TERRORYZM

studia
analizy
prewencja

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

ISSN 2720-4383
e-ISSN 2720-6351

Recenzji są poddawane materiały zamieszczone w dziale Artykuły
oraz artykuły recenzyjne zamieszczone w dziale
Artykuły recenzyjne/recenzje

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 58 695
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Numer zamknięto i oddano do druku w grudniu 2025 r.

Druk
Mazowieckie Centrum Poligrafii Sp. z o.o.
ul. Ciurlionisa 4, 05-270 Marki
tel: 505 727 782

SPIS TREŚCI

7 **Wstęp redaktora naczelnego**

ARTYKUŁY

13 **Bioterroryzm w sektorze rolno-spożywczym – niedoszacowane ryzyko i wyzwania dla biobezpieczeństwa na przykładzie wybranych państw**
Matylda Augustyn-Barwicz

53 **Dwadzieścia lat od ataków na londyński system transportu miejskiego. Problem terroryzmu islamskiego w Wielkiej Brytanii**
Krzysztof Izak

101 **Zagrożenia terrorystyczne w Unii Europejskiej w 2024 roku. Analiza „TE-SAT. European Union Terrorism Situation and Trend Report 2025"**
Sebastian Wojciechowski, Artur Wejkszner

125 **Rola i znaczenie Eurojustu w przeciwdziałaniu terroryzmowi**
Dariusz Pożaroszczyk

ARTYKUŁY RECENZYJNE / RECENZJE

155 **Jerzy Trocha,**
Paradygmat bezpieczeństwa dworców kolejowych
Jacek Lasota, Małgorzata Lasota

PRACE KONKURSOWE

165 **Zdolności Sił Zbrojnych Rzeczpospolitej Polskiej w obszarze likwidacji skażeń – wybrane aspekty**
Krzysztof Tokarczyk

VARIA

203 **Jak samorządy mogą chronić przestrzenie publiczne przed atakami z użyciem pojazdów?**
Mariusz Cichomski

Załącznik
Ochrona przestrzeni publicznych przed atakami z użyciem pojazdów – rekomendacje dla samorządów

235 **Terroryści, sabotażyści, szpiedzy przebywający w polskich jednostkach penitencjarnych – rola Służby Więziennej**
Andrzej Leńczuk

255 **Od phishingu po sabotaż – ewolucja cyberzagrożeń wobec Polski. Wnioski z raportu CSIRT GOV za 2024 rok**
Monika Stodolnik

271 **Budowanie odporności europejskiego sektora kolejowego na zagrożenia hybrydowe. Polski wkład w dobre praktyki i zwiększenie bezpieczeństwa**
Tomasz Lachowicz

283 **Global Internet Forum to Counter Terrorism. Zwalczanie treści terrorystycznych i ekstremistycznych w przestrzeni cyfrowej**
Wywiad z dyrektor wykonawczą GIFCT Naureen Chowdhury Fink

291 English language version

Szanowni Państwo!

Gdy kilka miesięcy temu rozpoczynaliśmy prace nad kolejnym numerem czasopisma „Terroryzm – studia, analizy, prewencja" (T-SAP), nie spodziewaliśmy się, że to wydanie będzie tak aktualne pod kątem poruszonej tematyki. Prezentowane w nim materiały wpisują się w bieżące potrzeby badawcze i praktyczne związane z dynamicznie zmieniającą się rzeczywistością, w tym w sferze zagrożeń o charakterze terrorystycznym, a podjęta problematyka dotyczy żywotnych wyzwań stojących przed instytucjami odpowiedzialnymi za bezpieczeństwo.

Od czasu wybuchu wojny w Ukrainie mamy do czynienia z intensyfikacją działań aktywnych prowadzonych w krajach Unii Europejskiej przez rosyjskie służby specjalne i jej proxy wobec obiektów handlowych, wodno-kanalizacyjnych czy infrastruktury strategicznej sektora transportu, energii oraz łączności. Jest to przedmiotem wielu analiz. Warto wspomnieć o raporcie przygotowanym w 2025 r. przez renomowane think tanki – słowacki GLOBSEC i niderlandzki ICCT. Prezentuje on jednoznaczne dane o działaniach hybrydowych Federacji Rosyjskiej w Europie, w tym w Polsce, realizowanych m.in. przy wsparciu grup przestępczych. Działania te obejmują także przestępstwa o charakterze terrorystycznym. Publikujemy statystyki dotyczące liczby osób przebywających w polskich jednostkach penitencjarnych m.in. w związku z działalnością na rzecz obcego wywiadu i tego rodzaju przestępstwami. Ich przykładem są akty dywersji wymierzone w polską infrastrukturę kolejową, do których w dniach 15–17 listopada 2025 r. doszło na strategicznej linii transportowej z Warszawy do graniczącego z Ukrainą Dorohuska. W tym numerze T-SAP znajdą Państwo – jakże aktualny w tym kontekście – materiał

dotyczący budowania odporności europejskiego sektora kolejowego na zagrożenia hybrydowe oraz roli Polski w tym obszarze. Przedstawicielstwo Polskich Kolei Państwowych S.A. w Brukseli podejmuje liczne działania na poziomie unijnym, które realnie poprawiają bezpieczeństwo w tej branży. Obejmuje ona wiele elementów, przy czym jednym z kluczowych są dworce. Problematyce ich ochrony w Polsce jest poświęcona wyjątkowa książka wydana w 2025 r. przez Akademię Sztuki Wojennej. Monografia pt. *Paradygmat bezpieczeństwa dworców kolejowych*, której recenzję zamieszczamy, zasługuje na uwagę nie tylko ekspertów do spraw bezpieczeństwa i obronności, lecz także wszystkich zainteresowanych funkcjonowaniem kolei jako elementu infrastruktury krytycznej państwa. Zamykając motyw przewodni tego numeru, czyli zagrożeń w sektorze transportu, zachęcam do przeczytania artykułu prezentującego historię zamachów na londyński system transportu miejskiego w 2005 r. Należały one do najtragiczniejszych ataków terrorystycznych w Europie. Wśród licznych ofiar były trzy Polki. Te wydarzenia wywarły istotny wpływ na zmianę podejścia do działań antyterrorystycznych na poziomie krajowym i unijnym.

Na łamach T-SAP regularnie prezentujemy strategiczne dokumenty dotyczące walki z terroryzmem. Tym razem eksperci omówili najważniejsze tegoroczne raporty Europolu, Eurojustu i CSIRT GOV. Ich analiza pozwala na lepsze zrozumienie skali i dynamiki zmian zachodzących w zjawisku terroryzmu, identyfikację wyzwań i dobrych praktyk w zakresie jego zwalczania, a także ukazuje istotę współpracy międzynarodowej.

W poprzednim numerze zamieściliśmy komentarz do zmiany polskiej ustawy o działaniach antyterrorystycznych w związku z przeciwdziałaniem rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Kontynuując ten temat, publikujemy w tym wydaniu wywiad z dyrektor Global Internet Forum to Counter Terrorism, która opowiada o zwalczaniu treści terrorystycznych i ekstremistycznych w przestrzeni cyfrowej oraz roli tego gremium (zrzeszającego ponad 30 największych światowych podmiotów z sektora technologicznego) we wzmacnianiu bezpieczeństwa międzynarodowego.

Kontynuujemy również tematykę luk w działaniach państw Unii Europejskiej w obszarze antyterroryzmu. Jedną

z nich jest możliwość wykorzystania czynników biologicznych do działań terrorystycznych wobec sektora rolno-spożywczego. To ryzyko pozostaje niedoszacowane w politykach bezpieczeństwa wielu państw, zwłaszcza w zakresie oceny prawdopodobieństwa jego zaistnienia oraz potencjalnych skutków. Artykuł poświęcony problematyce bioterroryzmu pokazuje, jak istotne jest wzmocnienie zdolności państw do skutecznego reagowania na zagrożenia biologiczne. Przedstawione w nim treści mają charakter perspektywiczny i stanowią kierunek do dalszych analiz i badań naukowych. W obszar zagadnień dotyczących odporności na zagrożenia biologiczne, a także chemiczne i promieniotwórcze wpisuje się artykuł na temat zdolności Sił Zbrojnych Rzeczpospolitej Polskiej do likwidacji skażeń. Jego autor postuluje modernizację sprzętu, standaryzację procedur oraz wzmocnienie współpracy wojska z podmiotami pozamilitarnymi.

Staramy się wspierać projekty i inicjatywy budujące i wzmacniające odporność na działania terrorystyczne. Z satysfakcją przyjęliśmy powstanie wytycznych dla samorządów dotyczących ochrony przestrzeni publicznych przed atakami z użyciem pojazdów. Zostały one przygotowane przez Ministerstwo Spraw Wewnętrznych i Administracji oraz Komendę Główną Policji, przy wsparciu innych instytucji systemu antyterrorystycznego w Polsce. Mając na uwadze, jak te rekomendacje są ważne, szczególnie w okresie świąteczno-noworocznym, w związku z którym są organizowane m.in. okolicznościowe jarmarki z udziałem wielu ludzi, poprosiliśmy współtwórcę tego projektu o jego omówienie. Warto dodać, że wśród źródeł eksperckich cytowanych w tych wytycznych znalazły się opracowania publikowane na łamach T-SAP.

Cieszy fakt, że nasze wysiłki są dostrzegane również za granicą. Miłym akcentem jest otrzymanie gratulacji od Edwarda Lucasa – światowego autorytetu w kwestii działań hybrydowych realizowanych przez Federację Rosyjską wobec krajów NATO. Z uznaniem odniósł się on do wydania specjalnego T-SAP poświęconego ochronie infrastruktury krytycznej przed działaniami terrorystycznymi i sabotażowymi, przygotowanego przez Agencję Bezpieczeństwa Wewnętrznego i Rządowe Centrum Bezpieczeństwa. To kolejny dowód na to, że podążamy

we właściwym kierunku. Jest to możliwe dzięki naszym autorom, recenzentom, członkom Rady Naukowej oraz wysiłkom zespołu redakcyjnego, któremu dziękuję za zaangażowanie i profesjonalizm.

Na zakończenie chciałbym powitać dr Aleksandrę Komar, która została zastępczynią redaktora naczelnego i wraz z zespołem współtworzyła to wydanie T-SAP. Jestem przekonany, że dzięki jej wsparciu czasopismo będzie się intensywniej rozwijać, nie tylko pod względem naukowym.

Redaktor naczelny
dr Damian Szlachter

ARTYKUŁY

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 13–52

https://doi.org/10.4467/27204383TER.25.045.23032

Artykuł

Bioterroryzm w sektorze rolno-spożywczym – niedoszacowane ryzyko i wyzwania dla biobezpieczeństwa na przykładzie wybranych państw

Bioterrorism in the agri-food sector – underestimated risk and challenges for biosecurity based on selected countries

MATYLDA AUGUSTYN-BARWICZ https://orcid.org/0009-0006-2882-8311

Instytut Pirbrighta

Abstrakt

Celem artykułu był opis zagrożeń bioterrorystycznych wobec sektora rolno-spożywczego, ze szczególnym uwzględnieniem agroterroryzmu, którego ryzyko pozostaje niedoszacowane w politykach bezpieczeństwa wielu państw, zwłaszcza w zakresie oceny prawdopodobieństwa jego zaistnienia oraz potencjalnych skutków. Realizacja celu wiązała się z rozwiązaniem problemu badawczego sformułowanego w postaci pytania: Jakie są zagrożenia bioterrorystyczne wobec sektora rolno-spożywczego? Próbę rozwiązania tego problemu podjęto na podstawie przeglądu literatury oraz aktów prawnych, z zastosowaniem teoretycznych metod badawczych, takich jak: analiza, synteza, abstrahowanie oraz wnioskowanie. Pomimo uznania sektora produkcji żywności za element infrastruktury krytycznej brakuje scenariuszy i procedur reagowania na skażenia dokonywane intencjonalnie. W artykule zostały opisane definicje bioterroryzmu, agroterroryzmu i agroprzestępczości oraz podziały zagrożeń biologicznych. Porównano systemy biobezpieczeństwa w wybranych państwach, podkreślono znaczenie lokalnych podmiotów w systemach wczesnego ostrzegania

oraz wskazano szerszy kontekst bezpieczeństwa – ochronę żywności, zdrowia zwierząt i ludzi, które zgodnie z koncepcją One Health tworzą powiązaną całość wymagającą skoordynowanego zarządzania. We wnioskach zwrócono uwagę na konieczność rozwoju interoperacyjnych systemów nadzoru, laboratoriów wysokiego poziomu bezpieczeństwa biologicznego, edukacji i cyfryzacji oraz włączenia sektora rolno-spożywczego do strategii bezpieczeństwa narodowego i unijnego, co pozwoli wzmocnić odporność biologiczną Europy na zagrożenia hybrydowe.

Słowa kluczowe

bioterroryzm, agroterroryzm, bezpieczeństwo żywności, One Health, zagrożenia biologiczne

Abstract

The aim of this article is to describe bioterrorism threats to the agri-food sector, with particular emphasis on agroterrorism, the risk of which remains underestimated in the security policies of many countries, especially in terms of assessing its likelihood and potential consequences. Achieving this objective involves solving the research problem formulated in the form of a question: What are the bioterrorism threats to the agri-food sector? An attempt to solve this problem was made on the basis of a review of literature and legal acts, using theoretical research methods such as analysis, synthesis, abstraction and inference. Despite the recognition of the food production sector as part of critical infrastructure, there is a lack of scenarios and procedures for responding to intentional contamination. The article describes the definitions of bioterrorism, agroterrorism and agrocrime, as well as the classification of biological threats. It compares biosafety systems in selected countries, emphasises the importance of local entities in early warning systems, and points to the broader context of safety – food protection, animal and human health, which, according to the One Health concept, form an interconnected whole requiring coordinated management. The conclusions emphasise the need to develop interoperable surveillance systems, high-level biosafety laboratories, education and digitalisation, as well as to include the agri-food sector in national and EU security strategies, thereby strengthening Europe's biological resilience to hybrid threats.

Keywords

bioterrorism, agroterrorism, food security, One Health, biological threats

Wprowadzenie

Sektor rolno-spożywczy stanowi atrakcyjny cel działań o charakterze hybrydowym, ze względu na dużą rozciągłość geograficzną, złożoność procesów logistycznych z nim związanych oraz relatywnie niski poziom zabezpieczeń fizycznych. Ataki biologiczne w tym sektorze są często asymetryczne – agresor korzysta z tanich, niekonwencjonalnych i trudnych do wykrycia metod, a obrońca musi ponosić wysokie koszty, aby się przed nimi zabezpieczyć i reagować na ich skutki, a mimo to ataki te pozostają bardzo skuteczne. Ich konsekwencje mogą obejmować masowe uboje zwierząt gospodarskich, przerwanie łańcuchów dostaw, wzrost cen żywności, panikę społeczną (ang. *moral panic*) oraz utratę zaufania do instytucji publicznych[1]. W obliczu globalizacji i zmian klimatycznych wzrasta ryzyko transgranicznego rozprzestrzeniania się patogenów, co sprawia, że takie zjawiska nabierają wymiaru międzynarodowego.

W odpowiedzi na te problemy powstała koncepcja One Health, która łączy zdrowie ludzi, zwierząt i środowiska z elementami bezpieczeństwa wewnętrznego i promuje zintegrowane, interdyscyplinarne podejście, aby skutecznie zapobiegać tego rodzaju zagrożeniom. Jest ona rozwijana przez Światową Organizację Zdrowia (World Health Organization, WHO), Światową Organizację Zdrowia Zwierząt (World Organisation for Animal Health, WOAH) i Organizację Narodów Zjednoczonych do spraw Wyżywienia i Rolnictwa (Food and Agriculture Organization of the United Nations, FAO).

Z analizy strategii bezpieczeństwa wybranych państw Unii Europejskiej wynika, że ryzyko zagrożeń agroterrorystycznych pozostaje niedoszacowane. Ani Polska, ani Niemcy, Francja i Włochy nie opracowały odrębnych planów reagowania na ataki ukierunkowane na sektor rolno-spożywczy. Podobną lukę można dostrzec w Wielkiej Brytanii, gdzie mimo rozwiniętych strategii bioasekuracji roślin i analiz odporności łańcucha żywnościowego nie funkcjonuje odrębny, kompleksowy plan reagowania na ataki agroterrorystyczne.

Celem artykułu była analiza zagrożeń dla sektora rolno-spożywczego w wybranych państwach. Problematykę badawczą skoncentrowano wokół następujących pytań:

[1] J.P. Dudley, M.H. Woodford, *Bioweapons, bioterrorism and biodiversity: potential impacts of biological weapons attacks on agricultural and biological diversity*, „Revue Scientifique et Technique" 2002, nr 21(1), s. 125–137. http://dx.doi.org/10.20506/rst.21.1.1328.

1. W jaki sposób bioterroryzm, a zwłaszcza agroterroryzm, stanowi zagrożenie dla sektora rolno-spożywczego w wybranych państwach?
2. Dlaczego ryzyko agroterroryzmu pozostaje niedoszacowane w politykach bezpieczeństwa oraz jak kształtuje się percepcja tego zagrożenia przez społeczeństwo i władze na poziomie lokalnym i centralnym?
3. Jaką rolę odgrywają rolnicy, lekarze weterynarii i władze samorządowe w lokalnych systemach wczesnego ostrzegania i gotowości operacyjnej?
4. Jakie działania systemowe – instytucjonalne, technologiczne i edukacyjne – mogą zwiększyć odporność biologiczną sektora rolnego na poziomie krajowym i unijnym?

Definicje: bioterroryzm, agroprzestępczość i agroterroryzm

Bioterroryzm stanowi rosnące wyzwanie dla bezpieczeństwa wewnętrznego, zdrowia publicznego i stabilności gospodarczej państw. WHO i WOAH definiują go jako celowe użycie czynników biologicznych – mikroorganizmów chorobotwórczych lub toksyn biologicznych – przeciwko ludziom, zwierzętom lub roślinom, aby wywołać szkody społeczne, polityczne lub ekonomiczne[2]. WOAH wyróżnia również pojęcie agroprzestępczości (ang. *agro-crime*) oznaczające naruszające prawo działania dotyczące zwierząt lub produktów pochodzenia zwierzęcego, zagrażające zdrowiu publicznemu, dobrostanowi zwierząt czy bezpieczeństwu żywności. Należą do nich m.in.: fałszowanie produktów żywnościowych, czyli wprowadzanie zmian w ich składzie lub jakości w celu obniżenia kosztów produkcji, przemyt, oszustwa żywnościowe, czyli wprowadzanie konsumenta w błąd, aby osiągniąć zysk (przykładem są fałszywe deklaracje na temat pochodzenia czy składu), a także celowe uwalnianie patogenów. Warto podkreślić, że zakres agroprzestępczości jest szerszy niż wynika to z definicji WOAH, która odnosi się wyłącznie do zwierząt i produktów pochodzenia zwierzęcego. Są to również przestępstwa dotyczące roślin, środków produkcji rolnej,

[2] *Laboratory Biosafety Manual. Fourth Edition*, WHO, 21 XII 2020 r., https://www.who.int/publications/i/item/9789240011311 [dostęp: 10 VI 2025]; *Terrestrial Animal Health Code*, https://rr-africa.woah.org/app/uploads/2023/09/en_csatvol1-2023.pdf [dostęp: 14 VI 2025].

obrotu żywnością, fałszowania produktów i nielegalnego handlu materiałem siewnym[3].

Agroterroryzm (ang. *agro-terrorism*) stanowi szczególną, motywowaną politycznie i ideologicznie formę agroprzestępczości. Jego celem jest destabilizacja społeczeństwa przez wywołanie chorób zwierząt lub roślin. Różnica między tymi kategoriami wynika z motywacji. W agroprzestępczości dominuje cel ekonomiczny, w agroterroryzmie – cel polityczny lub społeczny[4].

W swoich strategiach WOAH stopniowo rozszerzała podejście do tego rodzaju zagrożeń. Dokument z 2015 r. koncentrował się na redukcji ryzyka biologicznego przez bioasekurację i współpracę międzynarodową, strategia z 2024 r. formalnie wprowadziła pojęcia *agro-crime* i *agro-terrorism* i położyła nacisk na prewencję, wykrywanie zagrożeń i koordynację działań służb weterynaryjnych, organów ścigania i instytucji bezpieczeństwa[5].

Mimo że w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2557 (nazywanej w skrócie dyrektywą CER, z ang. *Critical Entities Resilience*)[6] oraz w planach Organizacji Traktatu Północnoatlantyckiego (North Atlantic Treaty Organization, NATO)[7] sektor produkcji żywności został uznany za element infrastruktury krytycznej, to nadal brakuje planów reagowania i spójnego wdrażania zasad biobezpieczeństwa. Unia postrzega bioterroryzm jako intencjonalne użycie patogenów lub toksyn w celu zastraszenia ludności i destabilizacji struktur państwowych, WOAH jako celowe wprowadzanie chorób zakaźnych do populacji zwierząt gospodarskich lub dzikich, a NATO klasyfikuje go w ramach zagrożeń CBRN (chemicznych, biologicznych, radiologicznych i nuklearnych)[8]. Te rozbieżności

[3] E. Barclay, *A Review of the Literature on Agricultural Crime. Report to the Criminology Research Council,* https://criminology.fsu.edu/sites/g/files/upcbnu3076/files/2021-03/A-Review-of-the-Literature-on-Agricultural-Crime.pdf, s. 5–18, 46–76 [dostęp: 2 XII 2025].

[4] J.P. Dudley, M.H. Woodford, *Bioweapons, bioterrorism and biodiversity*...

[5] *Biological threat reduction strategy. Strengthening global biological security*, https://www.woah.org/app/uploads/2021/03/biothreat-strategy-veng-revised-1st-edition.pdf, s. 3–12 [dostęp: 14 VI 2025]; *Building resilience against agro-crime and agro-terrorism*, https://www.woah.org/app/uploads/2023/02/building-resilience-against-agro-crime-and-agro-terrorism.pdf, s. 1–10 [dostęp: 14 VI 2025].

[6] *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*.

[7] *NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy*, NATO, 14 VII 2022 r., https://www.nato.int/cps/en/natohq/official_texts_197768.htm [dostęp: 2 XII 2025].

[8] Tamże.

definicyjne i priorytetowe dodatkowo utrudniają tworzenie spójnych strategii reagowania na incydenty bioterrorystyczne w sektorze rolno-spożywczym oraz zapobiegania im[9].

Sektor rolno-spożywczy jako potencjalny cel ataku bioterrorystycznego

Sektor rolno-spożywczy stanowi jeden z najważniejszych elementów infrastruktury krytycznej, a jednocześnie jeden z najbardziej podatnych na działania o charakterze bioterrorystycznym. Złożoność systemu produkcji żywności, obejmującego produkcję, transport, przetwórstwo, magazynowanie i dystrybucję, powoduje, że punktów, w których można dokonać ingerencji, w tym skażenia surowców, paszy czy wody, jest wiele. Nawet incydent o charakterze lokalnym może prowadzić do efektu kaskadowego, skutkującego poważnymi konsekwencjami zdrowotnymi, gospodarczymi i społecznymi[10]. Newralgicznym elementem systemu pozostaje logistyka oparta na modelu *just-in-time*. Jest on efektywny pod względem kosztów, ale ogranicza zdolność reagowania na nagłe zakłócenia.

Pandemia COVID-19 i zmiany związane z brexitem ujawniły wrażliwość globalnych łańcuchów dostaw żywności[11]. Komisja Europejska podkreśla potrzebę zwiększenia odporności tego sektora przez dywersyfikację źródeł zaopatrzenia, tworzenie rezerw strategicznych oraz wzmocnienie mechanizmów wczesnego ostrzegania[12]. Badania Europejskiego Urzędu ds. Bezpieczeństwa Żywności (European Food Safety Authority, EFSA) wskazują ponadto, że bezpieczeństwo żywności powinno być analizowane

[9] *Deliverable D6.5 – Guiding Document on cross-sectoral preparedness and response to biological and/or chemical terror attack. Collaboration between health, civil protection and security*, https://www.jaterror.eu/wp-content/uploads/2024/11/6.5-Guiding-Document.pdf, s. 17, 19–26, 33, 41 [dostęp: 8 XII 2025].

[10] *The European Union One Health 2023 Zoonoses Report*, EFSA, 10 XII 2024 r. https://doi.org/10.2903/j.efsa.2024.9106.

[11] P. Garnett, B. Doherty, T. Heron, *Vulnerability of the United Kingdom's food supply chains exposed by COVID-19*, „Nature Food" 2020, nr 1, s. 315–318. https://doi.org/10.1038/s43016-020-0097-7.

[12] *Proofing the EU food supply chains against crises: new set of recommendations published*, European Commission, 23 VII 2024 r., https://agriculture.ec.europa.eu/media/news/proofing-eu-food-supply-chain-against-crises-new-set-recommendations-published-2024-07-23_en [dostęp: 14 VI 2025].

w kontekście czynników zdrowotnych, logistycznych i politycznych, rozpatrywanych łącznie i wymagających wspólnotowego podejścia do zarządzania ryzykiem[13]. W przypadku zagrożeń biologicznych logistyka kryzysowa ma decydujące znaczenie dla skutecznej izolacji ognisk zakażeń, sprawnej dystrybucji szczepionek i utrzymania alternatywnych kanałów dostaw[14]. Utrudnienia w transporcie – wynikające z blokad sanitarnych czy zamknięcia granic – mogą znacznie komplikować działania interwencyjne i potęgować negatywne skutki gospodarcze. Równie istotny jest wymiar psychologiczny ataków. Bioterroryzm wymierzony w sektor rolno-spożywczy może wywołać zjawisko paniki społecznej, prowadzące do paniki konsumenckiej, bojkotów produktów i dezinformacji – nierzadko o skutkach poważniejszych niż sam incydent z wykorzystaniem czynników biologicznych[15].

Przykładem ataku bioterrorystycznego w sektorze żywności jest masowe jej zatrucie przez członków sekty Rajneesha. Do zdarzenia doszło w 1984 r. w Oregonie (USA) – w restauracjach rozprowadzono bakterie *Salmonella typhimurium*, które spowodowały ponad 750 zachorowań[16]. Chociaż tego typu ataki są rzadkie, to pokazują, jaką skalę mogą mieć skutki intencjonalnego skażenia żywności.

Atak bioterrorystyczny może polegać również na zakażeniu zwierząt gospodarskich patogenami o wysokiej zaraźliwości, wywołującymi choroby

[13] *Food Risk Assess Europe*, EFSA, https://www.efsa.europa.eu/en/publications/food-risk-assess-europe [dostęp: 13 XII 2025].

[14] W.S. Carus, *Bioterrorism and Biocrimes: the Illicit Use of Biological Arms in the 20th Century*, August 1998, https://wmdcenter.ndu.edu/Publications/Publication-View/Article/626562/bioterrorism-and-biocrimes-the-illicit-use-of-biological-arms-in-the-20th-centu/ [dostęp: 14 VI 2025].

[15] *First report on world's animal health reveals changing spread of disease impacting food security, trade and ecosystems*, WOAH, 23 V 2025 r., https://www.woah.org/en/first-report-on-worlds-animal-health-reveals-changing-spread-of-disease-impacting-food-security-trade-and-ecosystems/ [dostęp: 15 VI 2025]; *What past disruptions can teach us about reviving supply chains after COVID-19*, World Economic Forum, 27 III 2020 r., https://www.weforum.org/stories/2020/03/covid-19-coronavirus-lessons-past-supply-chain-disruptions/ [dostęp: 27 V 2025]; D. Ivanov, A. Dolgui, *Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak*, „International Journal of Production Research" 2020, t. 58, nr 10, s. 2904–2915. https://doi.org/10.1080/00207543.2020.1750727.

[16] T.J. Török i in., *A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars*, „The Journal of the American Medical Association" 1997, t. 278, nr 5, s. 389–393. https://doi.org/10.1001/JAMA.1997.03550050051033.

takie jak wąglik, pryszczyca (ang. *foot and mouth disease*, FMD) czy afrykański pomór świń (ang. *African swine fever*, ASF)[17]. Może to prowadzić do epizootii, czyli zjawiska masowego występowania chorób zakaźnych wśród zwierząt na określonym obszarze i w określonym czasie, oraz przynosić negatywne skutki ekonomiczne. Przykładem jest epizootia FMD w Wielkiej Brytanii w 2001 r. W jej przebiegu odnotowano ponad 2000 ognisk choroby i przymusowo wybito ponad 6 mln zwierząt gospodarskich. Straty ekonomiczne oszacowano na ok. 8 mld funtów, w tym 3 mld w sektorze rolnym oraz 5 mld w sektorze turystyki i rekreacji. To zdarzenie nie miało charakteru bioterrorystycznego, ale ukazało gospodarcze, społeczne i psychologiczne konsekwencje szerzenia się chorób zakaźnych zwierząt, a także przyczyniło się do reformy brytyjskiego systemu zarządzania kryzysowego w rolnictwie[18].

Celowe wprowadzenie patogenów do sektora rolno-spożywczego mogłoby wywołać skutki porównywalne z naturalną epizootią. W czerwcu 2025 r. amerykańskie władze oskarżyły chińskich naukowców – Yunqing Jian i Zunyong Liu – o próbę przemytu do Stanów Zjednoczonych niebezpiecznego patogenu roślinnego – grzyba *Fusarium graminearum*[19]. Gatunek ten atakuje pszenicę, jęczmień, kukurydzę i ryż, wywołując fuzariozę kłosów zbóż (ang. *fusarium head blight*). Może ona powodować znaczne straty plonów oraz skażenie ziarna groźnymi mykotoksynami – przede wszystkim deoksyniwalenolem, wywołującym u ludzi i zwierząt m.in. wymioty, uszkodzenia wątroby, immunosupresję oraz zaburzenia reprodukcyjne. *Fusarium graminearum* jest uznawany za organizm, który może zostać użyty jako broń w działaniach bioterrorystycznych z uwagi na łatwość jego pozyskania, odporność środowiskową i zdolność do szybkiego

[17] M. Wheelis, R. Casagrande, L.V. Madden, *Biological Attack on Agriculture: Low-Tech, High-Impact Bioterrorism: Because bioterrorist attack requires relatively little specialized expertise and technology, it is a serious threat to US agriculture and can have very large economic repercussions*, „BioScience" 2002, t. 52, nr 7, s. 569–576. https://doi.org/10.1641/0006-3568(2002)052[0569:BAOALT]2.0.CO;2.

[18] D. Thompson i in., *Economic costs of the foot and mouth disease outbreak in the United Kingdom in 2001*, „Revue Scientifique et Technique" 2002, nr 21(3), s. 675–687. https://doi.org/10.20506/RST.21.3.1353.

[19] *Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory*, United States Attorney's Office, 3 VI 2025 r., https://www.justice.gov/usao-edmi/pr/chinese-nationals-charged-conspiracy-and-smuggling-dangerous-biological-pathogen-us [dostęp: 20 VI 2025].

rozprzestrzeniania się w systemach rolnych[20]. Wystarczy lokalne skażenie nasion lub materiału uprawnego, by wprowadzić go do łańcucha produkcji żywności w skali regionalnej czy międzynarodowej[21]. Opisywane zdarzenie z udziałem chińskich naukowców potwierdza, że obawy dotyczące środków ochrony biologicznej i wykorzystania patogenów roślinnych jako narzędzi agroterroryzmu są zasadne.

Typologie czynników biologicznych mogących zostać użytych jako broń przeciwko sektorowi rolno-spożywczemu

Aby uchwycić pełne spektrum zagrożeń wynikających z celowego użycia czynników biologicznych w sektorze rolno-spożywczym, warto wyróżnić główne kategorie środków, które mogą być użyte w działaniach agroterrorystycznych.

Patogeny zwierzęce

Wśród najgroźniejszych epizootii wymienia się ASF. Wywołujący go wirus charakteryzuje się niemal stuprocentową śmiertelnością u świń i dzików oraz wysoką odpornością na niekorzystne warunki środowiskowe. Od 2014 r. Europa i Azja ponoszą z jego powodu znaczne straty[22]. Równie poważnym zagrożeniem jest wysoce zjadliwa grypa ptaków (ang. *highly pathogenic avian influenza,* HPAI), zwłaszcza wywołana przez podtypy wirusa grypy typu A – H5N1 i H5N8, która prowadzi do masowych ubojów drobiu, blokad eksportowych i strat liczonych w miliardach dolarów[23]. Skutki ekstremalnej zoonozy obserwowano w 2001 r. podczas wspomnianej już epidemii FMD w Wielkiej Brytanii.

[20] E. White, *US says it broke up effort to bring toxic fungus to Michigan lab from China*, AP News, 3 VI 2025 r., https://apnews.com/article/chinese-scientists-charged-toxic-fungus-5ccaba9aff8e5941ebcea71b9b6690b2 [dostęp: 20 VI 2025].

[21] A. Ramakrishnan, *What is Fusarium graminearum, the fungus US authorities say was smuggled in from China?*, AP News, 4 VI 2025 r., https://apnews.com/article/fusarium-graminearum-fungus-head-blight-china-8ce925ae96d9c437b987e58c336cd45f [dostęp: 20 VI 2025].

[22] *African swine fever*, EFSA, 19 V 2025 r., https://www.efsa.europa.eu/en/topics/topic/african-swine-fever [dostęp: 16 VI 2025].

[23] G. Pavade, *WOAH Updates – Global HPAI situation and current standards and recommendations regarding AI surveillance and vaccination*, https://www.izsvenezie.com/documents/reference-laboratories/avian-influenza/workshops/2022/pavade.pdf [dostęp: 16 VI 2025].

Patogeny roślinne

Analogiczny potencjał destabilizacyjny wykazują patogeny roślinne, które mogą zostać użyte do zakłócenia produkcji zbóż, owoców i warzyw. Próba przemytu do USA zarodników grzyba *Fusarium graminearum* została potraktowana jako incydent o potencjalnym charakterze bioterrorystycznym. Inne patogeny wysokiego ryzyka to: bakteria *Xylella fastidiosa* infekująca drzewa oliwne i cytrusy w południowej Europie, szczep Ug99 rdzy źdźbłowej zbóż (wywoływanej przez grzyb *Puccinia graminis forma tritici*)[24] oraz bakteria *Ralstonia solanacearum* atakująca ziemniaki i pomidory[25]. Patogeny te zostały uwzględnione w narodowych strategiach bioobronnych wielu państw, w tym USA, Australii[26] i Niemiec[27].

Patogeny wektorowe

Kolejną kategorię stanowią patogeny wektorowe przenoszone przez takie organizmy, jak:

- komary (*Aedes sp.*, *Culex sp.*), które mogą przenosić wirusy dengi, Zika, żółtej febry, Zachodniego Nilu,
- kleszcze (*Ixodes spp.*), które mogą przenosić bakterię *Borrelia burgdorferi* (wywołującą boreliozę), wirusa kleszczowego zapalenia mózgu oraz bakterię *Anaplasma phagocytophilum* (wywołującą anaplazmozę u zwierząt i ludzi),

[24] *USDA Coordinated Approach to Address New Virulences in Wheat and Barley Stem Rust – Pgt-Ug99*, United States Department of Agriculture, 20 IX 2017 r., https://www.ars.usda.gov/ug99/ [dostęp: 16 VI 2025]; R.P. Singh i in., *The emergence of Ug99 races of the stem rust fungus is a threat to world wheat production*, „Annual Review of Phytopathology" 2011, nr 49, s. 465–481. https://doi.org/10.1146/annurev-phyto-072910-095423.

[25] *What is EPPO Global Database?*, https://gd.eppo.int/ [dostęp: 10 VI 2025].

[26] *National biodefense strategy and implementation plan for countering biological threats, enhancing pandemic preparedness, and achieving global health security*, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf [dostęp: 10 VI 2025]; *National Priority Plant Pests (2024)*, Australian Government. Department of Agriculture, Fisheries and Forestry, https://www.agriculture.gov.au/biosecurity-trade/pests-diseases-weeds/plant/national-priority-plant-pests/ [dostęp: 10 VI 2025].

[27] *Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy*, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf [dostęp: 11 VI 2025].

- muchówki (*Culicoides spp.*), które mogą przenosić wirusy wywołujące choroby: niebieskiego języka i afrykańskiego pomoru koni (ang. *African horse sickness*)[28].

Patogeny takie jak bakterie: *Francisella tularensis* (wywołuje tularemię), *Coxiella burnetii* (wywołuje gorączkę Q) i z rodzaju *Brucella spp.* (wywołują brucelozę) są uznawane przez Amerykańskie Centrum Kontroli i Zapobiegania Chorobom (U.S. Centers for Disease Control and Prevention, CDC) za potencjalne środki bioterrorystyczne ze względu na łatwość ich aerozolizacji i trudności z identyfikacją, co stanowi wyzwanie dla systemów nadzoru i reagowania[29].

[28] *Transmission of Zika Virus*, Centers for Disease Control and Prevention, 30 I 2025 r., https://www.cdc.gov/zika/php/transmission/index.html [dostęp: 10 IX 2025]; *Dengue*, World Health Organization, 21 VIII 2025 r., https://www.who.int/news-room/fact-sheets/detail/dengue-and-severe-dengue [dostęp: 10 IX 2025]; *Aedes aegypti – Factsheet for experts*, European Centre for Disease Prevention and Control, 2 I 2023 r., https://www.ecdc.europa.eu/en/disease-vectors/facts/mosquito-factsheets/aedes-aegypti [dostęp: 10 IX 2025]; *West Nile: Causes and How It Spreads*, Centers for Disease Control and Prevention, 19 VIII 2025 r., https://www.cdc.gov/west-nile-virus/causes/index.html [dostęp: 10 IX 2025]; *Tick-Borne Encephalitis*, Centers for Disease Control and Prevention, 23 IV 2025 r., https://www.cdc.gov/yellow-book/hcp/travel-associated-infections-diseases/tick-borne-encephalitis.html [dostęp: 10 IX 2025]; *Factsheet about tick-borne encephalitis (TBE)*, European Centre for Disease Prevention and Control, 22 I 2024 r., https://www.ecdc.europa.eu/en/tick-borne-encephalitis/facts/factsheet [dostęp: 10 IX 2025]; *How Lyme Disease Spreads*, Centers for Disease Control and Prevention, 24 IX 2024 r., https://www.cdc.gov/lyme/causes/index.html [dostęp: 10 IX 2025]; *About Anaplasmosis*, Centers for Disease Control and Prevention, 4 IX 2024 r., https://www.cdc.gov/anaplasmosis/about/index.html [dostęp: 10 IX 2025]; *Bluetongue*, World Organisation for Animal Health, https://www.woah.org/en/disease/bluetongue/ [dostęp: 10 IX 2025]; *Bluetongue*, U.S. Department of Agriculture, Animal and Plant Health Inspection Service, https://www.aphis.usda.gov/livestock-poultry-disease/cattle/bluetongue [dostęp: 10 IX 2025].

[29] *CDC Bioterrorism Agents*, https://biosecurity.fas.org/resource/documents/CDC_Bioterrorism_Agents.pdf [dostęp: 10 VI 2025]; *Emergency preparedness, resilience and response concept of operations*, UK Health Security Agency, 15 I 2025 r., https://www.gov.uk/government/publications/emergency-preparedness-resilience-and-response-concept-of-operations/emergency-preparedness-resilience-and-response-concept-of-operations [dostęp: 10 VI 2025]; D.T. Dennis i in., *Tularemia as a biological weapon: medical and public health management*, „The Journal of the American Medical Association" 2001, t. 285, nr 21, s. 2763–2773. https://doi.org/10.1001/JAMA.285.21.2763; *Bluetongue*, World Organisation for Animal Health…

Elementy środowiska naturalnego jako rezerwuary patogenów

Elementy środowiska naturalnego to istotne, choć często niedoceniane rezerwuary potencjalnych zagrożeń biologicznych mogących oddziaływać na sektor rolnictwa i produkcji żywności. W przeciwieństwie do klasycznych nośników środowisko wodno-glebowe może działać jako długoterminowy rezerwuar dla patogenów, umożliwiając ich przetrwanie i skryte rozprzestrzenianie[30]. W scenariuszach bioterrorystycznych woda może zostać skażona celowo, np. przez wprowadzenie patogenów do zbiorników wodnych lub systemów irygacyjnych. Trudność w wykryciu infekcji oraz jej opóźnione objawy sprawiają, że takie działania są szczególnym wyzwaniem dla systemów wczesnego ostrzegania, zwłaszcza w przypadku epifitoz roślinnych, takich jak zaraza ziemniaka (wywoływana przez lęgniowca *Phytophthora infestans*), mączniak prawdziwy zbóż (wywoływany przez grzyb *Blumeria graminis*), fuzarioza kukurydzy (wywoływana przez grzyby z rodzaju *Fusarium spp.*), bakteryjne zgnilizny drzew owocowych (wywoływane przez bakterię *Erwinia amylovora*), czyli chorób rozprzestrzeniających się masowo w populacjach roślin uprawnych i trudnych do wykrycia we wczesnej fazie ostrzegania[31]. Woda wykorzystywana do nawadniania, pojenia zwierząt czy mycia plonów bywa źródłem skażeń patogenami zoonotycznymi i pokarmowymi, takimi jak bakterie: *Escherichia coli*, *Listeria monocytogenes*, z rodzaju *Salmonella spp.* czy norowirusy[32]. Największe ryzyko dotyczy produktów spożywanych na surowo, np. warzyw liściastych i owoców jagodowych. Źródłem zanieczyszczeń mogą być m.in. odchody zwierzęce, wycieki z gospodarstw, ścieki z oczyszczalni, ale mogą one być również skutkiem działań bioterrorystycznych.

Gleba, kurz i aerozole mogą przenosić przetrwalniki bakterii, takich jak *Bacillus anthracis*, które pozostają aktywne przez dekady i mogą powodować wtórne ogniska zakażeń[33]. Negatywnym skutkom – zarówno pod względem epidemicznym, jak i ekonomicznym – sprzyja zdolność

[30] *Guidelines for drinking-water quality: fourth edition incorporating the first addendum*, Geneva 2017.

[31] *Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems*, Geneva 2002.

[32] *Foodborne Disease Outbreaks: Guidelines for Investigation and Control*, Geneva 2008.

[33] J.P. Wood i in., *Environmental Persistence of Bacillus anthracis and Bacillus subtilis Spores*, „PLoS ONE" 2015. https://doi.org/10.1371/journal.pone.0138083.

przetrwalników do długotrwałego przetrwania w środowisku[34] oraz ich potencjał do wywoływania nagłych, trudnych do opanowania epidemii[35]. Obciąża to systemy ochrony zdrowia, destabilizuje produkcję rolną i generuje znaczne straty finansowe[36].

Koncepcja One Health – zintegrowane ramy ochrony przed zagrożeniami bioterrorystycznymi

W ostatniej dekadzie doszło do wyraźnej zmiany w postrzeganiu zagrożeń biologicznych w Europie. Jeszcze przed 2020 r. czynniki ryzyka związane z sabotażem biologicznym były w dużej mierze bagatelizowane. W debacie publicznej dominowały kwestie zmian klimatycznych, bezpieczeństwa chemicznego czy cybernetycznego. Pandemia COVID-19 ujawniła, że skutki zagrożeń biologicznych mogą być równie daleko idące jak kryzysy gospodarcze czy klimatyczne i prowadzić do zakłóceń w łańcuchach dostaw, destabilizacji systemów zdrowotnych i poważnych strat społecznych[37]. W Europie zwrócono uwagę również na ryzyko związane z ogniskami chorób odzwierzęcych, jak np. SARS-CoV-2 na fermach norek w Danii i Holandii, a także na rozprzestrzenianie się ASF, które wymusiło wdrożenie zaostrzonych środków biobezpieczeństwa w rolnictwie[38]. Nie bez znaczenia było zdarzenie z 2018 r., które zostało zakwalifikowane jako zagrożenie CBRN. W Kolonii zatrzymano mężczyznę podejrzanego o wytwarzanie

[34] R. Sinclair i in., *Persistence of Category A Select Agents in the Environment*, „Applied and Environmental Microbiology" 2008, nr 74(3), s. 555–563. https://doi.org/10.1128/AEM.02167-07.

[35] S. Shadomy i in., *Anthrax Outbreaks: a warning for improved prevention, control and heightened awareness*, „Food and Agriculture Organization of the United Nations" 2016, t. 37, https://openknowledge.fao.org/server/api/core/bitstreams/59269d58-654e-4790-ac60-a9ea7edd3a99/content [dostęp: 16 IV 2025].

[36] S.A. Sarker i in., *An integrated model for anthrax-free zone development*, „Journal of Infection and Public Health" 2023, t. 16, s. 141–152. https://doi.org/10.1016/j.jiph.2023.10.024.

[37] *Lessons from the COVID-19 pandemic*, https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-lessons-learned-may-2023.pdf [dostęp: 16 IV 2025].

[38] C. Adlhoch i in., *Avian influenza overview February – May 2021*, „EFSA Journal" 2021, t. 19, nr 12. https://doi.org/10.2903/j.efsa.2021.6951; J.V. Baños i in., *Epidemiological analyses of African swine fever in the European Union*, „EFSA Journal" 2022, t. 20, nr 5. https://doi.org/10.2903/j.efsa.2022.7290.

broni biologicznej na bazie silnie trującej rycyny[39]. Problemem jest sporadyczne włączanie zagadnień z zakresu agroterroryzmu i przestępczości z wykorzystaniem czynników biologicznych w dokumenty dotyczące bezpieczeństwa państw UE, w tym Polski, mimo że organizacje międzynarodowe (WHO, WOAH, Interpol) zalecają przygotowanie planów reagowania na ataki wymierzone w systemy zaopatrzenia w żywność[40].

Odpowiedzią na te niedostatki stała się koncepcja One Health, która łączy zdrowie ludzi, zwierząt i środowiska z elementami bezpieczeństwa wewnętrznego i zakłada ścisłą współpracę sektorów ochrony zdrowia ludzi, zwierząt i środowiska[41]. Uzupełnieniem takiego podejścia są regulacje: Międzynarodowa konwencja ochrony roślin (ang. International Plant Protection Convention, IPPC)[42], Kodeks zdrowia zwierząt (ang. Terrestrial Animal Health Code)[43] oraz Konwencja o zakazie broni biologicznej i toksycznej (ang. Biological Weapons Convention, BWC)[44]. Ponadto w UE funkcjonują systemy wczesnego ostrzegania, m.in. Rapid Alert System for Food and Feed (RASFF), Early Warning and Response System (EWRS) i Animal Disease Notification System (ADNS), wspierające reagowanie na incydenty biologiczne[45]. W wymiarze globalnym przyjęto Quadripartite One Health Joint Plan of Action 2022–2026, wskazujący m.in. wspólne ramy nadzoru,

[39] *Update: Cologne couple in court over 'biological bomb plot'*, The Local Germany, 7 VI 2019 r., https://www.thelocal.de/20190607/tunisian-german-couple-in-court-over-ricin-attack-plot [dostęp: 16 IV 2025].

[40] *Animal agrocrime and agroterrorism*, Interpol, https://www.interpol.int/Crimes/Terrorism/Bioterrorism/Animal-agrocrime-and-agroterrorism [dostęp: 10 VI 2025]; A. Elbers, R. Knutsson, *Agroterrorism Targeting Livestock: A Review with a Focus on Early Detection Systems*, „Biosecurity and Bioterrorism: Biodefense Strategy, Practise, and Science" 2013. https://doi.org/10.1089/bsp.2012.0068; C. Gyles, *Agroterrorism*, https://pmc.ncbi.nlm.nih.gov/articles/PMC2839819/pdf/cvj_04_347.pdf [dostęp: 10 VI 2025].

[41] *One health joint plan of action 2022–2026: working together for the health of humans, animals, plants and the environment*, World Health Organization, https://www.who.int/publications/i/item/9789240059139 [dostęp: 10 VI 2025].

[42] *International Plant Protection Convention (1997)*, Rome 2024, https://openknowledge.fao.org/server/api/core/bitstreams/30cc2e83-a6fd-4e2c-a5ee-312093d5a307/content [dostęp: 10 VI 2025].

[43] *Terrestrial Animal Health Code*...

[44] *Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz ich zniszczeniu*.

[45] *Commission publishes 2023 Annual Report on food safety alerts and agri-food fraud investigations*, European Commission, 16 IX 2024 r., https://ec.europa.eu/newsroom/sante/items/847722/en [dostęp: 14 VI 2025].

przygotowania i reagowania. W UE program EU4Health (2021–2027) formalnie wpisał One Health w strukturę działań zdrowotnych i mechanizmy finansowania[46]. Na poziomie prawnym przełomowe znaczenie miało *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE*, które wzmacnia monitorowanie zagrożeń, wczesne ostrzeganie i koordynację na poziomie unijnym działań laboratoriów referencyjnych.

W Polsce implementacja One Health napotyka bariery, takie jak: brak kompleksowej strategii ustawowej i instytucjonalnej, rozproszenie baz danych, ograniczona interoperacyjność oraz różnice kompetencyjne między sektorami. Wyzwania te przekładają się na trudności w integracji pasywnego i aktywnego nadzoru (sieci sentinel, czyli sieci lekarzy weterynarii monitorujących sytuację w terenie i przekazujących informacje do instytucji centralnych), włączającego rolników, lekarzy weterynarii, laboratoria referencyjne i służby bezpieczeństwa biologicznego. Rekomendowane byłoby stworzenie centralnych struktur koordynacyjnych, które umożliwią skuteczne wdrażanie zintegrowanego podejścia oraz rozwój nowoczesnych systemów wczesnego ostrzegania i biomonitoringu.

Systemy biobezpieczeństwa w Polsce i wybranych państwach

Systemy biobezpieczeństwa pozwalają zidentyfikować najważniejsze czynniki mające wpływ na skuteczność zapobiegania zagrożeniom biologicznym w sektorze rolno-spożywczym, na wykrywanie tych zagrożeń i reagowanie na nie.

Polska

W Polsce funkcjonuje kilka kluczowych instytucji odpowiedzialnych za realizację zadań w zakresie biobezpieczeństwa, obejmujących ochronę zdrowia ludzi, zwierząt i roślin, bezpieczeństwo żywności oraz zapobieganie zagrożeniom biologicznym, w tym bioterroryzmowi. Są to:

[46] *One health joint plan of action (2022–2026): working together for the health of humans, animals, plants and the environment*, Rome 2022; *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/522 z dnia 24 marca 2021 r. w sprawie ustanowienia Programu działań Unii w dziedzinie zdrowia („Program UE dla zdrowia") na lata 2021–2027 oraz uchylenia rozporządzenia (UE) nr 282/2014*.

- Państwowa Inspekcja Sanitarna (PIS) działająca w ramach Ministerstwa Zdrowia na podstawie *Ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej*. Jej zadania obejmują m.in. nadzór nad zdrowiem publicznym, higieną środowiska, obiektów użyteczności publicznej, wody oraz bezpieczeństwem żywności pochodzenia niezwierzęcego;
- Inspekcja Weterynaryjna (IW) funkcjonująca na podstawie *Ustawy z dnia 29 stycznia 2004 r. o Inspekcji Weterynaryjnej*. Jest ona odpowiedzialna za ochronę zdrowia zwierząt, nadzór nad produktami pochodzenia zwierzęcego, zwalczanie chorób zakaźnych oraz kontrolę graniczną w zakresie przemieszczania zwierząt i produktów;
- Państwowa Inspekcja Ochrony Roślin i Nasiennictwa (PIORiN), której zadania wynikają z *Ustawy z dnia 18 grudnia 2003 r. o ochronie roślin* oraz *Ustawy z dnia 13 lutego 2020 r. o Państwowej Inspekcji Ochrony Roślin i Nasiennictwa*. Odpowiada ona za monitorowanie zdrowia roślin, zapobieganie rozprzestrzenianiu się agrofagów oraz kontrolę jakości materiału siewnego;
- Inspekcja Jakości Handlowej Artykułów Rolno-Spożywczych (IJHARS) działająca na podstawie *Ustawy z dnia 21 grudnia 2000 r. o jakości handlowej artykułów rolno-spożywczych*. Nadzoruje ona jakość handlową, znakowanie i zgodność produktów rolno-spożywczych z wymaganiami prawa;
- Europejski Urząd ds. Bezpieczeństwa Żywności, którego zadania w Polsce realizuje krajowy punkt kontaktowy zgodnie z *Rozporządzeniem (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiającym ogólne zasady i wymagania prawa żywnościowego*.

Współpraca tych instytucji stanowi fundament krajowego systemu biobezpieczeństwa, obejmującego monitorowanie i wykrywanie zagrożeń biologicznych oraz reagowanie na nie, w tym: celowe skażenia łańcucha żywnościowego, epidemie chorób zakaźnych ludzi, zwierząt i roślin. Dotyczy to także zjawisk o charakterze transgranicznym. Ich działania są zintegrowane w ramach krajowych oraz europejskich systemów wymiany informacji i wczesnego ostrzegania, takich jak RASFF, ADNS czy Trade Control and Expert System (TRACES), co umożliwia szybkie i skoordynowane reagowanie na sytuacje kryzysowe[47].

[47] *Rapid Alert System for Food and Feed (RASFF)*, European Commission, https://food.ec.europa.eu/safety/rasff_en [dostęp: 10 X 2025].

Nadzór nad biobezpieczeństwem w Polsce jest realizowany przez współdziałanie Głównego Inspektoratu Sanitarnego, Głównego Inspektoratu Weterynarii, PIORiN, IJHARS oraz innych instytucji administracji publicznej, których kompetencje obejmują ochronę zdrowia ludzi, zwierząt i środowiska. Pomimo obowiązujących regulacji prawnych, takich jak *Ustawa z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt*, a także *Ustawa z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia*, nadal brakuje w Polsce – o czym już wspomniano – zintegrowanej strategii, obejmującej koordynację działań w obszarze zdrowia ludzi, zwierząt i bezpieczeństwa żywności zgodnie z koncepcją One Health[48].

Ważną rolę w systemie ochrony biologicznej odgrywają laboratoria specjalizujące się w diagnostyce patogenów i monitoringu zagrożeń. W Polsce działa kilka laboratoriów 3 klasy bezpieczeństwa biologicznego (BSL, od ang. *biosafety level*)[49], m.in. w Państwowym Instytucie Weterynaryjnym – Państwowym Instytucie Badawczym (PIWet-PIB) w Puławach. Pełni ono funkcję krajowego laboratorium referencyjnego dla chorób zwierzęcych o znaczeniu epizootycznym i zoonotycznym[50]. Większość laboratoriów BSL-3, m.in. w Narodowym Instytucie Zdrowia Publicznego – Państwowym Zakładzie Higieny – Państwowym Instytucie Badawczym oraz w jednostkach akademickich (Uniwersytet Gdański i Gdański Uniwersytet Medyczny), koncentruje się na diagnostyce chorób ludzi i w związku z tym mają one jedynie pośredni wkład w bezpieczeństwo żywności. Równolegle funkcjonuje sieć laboratoriów wojskowych, w tym w Wojskowym Instytucie Higieny i Epidemiologii (WIHiE), który dysponuje laboratoriami BSL-3[51]. W strukturze WIHiE działa Ośrodek Diagnostyki i Zwalczania Zagrożeń Biologicznych (ODIZZB),

[48] K.M. Małgieś, *The Evolution of One Health concept – a European perspective*, „Review of European and Comparative Law" 2024, t. 57, nr 2. https://doi.org/10.31743/recl.17467; P. Kaczmarek i in., *The One Health Concept: A Holistic Approach to Protect Human and Environmental Health*, „Medycyna Pracy. Workers' Health and Safety" 2024, nr 5, s. 433–444.

[49] K. Chomiczewski, M. Bartoszcze, A. Michalski, *Budowanie nowoczesnego systemu obrony przed bronią biologiczną Sił Zbrojnych RP zgodnego z wymaganiami NATO*, „Lekarz Wojskowy" 2019, nr 1, s. 56–64.

[50] *Krajowe Laboratoria Referencyjne*, Państwowy Instytut Weterynaryjny – Państwowy Instytut Badawczy, https://www.piwet.pulawy.pl/krajowe-laboratoria-referencyjne/ [dostęp: 29 VII 2025].

[51] *Wojskowy Instytut Higieny i Epidemiologii im. Generała Karola Kaczkowskiego*, https://wihe.pl/wihe/o-nas [dostęp: 29 VII 2025].

zlokalizowany m.in. w Puławach[52]. Laboratoria wojskowe zajmują się diagnostyką czynników biologicznych o potencjale epidemicznym i bioterrorystycznym oraz wspierają reagowanie kryzysowe i współpracę międzynarodową[53]. Laboratoria BSL-3 to zasadniczy element krajowego systemu ochrony biologicznej – umożliwiają wczesne wykrywanie i analizę zagrożeń oraz wzmacniają zdolności państwa do reagowania na ataki bioterrorystyczne.

Pomimo istnienia powyższych struktur i mechanizmów nadal występuje luka w zdolnościach szybkiego wykrywania intencjonalnych skażeń żywności lub pasz i reagowania na nie, w odniesieniu zarówno do produkcji roślinnej, jak i zwierzęcej. Brakuje także laboratoriów klasy BSL-4, które umożliwiają bezpieczne badania nad najniebezpieczniejszymi patogenami. Stanowi to ograniczenie w przygotowaniu państwa na najpoważniejsze zagrożenia biologiczne, w tym potencjalne ataki bioterrorystyczne[54].

Niemcy

Niemcy posiadają zaawansowaną infrastrukturę biobezpieczeństwa, koordynowaną przez Federalne Ministerstwo Wyżywienia i Rolnictwa (Bundesministerium für Landwirtschaft, Ernährung und Heimat). Jednostki takie jak Instytut im. Friedricha Loefflera (Friedrich Loeffler Institut, FLI) oraz Instytut Roberta Kocha (Robert Koch Institute, RKI) odgrywają istotną rolę w nadzorze nad chorobami zakaźnymi, w ich badaniu i diagnostyce w odniesieniu – odpowiednio – do zwierząt i ludzi. Instytut Kocha prowadzi na szczeblu globalnym projekt RefBio. Wspiera w ten sposób międzynarodową sieć laboratoriów w ramach mechanizmu dochodzeniowego Sekretarza Generalnego ONZ w związku z domniemanym użyciem broni chemicznej i biologicznej lub toksycznej (United Nations Secretary-General's Mechanism to Investigate Suspected Use of Biological Weapons, UNSGM) oraz organizuje ćwiczenia, warsztaty i zapewnia transfer wiedzy[55].

---

[52] *Ośrodek Diagnostyki i Zwalczania Zagrożeń Biologicznych*, Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/zaklady/odizzb/organizacja [dostęp: 29 VII 2025].

[53] *Zadania badawczo-rozwojowe*, Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/wihe/zadania [dostęp: 29 VII 2025].

[54] K. Goniewicz i in., *Bioterrorism Preparedness and Response in Poland: Prevention, Surveillance and Mitigation Planning*, „Disaster Medicine and Public Health Preparedness" 2021, nr 15(6), s. 697–702.

[55] *RefBio – German Contribution to Strengthen the Reference Laboratories Bio in the UNSGM*, Robert Koch Institut, 10 V 2019 r., https://www.rki.de/EN/Institute/International-activities/Biosecurity-Programme/RefBio.html [dostęp: 16 VI 2025].

Niemcy dysponują także laboratoriami najwyższej, 4 klasy bezpieczeństwa biologicznego – BSL-4 (m.in. w Berlinie)[56]. System zarządzania kryzysowego opiera się na federalnym modelu organizacyjnym, z silną koordynacją działań między landami. Gotowość operacyjną państwa znacznie podnoszą regularne ćwiczenia symulacyjne pod kryptonimem LÜKEX. Podczas tych ćwiczeń testuje się różne scenariusze zarządzania kryzysowego, takie jak warianty pandemiczne czy kryzysy energetyczne, i systemy wczesnego ostrzegania[57]. Dla porównania, w Polsce takie ćwiczenia są prowadzone rzadziej i z ograniczonym komponentem agro-bio. Wzmacnia to postulat, aby uwzględniać w nich odrębny moduł rolny.

Francja

Francja integruje działania sanitarne, weterynaryjne i środowiskowe za pośrednictwem Krajowej Agencji ds. Bezpieczeństwa Żywności, Środowiska i Pracy (Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail, ANSES). W Lyonie funkcjonuje referencyjne laboratorium klasy BSL-4 – Laboratoire P4 Inserm Jean Mérieux[58]. Pomimo istnienia silnej bazy instytucjonalnej w raportach wskazuje się na trudności we współpracy pomiędzy służbami oraz na potrzebę lepszej integracji danych międzysektorowych[59].

Włochy

We Włoszech system biobezpieczeństwa jest koordynowany przez Ministerstwo Zdrowia i regionalne służby weterynaryjne. Sieć Instytutów

[56] *The Biosafety Level-4 Laboratoty at RKI*, Robet Koch Institut, 31 I 2024 r., https://www.rki.de/EN/Topics/Research-and-data/Specialised-laboratories/BSL-4-laboratory/bsl-4-laboratory-at-the-robert-koch-institute-node.html [dostęp: 16 VI 2025]; *FLI tests mobile One Health laboratory for diagnosing highly pathogenic pathogens*, Friedrich Loeffler Institut, 13 VI 2025 r., https://www.fli.de/en/press/press-releases/press-singleview/fli-tests-mobile-one-health-laboratory-for-diagnosing-highly-pathogenic-pathogens/ [dostęp: 20 VI 2025].

[57] *Germany*, European Commission, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-disaster-management-system/germany_en?utm [dostęp: 15 XII 2025]; *Historie der LÜKEX Krisenmanagementübungen*, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Historie/historie_node.html [dostęp: 15 XII 2025].

[58] *ANSES Laboratories*, ANSES, 15 II 2013 r., https://www.anses.fr/en/content/anses-laboratories [dostęp: 20 VI 2025].

[59] T. Lefrançois i in., *One Health approach at the heart of the French Committee for monitoring and anticipating health risks*, „Natura Communication" 2023, nr 14, s. 9. https://doi.org/10.1038/s41467-023-43089-2.

Zooprofilaktycznych (Istituti Zooprofilattici Sperimentali) pełni funkcję laboratoriów referencyjnych ds. chorób zwierząt. W Rzymie, w ramach Krajowego Instytutu Chorób Zakaźnych (Istituto Nazionale per le Malattie Infettive), działa laboratorium klasy BSL-4[60]. Wyzwaniami w reagowaniu na zagrożenia biologiczne są m.in. brak centralnej platformy do integracji danych oraz różnice pomiędzy regionami w zdolnościach do reagowania na te zagrożenia[61].

Wielka Brytania

Epidemia FMD z 2001 r. stała się punktem zwrotnym w polityce biobezpieczeństwa Wielkiej Brytanii. Po kryzysie wprowadzono rozbudowany system zarządzania ryzykiem biologicznym, obejmujący prewencję i szybkie reagowanie. Czołową instytucją jest Animal and Plant Health Agency, która jest odpowiedzialna za nadzór i diagnostykę (zarówno rutynową, jak i w sytuacjach kryzysowych), a także za koordynację działań w razie zagrożeń[62]. Agencja współpracuje z Instytutem Pirbrighta (The Pirbright Institute), który prowadzi badania nad wirusami wywołującymi choroby u zwierząt[63] i posiada laboratorium SAPO 4 (Specified Animal Pathogens Order class 4), pełniące funkcję referencyjną dla FAO, WOAH i UE[64]. Instytut prowadzi badania, szkolenia oraz opracowuje szczepionki.

Rządowy Departament Środowiska, Żywności i Spraw Wsi (Department for Environment, Food and Rural Affairs, DEFRA) oraz Brytyjska Agencja Bezpieczeństwa Zdrowotnego (UK Health Security Agency, UKHSA) opracowały zintegrowane plany zarządzania zagrożeniami zoonotycznymi i fitopatologicznymi w ramach podejścia One Health[65]. Stanowią one podstawę

[60] *INMI Lazzaro Spallanzani IRCCS, Istituto Nazionale Malettie Infettive,* https://www.inmi.it/ [dostęp: 20 VI 2025].

[61] A. Perella, M. Bisogno, *The strength and resilience of Italy's health data system,* „The Lancet Regional Health" 2025, t. 51. https://doi.org/10.1016/j.lanepe.2025.101255.

[62] *Animal and Plant Health Agency framework document,* Department for Environment, Food & Rural Affairs, 7 III 2024 r., https://www.gov.uk/government/publications/animal-and-plant-health-agency-framework-document/animal-and-plant-health-agency-framework-document [dostęp: 20 VI 2025].

[63] *Our science,* The Pirbright Institute, https://www.pirbright.ac.uk/our-science [dostęp: 20 VI 2025].

[64] *Reference Laboratories,* The Pirbright Institute, https://www.pirbright.ac.uk/facilities-and-resources/reference-laboratories [dostęp: 17 VI 2025].

[65] *UKHSA Strategic Plan 2023 to 2026,* https://assets.publishing.service.gov.uk/media/650d530e52e73c00139426c1/UKHSA_3_year_strategy.pdf [dostęp: 18 VI 2025].

krajowych planów gotowości na wypadek pojawienia się chorób niewystępujących endemicznie[66]. Po 2001 r. rozwinięto współpracę między administracją, służbami weterynaryjnymi, laboratoriami referencyjnymi i partnerami międzynarodowymi. Ćwiczenia symulacyjne oraz raporty, przygotowywane m.in. przez Anderson Report[67] i National Audit Office[68], przyczyniły się do wzmocnienia systemów analitycznych i wczesnego ostrzegania. W strategii z 2023 r. dotyczącej biobezpieczeństwa określono ramy ochrony przed zagrożeniami naturalnymi, przypadkowymi i celowymi, w tym bioterrorystycznymi[69]. Opiera się ona na czterech filarach: zrozumieniu (ang. *understand*), przeciwdziałaniu (ang. *prevent*), wykryciu (ang. *detect*) i odpowiedzi (ang. *respond*), wspieranych przez władze państwowe, rozwój naukowo-technologiczny i współpracę międzynarodową. Strategia ta zakłada osiągnięcie pełnej gotowości do 2030 r. oraz utworzenie Narodowego Centrum Biobezpieczeństwa (National Biosecurity Centre), z budżetem w wysokości ok. 1 mld funtów. Ma ono osiągnąć pełną zdolność do działania w latach 2033–2034[70].

Instytucje badawcze i narzędzia informacyjne w UE

Państwa UE korzystają ze wspólnych sieci nadzoru, takich jak RASFF, TRACES i EWRS, które wspierają wymianę informacji i koordynację działań[71]. W Niemczech i Francji funkcjonują sprawne struktury instytucjonalne, m.in. FLI i ANSES[72]. W Polsce i we Włoszech brakuje jednolitego systemu

[66] *Contingency plan for exotic notifiable diseases of animals in England*, https://assets.publishing.service.gov.uk/media/691c80cd84a267da57d706da/Defra-contingency-plan-exotic-notifiable-diseases-animals-England.pdf [dostęp: 18 VI 2025].

[67] I. Anderson, *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry Report*, London 2002.

[68] *The 2001 Outbreak of Foot and Mouth Disease*, London 2002.

[69] *UK Biological Security Strategy*, Cabinet Office, 12 VI 2023 r., https://www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html [dostęp: 10 VI 2025].

[70] *UK pledges 1 billion pounds to build new biosecurity centre*, Reuters, 24 VI 2025 r., https://www.reuters.com/business/healthcare-pharmaceuticals/uk-pledges-1-billion-pounds-build-new-biosecurity-centre-2025-06-23 [dostęp: 8 VIII 2025]; *Dowden: world-class crisis capabilities deployed to defeat biological threats of tomorrow*, 12 VI 2023 r., https://www.gov.uk/government/news/dowden-world-class-crisis-capabilities-deployed-to-defeat-biological-threats-of-tomorrow [dostęp: 8 VIII 2025].

[71] *One Health: a joint framework for action published by five EU agencies*, European Centre for Disease Prevention and Control, 7 V 2024 r., https://www.ecdc.europa.eu/en/news-events/one-health-joint-framework-action-published-five-eu-agencies [dostęp: 10 VI 2025].

[72] *FLI tests mobile One Health laboratory...*; *ANSES Laboratories...*

koordynacyjnego łączącego sektor weterynaryjny, fitosanitarny i zdrowia publicznego. Polska ma Krajowy Plan Zarządzania Kryzysowego, ale jego ramowy charakter nie zapewnia operacyjnej integracji międzysektorowej. Istotnym ograniczeniem pozostaje brak laboratoriów BSL-4, które są w Niemczech, Francji, USA i Wielkiej Brytanii[73]. W Wielkiej Brytanii jest widoczna skuteczna współpraca między sektorami rolnictwa, zdrowia publicznego, obronności i środowiska, wsparta strategicznymi regulacjami prawnymi[74].

W UE pomimo istnienia narzędzi wspólnotowych wdrażanie podejścia One Health przebiega nierównomiernie[75]. W analizie przedstawionej w publikacji *Countering Agricultural Bioterrorism* podkreślono, że zagrożenia bioterrorystyczne są nadal niedoszacowane w politykach bezpieczeństwa państw UE[76]. Brakuje kompleksowych scenariuszy reagowania, zwłaszcza dotyczących odpowiedzi na akt agroterroryzmu, mimo uznania sektora żywnościowego za element infrastruktury krytycznej.

Rola kluczowych interesariuszy w systemie wczesnego ostrzegania: rolnicy, lekarze weterynarii i władze samorządowe

Skuteczne wzmacnianie systemu biobezpieczeństwa w sektorze rolno-spożywczym nie jest możliwe bez aktywnego zaangażowania rolników, lekarzy weterynarii oraz władz samorządowych. To właśnie te grupy stanowią pierwszą linię wykrywania niepokojących symptomów oraz odgrywają decydującą rolę we wczesnym reagowaniu na incydenty o charakterze biologicznym.

