpańska Guardia Civil, sprawująca je za pośrednictwem Grupo de Acción Rápida (GAR).

Grupo de Acción Rápida została utworzona w 1978 r. jako Unidad Antiterrorista Rural (UAR), a jej głównym zadaniem była walka z organizacją Euskadi Ta Askatasuna (ETA) – hiszpańską narodowosocjalistyczną grupą

[1] Unijny plan działania *Unia bezpieczeństwa: Ochrona przestrzeni publicznych*, październik 2017 r.

terrorystyczną, za sprawą której w ciągu 42 lat zginęło ponad 850 osób. GAR ma ponadczterdziestoletnie doświadczenie w walce z terroryzmem. Jednostka była wysyłana do Kosowa, Bośni, Afganistanu, Iraku, Haiti, Republiki Środkowoafrykańskiej i Libanu, m.in. pod auspicjami NATO i ONZ.

Rysunek 2. Logo Grupo de Acción Rápida.

Źródło: materiały własne Grupo de Acción Rápida.

Z powodu pandemii COVID-19 niektóre działania EU-HRSN zostały wstrzymane lub opóźnione o dziesięć miesięcy. Doprowadziło to do przedłużenia o pół roku prezydencji sprawowanych najpierw przez holenderski HRB, a następnie przez hiszpańską GAR. Ta druga zakończy się 1 stycznia 2024 r. Negatywny wpływ na rozwój idei EU-HRSN wywarła śmierć płk. Jesúsa Gayoso Reya, szefa GAR i współzałożyciela EU-HRSN, który zmarł z powodu infekcji koronawirusem. Był on jednym z głównych animatorów zarówno tej, jak i innych inicjatyw UE. Miejmy nadzieję, że następna prezydencja, która będzie sprawowana przez portugalską Guarda Nacional Republicana (GNR), za pośrednictwem Grupo de Intervenção de Ordem Pública (GIOP), nie będzie musiała mierzyć się z tego rodzaju problemami. Nieprzewidziane wyzwania są domeną członków sieci EU-HRSN, ale gdy współpracują ze sobą ludzie o tym samym sposobie myślenia, to nie ma przeszkód nie do pokonania.

Cele EU-HRSN

Najważniejsze cele powstania sieci to:

1. Wymiana najlepszych praktyk, przeprowadzanie szkoleń krzyżowych, dzielenie się wiedzą na temat procedur i innymi szczegółami

operacyjnymi oraz budowanie struktur współpracy na taktycznym poziomie dowodzenia i kontroli w celu poprawy odporności na akty poważnej przemocy lub terroryzmu wymierzone w cywilną infrastrukturę krytyczną, cele miękkie i węzły transportowe w państwach członkowskich UE.

2. Zwiększanie zasobów wiedzy wszystkich członków poprzez podejmowanie działań, dzięki którym wiedza na temat TTP, standardowych protokołów operacyjnych (*standard operating protocols*), oceny ryzyka i profilowania (prognostycznego) jest wymieniana w ramach szkoleń krzyżowych.
3. Doradzanie organizacjom UE odpowiedzialnym za kwestie bezpieczeństwa z uwzględnieniem wniosków płynących z wymiany doświadczeń między państwami członkowskimi EU-HRSN.
4. Dzielenie się zdobytymi doświadczeniami za pośrednictwem określonych kanałów komunikacji z innymi organizacjami współpracującymi w zakresie bezpieczeństwa w UE. Nie dotyczy to pracy nad wspólnymi standardami lub praktykami, ale obejmuje – w stosownych przypadkach i gdy jest to zgodne z prawem krajowym – dostosowanie najlepszych praktyk i taktyk oraz zebranie wypracowanych technik jako wspólnej doktryny, aby zapewnić im największą skuteczność. Celem jest uzyskanie efektu synergii, a służyć temu mają spotkania poświęcone procedurom działania kryzysowego obowiązującym w poszczególnych krajach i czerpanie z różnych rozwiązań.

Członkostwo w EU-HRSN

Członkami EU-HRSN są mundurowe formacje specjalne ds. działań wysokiego ryzyka (cywilne i wojskowe) będące częścią organów ścigania lub jednostek wykonujących zadania wspierające działania operacyjne lub ochronne w celu zapewnienia ochrony miejsc publicznych, celów miękkich oraz infrastruktury krytycznej przed aktami o charakterze terrorystycznym, a także wykrywania i ścigania ich sprawców.

Członkostwo w EU-HRSN jest możliwe po złożeniu pisemnego wniosku do przewodniczącego. Wniosek ten podlega zatwierdzeniu większością dwóch trzecich głosów państw członkowskich sieci. Jednym z warunków przyjęcia jest zaakceptowanie i podpisanie Karty EU-HRSN.

Alternatywną opcją jest członkostwo stowarzyszone, które umożliwia zainteresowanym stronom uczestnictwo w EU-HRSN bez spełnienia wszystkich wymogów dla członków sieci. Koszt takiego członkostwa nie jest jednak pokrywany z budżetu UE.