Pierwszym ogniwem w systemie wczesnego powiadamiania i ostrzegania są rolnicy. Ich codzienny kontakt ze zwierzętami i roślinami pozwala na szybkie wychwycenie symptomów ASF, FMD czy infekcji roślin wywoływanej przez bakterię *Xylella fastidiosa*[77]. Ważne, aby rolnicy znali objawy

[73] *Laboratory Biosafety Manual…*

[74] *UK Biological Security Strategy…*

[75] *One Health: a joint framework for action published…*

[76] *Countering Agricultural Bioterrorism*, Washington 2022. https://doi.org/10.17226/10505.

[77] C. Guinat i in., *English Pig Farmers' Knowledge and Behaviour towards African Swine Fever Suspicion and Reporting*, „PLoS ONE" 2016, nr 9. https://doi.org/10.1371/JOURNAL.PONE.0161431; S. Costard i in., *Epidemiology of African swine fever virus*, „Virus Research" 2013, t. 173, nr 1, s. 191–197. https://doi.org/10.1016/J.VIRUSRES.2012.10.030.

oraz procedury zgłaszania, a także mieli zaufanie do instytucji państwowych. To pozwala skrócić czas reakcji. Niestety, niski poziom świadomości, ograniczony dostęp do aktualnych informacji oraz obawa przed konsekwencjami administracyjnymi często powodują opóźnienia we wdrażaniu procedur[78]. Brakuje także formalnych mechanizmów zachęcających do szybkiego raportowania, np. wsparcia finansowego czy ochrony prawnej zgłaszających.

Lekarze weterynarii stanowią element łączący lokalne społeczności rolnicze z systemem monitorowania diagnostyki zagrożeń zoonotycznych. Ich zadania obejmują nie tylko rozpoznawanie epizootii, lecz także edukację rolników, wczesne ostrzeganie i przekazywanie danych do służb weterynaryjnych oraz laboratoriów referencyjnych[79]. W wielu krajach UE funkcjonuje nadzór typu sentinel[80].

W Polsce podobne rozwiązania dopiero się rozwijają i są wdrażane głównie w ramach Państwowej Inspekcji Weterynaryjnej, która koordynuje monitoring chorób zakaźnych zwierząt na podstawie krajowych oraz unijnych programów nadzoru. Ważną rolę odgrywa cyfryzacja i integracja systemów, takich jak IRZplus (Identyfikacja i Rejestracja Zwierząt), TRACES oraz krajowe bazy danych o chorobach zwierząt. Coraz większe znaczenie mają również platformy wymiany danych i raportowania do Głównego Lekarza Weterynarii oraz do europejskich instytucji, m.in. EFSA i systemu RASFF. Nadal jednak istnieją ograniczenia w zakresie pełnej interoperacyjności systemów oraz włączenia lekarzy prowadzących prywatną praktykę do sieci

[78] M.C. Gates, L. Earl, G. Enticott, *Factors influencing the performance of voluntary farmer disease reporting in passive surveillance systems: A scoping review*, „Preventive Veterinary Medicine" 2021, t. 196, s. 1–2, 5–7. https://doi.org/10.1016/j.prevetmed.2021.105487; G. Enticott, L. Earl, M.C. Gates, *A systematic review of social research data collection methods used to investigate voluntary animal disease reporting behaviour*, „Transboundary and Emerging Diseases" 2021, nr 5, s. 2573–2587. https://doi.org/10.1111/tbed.14407; J.C. Mariner i in., *Rift Valley fever action framework*, Italy 2022. https://doi.org/10.4060/cb8653en.

[79] O.A. Hassan, K. de Balogh, A.S. Winkler, *One Health early warning and response system for zoonotic diseases outbreaks: Emphasis on the involvement of grassroots actors*, „Veterinary Medicine and Science" 2023, t. 9, nr 4, s. 1881–1889. https://doi.org/10.1002/vms3.1135.

[80] C. Saegerman i in., *Clinical Sentinel Surveillance of Equine West Nile Fever, Spain*, „Transboundary and Emerging Diseases" 2014, t. 63, nr 2, s. 161–164. https://doi.org/10.1111/tbed.12243; C. Plaza-Rodriguez i in., *Wildlife as Sentinels of Antimicrobial Resistance in Germany?*, „Frontiers in Veterinary Science" 2021, t. 7, s. 1–11. https://doi.org/10.3389/fvets.2020.627821; R. Özçelik i in., *Evaluating 5.5 Years of Equinella: A Veterinary-Based Voluntary Infectious Disease Surveillance System of Equines in Switzerland*, „Frontiers in Veterinary Science" 2020, t. 7, s. 1–4. https://doi.org/10.3389/fvets.2020.00327.

szybkiego ostrzegania, co ogranicza skuteczność nadzoru sentinelowego w porównaniu z rozwiązaniami stosowanymi np. w Niemczech czy Francji[81].

Władze lokalne – wojewódzkie, powiatowe i gminne – odgrywają najważniejszą rolę w praktycznym wdrażaniu zasad biobezpieczeństwa oraz systemów reagowania na zagrożenia biologiczne, współpracując z administracją centralną i operatorami infrastruktury krytycznej. Pomimo dostępności narzędzi analitycznych, takich jak matryce ryzyka, modele podatności czy scenariusze predykcyjne, ich efektywność w praktyce pozostaje ograniczona ze względu na niski poziom świadomości i brak konsekwentnego wdrażania wśród podmiotów odpowiedzialnych.

W Polsce Krajowy Plan Zarządzania Kryzysowego oraz Krajowy System Wykrywania Skażeń i Alarmowania formalnie przewidują mechanizmy oceny i monitorowania zagrożeń, w tym biologicznych, jednak ich skuteczność jest warunkowana nie tylko dostępnością narzędzi, lecz także właściwą interpretacją i wykorzystaniem przez administrację i operatorów infrastruktury krytycznej.

Rola lokalnych instytucji powinna być wzmacniana przez systematyczne szkolenia, budowanie zaufania oraz zapewnianie dostępu do narzędzi cyfrowych (np. platform do e-learningu, aplikacji wspierających monitoring i raportowanie). Stałe programy edukacyjne, prowadzone we współpracy z izbami rolniczymi, służbami weterynaryjnymi i instytutami badawczymi, powinny obejmować nie tylko rozpoznawanie objawów chorób zakaźnych, lecz także procedury reagowania i współpracy międzyinstytucjonalnej. Dobrym przykładem są programy edukacyjne realizowane w Niemczech i Holandii, w których lokalni producenci żywności uczestniczą w symulacjach sytuacji kryzysowych[82].

W kontekście Polski opisane działania mają charakter rekomendacji, a nie obowiązujących programów na skalę krajową czy wojewódzką. Ich celem byłaby adaptacja dobrych praktyk z poziomu UE, np. inicjatyw EFSA i Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób

[81] *Zwalczanie i monitoring wybranych chorób zakaźnych zwierząt*, Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/nadzor-weterynaryjny/programy-zwalczaniamonitorowania-chorob-zakaznych-zwierzat [dostęp: 1 IX 2025]; *European Commission*, https://ec.europa.eu [dostęp: 1 IX 2025]; *Aplikacja IRZplus*, Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/systemy-informatyczne/cbd-irzgo [dostęp: 1 IX 2025]; *EFSA*, https://www.efsa.europa.eu [dostęp: 1 IX 2025]; *Rapid Alert System for Food and Feed (RASFF)*...

[82] *Chemical and biological deliberate events*, World Health Organization, https://openwho.org/emergencymgmt/501116/Chemical+and+biological+deliberate+events [dostęp: 1 IX 2025].

(European Centre for Disease Prevention and Control, ECDC), w ramach bezpieczeństwa żywności oraz zdrowia publicznego, w tym mechanizmów edukacyjnych takich jak Better Training for Safer Food[83]. Rekomendowane rozwiązania powinny być wdrażane w strukturach krajowych i regionalnych przez wojewódzkie i powiatowe zespoły zarządzania kryzysowego, służby weterynaryjne oraz izby rolnicze i w ścisłej integracji z lokalnymi planami reagowania[84]. Takie zintegrowane działania powinny być uzupełniane regularnymi ćwiczeniami symulacyjnymi[85], które pozwalają na praktyczne sprawdzenie skuteczności wdrożonych procedur oraz koordynacji międzysektorowej.

Odpowiednio rozwinięta infrastruktura logistyczna ma decydujące znaczenie dla reagowania na zagrożenia biologiczne, jednak w wielu krajach pozostaje ona niewystarczająca. Francja dysponuje zaawansowanymi łańcuchami chłodniczymi i rezerwami szczepionek, co skraca czas reakcji[86]. Polska posiada nowoczesne centra logistyczne, takie jak magazyny NewCold, oraz systemowe rezerwy szczepionek i wyrobów diagnostycznych utrzymywane przez Rządową Agencję Rezerw Strategicznych[87], jednak ich zakres i dostępność – zwłaszcza na poziomie regionalnym – są

[83] *Empowering food safety through enhanced training,* European Commission, 9 IX 2024 r., https://ec.europa.eu/newsroom/btsf/items/846699/en [dostęp: 1 IX 2025].

[84] Tamże; *Breaking language barriers: translation of training materials on food safety regulations now available,* European Commission, 25 III 2025 r., https://hadea.ec.europa.eu/news/breaking-language-barriers-translation-training-materials-food-safety-regulations-now-available-2025-03-25_en [dostęp: 1 IX 2025]; *HaDEA launches third call for tenders under BTSF,* European Commission, 5 VIII 2022 r., https://hadea.ec.europa.eu/news/hadea-launches-third-call-tenders-under-btsf-2022-08-05_en?utm [dostęp: 1 IX 2025]; *Digitalising the EU agricultural sector,* European Commission, https://digital-strategy.ec.europa.eu/en/policies/digitalisation-agriculture [dostęp: 1 IX 2025]; *Transparency solutions for transforming the food system,* EU CAP Network, https://eu-cap-network.ec.europa.eu/projects/transparency-solutions-transforming-food-system_en [dostęp: 1 IX 2025].

[85] *Field simulation trainings to support emergency preparedness,* World Organisation for Animal Health, 13 IV 2023 r., https://www.woah.org/en/article/field-simulation-trainings-to-support-emergency-preparedness/ [dostęp: 10 VI 2025].

[86] Y. He, M. Liu, *Research on sustainable development of agricultural product cold chain logistics under public safety emergencies,* „Frontiers in Sustainable Food Systems" 2023, t. 7. https://doi.org/10.3389/fsufs.2023.1174221; A. Spitalleri i in., *BioTrak: A Blockchain-based Platform for Food Chain Logistics Traceability,* International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia 2023, s. 105–110. https://doi.org/10.1109/ICCNS58795.2023.10193341.

[87] *Rezerwy medyczne,* Rządowa Agencja Rezerw Strategicznych, https://www.gov.pl/web/rars/rezerwy-medyczne [dostęp: 30 IX 2025].

ograniczone. Mimo odporności sektora chłodniczego podczas kryzysów konieczne są dalsze inwestycje w cyfryzację, interoperacyjność i rezerwy strategiczne[88].

Podsumowanie i wnioski

Przez wiele lat w politykach bezpieczeństwa omawianych państw było widoczne przekonanie, że prawdopodobieństwo wystąpienia poważnych incydentów biologicznych jest niskie. Założenie to prowadziło do niedoszacowywania ryzyka, ograniczania inwestycji w działania profilaktyczne oraz braku procedur reagowania – szczególnie w sektorze rolno-spożywczym, co skutkowało obniżeniem gotowości operacyjnej. Niedostatek szkoleń systemowych, niewielkie nakłady na profilaktykę oraz pomijanie scenariuszy bioterroryzmu w lokalnych planach zarządzania kryzysowego pogłębiały rozbieżność między zapisami strategii a rzeczywistą zdolnością instytucji do skutecznego działania[89].

W ostatniej dekadzie nastąpiła istotna zmiana percepcji zagrożeń biologicznych. Pandemia COVID-19 dowiodła, że kryzysy biologiczne mogą generować skutki porównywalne z kryzysami gospodarczymi czy klimatycznymi, prowadząc do poważnych zakłóceń łańcuchów dostaw, obciążeń systemów zdrowotnych oraz strat społecznych[90]. Więcej uwagi zaczęto poświęcać również zagrożeniom związanym z chorobami odzwierzęcymi, takimi jak ASF, SARS-CoV-2, czy incydentom klasyfikowanym jako zagrożenie CBRN[91]. Pomimo istnienia rekomendacji WHO, WOAH i Interpolu dotyczących potrzeby przygotowania planów reagowania na intencjonalne skażenie systemów żywnościowych, zagadnienia związane ze zjawiskiem agroterroryzmu nadal są marginesowo traktowane w dokumentach strategicznych

[88] *Poland Cold Chain Logistics et 2025–2034 – Size, Share, Trends, Analysis & Forecast 2025–2034*, MarkWide Research, https://markwideresearch.com/poland-cold-chain-logistics-market/ [dostęp: 18 VI 2025].

[89] *Deliberate events*, World Health Organization, 2 IV 2024 r., https://www.who.int/news-room/fact-sheets/detail/deliberate-events [dostęp: 18 VI 2025].

[90] *Lessons from the COVID-19 pandemic*...

[91] F. Flade, *The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror*, https://ctc.westpoint.edu/june-2018-cologne-ricin-plot-new-threshold-jihadi-bio-terror/ [dostęp: 16 IX 2025].

państw UE, w tym Polski[92]. Podejście One Health ma na celu wypełnienie tej luki przez integrację zdrowia ludzi, zwierząt i środowiska w jeden spójny system zarządzania zagrożeniami biologicznymi. Wdrażanie tej koncepcji nie jest jednak jednolite i napotyka duże bariery. Utrudnia to integrację nadzoru pasywnego i aktywnego oraz włączanie rolników, lekarzy weterynarii, laboratoriów i władz lokalnych do sieci wczesnego ostrzegania. Przykłady z Niemiec i Holandii pokazują, że skuteczne wdrażanie One Health wymaga nie tylko narzędzi prawnych, lecz także systemowych szkoleń, budowania zaufania oraz cyklicznych ćwiczeń symulacyjnych, w które włącza się lokalnych producentów żywności[93]. Równolegle konieczne jest wzmacnianie infrastruktury logistycznej, w tym łańcuchów chłodniczych, rezerw szczepionek, materiałów diagnostycznych, a także dalsze inwestowanie w interoperacyjność, cyfryzację i zarządzanie rezerwami strategicznymi.

Ze względu na rosnącą złożoność zagrożeń zasadne jest rozważenie utworzenia wyspecjalizowanej unijnej instytucji ds. agrobiobezpieczeństwa, analogicznej do ECDC[94], lecz skoncentrowanej na zagrożeniach dla sektora rolno-spożywczego. Instytucja taka mogłaby prowadzić badania strategiczne, analizy ryzyka, rozwijać systemy wczesnego ostrzegania oraz koordynować działania służb bezpieczeństwa żywności, weterynaryjnych, sanitarnych, laboratoriów referencyjnych i ośrodków naukowych. Istotna byłaby w tym kontekście ścisła współpraca z Dyrekcją Generalną ds. Zdrowia i Bezpieczeństwa Żywności (Directorate-General for Health & Food Safety)[95], EFSA oraz systemem RASFF. Ważne jest także prowadzenie badań jakościowych i ilościowych wśród interesariuszy – rolników, lekarzy weterynarii, laboratoriów, służb sanitarnych i administracji – pozwalających identyfikować realne bariery operacyjne we wdrażaniu procedur biobezpieczeństwa oraz oceniać gotowość do współpracy międzyinstytucjonalnej. Równolegle należy prowadzić analizy systemowe, w tym mapowanie procesów decyzyjnych i komunikacyjnych, pozwalające wykrywać luki w koordynacji i interoperacyjności. Zgromadzony materiał badawczy

[92] *Animal agrocrime and agroterrorism...*; *Agro-crime and agro-terrorism,* World Organisation for Animal Health, https://www.woah.org/en/what-we-offer/emergency-preparedness/agro-crime-and-agro-terrorism/ [dostęp: 16 IX 2025].

[93] *Field simulation trainings to support emergency preparedness...*

[94] *What We Do,* European Centre for Disease Prevention and Control, https://www.ecdc.europa.eu/en/about-ecdc/what-we-do [dostęp: 30 IX 2025].

[95] *Health and Food Safety*, European Commission, https://commission.europa.eu/about/departments-and-executive-agencies/health-and-food-safety_en [dostęp: 15 XII 2025].

stanowiłby podstawę do utworzenia instytucji efektywnej organizacyjnie i społecznie osadzonej – odpowiadającej na realne potrzeby podmiotów działających na pierwszej linii oraz wzmacniającej zdolność UE i jej państw członkowskich do skutecznego reagowania na zagrożenia biologiczne.

Podsumowując, wzmocnienie odporności na ataki bioterrorystyczne wymaga:

- pełnej integracji działań w modelu One Health,
- rozwinięcia interoperacyjnych systemów nadzoru i laboratoriów,
- systematycznego organizowania szkoleń i ćwiczeń,
- włączenia lokalnych aktorów do nadzoru sentinelowego,
- budowy wydolnej logistyki w sytuacjach kryzysowych,
- uwzględnienia sektora rolno-spożywczego w planach bezpieczeństwa narodowego i europejskiego.

Realizacja tych postulatów zwiększyłaby skuteczność reagowania na zagrożenia biologiczne – zarówno naturalne, jak i intencjonalne – oraz wzmocniłaby odporność państw na zagrożenia hybrydowe.

Bibliografia

Adlhoch C., Fusaro A., Gonzales J.L., Kuiken T., Marangon S., Niqueux E., Staubach Ch., Terregino C., Aznar I., Guajardo I.M., Lima E., Baldinelli F., *Avian influenza overview February – May 2021*, „EFSA Journal" 2021, t. 19, nr 12. https://doi.org/10.2903/j.efsa.2021.6951.

Anderson I., *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry Report*, London 2002.

Baños J.V., Boklund A., Gogin A., Gortázar Ch., Guberti V., Helyes G., Kantere M., Korytarova D., Linden A., Masiulis M., Miteva A., Neghirla I., Oļševskis E., Ostojic S., Petr S., Staubach Ch., Thulke H.H., Viltrop A., Wozniakowski G., Broglia A., Cortiñas J.A., Dhollander S., Mur L., Papanikolaou A., Van der Stede Y., Zancanaro G., Ståhl K., *Epidemiological analyses of African swine fever in the European Union*, „EFSA Journal" 2022, t. 20, nr 5. https://doi.org/10.2903/j.efsa.2022.7290.

Chomiczewski K., Bartoszcze M., Michalski A., *Budowanie nowoczesnego systemu obrony przed bronią biologiczną Sił Zbrojnych RP zgodnego z wymaganiami NATO*, „Lekarz Wojskowy" 2019, nr 1, s. 56–64.

Costard S., Mur L., Lubroth J., Sanchez-Vizcaino J.M., Pfeiffer D.U., *Epidemiology of African swine fever virus*, „Virus Research" 2013, t. 173, nr 1, s. 191–197. https://doi.org/10.1016/J.VIRUSRES.2012.10.030.

Countering Agricultural Bioterrorism, Washington 2022. https://doi.org/10.17226/10505.

Dennis D.T., Inglesby T.V., Henderson D.A., Bartlett J.G., Ascher M.S., Eitzen E., Fine A.D., Friedlander A.M., Hauer J., Layton M., Lillibridge S.R., McDade J.E., Osterholm M.T., O'Toole T., Parker G., Trish M.P., Russell P.K., Tonat K., *Tularemia as a biological weapon: medical and public health management*, „The Journal of the American Medical Association" 2001, t. 285, nr 21, s. 2763–2773. https://doi.org/10.1001/JAMA.285.21.2763.

Dudley J.P., Woodford M.H., *Bioweapons, bioterrorism and biodiversity: potential impacts of biological weapons attacks on agricultural and biological diversity*, „Revue Scientifique et Technique" 2002, nr 21(1), s. 125–137. http://dx.doi.org/10.20506/rst.21.1.1328.

Elbers A., Knutsson R., *Agroterrorism Targeting Livestock: A Review with a Focus on Early Detection Systems*, „Biosecurity and Bioterrorism: Biodefense Strategy, Practise, and Science" 2013. https://doi.org/10.1089/bsp.2012.0068.

Enticott G., Earl L., Gates M.C., *A systematic review of social research data collection methods used to investigate voluntary animal disease reporting behaviour*, „Transboundary and Emerging Diseases" 2021, nr 5, s. 2573–2587. https://doi.org/10.1111/tbed.14407.

Foodborne Disease Outbreaks: Guidelines for Investigation and Control, Geneva 2008.

Garnett P., Doherty B., Heron T., *Vulnerability of the United Kingdom's food supply chains exposed by COVID-19*, „Nature Food" 2020, nr 1, s. 315–318. https://doi.org/10.1038/s43016-020-0097-7.

Gates M.C., Earl L., Enticott G., *Factors influencing the performance of voluntary farmer disease reporting in passive surveillance systems: A scoping review*, „Preventive Veterinary Medicine" 2021, t. 196. https://doi.org/10.1016/j.prevetmed.2021.105487.

Goniewicz K., Osiak B., Pawłowski W., Czerski R., Burkle F.M., Lasota D., Goniewicz M., *Bioterrorism Preparedness and Response in Poland: Prevention, Surveillance and Mitigation Planning*, „Disaster Medicine and Public Health Preparedness" 2021, nr 15(6), s. 697–702.

Guidelines for drinking-water quality: fourth edition incorporating the first addendum, Geneva 2017.

Guinat C., Wall B., Dixon L., Pfeiffer D.U., *English Pig Farmers' Knowledge and Behaviour towards African Swine Fever Suspicion and Reporting*, „PLoS ONE" 2016, nr 9. https://doi.org/10.1371/JOURNAL.PONE.0161431.

Hassan O.A., Balogh K. de, Winkler A.S., *One Health early warning and response system for zoonotic diseases outbreaks: Emphasis on the involvement of grassroots actors*, „Veterinary Medicine and Science" 2023, t. 9, nr 4, s. 1881–1889. https://doi.org/10.1002/vms3.1135.

He Y., Liu M., *Research on sustainable development of agricultural product cold chain logistics under public safety emergencies*, „Frontiers in Sustainable Food Systems" 2023, t. 7. https://doi.org/10.3389/fsufs.2023.1174221.

Ivanov D., Dolgui A., *Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak*, „International Journal of Production Research" 2020, t. 58, nr 10, s. 2904–2915. https://doi.org/10.1080/00207543.2020.1750727.

Kaczmarek P., Wiszniewska M., Słomka S., Walusiak-Skorupa J., *The One Health Concept: A Holistic Approach to Protect Human and Environmental Health*, „Medycyna Pracy. Workers' Health and Safety" 2024, nr 5, s. 433–444.

Lefrançois T., Lina B., Autran B., Caille Y., Carrat F., Cauchemez S., Contenti J., Degrées du Loû A., Druet-Faivre L., Fontenille D., Giraudoux P., Heard M., De Lamballerie X., Lefrançois T., Le Grand R., Lescure F.X., Lina B., Loyer V., Malvy D., Offerle C., Raude J., Saint-Lary O., Slama R., *One Health approach at the heart of the French Committee for monitoring and anticipating health risks*, „Natura Communication" 2023, nr 14, s. 9. https://doi.org/10.1038/s41467-023-43089-2.

Mariner J.C., Raizman E., Pittglio C., Bebay C., Kivaria F., Lubroth J., Makonnen Y., *Rift Valley fever action framework*, Italy 2022. https://doi.org/10.4060/cb8653en.

Mełgieś K.M., *The Evolution of One Health concept – a European perspective*, „Review of European and Comparative Law" 2024, t. 57, nr 2. https://doi.org/10.31743/recl.17467.

One health joint plan of action (2022–2026): working together for the health of humans, animals, plants and the environment, Rome 2022.

Özçelik R., Graubner C., Remy-Wohlfender F., Dürr S., Faverjon C., *Evaluating 5.5 Years of Equinella: A Veterinary-Based Voluntary Infectious Disease Surveillance System of Equines in Switzerland*, „Frontiers in Veterinary Science" 2020, t. 7, s. 1–4. https://doi.org/10.3389/fvets.2020.00327.

Perella A., Bisogno M., *The strength and resilience of Italy's health data system*, „The Lancet Regional Health" 2025, t. 51. https://doi.org/10.1016/j.lanepe.2025.101255.

Plaza-Rodriguez C., Alt K., Grobbel M., Hammerl J.A., Irrgang A., Szabo I., Stingl K., Schuh E., Wiehle L., Pfefferkorn B., Naumann S., Kaesbohrer A., Tenhagen B.A., *Wildlife as Sentinels of Antimicrobial Resistance in Germany?*, „Frontiers in Veterinary Science" 2021, t. 7, s. 1–11. https://doi.org/10.3389/fvets.2020.627821.

Saegerman C., Alba-Casals A., Garcia-Bocanegra I., Dal Pozzo F., Galen G. van, *Clinical Sentinel Surveillance of Equine West Nile Fever, Spain*, „Transboundary and Emerging Diseases" 2014, t. 63, nr 2, s. 161–164. https://doi.org/10.1111/tbed.12243.

Sarker S.A., Shahid A.H., Rahman B., Nazir N.H., *An integrated model for anthrax-free zone development*, „Journal of Infection and Public Health" 2023, t. 16, s. 141–152. https://doi.org/10.1016/j.jiph.2023.10.024.

Sinclair R., Boone S.A., Greenberg D., Keim P., Gerba C.P., *Persistence of Category A Select Agents in the Environment*, „Applied and Environmental Microbiology" 2008, nr 74(3), s. 555–563. https://doi.org/10.1128/AEM.02167-07.

Singh R.P., Hodson D.P., Huerta-Espino J., Jin Y., Bhavani S., Njau P., Herrera-Foessel S., Singh P.S., Singh S., Govindan V., *The emergence of Ug99 races of the stem rust fungus is a threat to world wheat production*, „Annual Review of Phytopathology" 2011, nr 49, s. 465–481. https://doi.org/10.1146/annurev-phyto-072910-095423.

Spitalleri A., Kavasidis I., Cartelli V., Mineo R., Rundo F., Palazzo S., Spampinato C., Giordano D., *BioTrak: A Blockchain-based Platform for Food Chain Logistics Traceability*, International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia 2023, s. 105–110. https://doi.org/10.1109/ICCNS58795.2023.10193341.

Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems, Geneva 2002.

The 2001 Outbreak of Foot and Mouth Disease, London 2002.

The European Union One Health 2023 Zoonoses Report, EFSA, 10 XII 2024 r. https://doi.org/10.2903/j.efsa.2024.9106.

Thompson D., Muriel P., Russell D., Osborne P., Bromley A., Rowland M., Creigh-Tyte S., Brown C., *Economic costs of the foot and mouth disease outbreak in the United Kingdom in 2001*, „Revue Scientifique et Technique" 2002, nr 21(3), s. 675–687. https://doi.org/10.20506/RST.21.3.1353.

Török T.J., Tauxe R.V., Wise R.P., Livengood J.R., Sokolow R., Mauvais S., Birkness K.A., Skeels M.R., Horan J.M., Foster L.R., *A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars*, „The Journal of the American Medical Association" 1997, t. 278, nr 5, s. 389–393. https://doi.org/10.1001/JAMA.1997.03550050051033.

Wheelis M., Casagrande R., Madden L.V., *Biological Attack on Agriculture: Low-Tech, High-Impact Bioterrorism: Because bioterrorist attack requires relatively little specialized expertise and technology, it is a serious threat to US agriculture and can have very large economic repercussions*, „BioScience" 2002, t. 52, nr 7, s. 569–576. https://doi.org/10.1641/0006-3568(2002)052[0569:BAOALT]2.0.CO;2.

Wood J.P., Meyer K.M., Kelly T.J., Choi Y.W., Rogers J.V., Riggs K.B., Willenberg Z.J., *Environmental Persistence of Bacillus anthracis and Bacillus subtilis Spores*, „PLoS ONE" 2015. https://doi.org/10.1371/journal.pone.0138083.

Źródła internetowe

About Anaplasmosis, Centers for Disease Control and Prevention, 4 IX 2024 r., https://www.cdc.gov/anaplasmosis/about/index.html [dostęp: 10 IX 2025].

Aedes aegypti – Factsheet for experts, European Centre for Disease Prevention and Control, 2 I 2023 r., https://www.ecdc.europa.eu/en/disease-vectors/facts/mosquito-factsheets/aedes-aegypti [dostęp: 10 IX 2025].

African swine fever, EFSA, 19 V 2025 r., https://www.efsa.europa.eu/en/topics/topic/african-swine-fever [dostęp: 16 VI 2025].

Agro-crime and agro-terrorism, World Organisation for Animal Health, https://www.woah.org/en/what-we-offer/emergency-preparedness/agro-crime-and-agro-terrorism/ [dostęp: 16 IX 2025].

Animal agrocrime and agroterrorism, Interpol, https://www.interpol.int/Crimes/Terrorism/Bioterrorism/Animal-agrocrime-and-agroterrorism [dostęp: 10 VI 2025].

Animal and Plant Health Agency framework document, Department for Environment, Food & Rural Affairs, 7 III 2024 r., https://www.gov.uk/government/publications/animal-and-plant-health-agency-framework-document/animal-and-plant-health-agency-framework-document [dostęp: 20 VI 2025].

ANSES Laboratories, ANSES, 15 II 2013 r., https://www.anses.fr/en/content/anses-laboratories [dostęp: 20 VI 2025].

Aplikacja IRZplus, Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/systemy-informatyczne/cbd-irzgo [dostęp: 1 IX 2025].

Barclay E., *A Review of the Literature on Agricultural Crime. Report to the Criminology Research Council*, https://criminology.fsu.edu/sites/g/files/upcbnu3076/files/2021-03/A-Review-of-the-Literature-on-Agricultural-Crime.pdf [dostęp: 2 XII 2025].

Biological threat reduction strategy. Strengthening global biological security, https://www.woah.org/app/uploads/2021/03/biothreat-strategy-veng-revised-1st-edition.pdf [dostęp: 14 VI 2025].

Bluetongue, U.S. Department of Agriculture, Animal and Plant Health Inspection Service, https://www.aphis.usda.gov/livestock-poultry-disease/cattle/bluetongue [dostęp: 10 IX 2025].

Bluetongue, World Organisation for Animal Health, https://www.woah.org/en/disease/bluetongue/ [dostęp: 10 IX 2025].

Breaking language barriers: translation of training materials on food safety regulations now available, European Commission, 25 III 2025 r., https://hadea.ec.europa.eu/news/breaking-language-barriers-translation-training-materials-food-safety-regulations-now-available-2025-03-25_en [dostęp: 1 IX 2025].

Building resilience against agro-crime and agro-terrorism, https://www.woah.org/app/uploads/2023/02/building-resilience-against-agro-crime-and-agro-terrorism.pdf [dostęp: 14 VI 2025].

Carus W.S., *Bioterrorism and Biocrimes: the Illicit Use of Biological Arms in the 20th Century*, August 1998, https://wmdcenter.ndu.edu/Publications/Publication-View/Article/626562/bioterrorism-and-biocrimes-the-illicit-use-of-biological-arms-in-the-20th-centu/ [dostęp: 14 VI 2025].

CDC Bioterrorism Agents, https://biosecurity.fas.org/resource/documents/CDC_Bioterrorism_Agents.pdf [dostęp: 10 VI 2025].

Chemical and biological deliberate events, World Health Organization, https://openwho.org/emergencymgmt/501116/Chemical+and+biological+deliberate+events [dostęp: 1 IX 2025].

Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory, United States Attorney's Office, 3 VI 2025 r., https://www.justice.gov/usao-edmi/pr/chinese-nationals-charged-conspiracy-and-smuggling-dangerous-biological-pathogen-us [dostęp: 20 VI 2025].

Commission publishes 2023 Annual Report on food safety alerts and agri-food fraud investigations, European Commission, 16 IX 2024 r., https://ec.europa.eu/newsroom/sante/items/847722/en [dostęp: 14 VI 2025].

Contingency plan for exotic notifiable diseases of animals in England, https://assets.publishing.service.gov.uk/media/691c80cd84a267da57d706da/Defra-contingency-plan-exotic-notifiable-diseases-animals-England.pdf [dostęp: 18 VI 2025].

Deliberate events, World Health Organization, 2 IV 2024 r., https://www.who.int/news-room/fact-sheets/detail/deliberate-events [dostęp: 18 VI 2025].

Deliverable D6.5 – Guiding Document on cross-sectoral preparedness and response to biological and/or chemical terror attack. Collaboration between health, civil protection and security, https://www.jaterror.eu/wp-content/uploads/2024/11/6.5-Guiding-Document.pdf [dostęp: 8 XII 2025].

Dengue, World Health Organization, 21 VIII 2025 r., https://www.who.int/news-room/fact-sheets/detail/dengue-and-severe-dengue [dostęp: 10 IX 2025].

Digitalising the EU agricultural sector, European Commission, https://digital-strategy.ec.europa.eu/en/policies/digitalisation-agriculture [dostęp: 1 IX 2025].

Dowden: world-class crisis capabilities deployed to defeat biological threats of tomorrow, 12 VI 2023 r., https://www.gov.uk/government/news/dowden-world-class-crisis-capabilities-deployed-to-defeat-biological-threats-of-tomorrow [dostęp: 8 VIII 2025].

EFSA, https://www.efsa.europa.eu [dostęp: 1 IX 2025].

Emergency preparedness, resilience and response concept of operations, UK Health Security Agency, 15 I 2025 r., https://www.gov.uk/government/publications/emergency-preparedness-resilience-and-response-concept-of-operations/emergency-preparedness-resilience-and-response-concept-of-operations [dostęp: 10 VI 2025].

Empowering food safety through enhanced training, European Commission, 9 IX 2024 r., https://ec.europa.eu/newsroom/btsf/items/846699/en [dostęp: 1 IX 2025].

European Commission, https://ec.europa.eu [dostęp: 1 IX 2025].

Factsheet about tick-borne encephalitis (TBE), European Centre for Disease Prevention and Control, 22 I 2024 r., https://www.ecdc.europa.eu/en/tick-borne-encephalitis/facts/factsheet [dostęp: 10 IX 2025].

Field simulation trainings to support emergency preparedness, World Organisation for Animal Health, 13 IV 2023 r., https://www.woah.org/en/article/field-simulation-trainings-to-support-emergency-preparedness/ [dostęp: 10 VI 2025].

First report on world's animal health reveals changing spread of disease impacting food security, trade and ecosystems, WOAH, 23 V 2025 r., https://www.woah.org/en/first-report-on-worlds-animal-health-reveals-changing-spread-of-disease-impacting-food-security-trade-and-ecosystems/ [dostęp: 15 VI 2025].

Flade F., *The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror*, https://ctc.westpoint.edu/june-2018-cologne-ricin-plot-new-threshold-jihadi-bio-terror/ [dostęp: 16 IX 2025].

FLI tests mobile One Health laboratory for diagnosing highly pathogenic pathogens, Friedrich Loeffler Institut, 13 VI 2025 r., https://www.fli.de/en/press/press-releases/press-singleview/fli-tests-mobile-one-health-laboratory-for-diagnosing-highly-pathogenic-pathogens/ [dostęp: 20 VI 2025].

Food Risk Assess Europe, EFSA, https://www.efsa.europa.eu/en/publications/food-risk-assess-europe [dostęp: 13 XII 2025].

Germany, European Commission, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-disaster-management-system/germany_en?utm [dostęp: 15 XII 2025].

Gyles C., *Agroterrorism*, https://pmc.ncbi.nlm.nih.gov/articles/PMC2839819/pdf/cvj_04_347.pdf [dostęp: 10 VI 2025].

HaDEA launches third call for tenders under BTSF, European Commission, 5 VIII 2022 r., https://hadea.ec.europa.eu/news/hadea-launches-third-call-tenders-under-btsf-2022-08-05_en?utm [dostęp: 1 IX 2025].

Health and Food Safety, European Commission, https://commission.europa.eu/about/departments-and-executive-agencies/health-and-food-safety_en [dostęp: 15 XII 2025].

Historie der LÜKEX Krisenmanagementübungen, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Historie/historie_node.html [dostęp: 15 XII 2025].

How Lyme Disease Spreads, Centers for Disease Control and Prevention, 24 IX 2024 r., https://www.cdc.gov/lyme/causes/index.html [dostęp: 10 IX 2025].

INMI Lazzaro Spallanzani IRCCS, Istituto Nazionale Malettie Infettive, https://www.inmi.it/ [dostęp: 20 VI 2025].

International Plant Protection Convention (1997), Rome 2024, https://openknowledge.fao.org/server/api/core/bitstreams/30cc2e83-a6fd-4e2c-a5ee-312093d5a307/content [dostęp: 10 VI 2025].

Krajowe Laboratoria Referencyjne, Państwowy Instytut Weterynaryjny – Państwowy Instytut Badawczy, https://www.piwet.pulawy.pl/krajowe-laboratoria-referencyjne/ [dostęp: 29 VII 2025].

Laboratory Biosafety Manual. Fourth Edition, WHO, 21 XII 2020 r., https://www.who.int/publications/i/item/9789240011311 [dostęp: 10 VI 2025].

Lessons from the COVID-19 pandemic, https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-lessons-learned-may-2023.pdf [dostęp: 16 IV 2025].

National biodefense strategy and implementation plan for countering biological threats, enhancing pandemic preparedness, and achieving global health security, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf [dostęp: 10 VI 2025].

National Priority Plant Pests (2024), Australian Government. Department of Agriculture, Fisheries and Forestry, https://www.agriculture.gov.au/biosecurity-trade/pests-diseases-weeds/plant/national-priority-plant-pests/ [dostęp: 10 VI 2025].

NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy, NATO, 14 VII 2022 r., https://www.nato.int/cps/en/natohq/official_texts_197768.htm [dostęp: 2 XII 2025].

One health joint plan of action 2022–2026: working together for the health of humans, animals, plants and the environment, World Health Organization, https://www.who.int/publications/i/item/9789240059139 [dostęp: 10 VI 2025].

One Health: a joint framework for action published by five EU agencies, European Centre for Disease Prevention and Control, 7 V 2024 r., https://www.ecdc.europa.eu/en/news-events/one-health-joint-framework-action-published-five-eu-agencies [dostęp: 10 VI 2025].

Ośrodek Diagnostyki i Zwalczania Zagrożeń Biologicznych, Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/zaklady/odizzb/organizacja [dostęp: 29 VII 2025].

Our science, The Pirbright Institute, https://www.pirbright.ac.uk/our-science [dostęp: 20 VI 2025].

Pavade G., *WOAH Updates – Global HPAI situation and current standards and recommendations regarding AI surveillance and vaccination*, https://www.izsvenezie.com/documents/reference-laboratories/avian-influenza/workshops/2022/pavade.pdf [dostęp: 16 VI 2025].

Poland Cold Chain Logistics et 2025–2034 – Size, Share, Trends, Analysis & Forecast 2025–2034, MarkWide Research, https://markwideresearch.com/poland-cold-chain-logistics-market/ [dostęp: 18 VI 2025].

Proofing the EU food supply chains against crises: new set of recommendations published, European Commission, 23 VII 2024 r., https://agriculture.ec.europa.eu/media/news/proofing-eu-food-supply-chain-against-crises-new-set-recommendations--published-2024-07-23_en [dostęp: 14 VI 2025].

Ramakrishnan A., *What is Fusarium graminearum, the fungus US authorities say was smuggled in from China?*, AP News, 4 VI 2025 r., https://apnews.com/article/fusarium-graminearum-fungus-head-blight-china-8ce925ae96d9c437b987e58c336cd45f [dostęp: 20 VI 2025].

Rapid Alert System for Food and Feed (RASFF), European Commission, https://food.ec.europa.eu/safety/rasff_en [dostęp: 10 X 2025].

RefBio - German Contribution to Strengthen the Reference Laboratories Bio in the UN-SGM, Robert Koch Institut, 10 V 2019 r., https://www.rki.de/EN/Institute/International-activities/Biosecurity-Programme/RefBio.html [dostęp: 16 VI 2025].

Reference Laboratories, The Pirbright Institute, https://www.pirbright.ac.uk/facilities-and-resources/reference-laboratories [dostęp: 17 VI 2025].

Rezerwy medyczne, Rządowa Agencja Rezerw Strategicznych, https://www.gov.pl/web/rars/rezerwy-medyczne [dostęp: 30 IX 2025].

Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf [dostęp: 11 VI 2025].

Shadomy S., Idrissi A.E., Raizman E., Bruni M., Palamara E., Pittglio C., Lubroth J., *Anthrax Outbreaks: a warning for improved prevention, control and heightened awareness*, „Food and Agriculture Organization of the United Nations" 2016, t. 37, https://openknowledge.fao.org/server/api/core/bitstreams/59269d58-654e-4790-ac60-a9ea7edd3a99/content [dostęp: 16 IV 2025].

Terrestrial Animal Health Code, https://rr-africa.woah.org/app/uploads/2023/09/en_csatvol1-2023.pdf [dostęp: 14 VI 2025].

The Biosafety Level-4 Laboratoty at RKI, Robet Koch Institut, 31 I 2024 r., https://www.rki.de/EN/Topics/Research-and-data/Specialised-laboratories/BSL-4-laboratory/bsl-4-laboratory-at-the-robert-koch-institute-node.html [dostęp: 16 VI 2025].

Tick-Borne Encephalitis, Centers for Disease Control and Prevention, 23 IV 2025 r., https://www.cdc.gov/yellow-book/hcp/travel-associated-infections-diseases/tick-borne-encephalitis.html [dostęp: 10 IX 2025].

Transmission of Zika Virus, Centers for Disease Control and Prevention, 30 I 2025 r., https://www.cdc.gov/zika/php/transmission/index.html [dostęp: 10 IX 2025].

Transparency solutions for transforming the food system, EU CAP Network, https://eu-cap-network.ec.europa.eu/projects/transparency-solutions-transforming-food-system_en [dostęp: 1 IX 2025].

UK Biological Security Strategy, Cabinet Office, 12 VI 2023 r., https://www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html [dostęp: 10 VI 2025].

UK pledges 1 billion pounds to build new biosecurity centre, Reuters, 24 VI 2025 r., https://www.reuters.com/business/healthcare-pharmaceuticals/uk-pledges-1-billion-pounds-build-new-biosecurity-centre-2025-06-23 [dostęp: 8 VIII 2025].

UKHSA Strategic Plan 2023 to 2026, https://assets.publishing.service.gov.uk/media/650d530e52e73c00139426c1/UKHSA_3_year_strategy.pdf [dostęp: 18 VI 2025].

Update: Cologne couple in court over 'biological bomb plot', The Local Germany, 7 VI 2019 r., https://www.thelocal.de/20190607/tunisian-german-couple-in-court-over-ricin-attack-plot [dostęp: 16 IV 2025].

USDA Coordinated Approach to Address New Virulences in Wheat and Barley Stem Rust – Pgt-Ug99, United States Department of Agriculture, 20 IX 2017 r., https://www.ars.usda.gov/ug99/ [dostęp: 16 VI 2025].

West Nile: Causes and How It Spreads, Centers for Disease Control and Prevention, 19 VIII 2025 r., https://www.cdc.gov/west-nile-virus/causes/index.html? [dostęp: 10 IX 2025].

What is EPPO Global Database?, https://gd.eppo.int/ [dostęp: 10 VI 2025].

What past disruptions can teach us about reviving supply chains after COVID-19, World Economic Forum, 27 III 2020 r., https://www.weforum.org/stories/2020/03/covid-19-coronavirus-lessons-past-supply-chain-disruptions/ [dostęp: 27 V 2025].

What We Do, European Centre for Disease Prevention and Control, https://www.ecdc.europa.eu/en/about-ecdc/what-we-do [dostęp: 30 IX 2025].

White E., *US says it broke up effort to bring toxic fungus to Michigan lab from China*, AP News, 3 VI 2025 r., https://apnews.com/article/chinese-scientists-charged-toxic-fungus-5ccaba9aff8e5941ebcea71b9b6690b2 [dostęp: 20 VI 2025].

Wojskowy Instytut Higieny i Epidemiologii im. Generała Karola Kaczkowskiego, https://wihe.pl/wihe/o-nas [dostęp: 29 VII 2025].

Zadania badawczo-rozwojowe, Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/wihe/zadania [dostęp: 29 VII 2025].

Zwalczanie i monitoring wybranych chorób zakaźnych zwierząt, Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/nadzor-weterynaryjny/programy-zwalczaniamonitorowania-chorob-zakaznych-zwierzat [dostęp: 1 IX 2025].

Akty prawne

Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz ich zniszczeniu (DzU z 1976 r. nr 1 poz. 1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE (Dz. Urz. UE L 314/26 z 6 XII 2022 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/522 z dnia 24 marca 2021 r. w sprawie ustanowienia Programu działań Unii w dziedzinie zdrowia („Program UE dla zdrowia") na lata 2021–2027 oraz uchylenia rozporządzenia (UE) nr 282/2014 (Dz. Urz. UE L 107/1 z 26 III 2021 r.).

Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego (Dz. Urz. UE L 31/1 z 1 II 2002 r.).

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. UE L 333/164 z 27 XII 2022 r.).

Ustawa z dnia 13 lutego 2020 r. o Państwowej Inspekcji Ochrony Roślin i Nasiennictwa (t.j. DzU z 2023 r. poz. 1992).

Ustawa z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia (t.j. DzU z 2023 r. poz. 1448, ze zm.).

Ustawa z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (t.j. DzU z 2023 r. poz. 1075).

Ustawa z dnia 29 stycznia 2004 r. o Inspekcji Weterynaryjnej (t.j. DzU z 2024 r. poz. 12).

Ustawa z dnia 18 grudnia 2003 r. o ochronie roślin (t.j. DzU z 2019 r. poz. 972, ze zm.).

Ustawa z dnia 21 grudnia 2000 r. o jakości handlowej artykułów rolno-spożywczych (t.j. DzU z 2023 r. poz. 1980).

Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (t.j. DzU z 2024 r. poz. 416).

Matylda Augustyn-Barwicz

Specjalista w zakresie biotechnologii, biobezpieczeństwa i zarządzania laboratoriami wysokiej klasy ochrony biologicznej. Obecnie pełni funkcję managera insektarium w Pirbright Institute (Wielka Brytania), gdzie odpowiada za nadzór nad laboratoriami CL2 oraz współpracę operacyjną z laboratoriami CL3 i SAPO 4.

Ukończyła biotechnologię i neuroendokrynologię na Uniwersytecie Jagiellońskim i w Polskiej Akademii Nauk. Jej doświadczenie zawodowe obejmuje wieloletnią służbę w formacjach państwowych odpowiedzialnych za bezpieczeństwo i reagowanie kryzysowe w strukturach Ministerstwa Spraw Wewnętrznych i Administracji i Ministerstwa Obrony Narodowej.

Kontakt: matylda.augustyn@gmail.com

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 53–99

https://doi.org/10.4467/27204383TER.25.046.23033

Artykuł

Dwadzieścia lat od ataków na londyński system transportu miejskiego. Problem terroryzmu islamskiego w Wielkiej Brytanii

Twenty years since the attacks on London's public transport system. The problem of Islamic terrorism in the United Kingdom

KRZYSZTOF IZAK

https://orcid.org/0000-0001-9815-6035

Autor niezależny

Abstrakt

Celem artykułu jest opisanie ataków terrorystycznych na londyński system transportu miejskiego, do których doszło 7 lipca 2005 r., oraz zagrożenia terrorystycznego w Wielkiej Brytanii związanego z radykalizacją środowisk muzułmańskich inspirowanych przez przywódców duchowych nawołujących do przemocy. Autor szeroko omówił podłoże tych ataków. Następnie m.in. na podstawie raportów z przeprowadzonego śledztwa przedstawił sylwetki sprawców, przygotowania do ataków, ich przebieg oraz próbę ich powtórzenia dwa tygodnie później. Wskazał problemy w zapewnieniu bezpieczeństwa antyterrorystycznego Wielkiej Brytanii, wynikające m.in. z polityki tolerancji wobec ekstremistów muzułmańskich.

Słowa kluczowe

Al-Muhadżirun, ekstremizm muzułmański, imigranci, służby specjalne, zagrożenie terrorystyczne, zamachy

Abstract

The aim of this article is to describe the terrorist attacks on London's public transport system that took place on 7 July 2005 and terrorist threat in Great Britain, posed by the radicalisation of Muslim communities inspired by spiritual leaders inciting violence. The author discussed the background to these attacks extensively. Then, based on investigation reports, among other sources, he presented profiles of the perpetrators, preparations for the attacks, their course and an attempt to repeat them two weeks later. He pointed out problems in ensuring anti-terrorist security in Great Britain, resulting, among other things, from a policy of tolerance towards Muslim extremists.

Keywords

Al-Muhajirun, Muslim extremism, immigrants, secret services, terrorist threat, attacks

Wprowadzenie

Wielka Brytania od początku XXI w. walczy z terroryzmem islamskim, którego źródłem są zewnętrzne uwarunkowania, m.in. aktywność organizacji globalnego salafickiego dżihadu, polityka władz w Londynie, w tym obecność brytyjskich wojsk w Iraku i Afganistanie, dynamiczny wzrost liczby imigrantów z krajów muzułmańskich oraz radykalizacja Brytyjczyków imigranckiego pochodzenia. W Wielkiej Brytanii znaleźli oni dogodne warunki do życia, korzystali z przywilejów i ściągali do tego kraju swoich krewnych. Domagali się dostosowania prawa do potrzeb ich mniejszości. Wywalczyli stosowanie prawa szariatu w sprawach cywilnych. Realizacja polityki społeczeństwa wielokulturowego w Wielkiej Brytanii sprawiła, że nie dostrzeżono zagrożenia wynikającego z niekontrolowanego rozprzestrzeniania się radykalnego islamu. Na azyl w Zjednoczonym Królestwie mogli liczyć dysydenci ścigani w krajach ojczystych za głoszenie antyrządowej propagandy oraz członkowie muzułmańskich organizacji ekstremistycznych, nie wyłączając terrorystów. W latach 90. XX w. młodzi obywatele brytyjscy pakistańskiego pochodzenia, stanowiący największą mniejszość muzułmańską, zaczęli licznie wyjeżdżać do kraju przodków. Przechodzili tam przeszkolenie wojskowe w obozach talibów i Al-Kaidy. Poznawali nowe dla nich idee, m.in. nienawiść do religii innych niż islam i wrogość do szyitów czy ahmadytów, i wracali z zamiarem szerzenia ich w Wielkiej Brytanii. Młodzież

pakistańskiego pochodzenia szybko się radykalizowała pod wpływem haseł głoszonych w meczetach przez imamów i innych przywódców duchowych. Szczególną aktywność zaczęli wykazywać po ataku 11 września 2001 r. w Stanach Zjednoczonych. Brytyjskie służby inwigilowały i zatrzymywały osoby podejrzane o przygotowywanie ataków terrorystycznych, jednak propagandyści dżihadu długo pozostawali bezkarni. Udział brytyjskich sił w operacjach wojskowych w Afganistanie i Iraku spowodował gwałtowny wzrost zagrożenia terrorystycznego w Wielkiej Brytanii.

Zamachy z 7 lipca 2005 r. na londyński system transportu miejskiego, podczas których zdetonowano cztery bomby (trzy w pociągach londyńskiego metra i jedna w autobusie miejskim), były pierwszymi z długiej serii udanych ataków i udaremnionych prób ich przeprowadzenia. Celem artykułu jest opisanie tych ataków oraz zagrożenia terrorystycznego w Wielkiej Brytanii związanego z radykalizacją środowisk muzułmańskich inspirowanych przez przywódców duchowych nawołujących do przemocy.

Ekstremizm islamski – zagrożenia terrorystyczne w Wielkiej Brytanii do 2005 roku

Do 2005 r. Wielkiej Brytanii udało się uniknąć ataków terrorystycznych w wykonaniu ekstremistów islamskich, mimo że mieszkała tam duża grupa radykałów otwarcie głoszących swoje poglądy. W Dewsbury w hrabstwie West Yorkshire w północnej Anglii utworzono siedzibę centrum koordynacyjnego Stowarzyszenia Krzewienia Wiary (Tablighi Dżama'at) na Europę. W Leicester w środkowej Anglii ulokowano siedzibę Federacji Organizacji Muzułmańskich (Federation of Muslim Organisations), znajdującej się pod silnym wpływem ruchu Braci Muzułmanów (Al-Ichwan al-Muslimin; Muslim Brotherhood, MB), który oddziałuje również na Stowarzyszenie Muzułmanów w Wielkiej Brytanii (Muslim Association in Britain, MAB). Jeden z założycieli MAB, Kamal al-Halbawi, został w 1995 r. oficjalnym rzecznikiem MB w Wielkiej Brytanii. W Leicester znajduje się również siedziba Fundacji Muzułmańskiej (Islamic Foundation, IF), utworzonej przez Khurshida Ahmada, działacza pakistańskiej partii religijnej Stowarzyszenie Muzułmańskie (Dżama'at-e Islami)[1]. Ruch MB operował w Wielkiej Brytanii za pośrednictwem wzajemnie powiązanych ze sobą organizacji pochodzenia

[1] S. Besson, *Islamizacja Zachodu? Historia pewnego spisku*, Warszawa 2006, s. 125–126, 129.

palestyńskiego, syryjskiego, libijskiego, somalijskiego, irackiego i egipskiego. Oprócz IF i MAB były to, by wymienić te najbardziej znaczące, Muzułmański Fundusz Społeczny (Muslim Welfare Trust), Palestyński Fundusz Pomocy i Rozwoju (Palestinian Relief and Development Fund, Interpal), Centrum Powrotu do Palestyny (Palestine Return Centre), Instytut Islamskiej Myśli Politycznej (Institute for Islamic Political Thought), Centrum Islamskie w Londynie (Islamic Centre in London), Muzułmański Komitet Spraw Publicznych (Muslim Public Affairs Committee), a ponadto firma medialna Maszrik Medias Services, która wydawała gazetę Hamasu „Filastin al-Muslima" (pol. Muzułmańska Palestyna) i prohamasowskie czasopismo w języku angielskim „Palestine Times"[2].

Stolica Wielkiej Brytanii stała się ważnym ośrodkiem ideologicznym ekstremizmu muzułmańskiego i sieci salafickiego dżihadu oddziałującym na cały świat. W latach 70. XX w. jeden z algierskich fundamentalistów oświadczył: *Tutaj w Londynie panuje wolność. Zostawiają nas w spokoju, a nawet pomagają*[3]. Przez ponad 40 lat Londyn był główną bazą ekstremizmu islamskiego, a w latach 1980–1990 – jego punktem kontaktowym. Ulokowały się w nim niemal wszystkie ruchy muzułmańskie, od tych umiarkowanych do najbardziej ekstremistycznych. Stolica Wielkiej Brytanii pozostawała miejscem rekrutacji i finansowania radykalnych organizacji muzułmańskich z różnych państw świata. Wielu ochotników udających się na front dżihadu w Afganistanie, Jemenie, Czeczenii, Bośni czy Kaszmirze przejeżdżało tranzytem przez Londyn. Wyjazdy ochotników były organizowane przez doskonale zorganizowane siatki korzystające ze wsparcia finansowego miejscowych organizacji charytatywnych[4].

Miasto określa się mianem „Londonistanu". Po raz pierwszy słowo to zostało użyte w 1990 r. przez francuskie służby do walki z terroryzmem oraz rządy Pakistanu i Arabii Saudyjskiej[5]. Odniesiono się tym samym do Londynu jako siedziby wielu ugrupowań ekstremistycznych oraz przebywających w nim radykalnych przywódców organizujących zamachy terrorystyczne w innych państwach. „Londonistan" stał się bezpieczną przystanią m.in. dla takich radykalnych działaczy muzułmańskich, jak Omar Bakri Mohammad,

[2] M. Whine, *The Penetration of Islamist Ideology in Britain*, Hudson Institute, 18 V 2005 r., https://www.hudson.org/national-security-defense/the-penetration-of-islamist-ideology-in-britain [dostęp: 18 XI 2025].

[3] X. Raufer, *Atlas radykalnego islamu*, Warszawa 2011, s. 87.

[4] Tamże.

[5] M. Zawadewicz, *Życie codzienne w muzułmańskim Londynie*, Warszawa 2008, s. 134.

jeden z założycieli brytyjskiego oddziału organizacji Islamska Partia Wyzwolenia (Hizb ut-Tahrir Islami), a następnie ugrupowania Emigranci (Al-Muhadżirun), otwarcie popierający ataki w USA z 11 września 2001 r. oraz wzywający do zjednoczenia muzułmanów i utworzenia światowego kalifatu. Jego bliskim znajomym był Mustafa Kamal Mustafa, lepiej znany jako Abu Hamza al-Masri, przywódca organizacji Zwolennicy Szariatu (Ansar asz-Szaria) i charyzmatyczny imam Wielkiego Meczetu w Finsbury Park, nawołujący do dżihadu i zniszczenia niewiernego Zachodu. Radykalne poglądy głosił również Omar Mahmud Osman alias Abu Katada al-Filastini, redaktor naczelny tygodnika „Al-Ansar" stanowiącego w latach 90. XX w. propagandowe wsparcie algierskiej Zbrojnej Grupy Islamskiej (Al-Dżama'a al-Islamijja al-Musallaha) przez zapewnianie jej medialnego rozgłosu i łączności z salafickim dżihadem. Abu Katada wspierał też działania Al-Kaidy w Europie[6].

W latach 90. XX w. Londyn stał się światowym centrum arabskiej prasy, w tym wspomnianej „Filastin al-Muslima" oraz „Al-Hayat" (pol. „Życie"), „Al-Kuds Al-Arabi" (pol. Arabska Jerozolima), „Asz-Szark al-Awsat" (pol. Bliski Wschód) i „Risalat al-Ichwan" (pol. Przesłanie Braci), a także Bliskowschodniej Korporacji Nadawczej (Middle East Broadcasting Corporation) i wielu specjalistycznych publikacji islamskich[7]. Niektóre fatwy Osamy bin Ladena zostały opublikowane najpierw w Londynie. Z kolei Ayman az-Zawahiri, zastępca Osamy bin Ladena, w grudniu 2001 r. ogłosił w „Asz-Szark al-Awsat" skrót swojego manifestu pt. *Fursan tahta rayat an-Nabi* (pol. Rycerze pod sztandarem Proroka). Przedstawił w nim strategię Al-Kaidy, począwszy od zamachów z 11 września 2001 r., które miały sprowokować atak USA na muzułmanów i doprowadzić do ogólnoświatowego dżihadu, oznaczającego walkę między islamem a wrogimi mu siłami, czyli mocarstwami zachodnimi i Rosją[8]. W grudniu 2002 r. Az-Zawahiri opublikował w „Al-Kuds al-Arabi" artykuł pt. *Al-wala wa al-bara* (pol. Lojalność i wyrzeczenie lub Wierność i rozłam), w którym przedstawił koraniczną

[6] K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, s. 127, 358–359.

[7] M. Phillips, *Londonistan. Jak Wielka Brytania stworzyła państwo terroru*, Warszawa 2010, s. 40–41.

[8] M.B. Shishani, *Salafi-Jihadists Geopolitical Perspective of Central Asia*, Central Asia – Caucasus Analist, https://www.cacianalyst.org/publications/analytical-articles/item/10050-analytical-articles-caci-analyst-2005-6-29-art-10050.html [dostęp: 29 VI 2025]. Pełny tekst manifestu zawarty został w książce Laury Mansfield, *His Own Words: Translation and Analysis of the Writings of Dr. Ayman Al Zawahiri*, New York 2006.

definicję muzułmańskiej tożsamości. Polega ona na wzajemnej wierności wszystkich muzułmanów oraz ich izolowaniu się od Żydów i chrześcijan, apostatów i heretyków[9]. W Londynie radykalne ugrupowania, zrzeszające imigrantów i uciekinierów politycznych z krajów muzułmańskich, zostały uformowane w ruch islamistyczny o światowym zasięgu. Na przełomie lat 80. i 90. XX w. zorganizowano w Wielkiej Brytanii serię konferencji. Jednoczyły one radykałów muzułmańskich z całego świata, począwszy od stosujących przemoc organizacji, takich jak Hamas czy Hezbollah, a kończąc na muzułmańskich partiach politycznych biorących udział w wyborach do parlamentu w Jordanii czy Malezji[10].

Wielka Brytania stanowiła schronienie dla radykalnych ideologów fundamentalizmu muzułmańskiego prześladowanych we własnych krajach. Korzystali oni z azylu politycznego, pod warunkiem że na terytorium Zjednoczonego Królestwa nie urzeczywistniali swoich idei. Mogli je jednak swobodnie wyrażać, również w skrajnej formie, otwarcie wzywając do dżihadu przeciwko Zachodowi. Nie zmieniło się to nawet po zamachach z 11 września. W dniu 14 grudnia 2001 r. parlament przyjął ustawę antyterrorystyczną (*Anti-terrorism, Crime and Security Act 2001*) pozwalającą na aresztowanie cudzoziemców podejrzanych o działalność terrorystyczną. Tolerowano jednak działalność organizacji ekstremistycznych, z których często wywodzili się terroryści. Były wśród nich osoby, które przeprowadzały operacje terrorystyczne albo próbowały dokonać zamachów w Europie, Azji, Afryce i Ameryce Północnej[11]. Na przykład 30 kwietnia 2003 r. dwóch terrorystów dokonało ataku samobójczego na bar Mikes Place na plaży w Tel Awiwie, odwiedzany przez obcokrajowców z Zachodu. Zginęły 3 osoby, a 65 zostało rannych. Sprawcy byli Brytyjczykami pakistańskiego pochodzenia. Pierwszy z nich, Asif Mohammad Hanif z Londynu, zginął podczas zamachu. Drugi, Omar Khan Sharif z Derby, przeżył, ale utonął podczas próby ucieczki. Był to pierwszy zamach, w którym Hamas wykorzystał terrorystów niebędących rodowitymi Palestyńczykami. Według brytyjskich służb sprawcy zostali zwerbowani w Wielkiej Brytanii, a następnie spędzili pewien czas w Syrii, gdzie spotkali się z bojownikami Hamasu i zostali przeszkoleni. W marcu 2004 r. Hamas opublikował nagranie

[9] J. Gilliam, *Why They Hate Us. An Examination of al-wala' wa-l-bara' in Salafi-Jihadist Ideology*, Military Review, 15 II 2018 r., https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Feb/They-Hate/ [dostęp: 15 VII 2025].

[10] M. Phillips, *Londonistan…*, s. 42.

[11] Tamże, s. 44.

wideo zawierające wspólny testament zamachowców oraz informację, że atak miał się zbiec z pierwszą rocznicą zamordowania przez izraelskie siły Ibrahima al-Makadmy, założyciela Brygad Izz ad-Din al-Kassam[12].

Chociaż w 2001 r. Londyn stanął u boku Waszyngtonu w wojnie z terroryzmem, to terytorium brytyjskie wydawało się zabezpieczone przed próbami ataku do czasu, kiedy niepokojące sygnały zmusiły rząd do radykalnej zmiany polityki. W 2002 r. opracowano rządową strategię zwaną w skrócie CONTEST (ang. *counter-terrorism strategy*), która połączyła działania wszystkich służb w celu zmniejszenia zagrożenia terroryzmem międzynarodowym[13]. Mimo to nie podejmowano zdecydowanych działań przeciwko przejawom ekstremizmu islamskiego i mowy nienawiści. 11 września 2002 r., w pierwszą rocznicę ataków w Stanach Zjednoczonych, organizacja Al-Muhadżirun zorganizowała w meczecie w Finsbury Park konferencję pod nazwą „Wielki dzień w historii", podczas której przedstawiono pozytywne – według organizacji – strony tego ataku. Al-Masri wygłosił na niej odczyt, w którym chwalił porywaczy samolotów, a Omar Bakri Mohammad nazwał ich „dziewiętnastką wspaniałych"[14]. W tym czasie meczet w Finsbury Park był jednym z najaktywniejszych ośrodków rekrutacyjnych islamskich bojowników w Londynie. Spotykali się tu ekstremiści muzułmańscy zarówno z Wielkiej Brytanii, jak i z innych krajów. Właśnie w tym meczecie zwerbowano Richarda Reida, słynnego „shoe bombera", który w końcu lat 90. XX w. odbył szkolenie wojskowe w Afganistanie, a po powrocie do Londynu został aktywnym członkiem ekstremistycznej komórki skupionej wokół Al-Masriego. Reid przemycił ładunek wybuchowy na pokład samolotu American Airlines lecącego 22 grudnia 2001 r. z Paryża do Miami. Został obezwładniony przez pasażerów podczas próby zdetonowania[15]. Słuchaczami kazań Al-Masriego było wielu innych terrorystów, w tym Hanif i Szarif,

[12] M. Levitt, *Hamas. Polityka, dobroczynność i terroryzm w służbie dżihadu*, Kraków 2008, s. 293–294.

[13] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c470140f0b62dffde1050/isc_terrorist_attacks_7july_report.pdf, s. 5 [dostęp: 18 XI 2025].

[14] *Abu Hamza profile*, BBC News, 9 I 2015 r., https://www.bbc.com/news/uk-11701269 [dostęp: 18 XI 2025]; *„Magnificent 19" risks further outrage*, The Standard, 13 IV 2012 r., https://www.standard.co.uk/hp/front/magnificent-19-risks-further-outrage-6948639.html [dostęp: 18 XI 2025].

[15] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism. The British Connections*, London 2010, s. 308–309.

Kamal Bourgass[16], Zacarias Moussaoui (domniemany dwudziesty zamachowiec z 11 września 2001 r.) i trzech z czterech zamachowców z 7 lipca 2005 r. (Mohammad Sidique Khan, Shehzad Tanweer i Jermaine Lindsay)[17].

W listopadzie 2002 r. zatrzymano w Londynie sześć osób pochodzących z Maroka i Tunezji. Zarzucono im przygotowanie zamachu w londyńskim metrze. Nie mieli oni stałego adresu zamieszkania i byli bezrobotni. Jeden z podejrzanych przyznał się do odbycia szkolenia wojskowego w Afganistanie. Miesiąc później w Londynie i Edynburgu aresztowano czterech obywateli Algierii podejrzanych o przygotowanie ataku terrorystycznego. W styczniu 2003 r. zatrzymano pięciu Algierczyków i Etiopczyka, którzy przybyli do Wielkiej Brytanii dwa lata wcześniej i poprosili o azyl. W ich mieszkaniu w północnym Londynie odkryto ślady rycyny[18].

W 2003 r. nastąpił wzrost zagrożenia terrorystycznego w Wielkiej Brytanii w związku z wkroczeniem do Iraku amerykańskich i brytyjskich sił. Zamknięto wówczas meczet w Finsbury Park, ponieważ znaleziono w nim m.in. gaz CS, ubiór chroniący przed bronią chemiczną i biologiczną, truciznę, kajdanki, broń gazową oraz wiele blankietów brytyjskich paszportów, praw jazdy i kart kredytowych, a także słynną 11-tomową encyklopedię afgańskiego dżihadu, stanowiącą podręcznik terroryzmu. Aresztowano wówczas siedem osób w związku z podejrzeniem posiadania rycyny[19]. Al-Masri pozostał na wolności. Zamknięcie meczetu nie przeszkodziło mu głosić kazań na ulicy przed budynkiem oraz w innych meczetach w środkowej Anglii. Nie podjęto jednak działań, by powstrzymać jego działalność, nawet po ogłoszeniu przez niego fatwy, w której stwierdził, że przez

[16] Algierczyk, który w styczniu 2003 r. w Manchesterze zabił detektywa Stephena Oake'a w trakcie próby zatrzymania przez brytyjską policję. Podejrzewany o próbę dokonania w Wielkiej Brytanii ataku terrorystycznego z wykorzystaniem rycyny, która jest silną trucizną. Zob. *Terror Watch: What Ricin?*, Newsweek, 12 IV 2005 r., https://www.newsweek.com/terror-watch-what-ricin-116577 [dostęp: 18 IX 2025].

[17] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism…*, s. 46–48, 213, 216, 220, 342, 384, 386; C. Marsden, *Britain: Why did it take so long to bring Abu Hamza to trial?*, World Socialist Web Site, 16 II 2006 r., https://www.wsws.org/en/articles/2006/02/hamz-f16.html [dostęp: 16 VII 2025]; D. Strieff, *Terror-tinged U.K. mosque gets a makeover*, NBC News, 5 VII 2006 r., https://www.nbcnews.com/id/wbna13501930 [dostęp: 18 IX 2025].

[18] X. Raufer, *Atlas radykalnego islamu…*, s. 92.

[19] W. Hoge, *Threats and Responses: Terror Suspects, Mosque Raid in London Results in 7 Arrests in Connection With Discovery of Poison*, The New York Times, 21 I 2003 r., https://www.nytimes.com/2003/01/21/world/threats-responses-terror-suspects-mosque-raid-london-results-7-arrests.html [dostęp: 18 IX 2025].

aktywne włączenie się Wielkiej Brytanii w inwazję na Irak i okupację tego kraju staje się ona uprawnionym celem ataku. Według m.in. dziennika „The Guardian" jego aresztowaniu byli przeciwni agenci służb bezpieczeństwa i policjanci, mający nadzieję, że będzie on informował o próbach przeprowadzenia ataku terrorystycznego w Wielkiej Brytanii[20].