Struktura organizacyjna EU-HRSN

Struktura EU-HRSN obejmuje:

a) kierownictwo w postaci: przewodniczącego, wiceprzewodniczącego i grupy sterującej. Wiceprzewodniczący jest wybierany w głosowaniu wśród członków grupy sterującej i po 24 miesiącach automatycznie staje się kolejnym przewodniczącym. Pozwala mu to na zdobycie wiedzy, doświadczenia i zbudowanie sieci kontaktów, potrzebnych do właściwego kierowania EU-HRSN podczas prezydencji. W skład obecnej grupy sterującej wchodzą: przedstawiciele prezydencji (hiszpańska Guardia Civil za pośrednictwem GAR), wiceprezydencji (portugalska GNR za pośrednictwem GIOP), Belgii (Police Fédérale), Estonii (Kaitsepolitsei), Irlandii (Garda Síochána za pośrednictwem Special Tactics & Operations Command, STOC), Holandii (Koninklijke Marechaussee za pośrednictwem HRB) oraz jednostka D2 ds. terroryzmu w DG HOME (Directorate-General for Migration and Home Affairs, DG HOME-D2) jako stały obserwator;
b) 25 pełnoprawnych członków (jednostek antyterrorystycznych) z 18 państw członkowskich;
c) Norwegię, Wielką Brytanię i USA jako członków stowarzyszonych;
d) sieć ATLAS (Atlas Network) i DG HOME jako obserwatorów.

Działania EU-HRSN

Sieć prężnie wymienia informacje z innymi antyterrorystycznymi inicjatywami Komisji Europejskiej oraz otrzymuje od nich organizacyjne i merytoryczne wsparcie. Dotyczy to przede wszystkim doświadczeń z prac nad tzw. taktyką Red Teaming[2] w ramach Policy Group on Public Spaces Protection,

[2] Red Teaming – rodzaj procedur związanych z oceną poziomu ochrony przed aktywnością o charakterze terrorystycznym oraz dotyczących działań zwiększających odporność na atak. Są one realizowane z wykorzystaniem systemów bezzałogowych (przyp. red.).

projektami realizowanymi w ramach podgrup bezpieczeństwa UE–USA (m.in. bezpieczeństwo wydarzeń specjalnych, seminarium na temat materiałów wybuchowych) oraz grupą unijnych doradców ds. budowania odporności na zagrożenia (Protective Security Advisors, PSA), która jest bardzo interesującą inicjatywą DG HOME-D2. Grupa ta składa się z wielu ekspertów z szeroką wiedzą specjalistyczną w zakresie ochrony przestrzeni publicznych (*public spaces protection*, PSP) oraz ochrony antyterrorystycznej podczas imprez masowych i ważnych wydarzeń z udziałem VIP (m.in. zagrożenia CBRN-E, C-IED, UAS/C-UAS[3], snajperzy, ratownictwo taktyczne i reagowanie, K2 – jednostka ds. psów służbowych, budowanie odporności na zagrożenia hybrydowe w infrastrukturze krytycznej)[4]. Mogą być oni zorganizowani w małe zespoły, doradzające danej służbie lub rządowi oraz wspierające kompleksowe podejście do zagadnienia bezpieczeństwa.

Zdjęcie 1. Spotkanie grupy Protective Security Advisors.

Źródło: materiały własne Grupo de Acción Rápida.

EU-HRSN prowadzi również intensywną wymianę z innymi sieciami UE, takimi jak ATLAS i ENLETS (The European Network of Law Enforcement Technology Services). Jest także reprezentowana na różnych forach,

[3] CBRN-E (*chemical, biological, radiological, nuclear and explosives*) – zagrożenia chemiczne, biologiczne, radiologiczne, jądrowe, wybuchowe; C-IED (*counter-improvised explosive device*) – zwalczanie improwizowanych urządzeń wybuchowych; UAS (*unmanned aerial system*) – bezzałogowy system powietrzny; C-UAS (*counter-unmanned aerial system*) – system zwalczania bezzałogowych systemów powietrznych (przyp. red.).

[4] Szerzej na ten temat zob. R. Olszewski, B. Zapletal, W. Wojtas, *EU Protective Security Advisors – inicjatywa Unii Europejskiej wspierająca wysiłki państw członkowskich w zakresie ochrony obywateli i infrastruktury krytycznej przed zamachami terrorystycznymi*, „Terroryzm – studia, analizy, prewencja" 2023, nr 4.

np. Operators and Practitioners, i ma ścisłe powiązania z grupami roboczymi UE zajmującymi się taką problematyką, jak CBRN-E, UAS/C-UAS, EDD[5]. Wszystko to służy upowszechnianiu najlepszych praktyk w zakresie ochrony dużych wydarzeń, przestrzeni publicznych, węzłów transportowych i komunikacyjnych czy miejsc kultu religijnego. Aby zrealizować te cele, w ramach EU-HRSN utworzono pięć grup roboczych:

- WG 1 – *Threat and Risk Assessment* – zajmująca się oceną podatności na ataki terrorystyczne, koordynowana przez EU PSA,
- WG 2 – *Tactical Use of UAV/C-UAV*[6] – zajmująca się bezzałogowymi statkami powietrznymi, koordynowana przez Hiszpanię (GAR),
- WG 3 – *Tactical Rescue and Response* – zajmująca się zagadnieniami z zakresu ratownictwa taktycznego i reagowania na incydenty wysokiego ryzyka, koordynowana przez Irlandię (STOC),
- WG 4 – *Human Factor* – zajmująca się zagadnieniami związanymi z doborem ludzi i procedurami ich szkolenia, koordynowana przez Holandię (policja krajowa),
- WG 5 – *Multi-agency command and control* – odpowiadająca za zarządzanie operacjami wysokiego ryzyka, koordynowana przez Wielką Brytanię (National Counter Terrorism Security Office).

Diagram. Grupy robocze działające w ramach sieci EU-HRSN.

Źródło: materiały własne Grupo de Acción Rápida.

[5] EDD (*explosives detection dogs*) – psy do wykrywania materiałów wybuchowych (przyp. red.).

[6] UAV (*unmanned aerial vehicle*) – bezzałogowy statek powietrzny; C-UAV (*counter-unmanned aerial vehicle*) – system zwalczania bezzałogowych statków powietrznych (przyp. red.).