W maju 2003 r. w ramach śledztwa prowadzonego w sprawie zamachu samobójczego w Tel Awiwie zatrzymano w Nottinghamshire w środkowej Anglii sześciu ekstremistów islamskich[21]. Funkcjonariusze Scotland Yardu szacowali wówczas, że ok. 50 doskonale przygotowanych bojowników spośród 200 Brytyjczyków szkolonych w Afganistanie powróciło do Wielkiej Brytanii i stworzyło grupy terrorystyczne[22]. W czerwcu powołano Wspólne Centrum Analiz Terroryzmu (Joint Terrorism Analysis Centre, JTAC), podlegające MI5, w celu oceny i analizy zagrożenia terrorystycznego w Wielkiej Brytanii. Wyróżniono pięć poziomów zagrożenia: niski (ang. *low*), umiarkowany (ang. *moderate*), znaczny (ang. *substanstial*), poważny (ang. *severe*), krytyczny (ang. *critical*)[23].

W listopadzie 2003 r. podczas wizyty w Londynie prezydenta George'a W. Busha doszło do zamachów w Stambule, w których terroryści muzułmańscy wzięli na cel brytyjski bank HSBC i konsulat[24]. W grudniu tego samego roku aresztowano afgańskiego weterana Andrew Rowe'a,

---

[20] P. Owen, *Clarke rejects Hamza inquiry calls*, The Guardian, 9 II 2006 r., https://www.theguardian.com/uk/2006/feb/09/terrorism.politics [dostęp: 18 IX 2025]; E.F. Vencat, *'Bleed the Enemy'*, Newsweek, 11 I 2006 r., https://www.newsweek.com/bleed-enemy-108227 [dostęp: 11 VII 2025]. W maju 2004 r. Abu Hamza al-Masri został aresztowany na prośbę Stanów Zjednoczonych wnoszących o jego ekstradycję. W październiku 2004 r. brytyjski wymiar sprawiedliwości przedstawił Al-Masriemu 15 zarzutów, w tym nawoływanie do zabijania niewiernych i posiadanie materiałów propagandowych zachęcających do podejmowania działań terrorystycznych. W lutym 2006 r. Al-Masri został uznany za winnego 11 z 15 wniesionych przeciwko niemu oskarżeń i skazany na 7 lat więzienia. W październiku 2012 r., po ośmioletniej batalii prawnej, został ekstradowany z Wielkiej Brytanii do USA. Tam w maju 2014 r. został uznany za winnego 11 zarzutów dotyczących terroryzmu. 9 stycznia 2015 r. skazano go na karę dożywotniego więzienia bez możliwości zwolnienia warunkowego. Zob. X. Raufer, *Atlas radykalnego islamu...*, s. 92; *Radical cleric Abu Hamza jailed for life by US court*, BBC News, 9 I 2015 r., https://www.bbc.com/news/world-us-canada-30754959 [dostęp: 18 IX 2025].

[21] X. Raufer, *Atlas radykalnego islamu...*, s. 92.

[22] Tamże.

[23] *Terrorism threat levels*, Security Service MI5, https://www.mi5.gov.uk/threats-and-advice/terrorism-threat-levels [dostęp: 23 VI 2025].

[24] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism...*, s. 18.

powiązanego z francuskim dżihadystą Lionelem Dumontem, członkiem tzw. gangu z Roubaix[25]. W marcu 2004 r. na przedmieściach Londynu odkryto 600 kg saletry potasowej służącej do produkcji materiałów wybuchowych. Aresztowano wówczas ośmiu Brytyjczyków pakistańskiego pochodzenia w wieku od 17 do 32 lat. Jeden z nich, Mohammed Babar, powiązany z Omarem Khyamem, zeznał, że grupa zamierzała przeprowadzić zamachy na dyskotekę w Londynie, centrum handlowe w Kent oraz infrastrukturę energetyczną i gazową[26]. W 2004 r. zdelegalizowano organizację Al-Muhadżirun, która rekrutowała muzułmańskich studentów brytyjskich uczelni na szkolenie ideologiczne i wojskowe w Pakistanie, Afganistanie, Jemenie i Sudanie. Jednak w miejsce Al-Muhadżirun powstały dwa współpracujące ze sobą ugrupowania: Sekta Zbawienia/Ocalenia (Firkat an-Nadżija) i Al-Ghuraba (Obcy). Obie grupy łączyła nie tylko idea moralnej czystości i propagowania ortodoksyjnego islamu w duchu pierwszych muzułmanów, lecz także osoba Anjema Choudary'ego, bliskiego współpracownika Omara Bakriego Mohammada[27]. Liderzy nowych ugrupowań unikali wypowiedzi zawierających agresywne treści i oficjalnie nabrali dystansu do ekstremistycznej propagandy. Usuwali wrogie hasła ze swoich stron internetowych zarejestrowanych na Wyspach Brytyjskich, utrzymywali jednak na nich odnośniki do witryn założonych w państwach muzułmańskich, m.in. w Indonezji i Bangladeszu, na których znajdowały się przypadkowe linki do tematyki ekstremistycznej, pozbawione słów kluczowych typowych dla propagandy radykalnych środowisk muzułmańskich[28].

W 2004 r. brytyjskie służby zwiększyły zainteresowanie grupami, w których skład wchodzili głównie obywatele brytyjscy pakistańskiego pochodzenia. Był to skutek odkrycia składu saletry potasowej oraz sprawy afgańskiego weterana, który odmówił wykonania misji samobójczej podobnej do tej Reida[29]. 3 sierpnia 2004 r. zatrzymano grupę związaną bezpośrednio

[25] Tamże.

[26] X. Raufer, *Atlas radykalnego islamu…*, s. 92; R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism…*, s. 18.

[27] W 2005 r. Omar Bakri Mohammad, po dwudziestoletnim pobycie w Wielkiej Brytanii, dobrowolnie wyjechał do Libanu, gdzie został poinformowany przez brytyjskie władze o dożywotnim zakazie powrotu do Zjednoczonego Królestwa. Nie zaprzestał jednak działalności i zdalnie uczestniczył w spotkaniach i konferencjach organizowanych w Londynie przez islamskich ekstremistów. Zob. K. Izak, *Leksykon organizacji…*, s. 359.

[28] Tamże, s. 358, 360.

[29] G. Chaliand, A. Blin, *Historia terroryzmu. Od starożytności do Da'isz*, Warszawa 2020, s. 393.

z Al-Kaidą, którą kierował Dhiren Barot alias Abu Musa al-Hindi, weteran wojny w Afganistanie[30]. W tym samym czasie nastąpiła próba dokonania zmiany w politycznej doktrynie brytyjskiej wielokulturowości. Zmiana ta dotyczyła poparcia dla niezależnego rozwoju kulturowego poszczególnych grup etnicznych i religijnych obcego pochodzenia, dowartościowywania różnic między nimi oraz ich specyficznych oznak tożsamości. Jednocześnie przywódcy wspólnot muzułmańskich mieli nawoływać w meczetach do przestrzegania porządku publicznego[31]. 3 kwietnia 2004 r. Mark Trevor Phillips, przewodniczący brytyjskiej parlamentarnej Komisji ds. Równości Rasowej (Commission for Racial Equality), która uczyniła z wielokulturowości kluczowy element polityki społecznej, po raz pierwszy stanowczo ją skrytykował. Powiedział w wywiadzie dla prasy, że wielokulturowość to wyrażenie, które (...) *straciło na znaczeniu* (...). *Wielokulturowość sugeruje bowiem separację.* (...) *Powinniśmy więc raczej mówić o tym, jak przejść od niej do społeczeństwa zintegrowanego, w którym wszyscy są równi wobec prawa i panują wspólne wartości: raczej demokracja niż przemoc, wspólne używanie języka angielskiego i podporządkowanie kulturze Wysp Brytyjskich*[32]. Ta wypowiedź została źle przyjęta przez wyznawców islamu. W czasie manifestacji zorganizowanej w Londynie w celu wyrażenia poparcia dla przebywających w więzieniach młodych Brytyjczyków pakistańskiego pochodzenia spalili oni brytyjską flagę z okrzykami „Allah Akbar"[33]. Wydarzenie to wywołało pytania dotyczące znaczenia integracji i polityki wielokulturowości, czynników warunkujących ich powodzenie lub klęskę[34].

Sprawcy ataku

Samobójczy atak w Londynie przeprowadziło czterech mężczyzn w wieku od 18 do 30 lat. Trzech z nich: Mohammad Sidique Khan (30 lat), Shehzad Tanweer (22 lata) i Hasib Hussain (18 lat) urodziło się w Wielkiej Brytanii. Ich rodzice przybyli do niej wiele lat wcześniej i osiedlili się w Beeston

[30] Tamże; *Al-Qaeda plotter jailed for life*, BBC News, 7 XI 2006 r., http://news.bbc.co.uk/2/hi/uk_news/6123236.stm [dostęp: 7 VIII 2025].

[31] Tamże.

[32] G. Kepel, *Fitna, wojna w sercu islamu*, Warszawa 2006, s. 222.

[33] Tamże.

[34] Intelligence and Security Committee, *Report into the London Terrorist Attacks*..., s. 17.

i Holbeck na przedmieściach Leeds. Znaleźli tu pracę i otrzymali brytyjskie obywatelstwo. Każdy z nich wywodził się z rodziny wielodzietnej. Wszyscy uczęszczali do lokalnych szkół i meczetów. Czwarty zamachowiec, Jermaine Lindsay (19 lat), pochodził z Jamajki[35].

Khan, najstarszy z nich, uznany później za przywódcę komórki terrorystycznej, został zapamiętany jako uczeń pilny, cichy i niesprawiający kłopotów. Po ukończeniu szkoły pracował dla miejscowej agencji pomocy, a następnie Departamentu Handlu i Przemysłu (Department of Trade and Industry)[36]. W 1996 r. rozpoczął studia biznesowe w Leeds Metropolitan University. Jeszcze podczas studiów rozpoczął pracę z młodzieżą, a po ich ukończeniu w 2001 r. został nauczycielem w szkole w Beeston, placówce oświatowej dla dzieci z trudnościami językowymi i behawioralnymi[37]. Cenili go zarówno inni nauczyciele, jak i rodzice. W 2002 r. udzielił wywiadu dla „Times Educational Supplement", w którym z pasją opowiadał o swojej pracy[38]. Jednocześnie dał się poznać jako gorliwy muzułmanin. Regularnie modlił się w pracy oraz w meczecie. Opowiadał, że nie miał spokojnej młodości, wdawał się w bójki, pił alkohol, zażywał narkotyki. Był też zamieszany w handel nimi i miał kilka konfliktów z policją, w tym dotyczących napaści i paserstwa. Zerwał z tym życiem i zwrócił się ku religii. Według otoczenia nie był agresywny, radykalny ani upolityczniony w sposobie, w jaki opowiadał podopiecznym o religii[39]. Były to jednak pozory, ponieważ Khan prowadził podwójne życie. Z jednej strony angażował się społecznie, a z drugiej ukrywał swoją działalność dżihadystyczną.

W lipcu 2001 r. Khan i jego bliski przyjaciel Wahid Ali udali się do prowadzonego przez Ruch Mudżahedinów (Harakat ul-Mudżhidin) obozu szkoleniowego Mansera, znajdującego się w części Kaszmiru kontrolowanej przez Pakistan. Stamtąd przedostali się do północno-wschodniego Afganistanu i dotarli do linii frontu talibów z Sojuszem Północnym. Wrócili do domu kilka dni przed zamachami z 11 września 2001 r. W szkole Khan oficjalnie wypowiedział się przeciwko tym atakom[40]. Według Artura Wejksznera,

[35] *Report of the Official Account of the Bombings in London on 7th July 2005*, https://assets.publishing.service.gov.uk/media/5a7c7bc840f0b626628ac62e/1087.pdf, s. 15–16 [dostęp: 7 VII 2025].

[36] Tamże, s. 13.

[37] Tamże.

[38] *Report of the Official Account*…, s. 14, 16.

[39] Tamże, s. 14.

[40] Tamże; *Profile: Mohammad Sidique Khan*, BBC News, 2 III 2011 r., https://www.bbc.com/news/uk-12621381 [dostęp: 2 VI 2025].

powołującego się na artykuł Simona Eleganta pt. *A London Bomber's Asia Tour*, zamieszczony w „The Time" z 26 września 2005 r., Khan po odbyciu szkolenia wojskowego w obozie Mansera przemieścił się do obozu talibów w pobliżu Bagram, niedaleko Kabulu. Po wkroczeniu amerykańskich sił do Afganistanu 7 października 2001 r. i udzieleniu przez nie wsparcia Sojuszowi Północnemu stanął w czynnej obronie reżimu talibów. Następnie odbył misję rekonesansową w Malezji, gdzie spotkał się z Riduanem Isamuddinem alias Hambali, członkiem indonezyjskiej Wspólnoty Muzułmańskiej (Dżimah Islamijja). Głównym zadaniem Khana było zdobycie wiedzy na temat wysokości środków finansowych potrzebnych tej organizacji na działalność terrorystyczną. Podczas wizyty na Borneo Khan spotkał się z Nasirem Abbasem, wysokim rangą członkiem Dżimah Islamijja, z którym udał się do bazy organizacji na filipińskiej wyspie Mindanao. Tam miał spotkać się z Azharim Husinem, który był odpowiedzialny za przygotowanie większości ładunków wybuchowych użytych przez terrorystów Dżimah Islamijja[41]. Według raportu służb specjalnych przygotowanego dla Izby Gmin informacje medialne dotyczące wizyty Khana w Malezji i na Filipinach zostały zbadane i uznano je za bezpodstawne[42].

Na przełomie 2001 r. i 2002 r. Khan zaczął regularnie odwiedzać londyński meczet w Finsbury Park, gdzie nawiązał kontakt z Al-Masrim i jego bliskim współpracownikiem Harunem Rashidem Aswatem, który odbył szkolenie wojskowe w Pakistanie i Afganistanie. Po powrocie do Londynu odpowiadał za rekrutację nowych członków. Khan osobiście wspierał rekrutację – a być może sam jej dokonał – Omara Sharifa i Asifa Hanify, którzy w kwietniu 2003 r. przeprowadzili samobójczy atak w Tel Awiwie. W lutym 2003 r. miał odwiedzić Izrael, prawdopodobnie po to, by przeprowadzić rekonesans przed tym zamachem[43].

Oficjalne życie towarzyskie Khana skupiało się wokół klubów młodzieżowych, muzułmańskiej księgarni i siłowni. Do 2003 r. zasiadał w komitecie zarządzającym jednego z takich klubów. Społeczna działalność Khana pozwoliła mu nawiązać bliskie kontakty z Tanweerem i Hussainem, dla których Khan, nazywany przez nich „Sidi", był mentorem.

[41] A. Wejkszner, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010, s. 346–347.

[42] *Report of the Official Account...*, s. 20.

[43] A. Wejkszner, *Ewolucja terroryzmu...*, s. 346; R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism...*, s. 213.

Praca z młodzieżą zaczęła ustępować miejsca nawiązywaniu kontaktów z islamskimi radykałami[44]. W 2003 r. Khan poznał Omara Khyama, Brytyjczyka pakistańskiego pochodzenia, który wcześniej podróżował do północnego Pakistanu, gdzie w obozie położonym w dystrykcie Malakand przeszedł przeszkolenie w zakresie produkcji bomb na bazie nawozów sztucznych. W tym samym roku obaj wyjechali do Pakistanu z grupą brytyjskich dżihadystów, prawdopodobnie również do Malakand. Po powrocie planowali kolejny wyjazd, ale Khan odłożył go ze względu na ciążę żony. W lutym i marcu 2004 r. Khan spotykał się wielokrotnie z Khyamem, który był obserwowany przez MI5. W kwietniu 2004 r. Khyam został aresztowany pod zarzutem kierowania spiskiem mającym na celu zdetonowanie w Londynie ładunku wybuchowego dużej mocy. Khan nie był podejrzanym w tej sprawie[45]. Zwolniono go jednak z pracy. Administracja szkoły uznała, że jego zwolnienie lekarskie od 20 września do 19 listopada 2004 r. nie miało podstaw. 19 listopada Khan wyjechał do Pakistanu[46].

Tanweer również mieszkał w Beeston. Pochodził z dobrze sytuowanej rodziny, był dobrym uczniem i utalentowanym sportowcem. Od najmłodszych lat poważnie traktował religię, ale nie wykazywał oznak ekstremizmu. W szkole został zapamiętany jako chłopiec spokojny, skromny i popularny wśród rówieśników. W wieku 16 lat stał się bardzo religijny. Sportowe zainteresowania rozwijał w Leeds Metropolitan University, gdzie po dwóch latach studiów otrzymał dyplom Higher National Diploma. W 2003 r. opuścił uczelnię i nie kontynuował nauki. Podczas studiów jeszcze bardziej zwrócił się w kierunku religii, której poświęcał coraz więcej czasu. To prawdopodobnie spowodowało, że porzucił uczelnię. Jeszcze w trakcie studiów uczęszczał do szkoły religijnej w Dewsbury. Nie zauważono jednak u niego oznak fanatyzmu religijnego, mimo że wielokrotnie pojawiał się w meczecie w Finsbury Park w towarzystwie Khana[47]. W kwietniu 2004 r. otrzymał ostrzeżenie za nieobyczajne zachowanie, ale poza tym nie miał kłopotów z policją. 19 listopada 2004 r. wyjechał do Pakistanu razem z Khanem, a po powrocie do Leeds nie pracował i był utrzymywany przez rodzinę.

Hussain mieszkał w dzielnicy Holbeck. Nie należał do wybitnych uczniów. W szkole był spokojny, nie miał wielu kolegów. Zaangażował się

[44] Tamże, s. 16.

[45] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism*..., s. 24–26.

[46] *Profile: Mohammad Sidique Khan*...

[47] A. Wejkszner, *Ewolucja terroryzmu*..., s. 346.

w protesty na tle rasowym, ale nie zwracał w nich uwagi agresywną postawą[48]. Na początku 2002 r. odbył wraz z rodziną tradycyjną pielgrzymkę do Mekki (hadżdż). Po powrocie zaczął manifestować swoją religijność. Nosił tradycyjną muzułmańską odzież i wychwalał Al-Kaidę, nazywając zamachowców z 11 września 2001 r. męczennikami. Swojemu nauczycielowi powiedział, że po skończeniu nauki chce zostać imamem. W 2004 r. został ukarany za kradzież w sklepie, ale poza tym incydentem nie miał problemów z policją. W 2005 r. uzyskał dyplom szkoły zawodowej na kierunku biznesu w South Leeds College[49].

Lindsay był outsiderem w grupie zamachowców. Urodził się na Jamajce w 1985 r., ojciec szybko ich opuścił. W następnym roku matka z synem i innym mężczyzną wyjechali do Wielkiej Brytanii. Zamieszkali w Huddersfield w Anglii. Jermaine uczęszczał do lokalnych szkół. Był popularny wśród rówieśników, inteligentny, uzdolniony artystycznie, muzycznie i sportowo. Trenował kickboxing i sztuki walki[50]. W 2000 r. matka Lindsaya przeszła na islam, a on uczynił to zaraz po niej, przyjmując imię Djamal. Konwersji na islam towarzyszyła zmiana środowiska, w którym często przebywał. Coraz więcej czasu spędzał w meczecie. W Huddersfield i sąsiednim Dewsbury podziwiano go za szybkość, z jaką osiągnął biegłość w języku arabskim i z jaką zapamiętywał duże fragmenty Koranu. Miał w tym czasie 15 lat. Mimo młodego wieku wykazywał się dojrzałością i powagą. Regularnie nosił długą arabską szatę (galabija)[51]. Uważa się, że duży wpływ na Lindsaya miał radykalny kaznodzieja Abdullah al-Faisal, również jamajskiego pochodzenia, współpracownik Al-Masriego, skazany w 2003 r., a następnie deportowany na Jamajkę za rozpowszechnianie materiałów propagandowych o charakterze ekstremistycznym, podżeganie do nienawiści rasowej i namawianie do zabijania „niewiernych"[52]. Jermaine został ukarany za rozdawanie w szkole ulotek popierających Al-Kaidę. W 2002 r. jego matka przeprowadziła się do USA, aby zamieszkać z trzecim z kolei partnerem, i zostawiła syna samego w rodzinnym domu. Wydarzenie to było dla niego traumatycznym przeżyciem. Opuścił szkołę i żył z zasiłku. Wykonywał przy tym dorywcze prace, m.in. sprzedawał telefony komórkowe i książki

[48] *Report of the Official Account...*, s. 15.

[49] Tamże.

[50] Tamże, s. 17.

[51] Tamże, s. 18.

[52] Tamże; R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism...*, s. 14–15.

o islamie[53]. Przez internet poznał Brytyjkę, Samanthę Lewthwaite, konwertytkę na islam, z którą uczestniczył w marszu „Stop the War" zorganizowanym w Londynie 30 października 2002 r. Pobrali się i zamieszkali w Huddersfield. Po zamknięciu meczetu w Finsbury Park w 2003 r. Lindsay i Tanweer odwiedzali Al-Masriego, gdy przed świątynią organizowano zgromadzenia z jego udziałem[54]. We wrześniu 2003 r. Lindsay przeprowadził się z żoną do Aylesbury, jednak dużo czasu spędzali w Huddersfield. Prawdopodobnie w drugiej połowie 2004 r. w Huddersfield lub Dewsbury Lindsay poznał Khana[55].

Przygotowania do ataku

Momentem przełomowym przygotowań do ataków terrorystycznych w Londynie był pobyt Khana i Tanweera w Pakistanie od 19 listopada 2004 r. do 8 lutego 2005 r. Wcześniej Khan podróżował tam sam lub w innym towarzystwie, a jego wyjazdy nie miały na celu odwiedzin rodziny. Tanweer poinformował rodzinę i znajomych, że jedzie do Pakistanu w celu poszerzenia wiedzy religijnej. Znajomi Khana uznali natomiast, że udaje się on do Pakistanu w celu przekroczenia granicy z Afganistanem, gdzie już wcześniej przebywał. W Pakistanie drogi obu mężczyzn się rozeszły. Tanweer zamieszkał u swojego wuja w Fajsalabadzie. Po tygodniu przyjechał po niego Khan i obaj udali się na północ. Tanweer poinformował rodzinę, że jadą w okolice Lahore zobaczyć jedną ze szkół religijnych[56]. Niewykluczone, że obaj pojechali do jednego z obozów szkoleniowych w Malakandzie, gdzie podczas wcześniejszej podróży Khan mógł nawiązać kontakty z Al-Kaidą. Jednym z jej przedstawicieli w Wielkiej Brytanii był Mohammed Kayyum Khan, który w lipcu 2003 r. zorganizował Khanowi podróż do obozu szkoleniowego w Malakandzie. Z kolei Tanweer nawiązał kontakty z organizacją Armia Muhammada (Dżaisz-e Mohammad)[57]. Wspomina się również, że obaj przeszli szkolenie w zakresie produkcji materiałów wybuchowych. Zorganizował je dla nich Rashid Rauf, obywatel brytyjski mieszkający

[53] *Report of the Official Account…*, s. 18.

[54] A. Wejkszner, *Ewolucja terroryzmu…*, s. 347.

[55] *Report of the Official Account…*, s. 18.

[56] Tamże, s. 20.

[57] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism…*, s. 213, 456.

w Pakistanie. Szkolenie to odbywało się w wynajętym domu w Islamabadzie, gdzie Khan i Tanweer nakręcili film na temat męczeństwa, który miał być opublikowany po ich śmierci[58]. Decyzja o przeprowadzeniu ataku w Londynie zapadła więc w Pakistanie. Tanweer twierdził, że nie znalazł tam odpowiedniej szkoły do nauki islamu[59].

Po powrocie Khan i Tanweer zaczęli wdrażać kluczowe elementy planu zamachu. Obaj zrezygnowali z pracy. Do działań włączyli Hussaina i Lindsaya. Od kwietnia 2005 r. mężczyźni spędzali ze sobą dużo czasu. W maju wynajęli mieszkanie przy ul. Alexandra Grove'a 18. W ten sposób znaleźli się z dala od dzielnicy Beeston, gdzie byli dobrze znani. W nowym miejscu nie rzucali się w oczy, ponieważ tę dzielnicę zamieszkiwali głównie studenci wynajmujący mieszkania. Obok znajdował się Wielki Meczet. Mieszkanie wynajął im Egipcjanin, Magdy Elnashar, którego w listopadzie 2004 r. Lindsay poznał w meczecie. W maju 2005 r. Elnashar obronił doktorat z chemii w Leeds Metropolitan University, a w czerwcu wyjechał na wakacje do kraju z zamiarem powrotu do Wielkiej Brytanii w celu kontynuowania pracy badawczej[60].

W wynajętym mieszkaniu zamachowcy przystąpili do konstruowania ładunku wybuchowego na bazie łatwo dostępnych i tanich substancji chemicznych. Aby nie budzić podejrzeń, kupowali je partiami. Pierwszego zakupu dokonali 31 marca 2005 r.[61] Można zatem przypuszczać, że zanim wynajęli mieszkanie, byli już w posiadaniu znacznej ilości środków chemicznych. Należały do nich aceton (rozpuszczalnik) i nadtlenek wodoru (wybielacz lub woda utleniona), kwas siarkowy lub solny i woda destylowana łączone w odpowiednich proporcjach. Otrzymuje się w ten sposób materiał wybuchowy w postaci proszku lub kryształków zwany TATP, od angielskiej nazwy: *triacetone triperoxide* (trimeryczny nadtlenek acetonu). Jest to substancja o potężnej sile wybuchu, niewiele mniejszej niż trotyl.

[58] *Shehzad Tanweer*, Counter Extremism Project, https://www.counterextremism.com/extremists/shehzad-tanweer [dostęp: 27 VI 2025].

[59] *Report of the Official Account...*, s. 20.

[60] *Chemistry student held in Cairo*, The Guardian, 15 VII 2005 r., https://www.theguardian.com/uk/2005/jul/15/july7.uksecurity10 [dostęp: 15 VII 2025]. Tydzień po atakach Magdy Elnashar został zatrzymany w Kairze. Początkowo uznano go za pomysłodawcę oraz inicjatora zamachów w Londynie lub twórcę grupy zamachowców. Ostatecznie egipskie władze oczyściły go z zarzutów i wypuściły na wolność w sierpniu 2005 r. Zob. X. Raufer, *Atlas radykalnego islamu...*, s. 93.

[61] *Report of the Official Account...*, s. 23.

TATP, powszechnie wykorzystywany przez terrorystów, zwany jest również „matką szatana". Próbował go zdetonować wspomniany Reid[62]. Z powodu uwalniania się duszących oparów chemicznych Tanweer i Lindsay musieli korzystać z masek i uchylać okna, co spowodowało obumarcie wierzchołków roślin znajdujących się na zewnątrz. Rozjaśnieniu uległy również włosy na głowach Tanweera i Hussaina, na co zwróciły uwagę ich rodziny kilka tygodni przed zamachem. Mężczyźni tłumaczyli, że jest to efekt działania chloru w basenie, w którym pływali w towarzystwie Khana. Wyprodukowany materiał wybuchowy został podzielony na cztery porcje o szacunkowej wadze od 2 do 5 kg i umieszczony w plecakach. Jest prawdopodobne, że grupa przeprowadziła eksplozję próbną, chociaż nie wiadomo, gdzie i kiedy do niej doszło[63].

Szacuje się, że koszt przygotowań do przeprowadzenia ataków wyniósł nie mniej niż 8000 funtów, wliczając w to podróże, wynajem samochodów i mieszkania oraz zakup środków chemicznych[64]. Wydaje się, że większość środków finansowych zapewnił Khan. Pracował trzy lata i założył kilka kont bankowych, na których deponował niewielkie kwoty na dłuższy czas i miał dobrą ocenę kredytową. Dzięki temu wziął pożyczkę w wysokości 10 000 funtów, jednak od marca 2005 r. zalegał z jej spłatą i miał debet na swoich kontach. Z kolei Lindsay dokonał kilku zakupów za pomocą czeków, których sprzedawcom nie udało się zrealizować[65].

28 czerwca trzech uczestników spisku (bez Hussaina) pojechało do Londynu identyczną trasą jak w dniu zamachu. Podobną podróż odbyli prawdopodobnie w połowie marca. Uważa się, że działali w sposób metodyczny i zdyscyplinowany, ostrożnie używali telefonów komórkowych oraz posługiwali się wypożyczonymi samochodami. Przypuszczano, że Khan mógł podejrzewać, iż jest inwigilowany, co wzmogło jego czujność[66].

W okresie przygotowań do ataków zmieniło się zachowanie Lindsaya. Stał się mniej religijny, nie modlił się z żoną, ogolił brodę i nosił ubrania

[62] G. Vince, *Explosives linked to London bombings identified*, New Scientist, 15 VII 2005 r., https://www.newscientist.com/article/dn7682-explosives-linked-to-london-bombings-identified/ [dostęp: 15 VII 2025]; P. Szymczak, *TATP, materiał wybuchowy zwany matką szatana. Czy można go wykryć?*, Focus.pl, 23 IX 2019 r., https://www.focus.pl/artykul/czy-tatp-materia-wybuchowy-zwany-matk-szatana-mona-wykry [dostęp: 23 VI 2025].

[63] *Report of the Official Account*..., s. 23.

[64] Tamże.

[65] Tamże.

[66] Tamże, s. 24.

w stylu zachodnim. Miał romans, ale utrzymywał też znajomości z innymi kobietami. Nawiązał kontakty z drobnymi przestępcami[67]. 27 maja uczestniczył w napadzie w Luton niedaleko Londynu, podczas którego użyto zarejestrowanego na niego samochodu. Lindsay nie został przesłuchany w tej sprawie przez policję[68]. Wydawał pieniądze na różne zakupy, które następnie wymieniał w internecie na materiały potrzebne do produkcji ładunków wybuchowych. Spędzał coraz mniej czasu w domu, a gdy w nim przebywał, zamykał się z komputerem w pokoju. Na krótko przed atakiem żona skonfrontowała go z wiadomościami od dziewczyny, które odkryła w jego telefonie. Poprosiła, żeby opuścił dom, co uczynił[69].

Hussain w kilkudniowym okresie poprzedzającym zamach często wychodził z domu. 4 lipca powiedział matce, że w ciągu najbliższych dni pojedzie do Londynu. Dwa dni później stwierdził, że jego podróż do stolicy została odłożona z powodu awarii samochodu, ale musi wyjechać tego wieczoru w inne miejsce. Około godziny 15.30 jego szwagierka zauważyła, że szykuje się do wyjścia. To był ostatni raz, kiedy widziała go rodzina[70].

Z kolei Tanweer 4 lipca poszedł odwiedzić dawnych przyjaciół ze szkoły. Następnego dnia poprosił matkę o przygotowanie torby na ubrania, ponieważ chce pojechać do Manchesteru, aby odwiedzić szkołę muzułmańską. 6 lipca do późnego wieczora grał w krykieta w lokalnym parku. Gdy wrócił do domu, powiedział, że zgubił telefon komórkowy. Ostatni raz widziano go w domu tuż po godzinie 23.00. Przypuszcza się, że wyszedł wkrótce potem[71].

Przebieg ataku

W dniu 7 lipca 2005 r. o godz. 5.07 Lindsay przyjechał z Leeds do Luton Fiatem Brava. Zatrzymał się na parkingu przy stacji kolejowej. Wszedł do środka i sprawdził rozkład jazdy. Następnie kilkakrotnie zmienił miejsce parkowania. O godz. 6.49 obok samochodu Lindsaya zatrzymał się Nissan Micra, z którego wysiedli Khan, Tanweer i Hussain. Mężczyźni założyli

[67] Tamże.

[68] Intelligence and Security Committee, *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c153540f0b61a825d6582/7-7_attacks_intelligence.pdf, s. 17 [dostęp: 23 VI 2025].

[69] Tamże, s. 24–25.

[70] Tamże, s. 25.

[71] Tamże.

duże plecaki i udali się na stację. Wyglądali jak turyści wybierający się na wycieczkę. O godz. 7.15 weszli na stację i skierowali się do bramek biletowych. W bilety zaopatrzyli się już wcześniej. Udali się na peron, gdzie ok. 20 minut czekali na pociąg do stacji King's Cross. Wyglądali na zrelaksowanych. Skład odjechał z peronu o godz. 7.40. Pociąg przyjechał do King's Cross o 8.23. Siedem minut później mężczyźni byli widziani w holu stacji, gdy obejmowali się przed rozstaniem. Każdy z nich udał się do metra[72]. Tanweer wsiadł do składu nr 204 linii Circle Line jadącego na wschód, Khan – do kolejki tej samej linii, zmierzającej w przeciwnym kierunku, a Lindsay do składu Piccadilly Line jadącego na południe. Hussain zmierzał do przystanku metra tej samej linii. O godz. 8.50 pociąg, którym jechał Tanweer, zatrzymał się na zatłoczonym peronie stacji Liverpool Street. Terrorysta siedział w drugim wagonie z przodu. Plecak znajdował się na podłodze przy jego nogach. Kilka sekund po odjeździe z peronu do stacji Aldgate doszło do eksplozji. Zginęło 8 osób, w tym sprawca, a 171 zostało rannych[73]. W ciągu minuty wybuchła bomba w drugim wagonie składu nr 216 odjeżdżającego ze stacji Edgware Road do stacji Paddington, którym jechał Khan. Śmierć poniosło 7 osób, a 163 zostało rannych. Eksplozja trzeciej bomby nastąpiła ok. dwie minuty po pierwszej, gdy skład nr 311 Piccadilly Line, którym jechał Lindsay, zbliżał się do stacji Russell Square. Bomba wybuchła w zatłoczonym pierwszym wagonie, w związku z tym liczba ofiar była największa. Zginęło 27 osób, a 340 zostało rannych[74].

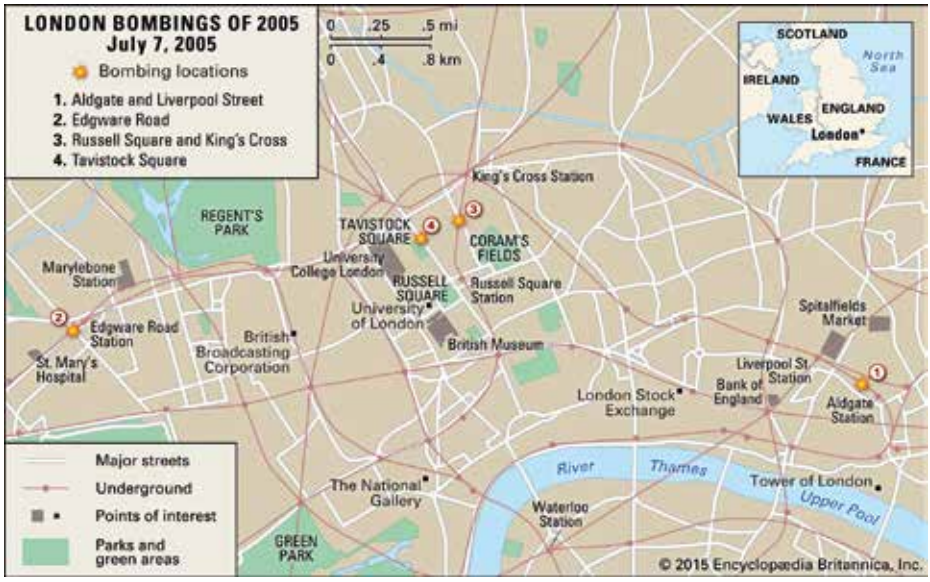
O godz. 8.55 Hussain wysiadł z metra Piccadilly Line na stacji Euston Road, gdzie przez kilka minut próbował bezskutecznie skontaktować się przez telefon komórkowy z pozostałymi zamachowcami. Następnie wrócił na stację King's Cross, gdzie kupił baterię 9 V, być może do zdetonowania ładunku. O godz. 9.06 wszedł do restauracji McDonald's na Eauston Road, którą opuścił po ok. 10 minutach. O godz. 9.19 był widziany w autobusie linii 91 jadącym z King's Cross do Eauston Station. Wyraźnie zdenerwowany przeciskał się między pasażerami. Na Eauston Station przesiadł się do autobusu linii 30 jadącego z Marble Arch na wschód. Pojazd był zatłoczony z powodu zamknięcia metra po wcześniejszych zamachach. Zajął miejsce na górnym pokładzie z tyłu, umieścił plecak na podłodze między stopami i coś w nim „majstrował". O godz. 9.47, kiedy autobus znajdował się

[72] *Report of the Official Account…*, s. 2–4.

[73] Tamże, s. 5.

[74] Tamże.

na Tavistock Square, zdetonował bombę, która zabiła 14 osób, w tym jego samego, i raniła ponad 110 (rysunek 1)[75].



Rysunek 1. Lokalizacja ataków terrorystycznych z 7 lipca 2005 r. w Londynie.

Źródło: M. Ray, *London bombings of 2005*, Britannica, https://www.britannica.com/event/London-bombings-of-2005 [dostęp: 12 VII 2025].

Do eksplozji w autobusie doszło w pobliżu siedziby Brytyjskiego Stowarzyszenia Medycznego (British Medical Association), z którego wybiegli lekarze, aby ratować rannych. Nie wiadomo, dlaczego terrorysta nie zdetonował ładunku o godz. 8.50, jak pozostali sprawcy. Być może powodem była niesprawna bateria, którą musiał wymienić[76]. Atak w Londynie nastąpił w czasie, kiedy w hotelu Gleneagles w Szkocji odbywał się szczyt państw G8 oraz dzień po decyzji Międzynarodowego Komitetu Olimpijskiego o przyznaniu Londynowi organizacji letnich igrzysk olimpijskich w 2012 r.[77]

[75] Tamże, s. 5–6.

[76] Tamże, s. 6; *Report of the 7 July Review Committee*, https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/archives/assembly-reports-7july-report.pdf, s. 37 [dostęp: 20 VI 2025].

[77] M. Phythian, *Intelligence, Policy-Making and the 7 July 2005 London Bombings*, „Crime, Law & Social Change" 2005, t. 44, nr 4–5, s. 362. https://doi.org/10.1007/s10611-006-9027-3.

O godz. 8.51 pod numer alarmowy 999 zostało przekazane pierwsze zgłoszenie przez pracownika metra ze stacji Aldgate. W tym samym czasie London Ambulance Service otrzymało zgłoszenie i wysłało karetkę na stację Liverpool Street. Pierwszy samochód strażacki dotarł do Aldgate o godz. 9.00 i w tym samym czasie wysyłano kolejne zespoły strażackie i ratownicze. Do działań przystąpili funkcjonariusze z British Transport Police, którzy poprosili o pomoc Policję Metropolitalną (Metropolitan Police Service). Sytuacja była jednak bardzo trudna. Po eksplozjach pasażerowie zostali pogrążeni w ciemnościach. Zgasły wewnętrzne światła wagonów i przestała działać wewnętrzna komunikacja między maszynistą i pasażerami. Z metra na powierzchnię wydobywał się dym. Utrata zasilania na niektórych odcinkach metra początkowo doprowadziła Centrum Kontroli Sieci Londyńskiego Metra (London Underground Network Control Centre) do wniosku, że w sieci wystąpiły skoki napięcia i na ten scenariusz zaczęto reagować. Niedługo potem centrum odebrało telefon z informacją, że na stacji Edgware Road doszło do wypadku. Podejrzewano wówczas, że pociąg uderzył w ścianę tunelu, a na torach znajdował się pasażer[78]. O 9.15 stało się jasne, że doszło do eksplozji, chociaż przyczyna i dokładne miejsce zdarzenia pozostawały nieznane. Na wczesnym etapie służby ratunkowe i policyjne działały chaotycznie, ponieważ nie było wiadomo, co się stało. Pasażerowie nie mogli skontaktować się z maszynistami, a ci z centralą, ponieważ przez pierwsze pół godziny po zamachu nie działała łączność. Początkowo służby ratunkowe wezwano do siedmiu miejsc. Przez pewien czas uważano, że doszło do pięciu oddzielnych incydentów w metrze. Mimo sprzecznych informacji Policja Metropolitalna uznała, że sytuacja jest poważna, bez określenia jej przyczyn[79]. O godz. 9.30 zostało uruchomione krajowe centrum kryzysowe. Pół godziny później jego posiedzeniu przewodniczył minister spraw wewnętrznych Charles Clarke. Wzięto pod uwagę możliwość dokonania ataku terrorystycznego, co o godz. 10.55 potwierdził szef ministerstwa spraw wewnętrznych. Poinformował przedstawicieli służb, że wybuchy spowodowały dużo ofiar, a także zawieszenie działania transportu publicznego. Na tej samej odprawie Ian Blair, komisarz londyńskiej Policji Metropolitalnej, stwierdził, że sytuacja była bardzo zagmatwana, ale obecnie jest pod kontrolą[80].

[78] *Report of the 7 July Review Committee…*, s. 12, 25.

[79] Tamże, s. 13.

[80] *Report of the Official Account…*, s. 7.

Na miejsca zamachów wysłano 101 karetek pogotowia i 25 zespołów medycznych szybkiego reagowania, które udzielały natychmiastowej pomocy. Zawodziła jednak łączność z Royal London Hospital, do którego przewożono rannych, ponieważ wszystkie sieci telefoniczne były przeciążone.

W atakach zginęło 56 osób, w tym 4 zamachowców, 53 osoby zmarły natychmiast w wyniku eksplozji, jedna w drodze do szpitala, a dwie w szpitalu. Rannych zostało 775 osób. London Hospital przyjął 27 poważnie rannych i 167 osób mogących poruszać się o własnych siłach. Siedemnastu pacjentów przeszło operacje. Część osób przewieziono do innych szpitali[81]. Wśród ofiar były trzy Polki: Monika Suchocka (23 lata), Karolina Glueck (29 lat) oraz Anna Brandt (43 lata). Trzech innych Polaków zostało lekko rannych[82].

O godz. 11.15, podczas pierwszej tego dnia konferencji prasowej, komisarz Ian Blair poinformował, że doszło do sześciu eksplozji[83]. W południe premier Tony Blair, uczestniczący w szczycie G8 w Szkocji, wydał oświadczenie, że w Londynie doszło do serii ataków terrorystycznych, a przywódcy „ósemki" wyrazili swoje potępienie dla sprawców. O godz. 12.55 minister spraw wewnętrznych złożył oświadczenie w parlamencie, w którym poinformował, że doszło do czterech eksplozji. Wymienił ich miejsca oraz stwierdził, że sprawcy pozostają nieznani, a wskazać ich ma wszczęte śledztwo. Dodał, że nieprawdziwe informacje, które wcześniej przekazywano, wynikały z faktu, że eksplozje następowały w pociągach znajdujących się między stacjami, co spowodowało, że pasażerowie wychodzili z obu stacji metra. To stwarzało wrażenie, że na każdej z nich doszło do incydentu. W tym samym czasie, gdy minister Clarke przemawiał w parlamencie, w internecie opublikowano oświadczenie, w którym odpowiedzialność za atak wzięła Tajna Organizacja Grupy Al-Kaidy w Europie (The Secret Organisation of al-Qaida in Europe). Zagroziła ona również rządom innych krajów, które wysłały wojska do Afganistanu i Iraku[84]. O godz. 17.30 premier Blair, który wrócił do Londynu,

[81] K.L. Koenig, *Medical Consequences of the 2005 London Terrorist Bombings*, NEJM Journal Watch, 25 I 2007 r., https://www.jwatch.org/em200701260000006/2007/01/26/medical-consequences-2005-london-terrorist [dostęp: 26 VI 2025].

[82] B. Hołyst, *Terroryzm. Tom 1*, Warszawa 2009, s. 708.

[83] *Report of the 7 July Review Committee...*, s. 13.

[84] *Report of the Official Account...*, s. 7–8. W dniu 9 lipca do ataku w Londynie przyznała się, związana z Al-Kaidą organizacja Brygady Abu Hafsa al-Masriego, ta sama, która wzięła odpowiedzialność za atak w Madrycie 11 marca 2004 r. Zob. C. Johnston, *Tube blasts 'almost simultaneous'*, The Guardian, 9 VII 2005 r., https://www.theguardian.com/uk/2005/jul/09/july7.uksecurity12 [dostęp: 9 VII 2025].

udał się na spotkanie krajowego centrum kryzysowego odbywające się w Sali Konferencyjnej Gabinetu Ministrów (Cabinet Office Briefing Rooms). Złożył tam oświadczenie, w którym zapowiedział intensywne działania policji i służb bezpieczeństwa, aby pociągnąć winnych do odpowiedzialności. Jeszcze przed północą na stacji metra Aldgate odnaleziono karty członkowskie klubów aktywności fizycznej należące do Khana i Tanweera[85]. Rozpoczęło się żmudne dochodzenie dotyczące sprawców ataku.

Śledztwo w sprawie ataku i próba powtórzenia zamachu

Śledczy przeanalizowali nagrania z ponad 2500 kamer monitorujących londyńskie metro. Przełom w poszukiwaniach nastąpił, gdy natrafiono na nagranie ze stacji King's Cross przedstawiające czterech mężczyzn idących razem z dużymi plecakami. Te same osoby znajdowały się na materiale filmowym z kamer na stacji kolejowej w Luton. Na parkingu przed dworcem odnaleziono samochody Nissan Micra i Fiat Brava, którymi przyjechali terroryści. W pierwszym aucie znajdowało się kilka małych ładunków wybuchowych, których przeznaczenia nie udało się wyjaśnić, w drugim znaleziono pistolet[86]. W wyniku śledztwa odkryto różne nagrania. Jedno z nich zawierało wypowiedź Khana: *Jesteśmy w stanie wojny, a ja jestem żołnierzem. Teraz i ty zasmakujesz rzeczywistości tej sytuacji*[87]. Śledztwo wykazało, że w dniu zamachu terroryści wykonywali połączenia na telefon komórkowy należący do Haruna Rashida Aswata, jednego z najbliższych współpracowników Al-Masriego, uznanego za inicjatora ataku z 7 lipca. Aswata aresztowano 20 lipca 2005 r. w Zambii[88]. Tego samego dnia brytyjska prasa opublikowała informację o zidentyfikowaniu wszystkich ofiar ataku w Londynie. Na propozycję premiera Blaira zorganizowania międzynarodowej konferencji na temat zwalczania ekstremizmu islamskiego przywódcy brytyjskich muzułmanów zareagowali żądaniem niezależnego dochodzenia sądowego w sprawie motywów działania czterech zamachowców

[85] *Report of the Official Account*..., s. 8.

[86] B. Hołyst, *Terroryzm*..., s. 708; B. Levitt, *The True Story Behind Attack on London: Hunting the 7/7 Bombers*, Time, 1 VII 2025 r., https://time.com/7299329/attack-on-london-netflix-true-story/ [dostęp: 1 VII 2025].

[87] B. Levitt, *The True Story*... Tłumaczenia w tekście pochodzą od autora (dop. red.).

[88] A. Wejkszner, *Ewolucja terroryzmu*..., s. 346, 348.

samobójców, którzy zaatakowali Londyn. Ostrzegli również, że społeczność muzułmańska sama nie jest w stanie wyeliminować ekstremizmu[89].

21 lipca 2005 r. doszło do nieudanej próby przeprowadzenia kolejnych ataków. Czterech zamachowców: Yassin Omar, Mukhtar Ibrahim, Ramzi Mohammad i Hussain Osman próbowało zdetonować bomby na trzech stacjach londyńskiego metra (Oval, Shepherd's Bush i Warren Street) i w autobusie na Hackney Road. Żadna z nich nie wybuchła. W dwóch zadziałały tylko detonatory, nie doszło jednak do detonacji materiału wybuchowego, a trzecia nie została aktywowana. Jedna osoba została ranna. Zamachowcy uciekli z miejsca zdarzenia[90].

Następnego dnia na stacji metra Stockwell funkcjonariusze policji zastrzelili Jeana Charlesa de Menezesa (27 lat), obywatela Brazylii, od trzech lat mieszkającego w Wielkiej Brytanii. Był on ścigany przez policjantów ubranych po cywilnemu, ale się nie zatrzymał i wbiegł na stację metra. Został tam obezwładniony przez dwóch funkcjonariuszy, a trzeci oddał siedem strzałów do leżącego na podłodze mężczyzny. Nie był on terrorystą i nie miał też żadnego związku z zamachami z 21 lipca.

Po wydarzeniach z 7 lipca zmieniono wytyczne policji dotyczące zasad postępowania z osobami podejrzanymi o zamiar przeprowadzenia zamachu samobójczego. Funkcjonariuszom nakazano strzelanie w głowę, by wyeliminować możliwość zdetonowania bomby przez rannego terrorystę. Cała sprawa odbiła się na wizerunku brytyjskiej policji, a szef Policji Metropolitalnej Ian Blair podał się do dymisji[91].

Pod koniec lipca w Londynie zatrzymano Mohammada i Ibrahima. Trzeciego zamachowca, Omara, aresztowano w Birmingham (przebranego w kobiecą burkę), w Rzymie natomiast zatrzymano Osmana i odesłano go do Wielkiej Brytanii[92]. Zamachowcy byli imigrantami z państw Rogu Afryki (dwóch z Somalii, jeden z Etiopii i jeden z Erytrei). Do Wielkiej Brytanii przybyli w latach 90. XX w. i oczekiwali na przyznanie im obywatelstwa. Nie nawiązali kontaktów z pakistańskimi dżihadystami.

Nie udało się potwierdzić jakichkolwiek powiązań między grupami zamachowców z 7 i 21 lipca. Terroryści z 21 lipca mieli niedostateczną

[89] *All 56 dead identified in July 7 attacks*, NBC News, 20 VII 2005 r., https://www.nbcnews.com/id/wbna8642326 [dostęp: 20 VII 2025].

[90] A. Wejkszner, *Ewolucja terroryzmu...*, s. 349; X. Raufer, *Atlas radykalnego islamu...*, s. 93.

[91] *Policja nie odpowie za śmierć w metrze*, TVN24, 13 II 2009 r., https://tvn24.pl/swiat/policja-nie-odpowie-za-smierc-w-metrze-ra85753-ls3724956 [dostęp: 13 VII 2025].

[92] A. Wejkszner, *Ewolucja terroryzmu...*, s. 350.

wiedzę na temat wytwarzania materiałów wybuchowych, jednak byli równie zdeterminowani jak ich poprzednicy i mieli podobną motywację „śmierci męczeńskiej". Była nią odpowiedź na obecność wojsk państw zachodnich, w tym Wielkiej Brytanii, w Afganistanie i Iraku[93]. Zamachowcy zostali skazani za udział w spisku w celu dokonania masowych zabójstw i każdy z nich otrzymał wyrok co najmniej 40 lat więzienia[94].

2 sierpnia 2005 r. katarska telewizja Al-Dżazira wyemitowała wystąpienie Az-Zawahiriego. Zastępca Osamy bin Ladena stwierdził, że ataki z 7 lipca były odpowiedzią na przedłużającą się obecność sił Zachodu w Iraku i Afganistanie oraz początkiem wielkiego starcia, które Amerykanom będzie przypominało drugi Wietnam[95]. Zaoferował też państwom zachodnim zawieszenie broni, jeśli wycofają się z Bliskiego Wschodu i zmuszą Izrael do pokoju z Palestyńczykami. 1 września w nagraniu rozpowszechnionym przez tę samą stację telewizyjną uzasadniał zamachy w Londynie, oświadczając: *Naszymi celami są ziemie i interesy państw, które biorą udział w agresji przeciwko Palestynie, Irakowi, Afganistanowi*[96]. 25 września Az-Zawahiri jednoznacznie potwierdził odpowiedzialność Al-Kaidy za zamachy w Londynie:

> Bracia, rycerze jedności i bohaterowie operacji w Londynie, niech Allah was umieści w swoich rajskich ogrodach i przyjmie wasze dobre czyny. W ich testamentach znalazły się poważne lekcje dla muzułmanów z Pakistanu i Zachodu, dotyczące odrzucenia taghut [bożków] i determinacji mudżahedinów islamu […], aby zemścić się na krzyżowcach i Żydach za zbrodnie, które popełnili rękoma zanurzonymi w krwi narodu muzułmańskiego. Błogosławiony atak na Londyn należy do szeregu ataków, które Al-Kaida miała zaszczyt przeprowadzić przeciwko arogancji brytyjskich krzyżowców w odpowiedzi na trwającą od ponad stu lat agresję Wielkiej Brytanii przeciwko narodowi muzułmańskiemu, na historyczną zbrodnię, jaką było powstanie Izraela i przeciwko ciągłym zbrodniom Brytyjczyków w stosunku do muzułmanów w Afganistanie i Iraku[97].

[93] A. Wejkszner, *Ewolucja terroryzmu…*, s. 350; X. Raufer, *Atlas radykalnego islamu…*, s. 93–94.

[94] B. Levitt, *The True Story…*

[95] A. Wejkszner, *Ewolucja terroryzmu…*, s. 350.

[96] X. Raufer, *Atlas radykalnego islamu…*, s. 95.

[97] Tamże, s. 96.

6 lipca 2006 r., przed pierwszą rocznicą zamachów w Londynie, Al-Dżazira wyemitowała pośmiertny testament Tanweera. Terrorysta oświadczył, że przeprowadzona akcja (...) *to jedynie początek ataków, które będą kontynuowane i coraz silniejsze, aż wycofacie wasze oddziały z Afganistanu i Iraku*. Nagraniu wideo towarzyszyło przesłanie Az-Zawahiriego, który oświadczył, że Khan i Tanweer szkolili się w obozach Al-Kaidy[98].

22 marca 2007 r. w Londynie aresztowano, podczas próby wyjazdu do Pakistanu, Mohammada Shakila i Waheeda Alego. Tego samego dnia w Leeds został zatrzymany Sadeer Saleem. Postawiono im zarzuty udziału w spisku mającym na celu przygotowanie zamachów z 7 lipca 2005 r.[99] Aresztowane osoby dobrze znały wykonawców tego ataku, jednak nie udowodniono im udziału w komórce terrorystycznej Khana. W kwietniu 2009 r. zostali skazani na siedem lat więzienia za udział w szkoleniach wojskowych w Pakistanie i próbę wyjazdu na kolejne takie szkolenie[100].

Problemy bezpieczeństwa antyterrorystycznego Wielkiej Brytanii

Atak terrorystyczny w Londynie podał w wątpliwość skuteczność działania MI5. Brytyjskie służby nie uwzględniły w pełni zagrożenia ze strony ekstremistów muzułmańskich, ponieważ zakładały, że środowiska te są skutecznie spenetrowane. Trzy tygodnie przed zamachami z 7 lipca obniżono poziom zagrożenia terrorystycznego z poważnego do znacznego (z 4 na 3 w pięciostopniowej skali), a szefowie służb zapewniali, że kontrolują sytuację. Należy jednak przypomnieć, że dwaj zamachowcy z 7 lipca, Khan i Tanweer, oraz jeden z zamachowców z 21 lipca byli w zainteresowaniu brytyjskich służb już w 2004 r. Stwierdzono, że nie stanowią poważnego zagrożenia. Nie doceniono determinacji i operacyjnego zaangażowania komórki Khana[101]. Renomowane brytyjskie instytucje bezpieczeństwa

[98] Tamże.

[99] A. Wejkszner, *Ewolucja terroryzmu...*, s. 351.

[100] *British 7/7 suspects jailed for terrorism camp plans*, Reuters, 29 IV 2009 r., https://www.reuters.com/article/world/british-7-7-suspects-jailed-for-terrorism-camp-plans-idUSTRE53S5SV/ [dostęp: 29 VI 2025].

[101] F. Eliott, S. Goodchild, *7/7 one year on: Why did it happen? The big questions still need answers*, The Independent, 2 VII 2006 r., https://www.independent.co.uk/news/uk/crime/7-7-one-year-on-why-did-it-happen-the-big-questions-still-need-answers-406351.html [dostęp: 2 VII 2025]; B. Levitt, *The True Story*...

z olbrzymim doświadczeniem w walce z północnoirlandzkim terroryzmem, wzmocnione po 11 września 2001 r. finansowo, kadrowo i organizacyjnie, nie były w stanie nie tylko powstrzymać zamachowców, lecz także prawidłowo ocenić skali zagrożenia[102]. W ciągu dwóch tygodni druga, niezależna grupa terrorystów mogła przyjąć podobny sposób działania i tylko brak profesjonalizmu jej członków w produkcji ładunków wybuchowych uchronił Londyn przed kolejnymi ofiarami.

Wydarzenia z 2005 r. zwiększyły nastroje antymuzułmańskie wśród Brytyjczyków i spowodowały nienotowany wcześniej wzrost poczucia zagrożenia terrorystycznego. Mimo że przywódcy brytyjskiej społeczności muzułmańskiej natychmiast potępili działania zamachowców (kilku liderów wydało nawet fatwy – orzeczenia teologiczne, w których stwierdzali, że ataki są sprzeczne z islamem), nastąpił wzrost liczby przestępstw motywowanych nienawiścią. Ich ofiarą padli zarówno muzułmanie, jak i osoby, których napastnicy niesłusznie uznali za wyznawców islamu[103]. Doszło do kilku ataków na meczety, m.in. w Londynie, Glasgow, Manchesterze, Birmingham, South-on-Sea i Exeter[104]. Nasiliło się zjawisko islamofobii, propagowanej głównie przez organizacje i partie skrajnie prawicowe. Wzrost zagrożenia terrorystycznego spowodował włączenie do rządowej strategii CONTEST programu Prevent. Jego celem było zapobieganie zamachom przez rozpoznanie osób wyrażających ekstremistyczne poglądy. Program ten był stale poszerzany, a osoby uznane za niebezpieczne kwalifikowano do części programu zwanej Channel. Mimo że Prevent stosowano wobec wszystkich ekstremistów, w tym skrajnej prawicy, od początku był krytykowany przez organizacje muzułmańskie za stygmatyzację ich społeczności. Wyrażano nawet opinię, że jest głęboko islamofobiczny. Najbardziej kontrowersyjną częścią programu był obowiązek zgłaszania osób podejrzewanych o sprzyjanie radykalizmowi, mogącemu przerodzić się w terroryzm. Obowiązek ten został nałożony na szkoły, policję, służbę zdrowia,

[102] Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world*, https://www.statewatch.org/media/documents/news/2010/oct/uk-national-security-strategy-2008.pdf, s. 4–5 [dostęp: 14 VI 2025].

[103] *20 lat temu zamachowcy Al Kaidy dokonali zamachów bombowych w londyńskim metrze*, PAP, 7 VII 2025 r., https://www.pap.pl/aktualnosci/20-rocznica-zamachow-bombowych-w-londynie#:~:text=7%20lipca%202005%20r.,ofiar%20zamachu%20wynosi%C5%82%2034%20lata [dostęp: 7 VII 2025].

[104] M. Zawadewicz, *Życie codzienne*..., s. 138.

organizacje samorządowe i inne instytucje publiczne [105]. W kwietniu 2006 r. weszła w życie nowa ustawa antyterrorystyczna (*The Terrorism Act 2006*), definiująca i nakazująca ściganie takich przestępstw, jak: gloryfikowanie terroryzmu (pochwalania aktów terrorystycznych w nadziei, że zachęci to innych do ich dokonania), udział w szkoleniu terrorystycznym lub jego organizowanie, planowanie i przygotowanie aktu terrorystycznego oraz rozpowszechnianie publikacji o treści terrorystycznej[106]. Z inicjatywą wprowadzenia karalności gloryfikowania terroryzmu rząd wystąpił tuż po zamachach w Londynie. Miał to być jeden z elementów pakietu środków wymierzonych w muzułmańskich przywódców duchowych, takich jak Al-Masri, których premier Blair uznał za podżegaczy do nienawiści. Nowe prawo miało dać policji możliwość zatrzymania podejrzanego o terroryzm na dłuższy czas – do 28 dni zamiast dotychczasowych 14 (rząd początkowo proponował 90 dni). Przepis wszedł w życie 25 lipca 2006 r. Ustawę oprotestowali aktywiści na rzecz ochrony praw człowieka, twierdzący, że skutkiem uchwalenia tej ustawy będzie ograniczenie wolności słowa i swobody działania organizacji pozarządowych[107].

Nowe prawo nie powstrzymało ekstremistów islamskich przed wrogimi działaniami. Po delegalizacji przez ministerstwo spraw wewnętrznych jednego ugrupowania zakładano nowe o innej nazwie. Na przykład po wydaniu zakazu działalności w lipcu 2006 r. wspomnianych wcześniej Firkat an-Nadżija i Al-Ghuraba, Choudary założył internetową organizację Islam4UK. Kontynuowała ona ideologiczny przekaz Al-Muhadżirun, motywując młodych islamskich radykałów do wyjazdów na szkolenia do Pakistanu. 6 sierpnia 2006 r. policja poinformowała o wykryciu spisku terrorystycznego mającego na celu wysadzenie samolotów lecących z Wielkiej Brytanii do Stanów Zjednoczonych. Zatrzymano 20 Brytyjczyków pakistańskiego pochodzenia,

[105] *About Prevent*, Prevent Watch, https://www.preventwatch.org/about-prevent/ [dostęp: 23 VII 2025]; A. Safdar, *Prevent: UK anti-terror plan „harms children's rights"*, AlJazeera, 13 VII 2016 r., https://www.aljazeera.com/features/2016/7/13/prevent-uk-anti-terror-plan-harms-childrens-rights [dostęp: 13 VII 2025].

[106] Była to czwarta ustawa antyterrorystyczna po: *Terrorism Act 2000*, *The Anti-Terrorism, Crime and Security Act 2001* i *The Prevention of Terrorism Act 2005*. Zob. A. Kalicki, *Aspekty prawne w brytyjskim systemie zwalczania terroryzmu*, w: *Terroryzm. Materia ustawowa?*, K. Indecki, P. Potejko (red.), Warszawa 2009, s. 92–100.

[107] *W. Brytania: Nowa ustawa antyterrorystyczna weszła w życie*, Wirtualna Polska, 13 IV 2006 r., https://www.money.pl/archiwum/wiadomosciagencyjne/pap/artykul/w;brytania;nowa;ustawa;antyterrorystyczna;weszla;w;zycie,28,0,152348.html [dostęp: 13 IV 2006]; A. Kalicki, *Aspekty prawne w brytyjskim systemie...*, s. 95.

z których ośmiu oskarżono o przygotowanie spisku terrorystycznego. Odbyli oni szkolenie na pograniczu afgańsko-pakistańskim. Tam też powstał plan zamachów, a przywódca grupy Abdullah Ahmed Ali otrzymał szczegółowe instrukcje dotyczące ich realizacji. Zamachowcy zamierzali wysadzić samoloty nad Atlantykiem za pomocą płynnych ładunków wybuchowych ukrytych w butelkach po napojach orzeźwiających. Od momentu ujawnienia planów tych zamachów na lotniskach wprowadzono zaostrzone rygory bezpieczeństwa, zakazujące wnoszenia płynów na pokłady samolotów[108]. W listopadzie 2006 r. dyrektor MI5 Eliza Manningham-Buller oświadczyła, że służby kontrolują 200 grup liczących ponad 1600 osób (głównie Brytyjczyków obcego pochodzenia), zaangażowanych w planowanie bądź wspieranie ataków terrorystycznych w Wielkiej Brytanii lub za granicą[109].

Pomimo zdecydowanych działań brytyjskich władz po 2005 r. strukturom terrorystycznym udało się zachować zdolności operacyjne. Potwierdzeniem tego był atak z 30 czerwca 2007 r. na lotnisko Glasgow. Nieco wcześniej, w styczniu 2007 r., brytyjskiej policji udało się udaremnić porwanie i zabicie brytyjskiego żołnierza[110]. Działania antyterrorystyczne brytyjskich służb wymusiły utajnienie aktywności wielu komórek terrorystycznych[111]. Wciąż jednak tolerowano propagandową działalność ideologów dżihadu. We wrześniu 2008 r. z okazji siódmej rocznicy zamachów w USA Islam4UK ogłosił w mediach informację na temat konferencji „Kalifat dla Wielkiej Brytanii – Boża alternatywa". Zaproszenia i plakaty reklamujące to spotkanie przedstawiały mapę Wielkiej Brytanii z powiewającą nad nią czarną flagą islamu i umieszczonym napisem „Kalifat". Podczas zgromadzenia, w którym uczestniczyło ponad 100 osób, Choudary stwierdził, że siedem lat wcześniej Osama bin Laden udzielił Amerykanom lekcji, ale „krzyżowcy" niczego się nie nauczyli. Na Wyspach Brytyjskich dojdzie zatem do kolejnego 11 września. Może także nadejść kolejny 7 lipca. Lider Islam4UK oświadczył wówczas: *Nigdy nie zintegrujemy się z chrześcijaństwem. Zapewniamy, że pewnego dnia to wy przyjmiecie szariat. Nasze oczy skierowane są na Downing Street. To dlatego Brytyjczycy tak się nas obawiają. Nie jest problemem dla nas zadeklarować dżihad w Wielkiej Brytanii, a wówczas każdy*

[108] K. Izak, *Leksykon organizacji…*, s. 361.

[109] X. Raufer, *Atlas radykalnego islamu…*, s. 96.

[110] A. Wejkszner, *Ewolucja terroryzmu…*, s. 351.

[111] Tamże.

z nas może stać się bombą zegarową czekającą na detonację[112]. Kolejną osobą, która wystąpiła z mową przepełnioną nienawiścią, był Sajful Islam, szef organizacji Salaficka Młodzież dla Propagowania Islamu (Salafi Youth for Islamic Propagation). Wychwalał on Bin Ladena za odwagę i ostrzegł przed powtórzeniem wydarzeń sprzed siedmiu lat, stwierdzając m.in., że: *Winę za zamachy z 11 września ponosi rząd amerykański i nikt inny. To oni są terrorystami. Szejk Osama wielokrotnie ostrzegał Amerykę, wszystko z powodu ich arogancji, bo myśleli, że są supermocarstwem i nikt nie może im zagrozić, więc Osama bin Laden udzielił USA lekcji, której wciąż jeszcze nie pojęli*[113]. Odnosząc się do sytuacji w Iraku i Afganistanie, ostrzegł Stany Zjednoczone i Wielką Brytanię: *Obudźcie się. Wycofajcie się. Musicie powstrzymać przemoc, w przeciwnym razie następny 11 września będzie miał miejsce w Wielkiej Brytanii, także następny 7 lipca może rozegrać się tutaj*[114].

Aktywność ekstremistów muzułmańskich przyczyniła się do powstania w 2009 r. w Luton antymuzułmańskiej organizacji Angielska Liga Obrony (English Defence Ligue, EDL). Miasto to zamieszkują przede wszystkim potomkowie imigrantów, głównie z państw muzułmańskich. Żyją zgodnie z zasadami szariatu i tworzą równoległe społeczeństwo. Bezpośrednią przyczyną powstania EDL była próba zaatakowania przez zwolenników Choudary'ego uczestników odbywającej się w Luton uroczystości powitania żołnierzy Royal Anglican Regiment wracających z Afganistanu[115]. Organizacja została utworzona w środowisku subkultury kibiców piłkarskich. Stała się trwałym elementem brytyjskiego życia politycznego. Organizowała cykliczne demonstracje, które przyciągały od kilkuset do kilku tysięcy uczestników. Jej liczebność szacowano na 25 000–30 000 członków, co czyniło ją jednym z największych ulicznych ruchów protestu w Wielkiej Brytanii[116]. W przeciwieństwie do tradycyjnych brytyjskich

[112] R. Watson, *Al-Muhajiroun and the long tail of UK terror*, The New Statesman, 22 II 2020 r., https://www.newstatesman.com/long-reads/2020/02/al-muhajiroun-and-long-tail-uk-terror [dostęp: 22 VII 2025].

[113] *'Have more babies and Muslims can take over the UK', hate fanatic says, as warning comes that* '*next 9/11 will be in UK'*, Daily Mail, 13 IX 2008 r., https://www.dailymail.co.uk/news/article-1054909/Have-babies-Muslims-UK-hate-fanatic-says-warning-comes-9-11-UK.html [dostęp: 13 VII 2025].

[114] Tamże.

[115] J. Barlett, M. Littler, *Inside the EDL: Populist Politics in a Digital Age*, https://demos.co.uk/wp-content/uploads/2011/10/Inside_the_edl_WEB.pdf, s. 10 [dostęp: 10 IX 2025].

[116] K. Jaskułowski, *Głośni i dumni: etnografia Angielskiej Ligi Obrony*, „Prace Etnograficzne" 2017, t. 45, z. 1, s. 117.

partii skrajnie prawicowych (takich jak Front Narodowy – National Front czy Brytyjska Partia Narodowa – British National Party) EDL nie odwoływała się w oficjalnych deklaracjach do ideologii antyimigranckiej i rasistowskiej, lecz głosiła, że występuje jedynie przeciwko islamowi. Liga postrzegała go nie tyle jako jedną z religii brytyjskiego społeczeństwa, ile jako agresywną i ekspansywną polityczną ideologię, która zagraża prawom człowieka i demokracji. Za obowiązek uważała konieczność moralnego wspierania brytyjskich oddziałów na Bliskim Wschodzie. Na tym tle często dochodziło do starć z muzułmanami protestującymi przeciwko obecności brytyjskich żołnierzy w Iraku i Afganistanie[117].

W styczniu 2010 r. Islam4UK ogłosiła zorganizowanie marszu „pustych trumien" na ulicach miasta Royal Wootton Bassett, do którego przywożono zwłoki brytyjskich żołnierzy zmarłych w Afganistanie. Krewni, przyjaciele poległych i mieszkańcy ustawiali się wzdłuż ulic, kiedy przykryte flagą trumny przewożono na katafalkach. Choudary oskarżył żołnierzy o popełnianie morderstw i zamieścił w internecie list otwarty zatytułowany *Do rodzin brytyjskich żołnierzy, którzy polegli lub obecnie przebywają w Afganistanie*, podający przyczyny zorganizowania marszu. Jego zapowiedź wywołała falę protestów[118]. Zmusiło to władze do zdelegalizowania ugrupowania Islam4UK. Decyzja weszła w życie 14 stycznia 2010 r.[119] Groźba kary więzienia nie wpłynęła na zmianę charakteru wypowiedzi Choudary'ego, który konsekwentnie głosił ekstremistyczną propagandę. Założył stronę internetową Muzułmanie przeciwko Krzyżowcom (Muslims Against Crusades, MAC). Nazwy tej używano także w odniesieniu do jego zwolenników. Korzystając z możliwości dostępu do mediów społecznościowych, Choudary docierał ze swoimi poglądami do rzesz muzułmanów i wpływał na poziom ich radykalizacji[120]. 11 września 2011 r. sympatycy MAC zorganizowali obok ambasady USA w Londynie manifestację z okazji 10. rocznicy ataku w USA. Doszło do

[117] Tamże.

[118] *Fury over British Muslim cleric's anti-war march threat*, CNN, 5 I 2010 r., https://edition.cnn.com/2010/WORLD/europe/01/04/britain.afghanistan.demo/index.html [dostęp: 5 I 2010].

[119] D. Orr, *Is the Islam4UK ban a blow against democracy?*, The Guardian, 14 I 2010 r., https://www.theguardian.com/commentisfree/2010/jan/14/deborah-orr-islam4uk [dostęp: 14 VII 2025].

[120] C. Gammell, *Muslims Against Crusades earn notoriety in less than a year*, The Telegraph, 21 IV 2011 r., https://www.telegraph.co.uk/news/8461436/Muslims-Against-Crusades-earn-notoriety-in-less-than-a-year.html [dostęp: 21 VI 2025].

starć z EDL[121]. Tego samego dnia aresztowano w Birmingham 11 brytyjskich muzułmanów przygotowujących w tym mieście atak terrorystyczny przy użyciu ośmiu bomb umieszczonych w plecakach. Część z nich odbyła przeszkolenie w obozach Al-Kaidy na pograniczu afgańsko-pakistańskim. Terroryści zamierzali przekształcić Birmingham w strefę małej wojny. Przywódca grupy Irfan Naseer (31 lat) został skazany na karę dożywotniego więzienia, a dwóch jego najbliższych współpracowników: Irfan Khalid (28 lat) i Ashik Ali (28 lat) – odpowiednio 23 i 20 lat pozbawienia wolności. Członkowie grupy znajdowali się pod ideologicznym wpływem Choudary'ego[122].

10 listopada 2011 r. brytyjskie ministerstwo spraw wewnętrznych podjęło decyzję o delegalizacji MAC. Była to 48. ekstremistyczna organizacja zdelegalizowana w Wielkiej Brytanii na mocy ustawy antyterrorystycznej i ustawy zabraniającej gloryfikacji terroryzmu. Zakaz działalności oznaczał prawo do zajęcia przez władze aktywów ugrupowania i uznanie członkostwa w organizacji za podlegające karze do 10 lat pozbawienia wolności. W wydanym oświadczeniu Choudary uznał delegalizację MAC za przejaw nienawiści brytyjskiego rządu do muzułmanów[123]. W miejsce MAC powstała organizacja Zjednoczona Umma (United Ummah), która 2 grudnia 2011 r. zorganizowała w Londynie demonstrację przeciwko nalotom amerykańskich samolotów bezzałogowych na kraje muzułmańskie[124].

22 maja 2013 r. dwóch Brytyjczyków nigeryjskiego pochodzenia: Michael Adebolayo (28 lat) i Michael Adebowale (22 lata) zabiło w londyńskiej dzielnicy Woolwich brytyjskiego żołnierza Lee Rigby'ego. Przechodzący przez ulicę mężczyzna został najpierw potrącony przez samochód, a następnie sprawcy usiłowali obciąć mu głowę, wznosząc okrzyki „Allah Akbar". Jego zwłoki przeciągnęli na środek ulicy, by przechodnie mogli je widzieć. Sprawcy nie zbiegli z miejsca zbrodni. W oczekiwaniu na policję rozmawiali z postronnymi osobami i próbowali im wyjaśniać swoje poglądy. Adebolayo wykrzyczał m.in.: *Przysięgamy na wszechmogącego Allaha, że nigdy nie przestaniemy z wami walczyć. Zabiliśmy tego mężczyznę tylko dlatego, że muzułmanie codziennie giną z rąk brytyjskich żołnierzy. Oko za oko,*

[121] D. Casciani, *Muslims Against Crusades banned by Theresa May*, BBC News, 10 XI 2011 r., https://www.bbc.com/news/uk-15678275 [dostęp: 10 XI 2025].

[122] *Wielka Brytania: 11 skazanych za planowanie zamachów w Birmingham*, Wirtualna Polska, 26 IV 2013 r., https://wiadomosci.wp.pl/wielka-brytania-11-skazanych-za-planowanie-zamachow-w-birmingham-6082107866088065a [dostęp: 26 VII 2025].

[123] D. Casciani, *Muslims Against Crusades*...

[124] K. Izak, *Leksykon organizacji*..., s. 365.

ząb za ząb[125]. Po przybyciu na miejsce policjantów mężczyźni próbowali ich zaatakować. Liczyli na to, że zostaną zabici i staną się męczennikami. Zostali zranieni. Adebolayo i Adebowale pochodzili z katolickich rodzin nigeryjskich imigrantów, ale w Wielkiej Brytanii przeszli na islam i się zradykalizowali[126]. Ten mord doprowadził do największej od ponad 30 lat społecznej mobilizacji, która objęła niemal cały kraj. Antymuzułmańskie demonstracje odbyły się w wielu miastach. W odpowiedzi na te wydarzenia premier David Cameron wypowiedział wojnę radykalizacji i ekstremizmowi. Bardziej stanowcze słowa skierował do EDL i BNP, twierdząc, że nie będzie tolerował prawicowej islamofobii. Zapowiedział też utworzenie specjalnej grupy roboczej TERFOR, której celem miało być zwalczanie ekstremistów[127]. Te obietnice nie zostały spełnione. Zaostrzono kurs wobec skrajnej prawicy, ale tolerowano ekstremistów islamskich i aktywistów oskarżających Brytyjczyków o islamofobię i rasizm.

Pojawiało się coraz więcej opinii, że służby specjalne mogły zapobiec zamachowi z 22 maja 2013 r., podobnie jak atakom w Londynie osiem lat wcześniej. Adebolayo był bowiem znany służbom już w 2010 r., kiedy w Somalii zamierzał przyłączyć się do zbrojnej organizacji Ruch Młodych Mudżahedinów (Harakat asz-Szabab al-Mudżahidin). Został jednak aresztowany w Kenii i odesłany do Wielkiej Brytanii[128]. Brytyjskie służby nie objęły go nadzorem i nie postawiły przed sądem, co powinny zrobić na mocy ustawy z 2006 r., w której za przestępstwo uznano podróż lub zamiar podróży za granicę z planem przyłączenia się do organizacji terrorystycznej lub przeprowadzenia zamachu. Podobnie wyglądała sytuacja z Adebowale, który był wcześniej obserwowany. Okazało się również, że obaj zamachowcy kierowali się nauczaniem Choudary'ego, który pozostawał na wolności i głosił mowę nienawiści[129]. Aresztowano go dopiero po złożeniu przez niego deklaracji wierności Państwu Islamskiemu w lipcu 2014 r. Dwa lata później został skazany na pięć i pół roku pozbawienia wolności, zamiast grożących mu dziesięciu lat. Wyrok uznający go za winnego poprzedziło śledztwo, które kosztowało miliony funtów. Wykazało ono, że jego nazwisko

[125] *Dożywocie i 45 lat więzienia dla „rzeźników z Londynu" za zabójstwo żołnierza*, TVN24, 26 II 2014 r., https://tvn24.pl/swiat/dozywocie-i-45-lat-wiezienia-dla-rzeznikow-z-londynu-za-zabojstwo-zolnierza-ra402449-ls3352033 [dostęp: 26 VII 2025].

[126] Tamże.

[127] G. Kayzer, *Radykałowie na celowniku*, „Gazeta Polska Codziennie", 29 V 2013 r.

[128] Tamże.

[129] Tamże; P. Falkowski, *Niespokojny Londyn*, „Nasz Dziennik", 3 VI 2013 r.

przewijało się przy większości ataków terrorystycznych w Wielkiej Brytanii. Miał on zainspirować do zamachów terrorystycznych ponad 100 obywateli Zjednoczonego Królestwa, a prawdopodobnie co czwarty z ponad 900 brytyjskich dżihadystów wyjechał walczyć w szeregach Państwa Islamskiego pod wpływem tego, co głosił ich mentor[130]. Inne dane statystyczne zostały zawarte w raporcie organizacji non profit Counter Extremism Project (CEP) pt. *Anjem Choudary's Ties to Extremist* (pol. Powiązania Anjema Choudary'ego z ekstremistami). Wymieniono w nim 33 organizacje i 112 osób, na które Choudary wywierał wpływ lub z którymi się komunikował w trakcie swojej kariery. Spośród nich 20 dokonało ataków terrorystycznych, 50 próbowało ich dokonać, 19 dołączyło lub próbowało dołączyć do Państwa Islamskiego w Syrii, a inni propagowali treści dżihadystyczne i rekrutowali do organizacji terrorystycznych[131].

Aktywność sieci dżihadystycznych w Wielkiej Brytanii kontynuowało Państwo Islamskie. Zamierzało ono przeprowadzić atak dla uczczenia pamięci sprawców zamachów w 2005 r. W 2015 r. wykryto jeden taki spisek, w następnym roku kolejny, a trzy w 2017 r.[132] Niestety, był to rok, w którym

[130] M.R. Chehab, *Kim jest Anjem Choudary, mentor ostatniego zamachowca z Londynu?*, Newsweek, 8 XII 2019 r., https://www.newsweek.pl/swiat/po-zamachu-w-londynie-kim-jest-anjem-choudary/n0plx7f [dostęp: 8 XI 2025].

[131] *Anjem Choudary's Ties to Extremist*, Counter Extremism Project, https://www.counterextremism.com/anjem-choudary-ties-to-extremists [dostęp: 23 X 2025]. Choudary odsiedział mniej niż połowę wyroku, reszta miała odbywać się pod ścisłym nadzorem, ale mimo to kontynuował swoją propagandową i agitacyjną aktywność. W 2019 r. zainicjował odrodzenie organizacji Al-Muhadżirun. Za pośrednictwem mediów społecznościowych prowadził nauczanie swoich zwolenników w USA i Kanadzie. Zaangażował się w działalność organizacji Stowarzyszenie Muzułmańskich Myślicieli (Islamic Thinkers Society) propagującej radykalne idee. Pod tą nazwą kryła się Al-Muhadżirun. Jego bliskim współpracownikiem w Kanadzie był Khaled Hussain, reprezentujący nowe pokolenie uczniów Choudary'ego, propagujący go w Ameryce Północnej. 17 lipca 2023 r., po przylocie Hussaina do Londynu w celu spotkania z Choudarym, obaj mężczyźni zostali aresztowani. 30 lipca 2024 r. Choudary'yego skazano na karę dożywotniego więzienia z możliwością jego opuszczenia po 28 latach, Khaled Hussein natomiast otrzymał wyrok 5 lat pozbawienia wolności. Zob. *International counter terrorism investigation leads to Anjem Choudary conviction*, Counter Terrorism Policing, 23 VII 2024 r., https://www.counterterrorism.police.uk/historic-met-and-international-police-counter-terrorism-investigation-leads-to-anjem-choudary-terror-conviction/ [dostęp: 23 VII 2025]; *CPS statement: Convictions of Anjem Choudary and Khaled Hussein*, Crown Prosecution Service, 31 VII 2024 r., https://www.cps.gov.uk/cps/news/cps-statement-convictions-anjem-choudary-and-khaled-hussein [dostęp: 31 VII 2025].

[132] A. Wejkszner, *Europejska armia kalifatu. Tom I. Centrum supersieci*, Warszawa 2020, s. 234–235.

doszło do trzech zamachów: w Londynie 22 marca (zginęło 6 osób, a co najmniej 49 zostało rannych)[133] i 3 czerwca (zginęło 8 osób, a ponad 40 zostało rannych)[134] oraz w Manchesterze 22 maja (zginęły 22 osoby, a 118 zostało rannych). Sprawcą tego ostatniego był Salman Ramadan Abedi, który zdetonował bombę umieszczoną w plecaku w momencie, gdy uczestnicy opuszczali salę po zakończeniu koncertu amerykańskiej piosenkarki Ariany Grande[135].

Urodzony w Wielkiej Brytanii Usman Khan (28 lat) zaatakował nożem przechodniów. Do zdarzenia doszło 29 listopada 2019 r. w okolicach Mostu Londyńskiego.. Zabił dwie osoby i ranił trzy inne. Napastnika próbowali powstrzymać świadkowie zdarzenia, w tym Polak Łukasz Koczocik, który został ranny. Terrorystę zastrzeliła policja. Jego idolem i mentorem był Choudary. Do zamachu przyznało się Państwo Islamskie. W 2010 r. Khan, działający pod pseudonimem Abu Saif, został aresztowany wraz z ośmioma innymi ekstremistami[136]. Przygotowywali oni serię zamachów, w tym na parlament, giełdę londyńską, ambasadę USA, mieszkanie ówczesnego burmistrza Londynu Borisa Johnsona i katedrę św. Pawła[137]. W 2012 r. Khan został skazany na 16 lat więzienia. Zwolniono go warunkowo. Następnego dnia po zamachu premier Boris Johnson skrytykował praktykę warunkowego wypuszczania terrorystów. Stwierdził, że gdyby Khan nie został przedterminowo zwolniony, nie przeprowadziłby ataku. Poinformował również, że w ramach zwolnienia warunkowego na wolności znajdują się 74 osoby skazane za terroryzm[138].

Dnia 15 października 2021 r. w Londynie obywatel brytyjski Ali Harbi Ali (26 lat) zabił nożem konserwatywnego polityka Davida Amessa. Zabójca pozostawał pod wpływem Choudary'ego. Eksperci poddali wówczas krytyce program Prevent, którego realizacja pochłonęła miliony funtów, a mimo to jego cel nie został osiągnięty. Wskazano, że przyczyn porażki należy szukać m.in. w paraliżowaniu programu przez duchownych muzułmańskich

[133] Tamże, s. 237.

[134] Tamże, s. 246.

[135] Tamże, s. 240, 243.

[136] M.R. Chehab, *Kim jest Anjem Choudary*...

[137] Tamże.

[138] *„Przygotowywał działalność terrorystyczną". Mężczyzna zatrzymany*, TVN24, 2 XII 2019 r., https://tvn24.pl/swiat/wielka-brytania-policja-zatrzymala-mezczyzne-podejrzanego-o-terroryzm-ra989867-ls2508450 [dostęp: 2 X 2025].

i działaczy społecznych oraz w nieustannym krytykowaniu go przez przedstawicieli opozycji[139].

29 lipca 2024 r. Axel Rudakubana (17 lat), Brytyjczyk rwandyjskiego pochodzenia, zabił nożem trzy dziewczynki uczestniczące w kursie tańca. Zranił również dziewięcioro innych dzieci i jedną osobę dorosłą, po czym został ujęty. Atak nastąpił w miasteczku Southport niedaleko Liverpoolu. Po zdarzeniu doszło do kilkudniowych antyimigranckich i antymuzułmańskich protestów i zamieszek w wielu brytyjskich miastach. Miały miejsce starcia z policjantami, zaatakowano posterunek policji i hotel dla nielegalnych imigrantów oczekujących na azyl[140].

Podsumowanie

Po ataku terrorystycznym Al-Kaidy w Londynie 7 lipca 2005 r. rząd Tony'ego Blaira podjął działania mające na celu poprawę bezpieczeństwa wewnętrznego i ochronę obywateli przed atakami ekstremistów. Te działania były jednak ograniczane z powodu sprzeciwu organizacji muzułmańskich i aktywistów obrony praw człowieka. Zwolennicy twardego kursu wobec ekstremizmu islamskiego krytykowali brytyjską praktykę tzw. czujnej tolerancji, która umożliwiała wielu radykalnym imamom nawoływanie do szerzenia nienawiści i stosowania przemocy. Brytyjskie władze podkreślały jednak, że strategia polegająca na koncentrowaniu się na środkach nadzoru i kontroli osób podejrzewanych o działalność terrorystyczną daje lepsze wyniki niż ich osadzanie w więzieniu, ponieważ pozwalała uzyskać informacje wywiadowcze[141]. W opinii niektórych ekspertów źródłem przedkładania prawa przestępców ponad bezpieczeństwo Brytyjczyków była ustawa o prawach człowieka (*Human Rights Act*), która w 1998 r. włączyła do brytyjskiego prawa regulacje zawarte w Europejskiej Konwencji Praw Człowieka.

[139] V. Dodd, *Ali Harbi Ali guilty of murdering MP David Amess in terrorist attack*, The Guardian, 11 IV 2022 r., https://www.theguardian.com/uk-news/2022/apr/11/david-amess-verdict-terrorist-attack-ali-harbi-ali-guilty [dostęp: 11 VI 2025].

[140] M. Czarnecki, *Po ataku nożownika w Southport rozruchy rozlały się na kolejne brytyjskie miasta. Aresztowano ponad 90 osób*, wyborcza.pl, 4 VIII 2024 r., https://wyborcza.pl/7,75399,31200497,po-ataku-nozownika-w-southport-rozruchy-rozlaly-sie-na-kolejne.html [dostęp: 4 VIII 2025].

[141] G. Wilk-Jakubowski, *Sytuacja społeczna muzułmanów w Wielkiej Brytanii*, Kraków 2013, s. 153.

Dosłownie interpretowane przepisy zezwalały na udzielanie azylu w Wielkiej Brytanii obcokrajowcom ściganym w ich krajach za przestępstwa, ponieważ mogliby tam być narażeni na „nieludzkie lub poniżające traktowanie”[142]. Na podstawie tego prawa oraz Rezolucji A/HRC/22/L.40 Rady Praw Człowieka ONZ, przyjętej w marcu 2013 r., za karaną islamofobię mogą uchodzić słowa najmniejszej krytyki skierowane w stronę mniejszości muzułmańskich, łącznie z określeniem „terroryzm islamski”[143].

Ta strategia się nie sprawdziła, a władze w końcu zostały zmuszone do aresztowania osób nawołujących do przemocy. Upłynęły jednak kolejne lata, zanim udało się je wydalić z kraju. Al-Masriego ekstradowano do USA dopiero w październiku 2012 r.[144], Abu Katadę przekazano Jordanii w lipcu 2013 r. Amman musiał jednak zapewnić, że wobec Abu Katady, którego wcześniej zaocznie skazano na dożywotnie więzienie za udział w przygotowaniu dwóch zamachów w stolicy Jordanii w 1999 r. i 2000 r., nie będą stosowane tortury w celu wymuszenia zeznań. Obaj po usłyszeniu niekorzystnych dla siebie wyroków odwoływali się do sądów wyższej instancji i Europejskiego Trybunału Praw Człowieka[145]. W ich obronie stawały

[142] A. Pearson, *Allison Pearson: We must get rid of the dreadful Human Rights Act*, The Telegraph, 13 V 2015 r., https://www.telegraph.co.uk/news/uknews/law-and-order/11602222/Allison-Pearson-We-must-get-rid-of-the-dreadful-Human-Rights-Act.html [dostęp: 13 VI 2025].

[143] W rezolucji tej stwierdza się, że terroryzm we wszystkich jego formach i przejawach nie może być powiązany z żadną religią, narodowością czy grupą etniczną. To by oznaczało, że nie istnieje terroryzm palestyński, baskijski, korsykański, tamilski, muzułmański i wiele innych. Większość organizacji terrorystycznych jednak miała i ma w swoich nazwach odniesienia do określeń etniczno-narodowych i religijnych. Przedstawiciel UE w ONZ potępił przepisy zawarte w dokumencie, odwołując się jednocześnie do międzynarodowego poparcia dla wolności słowa: „(…) Ameryka jest nadal ostatnim bastionem wolności słowa, ale jest jasne, że nawet tutaj zjeżdżamy po równi pochyłej w stronę upadku swobodnej wypowiedzi. To smutne i przerażające. Mam nadzieję, że ludzie obudzą się, ponieważ po cichu im się tę wolność odbiera, podczas gdy wielu z nich żyje w przekonaniu, że zawsze będą ją mieli”. Zob. D. Weiss, *If You Criticize Islam, You Will Suffer Consequences*, Citizen Times, 13 VII 2014 r., http://www.citizentimes.eu/2013/06/13/if-you-criticize-islam-you-will-suffer-consequences/ [dostęp: 13 VIII 2024].

[144] *Ekstradycja Abu Hamzy do USA wstrzymana przez apelację*, Wirtualna Polska, 26 IX 2012 r., https://wiadomosci.wp.pl/ekstradycja-abu-hamzy-do-usa-wstrzymana-przez-apelacje-6082120547132033a [dostęp: 26 IX 2025].

[145] *Wydalony z Wielkiej Brytanii Abu Katada, oskarżony o terroryzm*, Wirtualna Polska, 7 VII 2013 r., https://wiadomosci.wp.pl/wydalony-z-wielkiej-brytanii-abu-katada-oskarzony-o-terroryzm-6031568274154113a [dostęp: 7 VII 2025]. We wrześniu 2014 r. sąd wojskowy w Jordanii ostatecznie uwolnił Abu Katadę od zarzutów działalności terrorystycznej mającej polegać na planowaniu ataków na Amerykanów i Izraelczyków i wypuścił go

międzynarodowe organizacje humanitarne, mimo że nawoływali do nienawiści, a Al-Masri organizował ataki terrorystyczne w Jemenie.

W Wielkiej Brytanii wobec muzułmanów nadal stosowano jednak politykę ustępstw i przywilejów. Nadawano im uprawnienia kosztem innych grup społecznych. Specjalny status zwalniał ich od przestrzegania norm, za których naruszenie członkom innych grup społecznych groziły sankcje. Pozwolono na stosowanie szariatu w sprawach cywilnych (m.in. małżeństwa i kwestie spadkowe). Program wspierania wielokulturowości zakładał powstrzymanie niezadowolenia wśród przybyszów, przede wszystkim z krajów muzułmańskich, i osłabienia ich krytycznego stosunku do nowej ojczyzny. Te założenia całkowicie zawiodły, a przyjazna polityka kolejnych rządów doprowadziła do wzrostu ekstremizmu islamskiego[146]. Ta sytuacja pogłębiła się po wielkiej fali migracyjnej w 2015 r. Brytyjska policja ukrywała przed opinią publiczną przestępstwa popełniane przez mniejszości muzułmańskie. Strach przed oskarżeniem o rasizm doprowadzał do paraliżu działań służb bezpieczeństwa. W Wielkiej Brytanii muzułmańskie gangi przez 10 lat wykorzystały seksualnie ok. 1400 brytyjskich dziewcząt, a policja tych danych nie upubliczniała. Kiedy sprawa wyszła na jaw, w raporcie napisano m.in., że powodem zaniechania działań, wyciszania i bagatelizowania przestępstw była obawa organów ścigania przed zarzutami o rasizm i politycznymi konsekwencjami zwrócenia się rdzennych Brytyjczyków przeciwko mniejszości etnicznej[147].

Wątpliwa wydaje się skuteczność programów deradykalizacyjnych ze względu na brak możliwości realnej oceny, czy ktoś złagodził swoje poglądy. Stwierdzenie takiej osoby, że porzuciła swoje idee, może być kłamstwem. Trudno jest także prognozować jej dalsze zachowanie. Pozorowanie zmiany postępowania może być sposobem na odwrócenie uwagi służb bezpieczeństwa. Na przykład Usman Khan, terrorysta z 29 listopada 2019 r., przed warunkowym zwolnieniem z więzienia zapewniał, że jest dobrym muzułmaninem i dobrym obywatelem brytyjskim, a jego zaangażowanie w planowanie zamachów było przejawem niedojrzałości[148]. Na wolności trafił do

na wolność. Zob. *Oskarżony o planowanie masakry niewinny. Abu Katada na wolności*, TVN24, 24 IX 2014 r., https://tvn24.pl/swiat/oskarzony-o-planowanie-masakry-niewinny-abu-katada-na-wolnosci-ra471293-ls3412841 [dostęp: 24 IX 2025].

146 G. Wilk-Jakubowski, *Sytuacja społeczna muzułmanów*..., s. 152–153.

147 G. Drymer, *Afery seksualne w Wielkiej Brytanii. Gwałty muzułmańskich gangów*, Rzeczpospolita, 1 X 2017 r., https://www.rp.pl/spoleczenstwo/art2411491-afery-seksualne-w-wielkiej-brytanii-gwalty-muzulmanskich-gangow [dostęp: 8 X 2025].

148 M.R. Chehab, *Kim jest Anjem Choudary*...

programu Learning Together, którego celem jest eliminowanie uprzedzeń do innych osób. Ofiarami Khana, które zostały śmiertelnie ranione nożem, byli koordynator tego programu i jego wolontariuszka. Nie sprawdziły się obowiązkowe programy deradykalizacyjne dla terrorystów opuszczających więzienia. W prywatnych rozmowach przyznawali, że nie zmienili swoich przekonań i że dla nich walka o państwo islamskie wciąż trwa[149].

8 października 2024 r. szef MI5, Ken McCallum, poinformował w publicznym wystąpieniu, że od 2017 r. jego służba i policja udaremniły 43 ataki terrorystyczne[150]. Zagrożenie terrorystyczne w Wielkiej Brytanii utrzymuje się na trzecim poziomie (zagrożenie znaczne) w pięciostopniowej skali, co oznacza, że atak jest prawdopodobny. Zgodnie z rządowymi ocenami zagrożenie to jest „trwałe i ewoluujące", a przy tym „mniej przewidywalne i trudniejsze do wykrycia i zbadania"[151]. Towarzyszy temu niepokój społeczny. Trzy czwarte brytyjskiego społeczeństwa postrzega ekstremistów muzułmańskich jako największe zagrożenie dla kraju[152].

Bibliografia

Besson S., *Islamizacja Zachodu? Historia pewnego spisku*, Warszawa 2006.

Chaliand G., Blin A., *Historia terroryzmu. Od starożytności do Da'isz*, Warszawa 2020.

Falkowski P., *Niespokojny Londyn*, „Nasz Dziennik", 3 VI 2013 r.

Hołyst B., *Terroryzm. Tom 1*, Warszawa 2009.

Izak K., *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014.

Jaskułowski K., *Głośni i dumni: etnografia Angielskiej Ligi Obrony*, „Prace Etnograficzne" 2017, t. 45, z. 1, s. 117–121.

[149] Tamże.

[150] *Director General Ken McCallum gives latest threat update*, Security Service MI5, 8 X 2024 r., https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update [dostęp: 8 X 2025].

[151] Tamże.

[152] M. Smith, *Which extremists do Britons see as threats in 2024?*, YouGov, 29 II 2024 r., https://yougov.co.uk/politics/articles/48784-which-extremists-do-britons-see-as-threats-in-2024 [dostęp: 29 VII 2025].

Kalicki A., *Aspekty prawne w brytyjskim systemie zwalczania terroryzmu*, w: *Terroryzm. Materia ustawowa?*, K. Indecki, P. Potejko (red.), Warszawa 2009, s. 92–100.

Kayzer G., *Radykałowie na celowniku*, „Gazeta Polska Codziennie", 29 V 2013 r.

Kepel G., *Fitna, wojna w sercu islamu*, Warszawa 2006.

Levitt M., *Hamas. Polityka, dobroczynność i terroryzm w służbie dżihadu*, Kraków 2008.

Mansfield L., *His Own Words: Translation and Analysis of the Writings of Dr. Ayman Al Zawahiri*, New York 2006.

Phillips M., *Londonistan. Jak Wielka Brytania stworzyła państwo terroru*, Warszawa 2010.

Phythian M., *Intelligence, Policy-Making and the 7 July 2005 London Bombings*, „Crime, Law & Social Change" 2005, t. 44, nr 4–5, s. 361–385. https://doi.org/10.1007/s10611-006-9027-3.

Raufer X., *Atlas radykalnego islamu*, Warszawa 2011.

Simcox R., Stuart H., Ahmed H., *Islamist Terrorism. The British Connections*, London 2010.

Wejkszner A., *Europejska armia kalifatu. Tom I. Centrum supersieci*, Warszawa 2020.

Wejkszner A., *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010.

Wilk-Jakubowski G., *Sytuacja społeczna muzułmanów w Wielkiej Brytanii*, Kraków 2013.

Zawadewicz M., *Życie codzienne w muzułmańskim Londynie*, Warszawa 2008.

Źródła internetowe

20 lat temu zamachowcy Al Kaidy dokonali zamachów bombowych w londyńskim metrze, PAP, 7 VII 2025 r., https://www.pap.pl/aktualnosci/20-rocznica-zamachow-bombowych-w-londynie#:~:text=7%20lipca%202005%20r.,ofiar%20 zamachu%20wynosi%C5%82%2034%20lata [dostęp: 7 VII 2025].

About Prevent, Prevent Watch, https://www.preventwatch.org/about-prevent/ [dostęp: 23 VII 2025].

Abu Hamza profile, BBC News, 9 I 2015 r., https://www.bbc.com/news/uk-11701269 [dostęp: 18 XI 2025].

Al-Qaeda plotter jailed for life, BBC News, 7 XI 2006 r., http://news.bbc.co.uk/2/hi/uk_news/6123236.stm [dostęp: 7 VIII 2025].

All 56 dead identified in July 7 attacks, NBC News, 20 VII 2005 r., https://www.nbcnews.com/id/wbna8642326 [dostęp: 20 VII 2025].

Anjem Choudary's Ties to Extremist, Counter Extremism Project, https://www.counterextremism.com/anjem-choudary-ties-to-extremists [dostęp: 23 X 2025].

Barlett J., Littler M., *Inside the EDL: Populist Politics in a Digital Age,* https://demos.co.uk/wp-content/uploads/2011/10/Inside_the_edl_WEB.pdf [dostęp: 10 IX 2025].

British 7/7 suspects jailed for terrorism camp plans, Reuters, 29 IV 2009 r., https://www.reuters.com/article/world/british-7-7-suspects-jailed-for-terrorism-camp-plans-idUSTRE53S5SV/ [dostęp: 29 VI 2025].

Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world,* https://www.statewatch.org/media/documents/news/2010/oct/uk-national-security-strategy-2008.pdf [dostęp: 14 VI 2025].

Casciani D., *Muslims Against Crusades banned by Theresa May,* BBC News, 10 XI 2011 r., https://www.bbc.com/news/uk-15678275 [dostęp: 10 XI 2025].

Chehab M.R., *Kim jest Anjem Choudary, mentor ostatniego zamachowca z Londynu?,* Newsweek, 8 XII 2019 r., https://www.newsweek.pl/swiat/po-zamachu-w-londynie-kim-jest-anjem-choudary/n0plx7f [dostęp: 8 XI 2025].

Chemistry student held in Cairo, The Guardian, 15 VII 2005 r., https://www.theguardian.com/uk/2005/jul/15/july7.uksecurity10 [dostęp: 15 VII 2025].

CPS statement: Convictions of Anjem Choudary and Khaled Hussein, Crown Prosecution Service, 31 VII 2024 r., https://www.cps.gov.uk/cps/news/cps-statement-convictions-anjem-choudary-and-khaled-hussein [dostęp: 31 VII 2025].

Czarnecki M., *Po ataku nożownika w Southport rozruchy rozlały się na kolejne brytyjskie miasta. Aresztowano ponad 90 osób,* wyborcza.pl, 4 VIII 2024 r., https://wyborcza.pl/7,75399,31200497,po-ataku-nozownika-w-southport-rozruchy-rozlaly-sie-na-kolejne.html [dostęp: 4 VIII 2025].

Director General Ken McCallum gives latest threat update, Security Service MI5, 8 X 2024 r., https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update [dostęp: 8 X 2025].

Dodd V., *Ali Harbi Ali guilty of murdering MP David Amess in terrorist attack*, The Guardian, 11 IV 2022 r., https://www.theguardian.com/uk-news/2022/apr/11/david-amess-verdict-terrorist-attack-ali-harbi-ali-guilty [dostęp: 11 VI 2025].

Dożywocie i 45 lat więzienia dla „rzeźników z Londynu" za zabójstwo żołnierza, TVN24, 26 II 2014 r., https://tvn24.pl/swiat/dozywocie-i-45-lat-wiezienia-dla-rzeznikow-z-londynu-za-zabojstwo-zolnierza-ra402449-ls3352033 [dostęp: 26 VII 2025].

Drymer G., *Afery seksualne w Wielkiej Brytanii. Gwałty muzułmańskich gangów*, Rzeczpospolita, 1 X 2017 r., https://www.rp.pl/spoleczenstwo/art2411491-afery-seksualne-w-wielkiej-brytanii-gwalty-muzulmanskich-gangow [dostęp: 8 X 2025].

Ekstradycja Abu Hamzy do USA wstrzymana przez apelację, Wirtualna Polska, 26 IX 2012 r., https://wiadomosci.wp.pl/ekstradycja-abu-hamzy-do-usa-wstrzymana-przez-apelacje-6082120547132033a [dostęp: 26 IX 2025].

Eliott F., Goodchild S., *7/7 one year on: Why did it happen? The big questions still need answers*, The Independent, 2 VII 2006 r., https://www.independent.co.uk/news/uk/crime/7-7-one-year-on-why-did-it-happen-the-big-questions-still-need-answers-406351.html [dostęp: 2 VII 2025].

Fury over British Muslim cleric's anti-war march threat, CNN, 5 I 2010 r., https://edition.cnn.com/2010/WORLD/europe/01/04/britain.afghanistan.demo/index.html [dostęp: 5 I 2010].

Gammell C., *Muslims Against Crusades earn notoriety in less than a year*, The Telegraph, 21 IV 2011 r., https://www.telegraph.co.uk/news/8461436/Muslims-Against-Crusades-earn-notoriety-in-less-than-a-year.html [dostęp: 21 VI 2025].

Gilliam J., *Why They Hate Us. An Examination of al-wala' wa-l-bara' in Salafi-Jihadist Ideology*, Military Review, 15 II 2018 r., https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/ Feb/They-Hate/ [dostęp: 15 VII 2025].

'Have more babies and Muslims can take over the UK' hate fanatic says, as warning comes that 'next 9/11 will be in UK', Daily Mail, 13 IX 2008 r., https://www.dailymail.co.uk/news/article-1054909/Have-babies-Muslims-UK-hate-fanatic-says-warning-comes-9-11-UK.html [dostęp: 13 VII 2025].

Hoge W., *Threats and Responses: Terror Suspects, Mosque Raid in London Results in 7 Arrests in Connection With Discovery of Poison*, The New York Times, 21 I 2003 r., https://www.nytimes.com/2003/01/21/world/threats-responses-terror-suspects-mosque-raid-london-results-7-arrests.html [dostęp: 18 IX 2025].

Intelligence and Security Committee, *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c153540f0b61a825d6582/7-7_attacks_intelligence.pdf [dostęp: 23 VI 2025].

Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c470140f0b62dffde1050/isc_terrorist_attacks_7july_report.pdf [dostęp: 18 XI 2025].

International counter terrorism investigation leads to Anjem Choudary conviction, Counter Terrorism Policing, 23 VII 2024 r., https://www.counterterrorism.police.uk/historic-met-and-international-police-counter-terrorism-investigation-leads-to-anjem-choudary-terror-conviction/ [dostęp: 23 VII 2024].

Johnston C., *Tube blasts 'almost simultaneous'*, The Guardian, 9 VII 2005 r., https://www.theguardian.com/uk/2005/jul/09/july7.uksecurity12 [dostęp: 9 VII 2025].

Koenig K.L., *Medical Consequences of the 2005 London Terrorist Bombings*, NEJM Journal Watch, 25 I 2007 r., https://www.jwatch.org/em200701260000006/2007/01/26/medical-consequences-2005-london-terrorist [dostęp: 26 VI 2025].

Levitt B., *The True Story Behind Attack on London: Hunting the 7/7 Bombers*, Time, 1 VII 2025 r., https://time.com/7299329/attack-on-london-netflix-true-story/ [dostęp: 1 VII 2025].

„Magnificent 19" risks further outrage, The Standard, 13 IV 2012 r., https://www.standard.co.uk/hp/front/magnificent-19-risks-further-outrage-6948639.html [dostęp: 18 XI 2025].

Marsden C., *Britain: Why did it take so long to bring Abu Hamza to trial?*, World Socialist Web Site, 16 II 2006 r., https://www.wsws.org/en/articles/2006/02/hamz-f16.html [dostęp: 16 VII 2025].

Orr D., *Is the Islam4UK ban a blow against democracy?*, The Guardian, 14 I 2010 r., https://www.theguardian.com/commentisfree/2010/jan/14/deborah-orr-islam4uk [dostęp: 14 VII 2025].

Oskarżony o planowanie masakry niewinny. Abu Katada na wolności, TVN24, 24 IX 2014 r., https://tvn24.pl/swiat/oskarzony-o-planowanie-masakry-niewinny-abu-katada-na-wolnosci-ra471293-ls3412841 [dostęp: 24 IX 2025].

Owen P., *Clarke rejects Hamza inquiry calls*, The Guardian, 9 II 2006 r., https://www.theguardian.com/uk/2006/feb/09/terrorism.politics [dostęp: 18 IX 2025].

Pearson A., *Allison Pearson: We must get rid of the dreadful Human Rights Act,* The Telegraph, 13 V 2015 r., https://www.telegraph.co.uk/news/uknews/law-and-order/11602222/Allison-Pearson-We-must-get-rid-of-the-dreadful-Human-Rights-Act.html [dostęp: 13 VI 2025].

Policja nie odpowie za śmierć w metrze, TVN24, 13 II 2009 r., https://tvn24.pl/swiat/policja-nie-odpowie-za-smierc-w-metrze-ra85753-ls3724956 [dostęp: 13 VII 2025].

Profile: Mohammad Sidique Khan, BBC News, 2 III 2011 r., https://www.bbc.com/news/uk-12621381 [dostęp: 2 VI 2025].

„Przygotowywał działalność terrorystyczną". Mężczyzna zatrzymany, TVN24, 2 XII 2019 r., https://tvn24.pl/swiat/wielka-brytania-policja-zatrzymala-mezczyzne-podejrzanego-o-terroryzm-ra989867-ls2508450 [dostęp: 2 X 2025].

Radical cleric Abu Hamza jailed for life by US court, BBC News, 9 I 2015 r., https://www.bbc.com/news/world-us-canada-30754959 [dostęp: 18 IX 2025].

Ray M., *London bombings of 2005,* Britannica, https://www.britannica.com/event/London-bombings-of-2005 [dostęp: 12 VII 2025].

Report of the 7 July Review Committee, https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/archives/assembly-reports-7july-report.pdf [dostęp: 20 VI 2025].

Report of the Official Account of the Bombings in London on 7th July 2005, https://assets.publishing.service.gov.uk/media/5a7c7bc840f0b626628ac62e/1087.pdf [dostęp: 7 VII 2025].

Safdar A., *Prevent: UK anti-terror plan „harms children's rights",* AlJazeera, 13 VII 2016 r., https://www.aljazeera.com/features/2016/7/13/prevent-uk-anti-terror-plan-harms-childrens-rights [dostęp: 13 VII 2025].

Shehzad Tanweer, Counter Extremism Project, https://www.counterextremism.com/extremists/shehzad-tanweer [dostęp: 27 VI 2025].

Shishani M.B., *Salafi-Jihadists Geopolitical Perspective of Central Asia,* Central Asia – Caucasus Analist, https://www.cacianalyst.org/publications/analytical-articles/item/10050-analytical-articles-caci-analyst-2005-6-29-art.-10050.html [dostęp: 29 VI 2025].

Smith M., *Which extremists do Britons see as threats in 2024?,* YouGov, 29 II 2024 r., https://yougov.co.uk/politics/articles/48784-which-extremists-do-britons-see-as-threats-in-2024 [dostęp: 29 VII 2025].

Strieff D., *Terror-tinged U.K. mosque gets a makeover*, NBC News, 5 VII 2006 r., https://www.nbcnews.com/id/wbna13501930 [dostęp: 18 IX 2025].

Szymczak P., *TATP, materiał wybuchowy zwany matką szatana. Czy można go wykryć?*, Focus.pl, 23 IX 2019 r., https://www.focus.pl/artykul/czy-tatp-materia-wybuchowy-zwany-matk-szatana-mona-wykry [dostęp: 23 VI 2025].

Terror Watch: What Ricin?, Newsweek, 12 IV 2005 r., https://www.newsweek.com/terror-watch-what-ricin-116577 [dostęp: 18 IX 2025].

Terrorism threat levels, Security Service MI5, https://www.mi5.gov.uk/threats-and-advice/terrorism-threat-levels [dostęp: 23 VI 2025].

Vencat E.F., *'Bleed the Enemy'*, Newsweek, 11 I 2006 r., https://www.newsweek.com/bleed-enemy-108227 [dostęp: 11 VII 2025].

Vince G., *Explosives linked to London bombings identified*, New Scientist, 15 VII 2005 r., https://www.newscientist.com/article/dn7682-explosives-linked-to-london-bombings-identified/ [dostęp: 15 VII 2025].

W. Brytania: Nowa ustawa antyterrorystyczna weszła w życie, Wirtualna Polska, 13 IV 2006 r., https://www.money.pl/archiwum/wiadomosciagencyjne/pap/artykul/w;brytania;nowa;ustawa;antyterrorystyczna;weszla;w;zycie,28,0,152348.html [dostęp: 13 IV 2006].

Watson R., *Al-Muhajiroun and the long tail of UK terror*, The New Statesman, 22 II 2020 r., https://www.newstatesman.com/long-reads/2020/02/al-muhajiroun-and-long-tail-uk-terror [dostęp: 22 VII 2025].

Weiss D., *If You Criticize Islam, You Will Suffer Consequences*, Citizen Times, 13 VII 2014 r., http://www.citizentimes.eu/2013/06/13/if-you-criticize-islam-you-will-suffer-consequences/ [dostęp: 13 VIII 2024].

Whine M., *The Penetration of Islamist Ideology in Britain*, Hudson Institute, 18 V 2005 r., https://www.hudson.org/national-security-defense/the-penetration-of-islamist-ideology-in-britain [dostęp: 18 XI 2025].

Wielka Brytania: 11 skazanych za planowanie zamachów w Birmingham, Wirtualna Polska, 26 IV 2013 r., https://wiadomosci.wp.pl/wielka-brytania-11-skazanych-za-planowanie-zamachow-w-birmingham-6082107866088065a [dostęp: 26 VII 2025].

Wydalony z Wielkiej Brytanii Abu Katada, oskarżony o terroryzm, Wirtualna Polska, 7 VII 2013 r., https://www.money.pl/archiwum/wiadomosci_agencyjne/pap/artykul/jordania;wydalony;z;wielkiej;brytanii;abu;katada;oskarzony;o;terroryzm,241,0,1341681.html [dostęp: 7 VII 2025].

Artykuł wyraża poglądy autora i nie reprezentuje stanowiska Agencji Bezpieczeństwa Wewnętrznego.

Krzysztof Izak

Emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego, pełniący służbę m.in. w pionach realizujących zadania w zakresie przeciwdziałania zagrożeniom terrorystycznym. Autor ponad 20 artykułów o tematyce terrorystycznej, które ukazały się na łamach wielu czasopism naukowych. Twórca *Leksykonu organizacji i ruchów islamistycznych* wydanego przez ABW.

Kontakt: lizior3@wp.pl

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 101–124

https://doi.org/10.4467/27204383TER.25.047.23034

Artykuł

Zagrożenia terrorystyczne w Unii Europejskiej w 2024 roku. Analiza „TE-SAT. European Union Terrorism Situation and Trend Report 2025"

Terrorist threat in the European Union in 2024. Analysis of the EU Terrorism Situation and Trend Report 2025

SEBASTIAN WOJCIECHOWSKI https://orcid.org/0000-0002-7972-6618
Uniwersytet im. Adama Mickiewicza w Poznaniu
Instytut Zachodni w Poznaniu

ARTUR WEJKSZNER https://orcid.org/0000-0002-7638-9708
Uniwersytet im. Adama Mickiewicza w Poznaniu

Abstrakt

Autorzy artykułu dokonali analizy zagrożeń terrorystycznych w Unii Europejskiej w 2024 r. na podstawie danych zawartych w raporcie Europolu pt. *TE-SAT. European Union Terrorism Situation and Trend Report 2025* oraz scharakteryzowali je z uwzględnieniem danych dotyczących poszczególnych państw UE. Pod uwagę został wzięty zarówno aspekt przedmiotowy tych zagrożeń (ze strony grup dżihadystycznych, prawicowych, lewicowych i anarchistycznych, etnonacjonalistycznych i separatystycznych oraz innych), jak i ilościowy (np. liczba ataków i osób aresztowanych z powodu terroryzmu). Z danych zawartych w raporcie wynika, że w 2024 r. w UE zmniejszyła się liczba ataków terrorystycznych w porównaniu z 2023 r. (z 120 do 58), ale jednocześnie zwiększyła się liczba państw członkowskich UE (z 7 do 14), w których doszło do ataków. Wzrosła również liczba ataków o charakterze dżihadystycznym

(z 14 do 24), a także liczba osób aresztowanych z powodu terroryzmu (z 426 do 449). Ponadto sukcesywnie obniża się wiek terrorystów. W działaniach terrorystycznych są wykorzystywane nowe rozwiązania technologiczne, np. drony, druk 3D czy sztuczna inteligencja. Bardzo niepokojącym zjawiskiem są coraz silniejsze powiązania terrorystów z grupami przestępczymi oraz służbami specjalnymi państw. Te zjawiska świadczą o ciągłych zmianach charakteru zagrożeń terrorystycznych w UE.

Słowa kluczowe

terroryzm, Unia Europejska, bezpieczeństwo, Europol, raport TE-SAT

Abstract

The authors of the article analysed the terrorist threats in the European Union in 2024 based on the data contained in the Europol report entitled *TE-SAT European Union Terrorism Situation and Trend Report 2025* and characterised them with reference to data concerning individual EU Member States. The authors described both the objective aspect of the threats (from jihadist, right-wing, left-wing and anarchist, ethno-nationalist and separatist groups, and others) and the quantitative aspect (e.g. the number of attacks and people arrested for terrorism). Data from the report indicate that in 2024, the number of terrorist attacks in the EU decreased compared to 2023 (from 120 to 58), but at the same time, the number of EU Member States experiencing attacks increased (from 7 to 14). The number of jihadist attacks has also escalated (from 14 to 24). An increase in the number of people arrested for terrorism-related crimes was also recorded (from 426 to 449). Furthermore, it is evident that the age of terrorists is gradually decreasing. New technological solutions, such as drones, 3D printing and artificial intelligence, are being used in terrorist activities. Of particular concern are the growing links between terrorists and criminal groups and the intelligence services of hostile states. All the above evidence demonstrates the constant changes in the nature of terrorist threats in the EU.

Keywords

terrorism, European Union, security, Europol, TE-SAT Report

Wprowadzenie

Zmiany, które dokonują się we współczesnym terroryzmie, zachodzą na wielu płaszczyznach i dotyczą różnych części świata[1]. Obejmują m.in. zmianę profilu sprawców (np. coraz niższy wiek), taktyk i strategii działania terrorystów czy wykorzystanie przez nich nowinek technologicznych (np. sztucznej inteligencji, druku 3D, dronów, systemów Starlink[2]). Można to potwierdzić na przykładzie sytuacji w Unii Europejskiej. W artykule autorzy przeanalizowali najnowszy raport Europolu pt. *TE-SAT. European Union Terrorism Situation and Trend Report 2025*[3] (dalej: raport TE-SAT 2025) oraz scharakteryzowali zagrożenia terrorystyczne z uwzględnieniem danych dotyczących poszczególnych państw członkowskich UE. Omówili zarówno aspekt przedmiotowy zagrożenia (ze strony grup dżihadystycznych, prawicowych, lewicowych i anarchistycznych, etnonacjonalistycznych i separatystycznych oraz innych), jak i ilościowy (np. liczba ataków i osób aresztowanych z powodu terroryzmu).

Międzynarodowy kontekst zagrożenia terrorystycznego w Unii Europejskiej

Analiza zagrożenia terrorystycznego w UE wymaga uwzględnienia szerszego kontekstu. Duży wpływ na to zagrożenie ma konflikt w Strefie Gazy, z którym wiążą się liczne ataki oraz wezwania do stosowania przemocy, szerzone przez fundamentalistów m.in. w internecie. Należy również zwrócić uwagę

[1] Na temat ewolucji zagrożenia terrorystycznego w UE w latach 2021–2024 zob. np.: S. Wojciechowski, *Hybrydowy wymiar współczesnego terroryzmu a infrastruktura krytyczna. Analiza raportów Europolu TE-SAT z lat 2021–2024*, „Terroryzm – studia, analizy, prewencja" 2025, wydanie specjalne: *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*. https://doi.org/10.4467/27204383TER.25.008.21511; S. Wojciechowski, *Terrorism – old wine in new bottles*, Defence24, 21 VII 2025 r., https://defence24.com/geopolitics/terrorism-old-wine-in-new-bottles [dostęp: 25 VII 2025].

[2] Komitet Rady Bezpieczeństwa ONZ ds. Zwalczania Terroryzmu uznał bezzałogowe systemy powietrzne za jedno z głównych zagrożeń terrorystycznych. Wynika to zarówno z rosnących zdolności logistyczno-finansowych struktur terrorystycznych, jak i z szybkiego rozwoju rynku dronów komercyjnych czy wojskowych. Zob. *Wojny dronów: jak to się robi w Afryce [ANALIZA]*, Defence24, 31 V 2025 r., https://defence24.pl/technologie/wojny-dronow-jak-to-sie-robi-w-afryce-analiza#goog_rewarded [dostęp: 18 VII 2025].

[3] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf [dostęp: 20 VII 2025].

na sukces opozycji w Syrii, szczególnie jej islamistycznych nurtów, co dżihadyści cały czas wykorzystują w celach propagandowych czy militarnych[4]. W kontekście analizy zagrożenia w UE ważne jest także to, że grupy powiązane z Państwem Islamskim czy Al-Kaidą bardzo umocniły swoją pozycję w Afryce, głównie w Sahelu. W ocenie Europolu celem bojówek szkolonych w Afryce jest Europa, a wspomniane grupy przekształcają państwa Sahelu (zwłaszcza Mali, Burkinę Faso i Niger) w centrum globalnego terroryzmu. Ma to bezpośredni wpływ na bezpieczeństwo w UE. Sahel stał się zapleczem dla coraz większej liczby terrorystów z zagranicy, którzy szukają nowych frontów walki po wycofaniu się np. z Syrii czy Iraku. Co więcej, działające tam formacje – np. powiązane z Al-Kaidą: Grupa Wsparcia Islamu i Muzułmanów (Jama'at Nusrat al-Islam wal-Muslimin, JNIM), Asz-Szabab (Harakat asz-Szabab al-Mudżahidin, HSM) oraz Państwo Islamskie Prowincji Zachodnioafrykańskiej (Islamic State West Africa Province, ISWAP) i Państwo Islamskie Prowincji Sahel (Islamic State Sahel Province, ISSP) – rozszerzają swoje wpływy. Obecnie zagrażają one również państwom położonym nad Zatoką Gwinejską, w tym Togo, Beninowi, Ghanie i Wybrzeżu Kości Słoniowej. Jednym ze skutków tej sytuacji są dramatyczne dane dotyczące liczby ofiar śmiertelnych spowodowanych działaniami terrorystycznymi na świecie. W 2024 r. ponad połowa tych osób (51%) zginęła w regionie Sahelu (w 2023 r. było to 48%)[5].

Jak już wspomniano, fundamentaliści w Afryce szerzą propagandę za pomocą platform cyfrowych. Jest ona rozpowszechniana w wielu językach i skierowana także do młodych Europejczyków. Poważnym problemem jest również wykorzystywanie przez terrorystów systemów Starlink – zarówno do komunikacji, jak i walki zbrojnej. Systemy te są przydatne zwłaszcza na rozległych obszarach Afryki Zachodniej, pozbawionych tradycyjnej infrastruktury komunikacyjnej. Zwraca na to uwagę w swoim raporcie Globalna Inicjatywa przeciwko Transnarodowej Przestępczości Zorganizowanej (Global Initiative against Transnational Organized Crime)[6]. W związku

[4] Jednym z przejawów jest atak ISIS na żołnierzy amerykańskich w Syrii 13 grudnia 2025 r. Zob. E. Kourdi, N. Bertrand, *Trump pledges retaliation after two US soldiers, one civilian interpreter killed in Syria*, CNN, https://edition.cnn.com/2025/12/13/politics/two-us-army-soldiers-killed-in-syria [dostęp: 17 XII 2025].

[5] *Europol: Afryka jest problemem dla bezpieczeństwa Unii Europejskiej*, Onet, 26 VI 2025 r., https://wiadomosci.onet.pl/swiat/europol-afryka-jest-problemem-dla-bezpieczenstwa-unii-europejskiej/f6pm9xl [dostęp: 20 VII 2025].

[6] *Observatory of Illicit Economies in West Africa*, https://riskbulletins.globalinitiative.net/download/wea-obs-012-screen-pdf.pdf [dostęp: 10 VII 2025].

z tym Europol wzywa państwa europejskie do zacieśniania współpracy z podmiotami afrykańskimi i przewidywania ryzyka związanego z potencjalnymi zagrożeniami, w tym napływem do Europy wyszkolonych terrorystów islamskich[7].

Kolejnym poważnym wyzwaniem dla bezpieczeństwa państw członkowskich UE jest terroryzm państwowy wspierany lub bezpośrednio realizowany przez Rosję i powiązane z nią państwa. Przejawia się on nie tylko w cyberatakach i aktach terroru, lecz także w werbowaniu cudzoziemców, m.in. za pomocą komunikatora Telegram, do organizowania sabotażu w Europie. Zwracają na to uwagę zarówno europejskie służby specjalne, jak i np. Organized Crime and Corruption Reporting Project – amerykańska organizacja pozarządowa zajmująca się dziennikarstwem śledczym[8]. Wprost nawiązuje do tego również raport *Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe*[9].

Zagrożenia terrorystyczne w Unii Europejskiej w 2024 roku na tle danych z lat 2022–2023

Prezentacja danych z 2024 r. na tle lat wcześniejszych umożliwi prześledzenie dynamiki zmian zachodzących w omawianych zjawiskach.

Ataki terrorystyczne – ogólna charakterystyka

Jak wynika z raportu TE-SAT 2025, w 2024 r. Europol odnotował łącznie 58 ataków terrorystycznych (w tym: 34 przeprowadzone, 5 nieudanych i 19 udaremnionych) w 14 państwach członkowskich UE. Najwięcej ataków było we Włoszech (20), następnie we Francji (14), Niemczech (6), Austrii i Grecji (po 3), Czechach, Danii, Litwie (po 2) oraz w Belgii, Irlandii, Holandii,

[7] Zob. np.: A. Wejkszner, *Europejska armia kalifatu. Tom 1. Centrum supersieci*, Warszawa 2020; A. Wejkszner, *Europejska armia kalifatu. Tom 2. Peryferie supersieci*, Warszawa 2023.

[8] *'Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder*, Organized Crime and Corruption Reporting Project, 26 IX 2024 r., https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder [dostęp: 20 VII 2025]; *How crime is accelerated by AI*, Europol, https://www.europol.europa.eu/media-press/europol-podcast/episode-21-how-crime-is-accelerated-by-ai [dostęp: 21 VII 2025].

[9] *Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe*, https://icct.nl/sites/default/files/2025-09/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool.pdf [dostęp: 16 XII 2025].

Słowacji, Hiszpanii i na Malcie (po 1). Terrorystom dżihadystycznym przypisano 24 ataki, lewicowym i anarchistycznym – 21, jako inną formę zagrożenia terrorystycznego sklasyfikowano 8 ataków, 4 miały charakter separatystyczny, a 1 – prawicowy (tabela 1).

Mimo że w 2024 r. liczba ataków zdecydowanie spadła (w 2023 r. było ich 120[10], w 2024 r. – 58), to dane zawarte w raporcie Europolu nie napawają optymizmem. Liczba państw członkowskich UE, w których doszło do ataków, wzrosła bowiem z 7 do 14. Jest to widoczne zwłaszcza w przypadku zagrożenia dżihadystycznego. W 2023 r. zarejestrowano 14 ataków o takim charakterze w 4 państwach, w 2024 r. było ich 24 i dotyczyły 7 krajów. Ataki o podłożu dżihadystycznym spowodowały największą liczbę ofiar śmiertelnych w porównaniu z atakami terrorystycznymi innego typu. W 2024 r. w ich wyniku w UE zginęło 5 osób, a 18 zostało rannych.

W 2024 r. najwięcej ataków (12) było wymierzonych w cywilów. Osiem ataków przeprowadzili dżihadyści, 3 – sprawcy powiązani z terroryzmem o podłożu etnonacjonalistycznym lub separatystycznym, a 1 sklasyfikowano jako inną formę terroryzmu. Drugim najczęściej atakowanym celem był sektor przemysłowy (państwowy) – 9 zdarzeń. Wszystkie ataki zorganizowali terroryści lewicowi i anarchistyczni. Inne popularne cele to: prywatne przedsiębiorstwa (5), podmioty/symbole religijne (5), infrastruktura krytyczna (4), podmioty polityczne (4) i organy ścigania (4). Ataki miały miejsce przede wszystkim w miastach (45), znacznie mniej było ich na obszarach wiejskich (13).

Najczęstszą formą działania terrorystów były podpalenia (wykorzystane w 22 atakach). Następne w kolejności były: zamachy bombowe (11 ataków), pchnięcia nożem (8), użycie broni palnej (6), zniszczenie mienia (6) oraz porwania (1). W większości ataków (15) zostały wykorzystane eskalatory ognia. Sięgali po nie przede wszystkim terroryści lewicowi i anarchistyczni (11 ataków). Improwizowanych urządzeń wybuchowych użyto w 10 przypadkach, broni białej również w 10 (ataki przeprowadzone przez dżihadystów), a improwizowanych urządzeń zapalających w 6.

[10] Zob. np. S. Wojciechowski, A. Wejkszner, *Nowe oblicze zagrożenia terrorystycznego w Unii Europejskiej. Analiza „TE-SAT. European Union Terrorism Situation and Trend Report 2024" i innych źródeł*, „Terroryzm – studia, analizy, prewencja" 2025, nr 7, s. 13–33. https://doi.org/10.4467/27204383TER.25.025.21802.

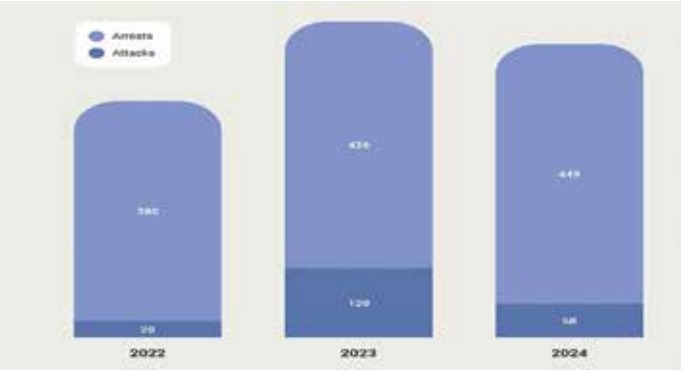
Tabela 1. Liczba zamachów terrorystycznych w państwach UE w 2024 r. z uwzględnieniem podziału na motywacje ideologiczne sprawców (prezentowane liczby obejmują ataki przeprowadzone, nieudane i udaremnione).

PAŃSTWO	TYP TERRORYZMU					RAZEM
	DŻIHADYSTYCZNY	PRAWICOWY	LEWICOWY I ANARCHISTYCZNY	ETNONACJONALISTYCZNY I SEPARATYSTYCZNY	INNE	
Austria	3					**3**
Belgia	1					**1**
Czechy					2	**2**
Dania					2	**2**
Francja	11			3		**14**
Grecja			3			**3**
Hiszpania	1					**1**
Holandia	1					**1**
Irlandia	1					**1**
Litwa					2	**2**
Malta					1	**1**
Niemcy	6					**6**
Słowacja					1	**1**
Włochy		1	18	1		**20**
RAZEM	**24**	**1**	**21**	**4**	**8**	**58**

Źródło: opracowanie własne na podstawie: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, s. 62 [dostęp: 20 VII 2025].

Aresztowania za przestępstwa terrorystyczne

Należy podkreślić, że wzrosła ogólna liczba osób aresztowanych za przestępstwa terrorystyczne[11]. W 2023 r. było tych osób 426, w 2024 r. – 449 (wykres 1) w 20 państwach członkowskich UE. Zatrzymani to głównie mężczyźni – 405 osób. Najwięcej aresztowań dokonano w Hiszpanii (90 osób), następnie we Francji (69), Włoszech (62) i Niemczech (55). W Polsce odnotowano 13 zatrzymań, przy czym 1 przypadek dotyczył działań terrorystycznych o charakterze dżihadystycznym, a za niesklasyfikowane uznano 12 zdarzeń.



Wykres 1. Liczba ataków terrorystycznych oraz liczba osób aresztowanych z powodu prowadzenia działalności terrorystycznej w UE w latach 2022–2024 (prezentowane liczby dotyczące ataków obejmują ataki przeprowadzone, nieudane i udaremnione).

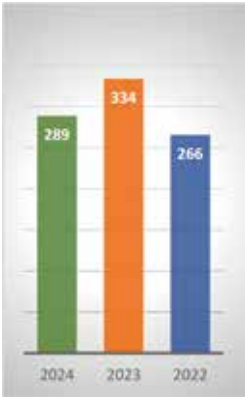
Źródło: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, s. 13 [dostęp: 20 VII 2025].

W UE większość aresztowań w 2024 r. dotyczyła sprawców terroryzmu dżihadystycznego (289). W porównaniu z rokiem poprzednim ta liczba spadła z 334 (wykres 2).

Prawie połowę (136) z 289 osób aresztowano w dwóch państwach – Francji i Hiszpanii. Zdecydowaną większość (88%) zatrzymanych stanowili mężczyźni. Byli to w dużej części nastolatkowie lub mężczyźni, którzy nie

[11] W *Dyrektywie Parlamentu Europejskiego i Rady UE 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW* „przestępstwo terrorystyczne" zostało określone jako czyn karalny popełniony w celu poważnego zastraszenia ludności, wywarcia nieuprawnionej presji na rząd lub organizację międzynarodową bądź destabilizacji kluczowych struktur państwa. Dyrektywa ta ustanawia wspólne ramy definicyjne, przepisy wewnętrzne państw członkowskich UE różnią się szczegółami.

ukończyli 27 lat. Niecałej połowie zatrzymanych postawiono zarzuty przynależności do organizacji terrorystycznej lub kolportowania dżihadystycznej propagandy w internecie[12].



Wykres 2. Liczba aresztowań osób podejrzewanych o przestępstwa terrorystyczne o charakterze dżihadystycznym w państwach członkowskich UE w latach 2022–2024.

Źródło: opracowanie własne na podstawie: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, s. 26 [dostęp: 20 VII 2025].

W przypadku innych form terroryzmu odnotowano wzrost liczby zatrzymanych. Dotyczy to zwłaszcza sprawców: terroryzmu skrajnie prawicowego, skrajnie lewicowego i anarchistycznego oraz niesklasyfikowanych jego przejawów[13].

W 2024 r. na terytorium państw członkowskich UE w związku z podejrzeniami o aktywność terrorystyczną motywowaną ideologią skrajnie prawicową aresztowano prawie dwa razy więcej osób niż rok wcześniej

[12] Europol, *TE-SAT*..., s. 26–27.

[13] Do tej grupy zaliczono np. przejawy sabotażu zgłoszone przez Polskę i Hiszpanię, a realizowane na zlecenie obcych służb. W analizowanym okresie zatrzymano w tych krajach 9 osób zwerbowanych przez rosyjskich agentów. Jak poinformował 29 VII 2025 r. Jacek Dobrzyński, rzecznik prasowy ministra koordynatora służb specjalnych: „Funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego ustalili, że za dwoma podpaleniami, które miały miejsce w 2024 roku w Polsce stoi 27-letni Kolumbijczyk działający na zlecenie rosyjskiego wywiadu. Do zdarzeń doszło 23 maja ubiegłego roku w Warszawie i tydzień później, 30 maja w Radomiu". Zob. *Pożary w Polsce. Kolumbijczyk miał działać na zlecenie Rosji. Ustalenia ABW*, Rzeczpospolita, 29 VII 2025 r., https://www.rp.pl/przestepczosc/art42769991-pozary-w-polsce-kolumbijczyk-mial-dzialac-na-zlecenie-rosji-ustalenia-abw [dostęp: 30 VII 2025].

(odpowiednio 47 i 26). Wśród zatrzymanych byli wyłącznie mężczyźni w wieku od 12 do 76 lat, mający unijne obywatelstwo.

W przypadku działań terrorystycznych motywowanych ideologią skrajnie lewicową i anarchistyczną policja aresztowała jednak relatywnie niewielką – wobec liczby tych działań – liczbę osób powiązanych z tego rodzaju aktywnością. Było to ogółem 28 osób, z czego 20 zatrzymano w Grecji. Wśród aresztowanych było prawie 5 razy więcej mężczyzn niż kobiet, a ich wiek mieścił się w przedziale od 26 do 78 lat. Nie ujawniono ich afiliacji terrorystycznej, wskazując, że należeli do niezależnych komórek działających w sposób autonomiczny. Greckim śledczym udało się jednak zidentyfikować co najmniej 3 grupy terrorystyczne, do których należało łącznie 10 zatrzymanych osób. Były to: „Partnerstwo Zemsty", „Konspiracja Zemsty" i „Zbrojna Odpowiedź".

W związku z podejrzeniami o ekstremizm motywowany ideologią etnonacjonalistyczną w 2024 r. zatrzymano na terytorium państw członkowskich UE 27 osób. Ponad połowa z nich należała do Partii Pracujących Kurdystanu (Partiya Karkerên Kurdistanê). Oskarżono ich o przygotowywanie ataku terrorystycznego, o członkostwo w organizacji terrorystycznej i finansowanie jej działalności oraz o szerzenie propagandy terrorystycznej[14].

Najczęściej powtarzającymi się przestępstwami powiązanymi z terroryzmem były: przynależność do organizacji terrorystycznej (110), planowanie lub przygotowywanie ataku (107) oraz tworzenie i/lub rozpowszechnianie propagandy terrorystycznej (90)[15].

Bardzo niepokojące jest to, że w 2024 r. w UE wzrosła liczba nieletnich i młodych osób zaangażowanych w działalność terrorystyczną i ekstremistyczną. Spośród 449 aresztowanych w 2024 r. 133 było w wieku od 12 do 20 lat, co stanowi ponad 29% wszystkich przypadków zatrzymań za przestępstwa terrorystyczne. Najmłodszy podejrzany miał 12 lat i aresztowano go za planowanie przeprowadzenia ataku. Zdecydowana większość sprawców młodocianych była powiązana z terroryzmem dżihadystycznym. Stawiane wobec nich zarzuty najczęściej dotyczyły: udziału w atakach, tworzenia i rozpowszechniania treści o charakterze radykalnym oraz przynależności do grupy terrorystycznej czy ekstremistycznej. Młodocianymi terrorystami byli przeważnie mężczyźni, którzy proces radykalizacji najczęściej przechodzili w sieci i działali w oderwaniu od struktur organizacyjnych[16].

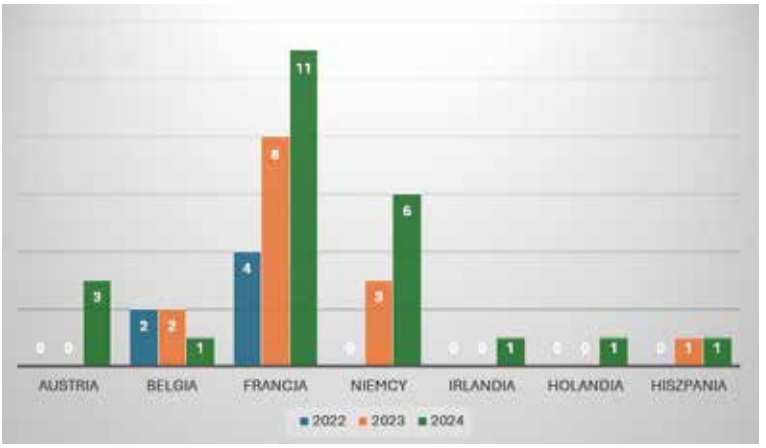
[14] Europol, *TE-SAT*..., s. 50–51.

[15] Tamże, s. 14.

[16] Tamże, s. 10.

Terroryzm motywowany ideologią dżihadystyczną

W 2024 r. terroryzm motywowany ideologią dżihadystyczną[17] stanowił istotne wyzwanie dla bezpieczeństwa państw UE. Świadczą o tym dane dotyczące zarówno przeprowadzonych, jak i nieudanych ataków terrorystycznych. Dżihadyści przeprowadzili po 2 zamachy we Francji i w Niemczech oraz po 1 w Irlandii i Holandii. W ich wyniku 5 osób poniosło śmierć, a 18 zostało rannych[18]. Nieudanych ataków było aż trzy razy więcej (wykres 3).



Wykres 3. Liczba ataków terrorystycznych motywowanych ideologią dżihadystyczną w państwach członkowskich UE w latach 2022–2024 (prezentowane liczby obejmują ataki przeprowadzone, nieudane i udaremnione).