Podczas obecnej hiszpańskiej prezydencji zostały podjęte (wspólnie z grupą sterującą) starania w celu wypracowania nowego podejścia do problematyki dotyczącej ochrony wydarzeń. Z doświadczeń GAR wynika bowiem, że nie ma lepszego sposobu wymiany wiedzy i dobrych praktyk niż praca w terenie, stawianie czoła realnym wyzwaniom i stosowanie różnych TTP, opracowanych w odmiennych środowiskach i ramach prawnych, oraz konfrontacja z wrogimi TTP napotykanymi w pracy służb poszczególnych krajów członkowskich. Z tego sposobu wymiany wiedzy i doświadczeń skorzystano po raz pierwszy w historii sieci EU-HRSN we wrześniu 2022 r. w Templemore (Irlandia), do którego irlandzka policja (Garda Síochána) zaprosiła ponad 60 ekspertów z 12 różnych krajów. Byli to specjaliści w dziedzinie ratownictwa taktycznego i reagowania kryzysowego, przedstawiciele wszystkich podmiotów, które byłyby zaangażowane w rzeczywistą sytuację wymagającą interwencji.

Z kolei w listopadzie 2022 r. w Logroño (Hiszpania), na Experiences Polygon for Special Forces (UAR, GAR i CoEST[7]), w celu wymiany doświadczeń spotkali się członkowie grupy WG 2. Byli wśród nich eksperci ze Stanów Zjednoczonych (FBI), Belgii, Portugalii, Francji i Irlandii.

Zdjęcie 2. Spotkanie grupy roboczej WG 2 – wymiana doświadczeń w zakresie C-UAS.

Źródło: materiały własne Grupo de Acción Rápida.

[7] CoEST (Centre of Excellence for Special Training) – Centrum Doskonałości ds. Szkoleń z Technik Specjalnych (przyp. red.).

Prace grupy WG 1 rozpoczęły się kilka tygodni później w Brukseli. W związku z tym, że są one ściśle powiązane z działaniami grupy EU PSA i osób zajmujących się taktyką Red Teaming, skorzystano z okazji, aby osoby zaangażowane w te trzy inicjatywy UE mogły wymienić się swoją wiedzą.

Zdjęcie 3. Spotkanie grupy roboczej WG 1 oraz osób zajmujących się taktyką Red Teaming w EU PSA.

Źródło: materiały własne Grupo de Acción Rápida.

W 2023 r. w Londynie odbyły się spotkanie grupy WG 5 oraz warsztaty na temat ataków terrorystycznych przeprowadzanych z wykorzystaniem pojazdów taranujących. Na drugą połowę roku zaplanowano spotkanie grupy WG 4, konferencję generalną, spotkania grupy sterującej oraz wspólne szkolenia i inne formy wymiany wiedzy organizowane w celu zwiększania odporności na terroryzm i stwarzania warunków utrudniających podejmowanie różnego rodzaju aktów terrorystycznych.

Działalność EU-HRSN nie ogranicza się tylko do obszaru UE. Bezpośrednio lub pośrednio wspiera ona również inne inicjatywy Unii poza jej granicami poprzez takie projekty, jak: GAR-SI SAHEL (Groupes d'Action Rapide – Surveillance et Intervention au Sahel), obejmujący Mauretanię, Burkina Faso, Mali, Niger, Senegal i Czad, już zakończony CT MENA (Counter-terrorism in the Middle East and North Africa) dotyczący Bliskiego Wschodu i Afryki Północnej oraz CT Public Spaces – w Ghanie, Kenii i Senegalu.

Sieć EU-HRSN jest potrzebna i dlatego ta inicjatywa będzie się rozwijać, gdyż zagrożenia terrorystyczne niestety nadal będą istniały. Wypracowanie wspólnego języka w środowisku antyterrorystycznym, dzielenie się wiedzą specjalistyczną i budowanie zaufania ma służyć stworzeniu silnego

zespołu, skutecznie przeciwdziałającego zagrożeniom terrorystycznym. EU-HRSN może okazać się jednym z najlepszych narzędzi w walce z tymi zagrożeniami.

Przydatne linki

CT Public Spaces:
https://www.ctpublicspaces.eu/

EU PSA:
https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en

GAR-SI SAHEL:
https://ec.europa.eu/trustfundforafrica/region/sahel-lake-chad/regional/gar-si-sahel-groupes-daction-rapide-surveillance-et-intervention_en

Sieci i inicjatywy UE:
https://ec.europa.eu/newsroom/pps/items/715174/en

Unijny plan działania na rzecz wspierania ochrony przestrzeni publicznej:
https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017DC0612

Kontakt: Presidency@HRSN.EU

Gregorio Salazar

Oficer operacyjny, a później instruktor. Specjalizuje się w ratownictwie taktycznym i reagowaniu, strzelectwie wyborowym, samoobronie policyjnej oraz ćwiczeniach interwencyjnych i strzeleckich. W latach 2014–2018 był oddelegowany jako szef ochrony Ambasady Hiszpanii w Wielkiej Brytanii. Strateg hiszpańskiej prezydencji w EU High Risk Security Network. Przez ponad 20 lat służył w formacji Guardia Civil. Dzieli się wiedzą i doświadczeniem w środowisku międzynarodowym.

https://doi.org/10.4467/27204383TER.23.027.18329

EU Protective Security Advisors

Inicjatywa Unii Europejskiej wspierająca wysiłki państw członkowskich w zakresie ochrony obywateli i infrastruktury krytycznej przed zamachami terrorystycznymi

Radosław Olszewski, Beate Zapletal, Wiktor Wojtas

Koncepcja EU PSA

Zabezpieczenie przestrzeni publicznej i infrastruktury krytycznej jest podstawowym obowiązkiem państw członkowskich Unii Europejskiej. Podobnie jak w wielu innych obszarach bezpieczeństwa wewnętrznego UE mogłaby odegrać istotną rolę w ułatwianiu dzielenia się dobrymi praktykami, zachęcaniu do wymiany doświadczeń i wspieraniu wzajemnej pomocy operacyjnej. Jednym z wartościowych przykładów takiego podejścia jest unijny program doradców ds. budowania odporności na zagrożenia (ang. EU Protective Security Advisors, EU PSA). Mimo że program EU PSA został oficjalnie ogłoszony w grudniu 2020 r., wraz z publikacją unijnej agendy antyterrorystycznej[1], ma on swoje źródło w pracach UE nad ochroną

[1] *Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0795 (przyp. red.).

obiektów w przestrzeni publicznej (zwanych wówczas celami miękkimi), które rozpoczęły się już w 2012 r. Urzędnicy Komisji Europejskiej zostali wówczas zaproszeni do zapewnienia wsparcia eksperckiego w zakresie środków bezpieczeństwa zastosowanych podczas XIV Mistrzostw Europy w Piłce Nożnej UEFA Euro 2012. To pozytywne doświadczenie zaowocowało kolejnymi zaproszeniami od państw członkowskich. Komisja Europejska przyczyniła się do ochrony wydarzeń politycznych wysokiego szczebla, takich jak szczyty NATO, lub imprez plenerowych, np. jarmarki bożonarodzeniowe lub festiwale muzyczne, m.in. festiwal Untold zorganizowany w Kluż-Napoce w Rumunii.

Ważnym krokiem w polityce UE w zakresie ochrony przestrzeni publicznej było przyjęcie w październiku 2017 r. planu działania poświęconego tym zagadnieniom[2]. W ramach jego realizacji opracowano m.in. unijne narzędzie oceny podatności na zagrożenia. Ten bardzo praktyczny instrument ułatwił ocenę wydarzeń wysokiego ryzyka, przeprowadzaną na miejscu wspólnie z udziałem ekspertów z KE i z państw członkowskich. Sukces tej inicjatywy pozwolił na stworzenie grupy specjalistów z organów ścigania oraz ze służb bezpieczeństwa i wywiadu, co doprowadziło do ustanowienia unijnego programu PSA. Warto podkreślić, że KE – mając jasny zamysł co do dalszych działań – korzystała ze wsparcia i wiedzy partnerów strategicznych UE, m.in. Stanów Zjednoczonych, które mają własny program PSA. Ponadto w USA i krajach UE zrealizowano wspólnie kilka przedsięwzięć oraz wymian najlepszych praktyk z innymi partnerami spoza Unii.

Zadania EU PSA

Celem EU PSA jest zapewnienie wsparcia państwom członkowskim, które o nie wnioskują. Działania podejmowane w ramach tego wsparcia obejmują:

– zwiększenie świadomości na temat podatności obiektów w przestrzeni publicznej i infrastruktury krytycznej na zagrożenia poprzez zapewnienie wspólnego systemu oceny poziomu bezpieczeństwa,

[2] *Plan działania na rzecz wspierania ochrony przestrzeni publicznej*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017DC0612 (przyp. red.).

- dzielenie się dobrymi praktykami i zachęcanie do poszerzania wiedzy w celu wyeliminowania zidentyfikowanych słabych punktów w sferze bezpieczeństwa,
- udzielanie państwom członkowskim wskazówek w zakresie organizowania imprez masowych i ochrony obiektów wysokiego ryzyka,
- stworzenie społeczności ekspertów poprzez organizację międzynarodowych szkoleń i przedsięwzięć przyczyniających się do rozwoju wspólnej kultury bezpieczeństwa w UE.

Grupa ekspertów EU PSA liczy ok. 100 osób z KE i państw członkowskich (w przypadku Polski są to eksperci z Policji, Agencji Bezpieczeństwa Wewnętrznego i Służby Ochrony Państwa). Są to osoby mające doświadczenie zawodowe w budowaniu ochrony i bezpieczeństwa obiektów publicznych, a jednocześnie dysponujące wiedzą specjalistyczną z różnych dziedzin. Państwo członkowskie zwracające się o wsparcie musi określić, z jakiego rodzaju pomocy chciałoby skorzystać. Każdy zespół EU PSA składa się ze specjalistów z kwalifikacjami w takich obszarach, jak np.: operacje bezzałogowymi statkami powietrznymi (ang. *unmanned aerial vehicle*, UAV), wykrywanie zagrożeń wybuchowych oraz związanych z użyciem środków chemicznych, biologicznych, radiologicznych i jądrowych (ang. *chemical, biological, radiological, and nuclear*, CBRN), interwencje specjalne i taktyki zwalczania terroryzmu, zarządzanie kryzysowe. W zależności od rodzaju zadania i celu udzielanego wsparcia może być ono ograniczone np. jedynie do fazy przygotowawczej w zakresie bezpieczeństwa wydarzenia lub obejmować również pomoc podczas samego wydarzenia. Konsultacja ekspertów ma charakter poufny i jest przeprowadzana wspólnie ze specjalistami z państwa przyjmującego. Stanowi ona okazję do podzielenia się dobrymi praktykami i zdobytym doświadczeniem, co pozwala zwiększyć świadomość na temat słabych punktów wspólnej kultury bezpieczeństwa i przyczynia się do jej stopniowego rozwoju w całej UE.