Źródło: opracowanie własne na podstawie: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, s. 24 [dostęp: 20 VII 2025].

[17] Według autorów raportu dżihadyzm jest definiowany jako radykalny nurt salafizmu (ruchu odrodzenia sunnickich muzułmanów). Jego zwolennicy odrzucają współczesną demokrację, gdyż ich zdaniem ustawodawstwo tworzone przez ludzi jest sprzeczne ze statusem Boga jako jedynego prawodawcy. Dżihadyści dążą do stworzenia państwa islamskiego rządzonego wyłącznie prawem islamskim (szariatem). W przeciwieństwie do innych nurtów salafickich, dżihadyści legitymizują stosowanie przemocy, odwołując się do klasycznych islamskich doktryn dżihadu (termin ten dosłownie oznacza „dążenie" lub „wysiłek", ale dżihadyści rozumieją go jako wojnę sankcjonowaną religijnie). Wszyscy, którzy sprzeciwiają się dżihadystycznym interpretacjom prawa islamskiego, są uważani za wrogów islamu, a zatem za uzasadnione cele ataków. Niektórzy dżihadyści jako wrogów postrzegają również szyitów i innych muzułmanów. Zob. tamże, s. 23.

[18] Tamże.

Modus operandi terrorystów dżihadystycznych należy uznać za charakterystyczny dla tej grupy ekstremistów religijnych. Obejmował on bowiem jedynie aktywność indywidualnych terrorystów dżihadystycznych[19]. Przynajmniej w dwóch przypadkach (Niemcy i Francja) podejrzewano lub potwierdzono związek sprawców z Państwem Islamskim[20]. Ich celem były przede wszystkim imprezy masowe, w tym mecze piłkarskie i inne imprezy sportowe we Francji oraz koncert w Austrii. Poza tym próbowano zaatakować miejsca kultu (głównie synagogi) oraz cele związane z wymiarem sprawiedliwości. Zamachowcy najczęściej używali prymitywnej broni – głównie noży. Jednym z przykładów wykorzystania takiej taktyki jest zamach przeprowadzony 2 marca 2024 r. w Zurychu przez 15-letniego chłopca. Zaatakował on 50-letniego ortodoksyjnego Żyda. Chwilę wcześniej opublikował w mediach społecznościowych przysięgę wierności kalifowi Państwa Islamskiego oraz wezwał do przeprowadzania ataków na Żydów i chrześcijan. Proces radykalizacji zamachowca (obywatela Szwajcarii o imigranckich korzeniach) rozpoczął się w Tunezji, w której przebywał w latach 2017–2021[21]. Ewenementem w przypadku tego zdarzenia była transmisja na żywo całego zdarzenia, co według sprawcy miało przynieść skutek propagandowy. Kolejnym przykładem wykorzystania wspomnianej taktyki jest zamach w Solingen, w Niemczech, przeprowadzony 23 sierpnia 2024 r. Zamachowiec zaatakował nożem przypadkowych uczestników miejskiego festiwalu i spowodował śmierć 3 osób[22]. Tuż przed atakiem skontaktował się za pośrednictwem komunikatora internetowego z przedstawicielem Państwa Islamskiego, który zachęcił go do udokumentowania swoich zamiarów, aby potem wykorzystać ten materiał w celach propagandowych[23]. Podobną taktykę zastosowano podczas ataków terrorystycznych dokonanych 15 sierpnia 2024 r. w Galway w Irlandii i 19 września 2024 r.

[19] Na temat tzw. indywidualnego terroryzmu dżihadystycznego zob. A. Wejkszner, *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej*, Warszawa 2018, s. 27–47.

[20] Europol, *TE-SAT*..., s. 23.

[21] *Anti-Semitism: Zurich attacker radicalised in Tunisia and online*, swissinfo.ch, 25 III 2024 r., https://www.swissinfo.ch/eng/swiss-politics/zurich-stabber-radicalized-in-tunisia-and-online/74284770 [dostęp: 20 VII 2025].

[22] *Anklage gegen ein mutmaßliches Mitglied der ausländischen terroristischen Vereinigung „Islamischer Staat (IS)" wegen des Messerangriffs in Solingen erhoben*, Der Generalbundesanwalt beim Bundesgerichtshof, 27 II 2025 r., https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2025/Pressemitteilung-vom-27-02-2025.html [dostęp: 20 VII 2025].

[23] Tamże.

w Rotterdamie w Holandii. Sprawcami byli młodzi mężczyźni w wieku 16 i 22 lat[24].

Omówione zdarzenia świadczą o utrzymywaniu się zagrożenia terroryzmem dżihadystycznym na terytorium państw UE (czy szerzej – w Europie Zachodniej) w analizowanym okresie. Potwierdza to także liczba osób aresztowanych w związku z podejrzeniami o udział w tego typu aktywności.

Jedną z głównych przesłanek procesu radykalizacji dżihadystycznej w UE w analizowanym okresie, w tym ataków na cele żydowskie i związane z państwem Izrael, były wydarzenia w Strefie Gazy w 2024 r. wywołane atakiem terrorystów z Hamasu na cele w Izraelu w październiku 2023 r. Propagandziści Al-Kaidy i Państwa Islamskiego wykorzystywali antyizraelską czy antychrześcijańską narrację, posiłkując się obrazami skutków działań odwetowych Izraela w Strefie Gazy[25].

Terroryzm motywowany ideologią skrajnie prawicową

Terroryzm grup skrajnie prawicowych[26] stanowił w UE w 2024 r. nieporównywalnie mniejsze zagrożenie niż terroryzm dżihadystyczny. W tym czasie doszło jedynie do 1 zamachu motywowanego tą ideologią (wykres 4).

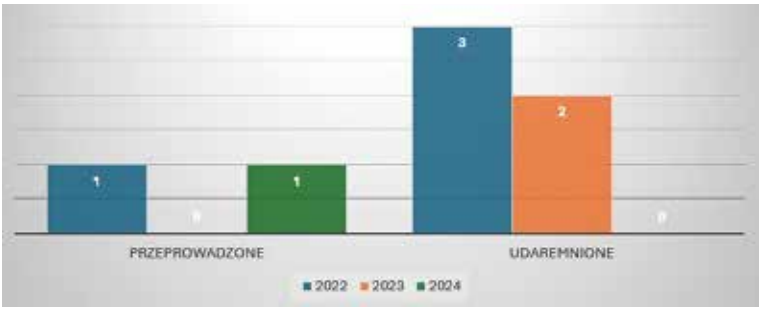
Atak ujęty w raporcie Europolu miał miejsce w Montello we Włoszech 18 marca 2024 r. Domniemany zamachowiec próbował podłożyć ogień przed wejściem do Centrum Islamskiego. Klasyfikacja tego przypadku wydaje się jednak wątpliwa, gdyż nie ujawniono ani politycznej agendy sprawcy, ani jego terrorystycznej afiliacji. Celami ataków motywowanych ideologią skrajnie prawicową miały być osoby ras innych niż biała oraz aktywiści skrajnej lewicy i bliżej niezidentyfikowani „wrogowie i zdrajcy"[27].

[24] Europol, *TE-SAT*..., s. 25.

[25] Tamże, s. 29–30.

[26] Twórcy raportu przez termin „terroryzm grup skrajnie prawicowych" rozumieją użycie przemocy w celu przekształcenia współczesnego systemu politycznego, społecznego i ekonomicznego w model autorytarny, w którym wartości i instytucje demokratyczne zostałyby odrzucone. Prawicowe ideologie odwołujące się do tego modelu wykorzystują agresywną narrację skupioną na nacjonalizmie, rasizmie, ksenofobii czy innych przejawach nietolerancji. Podstawową koncepcją prawicowego ekstremizmu jest supremacja narodu czy rasy. W praktyce oznacza to, że jakiś wspólny element charakteryzujący daną grupę osób sprawia, że są oni lepsi od innych i uważają dominację nad resztą populacji za swoje naturalne prawo. Ponadto prawicowe ideologie ekstremistyczne popularyzują też idee sprzeciwiające się różnorodności społeczeństwa i równym prawom mniejszości, np. mizoginię, wrogość wobec społeczności LGBTQ+, postawy antyimigracyjne. Zob. tamże, s. 34.

[27] Tamże, s. 36–37.



Wykres 4. Liczba ataków terrorystycznych motywowanych ideologią skrajnie prawicową w państwach członkowskich UE w latach 2022–2024.

Źródło: opracowanie własne na podstawie: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, s. 36 [dostęp: 20 VII 2025].

Aby zintensyfikować proces rekrutacji nowych ekstremistów i skłonić ich do wykorzystania przemocy, zwolennicy tej ideologii korzystali z narzędzi internetowych. Swoje wysiłki adresowali przede wszystkim do przedstawicieli środowisk dysfunkcyjnych pod względem społecznym i ekonomicznym, w których dominował kult siły i sprzeciw wobec aktualnych procesów społecznych (np. legalnej i nielegalnej migracji). W tym kontekście szczególnie niebezpieczne były środowiska neonazistowskie, których sieciowa struktura (przypominająca tę tworzoną przez dżihadystów) utrudniała policji i wymiarowi sprawiedliwości ich efektywną penetrację. Na marginesie warto zauważyć, że przedstawiciele tych środowisk doświadczenia związane z użyciem różnych rodzajów broni zdobywali podczas konfliktu rosyjsko-ukraińskiego, walcząc notabene po obu stronach konfliktu[28].

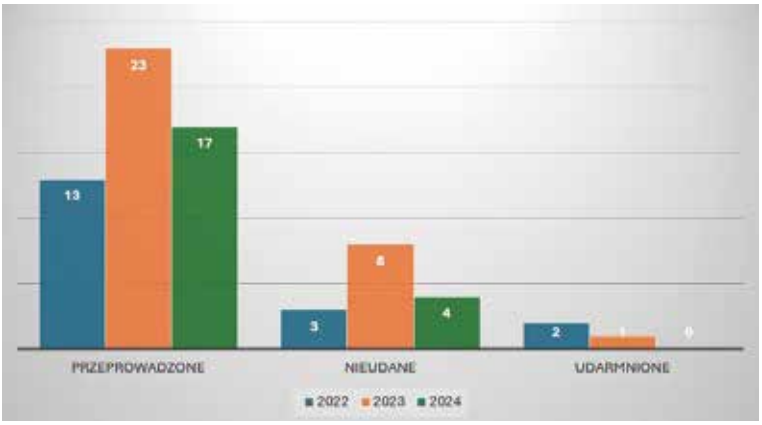
Terroryzm motywowany ideologią skrajnie lewicową i anarchistyczną

W 2024 r. zauważalnie większą aktywność w porównaniu z dwoma powyżej omówionymi przypadkami wykazywały w UE grupy skrajnie lewicowe i anarchistyczne[29]. Przypisano im łącznie 21 ataków terrorystycznych –

[28] Tamże, s. 38.

[29] W raporcie przez aktywność terrorystyczną grup skrajnie lewicowych rozumie się aktywność związaną z użyciem przemocy i mającą na celu wywołanie rewolucji motywowanej ideologią marksistowsko-leninowską, skierowanej przeciwko demokratycznemu państwu. Celem takich działań jest ustanowienie socjalizmu, komunizmu czy też bezklasowego społeczeństwa. Terroryzm anarchistyczny to z kolei taka forma przemocy politycznej, której

17 przeprowadzonych i 4 nieudane (wykres 5). Zostały przeprowadzone głównie we Włoszech i w Grecji.



Wykres 5. Liczba ataków terrorystycznych motywowanych ideologią skrajnie lewicową i anarchistyczną w państwach członkowskich UE w latach 2022–2024.

Źródło: opracowanie własne na podstawie: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, s. 42 [dostęp: 20 VII 2025].

Modus operandi sprawców nie zmienił się istotnie w porównaniu z latami wcześniejszymi. Ataki były wymierzone głównie w infrastrukturę krytyczną, w tym nieruchomości należące do instytucji państwowych. Z taktycznego punktu widzenia najbardziej efektywne były podpalenia. Spośród 13 przypadków, w których użyto tej taktyki, w 2 wykorzystano tzw. improwizowane urządzenia zapalające, w 4 – improwizowane urządzenia wybuchowe. Za 10 ataków terrorystycznych sprawcy wzięli polityczną odpowiedzialność, umieszczając w większości przypadków oświadczenie w internecie. Najczęściej przywoływanymi powodami podjęcia takiej aktywności były sprzeciw wobec polityki rządu (głównie wobec polityki migracyjnej), a także poglądy antywojenne i antykapitalistyczne. W mniejszym stopniu kładziono nacisk na walkę o prawa zwierząt czy solidarność z towarzyszami represjonowanymi przez wymiar sprawiedliwości. W raporcie Europolu jako przykład ataku terrorystycznego mieszczącego się

celem jest zniszczenie aktualnego modelu władzy politycznej i zastąpienia go modelem antydyskryminacyjnym i antykapitalistycznym, promującym równość, wolność i sprawiedliwość społeczną. Zob. tamże, s. 42.

w ramach analizowanego typu podano zamach na farmę fotowoltaiczną w Tuili we Włoszech dokonany 10 września 2024 r. W wyniku podpalenia zniszczono ok. 2000 paneli należących do portugalskiej firmy Greenvolt Power, co spowodowało straty w wysokości co najmniej 1 mln euro[30]. Nie zidentyfikowano sprawców. W związku z tym przypisanie tej aktywności kryminalnej do wskazanej grupy zamachów terrorystycznych tylko na podstawie modus operandi sprawców należy uznać za metodologicznie wątpliwe.

Wśród głównych motywów propagandowych popularyzowanych przez członków grup skrajnie lewicowych i anarchistycznych znajdowały się hasła antyfaszystowskie, antyimperialistyczne, antykolonialne, antywojenne i antyautorytarne. Głoszono również hasła solidarności z prześladowanymi Palestyńczykami i Kurdami, a także krytykowano NATO i UE[31].

Terroryzm motywowany ideologią etnonacjonalistyczną

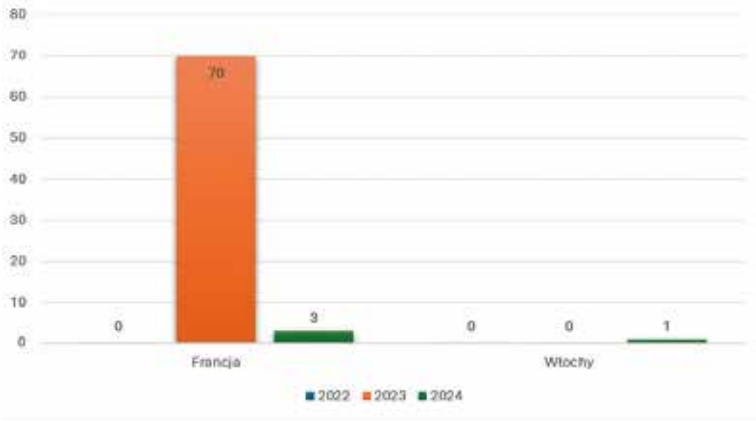
Terroryści motywowani ideologią etnonacjonalistyczną[32] podjęli w 2024 r. relatywnie niewiele, w stosunku do opisanych wcześniej sprawców o innych motywacjach, działań o charakterze terrorystycznym. Odpowiedzialni byli tylko za 4 ataki, co stanowi znaczny spadek w porównaniu z poprzednim rokiem (70 zamachów). Trzy ze wspomnianych zamachów miały miejsce we Francji, a jeden we Włoszech[33] (wykres 6). Za ataki we Francji odpowiedzialność ponoszą, zdaniem tamtejszej policji, Narodowy Front Wyzwolenia Korsyki (Front de libération nationale corse) oraz Tajna Młodzież Korsykańska (Ghjuventù Clandestina Corsa). Nie zmieniła się taktyka przeprowadzanych zamachów (podpalanie nieruchomości).

[30] *Attack in Tuili during the night: hundreds of photovoltaic panels destroyed*, L'Unione Sarda.it, 10 IX 2024 r., https://www.unionesarda.it/en/sardinia/attack-in-tuili-during-the-night-hundreds-of-photovoltaic-panels-destroyed-nuyrob0o [dostęp: 20 VII 2025].

[31] Europol, *TE-SAT*..., s. 46–47.

[32] Pojęcie grup terrorystycznych o charakterze etnonacjonalistycznym czy separatystycznym obejmuje grupy, których członkowie odwołują się w ramach agendy politycznej do ideologii nacjonalistycznych czy przynależności etnicznej lub narodowej. Celem strategicznym tych grup jest oddzielenie jakiegoś terytorium od już istniejącego państwa i/lub przyłączenie jakiegoś terytorium do innego państwa. Zob. tamże, s. 49.

[33] Tamże, s. 50.



Wykres 6. Liczba ataków terrorystycznych motywowanych ideologią etnonacjonalistyczną i separatystyczną w UE w latach 2022–2024 (prezentowane liczby obejmują ataki przeprowadzone, nieudane i udaremnione).

Źródło: opracowanie własne na podstawie: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, s. 50 [dostęp: 20 VII 2025].

Raport TE-SAT 2025 zawiera także informacje o aktywności podejmowanej przez irlandzkich terrorystów powiązanych z grupami, które nie popierają procesu pokojowego w Irlandii Północnej (Nowa IRA, IRA Kontynuacji). W analizowanym okresie członkowie żadnej z nich nie powrócili jednak do aktywności terrorystycznej[34].

Inne formy aktywności terrorystycznej

W raporcie TE-SAT 2025 wspomniano również o 8 innych przypadkach aktywności terrorystycznej, ale nie sprecyzowano, o jaką afiliację sprawców chodzi. Najbardziej znanym przykładem jest próba zabójstwa premiera Roberta Fico, do której doszło 15 maja 2024 r. w miejscowości Handlova na Słowacji. Sprawca, Juraj Cintula, miał planować atak co najmniej od kwietnia[35]. Zabrakło jednak – charakterystycznego w przypadku ataku indywidualnego terrorysty – manifestu publikowanego zazwyczaj tuż przed atakiem, w którym zamachowiec wskazywałby motywy użycia przemocy.

[34] Tamże, s. 53.

[35] J. Zadražilová, *Atentátník se k činu rozhodl hned po prezidentských volbách*, Novinky.cz, 15 V 2024 r., https://www.novinky.cz/clanek/zahranicni-atentatnik-se-k-cinu-rozhodl-hned-po-prezidentskych-volbach-rekl-ministr-40471949 [dostęp: 20 VII 2025].

Polityczne motywacje do jego działań o charakterze kryminalnym zostały przypisane a posteriori przez słowackie służby zajmujące się śledztwem w sprawie[36]. Równie dyskusyjny jest wspomniany w raporcie atak, do którego doszło 30 maja 2024 r. na Malcie. W pobliżu biura Partii Pracy 18-letni kryminalista zdetonował materiał wybuchowy TATP (trimeryczny nadtlenek acetonu). Zdaniem służb prowadzących śledztwo w tej sprawie sprawca był niepoczytalny w okresie, w którym doszło do ataku. To uniemożliwia zaklasyfikowanie jego czynu jako aktu terrorystycznego[37]. Trudno bowiem zgodzić się z decyzją o uznaniu czynu kryminalnego za aktywność terrorystyczną, gdy nie ma możliwości odtworzenia agendy politycznej czy potwierdzenia deklarowanej afiliacji terrorystycznej osoby podejrzewanej o taką aktywność. Wskazanie w raporcie takiego typu aktywności terrorystycznej należy więc uznać za dyskusyjne. Tym bardziej że w kontekście aresztowań osób podejrzewanych o związki z terroryzmem jest mowa raczej o członkach zorganizowanych grup przestępczych, których aktywność przypomina typowe działania kryminalne (nielegalne gromadzenie broni i materiałów wybuchowych, akcje sabotażowe, działania dezinformacyjne) lub – w ostateczności – wpisuje się działania hybrydowe podejmowane przez państwa trzecie nieprzyjazne państwom członkowskim UE.

Wykorzystanie sieci do działań o charakterze terrorystycznym

Gwałtownie narastającym problemem jest zwiększająca się liczba różnych platform internetowych wykorzystywanych np. do rekrutowania nieletnich do działań terrorystycznych czy dokonywania aktów przemocy. Grupy powiązane z taką aktywnością w sieci często opowiadają się za rozpadem struktur demokratycznych przez wprowadzanie chaosu czy stosowanie terroru. Wiele z nich reprezentuje poglądy ideologiczne powiązane z terroryzmem dżihadystycznym, skrajnie prawicowym, skrajnie lewicowym, ale też z satanizmem czy okultyzmem.

W 2024 r. liczba nowych usług w cyberprzestrzeni wykorzystujących do tworzenia i rozpowszechniania propagandy czy mowy nienawiści nowe technologie, w tym sztuczną inteligencję, osiągnęła rekordowy poziom. Odnosi się to szczególnie do terroryzmu skrajnie prawicowego, ale dotyczy też – w różnym stopniu – skrajnie lewicowych i anarchistycznych grup

[36] B. Szandelszky, P.D. Josek, P. Jenne, *Slovak authorities charge 'lone wolf' with assassination attempt on the prime minister*, AP, 16 V 2024 r., https://apnews.com/article/slovakia-prime-minister-shooting-fico-23faba11c0f371ef0f69a34861337ae0 [dostęp: 20 VII 2025].

[37] Europol, *TE-SAT*..., s. 56.

terrorystycznych. Jako przykład można wskazać anarchistyczną organizację terrorystyczną Partnership of Revenge. Większość jej członków nie deklarowała przynależności ideologicznej. Do działania motywował ich głównie zysk finansowy, co wskazuje na zerwanie z tradycyjnymi praktykami stosowanymi do tej pory przez terrorystów o motywacjach anarchistycznych[38].

Przez cały 2024 r. bardzo aktywnie była prowadzona propaganda Al-Kaidy i Państwa Islamskiego, w której wykorzystywano – o czym już wspomniano – m.in. wydarzenia w Strefie Gazy. Kilka skoordynowanych kampanii propagandowych dżihadystów było nakierowanych na nakłanianie swoich zwolenników do przeprowadzania ataków. Taką aktywność wykazywali również przedstawiciele innych nurtów terrorystycznych[39].

Zwalczanie terroryzmu w Unii Europejskiej

Unia Europejska cały czas podejmuje działania mające na celu zapobieganie terroryzmowi i zwalczanie go. Przykładami takich działań mogą być: „Referral Action Days" – akcja błyskawicznego zgłaszania i usuwania treści terrorystycznych z internetu, tworzenie zespołów zadaniowych zajmujących się np. kryptowalutami i aktualizacją listy zagranicznych bojowników czy wykorzystywanie mobilnych laboratoriów do analizy improwizowanych ładunków wybuchowych. Działania te należy jednak uznać za niewystarczające. Unia potrzebuje nowego, kompleksowego podejścia do terroryzmu. Jest to istotne ze względu na eskalację i ewolucję tego zagrożenia, obejmującą m.in.: masowy przemyt broni z Bałkanów czy Ukrainy, wykorzystanie przez terrorystów nowoczesnych rozwiązań, np. dronów, broni wytworzonej w technologii 3D, sztucznej inteligencji, kryptowalut. Konieczne jest również zwalczanie działań terrorystycznych prowadzonych w cyberprzestrzeni i powiązań terrorystów z grupami przestępczymi i służbami specjalnymi państw. Dotyczy to zwłaszcza polityki Rosji i współpracujących z nią podmiotów, wymierzonej m.in. w Polskę, Czechy, Rumunię, Hiszpanię i państwa bałtyckie.

[38] Tamże, s. 8.

[39] Zob. np. *Steal, deal and repeat: How cybercriminals trade and exploit your data*, Europol, https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data [dostęp: 15 VII 2025].

Skuteczne przeciwdziałanie zagrożeniu terrorystycznemu musi być realizowane nie tylko przez pogłębioną współpracę (wywiadowczą, logistyczną, prawną, polityczną) wszystkich państw członkowskich UE, lecz także przez rozszerzone współdziałanie z NATO oraz innymi sojusznikami w różnych częściach świata, np. na Bliskim Wschodzie czy w Afryce. Celem jest budowanie wieloaspektowej odporności w wymiarze zewnętrznym i wewnętrznym. Zagrożeniem dla skutecznej realizacji planów przeciwdziałania terroryzmowi mogą być partykularne interesy poszczególnych państw członkowskich UE, trwający w niektórych z nich kryzys polityczny, rozdźwięk w relacjach transatlantyckich, brak środków finansowych czy coraz częściej zapowiadany krach ekonomiczny.

Wnioski

1. Wskazane w raporcie TE-SAT 2025 zmiany w obrębie zjawiska terroryzmu dotyczą m.in. sukcesywnego obniżania się wieku terrorystów, a także wykorzystywania przez sprawców ataków coraz nowszych rozwiązań technologicznych, np. dronów, druku 3D czy sztucznej inteligencji.
2. Szczególnie niepokojącym zjawiskiem są coraz silniejsze powiązania terrorystów z grupami przestępczymi oraz służbami specjalnymi państw. Ich przejawem są m.in. częste przypadki terroru czy dywersji w państwach członkowskich UE.
3. Chociaż w 2024 r. znacznie spadła liczba ataków terrorystycznych, to należy podkreślić wzrost liczby państw członkowskich UE, w których doszło do ataków. Wzrosła też liczba osób aresztowanych z powodu terroryzmu oraz skala międzynarodowych powiązań struktur terrorystycznych.
4. Dwa typy terroryzmu: dżihadystyczny oraz skrajnie lewicowy i anarchistyczny stanowiły najpoważniejsze wyzwanie dla bezpieczeństwa w wielu państwach członkowskich UE (ze względu m.in. na liczbę incydentów). Jedynie incydenty terrorystyczne we Włoszech miały znacznie szersze podłoże ideologiczne.
5. Unia Europejska potrzebuje nowego kompleksowego podejścia do zagrożeń związanych z terroryzmem. Jest to istotne ze względu na nasilenie i ewolucję analizowanego zagrożenia. Skuteczne przeciwdziałanie terroryzmowi musi być realizowane nie tylko

przez pogłębioną współpracę państw członkowskich UE, lecz także przez szersze współdziałanie z innymi sojusznikami.

Bibliografia

Wejkszner A., *Europejska armia kalifatu. Tom 1. Centrum supersieci*, Warszawa 2020.

Wejkszner A., *Europejska armia kalifatu. Tom 2. Peryferie supersieci*, Warszawa 2023.

Wejkszner A., *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej*, Warszawa 2018.

Wojciechowski S., *Hybrydowy wymiar współczesnego terroryzmu a infrastruktura krytyczna. Analiza raportów Europolu TE-SAT z lat 2021–2024. Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, „Terroryzm – studia, analizy, prewencja" 2025, wydanie specjalne: *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*. https://doi.org/10.4467/27204383TER.25.008.21511.

Wojciechowski S., Wejkszner A., *Nowe oblicze zagrożenia terrorystycznego w Unii Europejskiej. Analiza „TE-SAT. European Union Terrorism Situation and Trend Report 2024" i innych źródeł*, „Terroryzm – studia, analizy, prewencja" 2025, nr 7, s. 13–33. https://doi.org/10.4467/27204383TER.25.025.21802.

Źródła internetowe

Anklage gegen ein mutmaßliches Mitglied der ausländischen terroristischen Vereinigung „Islamischer Staat (IS)" wegen des Messerangriffs in Solingen erhoben, Der Generalbundesanwalt beim Bundesgerichtshof, 27 II 2025 r., https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2025/Pressemitteilung-vom-27-02-2025.html [dostęp: 20 VII 2025].

Anti-Semitism: Zurich attacker radicalised in Tunisia and online, swissinfo.ch, 25 III 2024 r., https://www.swissinfo.ch/eng/swiss-politics/zurich-stabber-radicalized-in-tunisia-and-online/74284770 [dostęp: 20 VII 2025].

Attack in Tuili during the night: hundreds of photovoltaic panels destroyed, L'Unione Sarda.it, 10 IX 2024 r., https://www.unionesarda.it/en/sardinia/attack-in-tuili-during-the-night-hundreds-of-photovoltaic-panels-destroyed-nuyrob0o [dostęp: 20 VII 2025].

Europol: Afryka jest problemem dla bezpieczeństwa Unii Europejskiej, Onet, 26 VI 2025 r., https://wiadomosci.onet.pl/swiat/europol-afryka-jest-problemem-dla-bezpieczenstwa-unii-europejskiej/f6pm9xl [dostęp: 20 VII 2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf [dostęp: 20 VII 2025].

How crime is accelerated by AI, Europol, https://www.europol.europa.eu/media-press/europol-podcast/episode-21-how-crime-is-accelerated-by-ai [dostęp: 21 VII 2025].

Kourdi E., Bertrand N., *Trump pledges retaliation after two US soldiers, one civilian interpreter killed in Syria*, CNN, https://edition.cnn.com/2025/12/13/politics/two-us-army-soldiers-killed-in-syria [dostęp: 17 XII 2025].

'Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder, Organized Crime and Corruption Reporting Project, 26 IX 2024 r., https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder [dostęp: 20 VII 2025].

Observatory of Illicit Economies in West Africa, https://riskbulletins.globalinitiative.net/download/wea-obs-012-screen-pdf.pdf [dostęp: 10 VII 2025].

Pożary w Polsce. Kolumbijczyk miał działać na zlecenie Rosji. Ustalenia ABW, Rzeczpospolita, 29 VII 2025 r., https://www.rp.pl/przestepczosc/art42769991-pozary-w-polsce-kolumbijczyk-mial-dzialac-na-zlecenie-rosji-ustalenia-abw [dostęp: 30 VII 2025].

Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe, https://icct.nl/sites/default/files/2025-09/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool.pdf [dostęp: 16 XII 2025].

Steal, deal and repeat: How cybercriminals trade and exploit your data, Europol, https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data [dostęp: 15 VII 2025].

Szandelszky B., Josek P.D., Jenne P., *Slovak authorities charge 'lone wolf' with assassination attempt on the prime minister*, AP, 16 V 2024 r., https://apnews.com/article/slovakia-prime-minister-shooting-fico-23faba11c0f371ef0f69a34861337ae0 [dostęp: 20 VII 2025].

Wojciechowski S., *Terrorism – old wine in new bottles*, Defence24, 21 VII 2025 r., https://defence24.com/geopolitics/terrorism-old-wine-in-new-bottles [dostęp: 25 VII 2025].

Wojny dronów: jak to się robi w Afryce [ANALIZA], Defence24, 31 V 2025 r., https://defence24.pl/technologie/wojny-dronow-jak-to-sie-robi-w-afryce-analiza#goog_rewarded [dostęp: 18 VII 2025].

Zadražilová J., *Atentátník se k činu rozhodl hned po prezidentských volbách*, Novinky.cz, 15 V 2024 r., https://www.novinky.cz/clanek/zahranicni-atentatnik-se-k-cinu-rozhodl-hned-po-prezidentskych-volbach-rekl-ministr-40471949 [dostęp: 20 VII 2025].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady UE 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88 z 31 III 2017 r.).

Prof. dr hab. Sebastian Wojciechowski

Kierownik Zakładu Studiów Strategicznych i Bezpieczeństwa Międzynarodowego na Wydziale Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza w Poznaniu. Główny analityk Instytutu Zachodniego w Poznaniu. Ekspert ds. bezpieczeństwa, w tym terroryzmu, Organizacji Bezpieczeństwa i Współpracy w Europie. Redaktor naczelny „Przeglądu Strategicznego".

Dwukrotny stypendysta Fundacji na rzecz Nauki Polskiej i Departamentu Stanu USA. Laureat nagrody naukowej Prezesa Rady Ministrów RP oraz nagrody naukowej ufundowanej przez Unię Europejską. Członek m.in.: Komisji Bałkanistyki PAN, Rady Naukowej Centrum Badań nad Terroryzmem Collegium Civitas.

Autor wielu ekspertyz i analiz przygotowanych dla polskich i zagranicznych instytucji, a także publikacji z zakresu stosunków międzynarodowych oraz bezpieczeństwa wewnętrznego i międzynarodowego. Ekspert ds. bezpieczeństwa NATO DEEP eAcademy.

Kontakt: sebastian.wojciechowski@amu.edu.pl

Dr hab. Artur Wejkszner, prof. UAM

Politolog, profesor w Zakładzie Studiów Strategicznych i Bezpieczeństwa Międzynarodowego na Wydziale Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza w Poznaniu. Autor kilkudziesięciu publikacji na temat współczesnych stosunków międzynarodowych oraz problematyki terroryzmu międzynarodowego i radykalizmu islamskiego, m.in. dwutomowej monografii pt. *Europejska armia kalifatu*.

Kontakt: artur.wejkszner@amu.edu.pl

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 125–151

https://doi.org/10.4467/27204383TER.25.048.23035

Artykuł

Rola i znaczenie Eurojustu w przeciwdziałaniu terroryzmowi

The role and significance of Eurojust in countering terrorism

DARIUSZ POŻAROSZCZYK https://orcid.org/0000-0003-0435-0529

Agencja Bezpieczeństwa Wewnętrznego

Abstrakt

W tekście przedstawiono rozwój Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojustu) oraz omówiono instytucje prawne, którymi dysponuje ona w celu realizacji powierzonych jej zadań. Następnie zostały przywołane dane dotyczące spraw terrorystycznych, w których Eurojust udzielił pomocy. Liczby spraw, w które zaangażował się Eurojust, oraz związane z nimi dane zostały zestawione z jednej strony z danymi z lat poprzednich, z drugiej – z danymi odnoszącymi się do terroryzmu zawartymi w raportach European Union Terrorism Situation and Trend Report Europolu. Zabieg ten doprowadził do konfirmacji postawionej hipotezy badawczej, że Eurojust stanowi ważny element złożonego systemu prawno-instytucjonalnego ukierunkowanego na zwalczanie terroryzmu, ale jego rola nie jest dostatecznie odzwierciedlona w jego raportach. W podsumowaniu podjęto próbę udzielenia odpowiedzi na pytania: 1. Dlaczego raporty Eurojustu nie odzwierciedlają w pełni jego pozycji w systemie przeciwdziałania terroryzmowi? 2. Jaką wartość w kontekście rozpoznania zjawiska terroryzmu mają raporty Eurojustu? 3. Co należy zrobić, aby znaczenie praktyczne i jakość merytoryczna tych raportów były większe?

Słowa kluczowe

Eurojust, raport roczny Eurojust, Europol, terroryzm, współpraca sądowa w sprawach karnych, śledztwa transgraniczne

Abstract

The text presents the development of the European Union Agency for Criminal Justice Cooperation (Eurojust) and discusses the legal institutions at its disposal for the performance of its tasks. Next, data was cited concerning terrorist cases in which Eurojust had provided assistance. The number of cases in which Eurojust was involved and the related data were compared, on the one hand, with data from previous years and, on the other hand, with data on terrorism contained in Europol's TE-SAT (European Union Terrorism Situation and Trend Report) reports. This procedure led to the confirmation of the research hypothesis that Eurojust is an important element of a complex legal and institutional system aimed at combating terrorism, but its role is not sufficiently reflected in its reports. The summary attempts to answer the following questions: 1. Why do Eurojust reports not fully reflect its position in the counter-terrorism system? 2. What is the value of Eurojust reports in the context of recognising the phenomenon of terrorism? 3. What should be done to increase the practical significance and substantive quality of these reports?

Keywords

Eurojust, Eurojust Annual Report, Europol, terrorism, judicial cooperation in criminal cases, cross-border investigations

Wprowadzenie

W artykule przedstawiono doroczny raport Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) i przeanalizowano jego znaczenie jako źródła wiedzy o zagrożeniu terrorystycznym w Unii Europejskiej. Ma to na celu weryfikację hipotezy, że o ile Eurojust stanowi ważny element złożonego systemu prawno-instytucjonalnego ukierunkowanego na zwalczanie terroryzmu, o tyle ta rola nie jest dostatecznie odzwierciedlona we wspomnianym raporcie.

Wybór zagadnienia i towarzyszącej mu hipotezy badawczej wynika z tego, że Eurojust odgrywa istotną rolę w koordynowaniu i wspieraniu transgranicznych postępowań karnych i tym samym jest ważnym forum umożliwiającym wymianę informacji na temat prowadzonych postępowań

karnych[1]. Działalność tę wykonuje przy pomocy wielu – opisanych w dalszej części artykułu – instytucji i rozwiązań organizacyjnych. Skutkiem tego jest gromadzenie licznych informacji dotyczących transgranicznych postępowań karnych, w tym w sprawach związanych z terroryzmem. Informacje pozyskiwane i przetwarzane przez Eurojust mają istotne znaczenie dla wspierania konkretnych postępowań. Wspomniane dane pozwalają ponadto na przedstawienie szerszego obrazu działalności realizowanej przez Eurojust, która mogłaby znaleźć odzwierciedlenie w analizowanym raporcie. To jednak nie następuje. Odpowiedź na pytanie o przyczynę tego stanu rzeczy wymaga wskazania, które z informacji gromadzonych przez Eurojust są przedstawiane we wspomnianym raporcie i jaki jest powód podawania wybranych danych. W artykule wyjaśniono, w jaki sposób, mimo niewątpliwych ograniczeń, raport Eurojustu pozwala lepiej zrozumieć złożony i łączący się z wieloma zagadnieniami fenomen terroryzmu. Omówiono także zadania Eurojustu oraz formy, instytucje i praktyki służące do ich realizacji. W ujęciu komparatystycznym zaprezentowano dane dotyczące spraw związanych z terroryzmem, w których Eurojust udzielał pomocy. Z jednej strony za punkt odniesienia posłużyły lata 2022–2023, z drugiej dane dotyczące terroryzmu i sposób ich przedstawienia przez Europol w European Union Terrorism Situation and Trend Report[2] (dalej: TE-SAT). W tym celu wykorzystano raporty Eurojustu z lat 2022–2024 oraz raporty Europolu z lat 2023–2025 , a uwagę skierowano przede wszystkim na rodzaj, źródło pochodzenia i szczegółowość danych zawartych w obu raportach. Przedstawienie tych danych pozwoliło na porównanie obu raportów.

W tekście oprócz metody komparatystycznej zastosowano metodę analizy dokumentów, w tym raportów, materiałów informacyjnych wydawanych przez Eurojust oraz odpowiedniej literatury naukowej.

W podsumowaniu podjęto próbę udzielenia odpowiedzi na pytania badawcze: 1. Dlaczego raporty Eurojustu nie odzwierciedlają w pełni jego pozycji w systemie przeciwdziałania terroryzmowi? 2. Jaką wartość w kontekście rozpoznania zjawiska terroryzmu mają raporty Eurojustu? 3. Co należy zrobić, aby znaczenie praktyczne i jakość merytoryczna tych raportów były większe?

[1] *Eurojust Annual Report 2024,* Luxembourg 2025, s. 3. https://doi.org/10.2812/2312311.

[2] Jest to coroczny raport przygotowywany przez Europol, przedstawiający sytuację i trendy dotyczące terroryzmu w państwach Unii Europejskiej w roku poprzednim.

Rozwój Eurojustu

Geneza Eurojustu wiąże się z postępem integracji europejskiej, początkowo ukierunkowanej na wzmocnienie współpracy ekonomicznej. W latach 70. i 80. XX w., gdy pogłębiała się integracja, wzrastało przeświadczenie, że rozwój kooperacji gospodarczej wymaga zapewnienia szeroko rozumianego bezpieczeństwa. Został podpisany Traktat z Maastricht[3], na podstawie którego powstała Unia Europejska oparta na trzech filarach[4]. Stworzony wówczas III filar nosił nazwę „Współpraca w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych"[5]. Jego kreacja miała służyć pogłębieniu współpracy między krajami wchodzącymi w skład UE w obszarze problematyki przestępczości. Szczegółowy zakres przedmiotowy III filara był wyznaczony przez zawarty w ówczesnym Tytule VI Traktatu o Unii Europejskiej art. K.1, który określał kwestie stanowiące „przedmiot wspólnego zainteresowania", tj.:

1) politykę azylową,
2) zasady regulujące przekraczanie granic zewnętrznych państw członkowskich i sprawowanie nad nimi kontroli,
3) politykę imigracyjną i politykę dotyczącą obywateli krajów trzecich,
4) walkę z narkomanią,
5) walkę z oszustwami na skalę międzynarodową,
6) współpracę sądową w sprawach cywilnych,
7) współpracę sądową w sprawach karnych,
8) współpracę celną,

[3] Traktat o Unii Europejskiej podpisany 7 lutego 1992 r. w Maastricht.

[4] W tej kwestii Krystian Bartosz napisał: „Do czasu wejścia w życie traktatu z Maastricht prawo wspólnotowe obejmowało przede wszystkim przepisy dotyczące gospodarki. Uznawało współpracę w sprawach karnych wyłącznie za suwerenny element polityki wewnętrznej kraju członkowskiego. Traktat ustalony w 1991 roku w Maastricht był niejako odpowiedzią na pogłębiający się problem przestępczości międzynarodowej, a także rosnącej siły organizacji terrorystycznych mogących realnie zagrozić bezpieczeństwu Europy". Zob. szerzej: K. Bartosz, *Prawne aspekty walki z terroryzmem*, „Security, Economy & Law" 2018, nr 1, s. 20. https://doi.org/10.24356/SEL/18/1.

[5] Zalążków III filara należy się dopatrywać w powołaniu wewnętrznej grupy ds. bezpieczeństwa utworzonej przez Radę Europejską w Rzymie w 1975 r. znaną jako TREVI (fr. Terrorisme, Radicalisme, Extrémisme, Violence Internationale). Już w 1976 r. w ramach TREVI wyłoniły się dwie podgrupy: TREVI I i TREVI II. Zadaniami TREVI I, której powstanie łączyło się ze wzmożoną działalnością takich organizacji terrorystycznych jak IRA, Czarny Wrzesień czy też RAF, miały być usprawnienie przepływu informacji na temat organizacji terrorystycznych oraz wspólna analiza generowanych przez nie zagrożeń.

9) współpracę policyjną w celu zapobiegania terroryzmowi i walki z nim, walki z nielegalnym handlem narkotykami i innymi poważnymi formami międzynarodowej przestępczości, włącznie z koniecznymi formami współpracy celnej, w związku ze zorganizowaniem obejmującego całą Unię systemu wymiany informacji w ramach Biura Policji Europejskiej (Europol).

Analiza art. K.1 wskazuje, że podstawowym motywem współpracy w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych było zapewnienie swobodnego przepływu osób. Szczegółowa interpretacja wskazanych „spraw wspólnego zainteresowania" pozwala stwierdzić, że za największe zagrożenia, z którymi miano się mierzyć w ramach III filara, uznano nielegalną imigrację, przestępczość zorganizowaną i terroryzm[6].

W następnych latach integracja europejska nabierała tempa. Na podstawie Traktatu Amsterdamskiego[7] zmieniono nazwę III filara na „Współpraca policyjna i sądowa w sprawach karnych" oraz wzmocniono kooperację w dziedzinie bezpieczeństwa, m.in. przez przeniesienie części zagadnień z III filara do uwspólnotowionego I filara.

Kolejnym istotnym etapem rozwoju było specjalne posiedzenie Rady Europejskiej, które odbyło się w dniach 15–16 października 1999 r. w fińskim mieście Tampere. Poświęcono je tworzeniu obszaru wolności, bezpieczeństwa i sprawiedliwości w UE. Omawiano na nim plany powołania organu sądowego mającego wzmocnić współpracę między organami krajowymi w zakresie zwalczania poważnej przestępczości zorganizowanej o charakterze transgranicznym[8]. W marcu 2001 r. w Brukseli, na podstawie decyzji

[6] Te zjawiska, a także cyberprzestępczość oraz handel ludźmi jako podstawowe zagrożenia wynikające z globalizacji wymienia również Marek Fałdowski. Zob. M. Fałdowski, *Międzynarodowa Organizacja Policji Kryminalnych – Interpol w zwalczaniu wybranych zagrożeń XXI w.*, „Wiedza Obronna" 2023, t. 282, nr 1, s. 198. https://doi.org/10.34752/2023-i282.

[7] *Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie oraz niektóre związane z nimi akty*.

[8] *Eurojust: Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych*, Haga 2020, s. 2. https://doi.org/10.2812/556790. W pkt. 46 konkluzji ze spotkania Rady Europejskiej w Tampere stwierdzono: „Pragnąc wzmocnić walkę ze zorganizowaną przestępczością, Rada Europejska zgodziła się co do tego, że powinna zostać utworzona jednostka o nazwie Eurojust, w skład której weszliby prokuratorzy, urzędnicy związani z wymiarem sprawiedliwości oraz oficerowie policji z poszczególnych państw członkowskich, zgodnie z ustawodawstwem krajowym. Eurojust byłby odpowiedzialny za koordynowanie działań krajowych organów prokuratorskich oraz wspieranie dochodzeń w sprawach karnych z dziedziny przestępczości zorganizowanej, przede wszystkim na podstawie analiz Europolu i w ścisłej współpracy z Europejską Siecią Sądową (...)".

Rady UE 2000/799/WSiSW z 14 grudnia 2000 r., rozpoczęła działalność Tymczasowa Jednostka ds. Współpracy Sądowej (Provisional Judicial Cooperation Unit), znana również pod nazwą Pro-Eurojust. Zamachy terrorystyczne w USA z 11 września 2001 r. stanowiły kolejny czynnik implikujący potrzebę zacieśnienia współpracy międzynarodowej, co skutkowało przyspieszeniem prac nad tworzeniem Eurojustu[9]. Organ ten został oficjalnie ustanowiony decyzją Rady 2002/187/WSiSW z 28 lutego 2002 r.[10] jako Europejska Jednostka Współpracy Sądowej. Cele Eurojustu określono w art. 3 wskazanej decyzji. Obejmowały one stymulowanie i poprawę koordynacji oraz współpracy między krajowymi organami śledczymi i organami ścigania, a także wspieranie na inne sposoby właściwych władz państw członkowskich w celu usprawnienia dochodzenia i ścigania w odniesieniu do poważnej przestępczości, szczególnie przestępczości zorganizowanej, dotyczącej dwóch lub więcej państw członkowskich. W tym miejscu należy zasygnalizować, że dokonane wówczas i utrzymane do chwili obecnej ograniczenie kompetencji Eurojustu do działań wobec przestępstw dotyczących więcej niż jednego państwa członkowskiego UE w istotny sposób wpływa na zakres danych gromadzonych przez ten organ. W przeciwieństwie do danych gromadzonych przez Europol i przedstawianych w raportach TE-SAT raporty Eurojustu podają jedynie informacje dotyczące spraw związanych z terroryzmem o charakterze transgranicznym, w których ściganie Eurojust był zaangażowany[11].

W następnych latach zarówno funkcjonowanie Eurojustu, jak i dotyczące go podstawy normatywne oraz założenia polityczne podlegały dalszym zmianom. W dniu 16 grudnia 2008 r. Rada UE przyjęła decyzję 2009/426/WSiSW w sprawie zmiany decyzji 2002/187/WSiSW[12], co doprowadziło do wzmocnienia koordynacyjnej roli Eurojustu. Dokonana wówczas reforma zakładała utworzenie Krajowego Systemu Koordynacyjnego Eurojustu, tzw. ENCS (Eurojust National Coordination System), którego zadaniami były usprawnienie przepływu informacji między Eurojustem i państwami członkowskimi oraz lepsze zarządzanie sprawami, m.in. przez pomoc w identyfikacji, czy sprawa powinna zostać skierowana do Eurojustu czy Europejskiej Sieci Sądowej oraz ustalenie właściwych organów do realizowania

[9] *Eurojust: Agencja Unii Europejskiej ds. Współpracy…*, s. 2.

[10] *Decyzja Rady z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością.*

[11] Ta kwestia zostanie szczegółowo rozwinięta w dalszej części artykułu.

[12] *Decyzja Rady 2009/426/WSiSW z dnia 16 grudnia 2008 r. w sprawie zmiany decyzji 2002/187/WSiSW ustanawiającej Eurojust w celu zintensyfikowania walki z poważną przestępczością.*

wniosków i decyzji związanych ze współpracą międzynarodową w sprawach karnych. ENCS działa w każdym państwie członkowskim UE. Jest zarządzany przez krajowych korespondentów Eurojustu oraz opiera się na punktach kontaktowych, które funkcjonują na mocy odrębnych przepisów[13].

W związku z podpisaniem Traktatu z Lizbony[14] aktualnie podstawy normatywne Eurojustu w prawie pierwotnym są określone w art. 85 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którym: *Zadaniem Eurojust jest wspieranie oraz wzmacnianie koordynacji i współpracy między krajowymi organami śledczymi i organami ścigania w odniesieniu do poważnej przestępczości,* ***która dotyka dwóch lub więcej Państw Członkowskich***[15] *lub która wymaga wspólnego ścigania, w oparciu o operacje przeprowadzane i informacje dostarczane przez organy Państw Członkowskich i Europol.* Do najważniejszych zadań Eurojustu opisanych w art. 85 TFUE należą:

a) wszczynanie śledztwa oraz występowanie z wnioskiem o wszczęcie ścigania prowadzonego przez właściwe organy krajowe, w szczególności dotyczącego przestępstw przeciwko interesom finansowym Unii,
b) koordynacja śledztw i ścigania, o których mowa w literze a),
c) wzmacnianie współpracy sądowej, w tym przez rozstrzyganie sporów o właściwość i ścisłą współpracę z Europejską Siecią Sądową.

Rezultatem ewolucji Eurojustu są dwa akty. Pierwszym jest – realizujące postanowienia Traktatu z Lizbony[16] – przyjęte 14 listopada 2018 r. rozporządzenie 2018/1727[17], które z dniem 12 grudnia 2019 r. zastąpiło decyzję 2002/187/WSiSW. Na jego podstawie Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych stała się następcą prawnym Eurojustu ustanowionego na mocy decyzji Rady 2002/187/WSiSW[18]. Grażyna Stronikowska wskazuje, że: *Celem rozp. 2018/1727 jest*

[13] G. Stronikowska, *Prokuratura Europejska jako instytucja ochrony interesów finansowych Unii Europejskiej*, Warszawa 2020, s. 231.

[14] *Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską*.

[15] Wyróżnienie pochodzi od autora (przyp. red.).

[16] Zob. G. Stronikowska, *Prokuratura Europejska jako instytucja…*, s. 250.

[17] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW*.

[18] Stronikowska wskazuje, że dokonana na mocy rozporządzenia 2018/1727 sukcesja obejmuje również wszelkie umowy i inne zobowiązania, które zaciągnął Eurojust, działając

dostosowanie Eurojustu do wymogów art. 85 TFUE poprzez wprowadzenie mechanizmu oceny jego działań przez Parlament Europejski i parlamenty narodowe, przyjęcie w miejsce decyzji formy rozporządzenia oraz przystosowanie agencji do współpracy z nowo powstającą PE[19]. Stronikowska podkreśla, że rozporządzenie 2018/1727 nie wprowadziło radykalnych zmian co do sposobu funkcjonowania Eurojustu i realizowanych przez niego zadań, odgrywało raczej rolę porządkującą i doprecyzowującą[20]. Należy wskazać, że w związku z rezygnacją z formalnego powiązania kompetencji przedmiotowej Eurojustu z właściwością przedmiotową Europolu zdefiniowano właściwość Eurojustu przez odwołanie się do rodzajów poważnej przestępczości wskazanych w załączniku do rozporządzenia 2018/1727[21].

Drugim aktem jest rozporządzenie 2023/2131 z 4 października 2023 r.[22] dotyczące cyfrowej wymiany informacji, który to akt ma usprawnić działanie powołanego w 2019 r. Rejestru Antyterrorystycznego Eurojust (Counter-Terrorism Register, dalej: CTR)[23]. Baza ta jest wykorzystywana do gromadzenia informacji o postępowaniach sądowych dotyczących terroryzmu. Zawiera m.in. dane na temat tożsamości podejrzanych o czyny związane

na podstawie decyzji 2002/187/WSiSW. Zob. G. Stronikowska, *Prokuratura Europejska jako instytucja…*, s. 251.

[19] Prokuratura Europejska (ang. European Public Prosecutor's Office, EPPO) jest to samodzielna jednostka działająca na podstawie *Rozporządzenia Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażającego wzmocnioną współpracę (art. 20 TUE i 329 TFUE) w zakresie ustanowienia Prokuratury Europejskiej*. Zakres właściwości rzeczowej i funkcjonalnej Prokuratury Europejskiej obejmuje prowadzenie postępowań przygotowawczych oraz wnoszenie i popieranie aktów oskarżenia przeciwko sprawcom przestępstw naruszających interesy finansowe Unii Europejskiej.

[20] G. Stronikowska, *Prokuratura Europejska jako instytucja…*, s. 251.

[21] Wśród form poważnej przestępczości, w odniesieniu do których Eurojust jest właściwy do podejmowania działań, wskazany załącznik wymienia terroryzm.

[22] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2131 z dnia 4 października 2023 r. w sprawie zmiany rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 oraz decyzji Rady 2005/671/WsiSW w odniesieniu do cyfrowej wymiany informacji w sprawach związanych z terroryzmem*.

[23] CTR to specjalna baza danych utworzona przez Eurojust w celu wzmocnienia reakcji, zwłaszcza przez przetwarzanie odpowiednich informacji, na zagrożenia terrorystyczne w państwach członkowskich UE. Podstawą CTR jest *Decyzja Rady 2005/671/WSiSW z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy dotyczącej przestępstw terrorystycznych*. CTR został uruchomiony jednak dopiero 1 IX 2019 r., w odpowiedzi na zamachy terrorystyczne z 13 X 2015 r. w Paryżu. Zob. szerzej: *Launch of Judicial Counter-Terrorism Register at Eurojust*, Eurojust, 5 IX 2019 r., https://www.eurojust.europa.eu/news/launch-judicial-counter-terrorism-register-eurojust [dostęp: 9 VIII 2025].

z terroryzmem i ich związkach z sieciami terrorystycznymi, a także inne szczegółowe informacje odnośnie do prowadzonych postępowań. Ze względu na wrażliwość gromadzonych informacji nie ma publicznego dostępu do CTR, co powoduje, że wskazane dane nie są przedstawiane i omawiane w raportach rocznych Eurojustu.

Formy działania i współpracy Eurojustu

Analiza przepisów regulujących funkcjonowanie Eurojustu, w tym zmian, które w nich zachodziły na przestrzeni lat, prowadzą do wniosku, że systematycznie zyskuje on coraz mocniejszą pozycję instytucjonalną w systemie prawnym UE[24], a zakres jego uprawnień się rozszerza. Mimo to nadal nie jest on samodzielnym organem prowadzącym niezależne postępowania przygotowawcze, lecz organem o charakterze pomocniczym. Cztery najważniejsze formy wsparcia udzielanego przez Eurojust w związku z prowadzeniem postępowań przygotowawczych przez właściwe organy państw członkowskich oraz EPPO to[25]:

- wspieranie wspólnych zespołów dochodzeniowo-śledczych[26],
- pomoc w korzystaniu z unijnych narzędzi współpracy sądowej, zwłaszcza z europejskiego nakazu aresztowania[27] i europejskiego nakazu dochodzenia[28],

[24] Aktualnie Eurojust działa na podstawie rozporządzenia, a nie decyzji.

[25] *Eurojust: Agencja Unii Europejskiej ds. Współpracy…*, s. 6–7.

[26] Specjalne zespoły śledcze (ang. Joint Investigation Teams, w skrócie JIT) tworzone na podstawie porozumienia między organami ścigania i wymiaru sprawiedliwości z dwóch lub więcej państw – najczęściej członkowskich UE – w celu prowadzenia wspólnego dochodzenia karnego. Ich celem jest koordynacja działań i bezpośrednia wymiana informacji oraz dowodów. Podstawą tworzenia JIT jest *Decyzja Ramowa Rady 2002/465/WSiSW z dnia 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych*. Szczegóły funkcjonowania JIT z udziałem polskich organów zostały doprecyzowane w Kodeksie postępowania karnego w art. 589b – 589f. Zob. szerzej: K. Leśniewski, *Słów kilka o instytucji wspólnych zespołów śledczych w pryzmacie polskiej procedury karnej*, „Przegląd Prawno-Ekonomiczny" 2019, nr 2(47), s. 177–186.

[27] Europejski nakaz aresztowania to uproszczona forma ekstradycji istniejąca między państwami członkowskimi UE, ustanowiona na mocy *Decyzji Ramowej Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami* członkowskimi. W Kodeksie postępowania karnego ta kwestia jest uregulowana w rozdziałach 65a i 65b.

[28] Europejski nakaz dochodzenia (tzw. END) opiera się na orzeczeniu wydanym przez właściwy organ wymiaru sprawiedliwości/ścigania jednego państwa członkowskiego UE.

– wsparcie przy organizacji spotkań koordynacyjnych[29],
– pełnienie funkcji centrów koordynacyjnych[30].

Omawiając kompetencje i możliwości Eurojustu dotyczące gromadzenia informacji, należy zauważyć, że postępująca globalizacja przekłada się na systematyczny wzrost mobilności ludzi. Skutkuje to m.in. tym, że przestępcy coraz częściej przekraczają zarówno wewnętrzne, jak i zewnętrzne granice państw członkowskich. W związku z tym rośnie potrzeba wspierania walki z poważną przestępczością transgraniczną wykraczającą poza obszar UE, co w praktyce Eurojustu ma wyraz w stałym wzroście liczby wspieranych postępowań, które zostały wszczęte w państwach nienależących do UE [31]. Ten trend powoduje, że niezbędny staje się rozwój, w tym instytucjonalizacja współpracy również z państwami spoza zjednoczonej Europy. Dotyczy to zwłaszcza zwalczania skomplikowanych przestępstw w obszarze nielegalnej migracji, przemytu i walki z terroryzmem. W marcu 2024 r. Eurojust przyjął *Strategię o kooperacji z partnerami międzynarodowymi na lata 2024–2027*, która określa działania ukierunkowane na wzmocnienie jego roli w zakresie współpracy z organami ścigania działającymi zarówno w ramach UE, jak i poza jej granicami.

W kontekście współpracy Eurojustu z krajami trzecimi należy wskazać, że aktualnie ma on swoje punkty kontaktowe w ponad 70 krajach oraz w trzech organizacjach międzynarodowych. Co więcej, ta sieć jest stale

Celem END jest przeprowadzenie w innym kraju UE wskazanych czynności procesowych ukierunkowanych na uzyskanie dowodów. Podstawą funkcjonowania END jest *Dyrektywa Parlamentu Europejskiego i Rady 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach* karnych. W Kodeksie postępowania karnego ta kwestia jest uregulowana w rozdziałach 62c i 62d.

[29] Spotkania koordynacyjne to forma współpracy umożliwiająca kontakty organów sądowych i organów ścigania z państw członkowskich UE oraz w niektórych przypadkach z państw trzecich. W ramach spotkań koordynacyjnych uczestnicy mają możliwość wymienienia się informacjami oraz omawiania i rozwiązywania problemów prawnych typowych dla współpracy transgranicznej, które najczęściej dotyczą konfliktów jurysdykcyjnych oraz kwestii przejęć i przekazań prowadzonych postępowań karnych. Spotkania koordynacyjne stwarzają również możliwość wypracowywania planów dotyczących dalszego prowadzenia postępowań karnych, w tym omówienia ewentualnej potrzeby powołania JIT. Zob. szerzej: *Eurojust: Agencja Unii Europejskiej ds. Współpracy…*, s. 7.

[30] Centra koordynacyjne Eurojustu stanowią specjalną formę współpracy, która jest organizowana w celu zarządzania w czasie rzeczywistym skoordynowanymi operacjami wymierzonymi w zorganizowane grupy przestępcze lub sieci terrorystyczne. Zob. szerzej: *Eurojust: Agencja Unii Europejskiej ds. Współpracy…*, s. 7.

[31] Tamże, s. 10.

rozwijana – w 2024 r. punkt kontaktowy został zorganizowany w Zjednoczonych Emiratach Arabskich oraz wznowiono działalność tego typu punktów w Nigerii i Mongolii[32]. Dwanaście państw trzecich delegowało do Eurojustu swoich prokuratorów łącznikowych – są to: Albania, Gruzja, Islandia, Mołdawia, Czarnogóra, Macedonia Północna, Norwegia, Serbia, Szwajcaria, Ukraina, Wielka Brytania i Stany Zjednoczone. Z wymienionymi państwami oraz dodatkowo z Liechtensteinem Eurojust ma podpisane umowy (porozumienia), które umożliwiają współpracę w zakresie wymiany informacji obejmujących również materiały o charakterze dowodowym i dane personalne. Z dziewięcioma kolejnymi krajami, tj. Nigerią, Panamą, Kostaryką, Boliwią, Chile, Ekwadorem, Peru, Egiptem i Koreą Południową, Eurojust zawarł tzw. porozumienia robocze umożliwiające strategiczną kooperację w zakresie wymiany informacji, w tym dzielenia się najlepszymi praktykami, jednak bez przekazywania informacji operacyjnych. Eurojust podpisał również porozumienie robocze z Iberoamerykańskim Stowarzyszeniem Prokuratorów (AIAMP)[33].

Eurojust jest ponadto zaangażowany w wiele dodatkowych działań bądź inicjatyw, umożliwiających lub przynajmniej stwarzających warunki do wymiany informacji relewantnych dla zwalczania przestępczości międzynarodowej. W październiku 2024 r. jego przedstawiciele uczestniczyli w pierwszym szczycie szefów prokuratur państw G20, którego gospodarzem była Federalna Prokuratura Brazylii. Udział w tym wydarzeniu został wykorzystany do zorganizowania spotkań dwustronnych z reprezentantami Argentyny, Australii, Brazylii, Chile, Egiptu, Indii, Nigerii, Arabii Saudyjskiej, Republiki Południowej Afryki, Zjednoczonych Emiratów Arabskich i Wielkiej Brytanii, które w przyszłości mogą zaowocować rozwojem

[32] *Eurojust Annual Report*..., s. 14. Warto wskazać, że Nigeria od lat mierzy się z terroryzmem islamskim szerzonym przede wszystkim przez organizację Boko Haram. Zob. szerzej: A. Wejkszner, *Boko Haram – the evolution of jihad activity in Nigeria 2015–2019,* „Przegląd Strategiczny" 2020, nr 13, s. 349. https://doi.org/10.14746/ps.2020.1.21. Należy również dodać, że według corocznego raportu *Global Terrorism Index* (GTI) opracowywanego przez Institute for Economics & Peace (IEP) Nigeria w 2025 r. przesunęła się z 8. na 6. miejsce wśród państw najbardziej dotkniętych terroryzmem. Równocześnie ten kraj jest ważnym partnerem gospodarczym UE, a jego postępująca destabilizacja grozi zachwianiem sytuacji w całym rejonie Sahelu, co może skutkować radykalnym wzrostem niepożądanej imigracji na teren UE. Rozwijanie wszelkich form współpracy z tym państwem ukierunkowanych na rozpoznawanie i zwalczanie terroryzmu należy więc uznać za niezwykle pożyteczne.

[33] *Eurojust Annual Report*..., s. 15.

współpracy z tymi państwami[34]. Należy podkreślić, że dobra współpraca z niektórymi z wymienionych państw, jak np. Nigerią[35], Arabią Saudyjską[36] czy Wielką Brytanią[37], może mieć szczególnie istotne znaczenie w zapobieganiu terroryzmowi i zwalczaniu go. Podobne pozytywne efekty może przynieść współorganizacja przez Eurojust wizyt studyjnych przedstawicieli prokuratur generalnych z Kazachstanu, Kirgistanu, Tadżykistanu, Turkmenistanu i Uzbekistanu[38] oraz udział przedstawicieli Eurojustu w warsztatach zorganizowanych w Bagdadzie, które były poświęcone zagadnieniom współpracy organów sądowych.

Oprócz tego, że są organizowane jednorazowe spotkania z niektórymi państwami, rozwijane są również bardziej trwałe formy współpracy. Przykładem jest EuroMed Justice Project, którego celem jest wzmacnianie transgranicznej współpracy w sprawach kryminalnych pomiędzy krajami UE a państwami takimi jak: Algieria, Egipt, Izrael, Jordania, Liban, Libia, Maroko, Palestyna i Tunezja. W ramach wskazanego programu zostało zorganizowanych m.in. 18 spotkań roboczych[39]. Warto wspomnieć również o projekcie Western Balkans Criminal Justice Project, w ramach którego Eurojust zacieśnia współpracę z Albanią, Bośnią i Hercegowiną, Kosowem, Macedonią Północną, Czarnogórą i Serbią i jak dotąd wsparł 25 postępowań transgranicznych, w tym dotyczących prania pieniędzy i przemytu broni. Wśród szczegółowych form wsparcia należy wymienić m.in. pomoc

[34] Tamże, s. 13.

[35] Zob. przyp. 32.

[36] Warto zwrócić uwagę na analizy dotyczące udziału ruchu wahabistycznego, wspieranego i odgrywającego ogromną rolę w państwie Saudów, w rozwoju terroryzmu islamskiego, zawarte w pracy Michała Harkota. Zob. M. Harkot, *Wpływ wahabizmu na pozycję społeczno-polityczną Arabii Saudyjskiej*, „Annales Universitatis Mariae Curie-Skłodowska Lublin – Polonia" 2020, nr 1, t. 27, s. 97–110. https://doi.org/10.17951/k.2020.27.1.97-110.

[37] Znaczenie współpracy z Wielką Brytanią w zakresie zwalczania terroryzmu wynika z tego, że ten kraj wielokrotnie mierzył się z motywowanym różnymi względami terroryzmem, co przekłada się na bogate doświadczenie brytyjskich służb w zwalczaniu tego zagrożenia.

[38] Na znaczne zaangażowanie mieszkańców Azji Centralnej w terroryzm dżihadystyczny wskazuje np. Krzysztof Strachota. Zob. K. Strachota, *Państwo Islamskie Chorasanu – nowa odsłona światowego dżihadu*, Ośrodek Studiów Wschodnich, 29 III 2024 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-03-29/panstwo-islamskie-chorasanu-nowa-odslona-swiatowego-dzihadu [dostęp: 15 VIII 2025].

[39] *Eurojust Annual Report*..., s. 16.

w organizacji trzech nowych wspólnych zespołów śledczych oraz dwóch tzw. dni akcji[40].

Oprócz współpracy z państwami czy też podmiotami zagranicznymi Eurojust kooperuje z organami ścigania państw członkowskich, jak i innymi unijnymi agencjami powołanymi do zwalczania przestępczości, tj. Europolem, Prokuraturą Europejską oraz Europejskim Urzędem ds. Zwalczania Nadużyć Finansowych[41].

Dane liczbowe dotyczące działalności Eurojustu

Stale powiększająca się sieć podmiotów, z którymi Eurojust współdziała w celu zapobiegania i przestępczości i zwalczaniu jej, przekłada się na systematyczne, w skali rok do roku, zwiększenie liczby spraw, w których udziela on pomocy. W 2019 r. takich spraw było ok. 8000. W 2024 r. liczba ta sięgnęła blisko 13 000, co oznacza wzrost o niemal 60%[42]. Były to sprawy obejmujące 14 kategorii poważnej transgranicznej przestępczości, m.in. przestępczość narkotykową, pranie pieniędzy, przestępstwa/oszustwa finansowe, organizowanie nielegalnej migracji oraz kradzież własności intelektualnej[43]. Trzy pierwsze kategorie stanowiły gros przestępczości zwalczanej przez Eurojust. W 2024 r. był on zaangażowany w ponad 4000 postępowań dotyczących oszustw finansowych i ok. 2000 spraw związanych z obrotem środkami odurzającymi i praniem pieniędzy. Łącznie wskazane trzy kategorie stanowiły ponad 2/3 spraw, w których Eurojust udzielał pomocy[44].

[40] Dni akcji to dni, kiedy w wielu państwach jednocześnie są przeprowadzane złożone działania procesowe, których koordynacja i zarządzanie w czasie rzeczywistym mogą być wspierane przez centra koordynacyjne Eurojustu.

[41] Europejski Urząd ds. Zwalczania Nadużyć Finansowych, znany jako OLAF, z fr. L'Office européen de lutte antifraude, został powołany na podstawie *Decyzji Komisji z dnia 28 kwietnia 1999 r. ustanawiającej Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF)*.

[42] *Eurojust Annual Report…*, s. 7. Równocześnie należy wskazać, że liczba postępowań karnych, w których Eurojust nie udziela pomocy, jest wielokrotnie wyższa – w 2024 r. tylko w Polsce Policja prowadziła 440 269 postępowań przygotowawczych. Zob. *Zwalczanie przestępczości kryminalnej*, Informacyjny Serwis Policyjny, 9 I 2025 r., https://isp.policja.pl/isp/aktualnosci/18325,Zwalczanie-przestepczosci-kryminalnej.html [dostęp: 2 XI 2025].

[43] *Eurojust Annual Report…*, s. 19.

[44] Tamże.