Zakres działań EU PSA

O ile na początku program EU PSA był wynikiem rozwoju na szczeblu UE polityki ochrony przestrzeni publicznej, o tyle obecnie dotyczy on również ochrony infrastruktury krytycznej. Lista ostatnich działań ekspertów z EU PSA obejmuje miejsca kultu religijnego i instytucje wyznaniowe,

wydarzenia kulturalne, np. duże festiwale muzyczne, wydarzenia z udziałem VIP-ów, takie jak szczyty UE, a także duże obiekty infrastrukturalne, np. lotnisko przesiadkowe (Warszawa) lub duży port morski (Konstanca, Rumunia). Należy podkreślić, że program EU PSA nie pokrywa się z unijnymi inspekcjami bezpieczeństwa lotniczego i morskiego, które mają inny zakres działań i cele. Biorąc pod uwagę niedawne skupienie się na szczeblu UE na zwiększaniu odporności infrastruktury krytycznej na zagrożenia terrorystyczne, można stwierdzić, że najprawdopodobniej w przyszłości będzie przeprowadzanych więcej ocen tego rodzaju obiektów.

Przykłady działań EU PSA

W ostatnich latach nastąpił gwałtowny wzrost liczby ataków na miejsca kultu religijnego, dlatego stały się one priorytetowymi lokalizacjami dla EU PSA. Zespół odwiedził np. katedry w Ulm i Münster w Niemczech, gdzie przyjrzał się m.in. zagrożeniu ze strony pojazdów taranujących, a także scenariuszowi ataku z udziałem aktywnego strzelca.

Wydarzeniem, które szczególnie skorzystało na wsparciu EU PSA, jest festiwal muzyczny Untold organizowany w Kluż-Napoce w Rumunii. Setki tysięcy osób co roku przyjeżdżają tam, aby cieszyć się muzyką i dobrze bawić. Zapewnienie odpowiedniego poziomu bezpieczeństwa w takim przypadku jest dużym wyzwaniem. Z tego powodu rumuńskie władze poprosiły EU PSA o wsparcie podczas trzech kolejnych edycji festiwalu. Z każdym następnym rokiem stosowano bardziej zaawansowane środki bezpieczeństwa. Jednocześnie zespół EU PSA zapewnił wsparcie operacyjne w zakresie wykrywania nieautoryzowanych dronów. Z prośbą o pomoc zwrócił się również operator największego polskiego portu lotniczego, tj. Lotniska Chopina w Warszawie. Zespół EU PSA ocenił m.in. bezpieczeństwo dostaw paliw i energii.

Przyszłość EU PSA

W związku z tym, że program EU PSA zyskuje coraz większe uznanie wśród władz państw członkowskich UE, a warunki geopolityczne pozostają niestabilne, można oczekiwać, że zainteresowanie działaniami EU PSA będzie rosło. Państwa członkowskie już zgłaszają zamiar zaproszenia KE i ekspertów

w celu przeprowadzenia oceny niektórych krajowych obiektów infrastruktury krytycznej, zwłaszcza w kontekście niedawno przyjętej dyrektywy[3] w sprawie odporności podmiotów o kluczowym znaczeniu. Z punktu widzenia EU PSA wiąże się to z pewnymi wyzwaniami – niektóre z wniosków dotyczą bardzo niszowych sektorów. W związku z tym znalezienie ekspertów mających odpowiednią wiedzę specjalistyczną może okazać się niełatwe. Tym bardziej że program EU PSA, chociaż rozwija się prężnie i stale wzrasta poziom wiedzy osób zaangażowanych w to przedsięwzięcie, jest wciąż stosunkowo nową inicjatywą. Mimo że jego kontynuacja może wiązać się z wieloma trudnościami, jedno jest pewne – w jego wyniku obywatele oraz operatorzy infrastruktury krytycznej państw członkowskich UE będą lepiej chronieni przed zagrożeniem terrorystycznym.

Zdjęcie. Członkowie zespołu EU PSA (od lewej: Radosław Olszewski, Wiktor Wojtas, Krzysztof Sowiński, Damian Szlachter) podczas oceny Lotniska Chopina w Warszawie, maj 2022 r.

Źródło: materiały własne Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej.

Autorzy pracują w jednostce antyterrorystycznej Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej. Artykuł odzwierciedla stan na dzień 1 III 2023 r., a wyrażone w nim poglądy są wyłącznie osobiste i nie reprezentują oficjalnego stanowiska Komisji Europejskiej.

[3] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE* (Dz. Urz. L 333/164 z 27 XII 2022 r.) – (przyp. red.).

Radosław Olszewski

Ekspert w jednostce ds. zwalczania terroryzmu Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej. Twórca i lider inicjatywy EU Protective Security Advisors. Marynarz i pilot statków powietrznych. Były audytor ochrony lotnictwa cywilnego w Komisji Europejskiej.

Beate Zapletal

Od lutego 2020 r. ekspertka krajowa oddelegowana do jednostki ds. zwalczania terroryzmu Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej. Jest zaangażowana w inicjatywę EU Protective Security Advisors. Wcześniej pracowała w Niemczech w Federalnym Ministerstwie Spraw Wewnętrznych i Federalnym Ministerstwie Transportu. Przed zatrudnieniem w służbie publicznej pracowała w Niemczech w sektorze finansowym.

Wiktor Wojtas

Od 2013 r. analityk ds. polityki w jednostce ds. zwalczania terroryzmu Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej. Wcześniej w tej dyrekcji pełnił funkcję kierownika programu zapobiegania i zwalczania przestępczości. Przed podjęciem pracy w Komisji Europejskiej w 2007 r. pracował w Polsce w sektorze finansowym. Jest zaangażowany w inicjatywę EU Protective Security Advisors.

https://doi.org/10.4467/27204383TER.23.028.18330
https://orcid.org/0000-0003-2763-9325

Po pierwsze prewencja

Szwedzki model ochrony antyterrorystycznej

W styczniu 2023 r. Szwecja objęła prezydencję w Radzie UE. Jednym z czterech priorytetów tej prezydencji było bezpieczeństwo, w tym ochrona przed zagrożeniami o charakterze terrorystycznym. Na temat rozwiązań antyterrorystycznych stosowanych w Szwecji, roli prewencji, edukacji i współpracy międzynarodowej w zwiększaniu poziomu bezpieczeństwa oraz wyzwań dla tamtejszych służb związanych z prezydencją, z **Danielem Hedmanem**, ekspertem sztokholmskiej policji ds. budowania odporności na ataki terrorystyczne, rozmawia Damian Szlachter.

Szwecja objęła półroczną prezydencję w Radzie UE. Czy ochrona przed terroryzmem będzie jednym z priorytetów tej prezydencji?

Daniel Hedman: Prezydencja w Radzie UE działa zawsze w tzw. trójce (klasyczna trójka składa się z państwa członkowskiego sprawującego prezydencję, państwa, które ją sprawowało poprzednio, oraz tego, które ją obejmie na kolejne pół roku – dop. D.Sz.). Prezydencja szwedzka będzie kontynuować program uzgodniony z pozostałymi dwoma krajami z tej trójki. Budowanie odporności na zagrożenia terrorystyczne to oczywiście jeden z priorytetów szwedzkiego rządu, a największy nacisk zostanie położony na prewencję terrorystyczną. Chodzi tu o prewencję w kontekście radykalizacji prowadzącej do działań ekstremistycznych z użyciem przemocy oraz zmniejszania podatności na groźne ideologie, jak również o samą aktywność o charakterze terrorystycznym, zarządzanie kryzysowe w przypadku ataku terrorystycznego i budowanie odporności na tego rodzaju ataki wśród podmiotów mogących stać się potencjalnymi celami. Prewencja to filar walki z terroryzmem. Takie podejście jest szczególnie bliskie szwedzkiemu społeczeństwu.

W jaki sposób ocenia się poziom zagrożenia terrorystycznego w Szwecji? Która instytucja odgrywa wiodącą rolę w tym zakresie?

D.H.: W Szwecji system klasyfikacji poziomu zagrożenia terrorystycznego jest bardzo podobny do rozwiązań obowiązujących w większości krajów UE. Obecnie ten poziom wynosi 3 (podwyższone zagrożenie, brak dowodów na planowanie – dop. D.Sz.) w 5-stopniowej skali (5 – nieuchronny atak, dowody na planowanie – dop. D.Sz.). Organem oceniającym poziom tego zagrożenia jest Narodowe Centrum Oceny Zagrożenia Terrorystycznego (ang. National Centre for Terrorist Threat Assessment, szw. Nationellt centrum för terrorhotbedömning, NCT). NCT jest stałą grupą roboczą w ramach Szwedzkiej Rady Współpracy na rzecz Zwalczania Terroryzmu (ang. Swedish Counter-Terrorism Cooperation Council, szw. Samverkansrådet mot terrorism) w Szwedzkiej Służbie Bezpieczeństwa (ang. Swedish Security Service, szw. Säkerhetspolisen,

Sapo), ale nie jest jej formalną częścią. NCT jest obsadzone przez personel Agencji Rozpoznania Radioelektronicznego (ang. National Defense Radio Establishment, szw. Försvarets radioanstalt, FRA), Dyrekcji Wywiadu Wojskowego i Bezpieczeństwa (ang. Military Intelligence and Security Directorate, szw. Militära underrättelse- och säkerhetstjänsten, MUST) oraz Szwedzkiej Służby Bezpieczeństwa. Oceny na temat zagrożenia terrorystycznego otrzymuje również 14 agencji rządowych wchodzących w skład Szwedzkiej Rady Współpracy na rzecz Zwalczania Terroryzmu. NCT opracowuje analizy, w tym analizy strategiczne, ale nie prowadzi dochodzeń w sprawie przestępstw. Formułuje jedynie ocenę dotyczącą stopnia zagrożenia. Ostateczną decyzję w sprawie jego poziomu podejmuje szef Szwedzkiej Służby Bezpieczeństwa.

Sztokholm plasuje się wysoko na liście europejskich miast, które w ostatnich kilkudziesięciu latach doświadczyły różnego rodzaju ataków terrorystycznych. Jak wygląda budowanie odporności na te ataki w stolicy Szwecji? Na co kładzie się nacisk?

D.H.: W tej chwili najważniejsze są dwie kwestie – kontynuacja współpracy w zakresie działań prewencyjnych mających na celu zapobieganie radykalizacji prowadzącej do terroryzmu oraz budowanie odporności na ataki kinetyczne. Budowanie tej odporności ma ścisły związek z obroną cywilną kraju i strategią obronną państwa, a ze względu na geopolityczne konsekwencje wojny w Ukrainie jest osadzone w obszarze integracji z NATO. W Szwecji mamy holistyczne podejście do zapewniania państwu ochrony przed współczesnymi zagrożeniami hybrydowymi. Dużą wagę przywiązuje się do budowania w społeczeństwie odporności na różnego rodzaju zagrożenia, a precyzyjniej rzecz ujmując – do kształtowania mentalności społecznej.