W odniesieniu do powyższych danych trzeba zauważyć, że choć wiele organizacji terrorystycznych działa równocześnie w wielu krajach, a dodatkowo wykorzystywanie nowoczesnych technologii przyczynia się do łatwego rozpowszechniania treści propagujących i ułatwiających terroryzm[45], to jednak liczba postępowań dotyczących terroryzmu, w które Eurojust był zaangażowany w 2024 r., jest wyraźnie mniejsza od dotyczących wskazanych rodzajów przestępczości o typowym kryminalnym i ekonomicznym charakterze. Powyższa sytuacja wydaje się wynikać z co najmniej dwóch przyczyn. Po pierwsze, ogólna liczba przestępstw o charakterze terrorystycznym jest znacznie mniejsza od liczby przestępstw typowo kryminalnych. Po drugie, mimo globalnego rozpowszechniania propagandy wzywającej do przemocy i gloryfikującej akty terroru znaczna część przestępstw terrorystycznych jest popełniana przez osoby działające samotnie, które nie mają rzeczywistych związków z organizacjami typu ISIS czy Al-Kaida, a co najwyżej są poddane wpływowi materiałów przez nie wytwarzanych[46]. Jedynie wirtualny kontakt sprawców wielu przestępstw terrorystycznych z wymienionymi organizacjami i ich członkami, którzy najczęściej przebywają w krajach (na terenach) niezapewniających międzynarodowej pomocy prawnej, powoduje, że sięganie po wsparcie oferowane przez Eurojust jest bezprzedmiotowe. Czasami też zdarza się, że nawet jeśli międzynarodowa pomoc w sprawach karnych teoretycznie jest zasadna i możliwa, to prowadzone postępowania są na tyle nieskomplikowane, że nie zachodzi konieczność angażowania w nie Eurojustu. Przykładem takich śledztw są te, w przypadku których za granicą muszą być wykonane jedynie pojedyncze czynności dowodowe[47]. Istnieje też grupa przestępstw terrorystycznych o charakterze stricte lokalnym – ich skutki ograniczają się do jednego państwa i,

[45] Warto podkreślić, że w wielu państwach już samo rozpowszechnianie treści propagujących terroryzm stanowi przestępstwo. Przykładowo w Polsce jest to penalizowane w art. 255a Kodeksu karnego, w Niemczech w art. 86 StGB (Strafgesetzbuch – niemiecki kodeks karny), a w Austrii w art. 282a öStGB (Österreichische Strafgesetzbuch – austriacki kodeks karny).

[46] Andrzej Czop proponuje określać takie osoby „solo terrorystami". Z kolei za „samotnego wilka" uważa: „sprawcę dokonującego aktów terroru w pojedynkę, całkowicie odizolowanego i pozbawionego powiązań pośrednich oraz bezpośrednich z grupami terrorystycznymi oraz nieposiadającego żadnego dowództwa". Zob. szerzej: A. Czop, *Nowe trendy terroryzmu i możliwości podniesienia efektywności jego zwalczania,* „Studia de Securitate" 2023, nr 13(2), s. 161. https://doi.org/10.24917/26578549.13.2.9.

[47] Kamil Leśniewski zwraca uwagę na konieczność każdorazowego analizowania potrzeby powołania wspólnego zespołu śledczego. Zob. szerzej: K. Leśniewski, *Słów kilka o instytucji…*, s. 181.

co istotne, są one popełniane przez grupy, których obszar aktywności ma również ściśle wyznaczony zakres. W tej kategorii można wymienić grupy korsykańskie aktywne szczególnie w 2023 r.

W 2024 r. w odniesieniu do postępowań karnych dotyczących spraw terrorystycznych Eurojust udzielił wsparcia w 191 przypadkach (63 sprawy nowe i 128 kontynuowanych). W związku z tymi sprawami działało 10 wspólnych zespołów śledczych (w tym dwa nowe, tj. powołane w 2024 r.). Zorganizowano 32 spotkania koordynacyjne i jedno centrum koordynacyjne[48]. Eurojust udzielał również wsparcia w stosowaniu europejskiego nakazu dochodzeniowego w zakresie wniosków o wzajemną pomoc prawną, a także pomagał w realizacji europejskich nakazów aresztowania. Na bieżąco gromadził w CTR informacje od organów krajowych dotyczące trwających i zakończonych postępowań karnych w sprawach o charakterze terrorystycznym, rozbudowując tym samym posiadaną bazę informacji na temat przestępczości, a zwłaszcza osób w nią zaangażowanych[49].

Najwięcej spraw przekazanych Eurojustowi zainicjowały Włochy, Francja, Hiszpania i Niemcy. Największa liczba wniosków o pomoc w sprawach terrorystycznych została natomiast skierowana za pośrednictwem Eurojustu do Holandii i Francji. Wśród krajów spoza UE do Eurojustu najczęściej zgłaszały sprawy Wielka Brytania i Norwegia. Najwięcej wniosków o pomoc zostało natomiast skierowanych do Ukrainy i Wielkiej Brytanii[50].

Na podstawie przedstawionych danych można zauważyć, że udział w międzynarodowych formach współpracy w sprawach karnych ma związek z poziomem zagrożenia terrorystycznego w danym kraju. Państwa, w których dochodzi do wielu przestępstw terrorystycznych, a w konsekwencji w których jest również większa liczba osób zaangażowanych w te przestępstwa, mogących korzystać z unijnej wolności przemieszczania się, w większym stopniu są zmuszone do prowadzenia postępowań transgranicznych, w związku z którymi zwracają się o pomoc do Eurojustu. Raport nie podaje konkretnych danych ani bardziej szczegółowych informacji na temat wskazanych postępowań, ograniczając się jedynie do dość lakonicznego przytoczenia liczby i charakteru poszczególnych czynów. W tym drugim zakresie zostało ogólnie wskazane, że sprawy wspierane przez Eurojust dotyczyły przestępstw terrorystycznych inspirowanych przez różne

[48] *Eurojust Annual Report*..., s. 20.

[49] Tamże.

[50] Tamże.

ideologie i obejmowały takie akty kryminalne, jak: przygotowanie ataków terrorystycznych, udział w organizacjach terrorystycznych, finansowanie terroryzmu, rekrutowanie do organizacji terrorystycznych, podżeganie do czynów terrorystycznych. W omawianym raporcie (również bez wskazywania konkretnych danych) zostało podane, że w niektórych przypadkach postępowania dotyczące przestępstw terrorystycznych obejmowały również czyny o typowo kryminalnym charakterze: zabójstwa/morderstwa, pozbawienie wolności (w tym wzięcie zakładników), nielegalny przemyt broni, materiałów wybuchowych i amunicji[51].

Dla porównania w 2023 r. Eurojust był zaangażowany w 205 spraw mających związek z terroryzmem (70 nowych i 135 przejętych z lat poprzednich). W związku z nimi wspierał 9 wspólnych zespołów śledczych (3 nowe i 6 zainicjowanych w latach poprzednich) oraz zorganizował 22 spotkania koordynacyjne. Raport z 2023 r., w przeciwieństwie do raportu z 2024 r., nie zawiera dodatkowych szczegółów, np. wskazujących państwa, które inicjowały największą liczbę spraw lub do których najczęściej były kierowane wnioski o pomoc[52].

W 2022 r. Eurojust udzielił pomocy w 203 sprawach (53 nowe i 150 zainicjowanych w latach wcześniejszych). W 2022 r. zaangażował się we wsparcie 8 wspólnych zespołów śledczych, spośród których 3 zostały zainicjowane w 2022 r. W analizowanym okresie zorganizowano 21 spotkań koordynacyjnych[53].

Dane z raportów TE-SAT Europolu

Z kolei zgodnie z raportami Europolu, tworzonymi na podstawie danych jakościowych i liczbowych przekazanych przez państwa członkowskie dotyczących ataków terrorystycznych, aresztowań, wyroków skazujących i kar za przestępstwa terrorystyczne, w 2024 r. odnotowano 58 ataków terrorystycznych (34 przeprowadzone, 5 nieudanych i 19 udaremnionych) w 14 krajach członkowskich[54]. Wśród nich 24 były związane z terroryzmem

[51] Tamże.

[52] *Eurojust Annual Report 2023*, Luxembourg 2024, s. 27. https://doi.org/10.2812/356222.

[53] *Eurojust Annual Report 2022*, Luxembourg 2023, s. 52. https://doi.org/10.2812/022275.

[54] *European Union terrorism situation and trend report 2025*, Luxembourg 2025, s. 13. https://doi.org/10.2813/5425593.

dżihadystycznym[55], co oznacza wzrost tego rodzaju ataków, 21 ataków było motywowane anarchizmem i ideologią lewicową[56], 4 miały charakter etnonacjonalistyczny/separatystyczny[57], podłożem 1 była ideologia prawicowa[58], a 8 zakwalifikowano jako niezwiązane z konkretną ideologią. Najbardziej śmiercionośną formą terroryzmu był ten motywowany ideologią dżihadystyczną. W jego wyniku zmarło 5 osób, a 18 zostało rannych. W 20 państwach członkowskich za przestępstwa związane z terroryzmem aresztowano 449 osób. Większość aresztowań dotyczyła terroryzmu dżihadystycznego (289), następnie terroryzmu prawicowego (47), lewicowego i anarchistycznego (28) oraz etnonacjonalistycznego i separatystycznego (27). Za przestępstwa terrorystyczne związane z innymi lub nieokreślonymi formami terroryzmu aresztowano 8 osób[59]. Najwięcej aresztowań miało miejsce w Hiszpanii (90), Francji (69), Włoszech (62) i Niemczech (55)[60].

W 2023 r. w UE odnotowano aż 120 ataków terrorystycznych, w tym 98 przeprowadzonych, 9 nieudanych i 13 udaremnionych. Najwięcej

[55] TE-SAT definiuje dżihadyzm jako agresywny podgatunek salafizmu, odrodzeniowego ruchu sunnickich muzułmanów, który odrzuca demokrację i wybieralne parlamenty, argumentując, że ludzkie prawodawstwo jest sprzeczne ze statusem Boga jako jedynego prawodawcy. Zob. szerzej: *European Union terrorism situation and trend report 2025*..., s. 23. Tłumaczenia w artykule pochodzą od autora (dop. red.).

[56] Zdaniem Europolu lewicowe ugrupowania terrorystyczne dążą do wywołania gwałtownej rewolucji przeciwko politycznemu, społecznemu i ekonomicznemu systemowi państwa, aby ustanowić socjalizm, a ostatecznie komunistyczne i bezklasowe społeczeństwo. Ich ideologia jest często marksistowsko-leninowska. Terroryzm anarchistyczny to termin używany do opisania aktów przemocy dokonywanych przez grupy lub jednostki promujące brak autorytetu jako modelu społecznego. Anarchiści realizują rewolucyjny, antykapitalistyczny i antyautorytarny program. Zob. szerzej: *European Union terrorism situation and trend report 2025*..., s. 34.

[57] Zgodnie z TE-SAT etnonacjonalistyczne i separatystyczne grupy terrorystyczne kierują się nacjonalizmem, przynależnością etniczną i/lub religią. Grupy separatystyczne dążą do wydzielenia dla siebie państwa z większego kraju lub aneksji terytorium jednego kraju do drugiego. Zob. szerzej: *European Union terrorism situation and trend report 2025*..., s. 49.

[58] Według TE-SAT terroryzm prawicowy jest związany z agresywnymi prawicowymi aktorami (grupami lub jednostkami), którzy dążą do użycia przemocy, aby przekształcić cały system polityczny, społeczny i gospodarczy w model autorytarny, odrzucając demokratyczny porządek, wartości i prawa podstawowe. Agresywne ideologie prawicowe posługują się narracjami skoncentrowanymi na wykluczającym nacjonalizmie, rasizmie, ksenofobii i/lub nietolerancji. Zob. szerzej: *European Union terrorism situation and trend report 2025*..., s. 42.

[59] Tamże, s. 8.

[60] Tamże, s. 14.

ataków było motywowanych ideologiami etnonacjonalistyczną i separatystyczną (70)[61], mniej poglądami anarchistycznymi i lewicowymi (32). W opisywanym okresie doszło do 14 ataków dżihadystycznych oraz 2 związanych z ideologią skrajnie prawicową. Aresztowano 426 osób oskarżonych o przestępstwa powiązane z terroryzmem. Najwięcej aresztowań odnotowano w Hiszpanii (84), Francji (78) oraz Belgii (75)[62]. Na czwartym miejscu, jednak z wyraźnie mniejszą liczbą aresztów, znalazły się Niemcy (51). W odniesieniu do rodzaju terroryzmu w 2023 r. najwięcej aresztowań (334) dotyczyło terroryzmu o charakterze dżihadystycznym, 26 osób aresztowano za terroryzm prawicowy, a 14 za lewicowy i anarchistyczny. Działalność terrorystyczna związana z terroryzmem separatystycznym oraz etnonacjonalistycznym skutkowała 25 aresztowaniami, z czego 18 aresztowań w sprawach terrorystycznych powiązano z innymi odmianami terroryzmu, a 9 zakwalifikowano jako nieokreślone[63].

W 2022 r. zarejestrowano 28 ataków, w tym 16 uznano za udane. W tym roku najwięcej było ataków o podłożu lewicowym i anarchistycznym (18, z tego 13 udanych), 6 ataków miało podłoże dżihadystyczne

[61] Do wszystkich ataków o tym charakterze doszło na Korsyce, z tego aż 34 zostały dokonane w nocy z 8 na 9 października 2022 r., i są one oceniane jako reakcja na wizytę na wyspie prezydenta Francji Emmanuela Macrona. Ataki te polegały na detonacji niewielkich ładunków wybuchowych umieszczonych w domkach letniskowych i na placach budowy. Nie spowodowały one poważnych zniszczeń ani ofiar. Zob. szerzej: *France's Corsica rocked by blasts claimed by separatist group*, RFI, 9 X 2023 r., https://www.rfi.fr/en/france/20231009-france-s-corsica-rocked-by-blasts-claimed-by-separatist-group [dostęp: 10 VIII 2025].

[62] Warto wskazać, że w stolicy Belgii znajduje się dzielnica Molenbeek, zamieszkiwana przez bardzo dużą liczbę muzułmanów. Wielu z nich uległo radykalizacji i wyjechało do Syrii i Iraku w celu wspierania ISIS. Dostępne dane za lata 2011–2017 wskazują, że aż 47 osób mieszkających w Molenbeek wyjechało na tereny opanowane przez tzw. Państwo Islamskie. Zob. *Molenbeek. Fabryka terrorystów w stolicy Europy*, Magazyn TVN24, https://archiwum.tvn24.pl/magazyn-tvn24/14/tvn24.pl/magazyn-tvn24/molenbeek-przystan-dzihadystow-w-sercu-europy%2c14%2c296.html [dostęp: 10 VIII 2025]. W przytoczonym artykule jest także wskazane, że właśnie wśród obywateli Belgii ISIS pozyskiwał najwięcej zagranicznych bojowników. Tożsame informacje potwierdzające, że najwyższy wskaźnik wyjazdów do ISIS *per capita* w Europie w II dekadzie XXI w. dotyczył Belgii, przytacza Matthew Levitt. Zob. M. Levitt, *My Journey Through Brussels' Terrorist Safe Haven,* The Washington Institute for Near East Policy, https://www.washingtoninstitute.org/policy-analysis/my-journey-through-brussels-terrorist-safe-haven [dostęp: 10 VIII 2025].

[63] *European Union terrorism situation and trend report 2024*, Luxembourg 2024, s. 11–13. https://doi.org/10.2813/4435152.

(z tego 2 udane) i 4 – prawicowe (1 udany i 3 nieudane). Aresztowano łącznie 380 osób. Z tej liczby 266 aresztowań dotyczyło przestępstw dżihadystycznych, a najwięcej zatrzymań dokonano we Francji (93), Hiszpanii (46), Niemczech (30), Belgii (22), Włoszech (21) oraz Holandii (21). Liczba aresztowań za terroryzm prawicowy wyniosła 45. Odnotowano również 18 aresztowań za terroryzm etnonacjonalistyczny i separatystyczny oraz 19 za terroryzm lewicowy i anarchistyczny. Za inne rodzaje terroryzmu aresztowano 26 osób. W przypadku 6 aresztowań nie sprecyzowano typu terroryzmu, z którym można je łączyć[64].

Oprócz wskazanych informacji raporty Europolu dotyczące przestępstw terrorystycznych zawierają wiele innych danych (chociaż zakres ich prezentacji może się różnić w zależności od wydania), jak np. kraj popełnienia przestępstwa, niekiedy liczbę ofiar z podziałem na zabitych i rannych, niektóre szczegóły dotyczące sprawców, jak ich wiek, płeć i obywatelstwo. Raporty TE-SAT dostarczają również danych dotyczących modus operandi sprawców, w tym informacji na temat używanych narzędzi, wskazując, czy atak został przeprowadzony za pomocą noża, improwizowanego ładunku wybuchowego, drona, broni palnej itd. W niektórych przypadkach są opisane kanały komunikacji oraz wykorzystane technologie. Dane Europolu dostarczają też wiedzy o wyrokach, które zapadły w sprawach związanych z terroryzmem. Ich ważnymi i poznawczo cennymi elementemi są przedstawienie większej liczby (niż w przypadku raportów Eurojustu) rzeczywistych spraw oraz pogłębiona analiza trendów przestępczości terrorystycznej. Z zachowaniem rozróżnienia co do rodzajów terroryzmu są przedstawione informacje dotyczące środowisk z nimi związanych, struktur poszczególnych grup czy organizacji, sposobów rekrutowania, w tym wśród osób pozbawionych wolności, charakterystyki wykorzystywanej propagandy, z podkreśleniem społecznych i politycznych zdarzeń, które są wykorzystywane do zwerbowania nowych sympatyków, sposobów finansowania. W TE-SAT wskazane i analizowane są także wydarzenia mogące mieć szczególny wpływ na poziom przestępczości terrorystycznej. Na przykład w raporcie z 2023 r. dotyczącym 2022 r. został m.in. omówiony możliwy wpływ wojny w Ukrainie na zjawisko terroryzmu[65].

[64] *European Union terrorism situation and trend report 2023*, Luxembourg 2023, s. 10. https://doi.org/10.2813/302117.

[65] Tamże, s. 17.

W TE-SAT 2024[66] skupiono uwagę m.in. na konflikcie w Gazie w kontekście jego wpływu na wzrost radykalizacji prowadzącej do terroryzmu. W TE-SAT 2025 ponownie poruszono temat implikacji izraelskich działań w Strefie Gazy oraz skutków osłabienia syryjskiego reżimu dla sytuacji w regionie[67]. Wspomniano również o rozwoju nowoczesnych technologii w kontekście ułatwiania działalności terrorystycznej, w tym o coraz poważniejszym zagrożeniu związanym z rozwojem druku 3D, za pomocą którego coraz łatwiej można pozyskać broń palną[68].

Porównanie raportów Eurojustu i Europolu

Z przedstawionych informacji wynika, że dane zawarte w TE-SAT są znacznie bardziej szczegółowe i tym samym dają pełniejszy obraz terroryzmu w UE[69]. Niewątpliwie jest to rezultatem tego, że celem raportów Europolu jest dokładne opisanie sytuacji dotyczącej zagrożenia terrorystycznego w krajach unijnych. Szeroki zakres wykorzystanych informacji i poruszonych kwestii implikuje obszerność omawianych dokumentów – przykładowo TE-SAT 2025 ma 75 stron. Dla porównania kwestiom terroryzmu w najnowszym raporcie Eurojustu zostały poświęcone 2 strony.

W tabeli 1 zostały zaprezentowane niektóre różnice pomiędzy dorocznymi raportami Eurojustu i TE-SAT Europolu.

[66] *European Union terrorism situation and trend report 2024*, s. 7.

[67] Raport powstał jeszcze przed upadkiem rządów Bashara Al-Assada, co nastąpiło w grudniu 2024 r.

[68] *European Union terrorism situation and trend report 2025*, s. 9–12.

[69] Na uwzględnienie szerszego kontekstu przez TE-SAT zwracają uwagę również Sebastian Wojciechowski i Artur Wejkszner. Zob. S. Wojciechowski, A. Wejkszner, *Nowe oblicze zagrożenia terrorystycznego w Unii Europejskiej. Analiza „TE-SAT. European Union Terrorism Situation and Trend Report 2024" i innych źródeł*, „Terroryzm – studia, analizy, prewencja" 2025, nr 7, s. 17. https://doi.org/10.4467/27204383TER.25.025.21802.

Tabela 1. Różnice między rocznymi raportami Eurojustu i TE-SAT Europolu.

Kryterium	Raporty Eurojustu	Raporty TE-SAT Europolu
Cel	Przedstawienie współpracy i koordynacji działań dotyczących zwalczania przestępczości transgranicznej. Zaprezentowanie działań Eurojustu w tym zakresie i ich efektów	Monitorowanie zagrożeń terrorystycznych, ich skali i trendów rozwojowych w celu dostarczenia decydentom i osobom zaangażowanym w zwalczanie terroryzmu precyzyjnego i szczegółowego obrazu tego zagrożenia
Zakres tematyczny	Zadania Eurojustu, szczegółowe formy ich realizacji w zakresie zwalczania najpoważniejszej przestępczości transgranicznej oraz ich rezultaty	Zjawisko terroryzmu na obszarze Unii Europejskiej. Jego skala, przejawy, trendy ewolucyjne i czynniki etiologiczne
Szczegółowość	Ogólne dane dotyczące różnych postaci poważnej przestępczości (przestępstwa finansowe, narkotykowe, pranie pieniędzy, handel ludźmi, przestępstwa o charakterze transgranicznym, cyberprzestępstwa, przestępstwa terrorystyczne). Dane dotyczące podstawowych form wsparcia udzielanego przez Eurojust w odniesieniu do poszczególnych rodzajów przestępczości. Zestawienia liczbowe z podziałem na poszczególne typy przestępstw wskazujące państwa, które najczęściej zwracały się do Eurojustu o pomoc i na odwrót	Szczegółowe i pogłębione dane, uzupełnione o dodatkowe analizy dotyczące przestępstw o charakterze terrorystycznym. Opisy i analizy wybranych przestępstw terrorystycznych. Omówienie konkretnych zjawisk wpływających na zwiększenie zagrożenia terrorystycznego (np. atak Izraela na Strefę Gazy, agresja Federacji Rosyjskiej wobec Ukrainy) i zmianę sposobu popełniania przestępstw terrorystycznych (np. rozwój druku 3D jako czynnik wpływający na łatwość uzyskiwania dostępu do broni palnej)

Kryterium	Raporty Eurojustu	Raporty TE-SAT Europolu
Rodzaj danych	Informacje dotyczące spraw związanych z przestępczością o charakterze transgranicznym, w których ściganie Eurojust był zaangażowany. Informacje na temat narzędzi/form wsparcia (wspólne zespoły śledcze, pomoc w korzystaniu z ENA i END, pomoc w organizacji spotkań i centrów koordynacyjnych) udzielanego przez Eurojust. Informacje dotyczące innych form współpracy Eurojustu z partnerami międzynarodowymi (państwa trzecie, organizacje międzynarodowe)	Bardzo szczegółowe dane dotyczące aktów terrorystycznych – liczba zamachów, charakter (podział na terroryzm dżihadystyczny, prawicowy, lewicowy, etnonacjonalistyczny i separatystyczny oraz inny), rezultat (zamachy udane, nieudane i udaremnione). Dodatkowo dane dotyczące liczby aresztowań, wyroków oraz wymiaru wymierzonych kar w związku z przestępstwami terrorystycznymi. Informacje na temat miejsc dokonania ataków, liczby ofiar, charakteru celów (obiekty cywilne, publiczne, związane z infrastrukturą krytyczną), modus operandi
Źródła danych	Prokuratury, sądy, organy ścigania państw członkowskich, partnerzy zagraniczni, OLAF, Interpol, Europol. Brak danych operacyjnych o charakterze wrażliwym/niejawnym, które są gromadzone w CTR	Organy ścigania i służby bezpieczeństwa/specjalne państw członkowskich, Eurojust, materiały własne Europolu przede wszystkim o charakterze analitycznym. Brak danych operacyjnych o charakterze wrażliwym/niejawnym, które są wykorzystywane w podstawowej działalności Europolu

Źródło: opracowanie własne.

Podsumowanie

Porównanie raportów Eurojustu i Europolu oraz stwierdzona szczegółowość tych drugich, zestawione ze wzrastającą rolą Eurojustu i narzędziami, którymi dysponuje, stanowią potwierdzenie postawionej na wstępie hipotezy. Odpowiadając na pytania badawcze, należy stwierdzić, że skromny katalog danych w raportach Eurojustu dotyczących terroryzmu oraz innych

rodzajów przestępczości jest spowodowany tym, że jego raporty z założenia są nastawione na przedstawienie jedynie pewnego aspektu wiążącego się z terroryzmem, a mianowicie postaci, skali i trendów rozwojowych dotyczących współpracy organów ścigania w zapobieganiu temu zjawisku i zwalczaniu go, nie zaś na przedstawienie go w ujęciu całościowym[70]. W przeciwieństwie do danych zawartych w TE-SAT, obejmujących szczegółowe statystyki jakościowe i liczbowe na temat ataków terrorystycznych wraz z pogłębioną analizą poszczególnych rodzajów terroryzmu, dane w raporcie Eurojustu obrazują tylko rozwój i formy współpracy w ramach transgranicznych postępowań karnych. W swoich raportach Eurojust nie ujmuje także szczegółowych danych operacyjnych pozyskanych od podmiotów, którym udziela pomocy, a które są gromadzone w CTR. Ograniczenie to, dotyczące również raportów Europolu, wynika z tego, że informacje na temat osób podejrzewanych o terroryzm nie mogą być publicznie udostępniane zarówno ze względów prawnych, jak i prakseologicznych.

Mimo że dane zawarte w raportach Eurojustu nie dają bezpośredniego obrazu przestępczości terrorystycznej, dzięki przedstawieniu skali współpracy organów ścigania w zakresie przestępczości międzynarodowej kreują dodatkową perspektywę, którą można przyjąć w analizie fenomenu terroryzmu. Pozwala ona przede wszystkim rozpoznać i zbadać trendy rozwojowe dotyczące współpracy transgranicznej w zakresie ścigania przestępstw terrorystycznych. W tym względzie dane wskazujące na systematyczny wzrost liczby spraw, w które angażuje się Eurojust, oraz towarzyszące temu zintensyfikowanie częstotliwości i różnorodności wykorzystywanych narzędzi prawnych, przy braku radykalnego wzrostu przestępczości terrorystycznej, można uznawać za argument przemawiający za tym, że wzrasta zrozumienie korzyści, jakie oferuje Eurojust. Zakładając, że z biegiem czasu będą się rozwijać również umiejętności w korzystaniu z narzędzi i rozwiązań oferowanych przez Eurojust, można przyjąć, że w kolejnych latach będzie stawał się on coraz ważniejszym elementem rozbudowanego systemu prawno-organizacyjnego ukierunkowanego na zapobieganie różnym przestępstwom i ściągnie ich, w tym tych o charakterze terrorystycznym. W tym kontekście można zaproponować, aby w przyszłości w raportach Eurojustu publikowano bardziej szczegółowe dane statystyczne, choćby

[70] Pełniejsze dane pozwalające na wypracowanie obrazu przestępczości terrorystycznej Eurojust prezentuje w innych wydawanych przez siebie materiałach. Zob. np. broszura *Eurojust Meeting on Counter-Terrorism. 27–28 November 2024. Outcome report*, Haga 2025. https://doi.org/10.2812/4325013.

w formie aneksu. Wartość raportów podniosłoby zaprezentowanie dodatkowych informacji dotyczących np. średniego czasu reakcji i realizacji wniosków o pomoc, tak aby można było ocenić efektywność współpracy. Dużą wartość eksplanacyjną miałoby również przytoczenie danych odnoszących się do rezultatów postępowań, np. w ilu przypadkach udało się doprowadzić do skazania, zamrożenia środków finansowych, wykrycia siatek przestępczych. Przedstawienie takich informacji z pewnością pozwoliłoby na bardziej pogłębione oceny dotyczące skuteczności i rozmiarów międzynarodowej współpracy w sprawach karnych i udziału w niej Eurojustu. Na znaczenie jego raportów w kontekście zwalczania terroryzmu pozytywnie wpłynęłaby również prezentacja większej liczby case studies oraz obszerniejsze rozważania dotyczące podstawowego zakresu aktywności Eurojustu, tj. analizy dotyczące problemów we współpracy transgranicznej. Szczegółowe omawianie trudności występujących w śledztwach międzynarodowych, w tym barier i ograniczeń prawnych, a także wypracowanych procedur i dobrych praktyk służących ich przezwyciężeniu, z dużym prawdopodobieństwem prowadziłoby do stopniowej eliminacji wskazanych przeszkód. Taki efekt raportów miałby walor nie tylko poznawczy, lecz także praktyczny.

Bibliografia

Bartosz K., *Prawne aspekty walki z terroryzmem*, „Security, Economy & Law" 2018, nr 1, s. 18–39. https://doi.org/10.24356/SEL/18/1.

Czop A., *Nowe trendy terroryzmu i możliwości podniesienia efektywności jego zwalczania*, „Studia de Securitate" 2023, nr 13(2), s. 153–169. https://doi.org/10.24917/26578549.13.2.9.

Fałdowski M., *Międzynarodowa Organizacja Policji Kryminalnych – Interpol w zwalczaniu wybranych zagrożeń XXI wieku*, „Wiedza Obronna" 2023, t. 282, nr 1, s. 193–210. https://doi.org/10.34752/2023-i282.

Harkot M., *Wpływ wahabizmu na pozycję społeczno-polityczną Arabii Saudyjskiej*, „Annales Universitatis Mariae Curie-Skłodowska Lublin – Polonia" 2020, t. 27, nr 1, s. 97–110. https://doi.org/10.17951/k.2020.27.1.97-110.

Leśniewski K., *Słów kilka o instytucji wspólnych zespołów śledczych w pryzmacie polskiej procedury karnej*, „Przegląd Prawno-Ekonomiczny" 2019, nr 2(47), s. 173–193.

Stronikowska G., *Prokuratura Europejska jako instytucja ochrony interesów finansowych Unii Europejskiej*, Warszawa 2020.

Wejkszner A., *Boko Haram – the evolution of jihad activity in Nigeria 2015–2019*, „Przegląd Strategiczny" 2020, nr 13, s. 349–360. https://doi.org/10.14746/ps.2020.1.21.

Wojciechowski S., Wejkszner A., *Nowe oblicze zagrożenia terrorystycznego w Unii Europejskiej. Analiza „TE-SAT. European Union Terrorism Situation and Trend Report 2024" i innych źródeł*, „Terroryzm – studia, analizy, prewencja" 2025, nr 7, s. 13–33. https://doi.org/10.4467/27204383TER.25.025.21802.

Źródła internetowe

France's Corsica rocked by blasts claimed by separatist group, RFI, 9 X 2023 r., https://www.rfi.fr/en/france/20231009-france-s-corsica-rocked-by-blasts-claimed-by-separatist-group [dostęp: 10 VIII 2025].

Launch of Judicial Counter-Terrorism Register at Eurojust, Eurojust, 5 IX 2019 r., https://www.eurojust.europa.eu/news/launch-judicial-counter-terrorism-register-eurojust [dostęp: 9 VIII 2025].

Levitt M., *My Journey Through Brussels' Terrorist Safe Haven*, The Washington Institute for Near East Policy, 27 III 2016 r., https://www.washingtoninstitute.org/policy-analysis/my-journey-through-brussels-terrorist-safe-haven [dostęp: 10 VIII 2025].

Molenbeek. Fabryka terrorystów w stolicy Europy, Magazyn TVN24, https://archiwum.tvn24.pl/magazyn-tvn24/14/tvn24.pl/magazyn-tvn24/molenbeek-przystan-dzihadystow-w-sercu-europy%2c14%2c296.html [dostęp: 10 VIII 2025].

Strachota K., *Państwo Islamskie Chorasanu – nowa odsłona światowego dżihadu*, Ośrodek Studiów Wschodnich, 29 III 2024 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-03-29/panstwo-islamskie-chorasanu-nowa-odslona-swiatowego-dzihadu [dostęp: 15 VIII 2025].

Zwalczanie przestępczości kryminalnej, Informacyjny Serwis Policyjny, 9 I 2025 r., https://isp.policja.pl/isp/aktualnosci/18325,Zwalczanie-przestepczosci-kryminalnej.html [dostęp: 2 XI 2025].

Inne dokumenty

Eurojust: Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych, Haga 2020, s. 1–12. https://doi.org/10.2812/556790.

Eurojust Annual Report 2022, Luxembourg 2023, s. 1–78. https://doi.org/10.2812/022275.

Eurojust Annual Report 2023, Luxembourg 2024, s. 1–96. https://doi.org/10.2812/356222.

Eurojust Annual Report 2024, Luxembourg 2025, s. 1–52. https://doi.org/10.2812/2312311.

Eurojust Meeting on Counter-Terrorism, 27–28 November 2024, Outcome report, Haga 2025, s. 1–14. https://doi.org/10.2812/4325013.

European Union terrorism situation and trend report 2023, Luxembourg 2023, s. 1–94. https://doi.org/10.2813/302117.

European Union terrorism situation and trend report 2024, Luxembourg 2024, s. 1–74. https://doi.org/10.2813/4435152.

European Union terrorism situation and trend report 2025, Luxembourg 2025, s. 1–75. https://doi.org/10.2813/5425593.

Akty prawne

Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (DzU z 2009 r. poz. 1569).

Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie oraz niektóre związane z nimi akty (Dz. Urz. UE C 340/1 z 10 XI 1997 r.).

Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana) – (Dz Urz. UE C 202/47 z 7 VI 2016 r.).

Traktat o Unii Europejskiej (Dz. Urz. UE C 191/1 z 29 VII 1992 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2131 z dnia 4 października 2023 r. w sprawie zmiany rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 oraz decyzji Rady 2005/671/WsiSW w odniesieniu do cyfrowej wymiany informacji w sprawach związanych z terroryzmem (Dz. Urz. UE L 2023/2131 z 11 X 2023 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz. Urz. UE L 295/138 z 21 XI 2018 r.).

Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej (Dz. Urz. UE L 283/1 z 10 I 2021 r.).

Dyrektywa Parlamentu Europejskiego i Rady 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dz. Urz. UE L 130/1 z 3 IV 2014 r.).

Decyzja Rady 2009/426/WSiSW z dnia 16 grudnia 2008 r. w sprawie zmiany decyzji 2002/187/WSiSW ustanawiającej Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz. Urz. UE L 138/14 z 4 VI 2009 r.).

Decyzja Rady 2005/671/WSiSW z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy dotyczącej przestępstw terrorystycznych (Dz. Urz. UE L z 253/22 z 20 IX 2005 r.).

Decyzja Ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz. Urz. UE L 190/1 z 18 VII 2002 r.).

Decyzja Ramowa Rady 2002/465/WSiSW z dnia 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych (Dz. Urz. UE L 162/1 z 20 VI 2002 r.).

Decyzja Rady z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz. Urz. UE L 63/1 z 6 III 2002 r.).

Decyzja Komisji z dnia 28 kwietnia 1999 r. ustanawiająca Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) – (Dz. Urz. UE L 136/20 z 31 V 1999 r.).

Artykuł wyraża poglądy autora i nie reprezentuje stanowiska Agencji Bezpieczeństwa Wewnętrznego.

Dr Dariusz Pożaroszczyk

Prawnik, funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

ARTYKUŁY RECENZYJNE / RECENZJE

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 155–161

https://doi.org/10.4467/27204383TER.25.049.23036

Recenzja

Jerzy Trocha, Paradygmat bezpieczeństwa dworców kolejowych[1]

Jacek Lasota
Akademia Sztuki Wojennej
https://orcid.org/0000-0002-1136-9829

Małgorzata Lasota
Akademia Sztuki Wojennej
https://orcid.org/0000-0001-7254-5593

Wynalezienie przez Jamesa Watta maszyny parowej w 1763 r. zmieniło oblicze świata. Blisko 200 lat temu powstała pierwsza kolejowa trakcja parowa na świecie, a ponad 180 lat temu zainaugurowano linię kolei żelaznej na polskich ziemiach. Ten rodzaj transportu przede wszystkim „zmniejszył świat" i stał się siłą napędową rozwoju cywilizacji. Linie kolejowe szybko stały się strategicznymi arteriami służącymi celom militarnym. Po raz pierwszy wojsko skorzystało z transportu kolejowego

[1] J. Trocha, *Paradygmat bezpieczeństwa dworców kolejowych*, Warszawa 2025, Akademia Sztuki Wojennej, 200 s.

w 1839 r. w Wielkiej Brytanii na trasie Liverpool–Manchester, ale było to tylko zdarzenie jednostkowe. W 1836 r. ukazał się krótki tekst pruskiego generała Helmutha von Moltkego pt. *Über die militärische Benutzung der Eisenbahn* (pol. O wykorzystaniu kolei na potrzeby wojska). Trzynaście lat później Rosjanie na wezwanie cesarza Franciszka Józefa przerzucili tym środkiem transportu z Krakowa przez Koźle do Uherské Hradiště 15-tysięczną dywizję do walki z węgierskimi powstańcami. Wiele doświadczeń wyniesiono także z wojny secesyjnej, wojny austriacko-pruskiej, prusko-francuskiej, wojny burskiej, a przede wszystkim z I i II wojny światowej. Dziś kolej odgrywa ważną rolę w działaniach wojennych w Ukrainie.

Wiele się mówi o lotniskach czy stadionach, a dworce kolejowe – miejsca, z których codziennie korzystają tysiące ludzi – pozostają w cieniu. A przecież w dobie zagrożeń terrorystycznych, rosnącego natężenia ruchu pasażerskiego i towarowego bezpieczeństwo na dworcach kolejowych jest tematem, który powinien być w centrum uwagi. Rzadko jednak jest on poruszany w polskim piśmiennictwie naukowym. Brakowało dotychczas całościowego, pogłębionego ujęcia tej problematyki. Publikacja Jerzego Trochy pt. *Paradygmat bezpieczeństwa dworców kolejowych* bez wątpienia wypełnia tę lukę i zasługuje na uwagę nie tylko ekspertów ds. bezpieczeństwa i obronności, lecz także wszystkich zainteresowanych funkcjonowaniem kolei jako elementu infrastruktury krytycznej państwa. Tym bardziej że autor robi to z dużym znawstwem.

Trocha współtworzy publikacje dotyczące bezpieczeństwa publicznego i zarządzania kryzysowego, a jego wcześniejsze opracowania, m.in. na temat ochrony ludności, zwróciły uwagę środowisk akademickich i eksperckich. To autor o solidnym zapleczu naukowym i praktycznym. Nie pisze „zza biurka", lecz z pozycji człowieka, który zna funkcjonowanie struktur bezpieczeństwa od środka. Należy do nielicznej grupy autorów, którzy potrafią zintegrować trzy perspektywy: analityka systemowego, funkcjonariusza odpowiedzialnego za bezpieczeństwo oraz obywatela. To połączenie sprawia, że jego książka nie jest jedynie akademickim ćwiczeniem intelektualnym, lecz ma silny potencjał wdrożeniowy.

Co znajdziemy między okładkami

Książka Trochy to solidna monografia naukowa. Jej konstrukcja umożliwia czytelnikowi stopniowe wprowadzenie w temat, a język pozostaje

zrozumiały również dla osób spoza środowiska eksperckiego. Nie jest to typowy podręcznik ani zbiór przepisów prawnych, lecz analityczna opowieść o dworcach, miejscach tak dobrze znanych, że przestajemy je dostrzegać.

Książka jest podzielona na cztery części, które układają się w logiczną strukturę: od historyczno-strukturalnej charakterystyki dworców w Polsce, przez analizę typologii zagrożeń, po opis systemów ochrony i zestaw rekomendacji zmierzających do poprawy obecnego stanu rzeczy.

Rozdział pierwszy ma charakter wprowadzający i kontekstualny. Autor dokonuje w nim przeglądu genezy transportu kolejowego w Polsce, osadzając rozwój kolei na tle historycznych, gospodarczych i politycznych uwarunkowań poszczególnych epok. Szczególną uwagę poświęca wpływowi zaborów na kształtowanie się infrastruktury kolejowej oraz procesy jej odbudowy i rozwoju po odzyskaniu niepodległości w 1918 r. W dalszej części przedstawia współczesne uwarunkowania prawne funkcjonowania dworców kolejowych w Polsce, w tym zagadnienia związane z ich strukturą własnościową i organizacyjną. Klasyfikuje także typy dworców kolejowych w zależności od pełnionych funkcji i skali obsługiwanego ruchu pasażerskiego.

Rozdział drugi stanowi krytyczną analizę czynników zagrażających bezpieczeństwu użytkowników i infrastruktury dworcowej. Trocha identyfikuje i szczegółowo charakteryzuje zarówno zagrożenia intencjonalne (m.in. działalność terrorystyczną oraz przestępstwa i wykroczenia), jak i zagrożenia losowe, w tym zdarzenia pożarowe, awarie techniczne oraz inne sytuacje nadzwyczajne. Autor podkreśla specyfikę dworców kolejowych jako miejsc o wysokiej koncentracji użytkowników, co w połączeniu z publicznym charakterem tych miejsc znacznie zwiększa podatność na wystąpienie incydentów o charakterze kryzysowym. W kontekście współczesnych zagrożeń szczególnie istotny jest omówiony przez autora wpływ kryzysu migracyjnego związanego z konfliktem zbrojnym w Ukrainie na poziom bezpieczeństwa obszarów kolejowych.

W rozdziale trzecim, który ma charakter systemowy i opisowy, Trocha koncentruje się na instytucjonalnych oraz technicznych mechanizmach zapewniania bezpieczeństwa dworców kolejowych. Omawia przede wszystkim rolę ochrony fizycznej, systemów zabezpieczeń technicznych oraz wyspecjalizowanych podmiotów i służb, m.in. Centrum Bezpieczeństwa Dworców Kolejowych, Straży Ochrony Kolei, Policji, a także formy współpracy między nimi. Analizuje również funkcjonowanie struktur zarządzania kryzysowego w sektorze kolejowym oraz znaczenie standardów

międzynarodowych i organizacji ponadnarodowych dla kształtowania praktyk w obszarze ochrony infrastruktury krytycznej.

Rozdział czwarty zawiera podsumowanie, wnioski i rekomendacje. Autor wskazuje najważniejsze problemy i niedoskonałości w aktualnie funkcjonującym systemie zabezpieczeń infrastruktury dworcowej w Polsce oraz przedstawia propozycje działań modernizacyjnych i wdrożeniowych, mających na celu podniesienie poziomu bezpieczeństwa na etapie projektowania, a także w czasie eksploatacji obiektów dworcowych. Szczególną wartość stanowi zestawienie autorskich rekomendacji dotyczących zmian w zakresie organizacyjnym, prawnym i technicznym. Opisane rozwiązania pozwalają – w opinii Trochy – na dostosowanie systemu ochrony dworców do współczesnych zagrożeń i oczekiwań społecznych.

Każdy z rozdziałów pełni odrębną, ale komplementarną funkcję: od zarysowania kontekstu, przez analizę zagrożeń i działań ochronnych, aż po rekomendacje zmian systemowych. Dzięki temu książka stanowi całościowe opracowanie tematu i może być zarówno źródłem wiedzy akademickiej, jak i praktycznym poradnikiem dla osób zajmujących się bezpieczeństwem infrastruktury krytycznej.

Publikacja *Paradygmat bezpieczeństwa dworców kolejowych* zawiera ciekawy materiał ikonograficzny – wykresy i tabele uzupełniają rozważania autora i pozwalają czytelnikowi lepiej zrozumieć treść. Monografia ma przejrzystą typografię i czytelny układ treści. Zwiększa to komfort pracy z tekstem, a przy tego typu publikacjach jest to istotna wartość dodana. Innymi słowy struktura książki umożliwia płynne przejście od diagnozy stanu i analizy zagrożeń, przez ocenę dostępnych mechanizmów ochronnych, aż do sformułowania propozycji zmian ukierunkowanych na poprawę bezpieczeństwa publicznego na dworcach kolejowych. Taki układ treści pozwala na pogłębione poznanie problematyki, a zarazem stanowi punkt wyjścia do dalszych badań naukowych i rozważań praktycznych w tym obszarze.

Mocne i słabe strony publikacji – refleksje subiektywne

Największym atutem publikacji jest jej interdyscyplinarność, łączy bowiem wiedzę z zakresu bezpieczeństwa, historii, prawa i zarządzania. Rzetelna bibliografia, aktualne dane oraz doświadczenie autora budują zaufanie odbiorcy do proponowanych wniosków.

Jednym z mankamentów może być używanie momentami specjalistycznego języka, co dla czytelnika mniej obytego w problematyce czyni niektóre fragmenty trudnymi w odbiorze. Brakuje również pogłębionych porównań z rozwiązaniami wykorzystywanymi za granicą, co mogłoby poszerzyć perspektywę publikacji. Wydaje się, że głównym niedociągnięciem recenzowanej książki jest brak wyjaśnienia terminu „paradygmat" – tego, jak autor go rozumie oraz czym są paradygmaty bezpieczeństwa dworców kolejowych. To wyrażenie pojawia się tylko raz – w tytule. Brak zdefiniowania kluczowego pojęcia stanowi niedopowiedzenie, które może utrudniać klasyfikację publikacji w obrębie ustalonego dyskursu nauk o bezpieczeństwie. Postawienie sobie jasno sprecyzowanego problemu badawczego pozwoliłoby – zdaniem recenzentów – uniknąć tego potknięcia. Uwzględnienie w szerszym wymiarze aparatu naukowego specyficznego dla nauk o bezpieczeństwie jeszcze bardziej podniosłoby walory naukowe tej monografii.

Podsumowanie – dla kogo jest ta książka

Paradygmat bezpieczeństwa dworców kolejowych to publikacja, która wymyka się prostym kategoriom. Nie jest to typowa monografia akademicka, chociaż spełnia wszystkie wymogi naukowości. Nie jest także poradnikiem praktycznym, choć z pewnością może posłużyć jako przewodnik dla zarządców infrastruktury czy funkcjonariuszy. To raczej przemyślany projekt analityczno-społeczny i diagnoza stanu, a zarazem apel o rozsądne i odpowiedzialne planowanie przestrzeni publicznej.

Szczególnie interesujący jest sposób, w jaki autor pokazuje dworzec. Jest to nie tylko obiekt fizyczny, lecz także miejsce styku różnych grup społecznych, interesów, kultur i niestety również zagrożeń. To przestrzeń, w której bezpieczeństwo przestaje być abstrakcją, a staje się codziennym doświadczeniem.

Nie znajdziemy tu nachalnego dydaktyzmu, ale też nie ma pobłażliwości dla bylejakości. Trocha pisze z odpowiedzialnością, która udziela się czytelnikowi. Po lekturze tej książki trudno już patrzeć na dworzec jak na zwykłe miejsce przesiadki.

Recenzowana publikacja zasługuje na uważną lekturę. Została napisana z myślą o specjalistach, ale pozostaje zrozumiała również dla szerszego

grona odbiorców, w tym osób niezwiązanych zawodowo z problematyką bezpieczeństwa. Polecamy ją szczególnie:

- studentom i wykładowcom kierunków związanych z bezpieczeństwem, obronnością, transportem i administracją publiczną,
- pracownikom struktur odpowiedzialnych za ochronę infrastruktury krytycznej,
- urzędnikom samorządowym i planistom przestrzennym,
- a także wszystkim obywatelom, którzy chcą świadomie uczestniczyć w kształtowaniu bezpiecznej przestrzeni publicznej.

Monografia autorstwa Jerzego Trochy[2] to rzadki przykład książki, która z powodzeniem łączy wiedzę ekspercką z poczuciem społecznej odpowiedzialności. Nie tylko diagnozuje problem, lecz także inspiruje do dalszego namysłu i działania. W czasach rosnącej niepewności takich publikacji potrzebujemy więcej.

Płk rez. dr hab. Jacek Lasota, prof. ASzWoj

Oficer dyplomowany, absolwent Wyższej Szkoły Oficerskiej Wojsk Pancernych w Poznaniu, studiów dyplomowych i III stopnia Akademii Obrony Narodowej (AON). Po ukończeniu studiów w 1993 r. pełnił służbę w 9 pz, 6 BKPanc, 34 BKPanc i 2 BOT. Brał udział w działaniach VIII zmiany PKW Irak w 2007 r. Od 2008 r. jest związany zawodowo z AON (od 2016 r. Akademia Sztuki Wojennej, ASzWoj). Obecnie jest dyrektorem Instytutu Historii i Polemologii w ASzWoj. Jego zainteresowania badawcze obejmują zagadnienia związane z teorią i historią sztuki wojennej, polemologią, bezpieczeństwem militarnym.

Kontakt: j.lasota@akademia.mil.pl

[2] Zachęcamy do zapoznania się z inną recenzją tej monografii. Recenzja ukazała się w numerze 33 czasopisma „Przegląd Bezpieczeństwa Wewnętrznego" wydawanego przez Agencję Bezpieczeństwa Wewnętrznego. Zob. E. Jakubiak, *Jerzy Trocha, Paradygmat bezpieczeństwa dworców kolejowych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2025, nr 33, s. 217–221. https://doi.org/10.4467/20801335PBW.25.027.22644 (przyp. red.).

Dr Małgorzata Lasota

Doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie, adiunkt w Katedrze Zarządzania Bezpieczeństwem i Ruchem Lotniczym Instytutu Zarządzania Lotnictwem Cywilnym Akademii Sztuki Wojennej. Ma wieloletnie doświadczenie zawodowe zdobyte w polskich i zagranicznych liniach lotniczych, gdzie pełniła funkcję instruktora personelu pokładowego. Jej zainteresowania badawcze koncentrują się na zarządzaniu bezpieczeństwem w lotnictwie cywilnym oraz szkoleniu, przygotowaniu i procedurach operacyjnych personelu pokładowego, ze szczególnym uwzględnieniem zagadnień związanych z bezpieczeństwem lotów.

Kontakt: m.lasota@akademia.mil.pl

PRACE KONKURSOWE

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 165–200

https://doi.org/10.4467/27204383TER.25.050.23037

Artykuł

Zdolności Sił Zbrojnych Rzeczpospolitej Polskiej w obszarze likwidacji skażeń – wybrane aspekty[1]

Capabilities of the Armed Forces of the Republic of Poland in the area of decontamination – selected aspects

Krzysztof Tokarczyk

Autor niezależny

https://orcid.org/0009-0004-4484-6179

Abstrakt

Artykuł omawia zdolności podsystemu likwidacji skażeń Sił Zbrojnych Rzeczpospolitej Polskiej w kontekście współczesnych wyzwań bezpieczeństwa, ze szczególnym uwzględnieniem zagrożeń chemicznych, biologicznych i promieniotwórczych. Autor dokonał charakterystyki podsystemu likwidacji skażeń – omówił jego strukturę i uwarunkowania funkcjonowania oraz porównał go z podsystemami Niemiec i Stanów Zjednoczonych. Wyniki analizy wskazują na ograniczenia technologiczne, organizacyjne i doktrynalne, które wpływają na efektywność podsystemu. Proponowane rozwiązania obejmują modernizację sprzętu, standaryzację procedur oraz wzmocnienie współpracy wojska z podmiotami pozamilitarnymi. Autor podkreśla także konieczność dostosowania podsystemu do wymogów NATO i współczesnych zagrożeń hybrydowych.

[1] Artykuł powstał na podstawie rozprawy doktorskiej pt. *Zdolność podsystemu likwidacji skażeń Sił Zbrojnych Rzeczpospolitej Polskiej do podjęcia działań* obronionej na Akademii Sztuki Wojennej. Rozprawa została wyróżniona w XIV edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Słowa kluczowe

likwidacja skażeń, Siły Zbrojne RP, CBRN, zdolności operacyjne, bezpieczeństwo

Abstract

This article analyses the capabilities of the decontamination subsystem of the Polish Armed Forces in the context of contemporary security challenges, with particular emphasis on chemical, biological radioactive (CBRN) threats. The author characterised the decontamination subsystem, discussed its structure and operating conditions, and compared it with the subsystems in Germany and the US. The results of the analysis indicate technological, organisational, and doctrinal limitations that impact the subsystem's effectiveness. Proposed solutions include equipment modernisation, procedure standardisation and strengthening cooperation between armed forces and non-military entities. The author emphasises the need to adapt the subsystem to NATO requirements and contemporary hybrid threats.

Keywords

decontamination, Polish Armed Forces, CBRN, operational capabilities, security

Wprowadzenie

Zagrożenia związane z użyciem broni masowego rażenia (BMR) pozostają jednym z istotnych wyzwań dla bezpieczeństwa państwa w kontekście zarówno potencjalnych aktów terrorystycznych, jak i konfliktów zbrojnych. Wskazują na to incydenty tego typu odnotowane w ciągu ostatnich 30 lat:

– 1995 r. – sekta Aum Shinrikyo przeprowadziła atak w tokijskim metrze, rozpylając sarin, co spowodowało śmierć 13 osób i zatrucie kilku tysięcy[2];

[2] *Rozproszenie gazu sarin w Tokio*, Terroryzm!com, 26 XII 2006 r., http://www.terroryzm.com/rozproszenie-gazu-sarin-w-tokio/ [dostęp: 25 VII 2025]; K. Pletcher, *Tokyo subway attack of 1995*, Britannica, 8 V 2025 r., https://www.britannica.com/event/Tokyo-subway-attack-of-1995 [dostęp: 25 VII 2025]; T. Okumara i in., *Report on 640 Victims of the Tokyo Subway Sarin Attack*, „Annals of Emergency Medicine" 1996, t. 26, nr 2, s. 129–135. https://doi.org/10.1016/S0196-0644(96)70052-5.

– 2006 r. – w Londynie otruto byłego oficera rosyjskiej Federalnej Służby Bezpieczeństwa (FSB) Aleksandra Litwinienkę przy użyciu substancji promieniotwórczej polon-210 podanej w herbacie, co w ciągu trzech tygodni doprowadziło do jego śmierci na skutek choroby popromiennej[3];
– 2015 r. i 2017 r. – znany z krytyki Kremla rosyjski polityk i dziennikarz Vladimir Kara-Murza dwukrotnie padł ofiarą podejrzanych zatruć, które doprowadziły do wielonarządowej niewydolności organizmu i śpiączki. W obu przypadkach rosyjskie szpitale i zagraniczne badania potwierdziły zatrucie niezidentyfikowaną substancją chemiczną[4];
– 2018 r. – w Salisbury w Wielkiej Brytanii użyto środka chemicznego nowiczok do próby otrucia byłego oficera rosyjskiego wywiadu wojskowego GRU Siergieja Skripala i jego córki Julii. Substancja naniesiona na klamkę drzwi ich domu doprowadziła do poważnego zatrucia Skripalów oraz funkcjonariusza policji Nicka Baileya, a także do śmierci Dawn Sturgess, która miała przypadkowy kontakt z porzuconą fiolką zawierającą truciznę[5];
– 2020 r. – lider rosyjskiej opozycji Aleksiej Nawalny został otruty środkiem chemicznym nowiczok podczas lotu z Tomska do Moskwy, co doprowadziło do jego hospitalizacji. Trucizna została naniesiona na jego ubranie (prawdopodobnie bieliznę). Obecność substancji potwierdziło pięć laboratoriów certyfikowanych przez Organisation for the Prohibition of Chemical Weapons (pol. Organizacja do spraw Zakazu Broni Chemicznej, OPCW)[6];

---

[3] *Alexander Litvinienko: Profile of murdered Russian spy*, BBC News, 21 I 2016 r., https://www.bbc.com/news/uk-19647226 [dostęp: 26 VII 2025].

[4] *Vladimir Kara-Murza Tailed by Members of FSB Squad Prior to Suspected Poisonings*, Bellingcat, 11 II 2021 r., https://www.bellingcat.com/news/2021/02/11/vladimir-kara-murza-tailed-by-members-of-fsb-squad-prior-to-suspected-poisonings/ [dostęp: 1 VIII 2025].

[5] S. Morris, *UK believes Putin personally authorized Salisbury novichok attack, inquiry told*, The Guardian, 14 X 2024 r., https://www.theguardian.com/uk-news/2024/oct/14/salisbury-novichok-poisonings-inquiry-sergei-skripal-vladmir-putin [dostęp: 25 VII 2025].

[6] F. Gardner, *Navalny 'Novichok poisoning' a test for the West,* BBC News, 2 IX 2020 r., https://www.bbc.com/news/world-europe-54003014 [dostęp: 1 VIII 2025]; *OPCW Issues Report on Technical Assistance Requested by Germany*, OPCW, 6 X 2020 r., https://www.opcw.org/media-centre/news/2020/10/opcw-issues-report-technical-assistance-requested-germany [dostęp: 1 VIII 2025]; D. Steindl i in., *Novichok nerve agent poisoning*, „The Lancet" 2021, t. 397, nr 10270, s. 249–252. https://doi.org/10.1016/S0140-6736(20)32644-1.

– 2017 r. – Kim Dzong Nam, brat przywódcy Korei Północnej, został zaatakowany na lotnisku w Kuala Lumpur przez dwie kobiety, które naniosły na jego twarz paralityczno-drgawkowy środek VX[7].

Incydenty związane z zatruciem obywateli Rosji są przypisywane jednostce FSB specjalizującej się w substancjach toksycznych i są łączone z działaniami rosyjskich służb specjalnych w celu eliminacji przeciwników politycznych Władimira Putina[8].

Wymienione zdarzenia, ze względu na ich celowy charakter i użycie zakazanych substancji przeciwko cywilom, można zaklasyfikować jako akty o charakterze terrorystycznym. Odmienny charakter miało użycie broni chemicznej, mimo obowiązywania konwencji o jej zakazie[9], podczas współczesnych konfliktów zbrojnych:

– w latach 2013–2018 w Syrii – OPCW potwierdziła co najmniej 85 przypadków użycia broni chemicznej[10], głównie sarinu i chloru. Działania te nieoficjalnie są przypisywane reżimowi Baszara al-Asada[11]. Użycie niebezpiecznych substancji spowodowało setki ofiar śmiertelnych i tysiące poszkodowanych[12];

---

[7] *Kim Jong-nam killing: 'VX nerve agent' found on his face*, BBC News, 24 II 2017 r., https://www.bbc.com/news/world-asia-39073389 [dostęp: 26 VII 2025].

[8] *The Lab: How FSB chemical weapons experts tried to poison Alexei Navalny*, The Insider, 14 XII 2020 r., https://theins.ru/en/politics/262611 [dostęp: 1 VIII 2025]; *Zabójstwo Aleksandra Litwinienki*, w: Konsorcjum Mall-CBRN, *Podręcznik zapobiegania i reagowania na zdarzenia CBRNE w centrach handlowych*, https://www.uni.lodz.pl/fileadmin/Projekty/MALL-CBRN/Materials_available_for_download_/Mall-CBRN-Handbook-PL-1.0.pdf, s. 24–25 [dostęp: 2 VIII 2025].

[9] *Konwencja o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów, sporządzona w Paryżu dnia 13 stycznia 1993 r.* Nad przestrzeganiem postanowień Konwencji czuwa jako organ wykonawczy OPCW z siedzibą w Hadze.

[10] W raporcie publicznego nadawcy radiowo-telewizyjnego BBC wskazano, że od września 2013 r. do wiosny 2018 r. na terenie Syrii doszło do 106 przypadków użycia broni chemicznej. Ani w tym, ani w żadnym z oficjalnych raportów Organizacji Narodów Zjednoczonych czy OPCW nie wskazano wprost sprawcy użycia zakazanych substancji. Zob. *Syria: BBC Investigation Reveals Widespread Chemical Weapons Use*, BBC, https://www.bbc.co.uk/programmes/w172w25d6yyjrc0 [dostęp: 25 X 2018].

[11] Inspekcje prowadzone przez OPCW na terenie Syrii potwierdzały użycie zakazanych środków trujących, jednak na podstawie zgromadzonych i zabezpieczonych dowodów nie można było jednoznacznie wskazać podmiotu odpowiedzialnego za ich użycie. Jednocześnie mając na uwadze fakt, że poszkodowanymi w atakach byli tzw. rebelianci oraz społeczność im sprzyjająca, z dużym prawdopodobieństwem można przyjąć, że środki były użyte przez siły wierne reżimowi prezydenta.

[12] *Syria: BBC Investigation Reveals*...

– od lutego 2022 r. w Ukrainie – OPCW odnotowała doniesienia o ponad 3000 przypadków użycia substancji toksycznych, w tym chloropikryny. Inspekcje techniczne OPCW podczas wizji lokalnych zebrały dowody użycia środków i zabezpieczyły stosowne ślady. Z procesowego punktu widzenia dowody są jednak niewystarczające i wymagają dalszego badania, by móc jednoznacznie stwierdzić, że te zdarzenia były spowodowane przez rosyjskie siły[13].

Użycie BMR przez przeciwnika (państwo, organizację, zamachowca) stanowi poważne zagrożenie dla operacji wojskowych, dla organów władzy państwowej w ramach szeroko rozumianego zarządzania kryzysowego, ale również dla nieprzygotowanych na takie ataki cywilów.

Analiza przywołanych zdarzeń uwidacznia ogrom nakładów, jakie należy ponieść, aby wyeliminować lub przynajmniej zminimalizować negatywne skutki skażeń powstałych w wyniku użycia środków chemicznych, biologicznych, radiologicznych i nuklearnych (ang. *chemical, biological, radiological and nuclear*, CBRN)[14]. Zalicza się do tego konieczność posiadania i rozwijania zdolności do prowadzenia szeroko rozumianej likwidacji skażeń (dekontaminacji), zarówno tych wewnętrznych (gdy środki wywołujące skażenie wniknęły przez skórę lub układ pokarmowy do organizmu człowieka), którą wykonują wykwalifikowane jednostki ochrony zdrowia, jak i skażeń zewnętrznych (powierzchniowych), do których unieszkodliwiania są angażowane inne służby, najczęściej siły wydzielone z zasobów Państwowej Straży Pożarnej (PSP) czy Sił Zbrojnych Rzeczpospolitej Polskiej (SZ RP).

Osiągnięta przez poszczególne służby zdolność do likwidacji skażeń musi sprostać usuwaniu (lub niszczeniu) skażeń powstałych zarówno w wyniku aktów terrorystycznych, jak i będących następstwem działań

[13] Sposób użycia zakazanej broni w wojnie rosyjsko-ukraińskiej przypomina działania w Syrii. Wspólną cechą dla obu przypadków jest brak dowodów umożliwiających jednoznaczne wskazanie sprawcy użycia BMR. Zob. *OPCW issues report on third Technical Assistance Visit to Ukraine following an incident of alleged use of toxic chemicals as a weapon*, OPCW, 26 VI 2025 r., https://www.opcw.org/media-centre/news/2025/06/opcw-issues-report-third-technical-assistance-visit-ukraine-following [dostęp: 26 VI 2025].

[14] W Wielkiej Brytanii do operacji rozpoznania skażeń, wielokrotnego pobierania próbek, a przede wszystkim likwidacji skażeń obiektów i terenu po próbie otrucia Siergieja Skripala i jego córki w 2018 r. zaangażowano niemal 800 żołnierzy pułku chemicznego. Działania, których efektem było przywrócenie infrastruktury do użytkowania, trwały prawie rok i pochłonęły miliony funtów. Zob. *Salisbury declared decontaminated after Novichok poisoning*, BBC, 1 III 2019 r., https://www.bbc.com/news/uk-england-wiltshire-47412390 [dostęp: 10 III 2019].

o charakterze militarnym. Należy przy tym uwzględniać przede wszystkim zasoby ludzkie i możliwie zunifikowane procedury postępowania, a także specyfikę potencjalnych zadań, czas oraz miejsce podejmowanych czynności, infrastrukturę, logistykę. Wydaje się zasadne funkcjonowanie na szczeblu państwa spójnego systemu w zakresie interoperacyjności i współdziałania poszczególnych służb w zależności od prowadzonej operacji.

W artykule przedstawiono wybrane aspekty zdolności podsystemu likwidacji skażeń SZ RP jako elementu systemu obrony przed bronią masowego rażenia (OPBMR)[15], w procesie osiągania zdolności do podjęcia działań. W skład podsystemu wchodzą wskazane struktury organizacyjne SZ RP, sprzęt i wyposażenie właściwe dla specyfiki zadań, sprawdzone procedury działania, a także relacje między strukturami zarządzającymi, realizującymi zabiegi likwidacji skażeń i wojskami poddawanymi temu procesowi. Podsystem ten można postrzegać również jako zbiór unikatowych zdolności. Ich osiągnięcie wpływa na potencjalne możliwości poszczególnych pododdziałów, wojsk, struktur organizacyjnych czy całych systemów.

Niniejszy artykuł ma na celu przedstawienie zdolności podsystemu likwidacji skażeń SZ RP, identyfikację jego słabych punktów oraz wskazanie kierunków rozwoju. Analiza opiera się na literaturze przedmiotu, dokumentach doktrynalnych NATO, badaniach autora stanowiących podstawę jego dysertacji oraz przykładach. W ramach dysertacji poszukiwano czynników, które determinują zdolności podsystemu likwidacji skażeń SZ RP oraz sposobów na jego usprawnienie w obliczu współczesnych zagrożeń CBRN[16]. Zastosowano podejście interdyscyplinarne – połączono analizę historyczną, porównawczą i systemową. Analiza posiadanych oraz pożądanych zdolności została przeprowadzona zgodnie z kryteriami DOTMLPFI[17] przyjętymi w NATO, ponieważ w pełni funkcjonalna zdolność

[15] System ten wchodzi w skład funkcjonalnego systemu przetrwania i ochrony wojsk, który tak jak inne systemy funkcjonalne powstał na podstawie Decyzji nr 56/Org./P5 Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie Organizatorów Systemów Funkcjonalnych Sił Zbrojnych RP (niepublikowana).

[16] Problem badawczy w dysertacji brzmiał: „Jakie wymagania powinien spełniać oraz jakie zdolności musi osiągnąć podsystem likwidacji skażeń SZ RP w wymiarze funkcjonalnym i strukturalnym, aby był w pełni gotowy do realizacji zadań, oraz w jaki sposób powinien on być zorganizowany w czasie pokoju i wojny?".

[17] DOTMLPFI to akronim z języka angielskiego utworzony z pierwszych liter poszczególnych komponentów zdolności: *doctrine, organisation, training, material, leader, personnel, facilities, interoperability* (pol. doktryna, organizacja, szkolenie, materiały, przywództwo,

musi uwzględniać nie tylko aspekt techniczny i technologiczny[18], lecz także wszystkie inne czynniki, które mają na nią wpływ.

Artykuł może stanowić punkt wyjścia do dyskusji i dalszych badań w zakresie potrzeby istnienia oraz funkcjonowania na szczeblu państwa międzyresortowego, spójnego systemu dekontaminacji, zdolnego do reagowania zarówno na zdarzenia o charakterze terrorystycznym, jak i w przypadku bojowego użycia zakazanej broni.

Struktura i rola podsystemu likwidacji skażeń SZ RP

Podsystem likwidacji skażeń[19] w SZ RP jest jednym z kluczowych podsystemów systemu OPBMR. Likwidacja skażeń, określana również jako dekontaminacja, ma na celu zapewnienie bezpieczeństwa ludziom, obiektom lub obszarom. Polega na sorpcji, zniszczeniu, neutralizacji, unieszkodliwieniu lub usunięciu chemicznych lub biologicznych substancji skażających albo usunięciu substancji promieniotwórczych z nich lub z ich otoczenia.

Ogólna charakterystyka podsystemu

Główne zadania podsystemu likwidacji skażeń w SZ RP to:

- neutralizacja skażeń chemicznych, biologicznych i radiologicznych w celu ochrony personelu i sprzętu,
- wielopoziomowa likwidacja skażeń personelu, umundurowania, sprzętu, w tym wrażliwego (ang. *sensitive equipment,* SE), oraz terenu,
- wsparcie operacji wojskowych i cywilnych w sytuacjach kryzysowych, takich jak incydenty terrorystyczne czy katastrofy przemysłowe i naturalne.

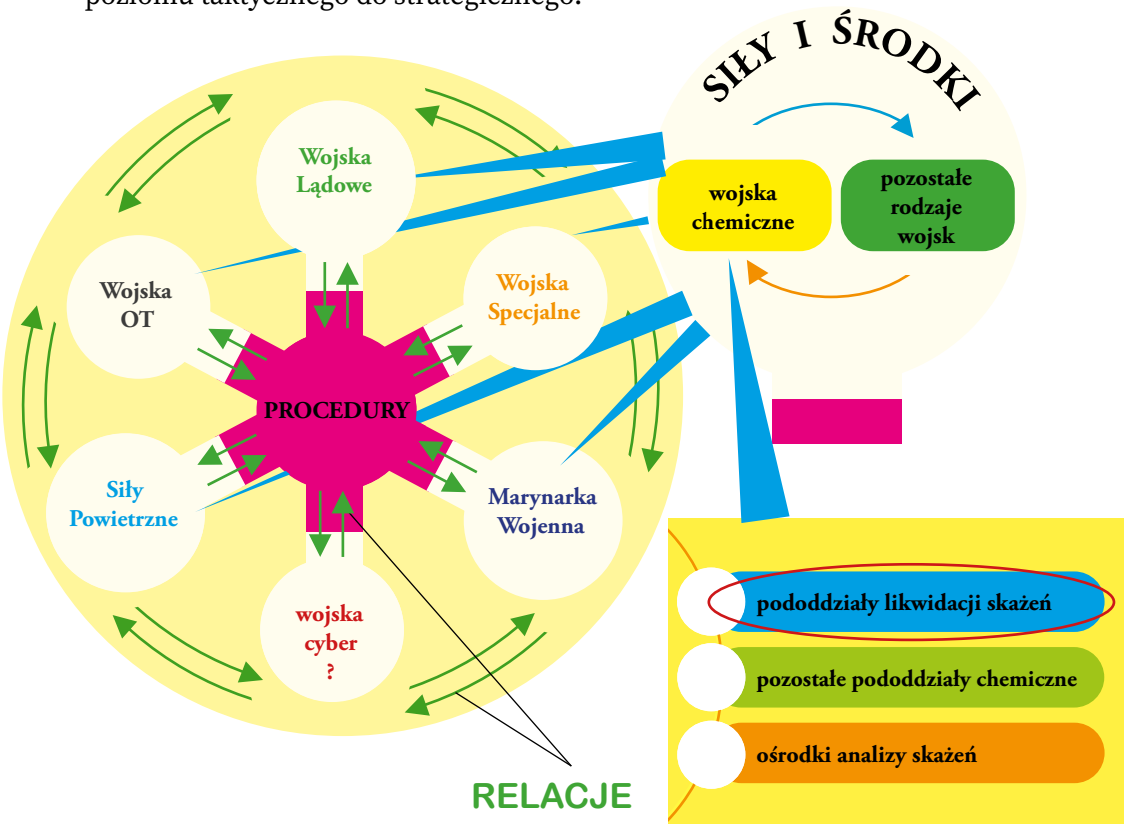
Zdolność żołnierza do przeprowadzania zabiegów likwidacji skażeń rozwija się już na etapie szkolenia podstawowego, jako jedną ze zdolności pozwalających na przetrwanie (ratowanie życia swojego lub innego żołnierza) oraz tworzenie warunków do kontynuowania przydzielonego mu

personel, obiekty i interoperacyjność). Ten rodzaj analizy pozwala na holistyczne postrzeganie zdolności.