Mamy pewne luki systemowe w dziedzinie prawodawstwa, na przykład w ocenie tego, czym jest infrastruktura krytyczna (IK), a czym nie, jak również tego, kto w administracji rządowej odpowiada za ochronę obiektów innych niż IK. Warto przy tym mieć na uwadze, że dane historyczne

i statystyczne zawsze opisują przeszłość, nie pozwalają natomiast jednoznacznie przewidzieć przyszłości (należy również pamiętać, że na przestrzeni lat zmienia się kwalifikacja konkretnych incydentów powiązanych z terroryzmem. Na przykład rok wcześniej jakieś zdarzenie mogło zostać zaklasyfikowane jako incydent ekstremistyczny, a po zmianach prawnych już jako atak terrorystyczny – dop. D.Sz.). Sztokholm jest niestety miastem szczególnie doświadczonym incydentami o charakterze terrorystycznym. Kilka z nich miało miejsce w centrum tej metropolii (pięć w ciągu 22 lat – dop. D.Sz.). Ta część miasta cechuje się dużą podatnością na atak, ponieważ znajdują się w niej takie obiekty, jak centra handlowe i biznesowe, budynki organów rządowych, biura parlamentarne, budynki o znaczeniu symbolicznym należące do szwedzkiej monarchii, strategiczne węzły komunikacji miejskiej. Pojawia się w niej wiele osób o statusie VIP, a także ogromna liczba turystów. To przyciąga zainteresowanie ekstremistów gloryfikujących przemoc jako narzędzie działań politycznych oraz terrorystów.

Jakiego rodzaju obiekty otrzymują w Szwecji wsparcie państwa w zakresie prewencji antyterrorystycznej?

D.H.: W latach 2014–2015 szwedzka policja zaczęła wspierać władze Sztokholmu w pierwszych inicjatywach antyterrorystycznych mających na celu wzmocnienie bezpieczeństwa fizycznego wybranych obiektów o dużej podatności na ataki terrorystyczne. Działania te zostały zintensyfikowane po ataku na norweskiej wyspie Utøya, który był ogromnym szokiem dla wszystkich krajów nordyckich i momentem przebudzenia. Na początku realizowania projektów prewencyjnych skupiliśmy się na zwiększeniu zdolności szwedzkiej policji do radzenia sobie ze skutkami ataków terrorystycznych, na zapobieganiu radykalizacji prowadzącej do terroryzmu (została pogłębiona współpraca między władzami lokalnymi a społecznościami narażonymi na radykalizację – dop. D.Sz.), opracowaniu programu doradczego ds. zwiększania odporności celów miękkich na ataki kinetyczne. Liderem w tym obszarze była

policja, którą na początkowym etapie prac wspierała rządowa Agencja ds. Zarządzania Kryzysowego/Zapewnienia Ciągłości Działania (ang. Swedish Civil Contingencies Agency, szw. Myndigheten för samhällsskydd och beredskap, MSB).

Od 2016 r. tworzyliśmy od podstaw ramy prawne, wybieraliśmy liderów terenowych, opracowywaliśmy metodykę oceny obiektów, procedury i normy standaryzujące rozwiązania systemowe do ochrony przed terroryzmem. Zostały przygotowane, również w języku angielskim, specjalistyczne poradniki w celu zmniejszenia podatności na atak, poświęcone m.in. bezpieczeństwu imprez masowych, reagowaniu na aktywnego strzelca czy ochronie miejsc publicznych. Są one uznawane za wzorcowe i wykorzystywane nie tylko w Szwecji, lecz także na poziomie UE (kolejne cztery poradniki są tłumaczone na język angielski – dop. D.Sz.), m.in. w unijnych ekspertyzach opublikowanych przez Wspólne Centrum Badawcze Komisji Europejskiej (ang. EU Joint Research Centre) w obszarze antyterroryzmu.

Mamy obecnie przepisy wiążące instytucje państwowe i 9 z 12 sektorów rządowych, które są klasyfikowane jako systemy infrastruktury krytycznej. Nie zostało jednak jednoznaczne określone, co jest tą infrastrukturą, a co nie. Na przykład Dworzec Centralny w Sztokholmie nie jest IK, dopóki zdarzenie powodujące poważne zakłócenie funkcjonowania tego strategicznego szlaku komunikacyjnego nie zostanie sklasyfikowane jako krytyczne. Innymi słowy, wsparcie tej konkretnej placówki przez szwedzkie służby specjalne ma miejsce tylko wtedy, gdy dochodzi do incydentu krytycznego dla zapewnienia ciągłości działania transportu kolejowego w mieście. Blisko 90% instytucji państwowych i organów z nimi związanych (usługi podstawowe – dop. D.Sz.) należy do szwedzkiej infrastruktury krytycznej i dlatego może być objęte programami poświęconymi budowaniu odporności na ataki terrorystyczne.

Dziś można powiedzieć, że Szwecja ma rozwiązania systemowe, w ramach których władze lokalne, przedstawiciele organizacji społecznych czy biznesu mogą zwrócić się do policji lub MSB z prośbą o wsparcie w budowaniu kompleksowej odporności na ataki terrorystyczne. Jeszcze pięć lat temu ludzie

praktycznie nie zdawali sobie sprawy z istnienia fizycznych barier antyterrorystycznych służących do powstrzymania ataku przeprowadzanego za pomocą samochodu. Obecnie w Szwecji istnieje system ochrony przed atakiem terrorystycznym i jego skutkami, w którym ważną rolę odgrywa dialog wszystkich stron. Powtórzę raz jeszcze, to są rozwiązania systemowe budowane od podstaw.

Co z perspektywy Twojego doświadczenia ma realny wpływ na zwiększenie odporności obiektu na ataki terrorystyczne? Jakie rozwiązania powinny być traktowane priorytetowo na przykład w przypadku siedzib organów państwowych czy obiektów transportowych stanowiących infrastrukturę krytyczną?

D.H.: Najważniejszą kwestią jest zaprojektowanie systemu detekcji, który wykorzystuje system czujników, kamer wideo, bramki wykrywające metalowe przedmioty czy punkty kontroli dostępu. Zwiększenie szans wykrycia to czynnik, który ma istotny wpływ na zapobieganie zagrożeniom terrorystycznym czy sabotażowym. Podstawowym warunkiem stworzenia skutecznego systemu detekcji jest wdrożenie strefy bezpieczeństwa poza chronionym obiektem, w odległości od 10 do 100 m od jego obrysu. Znaczenie ma również widoczność każdego systemu bezpieczeństwa. To drogie rozwiązanie, ale na bezpieczeństwie oszczędzać nie warto. W ten właśnie sposób budujemy odporność na zagrożenia terrorystyczne Dworca Centralnego w Sztokholmie, o którym wspomniałem wcześniej. Za kilka miesięcy poznamy pierwsze dane, czy nowy model ochrony tego obiektu się sprawdza. Warto również zadbać o to, aby ten system detekcji zaprojektować w jak najprostszy sposób i z zachowaniem swobód obywatelskich. Szwecja jest przykładem kraju, który udowadnia, że ta równowaga jest osiągalna i akceptowalna dla społeczności lokalnych.

Szwecja bardzo aktywnie działa w UE w obszarze prewencji terrorystycznej i podejmuje liczne inicjatywy edukacyjne w zakresie bezpieczeństwa. Które z nich mają wymiar europejski i mogłyby być z powodzeniem wdrażane w innych krajach?

D.H.: W odniesieniu do aktywności o charakterze naukowym warto podkreślić dokonania szwedzkich badaczy zajmujących się zagrożeniami terrorystycznymi i procesami radykalizacji społecznej, którzy współkierują pracami unijnej sieci RAN (ang. Radicalization Awareness Network). Mam na myśli przede wszystkim dwóch profesorów – Magnusa Ranstorpa i Hansa Bruna. Jeśli chodzi o kwestie ochrony fizycznej przed atakami terrorystycznymi, z pewnością warto wspomnieć o tworzeniu międzyinstytucjonalnych antyterrorystycznych zespołów konsultacyjnych (rodzaj centrum wymiany doświadczeń i wiedzy – dop. D.Sz.) dla społeczności lokalnych. Tę inicjatywę warto podjąć w innych krajach członkowskich UE oraz w strukturach unijnych. Na przykład utworzyć antyterrorystyczne zespoły doradcze czy centra doskonalenia umiejętności w zakresie zwalczania terroryzmu, składające się z przedstawicieli wszystkich komórek organizacyjnych (dyrekcji generalnych) Komisji Europejskiej. Obecnie każdy organ unijny tworzy własne rekomendacje i podręczniki dotyczące ochrony przed zagrożeniami terrorystycznymi, ograniczając się jedynie do swojego obszaru kompetencji. Warto iść w stronę zasady „jeden za wszystkich".

Co było największym wyzwaniem podczas szwedzkiej prezydencji w UE w obszarze ochrony przed terroryzmem?[1]

D.H.: Największe wyzwanie stanowiła duża liczba spotkań oraz to, że odbywały się one w kilku różnych miejscach – na północy i południu Szwecji. Niektóre nasze jednostki policyjne na poziomie regionalnym nie mają wprawy w obsłudze tego rodzaju spotkań, częściowo brakuje im umiejętności operacyjnych niezbędnych do tego, by sobie z takim wyzwaniem poradzić. To wymuszało dokonywanie dużych ruchów zasobów osobowych i sprzętowych w krótkim czasie. Organizowanie

[1] Wywiad przeprowadzono w lutym 2023 r. Ostatnie pytanie zostało zadane podczas autoryzacji – w lipcu 2023 r., już po zakończeniu przez Szwecję prezydencji w Radzie UE (przyp. red.).

ochrony spotkań było utrudnione z uwagi na konieczność stałej modyfikacji bieżącej analizy zagrożenia w różnych miejscach organizacji wydarzeń, która musiała bazować na strategicznym poziomie oceny zagrożenia terrorystycznego w kraju. Dotyczyło to zwłaszcza tych spotkań, na których pojawiały się w sposób nieplanowany osoby o statusie VIP. Biorąc pod uwagę to, że niepożądane zdarzenia mogły poważnie zaszkodzić wizerunkowi Szwecji, konieczne było ponadnormatywne zwiększenie wysiłków w celu zapewnienia kompleksowej ochrony przed kilkoma różnymi rodzajami zagrożeń, w tym w zakresie gromadzenia danych wywiadowczych dotyczących przestępstw o charakterze terrorystycznym i ich monitorowania w sytuacji kryzysowej.

Rozmawiał: Damian Szlachter

Daniel Hedman

Nadinspektor, od ponad 30 lat funkcjonariusz szwedzkiej policji. Zatrudniony w jednostce ds. porządku i bezpieczeństwa publicznego, w której odpowiada za obsługę dużych wydarzeń, budowanie zdolności ochronnych w szwedzkim społeczeństwie oraz doradztwo dotyczące bezpieczeństwa na poziomie krajowym i unijnym. Ma duże doświadczenie w zakresie dowodzenia operacyjnego i kontroli nad specjalnymi operacjami policyjnymi oraz współpracy wieloagencyjnej. Pracował m.in. w Krajowej Radzie ds. Zwalczania Terroryzmu, w której był odpowiedzialny za zwiększenie zdolności szwedzkiej policji do walki z terroryzmem. Służył również w Szwedzkich Siłach Zbrojnych.