[18] Wyposażenie w sprzęt oraz techniczną umiejętność posługiwania się nim.

[19] Zob. *Słownik terminów i definicji NATO* AAP-6(2014), s. 129; *Słownik terminów i definicji NATO dotyczący zagrożeń chemicznych, biologicznych, radiologicznych i nuklearnych* AAP-21(B), s. 18; NO-01-A006:2010 *Obrona przed bronią masowego rażenia. Terminologia*, s. 17.

zadania. Likwidacja skażeń jest zatem obecna i doskonalona na każdym szczeblu organizacyjnym (od żołnierza do komponentu Rodzaju Sił Zbrojnych – rysunek 1), a tym samym na każdym poziomie organizacyjnym – od poziomu taktycznego do strategicznego.



Rysunek 1. Ogólna struktura podsystemu likwidacji skażeń SZ RP.

Źródło: opracowanie własne.

Najszerszy zakres działań w tym obszarze został przypisany żołnierzom pododdziałów likwidacji skażeń wchodzących w skład wojsk chemicznych i mają oni najlepsze wyszkolenie pod tym względem. W cywilnych strukturach państwa dekontaminacja do niedawna była uwzględniana nawet na poziomie polityczno-strategicznym[20]. Im wyższy szczebel organizacyjny

[20] W § 16 pkt 8 lit. f uchylonego *Rozporządzenia Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym* wskazano, że

lub poziom dowodzenia, tym szerszy zakres realizowanych zadań, który w doktrynie wojskowej ogólnie zapisano jako (...) *stworzenie wojskom warunków do realizacji zadań w sytuacjach zagrożenia skażeniami i skażeń*[21].

W każdym przypadku, w ramach procesu planowania zadania, operacji lub misji, uwzględnia się właściwy zakres likwidacji skażeń, który jest funkcją zmiennych takich jak:

- poziom organizacyjny,
- szczebel dowodzenia,
- zadanie, operacja lub misja,
- teatr działań, uwzględniający warunki terenowe, a nawet strefy klimatyczne,
- dostępność infrastruktury terenowej obszaru działań,
- system logistyczny,
- stopień szczegółowości rozpoznawczego przygotowania pola walki,
- przeciwnik, jego zdolności OPBMR i możliwości oddziaływania,
- poziom zagrożenia CBRN,
- siły i środki przeznaczone do realizacji zadania, operacji lub misji,
- warunki meteorologiczne.

Ostatni czynnik odgrywa szczególną rolę, dlatego oddziaływanie sił natury na skażenia bez udziału czynnika ludzkiego zostało potraktowane jako forma likwidacji skażeń (tzw. bierna likwidacja skażeń)[22]. Pogoda, a dokładnie wybrane parametry warunków meteorologicznych, jest uwzględniana w procesie planowania. Ponieważ człowiek nie ma wpływu na te warunki, to aby modelować bądź optymalizować funkcjonowanie systemu, można rozpatrywać tylko kwestie zależne od człowieka. W SZ RP są one traktowane jako aktywna likwidacja skażeń.

w zakres przygotowania stanowisk kierowania poszczególnych organów władzy publicznej wchodzi przygotowanie **punktów zabiegów specjalnych**. Tymczasem w *Rozporządzeniu Rady Ministrów z dnia 25 marca 2025 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym,* które uchyliło uprzedni akt wykonawczy, ogólnie określono, że są realizowane czynności ochronne oraz ratownicze w stosunku do głównego stanowiska kierowania, bez wskazania wykonawcy oraz zakresu tych czynności.

[21] *Obrona przed bronią masowego rażenia w operacjach połączonych* DD/3.8(A), Szkol. 869/2013, s. 14.

[22] Bierna likwidacja skażeń, zwana naturalną likwidacją skażeń lub oddziaływaniem czynników atmosferycznych, jest naturalnym procesem oczyszczania ze skażenia, niewymagającym zaangażowania sił i środków. Obiekty pozostawione do biernego odkażania powinny być izolowane i oznakowane jako niebezpieczne. Zob. *Obrona przed bronią masowego rażenia w operacjach połączonych* DD/3.8(A)..., s. 50.

Likwidacja skażeń realizowana przez SZ RP na rzecz wojsk obejmuje podział ze względu na:

1) środek powodujący skażenie:
   – odkażanie – oddziaływanie na środki chemiczne (C),
   – dezaktywację – oddziaływanie na środki promieniotwórcze (R, N),
   – dezynfekcję – oddziaływanie na środki biologiczne (B),
2) podmiot oddziaływania (wobec którego jest prowadzona likwidacja skażeń):
   – ludzi – zarówno skażonych, nadal zdolnych do realizacji zadań po przeprowadzonych zabiegach, jak i porażonych rannych, dla których zabiegi są etapem wstępnym, pozwalającym na dalszy proces leczenia i rehabilitacji,
   – wyposażenie indywidualnego żołnierza,
   – sprzęt bojowy (lądowy, statki powietrzne i okręty) i uzbrojenie,
   – sprzęt elektroniczny, optyczny, optoelektroniczny, uważany za wrażliwy (SE),
   – obiekty,
   – teren.

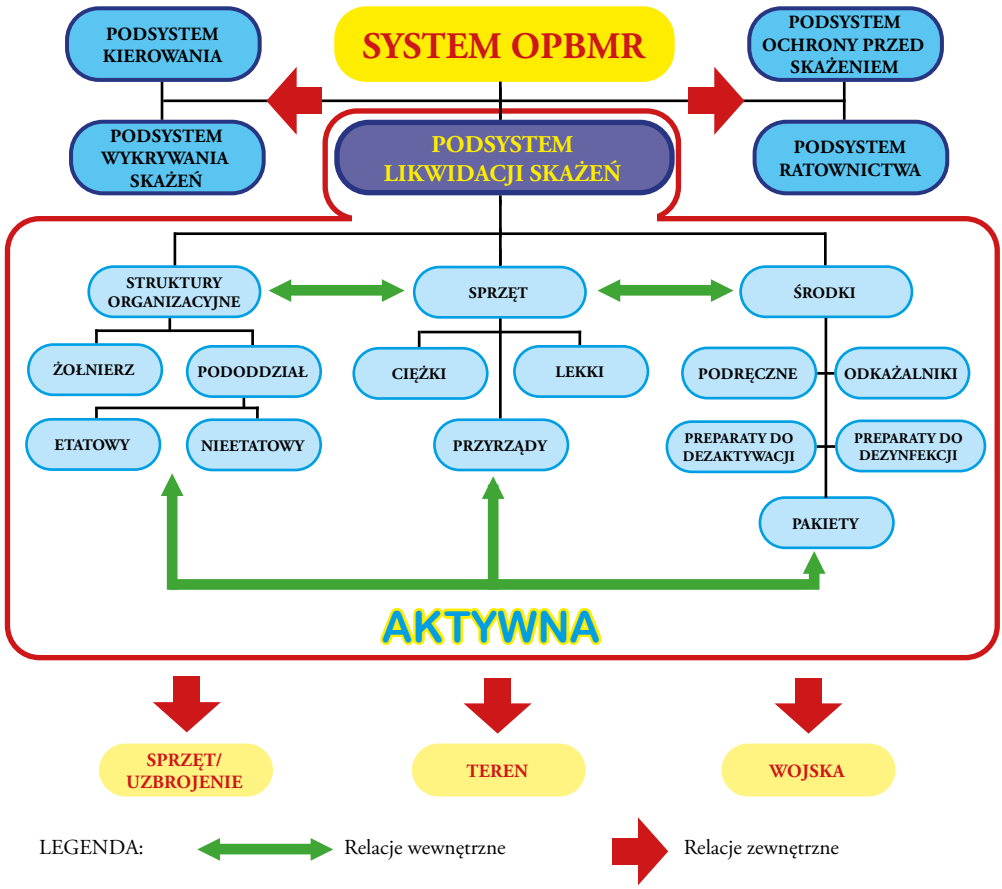
W procesie likwidacji skażeń są stosowane metody mechaniczne, fizyczne i chemiczne[23]. Wybór metody zależy od środka powodującego skażenie oraz od czasu, jaki upłynął od skażenia. Środki chemiczne należy usunąć tak szybko, jak to możliwe, przy użyciu najlepszych dostępnych sposobów. Zasada „tak szybko, jak to możliwe" w OPBMR jest kluczowa.

Struktura podsystemu

Podsystem likwidacji skażeń tworzą (rysunek 2):

- **struktury organizacyjne** (część przedsięwzięć OPBMR jest realizowana przez wszystkich żołnierzy, a zatem każdy żołnierz jest częścią podsystemu),
- **sprzęt**, za pomocą którego są realizowane zadania,
- **środki** bezpośrednio oddziałujące na skażenia,
- **procedury** i **relacje**, określające wykonywanie zadań i zasady współdziałania.

[23] W literaturze przedmiotu można spotkać różne podejście do tego zagadnienia. W artykule przyjęto najczęściej spotykaną nomenklaturę zawartą w instrukcji *Zabiegi specjalne terenu i polowych obiektów obronnych*, Sygn. 1984 Chem. 321, Warszawa 1985 oraz w: A. Leosz, S. Sawczak, *Sprzęt likwidacji skażeń*, WSO–TK wewn. 57/96.



Rysunek 2. Elementy podsystemu likwidacji skażeń SZ RP.

Źródło: opracowanie własne.

Chociaż tylko pododdziały likwidacji skażeń wojsk chemicznych są zdolne do realizacji pełnego spektrum zadań dotyczących tego obszaru tematycznego[24], to natychmiastowe podjęcie właściwych działań zaradczych przez każdego żołnierza po potencjalnym kontakcie ze środkiem

[24] Pododdziały likwidacji skażeń realizują zadania III poziomu, czyli gruntowną likwidację skażeń, głównie w punktach likwidacji skażeń (PLSk). W PLSk jest realizowane pełne spektrum zadań, tj. w stosunku do skażonych ludzi i sprzętu bojowego. W przypadku likwidacji skażeń prowadzonej w ugrupowaniu wojsk (w rejonach rozmieszczenia wojsk) zabiegom podlega przede wszystkim sprzęt. Likwidacja skażeń ludzi wymaga czasu i jest zbyt newralgicznym procesem, aby można było ją prowadzić blisko linii styczności wojsk (w zasięgu podstawowych środków ogniowych przeciwnika).

skażającym ma znaczenie dla jego życia. Z zakresem przydzielonych zadań wiąże się również dobór sprzętu i wyposażenia. Żołnierze pododdziałów likwidacji skażeń posiadają specjalistyczne urządzenia i środki do likwidacji skażeń, podczas gdy żołnierze innych rodzajów wojsk są wyposażani w sprzęt i środki niezbędne do przeprowadzenia natychmiastowej[25] i/lub operacyjnej[26] likwidacji skażeń w zależności od szczebla organizacyjnego, potrzeb i możliwości.

Wymagania zdolnościowe dla podsystemu

Pojęcie zdolności operacyjnej w SZ RP zostało wprowadzone decyzją nr 95/MON Ministra Obrony Narodowej z 27 lutego 2007 r. w sprawie wytycznych do Przeglądu Potrzeb Operacyjnych[27]. W 2014 r. decyzja została znowelizowana i wówczas zaczęła uwzględniać model DOTMLPFI. Zdolności te opisano w Katalogu zdolności Sił Zbrojnych RP[28], w obszarze P – przetrwanie i ochrona wojsk, w którym podsystem likwidacji skażeń stanowi kluczowy element systemu OPBMR. Autor zidentyfikował cztery główne zdolności likwidacji skażeń ludzi (stanów osobowych), sprzętu, obiektów i terenu (rysunek 3).

Zdolność likwidacji skażeń ludzi obejmuje zabiegi dla żołnierzy i cywilów, przy czym procedury na czas wojny i pokoju, w tym wsparcie podczas ewentualnych skażeń powstałych podczas imprez masowych (inspiracją był proces zabezpieczania EURO 2012), są zunifikowane[29].

---

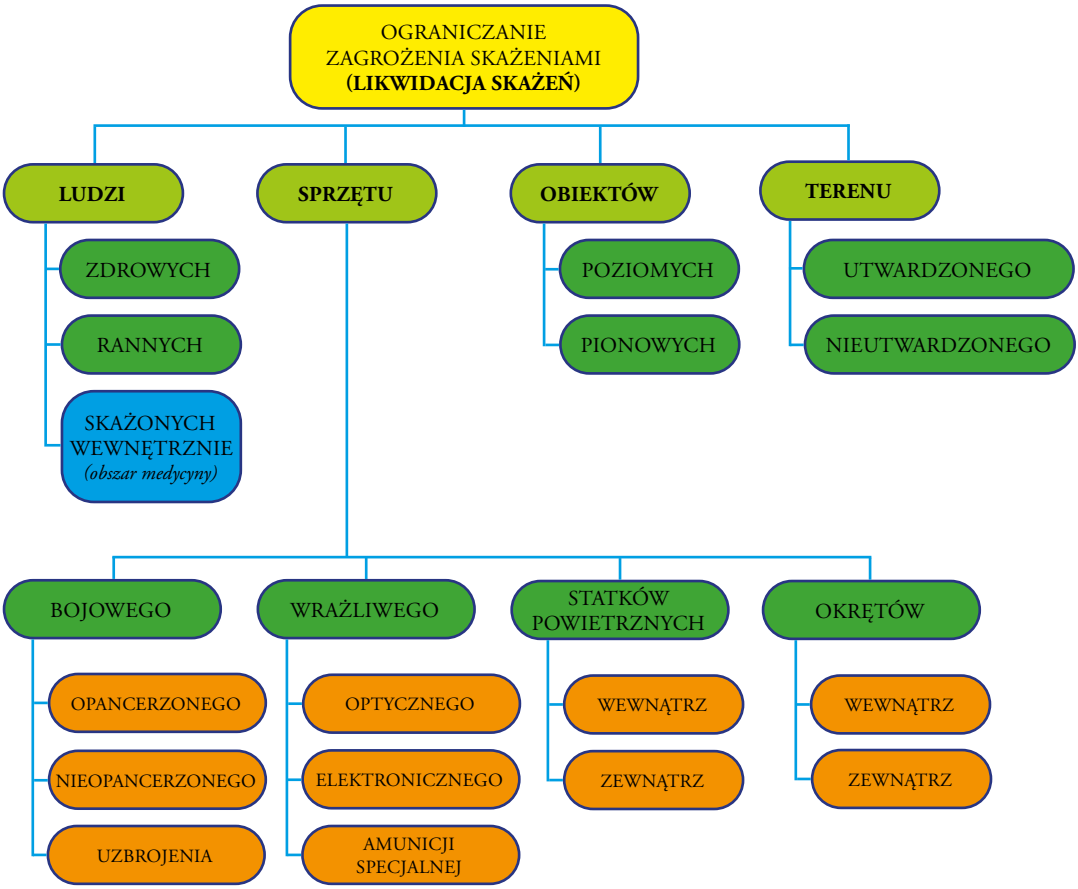
[25] Każdy żołnierz podejmuje natychmiastową likwidację skażeń niezwłocznie po wykryciu skażenia. Zabiegom, do których wykorzystuje swój indywidualny pakiet ochronny, czyli głównie: indywidualny pakiet przeciwchemiczny IPP-95 oraz indywidualny pakiet do likwidacji skażeń IPLS-1, są poddawane: odkryte części powierzchni ciała, umundurowanie, części uzbrojenia i oporządzenia istotne dla dalszego użytkowania.

[26] Te zabiegi są wykonywane przede wszystkim przez zespoły likwidacji skażeń zespołów OPBMR szczebla kompanii (pododdziału równorzędnego) oraz etatowe obsługi sprzętu bojowego typu czołgi, wozy bojowe czy samochody. Do prowadzenia zabiegów są wykorzystywane pododdziałowe zestawy do likwidacji skażeń PZLS-1 oraz przyrządy wchodzące w skład wyposażenia sprzętu bojowego, np.: eżektorowy zestaw samochodowy DK-4, zestawy do odkażania ZOd-2, ZO-E, ZO-1 lub ZO-2.

[27] *Decyzja nr 95/MON Ministra Obrony Narodowej z dnia 27 lutego 2007 r. w sprawie wprowadzenia do użytku „Wytycznych do przeprowadzenia Przeglądu Potrzeb Operacyjnych"*.

[28] Dokument niejawny. Katalog jest jednym z narzędzi do planowania rozwoju SZ RP.

[29] Planowanie, organizacja oraz sposób prowadzenia likwidacji skażeń w SZ RP, w tym likwidacji skażeń ludzi, zasadniczo są określane przez następujące dokumenty: *Regulamin działań wojsk chemicznych wojsk lądowych*, DWLąd. Wewn. 183/2011 oraz *Zabiegi sanitarne oraz zabiegi specjalne uzbrojenia i sprzętu bojowego*, Instrukcja Chem. 278/79.



Rysunek 3. Zdolności podsystemu likwidacji skażeń systemu OPBMR.

Źródło: opracowanie własne na podstawie Katalogu zdolności Sił Zbrojnych RP.

Systemy likwidacji skażeń ludzi mogą być polowe (w namiotach, kontenerach, pojazdach) lub stacjonarne, przy zachowaniu takich wymagań jak: określona przepustowość (liczba osób na godzinę w zależności od ich stanu), ciągi komunikacyjne eliminujące kontakt skażonych z czystymi, rozdzielenie stref czystych i brudnych, zabezpieczenie wody i środków odkażających, podgrzewanie wody, zbieranie skażonych odpadów powstałych po zabiegach, kontrola skażeń, stanowiska medyczne oraz odrębne ciągi dla kobiet i mężczyzn.

Zdolność leczenia osób porażonych wewnętrznie środkami chemicznymi lub promieniotwórczymi wykracza poza kompetencje wojsk

chemicznych i została przypisana ochronie zdrowia. Tacy pacjenci wymagają jednak wstępnej likwidacji skażeń, zanim trafią do szpitala.

W ramach podsystemu likwidacji skażeń sprzęt poddawany temu procesowi jest podzielony na następujące grupy: bojowy, wrażliwy, okręty (zabiegi zewnętrzne i wewnętrzne, w morzu lub porcie) oraz statki powietrzne (zabiegi zewnętrzne i wewnętrzne). Stosowane metody różnią się w zależności od budowy i przeznaczenia sprzętu, z uwzględnieniem jego różnych powierzchni.

Zdolność likwidacji skażeń obiektów obejmuje budynki o wysokości do 15 m, infrastrukturę stacjonarną (urzędy, szkoły) po powodziach lub pandemii, a także utwardzone nawierzchnie, drogi i place.

Zgodnie z wymaganiami NATO zdolność likwidacji skażeń terenu wymaga samodzielności pododdziałów przez trzy dni i utrzymywania możliwości transportu 90 m^3 wody oraz jej oczyszczania w ilości 240 m^3/dobę[30].

Uwarunkowania funkcjonowania podsystemu likwidacji skażeń SZ RP

Funkcjonowanie podsystemu likwidacji skażeń SZ RP jest determinowane przez uwarunkowania operacyjne, doktrynalne, technologiczne, finansowe i organizacyjne oraz szkoleniowe.

Uwarunkowania operacyjne

Uwarunkowania operacyjne podsystemu likwidacji skażeń w SZ RP determinują jego organizację i funkcjonowanie, z uwzględnieniem przewidywanych zagrożeń, rodzaju misji oraz układu sił w operacjach narodowych i sojuszniczych. Jednocześnie współczesne środowisko pola walki stało się niezwykle skomplikowanym i wymagającym obszarem działań ze względu na integrację użytkowanych systemów w cyberprzestrzeni czy robotykę wykorzystującą sztuczną inteligencję. W sprzęcie jest coraz więcej elektroniki, co wymusza poszukiwanie coraz bardziej zaawansowanych technologii likwidacji skażeń (np. wykorzystanie próżni, waporyzowanego nadtlenku wodoru, nanosorbentów, enzymów czy zimnej plazmy) i zastępowanie nimi uniwersalnego sprzętu. Siły Zbrojne RP muszą umiejętnie reagować na różne scenariusze zagrożeń pochodzących od środków CBRN, zarówno

[30] *BI-SC Capability Codes and Capability Statements*, 26 I 2016 r., https://www.scribd.com/document/382349178/Capability-Codes-and-Capability-Statements-2016-Bi-sc-Nu0083, s. 304 [dostęp: 2 VIII 2025].

w kraju (podczas konfliktu zbrojnego lub incydentu terrorystycznego), jak i poza naszym terytorium. Analiza zagrożeń przetwarzana na scenariusze wpływa na planowanie adekwatnych do sytuacji środków zaradczych, a to często wiąże się z pozyskiwaniem nowszego sprzętu i technologii. Te oczywiście są badane i sprawdzane podczas testów, jednak rzeczywistość weryfikuje prawidłowość wdrażanych rozwiązań i obnaża ewentualne braki i błędy. Incydent w Salisbury w 2018 r., w którym użyto środka chemicznego nowiczok, pokazał niedoskonałości w zdolnościach służb cywilnych i wojska, takie jak trudności w odkażaniu środowiska cywilnego, oraz konieczność ich współdziałania. Przywrócenie skażonego terenu do publicznego użytkowania trwało niemal rok, gdyż przeprowadzone tam zabiegi były na najwyższym, tj. IV poziomie oczyszczającym (ang. *clearance decontamination*)[31]. W SZ RP, do czasu zakończenia badań prowadzonych w ramach dysertacji, nie funkcjonowały procedury takiego działania. Co więcej, używane przez polskie wojsko odkażalniki nie były sprawdzone w zakresie ich skuteczności wobec środków typu nowiczok.

Ponadto, o ile interoperacyjność SZ RP z wojskami Sojuszu jest osiągana na różnych poziomach integracyjnych[32], a także na poziomach sprzętowym, organizacyjnym, doktrynalnym, proceduralnym oraz szkoleniowym[33], o tyle w obszarze likwidacji skażeń trudno mówić o wspólnych standardach postępowania SZ RP ze służbami cywilnymi. Interoperacyjność jest jednym z wyzwań w ramach budowania gotowości podsystemu likwidacji skażeń do realizacji specjalistycznych zadań.

[31] Poziom IV zabiegów oznacza likwidację skażeń do osiągnięcia całkowitego bezpieczeństwa przed skażeniami CBRN. Zob. *Obrona przed bronią masowego rażenia w operacjach połączonych* DD/3.8(A)...

[32] Interoperacyjność w definicji NATO to zdolność do spójnego, skutecznego i efektywnego działania w celu osiągnięcia celów Sojuszu. Jej poziom zależy od stopnia, w jakim różne systemy i siły mogą współpracować. Można wyróżnić trzy poziomy interoperacyjności: wspólność (ang. *commonality*) – gdy wszystkie siły zaangażowane do wspólnego działania używają tych samych doktryn, procedur i wyposażenia; wymienność (ang. *interchangeability*) – możliwość wykorzystania określonego produktu, procesu czy usługi w zamian za inny, by spełnić te same wymagania; zgodność (ang. *compatibility*) – przydatność produktów, procesów lub usług do wykorzystania w określonych warunkach, by spełnić wymagania bez powodowania niedopuszczalnych interakcji między nimi.

[33] Wymagania w tym zakresie zostały określone w dokumentach standaryzacyjnych (STANAG-ach), planistycznych (np. *BI-SC Capability Codes and Capability Statements*...), szkoleniowych, doktrynach czy regulaminach.

Uwarunkowania doktrynalne

Uwarunkowania doktrynalne podsystemu likwidacji skażeń w SZ RP kształtuje hierarchiczny system dokumentów standaryzacji operacyjnej, obejmujący:

- doktryny (jako dokumenty poziomu 1),
- dokumenty doktrynalne (poziom 2),
- dokumenty uzupełniające (poziom 3).

Kwestie OPBMR, a tym samym podsystemu likwidacji skażeń, są poruszane w kilkudziesięciu publikacjach. Najważniejszą z nich jest cyklicznie aktualizowany dokument doktrynalny *Obrona przed bronią masowego rażenia w operacjach połączonych* DD/3.8[34], który w aktualnej wersji (B) wprowadza trójfilarowe podejście do OPBMR, obejmujące zapobieganie (ang. *prevent*), ochronę (ang. *protect*) i odtwarzanie (ang. *recover*). Dokument ten normuje kwestie planowania, wykonania i wsparcia operacji w warunkach zagrożenia lub użycia BMR. Zmiany wprowadzone w wersji (B) są odzwierciedleniem m.in. aktywnego modelu zwalczania zagrożeń, inspirowanego amerykańskimi rozwiązaniami[35].

Istotne z punktu widzenia tworzenia podsystemu likwidacji skażeń są również takie dokumenty, jak: dokument doktrynalny *Ochrona wojsk* DD/3.14[36], który precyzuje zasady ochrony personelu, sprzętu, infrastruktury i zdolności operacyjnych w operacjach połączonych i wielonarodowych, traktując OPBMR jako element składowy ochrony; *Instrukcja zgrywania systemów walki* DD/7.1.2[37], określająca zasady zgrywania podsystemu likwidacji skażeń podczas treningów i ćwiczeń, oraz *Regulamin działań wojsk chemicznych wojsk lądowych*[38], który normuje planowanie i realizację zadań, w tym wsparcie w różnych formach działań bojowych.

---

[34] *Obrona przed bronią masowego rażenia w operacjach połączonych* DD/3.8(A)... to odpowiednik dokumentu NATO Standard AJP-3.8 *Allied joint doctrine for chemical, biological, radiological, and nuclear defence*, Edition A Version 1, 2012, https://assets.publishing.service.gov.uk/media/5bf40787ed915d18301589b4/archive_doctrine_nato_cbrn_defence_ajp_3_8.pdf [dostęp: 2 VIII 2025]. Podczas prowadzenia badań obowiązywała wersja DD/3.8 (A), a od roku 2018 – wersja DD/3.8 (B).

[35] M.F. Kelly, *United States Army Chemical, Biological, Radiological and Nuclear Corps Capability for Combating the Contemporary Weapons of Mass Destruction Threat*, Master's Thesis, Fort Leavenworth, Kansas 2012, https://apps.dtic.mil/sti/tr/pdf/ADA563129.pdf, s. 67–69 [dostęp: 2 VIII 2025].

[36] DD-3.14 (A) *Ochrona wojsk*, Szkol. 915/2015.

[37] Dokument niejawny.

[38] *Regulamin działań wojsk chemicznych wojsk lądowych*...

W NATO aspekty medyczne w zakresie OPBMR są regulowane przez publikacje CBRN Medical Publications: AJMedP-7 (wsparcie medyczne w operacjach CBRN)[39], AMedP-7.1[40] (zarządzanie ofiarami CBRN) oraz AMedP-7.3[41] (szkolenie medyczne w CBRN), w których akcent został położony na likwidację skażeń rannych.

Procedury likwidacji skażeń w SZ RP zasadniczo są zgodne z normami NATO, z wyjątkiem *clearance decontamination*.

Uwarunkowania technologiczne

Uwarunkowania technologiczne podsystemu mają swoje implikacje wynikające z członkostwa Polski w NATO, takie jak sojusznicze standardy, wypełnienie wymagań celów sił zbrojnych oraz osiągnięcie pełnej interoperacyjności w działaniach taktycznych, operacyjnych, procedurach i technologii. Tymczasem sprzęt projektowany w latach 70. i 80. XX w. i eksploatowany w SZ RP nie jest w stanie sprostać niektórym wymaganiom i ogranicza zdolności podsystemu w zakresie neutralizacji skażeń pochodzących od środków CBRN. Brak nowoczesnych technologii w tym obszarze jest rekompensowany przez zdolności Sojuszu w operacjach sojuszniczych. Należy się jednak zastanowić, jakie będą konsekwencje tych braków w przypadku operacji narodowych lub działań w ramach reagowania kryzysowego.

Rozwój nowoczesnych technologii, w tym systemów optoelektronicznych i wyposażenia naszpikowanego elektroniką, wymaga innowacyjnych metod dekontaminacji wykluczających tradycyjne metody mokre, które mogą doprowadzić do uszkodzenia odkażanego sprzętu i utraty jego zdolności bojowych. Współczesne rozwiązania w obszarze likwidacji skażeń zastępują starsze technologie, aby umożliwić poddawanie zabiegom nowoczesnego sprzętu[42]. Trendy technologiczne wpływają zatem na potrzeby

[39] NATO Standard AJMedP-7 *Allied Joint Chemical, Biological, Radiological and Nuclear (CBRN) Medical Support Doctrine*, Edition B Version 1, 2022, https://www.coemed.org/files/stanags/02_AJMEDP/AJMedP-7_EDB_V1_E_2596.pdf [dostęp: 28 VII 2025].

[40] NATO Standard AMedP-7.1 *Medical Management of CBRN Casualities*, Edition A Version 1, 2018, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.1_EDA_V1_E_2461.pdf [dostęp: 28 VII 2025].

[41] NATO Standard AJMedP-7.3 *Training of Medical Personnel for Chemical, Biological, Radiological, and Nuclear (CBRN) Defence*, Edition A Version 1, 2016, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.3_EDA_V1_E_2954.pdf [dostęp: 28 VII 2025].

[42] NATO, Science and Technology Organization, *TR-HFM-233, Sensitive Equipment Decontamination*, 2017, https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-233/$$TR-HFM-233-ALL.pdf [dostęp: 2 VIII 2025].

zmian organizacyjnych, taktyki oraz procedur działania, wymuszając restrukturyzację pododdziałów specjalistycznych oraz pozyskiwanie nowych zdolności.

Uwarunkowania finansowe i organizacyjne

Globalna tendencja wzrostu wydatków na obronność wynika głównie z wdrażania nowoczesnych technologii. Dotyczy to również Polski. Tymczasem środki przeznaczone na rozwój podsystemu likwidacji skażeń SZ RP są daleko niewystarczające i dotyczą głównie utrzymywania zapasów środków do likwidacji skażeń. Wydatki na rozwój technologiczny pozostają bliskie zera[43]. W obszarze pozyskiwania nowych technologii OPBMR skala tych wydatków niewiele się zmieni do 2026 r.[44]

W raporcie Ministerstwa Obrony Narodowej z lat 2010–2011 podkreślono potrzebę wzmocnienia zdolności likwidacji skażeń jako elementu przetrwania i ochrony wojsk. Przewidziano poprawę wyposażenia do 2018 r.[45]

Analiza uwarunkowań organizacyjnych podsystemu wykazała, że o ile przez lata transformacji w SZ RP bywały okresy rozkwitu, o tyle wojska chemiczne w większości przypadków podlegały redukcjom.

---

[43] Plany modernizacji technicznej SZ RP (PMT) są dokumentami niejawnymi, ale ich realizacja podlega kontroli. Jedną z nich była kontrola przeprowadzona przez NIK w 2017 r. w zakresie wykonania budżetu państwa w 2016 r. w części obrona narodowa. Zob. Najwyższa Izba Kontroli Departament Obrony Narodowej, *Informacja o wynikach kontroli wykonania budżetu państwa w 2016 r. w części 29 – Obrona narodowa oraz wykonania planów finansowych Funduszu Modernizacji Sił Zbrojnych i Agencji Mienia Wojskowego*, https://www.nik.gov.pl/plik/id,14141.pdf [dostęp: 20 VII 2025]. Dane z tego raportu wskazują poziom finansowania całego obszaru Przetrwanie i ochrona wojsk na poziomie 0,07% budżetu przeznaczonego na modernizację techniczną (poz. 11.1.5. Zdolność do przetrwania i ochrony, s. 33). Wspomniany obszar uwzględnia zakupy sprzętu dla całego systemu OPBMR, którego częścią jest podsystem likwidacji skażeń. Dane za rok 2016 w tym zakresie nie różnią się zasadniczo od danych z lat poprzedzających i następujących po przywołanym raporcie.

[44] Priorytety modernizacji przyjęte przez resort obrony narodowej są ogólnie dostępne. Zob. Ministerstwo Obrony Narodowej, *Plan Modernizacji Technicznej do 2026 r. Wybrane zagadnienia*, https://www.wojsko-polskie.pl/u/e1/aa/e1aa4b89-1045-4d1c-8a5c-7ffd4026e8d5/plan_modernizacji_technicznej_do_2026_r.pdf [dostęp: 28 VII 2025]. Opis dotyczy okresu prowadzonych badań. Od tamtej pory nakłady na modernizację techniczną znacznie wzrosły, jednak nie przełożyło się to na rozwój technologiczny analizowanego podsystemu.

[45] Ministerstwo Obrony Narodowej, *Strategiczny Przegląd Obronny. Profesjonalne Siły Zbrojne RP w nowoczesnym państwie. Raport*, Warszawa 2011, https://gdziewojsko.wordpress.com/wp-content/uploads/2011/05/raport_spo_14042011.pdf, s. 15 [dostęp: 2 VIII 2025].

Analogii można się doszukiwać w procesach planistycznych. O ile w Strategii Obronności RP z 2009 r., opracowanej na podstawie Strategii Bezpieczeństwa Narodowego RP z 2007 r., OPBMR był wskazywany jako jeden z głównych systemów funkcjonalnych[46], o tyle w 2011 r. w Strategicznym Przeglądzie Obronnym[47] OPBMR zaklasyfikowano jako element przetrwania i ochrony wojsk. Na podstawie Koncepcji Organizatorów Systemów Funkcjonalnych z 2012 r. i decyzji nr 56/MON z 2013 r.[48] odpowiedzialność za system OPBMR została rozdzielona między różne podmioty organizacyjne SZ RP, bez jednoczesnego wskazania mechanizmów przygotowania kadr na potrzeby systemu[49]. Wprowadziło to chaos organizacyjny, który utrudnił tym samym rozwój systemu, technologii i zintegrowanego szkolenia.

Dodatkowo w ostatniej dekadzie wzmocnił się trend tworzenia struktur ekspedycyjnych i wielofunkcyjnych, np. grupy zadaniowe, kompanie chemiczne. W przypadku tych drugich nie zwiększyło to posiadanych dotychczas zdolności specjalistycznych, a raczej negatywnie wpłynęło na możliwości bojowe pododdziałów.

Porównanie podsystemu likwidacji skażeń SZ RP z rozwiązaniami funkcjonującymi w NATO

Porównanie zdolności podsystemu likwidacji skażeń SZ RP z analogicznymi podsystemami sił zbrojnych wybranych państw NATO ujawnia różnice w podejściu technologicznym, organizacyjnym, doktrynalnym oraz zdolnościach do współdziałania ze służbami cywilnymi w ramach reagowania kryzysowego.

[46] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007*, https://www.bbn.gov.pl/ftp/dokumenty/SBN_RP.pdf [dostęp: 2 VIII 2025]; Ministerstwo Obrony Narodowej, *Strategia Obronności Rzeczypospolitej Polskiej. Strategia sektorowa do Strategii Bezpieczeństwa Narodowego*, https://mkuliczkowski.pl/static/pdf/strategia_obronnosci.pdf, pkt. 94, s. 19 [dostęp: 2 VIII 2025].

[47] Ministerstwo Obrony Narodowej, *Strategiczny Przegląd Obronny*..., s. 93.

[48] Sztab Generalny Wojska Polskiego, Koncepcja ustanowienia Organizatorów Systemów Funkcjonalnych zatwierdzona przez Ministra Obrony Narodowej 19 października 2012 r. (niepublikowana); *Decyzja nr 56/Org./P5 Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie Organizatorów Systemów Funkcjonalnych Sił Zbrojnych Rzeczypospolitej Polskiej* (niepublikowana).

[49] Sztab Generalny Wojska Polskiego, Koncepcja ustanowienia Organizatorów..., s. 22–23.

Niemcy

Główny wysiłek armii

Wysiłek Bundeswehry skupia się na zapewnieniu kompleksowej obrony przed zagrożeniami CBRN w ramach operacji sojuszniczych (NATO, Unia Europejska) i narodowych, z naciskiem na reagowanie kryzysowe, ochronę ludności i wsparcie w misjach stabilizacyjnych.

ABC-Abwehrkommando der Bundeswehr, czyli dowództwo, które odpowiada za system OPBMR w niemieckiej armii, koncentruje się na szybkiej detekcji, dekontaminacji i neutralizacji zagrożeń, w tym w asymetrycznych, jak terroryzm lub incydenty przemysłowe. Odzwierciedla to rezyliencję i interoperacyjność, które zostały podkreślone w niemieckiej strategii obrony narodowej. Armia wspiera władze na poziomie gmin, powiatów, miast, krajów związkowych i federacji[50] w sytuacjach zagrożenia CBRN, integrując wojskowe zdolności ze strukturami cywilnymi.

Podobieństwa niemieckiego i polskiego systemu likwidacji skażeń

Podobieństwa wynikają z przynależności do NATO, która wymusza zgodność ze standardami określonymi w doktrynie CBRN, czyli podejście trójfilarowe i skupienie uwagi na ochronie personelu i sprzętu. W obu krajach podsystem likwidacji skażeń jest częścią OPBMR, z naciskiem na zdolności do zabezpieczenia wojsk w operacjach połączonych. W obu armiach są rozwijane punkty likwidacji skażeń. Chociaż istnieją różnice w taktyce ich rozwijania, to podkreśla się rolę szkolenia wojsk w zakresie prowadzonych zabiegów, szczególnie na poziomie I i II, czyli natychmiastowej i operacyjnej likwidacji skażeń.

Różnice między niemieckim i polskim systemem likwidacji skażeń

- Organizacyjne i funkcjonalne – ABC-Abwehrkommando der Bundeswehr posiada scentralizowane dowodzenie w obszarze OPBMR, co umożliwia efektywne zarządzanie podległymi siłami oraz rozwijanie systemu[51]. Niemcy dzielą zdolności OPBMR na siedem

[50] Zob. H. Wyligała, *Uwarunkowania systemu zarządzania kryzysowego w Republice Federalnej Niemiec*, „Rocznik Bezpieczeństwa Międzynarodowego" 2011, t. 5, s. 133–154. https://doi.org/10.34862/rbm.2011.9.

[51] ABC-Abwehrkommando der Bundeswehr, https://www.bundeswehr.de/de/organisation/unterstuetzungsbereich/abc-abwehr-bundeswehr/abc-abwehrkommando-der-bundeswehr-in-bruchsal [dostęp: 2 VIII 2025].

podobszarów[52], w ramach których są realizowane poszczególne zadania na trzech poziomach zaawansowania: I – podstawowym, II – rozszerzonym, III – kwalifikowanym lub specjalistycznym.
- Technologiczne – Niemcy stosują zaawansowane systemy likwidacji skażeń, a niektóre z tych rozwiązań integrują robotykę i automatyzację systemów.
- Doktrynalne – w niemieckiej doktrynie HDv 330/100[53] obszar OPBMR zintegrowano z cywilną ochroną, uwzględniono przy tym aktywne podejście do likwidacji skażeń (trzy fazy: wstępna, operacyjna, dogłębna), oraz zaimplementowano wytyczne NATO (AJMedP-7) w zakresie zabiegów skażonych i zakażonych rannych.

Zdolność do współdziałania ze służbami cywilnymi

Współdziałanie Bundeswehry ze służbami cywilnymi opiera się na zapisach ustawy zasadniczej (niem. *Grundgesetz für die Bundesrepublik Deutschland*, GG)[54], umożliwiających użycie wojska w sytuacjach kryzysowych, np. podczas katastrof, aktów terroru, incydentów CBRN, klęsk żywiołowych, na wniosek władz federalnych lub władz danego kraju związkowego. Wojska mogą realizować zadania: likwidacji skażeń (ludzi, pojazdów i infrastruktury), dostawy wody i/lub środków dezynfekcyjnych, wsparcia w obszarze medycznym i logistycznym. W Bundeswehrze interoperacyjność jest na wysokim poziomie dokumentacyjnym, proceduralnym (wspólne ćwiczenia) i sprzętowym (kompatybilny sprzęt firmy Kärcher używany przez wojsko i służby cywilne).

Stany Zjednoczone

Główny wysiłek armii

Wysiłek armii USA w zakresie zwalczania BMR koncentruje się na działaniach globalnych, misjach ekspedycyjnych, kontrterroryzmie oraz

[52] Są to: 1) ochrona indywidualna, 2) ochrona zbiorowa, 3) medyczna obrona przed BMR, 4) rozpoznanie skażeń, 5) likwidacja skażeń (aktywna), 6) doradztwo specjalistyczne w zakresie OPBMR, 7) kompatybilność technologii OPBMR.

[53] Jest to odpowiednik polskiej doktryny/regulaminu w obszarze dowodzenia wojskami chemicznymi. Zob. *HDv 330/100 (zE) VS-NfD Führung der ABC-Abwehrtruppe*, 1999 r., https://www.scribd.com/document/58550605/HDv-330-100-Fuhrung-ABC-Abwehrtruppe [dostęp: 3 VIII 2025].

[54] Zob. art. 35 ust. 2 i 3 *Ustawy Zasadniczej Republiki Federalnej Niemiec z dnia 23 maja 1949 r.* (*Grundgesetz für die Bundesrepublik Deutschland*), https://biblioteka.sejm.gov.pl/wp-content/uploads/2016/02/Niemcy_pol_010711.pdf [dostęp: 3 VIII 2025].

wsparciu władz i służb cywilnych w realizowanych zadaniach (Defense Support of Civil Authorities, DSCA), z naciskiem na aktywne przeciwdziałanie proliferacji BMR poza granicami kraju, zgodnie z *National Security Strategy*[55].

Amerykańskie dowództwo CBRNE (20th CBRNE Command) integruje system CBRN w operacjach połączonych, wspierając Dowództwo Sił Lądowych Stanów Zjednoczonych (U.S. Army Forces Command, FORSCOM) i Dowództwo Północne Stanów Zjednoczonych (U.S. Northern Command, USNORTHCOM)[56] w prowadzonych działaniach.

Podobieństwa amerykańskiego i polskiego systemu likwidacji skażeń

Podobieństwa obejmują podejście trójfilarowe i skupienie uwagi na ochronie personelu i sprzętu. W obu państwach w operacjach połączonych duży nacisk jest położony na likwidację skażeń. Armia USA, tak jak polska, rozwija punkty likwidacji skażeń w terenie (w ramach gruntownej likwidacji skażeń) oraz prowadzi operacyjną likwidację skażeń w czasie nie dłuższym niż sześć godzin od skażenia. Dla wojska niezwykle istotna jest natychmiastowa likwidacja skażeń, tj. odkrytych części skóry (ciała) w czasie do minuty od skażenia, a innych skażonych powierzchni (np. uzbrojenia, wyposażenia osobistego) w czasie nie dłuższym niż 15 minut[57].

Różnice między amerykańskim i polskim systemem likwidacji skażeń

- Organizacyjne i funkcjonalne – Stany Zjednoczone mają scentralizowany system dowodzenia w obszarze OPBMR. 20th CBRNE Command dowodzi siłami podzielonymi na armię czynną, rezerwę i Gwardię Narodową. Umożliwia to elastyczne tworzenie grup zadaniowych do misji ekspedycyjnych.

  W zależności od rodzaju służby poszczególne jednostki wojsk chemicznych i personel OPBMR są przygotowywane w różnym zakresie. Do zadań pododdziałów armii czynnej należy wsparcie

[55] *Nowa Strategia Bezpieczeństwa Narodowego na nową erę*, Ambasada i Konsulat USA w Polsce, https://pl.usembassy.gov/pl/nss_pl/ [dostęp: 11 XII 2019].

[56] USNORTHCOM to główny organ wojskowy odpowiedzialny za obronę kontynentalnego terytorium Stanów Zjednoczonych, Alaski, Kanady, Meksyku, Kuby, Bahamów i okolicznych wód. Dowództwo zapewnia również wsparcie władzom cywilnym na terytorium USA. Zob. U.S. Northern Command, https://www.northcom.mil/ [dostęp: 2 VIII 2025].

[57] Zob. FM 3-11 *Chemical, Biological, Radiological, and Nuclear Operations*, May 2019, https://irp.fas.org/doddir/army/fm3_11.pdf, s. Chapter 3 3-24 [dostęp: 2 VIII 2025]; FM 3-5, MCWP 3-37.3 *NBC Decontamination*, 2000, https://www.globalsecurity.org/wmd/library/policy/army/fm/3-5/fm3-5.pdf, s. Introduction 1-3 [dostęp: 2 VIII 2025].

wojska w zakresie pasywnej OPBMR w przydzielonych rejonach odpowiedzialności (w rejonach prowadzonych operacji) oraz działania aktywne w ramach operacji przeciwdziałania rozprzestrzenianiu się broni masowego rażenia (ang. *counterproliferation*, CP[58]) i jej zwalczania (ang. *World Mass Destruction-elimination*, WMD-E)[59]. W Armii Rezerwowej siły CBRNE są przygotowywane do realizacji przede wszystkim zadań pasywnej OPBMR, choć mogą wspierać również operacje przeciwdziałania rozprzestrzenianiu się BMR czy doradzać służbom cywilnym w przypadku zdarzenia z użyciem BMR[60]. Z kolei siły wchodzące w skład Gwardii Narodowej są szkolone – tak jak całe siły zbrojne – do realizacji przedsięwzięć pasywnej OPBMR, jednak w związku z tym, że ich głównym przeznaczeniem jest służba w kraju, jest to przede wszystkim szeroko rozumiane reagowanie kryzysowe. Wspierają władze cywilne na terytorium kraju podczas zdarzeń, takich jak:

- użycie lub groźba użycia BMR,
- atak terrorystyczny lub groźba ataku terrorystycznego,
- celowe lub niezamierzone uwolnienie środków CBRN (w tym toksycznych środków przemysłowych),
- klęski żywiołowe lub katastrofy spowodowane przez człowieka, które skutkują lub mogą skutkować katastrofą, utratą życia lub mienia.

W USA bardzo dobrze przygotowany pod względem planistycznym i organizacyjnym jest IV poziom likwidacji skażeń – *clearance decontamination*.

- Technologiczne – służby w USA stosują zarówno starsze, sprawdzone technologie, jak i te nowoczesne, w tym m.in. zdolne do likwidacji skażeń sprzętu wrażliwego. Wykorzystują do tego nanosorbenty, odkażalniki enzymatyczne czy nowoczesne modułowe systemy do

[58] Joint Publication 3-40, *Joint Countering Weapons of Mass Destruction*, 2019, https://irp.fas.org/doddir/dod/jp3_40.pdf, s. GL-5 [dostęp: 2 VIII 2025].

[59] M.F. Kelly, *United States Army Chemical, Biological...*

[60] Zajmuje się tym np. 773. Civil Support Team dyslokowany w Keiserlautern w Niemczech. Zob. *Army Reserve Component CBRN Units*, https://home.army.mil/wood/application/files/7315/9352/6705/UnitLocations.pdf [dostęp: 2 VII 2025]; D. Friedberg, *U.S. Army North certyfies the only Civil Support Team in Europe*, U.S. Army, 16 IX 2017 r., https://www.army.mil/article/193991/u_s_army_north_certifies_the_only_civil_support_team_in_europe [dostęp: 2 VII 2025].

likwidacji skażeń, w tym technologię rozwijaną przez firmę Kärcher, np. Kärcher Multipurpose Power Driven System (MPDS).

Zdolności do współdziałania ze służbami cywilnymi

Współdziałanie wojsk z właściwymi służbami w przypadku incydentów CBRN, terrorystycznych, uwolnienia toksycznych środków przemysłowych (TSP) i klęsk żywiołowych dotyczy likwidacji skażeń, wsparcia medycznego, ewakuacji i zabezpieczenia logistycznego (np. dostawy indywidualnych środków ochrony przed skażeniami). W USA armia wykazuje dużą interoperacyjność ze służbami cywilnymi, zarówno dokumentacyjną, proceduralną, jak i sprzętową.

Wnioski z porównania

W porównaniu z Niemcami i Stanami Zjednoczonymi SZ RP pozostają w tyle pod względem technologii, organizacji i interoperacyjności. Polska nie ma zintegrowanych struktur na poziomie dowództwa CBRNE, a sprzęt typu IRS-2, jaki ma na wyposażeniu, nie spełnia wymagań nowoczesnych operacji. Brak regularnych ćwiczeń oraz niewystarczające współdziałanie z sektorem cywilnym ograniczają zdolności podsystemu.

Tabela 1. Porównanie zdolności likwidacji skażeń Polski, Niemiec i Stanów Zjednoczonych.

Kraj	Struktura dowodzenia/ odpowiedzialność za system	Dominująca technologia	Interoperacyjność	Współpraca z sektorem cywilnym
Polska	rozproszona	IRS-2, UG, Millagro	ograniczona	słaba
Niemcy	scentralizowana (ABC-Abwehrkommando)	zestawy mobilne (Kärcher Futuretech)	wysoka	dobra
USA	scentralizowana (20th CBRNE Command)	zestawy mobilne (systemy pianowe, pojazdy bezzałogowe)	wysoka	bardzo dobra

Źródło: opracowanie własne.

Analiza SWOT podsystemu likwidacji skażeń SZ RP

Analiza SWOT pozwala na syntetyczne ujęcie mocnych i słabych stron podsystemu likwidacji skażeń SZ RP oraz szans i zagrożeń dla jego rozwoju. Stan posiadanych zdolności oraz braków ilustruje tabela 2.

Mocne strony

- dobrze wykształcona i doświadczona kadra zdolna do współdziałania w ramach rozwijania nowoczesnych technologii OPBMR, w tym w obszarze likwidacji skażeń. Polska dysponuje m.in. dobrze wyszkolonym personelem w zasadniczych jednostkach chemicznych – wojska chemiczne są dobrze postrzegane wśród partnerów NATO. W tym zakresie Polska stanowi jeden z głównych filarów systemu OPBMR NATO,
- istniejąca infrastruktura, możliwa do zaadaptowania jako stacjonarne punkty likwidacji skażeń (PLSk) w głównych garnizonach,
- członkostwo w NATO, które umożliwia dostęp do doświadczeń i standardów sojuszniczych, co z kolei pomaga w osiąganiu interoperacyjności, wspiera w rozwiązywaniu problemów w ramach systemu Lessons Learned, wymusza osiąganie nowych zdolności, wskazuje kierunki rozwoju nowych technologii.

Słabe strony

- sprzęt i technologia – przestarzały sprzęt mający znaczne braki w wymaganych zdolnościach likwidacji skażeń sprzętu wrażliwego, obiektów wysokiej infrastruktury, wnętrz statków powietrznych, zewnętrznych powierzchni dużych statków powietrznych typu C-130, wnętrz okrętów, skażonych rannych,
- niespójność organizacyjna, technologiczna oraz stosowanej taktyki działania z oficjalnie obowiązującymi podręcznikami i instrukcjami,
- brak badań potwierdzających zdolność użytkowanej technologii do likwidacji skażeń pochodzących od środków nowej generacji,
- brak pełnej zgodności z procedurami i standardami NATO, szczególnie w zakresie *clearance decontamination*,
- ograniczone środki finansowe na modernizację i rozwój technologii likwidacji skażeń,
- rozproszenie organów odpowiedzialnych za funkcjonowanie i rozwój systemu OPBMR, w tym podsystemu likwidacji skażeń – brak scentralizowanego dowodzenia, merytorycznego kreatora systemu, decydenta w zakresie wdrażanych i rozwijanych technologii.

Szanse

- możliwość skupienia wysiłku na pozyskaniu kluczowych zdolności decydujących o gotowości wojsk do podejmowania działań, na podstawie zidentyfikowanych braków i niedoborów,
- możliwość pozyskania funduszy (w tym unijnych) na rozwój i modernizację sprzętu, technologii i infrastruktury w obszarze likwidacji skażeń,
- współpraca międzynarodowa w ramach NATO, w tym udział w ćwiczeniach, misjach oraz wymiana doświadczeń w obszarze użytkowanych technologii i taktyki działania,
- rozwój współpracy z Krajowym Systemem Ratowniczo-Gaśniczym (KSRG) i służbami (formacjami) cywilnymi w obszarze likwidacji skażeń (zagrożeń) w celu zwiększenia efektywności reagowania – opracowanie rozwiązań, w tym jednolitych standardów w celu umożliwienia wspólnej realizacji zadań w operacjach militarnych (narodowych i sojuszniczych) oraz w ramach reagowania kryzysowego, pozwoli na rozwijanie i wykorzystywanie technologii podwójnego zastosowania oraz efektywniejsze gospodarowanie przydzielonymi środkami finansowymi, a jednocześnie na zwiększenie potencjału ratowniczego zarówno w czasie pokoju, jak i wojny.

Zagrożenia

- wzrost zagrożeń hybrydowych, w tym użycia środków chemicznych i biologicznych nowej generacji,
- spowolnienie tempa modernizacji w porównaniu z innymi państwami NATO w obszarze likwidacji skażeń,
- potencjalne braki kadrowe wynikające z niewystarczającego szkolenia i niewłaściwej polityki kadrowej wojsk chemicznych.

Tabela 2. Stan zdolności i braków podsystemu likwidacji skażeń SZ RP – podsumowanie.

Przetrwanie i ochrona wojsk Obrona przed BMR Likwidacja skażeń					
Klasyfikacja			**Tak**	**Tak, ale z ograniczeniami**	**Nie**
LUDZIE	**zdrowi skażeni**			– brak możliwości zbierania odpadów po przeprowadzonych zabiegach, – odkażalniki dla sprzętu i wyposażenia osobistego nie spełniają wymogów ochrony środowiska	
	ranni skażeni				X
SPRZĘT	**bojowy**	**opancerzony**		– odkażalniki nie spełniają wymogów ochrony środowiska, – brak zdolności likwidacji skażeń wnętrza sprzętu	
		nieopancerzony		– odkażalniki nie spełniają wymogów ochrony środowiska, – brak zdolności likwidacji skażeń wnętrza sprzętu	
		uzbrojenie		– odkażalniki nie spełniają wymogów ochrony środowiska, – brak zdolności likwidacji skażeń wnętrza sprzętu	
	wrażliwy	**optyczny**			X
		elektroniczny			X
		amunicja specjalna			X
	okręty	**wewnątrz**			X
		na zewnątrz		odkażalniki nie spełniają wymogów ochrony środowiska	
	statki powietrzne	**wewnątrz**			X
		na zewnątrz		– brak odpowiednich odkażalników, – brak zdolności likwidacji skażeń dużych statków powietrznych	

Przetrwanie i ochrona wojsk Obrona przed BMR Likwidacja skażeń				
Klasyfikacja		**Tak**	**Tak, ale z ograniczeniami**	**Nie**
OBIEKTY	**pionowe**			X
	poziome		odkażalniki nie spełniają wymogów ochrony środowiska	
TEREN	**utwardzony**		odkażalniki nie spełniają wymogów ochrony środowiska	
	nieutwardzony			
DOSTARCZANIE WODY			brak cystern z zespołem napełniania i systemem wstępnego oczyszczania wody	
RATOWNICTWO CHEMICZNE	**ograniczanie skażeń**	X		

Źródło: opracowanie własne.

Kierunki doskonalenia podsystemu likwidacji skażeń SZ RP

Na podstawie literatury, analizy porównawczej i przykładów autor proponuje następujące kierunki zmian.

1. **Modernizacja techniczna**
   1) niezwłoczne pozyskanie i wdrożenie do wojsk nowoczesnych technologii likwidacji skażeń, a w tym dla:
      – sprzętu wrażliwego,
      – statków powietrznych,
      – wnętrz okrętów,
      – obiektów pionowych,
      – porażonych rannych,
   2) zwiększenie zdolności do likwidacji skażeń ludzi i zasadniczego sprzętu bojowego,
   3) wprowadzenie robotyzacji w obszarze likwidacji skażeń w celu zwiększenia bezpieczeństwa personelu.
2. **Standaryzacja operacyjna**
   1) dostosowanie wszystkich procedur do standardów NATO, w tym wprowadzenie *clearance decontamination* jako standardu operacyjnego,
   2) stała aktualizacja doktryn i dokumentów doktrynalnych uwzględniających obszar OPBMR,
   3) włączenie pododdziałów wojsk chemicznych w zintegrowany system pola walki zapewniający możliwość reagowania na zdarzenia w czasie rzeczywistym.
3. **Rozwój programów szkoleniowych**
   1) wdrożenie cyklicznych, interdyscyplinarnych ćwiczeń z udziałem jednostek chemicznych, służb cywilnych i sojuszników NATO,
   2) rozwój specjalistycznych kursów w zakresie obsługi nowoczesnych systemów dekontaminacyjnych oraz reagowania na incydenty CBRN we współdziałaniu z formacjami cywilnymi.
4. **Integracja z systemem pozamilitarnym**
   1) wzmocnienie współpracy z KSRG, Policją, Strażą Graniczną i innymi służbami, w tym Agencją Bezpieczeństwa Wewnętrznego, w celu wypracowania wspólnych standardów i procedur reagowania na incydenty CBRN w środowisku cywilnym oraz zabezpieczenia wojsk NATO w potencjalnej operacji sojuszniczej na terenie kraju,
   2) utworzenie wspólnych zespołów reagowania kryzysowego, obejmujących pododdziały SZ RP (w tym wojsk chemicznych) i formacji cywilnych, zdolnych do reagowania na incydenty z użyciem środków CBRN.

5. **Centralizacja struktur organizacyjnych**
   1) stworzenie centralnego dowództwa/komórki organizacyjnej do kierowania OPBMR, wzorowanego na amerykańskim 20th CBRNE Command lub niemieckim ABC-Abwehrkommando der Bundeswehr, które posiadałoby zdolności do identyfikacji potrzeb operacyjnych dla całych SZ RP, koordynowałoby rozwój systemu OPBMR, w tym podsystemu likwidacji skażeń, oraz działania jednostek chemicznych w SZ RP,
   2) optymalizacja rozmieszczenia infrastruktury zdolnej do funkcjonowania jako stacjonarne i mobilne PLSk w celu zwiększenia elastyczności operacyjnej.
6. **Zwiększenie finansowania**
   1) zaangażowanie funduszy unijnych i narodowych w programy modernizacyjne, w tym zakup nowego sprzętu i technologii likwidacji skażeń oraz rozwój infrastruktury z obszaru OPBMR,
   2) priorytetowe traktowanie podsystemu likwidacji skażeń w budżetach obronnych w celu wyjścia z zapaści technologicznej.

Perspektywy dalszego rozwoju

Dalsze badania nad podsystemem likwidacji skażeń SZ RP powinny koncentrować się na następujących obszarach:

- rozwoju technologii do neutralizacji środków chemicznych i biologicznych nowej generacji, takich jak nowiczok czy zmodyfikowane patogeny,
- optymalizacji modeli organizacyjnych, w tym na wpływie scentralizowania dowodzenia na efektywność prowadzonych zabiegów,
- rozbudowie współpracy międzynarodowej, np. przez wspólne projekty badawcze z NATO lub UE,
- analizie wpływu zmian klimatycznych oraz lokalnych konfliktów zbrojnych na potencjalne zagrożenia CBRN, np. wpływ migracji na wzrost zagrożeń biologicznych.

Podsumowanie i wnioski

Podsystem likwidacji skażeń SZ RP odgrywa istotną rolę w przeciwdziałaniu zagrożeniom chemicznym, biologicznym i promieniotwórczym, jednak jego efektywność jest ograniczona. Czynniki, które mają na to wpływ i wymagają pilnych działań naprawczych, to: przestarzały sprzęt, brak pełnej interoperacyjności z NATO, niewystarczające szkolenie oraz ograniczone współdziałanie z sektorem cywilnym. Wskazuje to na konieczność kompleksowej zmiany, obejmującej:

- wprowadzenie nowoczesnych technologii likwidacji skażeń,
- osiągnięcie pełnej interoperacyjności z siłami NATO oraz służbami cywilnymi,
- rozwój programów szkoleniowych i współpracy międzysektorowej,
- centralizację struktur organizacyjnych i zwiększenie finansowania.

Wdrożenie tych rozwiązań powinno stworzyć warunki do zwiększenia gotowości operacyjnej SZ RP, wzmocnienia bezpieczeństwa narodowego oraz skuteczniejszego współdziałania z sojusznikami w ramach NATO.

Bibliografia

Okumara T., Takasu N., Ishimatsu S., Kumada K., Tanaka K., Hinohara S., *Report on 640 Victims of the Tokyo Subway Sarin Attack*, „Annals of Emergency Medicine" 1996, t. 26, nr 2, s. 129–135. https://doi.org/10.1016/S0196-0644(96)70052-5.

Słownik terminów i definicji NATO AAP-6(2014) – (pozycja dostępna po zalogowaniu do systemu NATO Standardization Office).

Słownik terminów i definicji NATO dotyczący zagrożeń chemicznych, biologicznych, radiologicznych i nuklearnych AAP-21(B) – (pozycja dostępna po zalogowaniu do systemu NATO Standardization Office).

Steindl D., Boehmerle W., Korner R., Preager D., Haug M., Nee J., Schreiber A., Scheibe F., Demin K., Jacoby P., Tauber R., Hartwig S., Endres M., Eckardt K-U., *Novichok nerve agent poisoning*, „The Lancet" 2021, t. 397, nr 10270, s. 249–252. https://doi.org/10.1016/S0140-6736(20)32644-1.

Wyligała H., *Uwarunkowania systemu zarządzania kryzysowego w Republice Federalnej Niemiec*, „Rocznik Bezpieczeństwa Międzynarodowego" 2011, t. 5, s. 133–154. https://doi.org/10.34862/rbm.2011.9.

Źródła internetowe

ABC-Abwehrkommando der Bundeswehr, https://www.bundeswehr.de/de/organisation/unterstuetzungsbereich/abc-abwehr-bundeswehr/abc-abwehrkommando-der-bundeswehr-in-bruchsal [dostęp: 2 VIII 2025].

Alexander Litvinienko: Profile of murdered Russian spy, BBC News, 21 I 2016 r., https://www.bbc.com/news/uk-19647226 [dostęp: 26 VII 2025].

Army Reserve Component CBRN Units, https://home.army.mil/wood/application/files/7315/9352/6705/UnitLocations.pdf [dostęp: 25 IX 2019].

BI-SC Capability Codes and Capability Statements, 26 I 2016 r., https://www.scribd.com/document/382349178/Capability-Codes-and-Capability-Statements-2016-Bi-sc-Nu0083 [dostęp: 2 VIII 2025].

FM 3-11 *Chemical, Biological, Radiological, and Nuclear Operations*, May 2019, https://irp.fas.org/doddir/army/fm3_11.pdf [dostęp: 2 VIII 2025].

FM 3-5, MCWP 3-37.3 *NBC Decontamination Operations*, 2000, https://www.globalsecurity.org/wmd/library/policy/army/fm/3-5/fm3-5.pdf [dostęp: 2 VIII 2025].

Friedberg D., *U.S. Army North certyfies the only Civil Support Team in Europe*, U.S. Army, 16 IX 2017 r., https://www.army.mil/article/193991/u_s_army_north_certifies_the_only_civil_support_team_in_europe [dostęp: 2 VII 2025].

Gardner F., *Navalny 'Novichok poisoning' a test for the West,* BBC News, 2 IX 2020 r., https://www.bbc.com/news/world-europe-54003014 [dostęp: 1 VIII 2025].

Joint Publication 3-40, Joint Countering Weapons of Mass Destruction, 2019, https://irp.fas.org/doddir/dod/jp3_40.pdf [dostęp: 2 VIII 2025].

Kelly M.F., *United States Army Chemical, Biological, Radiological and Nuclear Corps Capability for Combating the Contemporary Weapons of Mass Destruction Threat*, Master's Thesis, Fort Leavenworth, Kansas 2012, https://apps.dtic.mil/sti/tr/pdf/ADA563129.pdf [dostęp: 2 VII 2025].

Kim Jong-nam killing: 'VX nerve agent' found on his face, BBC News, 24 II 2017 r., https://www.bbc.com/news/world-asia-39073389 [dostęp: 26 VII 2025].

Ministerstwo Obrony Narodowej, *Plan Modernizacji Technicznej do 2026 r. Wybrane zagadnienia,* https://www.wojsko-polskie.pl/u/e1/aa/e1aa4b89-1045-4d1c-8a5c-7ffd4026e8d5/plan_modernizacji_technicznej_do_2026_r.pdf [dostęp: 28 VII 2025].

Ministerstwo Obrony Narodowej, *Strategiczny Przegląd Obronny. Profesjonalne Siły Zbrojne RP w nowoczesnym państwie. Raport*, Warszawa 2011, https://gdziewojsko.wordpress.com/wp-content/uploads/2011/05/raport_spo_14042011.pdf [dostęp: 2 VIII 2025].

Morris S., *UK believes Putin personally authorized Salisbury novichok attack, inquiry told*, The Guardian, 14 X 2024 r., https://www.theguardian.com/uk-news/2024/oct/14/salisbury-novichok-poisonings-inquiry-sergei-skripal-vladmir-putin [dostęp: 25 VII 2025].

Najwyższa Izba Kontroli Departament Obrony Narodowej, *Informacja o wynikach kontroli wykonania budżetu państwa w 2016 r. w części 29 – Obrona narodowa oraz wykonania planów finansowych Funduszu Modernizacji Sił Zbrojnych i Agencji Mienia Wojskowego*, https://www.nik.gov.pl/plik/id,14141.pdf [dostęp: 20 VII 2025].

NATO Standard AJMedP-7 *Allied Joint Chemical, Biological, Radiological and Nuclear (CBRN) Medical Support Doctrine*, Edition B Version 1, 2022, https://www.coemed.org/files/stanags/02_AJMEDP/AJMedP-7_EDB_V1_E_2596.pdf [dostęp: 3 VIII 2025].

NATO Standard AJMedP-7.1 *Medical Management of CBRN Casualities*, Edition A Version 1, 2018, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.1_EDA_V1_E_2461.pdf [dostęp: 3 VIII 2025].

NATO Standard AJMedP-7.3 *Training of Medical Personnel for Chemical, Biological, Radiological, and Nuclear (CBRN) Defence*, Edition A Version 1, 2016, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.3_EDA_V1_E_2954.pdf [dostęp: 3 VIII 2025].

NATO Standard AJP-3.8 *Allied joint doctrine for chemical, biological, radiological, and nuclear defence*, Edition A Version 1, 2012, https://assets.publishing.service.gov.uk/media/5bf40787ed915d18301589b4/archive_doctrine_nato_cbrn_defence_ajp_3_8.pdf [dostęp: 3 VIII 2025].

NATO, Science and Technology Organization, *TR-HFM-233, Sensitive Equipment Decontamination*, 2017, https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-233/$$TR-HFM-233-ALL.pdf [dostęp: 2 VIII 2025].

Nowa Strategia Bezpieczeństwa Narodowego na nową erę, Ambasada i Konsulat USA w Polsce, https://pl.usembassy.gov/pl/nss_pl/ [dostęp: 11 XII 2019].

OPCW Issues Report on Technical Assistance Requested by Germany, OPCW, 6 X 2020 r., https://www.opcw.org/media-centre/news/2020/10/opcw-issues-report-technical-assistance-requested-germany [dostęp: 1 VIII 2025].

OPCW issues report on third Technical Assistance Visit to Ukraine following an incident of alleged use of toxic chemicals as a weapon, OPCW, 26 I 2025 r., https://www.opcw.org/media-centre/news/2025/06/opcw-issues-report-third-technical-assistance-visit-ukraine-following [dostęp: 26 VI 2025].

Pletcher K., *Tokyo subway attack of 1995*, Britannica, 8 V 2025 r., https://www.britannica.com/event/Tokyo-subway-attack-of-1995 [dostęp: 25 VII 2025].

Rozproszenie gazu sarin w Tokio, Terroryzm!com, 26 XII 2006 r., http://www.terroryzm.com/rozproszenie-gazu-sarin-w-tokio/ [dostęp: 25 VII 2025].

Salisbury declared decontaminated after Novichok poisoning, BBC, 1 III 2019 r., https://www.bbc.com/news/uk-england-wiltshire-47412390 [dostęp: 10 III 2019].

Syria: BBC Investigation Reveals Widespread Chemical Weapons Use, BBC, https://www.bbc.co.uk/programmes/w172w25d6yyjrc0 [dostęp: 25 X 2018].

The Lab: How FSB chemical weapons experts tried to poison Alexei Navalny, The Insider, 14 XII 2020 r., https://theins.ru/en/politics/262611 [dostęp: 1 VIII 2025].

U.S. Northern Command, https://www.northcom.mil/ [dostęp: 2 VIII 2025].

Vladimir Kara-Murza Tailed by Members of FSB Squad Prior to Suspected Poisonings, Bellingcat, 11 II 2021 r., https://www.bellingcat.com/news/2021/02/11/vladimir-kara-murza-tailed-by-members-of-fsb-squad-prior-to-suspected-poisonings/ [dostęp: 1 VIII 2025].

Zabójstwo Aleksandra Litwinienki, w: Konsorcjum Mall-CBRN, *Podręcznik zapobiegania i reagowania na zdarzenia CBRNE w centrach handlowych*, https://www.uni.lodz.pl/fileadmin/Projekty/MALL-CBRN/Materials_available_for_download_/Mall-CBRN-Handbook-PL-1.0.pdf, s. 24–25 [dostęp: 2 VIII 2025].

Akty prawne

Ustawa Zasadnicza Republiki Federalnej Niemiec z dnia 23 maja 1949 r. (*Grundgesetz für die Bundesrepublik Deutschland*), https://biblioteka.sejm.gov.pl/wp-content/uploads/2016/02/Niemcy_pol_010711.pdf [dostęp: 3 VIII 2025].

Konwencja o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów, sporządzona w Paryżu dnia 13 stycznia 1993 r. (DzU z 1999 r. nr 63 poz. 703).

Rozporządzenie Rady Ministrów z dnia 25 marca 2025 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym (DzU z 2025 r. poz. 407).

Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym (DzU z 2004 r. nr 98 poz. 978).

Inne dokumenty

DD-3.14 (A) *Ochrona wojsk*, Szkol. 915/2015.

Decyzja nr 56/MON Ministra Obrony Narodowej z dnia 8 marca 2013 r. zmieniająca decyzję w sprawie wprowadzenia do użytku w resorcie obrony narodowej metodyki zaopatrywania żołnierzy zawodowych w przedmioty umundurowania i wyekwipowania, kalkulacji równoważników pieniężnych przysługujących w zamian za te przedmioty, a także monitorowania cen tych przedmiotów oraz usług (Dz. Urz. MON z 2013 r. poz. 64).

Decyzja nr 56/Org./P5 Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie Organizatorów Systemów Funkcjonalnych Sił Zbrojnych RP (niepublikowana).

Decyzja nr 95/MON Ministra Obrony Narodowej z dnia 27 lutego 2007 r. w sprawie wprowadzenia do użytku „Wytycznych do przeprowadzenia Przeglądu Potrzeb Operacyjnych" (Dz. Urz. MON z 2007 r. nr 5 poz. 67).

HDv 330/100 (zE) VS-NfD Führung der ABC-Abwehrtruppe, 1999 r., https://www.scribd.com/document/58550605/HDv-330-100-Fuhrung-ABC-Abwehrtruppe [dostęp: 3 VIII 2025].

Leosz A., Sawczak S., *Sprzęt likwidacji skażeń*, WSO–TK wewn. 57/96 (w archiwum Akademii Wojsk Lądowych, pozycja udostępniona przez MON).

Ministerstwo Obrony Narodowej, *Strategia Obronności Rzeczypospolitej Polskiej. Strategia sektorowa do Strategii Bezpieczeństwa Narodowego*, https://mkuliczkowski.pl/static/pdf/strategia_obronnosci.pdf [dostęp: 2 VIII 2025].

NO-01-A006:2010 Obrona przed bronią masowego rażenia. Terminologia (dokument w Wojskowym Centrum Normalizacji, Jakości i Kodyfikacji).

Obrona przed bronią masowego rażenia w operacjach połączonych DD/3.8(A), Szkol. 869/2013 (pozycja udostępniona przez MON).

Regulamin działań wojsk chemicznych wojsk lądowych, DWLąd. Wewn. 183/2011.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007, https://www.bbn.gov.pl/ftp/dokumenty/SBN_RP.pdf [dostęp: 2 VIII 2025].

Sztab Generalny Wojska Polskiego, Koncepcja ustanowienia Organizatorów Systemów Funkcjonalnych zatwierdzona przez Ministra Obrony Narodowej 19 października 2012 r. (pozycja udostępniona przez MON).

Zabiegi sanitarne oraz zabiegi specjalne uzbrojenia i sprzętu bojowego, Instrukcja Chem. 278/79 (pozycja udostępniona przez MON).

Zabiegi specjalne terenu i polowych obiektów obronnych, Sygn. 1984 Chem. 321, Warszawa 1985 (pozycja udostępniona przez MON).

Płk rez. dr Krzysztof Tokarczyk

Pułkownik rezerwy, doktor nauk społecznych w dyscyplinie nauki o bezpieczeństwie. Ekspert Fundacji Stratpoints. Były oficer korpusu osobowego wojsk chemicznych. Zakończył służbę w Siłach Zbrojnych RP na stanowisku służbowym szefa oddziału – zastępcy szefa Zarządu Operacyjnego Dowództwa Generalnego Rodzajów Sił Zbrojnych. Specjalizuje się w obszarze likwidacji skażeń (dekontaminacji). Autor kilku poradników dla Sił Zbrojnych, opracowanych w ramach Systemu Wykorzystania Doświadczeń, oraz współautor kilku instrukcji i podręczników o tematyce obrony przed BMR.

Kontakt: ktokarczyk1@wp.pl

VARIA

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 203–233

https://doi.org/10.4467/27204383TER.25.051.23038

Varia

Jak samorządy mogą chronić przestrzenie publiczne przed atakami z użyciem pojazdów?

Mariusz Cichomski
Ministerstwo Spraw Wewnętrznych i Administracji
https://orcid.org/0000-0003-3707-7856

Od 16 kwietnia 2022 r. nieprzerwanie na całym terytorium Polski obowiązuje drugi w czterostopniowej skali stopień alarmowy BRAVO[1]. Stopnie alarmowe są wprowadzane na podstawie *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym lub wystąpienia takiego zdarzenia. Drugi stopień alarmowy jest wprowadzany, gdy zaistnieje zwiększone i przewidywalne zagrożenie wystąpieniem zdarzenia o charakterze terrorystycznym, gdy konkretny cel ataku nie został zidentyfikowany[2].

[1] Stopień alarmowy BRAVO od 6 października 2022 r. obowiązuje również wobec polskiej infrastruktury energetycznej mieszczącej się poza granicami Rzeczypospolitej Polskiej. Od 19 listopada 2025 r. na obszarach linii kolejowych zarządzanych przez PKP PLK i PKP LHS wprowadzono trzeci stopień alarmowy (CHARLIE). Wprowadzono ponadto drugi stopień alarmowy w odniesieniu do zagrożeń w cyberprzestrzeni (BRAVO-CRP), który obowiązuje od 1 marca 2024 r. Wcześniej, tj. od 21 lutego 2022 r. do 29 lutego 2024 r., obowiązywał trzeci stopień alarmowy CHARLIE-CRP, a od 15 lutego 2022 r. do 21 lutego 2022 r. – pierwszy stopień alarmowy ALFA-CRP.

[2] Artykuł 15 ust. 4 *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*.

Wprowadzenie stopnia alarmowego BRAVO miało wymiar prewencyjny. Było spowodowane sytuacją geopolityczną w regionie związaną z różnymi działaniami typowymi dla ataku hybrydowego prowadzonymi przez Federację Rosyjską i Białoruś wobec Polski i innych państw Unii Europejskiej oraz z konsekwencjami zbrojnego ataku Rosji na Ukrainę. Jak wskazuje Ministerstwo Spraw Wewnętrznych i Administracji, (...) *stopnie alarmowe są przede wszystkim sygnałem dla służb dbających o bezpieczeństwo i całej administracji publicznej do zachowania szczególnej czujności*[3].

Z instrumentu prawnego, jakim jest wprowadzenie stopni alarmowych, korzystano już wcześniej, jednak w 2022 r. zarówno przesłanki, jak i skutki tego działania różniły się od wcześniejszych przypadków. Tym razem stopnie alarmowe nie zostały bowiem wprowadzone w związku z organizacją określonego przedsięwzięcia, takiego jak uroczystości państwowe, spotkania międzynarodowe czy wybory, lecz jako następstwo wydarzeń niezależnych od polskich władz i odpowiedź na bezpośrednie intencjonalne działania innych państw. Pierwszym elementem wspomnianego ataku o charakterze hybrydowym był kryzys migracyjny na granicy polsko-białoruskiej stanowiącej jednocześnie zewnętrzną granicę UE. Został on sztucznie wywołany przez władze Białorusi we współpracy z władzami Federacji Rosyjskiej. Z czasem działania hybrydowe zaczęły przybierać inne formy, np. testowania odporności polskiej infrastruktury krytycznej, podpaleń sklepów i magazynów, cyberataków czy ataków na infrastrukturę kolejową powodujących bezpośrednie zagrożenie dla życia i zdrowia ludzi.

Istotną różnicę w stosunku do poprzednich przypadków zarządzenia stopni alarmowych stanowi również okres ich obowiązywania. Wcześniej były one wprowadzane na krótko w związku z jakimś wydarzeniem. Tym razem obowiązują nieprzerwanie od ponad trzech lat i trudno ocenić, kiedy zostaną zniesione[4]. W efekcie właściwe służby, organy administracji publicznej i inne podmioty, na których pracę oddziałują stopnie alarmowe, są zobowiązane do zachowania, na długi okres, podwyższonej gotowości oraz wdrażania szczegółowych rozwiązań w tym zakresie. Jest to również okazja do weryfikacji prawidłowości i adekwatności obowiązujących

[3] *Stopnie alarmowe BRAVO i BRAVO-CRP na terenie całego kraju wciąż obowiązują*, Serwis Rzeczypospolitej Polskiej, 29 VIII 2025 r., https://www.gov.pl/web/mswia/stopnie-alarmowe-bravo-i-bravocrp-na-terenie-calego-kraju-wciaz-obowiazuja3 [dostęp: 11 X 2025].

[4] M. Cichomski, I. Idzikowska-Ślęzak, *Stopnie alarmowe – praktyczny i prawny wymiar ich stosowania*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 58–64. https://doi.org/10.4467/27204383TER.22.018.16338.

przepisów i procedur, a także kluczowy moment do wdrażania mechanizmów zapobiegania zagrożeniom czy minimalizacji ich skutków.

Niezależnie od przyczyn wprowadzenia stopni alarmowych w Polsce niezbędna pozostaje bieżąca analiza zamachów terrorystycznych, do których doszło w innych państwach, i wskazywanie na jej podstawie potencjalnych celów takich ataków. Ta analiza nie może się ograniczać do zagrożeń specyficznych dla działań hybrydowych, ale powinna uwzględniać szerszy kontekst, niezwiązany tylko z regionalnymi uwarunkowaniami.

W obecnych okolicznościach istotne jest podejmowanie działań zorientowanych na zapobieganie zdarzeniom o charakterze terrorystycznym bądź minimalizację skutków w przypadku ich wystąpienia. Zgodnie z art. 3 ust. 2 ustawy o działaniach antyterrorystycznych: *minister właściwy do spraw wewnętrznych odpowiada za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia*. Należy zaznaczyć, że te działania nie muszą być realizowane bezpośrednio przez ministra właściwego do spraw wewnętrznych. Istotne pozostaje ich inicjowanie lub wspieranie innych organów, które podejmą obowiązek przygotowania na zagrożenia o charakterze terrorystycznym.

Minister właściwy do spraw wewnętrznych przewodniczy Międzyresortowemu Zespołowi do Spraw Zagrożeń Terrorystycznych. Do zadań tego zespołu należy inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej w zakresie przygotowania do zapobiegania zdarzeniom o charakterze terrorystycznym, przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć oraz reagowania na nie[5]. Rola przewodniczącego jest zatem powiązana

[5] Zob. § 2 ust. 2 pkt 3 *Zarządzenia nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*. Aktualny stan prawny: *Zarządzenie nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*, zmienione zarządzeniem nr 95 Prezesa Rady Ministrów z dnia 4 września 2008 r., zarządzeniem nr 74 Prezesa Rady Ministrów z dnia 21 września 2009 r., zarządzeniem nr 18 Prezesa Rady Ministrów z dnia 3 kwietnia 2014 r., zarządzeniem nr 84 Prezesa Rady Ministrów z dnia 18 września 2015 r., zarządzeniem nr 86 Prezesa Rady Ministrów z dnia 5 lipca 2016 r., zarządzeniem nr 32 Prezesa Rady Ministrów z dnia 27 kwietnia 2017 r., zarządzeniem nr 160 Prezesa Rady Ministrów z dnia 9 listopada 2017 r., zarządzeniem nr 92 Prezesa Rady Ministrów z dnia 7 czerwca 2018 r. oraz zarządzeniem nr 37 Prezesa Rady Ministrów z dnia 8 kwietnia 2021 r. Por. M. Cichomski, I. Idzikowska-Ślęzak, *Poziom strategiczny polskiego systemu antyterrorystycznego – 15 lat Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*,

z ustawową odpowiedzialnością za fazę przygotowania na wystąpienie zdarzeń o charakterze terrorystycznym, jak również wpisuje się w całokształt odpowiedzialności za bezpieczeństwo i porządek publiczny.

Jedną z wykorzystanych już w różnych państwach, w tym państwach Unii Europejskiej, metod zamachów terrorystycznych jest atak z wykorzystaniem pojazdu taranującego. Użycie pojazdu do atakowania ludzi w miejscach publicznych jest jednym z najpoważniejszych zagrożeń w przestrzeniach miejskich, choćby z uwagi na dużą dostępność tego narzędzia. Zapobieganie zdarzeniom tego typu nie jest wyłącznie zadaniem służb. W przypadku organizacji w przestrzeni publicznej wydarzeń o charakterze otwartym i masowym odpowiedzialność za ich zabezpieczenie, szczególnie w zakresie infrastruktury, która może zostać wykorzystana do podniesienia poziomu bezpieczeństwa danego przedsięwzięcia, leży przede wszystkim po stronie władz samorządowych.

W związku z tym z inicjatywy Ministra Spraw Wewnętrznych i Administracji został przygotowany dokument pt. *Ochrona przestrzeni publicznych przed atakami z użyciem pojazdów – rekomendacje dla samorządów*. Opracowali go policyjni eksperci przy współpracy z MSWiA oraz Agencją Bezpieczeństwa Wewnętrznego i z wykorzystaniem doświadczeń innych państw. Rekomendacje mają być pomocne zarówno w planowaniu inwestycji mających na celu zapewnienie bezpieczeństwa przestrzeni publicznych, np. automatycznych zapór antyterrorystycznych lub innych stałych konstrukcji, jak i w usprawnianiu już stosowanych rozwiązań technicznych i architektonicznych. Dokument został przygotowany we wrześniu 2025 r. i przekazany do prezydentów miast wojewódzkich oraz do wojewodów w celu jego dalszej dystrybucji do władz samorządowych.

Jak wskazano w rekomendacjach, obecnie wiele rozwiązań architektonicznych i technicznych – od słupków parkingowych, przez przeszkody mające charakter elementów małej architektury, aż po atestowane systemy zapór drogowych, które mogą zminimalizować lub nawet wyeliminować zagrożenia związane z użyciem pojazdu taranującego – jest już dostępnych na rynku. Skuteczność tych środków zazwyczaj rośnie wraz z kosztami ich zakupu i utrzymania. W związku z tym decyzje podejmowane w tych sprawach muszą służyć zapewnieniu możliwie jak najwyższej ochrony

„Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 66–89. https://doi.org/10.4467/27204383TER.22.003.15419.

w ramach posiadanych zasobów, w tym również efektywnego wykorzystania służb porządkowych, a także być adekwatne do zagrożeń.

Rekomendacje zawierają m.in. charakterystykę zagrożeń z użyciem pojazdu taranującego, opis procesu planowania zabezpieczeń różnych przestrzeni publicznych, infrastrukturalnych i architektonicznych środków ochronnych, a także możliwych form integracji zabezpieczeń z miejską architekturą czy możliwości wykorzystania tymczasowych zabezpieczeń i innych istniejących elementów architektonicznych jako barier. W dokumencie opisano również rolę lokalnych służb porządkowych (straży miejskich i gminnych) oraz wymagania formalne dotyczące bezpieczeństwa dla wykonawców i pracowników realizujących czynności w zakresie systemów kontroli dostępu do barier antyterrorystycznych lub ich integracji.

Warto zaznaczyć, że rekomendacje obejmują różne typy przestrzeni publicznych, które mogą stać się celem ataku terrorystycznego z użyciem pojazdu, takie jak rynki i place miejskie, deptaki i strefy pieszych, miejsca imprez masowych oraz ogólnodostępne przestrzenie o uniwersalnym charakterze.

Dokument nie ma charakteru normatywnego, a zatem jego wykorzystanie będzie zależało od chęci i możliwości władz lokalnych. Zawarte w nim wskazówki można dostosować do miejscowych warunków[6].

Mariusz Cichomski

Prawnik, socjolog. Zawodowo zajmuje się zagadnieniami związanymi z terroryzmem, przestępczością zorganizowaną, nadzorem nad działalnością służb, legislacją w zakresie bezpieczeństwa oraz sprawami dotyczącymi stosowania krajowych środków ograniczających. Autor ponad 30 publikacji z zakresu bezpieczeństwa, zwłaszcza w wymiarze prawnym, i socjologii.

[6] Dokument publikujemy na następnych stronach jako załącznik do tekstu (przyp. red.).

Ochrona przestrzeni publicznych przed atakami z użyciem pojazdów – rekomendacje dla samorządów[1]

Wprowadzenie

Zagrożenia, jakie stanowią ataki z użyciem pojazdów, tzw. pojazdów - taranów do rozjeżdżania ludzi, stanowią obecnie jeden z powodów rosnącej liczby zdarzeń o charakterze terrorystycznym. Tego rodzaju ataki podejmowano w Europie i na świecie od wielu lat, a w ostatnim czasie widoczne jest ich nasilenie przy jednoczesnym wzroście liczby ich ofiar śmiertelnych. Przykładem może tu być zdarzenie, do którego doszło w lipcu 2016 roku w Nicei podczas obchodów święta narodowego Francji, kiedy prowadzona przez zamachowca ciężarówka staranowała bariery i wjechała w ludzi znajdujących się na promenadzie zabijając 87 osób i raniąc kolejne 434. Analogiczne ataki zostały przeprowadzone w innych dużych miastach Europy i Ameryki, w tym w Berlinie, Barcelonie, Londynie, Sztokholmie, Nowym Jorku, Toronto. Polska jest krajem bezpiecznym, ale wystąpienie zdarzenia o charakterze terrorystycznym jest możliwe również w naszym Państwie, dlatego też niezbędne jest podejmowanie działań zapobiegawczych lub minimalizujących skutki ewentualnych ataków.

Należy zauważyć, że atak pojazdem - taranem jest stosunkowo łatwo dostępnym narzędziem. Nawet zwykły pojazd osobowy może doprowadzić do licznych ofiar oraz wywołać masową panikę. Z drugiej strony ten rodzaj zagrożenia spowodował, że dostępne stały się liczne rozwiązania architektoniczne i techniczne. Są to różnego rodzaju zabezpieczenia od prostych słupków parkingowych uznawanych za zabezpieczenie porządkowe, poprzez przeszkody mające charakter elementów małej architektury potrafiące zatrzymać pojazdy, aż po atestowane systemy zapór drogowych o najwyższym poziomie zabezpieczenia. Z powodu różnorodności dostępnych rozwiązań, ich dobór nie jest rzeczą prostą. Z jednej strony zależy to od rodzaju obiektów lub ukształtowania

[1] Dokument publikujemy w wersji oryginalnej. Dokonano jedynie zmian w układzie graficznym tabeli (przyp. red.).

przestrzeni, które podlegałyby ochronie, z drugiej strony często zależy to od wielkości budżetu, który został przeznaczony na ten cel.

Podsumowując, używanie pojazdu środka do przeprowadzenia zamachu terrorystycznego, staje się zjawiskiem wpisującym w aktualny obraz zagrożeń miejskich choćby z uwagi na stosunkowo prosty mechanizm działania ich sprawców. Otwartość i dostępność przestrzeni miejskich sprawiają, że całkowite wyeliminowanie ryzyka ataku pojazdem jest niemożliwe, jednak odpowiednie planowanie infrastruktury może znacznie utrudnić jego przeprowadzenie i zminimalizować skutki. W szczególności chodzi tu o infrastrukturę, która może w takich sytuacjach zostać wykorzystana do podniesienia poziomu bezpieczeństwa danego przedsięwzięcia publicznego, jak również zostać odpowiednio wkomponowana w zasoby służb porządkowych, w tym np. straży gminnych.

Niniejsze rekomendacje zostały opracowane przez Policję, we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji oraz Agencją Bezpieczeństwa Wewnętrznego, z troską o bezpieczeństwo polskich miast i miasteczek i mają stanowić praktyczny poradnik oparty na doświadczeniach ekspertów oraz dobrych praktykach międzynarodowych (m.in. z Wielkiej Brytanii, Niemiec i Holandii). Bazują na sprawdzonych rozwiązaniach stosowanych w innych krajach oraz wiedzy specjalistycznej, nie odnosząc się do szczegółowych lokalnych analiz zagrożeń. Celem tego opracowania jest bowiem przedstawienie uniwersalnych zasad, które każda gmina – niezależnie od wielkości i posiadanego budżetu – będzie mogła dostosować do własnych warunków w celu zapobiegania lub ograniczania skutków zamachu z użyciem pojazdu.

Założeniem skierowania niniejszego dokumentu do włodarzy miast i gmin jest, że zawarte w nim treści okażą się przydatne przy podejmowaniu często trudnych decyzji odnośnie sposobów ochrony przestrzeni publicznych, zarówno w perspektywie przyszłych procesów inwestycyjnych, jak i w kontekście zagospodarowania już posiadanych zasobów.

Zakres i zastosowanie rekomendacji

Rekomendacje obejmują różne typy **przestrzeni publicznych**, które mogą stać się celem ataku z użyciem rozpędzonego pojazdu. Dotyczy to w szczególności:

- **rynków i placów miejskich** – centralnych przestrzeni gromadzenia się ludzi (np. rynek miejski, place przed ratuszem), często wykorzystywanych na jarmarki, zgromadzenia lub wydarzenia okolicznościowe,
- **deptaków i stref pieszych** – ulic wyłączonych z ruchu kołowego, gdzie codziennie przebywają piesi (ulice handlowe, promenady),
- **miejsc imprez masowych** – terenów, na których odbywają się koncerty, festyny, imprezy sportowe itp., zarówno stałych (stadiony, esplanady), jak i tymczasowo aranżowanych (np. ulice zamykane na czas biegu ulicznego),
- **ogólnodostępnych przestrzeni o uniwersalnym charakterze** – np. parków, skwerów, bulwarów, terenów rekreacyjnych i turystycznych, które z natury są otwarte, a jednocześnie mogą gromadzić duże grupy ludzi.

Dla każdej z powyższych kategorii przestrzeni wskazane zostały typowe **zagrożenia i wyzwania** oraz **adekwatne środki zaradcze**. Dokument koncentruje się na **infrastrukturalnych i architektonicznych rozwiązaniach ochronnych** – takich jak zapory fizyczne (stałe i automatyczne), słupki, barierki czy specjalnie zaprojektowane elementy małej architektury pełniące funkcje zabezpieczające. Ponadto omówiono **metody tymczasowego zabezpieczenia** przestrzeni podczas podwyższonego ryzyka (np. w trakcie imprez masowych) z użyciem przenośnych barier i innych dostępnych środków. Rekomendacje określają również **zadania lokalnych służb porządkowych** (straży miejskich/gminnych) we wspieraniu tych zabezpieczeń oraz poruszają **aspekty prawne i organizacyjne** niezbędne do skutecznej realizacji działań (podział odpowiedzialności, współpraca z podmiotami prywatnymi, zgodność z przepisami).

Uwaga: Rekomendacje należy traktować jako punkt wyjścia – powinny one być dostosowane do specyfiki lokalnej (układu urbanistycznego, skali zagrożenia, dostępnych zasobów finansowych). W miarę możliwości wskazane zostały warianty rozwiązań od prostych i nisko kosztowych po zaawansowane i wymagające większych nakładów, aby ułatwić ich implementację w różnych gminach.

Charakterystyka zagrożenia atakiem z użyciem pojazdu

Zanim przejdziemy do rozwiązań, warto zrozumieć specyfikę zagrożenia:

- **Element zaskoczenia:** Atak z użyciem pojazdu może nastąpić **nagle i bez ostrzeżenia**, w dowolnym miejscu, gdzie obecny jest tłum. Sprawca może wykorzystać pojazd osobowy, dostawczy lub ciężarowy – także wynajęty lub skradziony – co utrudnia wcześniejsze wykrycie zamiaru[2].
- **Duża siła rażenia:** Rozpędzony pojazd (nawet średniej wielkości) jest w stanie spowodować ciężkie straty w ludziach. Ciężarówka o masie kilkunastu ton jadąca z dużą prędkością może taranować przeszkody i ofiary na przestrzeni kilkudziesięciu metrów[3].
- **Wielość potencjalnych celów:** Przestrzeni, gdzie gromadzą się ludzie, jest bardzo dużo – od ulic handlowych po imprezy plenerowe. Nie sposób zabezpieczyć dosłownie każdego miejsca o każdym czasie, dlatego działania koncentrują się na **lokalizacjach najbardziej narażonych** (centra miast, strefy piesze, obiekty użyteczności publicznej) oraz na **wydarzeniach przyciągających tłumy**.
- **Ograniczenia środków technicznych:** Dostępne zabezpieczenia mogą **utrudnić lub powstrzymać** atak, lecz nie dają gwarancji pełnej ochrony. Nawet solidne bariery mają swoją wytrzymałość graniczną, a napastnik może znaleźć lukę (np. niezabezpieczony wjazd). Podczas testów zderzeniowych jednym z parametrów uwzględnianych przy sprawdzaniu skuteczności zabezpieczenia jest tzw. przebicie, które określa odległość, jak daleko poza linię zapory może przemieścić się pojazd. Znając ten parametr należy go uwzględnić podczas projektowania odległości bariery od chronionych obiektów lub ciągów pieszo-jezdnych. Dlatego ważny jest **przemyślany plan rozmieszczenia** zapór – decyzje, gdzie je ustawić, nie pozostawiają marginesu błędu[4].

[2] https://www.rand.org/randeurope/research/projects/2022/preventing-and-mitigating-terrorism-attacks-using-vehicles.html#:~:text=The%20frequency%20of%20vehicle,such%20attacks%20in%20the%20future

[3] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrier

[4] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=helped%20prevent%20Saturday%27s%20attack%20because,among%20those%20to%20be%20protected

- **Wpływ psychologiczny:** Obecność zabezpieczeń wpływa na poczucie bezpieczeństwa mieszkańców i odwiedzających. Należy dążyć do **złagodzenia „syndromu bunkra"**, tj. unikać przekształcania miasta w widoczną twierdzę, co mogłoby wywoływać niepokój. Rozwiązania powinny być **dyskretnie wkomponowane** w przestrzeń miejską – tak, by ludzie mogli czuć się swobodnie, nawet nie zdając sobie sprawy, że są chronieni. Jak podkreślają eksperci, **zachowanie otwartego charakteru miasta** jest istotne – nie chcemy, by strach dyktował wygląd naszych ulic.

Ustalając rodzaje ryzyka dla konkretnego miejsca należy uwzględnić zarówno zagrożenie, jak i potencjalne konsekwencje zdarzenia oraz podatności danego miejsca na atak z wykorzystaniem pojazdu, jako środka jego przeprowadzenia[5].

Znając te uwarunkowania, samorządy mogą podejść do problemu realistycznie: **redukcja ryzyka zamiast całkowitej eliminacji**. Celem jest takie przekształcenie i zarządzanie przestrzenią publiczną, by potencjalny zamachowiec napotkał **fizyczne bariery opóźniające lub uniemożliwiające** osiągnięcie celu, a służby miały szansę zareagować zanim dojdzie do największych strat. Poniżej przedstawiamy konkretne zalecenia, jak to osiągnąć.

Planowanie zabezpieczeń w różnych przestrzeniach publicznych

Charakter i układ przestrzeni wpływają na dobór środków bezpieczeństwa. Poniżej opisano kluczowe typy miejsc oraz rekomendowane podejścia do ich zabezpieczenia przed wjazdem groźnego pojazdu:

- **Rynki i place miejskie:** Otwarte place często otoczone są ulicami, z których potencjalnie może wjechać pojazd. **Stałe bariery na obwodzie placu** (np. ciągi słupków, murki, masywne donice) tworzą pierwszą linię obrony, chroniąc przebywających na środku ludzi. Należy zwrócić uwagę na zabezpieczenie głównych **wjazdów na plac** – tam warto zainstalować **zapory stałe lub automatyczne**, uniemożliwiające wjazd nieuprawnionych pojazdów. Jeśli plac służy okazjonalnie za parking lub punkt

[5] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, s. 129.

dostaw, można zastosować **chowane słupki (bollardy)** otwierane na czas przejazdu uprawnionych pojazdów. Przy planowaniu nowych placów zaleca się **projektowanie dróg dojazdowych pod kątem bezpieczeństwa** – np. zastosowanie łuków, zwężeń czy zmiany poziomów nawierzchni, aby uniemożliwić pojazdom nabranie dużej prędkości na wprost placu. W razie organizacji wydarzeń masowych na placu, wskazane jest dodanie **dodatkowych barier tymczasowych** na czas imprezy (szczegóły w dalszej części dokumentu).

- **Deptaki i strefy piesze:** Stałe deptaki (ulice wyłączone z ruchu) wymagają zabezpieczenia głównie na **początku i końcu strefy** – tam, gdzie normalnie zaczyna się obszar dla pieszych. Standardową praktyką jest montaż **stałych słupków** lub **zapór automatycznych** przy wlotach ulic dochodzących do deptaku, tak aby żaden pojazd nie mógł wjechać bez zgody. W wielu miastach Europy (np. we Francji) stosuje się kombinację **słupków stałych i chowanych** – stałe blokują wjazd przez większość czasu, a automatyczne mogą być opuszczane dla pojazdów uprzywilejowanych lub zaopatrzenia w określonych godzinach[6]. Ważne jest zachowanie **ciągłości zabezpieczeń** – np. jeśli deptak krzyżuje się z ulicą, na której ruch nie jest całkowicie zamknięty, należy rozważyć **osłonięcie ciągu pieszego barierami lub masywnymi elementami małej architektury** na odcinku skrzyżowania. Dodatkowym rozwiązaniem podnoszącym bezpieczeństwo jest **„naturalne" spowalnianie ruchu** wokół deptaku: wyspy dzielące pasy jezdni, szykany czy wyniesione przejścia, które zmuszają kierowców do wolnej jazdy i utrudniają gwałtowne skierowanie pojazdu w tłum.
- **Tereny imprez masowych:** w przypadku wydarzeń gromadzących tłumy (koncerty, festiwale uliczne, jarmarki sezonowe) organizowanych na otwartej przestrzeni, **szczególne znaczenie ma tymczasowe zabezpieczenie perymetru imprezy**. Należy zidentyfikować wszystkie możliwe drogi, którymi mógłby wjechać pojazd, i zawczasu je zablokować. **Zamknięcie ulic dojazdowych** powinno odbyć się w odpowiedniej odległości od zgromadzonych ludzi – tak, by ewentualny rozpędzony pojazd nie miał szans dotarcia do tłumu. W praktyce stosuje się kombinację środków:

[6] Tamże.

ciężkie fizyczne bariery (betonowe lub stalowe) ustawione w poprzek ulic, **specjalne mobilne zapory antyterrorystyczne** (moduły rozstawiane na jezdni) albo **pojazdy służb jako blokady**. Przykładowo, w Niemczech po zamachu na jarmark w Berlinie wprowadzono rutynowe zabezpieczanie dużych imprez – podczas festiwali w Stuttgarcie i innych miastach ustawiano na ulicach dojazdowych wielotonowe ciężarówki, tworząc barierę dla ewentualnego ataku[7]. Należałoby również dążyć do tego, aby pojazdy służb wykorzystywane jako blokady miały odpowiednią masę własną, aby spełniać funkcję realnego zabezpieczenia (samochód o masie 1,5 czy nawet 3,5 tony może nie stanowić skutecznej bariery, zatem należałoby w miarę możliwości dążyć do realizacji zabezpieczenia przy użyciu pojazdów ciężarowych, o masie powyżej 12 ton, traktowanych oczywiście jedynie jako środki doraźne). Organizatorzy powinni współpracować z Policją i samorządem, aby **plan zabezpieczeń imprezy (wymagany ustawą o bezpieczeństwie imprez masowych) uwzględniał scenariusz ataku z użyciem pojazdu** – łącznie z procedurą szybkiego zamknięcia dróg i gotowością do użycia dostępnych zapór.

- **Uniwersalne przestrzenie publiczne (parki, bulwary, itp.):** w otwartych przestrzeniach trudno o fizyczne bariery na całym obwodzie, warto jednak ocenić, **gdzie pojazd potencjalnie mógłby wjechać z dużą prędkością** (np. długi prosty odcinek alejki prowadzący w głąb parku, bulwar wzdłuż rzeki z dojazdem technicznym). W takich newralgicznych punktach zaleca się **punktowe instalowanie przeszkód**: np. zwężenie wjazdu do parku słupkami lub głazami dekoracyjnymi, ustawienie **blokad ograniczających wjazd** (szlabany, barierki) przy bocznych drogach dojazdowych wykorzystywanych tylko przez służby. **Mała architektura** może tu odgrywać rolę – ławki, donice, stojaki na rowery ustawione w ciągu mogą uniemożliwić rozpędzenie pojazdu po ścieżce parkowej. Trzeba przy tym zachować równowagę między dostępnością terenu dla mieszkańców (np. nie zamykać niepotrzebnie wejść do parku) a bezpieczeństwem – często

[7] https://www.dw.com/pl/niemieckie-miasta-reaguj%C4%85-na-zamach-w-barcelonie/a-40160693#:~:text=W%20STUTTGARCIE%20i%20innych%20miastach,kampanii%20wyborczej%20oraz%20na%20festynach

wystarczy utrudnić wjazd i wprowadzić element zaskoczenia, by zniechęcić potencjalnego sprawcę.

Niezależnie od rodzaju przestrzeni, kluczowe jest **warstwowe podejście**: im więcej kolejnych barier i utrudnień napotka pojazd, tym większa szansa na jego zatrzymanie lub spowolnienie, co daje ludziom czas na ucieczkę, a służbom – na reakcję. Poniżej opisano konkretne rozwiązania inżynieryjne i organizacyjne, które można zastosować.

Każdorazowo przed instalacją zapór antyterrorystycznych konieczne jest przeprowadzenie stosownej analizy ryzyka, jak również dokonanie rekonesansu uwzględniającego ukształtowanie terenu i rys urbanistyczny miejsc, w obrębie których planowana jest tego typu inwestycja. Wskazać bowiem należy, że samo ukształtowanie terenu lub rozmieszczenie ulic aglomeracji miejskich (np. kręta, wąska droga uniemożliwiająca rozpędzenie pojazdu) mogą determinować brak konieczności instalacji tego typu zapór, bądź stanowić indykator zwiększonego prawdopodobieństwa efektywnego zdarzenia o charakterze terrorystycznym z wykorzystaniem samochodu tarana w danym miejscu (np. szeroki deptak położony w pobliżu głównych ciągów komunikacyjnych miasta, plac położony w pobliżu zbocza umożliwiającego szybkie rozpędzenie się pojazdu, itp.).

Infrastrukturalne i architektoniczne środki ochronne

W tej części przedstawiono dostępne **rozwiązania techniczne** służące zabezpieczeniu przestrzeni publicznej przed wtargnięciem pojazdu. Obejmują one zarówno **stałe elementy infrastruktury**, które stają się częścią krajobrazu miejskiego, jak i **urządzenia automatyczne** oraz **sprzęt mobilny**. Ważne jest zrozumienie możliwości i ograniczeń poszczególnych środków – tak, by dobrać kombinację najlepiej pasującą do lokalnych potrzeb. Poniższa tabela zestawia podstawowe typy zapór i ich charakterystykę, a dalszy opis przedstawia ich rolę i przykłady zastosowań.

Tabela 1. Przegląd rodzajów zapór antyterrorystycznych i ich charakterystyki.

Stałe słupki i bariery (stalowe, betonowe)			
Orientacyjny koszt	**Skuteczność**	**Wymogi instalacyjne**	**Przykładowe zastosowania / uwagi**
Średni (jednorazowy montaż)	**Wysoka przeciwko autom osobowym**; przy zastosowaniu atestowanych słupów – także przeciw cięższym pojazdom przy umiarkowanych prędkościach. Certyfikowane modele zatrzymują nawet ciężarówki (7,5 t przy ~80 km/h). Wykazują skuteczność również jako kontrola dostępu na co dzień.	Wymagają prac ziemnych (fundamenty), projektu wpasowania w przestrzeń. Po instalacji – minimalne koszty utrzymania.	Stałe wygrodzenie deptaków, otoczenie placów, ochrona chodników przed wjazdem aut. Estetycznie można dopasować (np. stylizowane słupki). Utrudniają wjazd służbom, jeśli brak przerw lub elementów demontowalnych[8].
Automatyczne zapory wysuwane (bollardy chowane, zapory hydrauliczne)			
Orientacyjny koszt	**Skuteczność**	**Wymogi instalacyjne**	**Przykładowe zastosowania / uwagi**
Wysoki (zakup i infrastruktura)	**Bardzo wysoka** (certyfikowane modele zatrzymują nawet ciężarówki ~7,5 t przy ~80 km/h). Skuteczne również jako kontrola dostępu na co dzień.	Wymagają zasilania i układu sterowania, solidnego montażu (choć dostępne są systemy płytkiego montażu). Konieczny serwis techniczny.	Wjazdy do stref zamkniętych (starówki, ważne obiekty). Umożliwiają wpuszczanie uprawnionych pojazdów (np. komunikacji miejskiej, zaopatrzenia w wyznaczonych godzinach). W razie awarii muszą mieć procedurę awaryjnego opuszczenia[9].

[8] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=The%20highest%20security,worth%20their%20often%20enormous%20cost

[9] Tamże.

Masywne elementy małej architektury (betonowe donice, ławki blokujące, murki)			
Orientacyjny koszt	**Skuteczność**	**Wymogi instalacyjne**	**Przykładowe zastosowania / uwagi**
Niski do średniego (często element projektowania przestrzeni)	**Średnia** – dobrze zaprojektowane mogą zatrzymać lub odchylić lżejsze pojazdy; **ograniczona wobec ciężarówek** (te mogą je przesunąć lub staranować). Certyfikowane modele zatrzymują nawet ciężarówki (7,5 t przy ~80 km/h). Wykazują skuteczność również jako kontrola dostępu na co dzień.	Montaż w ramach aranżacji terenu (donice/ławki mogą wymagać kotwienia do podłoża dla stabilności). Potrzebna konserwacja jak przy zwykłej małej architekturze.	Mogą pełnić podwójną rolę: estetyczną i ochronną. Stosowane na starówkach, przy budynkach publicznych (np. ciągi donic ze zbrojonego betonu przed urzędem mogą zatrzymać ciężki pojazd). Powinny być **rozmieszczone tak, by nie pozostawiać szerokich luk**. Warto łączyć w grupy lub z dodatkowymi stalowymi elementami dla wzmocnienia efektu.
Barierki drogowe tymczasowe (przegrody, blokady betonowe typu Jersey)			
Orientacyjny koszt	**Skuteczność**	**Wymogi instalacyjne**	**Przykładowe zastosowania / uwagi**
Niski (często już w posiadaniu służb drogowych lub łatwe do wypożyczenia)	**Niska do średniej** – standardowe lekkie barierki metalowe nie stanowią przeszkody dla pojazdu (jedynie sygnał wizualny). Ciężkie bloki betonowe **spowalniają i utrudniają** wjazd, lecz **nie zatrzymają rozpędzonej ciężarówki** (testy DEKRA: ciężarówka 50 km/h pokonała betonowe bloki, zatrzymując się dopiero 80 m dalej).	Łatwe w użyciu – wystarczy ustawić w żądanym miejscu. Bloki betonowe wymagają sprzętu do transportu (dźwig, wózek widłowy). Ustawienie powinno uwzględniać pozostawienie przejścia dla pieszych.	Tymczasowe zamknięcie ulic na czas imprezy, wytyczenie strefy bezpieczeństwa. Zalecane **spinanie bloków w ciąg** (np. stalową liną lub łączenie modułowe), co zwiększa ich skuteczność. Lekkie barierki stosować tylko pomocniczo (do wygradzania terenu, kierowania ruchu), nigdy jako główna zapora antypojazdowa[10].

[10] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrier

Barierki drogowe tymczasowe (przegrody, blokady betonowe typu Jersey)			
Orientacyjny koszt	**Skuteczność**	**Wymogi instalacyjne**	**Przykładowe zastosowania / uwagi**
			Stanowią uzupełnienie dla barier antypodjazdowych. Ich zastosowanie – na przykład w formie szykan – może skutecznie obniżyć prędkość nadjeżdżającego pojazdu. W związku z tym możliwe jest zastosowanie barier certyfikowanych o niższej odporności na uderzenie, ponieważ niższa prędkość i masa pojazdu oznaczają mniejsze siły działające przy kolizji. Może to również obniżyć koszty instalacji barier certyfikowanych, przy zachowaniu ich skuteczności w odpowiednio przygotowanych warunkach.
Mobilne zapory antyterrorystyczne (moduły zaporowe)			
Orientacyjny koszt	**Skuteczność**	**Wymogi instalacyjne**	**Przykładowe zastosowania / uwagi**
Średni (koszt zakupu lub wynajmu zestawu)	**Wysoka** – certyfikowane moduły stalowe potrafią zatrzymać rozpędzony pojazd (dostępne konstrukcje testowane na ciężarówkach). Skuteczność zależna od modelu i konfiguracji modułów.	Wymagają krótkiego czasu na rozstawienie przez przeszkolony personel. Nie potrzebują stałego montażu – ustawia się je na nawierzchni, często klinuje własną masą i tarciem. Potrzebne miejsce składowania, transport na miejsce oraz obsługa przy rozkładaniu.	Najlepsze zabezpieczenie **doraźne** przy podwyższonym zagrożeniu lub eventach. Moduły umożliwiają swobodne przemieszczanie się pieszych i rowerzystów, jednocześnie chroniąc teren przed pojazdem taranującym.

			Po zakończeniu imprezy łatwo je usunąć. Rekomendowane do ochrony tras procesji, zgromadzeń publicznych, wizyt VIP itp. – wszędzie tam, gdzie nie ma stałych zapór, a ryzyko jest czasowo zwiększone.
Wykorzystanie pojazdów jako blokady (np. ciężarówki, autobusy miejskie)			
Orientacyjny koszt	**Skuteczność**	**Wymogi instalacyjne**	**Przykładowe zastosowania / uwagi**
Niski (wykorzystanie własnych zasobów, paliwo i ewentualne nadgodziny kierowców)	**Wysoka dla aut osobowych i średnia dla ciężarowych** – odpowiednio ustawiony ciężki pojazd (piaskarka, autobus) stanowi bardzo trudną do sforsowania barierę. Jednak **nie jest zakotwiczony**, więc rozpędzona ciężarówka może go przesunąć lub częściowo zepchnąć. Pojazdy służb wykorzystywane jako blokady powinny mieć odpowiednią masę własną, aby spełniały funkcję realnego zabezpieczenia. Samochód o masie 1,5 czy nawet 3,5 tony może nie stanowić skutecznej bariery, zatem należałoby w miarę możliwości dążyć do realizacji zabezpieczenia przy użyciu pojazdów ciężarowych, o masie powyżej 12 ton. Należy je traktować jedynie jako środki doraźne.	Wymaga dostępności ciężkich pojazdów i kierowców, a także uzgodnienia ze służbami (np. Policją). Pojazdy powinny być ustawione pod odpowiednim kątem (najlepiej bokiem do kierunku potencjalnego najazdu) i zabezpieczone (hamulec, kliny).	Metoda prowizoryczna, stosowana np. przez niemieckie miasta przed zabezpieczeniem imprez masowych. Dobra jako **ostatnia linia obrony** lub środek awaryjny – np. ustawienie pojazdów na końcu deptaku podczas dużego jarmarku świątecznego. Pojazdy-blokady wymagają stałej gotowości do ich przemieszczenia w razie potrzeby (np. przepuszczenia karetki), dlatego powinny stać z kierowcą w pobliżu lub możliwością szybkiego odjazdu.

***Orientacyjny koszt*:** „niski" – rozwiązanie tanie lub istniejące (do wykorzystania w ramach bieżących zasobów), „średni" – umiarkowany koszt zakupu/instalacji, „wysoki" – znaczny koszt inwestycyjny i utrzymania.

***Skuteczność*:** ocena względna przeciwko atakom – realna zdolność zatrzymania pojazdu zależy od masy i prędkości pojazdu oraz specyfikacji danej bariery.

***Wymogi instalacyjne*:** kluczowe wymagania techniczne, logistyczne lub formalne przy wdrażaniu danego środka.

Komentarz do powyższych rozwiązań: Należy podkreślić, że **atutem najlepszych systemów** (atestowanych zapór) jest ich **przewidywalna skuteczność** – przeszły one standaryzowane crash-testy (np. wg norm PAS 68, IWA 14-1 czy ASTM F2656, DOS (K4, K8, K12) lub ISO 22343), co oznacza, że wiadomo, jakiej masy i prędkości pojazd są w stanie zatrzymać. W praktyce jednak samorządy często muszą posiłkować się także rozwiązaniami prowizorycznymi lub o niższym standardzie (ze względów budżetowych lub estetycznych). Nawet one mogą **zmniejszyć ryzyko**: obecność choćby częściowych barier może zniechęcić sprawcę, który oceni mniejsze szanse powodzenia[11]. Trzeba jednak być świadomym ograniczeń – np. **zwykłe barierki drogowe czy luźno ustawione betonowe klocki nie zatrzymają rozpędzonej ciężarówki[12]**. Dlatego zawsze, gdy to możliwe, **należy wybierać rozwiązania sprawdzone i certyfikowane** lub zwiększające efektywność prostych środków (np. łącząc bloki w ciąg, stosując podwójne rzędy zapór, wykorzystując naturalne ukształtowanie terenu jak krawężniki, drzewa, słupy oświetleniowe itp. jako dodatkowe przeszkody).

Integracja zabezpieczeń z architekturą miasta

Dążąc do zabezpieczenia przestrzeni publicznej, warto wykorzystywać **podejście „Security by design"**, czyli wkomponowanie elementów ochronnych w projekt urbanistyczny i architektoniczny. Dzięki temu

[11] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, s. 133.

[12] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrie%20r

miasto może być bezpieczne **bez naruszania swojego uroku i funkcjonalności**. Oto dobre praktyki takiej integracji:

- **Elementy dekoracyjne o funkcji ochronnej:** Wiele fizycznych barier da się zamienić w atrakcyjne wizualnie instalacje. Przykładem jest stadion Emirates w Londynie, gdzie **duże betonowe litery tworzące napis „ARSENAL" pełnią rolę zapory antypojazdowej** chroniącej wejście na obiekt. Podobnie **betonowe ławki i rzeźby** mogą blokować drogi dojazdu, wyglądając jednocześnie jak część małej architektury. Takie „odporne na staranowanie cechy krajobrazu" były z powodzeniem stosowane wokół gmachów rządowych w Londynie (np. dyskretnie wbudowane barierki przy ulicy Whitehall).
- **Kwietniki i zieleń miejska: Masywne donice z roślinami** ustawione w ciągach to popularny sposób blokowania potencjalnej drogi pojazdu. Są estetyczne, a odpowiednio wykonane (ze zbrojonego betonu lub stali i wypełnione ziemią) stanowią solidną przeszkodę. Eksperci wskazują, że **nawet niewinnie wyglądające kwietniki mogą zatrzymać ciężarówkę, jeśli mają wewnątrz konstrukcję antyramową**. Takie donice stosuje się m.in. we Francji przed budynkami urzędów czy w Wielkiej Brytanii przy centrach handlowych. Tego typu wyroby, tj. kwietniki i donice, mogą również być certyfikowane.
- **Projektowanie ulic z myślą o bezpieczeństwie:** Architekci krajobrazu zalecają, by **układ ciągów komunikacyjnych nie dawał możliwości długiego, prostego rozpędzania pojazdu w stronę tłumu**. Można to osiągnąć poprzez **zakręty, ronda, szykany, zwężenia** – cokolwiek, co zmusi potencjalny pojazd do zwolnienia lub manewrowania. Przykładowo, deptak może być zaprojektowany z lekkim meandrowaniem zamiast idealnie prostej linii, a plac miejski może mieć wokół siebie **strefę buforową** z drzewami, latarniami i ławkami ustawionymi tak, by utrudnić pojazdowi rozpędzenie się.
- **Standardy odporności i atesty:** Jeśli to możliwe, **należy korzystać z produktów posiadających certyfikaty** potwierdzające ich skuteczność w zatrzymywaniu pojazdów. Na świecie przyjęto normy, jak brytyjskie **PAS 68** czy międzynarodowe **IWA 14-1**, ISO 22343, klasyfikujące bariery według zatrzymywanej masy i prędkości pojazdu. W praktyce oznacza to np., że słupek z certyfikatem może wytrzymać uderzenie ciężarówki 7,5 t przy

50 km/h, podczas gdy element nieatestowany o podobnym wyglądzie może zostać złamany już przez samochód osobowy. **Nie wolno mylić zwykłych barier drogowych z antyterrorystycznymi** – te pierwsze projektuje się z myślą o ograniczeniu skutków wypadków, a nie celowego ataku[13]. Dlatego np. **szare betonowe separatory drogowe** używane na drogach (tzw. „New Jersey") nie gwarantują zatrzymania ciężarówki i powinny być traktowane jedynie jako środek pomocniczy.

- **Unikanie błędów instalacji:** Nawet najlepsza zapora nie zadziała, jeśli zostanie źle zastosowana. **Niezakotwiczone, źle dobrane bariery mogą zostać przesunięte przez pojazd**, czyniąc więcej szkody – pchana ciężarówką barykada może wpaść w tłum, zamiast go ochronić[14]. Dlatego planując instalację, należy zwrócić uwagę na **techniczne wymogi montażu** (czy dany element powinien być przytwierdzony do podłoża, jak głęboki fundament jest potrzebny, w jakiej odległości od chronionego obiektu go ustawić). Jeśli stosowane są tymczasowo betonowe bloki, należy postarać się je **połączyć ze sobą** lub z innymi strukturami (np. ustawić za latarnią lub drzewem), by zwiększyć ich opór. Z kolei decydując się na automatyczne słupki, należy upewnić się, że mają one **system zasilania awaryjnego** lub możliwość ręcznego opuszczenia w razie zaniku prądu – tak, by w sytuacji krytycznej służby ratunkowe nie utknęły przed własnymi zaporami.

Tymczasowe zabezpieczenia i wykorzystanie istniejących barier

Jednostki samorządu terytorialnego stoją często przed wyzwaniem zabezpieczenia jednorazowych lub cyklicznych wydarzeń (np. doroczny festyn, maraton uliczny) bez posiadania na stałe rozbudowanej infrastruktury antyterrorystycznej. W takich sytuacjach kluczowe jest **skuteczne wykorzystanie dostępnych środków tymczasowych**. Poniżej opisano zalecenia w tym zakresie.

[13] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, s. 122.

[14] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, s. 127.

- **Barierki i zapory drogowe w nowej roli:** Typowe barierki używane przy organizacji ruchu (stalowe przęsła, pachołki, zapory drogowe) **same w sobie nie powstrzymają ataku**, ale mogą być użyte pomocniczo. Przykładowo, **ustawienie szeregu barier drogowych** może posłużyć do wyznaczenia toru przeszkód, zmuszając pojazd do slalomu i uniemożliwiając rozpędzenie się na wprost w tłum. Barierki metalowe można też wykorzystać do odgradzania strefy dla pieszych od jezdni, utrzymując dystans. **Zapewniają one jednak samodzielnie jedynie częściową ochronę**. Jeśli dysponujemy betonowymi segmentami (np. z remontów dróg), można je ustawić za taką linią barierek jako fizyczne wzmocnienie. **Woda i piasek** – wypełnienie pojemników – poprawią masę zapory, ale i tak ich skuteczność będzie ograniczona przy większych pojazdach[15].
- **Wypożyczanie lub dzielenie się mobilnymi zaporami:** Coraz więcej firm oferuje **wynajem mobilnych zapór antyterrorystycznych**. Samorządy w regionie mogą rozważyć **wspólny zakup** takiego sprzętu na potrzeby zabezpieczania różnych imprez. Alternatywnie, warto ustalić współpracę z firmami prywatnymi posiadającymi takie zapory (np. wynajmując je na duże wydarzenia miejskie). Ważne jest, by zawczasu przećwiczyć montaż – zapewnić przeszkolenie pracowników lub strażników miejskich w szybkim rozstawianiu i demontażu modułów. Mobilne bariery powinny być **rozmieszczone strategicznie**: np. zamiast stawiać pojedynczy rząd zapór tuż przed sceną koncertu, lepiej ustawić dwa rzędy w odstępie kilkunastu metrów na ulicach dojazdowych do miejsca imprezy (tworząc strefę buforową). Pamiętajmy także o **możliwości łączenia technik** – mobilne zapory można uzupełnić pojazdami służb, taśmami ostrzegawczymi, a nawet naturalnymi elementami otoczenia (np. zastawiając wjazd między budynki ciężkim kontenerem na śmieci czy betonowymi śmietnikami miejskimi).
- **Wykorzystanie pojazdów komunalnych i służbowych:** Zgodnie z danymi przedstawionymi w tabeli, użycie ciężkich pojazdów jako blokad to sprawdzony doraźny sposób. **Plan zarządzania**

[15] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrie%20r

kryzysowego dla imprezy masowej powinien przewidywać, skąd w razie potrzeby wziąć takie pojazdy – czy to z floty miejskiej (śmieciarki, piaskarki, autobusy), czy od partnerów (firm budowlanych, komunikacji publicznej). Warto **ustalić procedurę**: kto decyduje o podstawieniu pojazdów, gdzie dokładnie mają stanąć, kto kieruje. Dobrą praktyką jest utrzymywanie pojazdów w pogotowiu na obrzeżach imprezy. Przykładowo, podczas kiermaszu świątecznego można umieścić za rogiem dwie posypywarki uliczne gotowe w razie sygnału zablokować główny wjazd. Należy pamiętać o **widoczności sygnałów uprzywilejowania** – pojazd wykorzystywany jako zapora powinien mieć włączone światła ostrzegawcze (koguty), aby był dobrze widoczny i jednoznacznie kojarzony z działaniami służb, co zapobiega panice i ułatwia komunikację (ludzie oraz kierowcy powinni widzieć, że blokada jest intencjonalna, a nie np. wynikła z wypadku).

- **Tymczasowe modyfikacje infrastruktury:** Jeśli dane miejsce jest regularnie używane na imprezy (np. plac miejski co roku na koncert sylwestrowy), można rozważyć **trwałe przygotowanie punktów montażowych** dla zapór tymczasowych. Mogą to być np. **zakotwienia w nawierzchni** zakryte na co dzień dekoracyjnymi zaślepkami, w które w razie potrzeby wstawiane są dodatkowe słupki/barierki. Innym pomysłem jest posiadanie **segmentów bariery łańcuchowej** pasujących do stałych elementów – np. jeśli plac otaczają na stałe słupki, można mieć łańcuchy lub belki, które szybko zamocujemy między nimi, tworząc ciągłą barierę. To proste rozwiązania, ale mogą zaoszczędzić cenny czas przy zabezpieczaniu terenu.

Podsumowując, w sytuacjach szczególnych **należy wykorzystywać kreatywnie to, czym dysponuje dany samorząd**. Nawet prowizoryczna zapora może uratować życie, jeśli zostanie mądrze użyta. Jednakże zawsze, gdy planowane są tylko tymczasowe środki, należy mieć tzw. **plan B** – co należy zrobić, jeśli one zawiodą. Dlatego tak ważna jest rola służb porządkowych podczas zabezpieczanych wydarzeń, o czym poniżej.

Rola lokalnych służb porządkowych (straży miejskiej/gminnej)

Straż miejska lub gminna, jako formacja podległa samorządowi, odgrywa istotną rolę we wsparciu zabezpieczeń architektonicznych i organizacyjnych przeciw zagrożeniom terrorystycznym. Jej zadania i kompetencje w tym kontekście obejmują:

- **Nadzór nad przestrzenią publiczną:** Strażnicy miejscy, pełniąc patrole na ulicach, mogą **monitorować stan zabezpieczeń** – sprawdzać, czy stałe bariery nie zostały uszkodzone lub celowo usunięte, pilnować, by automatyczne słupki nie pozostawały nieopuszczone bez potrzeby, kontrolować, czy nie ma nieuprawnionego ruchu pojazdów w strefach chronionych. Są „oczami i uszami" samorządu w terenie, więc ich spostrzeżenia mogą szybko wychwycić potencjalne słabe punkty (np. otwartą blokadę drogową, zepsuty mechanizm zapory, objazd, który umożliwia wjazd od innej strony).
- **Egzekwowanie zakazów ruchu:** Większość rozwiązań architektonicznych działa w powiązaniu z przepisami – np. znakami zakazu ruchu w strefie zamkniętej dla pojazdów, godzinami dostaw itp. Straż miejska ma uprawnienia do egzekwowania tych lokalnych przepisów (stosowanie postępowania mandatowego za wjazd w niedozwoloną strefę, usuwanie nieprawidłowo zaparkowanych pojazdów). **Usuwanie nielegalnie parkujących aut** z chodników czy deptaków to nie tylko kwestia porządku, ale i bezpieczeństwa – pozostawiony samochód mógłby posłużyć jako środek do popełnienia zamachu terrorystycznego lub utrudnić działanie zapór (np. ktoś omija słupek jadąc po chodniku). Dlatego strażnicy powinni kłaść nacisk na **utrzymanie stref ochronnych wolnych od pojazdów**.
- **Wsparcie przy zamykaniu ulic i organizacji imprez:** Przy czasowych zamknięciach dróg (np. na czas manifestacji, biegu ulicznego, koncertu) w kontekście antyterrorystycznym strażnicy mogą **ustawiać i pilnować barykad** – np. stacjonować przy wlocie zamkniętej ulicy z radiowozem w poprzek drogi, by w razie potrzeby *fizycznie* zastopować próbę wjazdu (radiowóz również może pełnić rolę bariery w sytuacji kryzysowej, choć oczywiście życie funkcjonariuszy jest tu priorytetem). Strażnicy mogą także

kierować pojazdy uprawnione objazdami, aby te nie podjeżdżały pod tłum.

- **Obsługa urządzeń bezpieczeństwa:** Wiele samorządów powierza straży miejskiej administrację systemami kontroli dostępu – np. **pilot do opuszczania automatycznych słupków** bywa w dyspozycji patroli lub dyżurnego straży. Strażnicy mogą mieć za zadanie otwierać zapory dla pojazdów służb komunalnych, zamykać je po przejechaniu dostaw, itp. Ważne, by istniały jasne procedury: kto i kiedy decyduje o podniesieniu/opuszczeniu słupka, by nie doszło do nieautoryzowanego wjazdu przez błąd komunikacji. Dobrą praktyką jest wyposażenie centrali straży w podgląd CCTV (monitoring miejski) na wjazdy do stref chronionych – strażnik może zdalnie zweryfikować potrzebę wjazdu i odblokować zaporę, mając jednocześnie nagranie zdarzenia.
- **Monitoring i szybkie reagowanie:** Wiele samorządów dysponuje **miejskim systemem monitoringu wizyjnego**, często obsługiwanym przez straż miejską. Operatorzy kamer powinni być przeszkoleni, by zwracać uwagę na nietypowe zachowania pojazdów w okolicy stref pieszych – np. samochód poruszający się z nadmierną prędkością w kierunku zamkniętej ulicy, czy wielokrotnie krążący van w pobliżu zgromadzenia. **Wczesne wykrycie zagrożenia** pozwoli straży lub Policji zareagować (ustawić dodatkową blokadę, zatrzymać kierowcę zanim wjedzie w tłum). Strażnicy miejscy jako pierwsi na miejscu mogą próbować **przekierować ruch** lub **ewakuować ludzi**, jeśli zauważą pędzący pojazd.
- **Współpraca z Policją i innymi służbami:** w sytuacji zagrożenia o charakterze terrorystycznym główna rola przypada Policji (w tym przede wszystkim policyjni kontrterrorystom), jednak straż miejska/gmina może pełnić funkcje pomocnicze – np. zabezpieczenie terenu wokół, kierowanie ludności w bezpieczne rejony, dostarczanie informacji do sztabu kryzysowego. Dobrze, jeśli zawczasu ustalone są kanały łączności i podział zadań (np. straż zamyka natychmiast ruch na sąsiednich ulicach, aby służby ratunkowe miały swobodny dojazd). Warto również **włączać strażników w szkolenia i ćwiczenia antykryzysowe** związane z atakami terrorystycznymi – ich znajomość topografii miasta i doświadczenie w pracy z mieszkańcami może znacząco usprawnić przebieg akcji.

- **Edukacja i budowanie świadomości:** Straż miejska może prowadzić **działania informacyjne** odnośnie właściwych zachowań w sytuacji zagrożenia na ulicy. Chodzi np. o przekazywanie rad „**co robić, gdy zauważysz pędzący samochód w tłum**" – uciekać bokiem, schować się za najbliższą przeszkodą (murkiem, drzewem, latarnią), ostrzec innych. Świadomy i czujny obywatel to dodatkowy element systemu bezpieczeństwa, a strażnicy mogą tę czujność kształtować, ucząc rozpoznawać sygnały zagrożenia i właściwie reagować.

Podsumowując, straż miejska/gminna jest naturalnym wsparciem w realizacji działań opisanych w tych rekomendacjach. Aby w pełni wykorzystać jej potencjał, **samorząd powinien doprecyzować zakres kompetencji** (np. w regulaminie straży uwzględnić zadania związane z zabezpieczeniem antyterrorystycznym) oraz **zapewnić odpowiednie szkolenia** z tego zakresu. Dobra współpraca straży z Policją, zarządcami dróg i organizatorami imprez przełoży się na sprawniejsze i skuteczniejsze zabezpieczenie na poziomie lokalnym.

Aspekty prawne i organizacyjne

Wdrożenie opisanych rozwiązań wymaga uwzględnienia szeregu kwestii prawnych i organizacyjnych. Poniżej omówiono najważniejsze z nich, które samorząd powinien mieć na uwadze:

- **Odpowiedzialność administracyjna:** Bezpieczeństwo przestrzeni publicznej leży w gestii organów samorządu oraz administracji rządowej. W praktyce **prezydent miasta / burmistrz / wójt** odpowiada za realizację zadań z zakresu porządku publicznego na swoim terenie, współpracując z wojewodą i służbami państwowymi. Instalacja stałych zabezpieczeń (słupków, zapór) na drogach gminnych wymaga decyzji zarządcy drogi (często to miejski zarząd dróg, podległy prezydentowi) – stąd samorząd musi zadbać o formalne zatwierdzenie projektów organizacji ruchu uwzględniających nowe bariery. W strukturach miejskich warto wyznaczyć **koordynatora ds. bezpieczeństwa przestrzeni publicznych** – osobę lub komórkę odpowiedzialną za planowanie i nadzorowanie wdrażania tych środków. Może to być element miejskiego zespołu zarządzania kryzysowego lub osobny pełnomocnik prezydenta ds. bezpieczeństwa. Ważne, aby jasno określić,

kto utrzymuje i monitoruje poszczególne urządzenia (np. czy za serwis automatycznych bollardów odpowiada wydział inwestycji, zarząd dróg czy może firma zewnętrzna).

- **Koordynacja z właścicielami i zarządcami prywatnych przestrzeni publicznych:** w miastach wiele przestrzeni **formalnie prywatnych** pełni de facto funkcję publiczną – np. pasaże przy centrach handlowych, place między biurowcami, kampusy prywatnych uczelni, parkingi supermarketów itp. Samorząd nie może jednostronnie narzucić tam swoich instalacji, ale **współpraca jest kluczowa**. Zaleca się zaproszenie zarządców takich obiektów do **wspólnych ustaleń** w ramach komisji bezpieczeństwa czy zespołu zarządzania kryzysowego. Warto opracować **standardy minimalne** zabezpieczenia takich miejsc – np. zachęcać (albo wymagać w decyzjach administracyjnych, jeśli to możliwe) instalacji słupków przed wejściami do galerii handlowych, montażu blokad przy podjazdach do pasaży. Można tu wykorzystać **audyt bezpieczeństwa**: miejskie służby (np. Państwowa Straż Pożarna, Policja, straż miejska) we współpracy z właścicielem dokonują przeglądu obiektu i sugerują ulepszenia. Również **ćwiczenia praktyczne** (np. symulacja ataku lub ewakuacji w centrum handlowym) z udziałem służb i personelu obiektu ujawnią braki i pozwolą wypracować procedury. Prawnie rzecz biorąc, właściciel terenu odpowiada za zapewnienie bezpieczeństwa użytkowników – gmina może więc argumentować, że **wdrożenie zabezpieczeń leży także w jego interesie (ograniczenie odpowiedzialności cywilnej)**. W przypadku dużych obiektów użyteczności publicznej (stadiony, centra handlowe) często wymagany jest plan ochrony uzgadniany z Policją – warto dopilnować, by uwzględniał on również **zagrożenie pojazdem**.
- **Zgodność z prawem budowlanym i przepisami technicznymi:** Instalacja stałych zapór antyterrorystycznych może podlegać przepisom prawa budowlanego. Niektóre elementy (np. murki, fundamenty pod zapory) będą wymagały projektu budowlanego i pozwolenia na budowę albo zgłoszenia robót budowlanych. Należy zapewnić, że projekt przygotuje osoba z odpowiednimi uprawnieniami. **Ustawienie barier na drogach publicznych** musi być zgodne z przepisami o ruchu drogowym – wymagane jest zatwierdzenie nowej organizacji ruchu (znaki, urządzenia bezpieczeństwa ruchu). Ponadto **przepisy BHP i przeciwpożarowe**

wymagają, by zabezpieczenia nie utrudniały ewakuacji ludzi i dojazdu służb ratunkowych. Oznacza to np., że **ciągi piesze obok słupków muszą pozostawać drożne** (zapewnienie minimalnej szerokości przejścia), a jeśli zamykamy ulicę, to trzeba zachować możliwość szybkiego usunięcia bariery w razie wjazdu straży pożarnej w obszarach objętych nadzorem konserwatora zabytków (np. starówki) **dobór formy zabezpieczeń** powinien być uzgodniony z konserwatorem – czasem nie można dowolnie ustawić betonowych bloków, bo szpecą historyczny układ, wtedy trzeba szukać rozwiązań alternatywnych (np. stylizowane słupki, które wpisują się w estetykę miejsca).

- **Ustawa o zarządzaniu kryzysowym i dokumenty planistyczne:** Zgodnie z ustawą o zarządzaniu kryzysowym, każda gmina powinna posiadać **Plan Zarządzania Kryzysowego**, który identyfikuje potencjalne zagrożenia (w tym o charakterze terrorystycznym) i określa procedury reagowania. W kontekście ataków z użyciem pojazdu warto, aby plan ten:
  - zawierał **scenariusz takiego zamachu** (analizę ryzyka, wskazanie najbardziej narażonych miejsc w gminie),
  - określał **siły i środki** do przeciwdziałania – czyli inwentarz dostępnych zabezpieczeń (np. lista lokalizacji, gdzie są stałe zapory; magazyn mobilnych barier; dostępne ciężarówki i pojazdy do blokady wraz z kontaktami do dysponentów),
  - przydzielał **role i obowiązki** – np. kto decyduje o podniesieniu poziomu zabezpieczeń przy podwyższonym stopniu alarmowym (BRAVO/CHARLIE/DELTA), kto odpowiada za fizyczne ustawienie barier w razie zagrożenia itd.,
  - uwzględniał **tryb współdziałania z innymi podmiotami** – np. z zarządcami dróg krajowych przebiegających przez miasto (jeśli trzeba zablokować zjazd z takiej drogi na teren imprezy), z sąsiednimi gminami (gdy zdarzenie ma szerszy wpływ), z wojewódzkim centrum zarządzania kryzysowego (raportowanie). Regularna aktualizacja planu oraz ćwiczenia (chociażby na poziomie gry decyzyjnej) pozwolą utrzymać gotowość. Poza planem kryzysowym, również **miejscowe plany zagospodarowania przestrzennego** dla newralgicznych obszarów mogą zawierać wytyczne dotyczące bezpieczeństwa (np. nakaz projektowania pasaży handlowych z elementami blokującymi wjazd).

- **Finansowanie inwestycji w bezpieczeństwo:** Zakup i instalacja profesjonalnych systemów antyterrorystycznych bywa kosztowna. Samorządy powinny poszukiwać dostępnych **źródeł finansowania zewnętrznego** – np. funduszy europejskich (Fundusz Bezpieczeństwa Wewnętrznego UE przewiduje środki na ochronę przestrzeni publicznych). Warto przygotować **projekty uzasadniające potrzebę** (np. wnioskując o dofinansowanie instalacji zapór automatycznych na starówce, powołać się na analizy zagrożeń i dobre praktyki z innych miast). Ponadto, angażując podmioty prywatne (np. galerie handlowe) we wspólne inicjatywy, można dzielić koszty – np. miasto buduje infrastrukturę pod automatyczne blokady, a centrum handlowe zapewnia same urządzenia. Należy również planować **koszty utrzymania**: serwis, naprawy, okresowe crash-testy (jeśli to wymagane przez producenta). Lepiej zainwestować w atestowane rozwiązanie niż ponosić odpowiedzialność za awaryjny półśrodek, który zawiedzie – ta świadomość powinna przyświecać decydentom przy alokacji środków.

Wymagania formalne w zakresie bezpieczeństwa dla wykonawców i pracowników, realizujących czynności w zakresie systemów kontroli dostępu do barier antyterrorystycznych lub ich integracji

Zasadne jest sprawdzenie czy wykonawca posiada koncesję MSWiA na prowadzenie działalności w zakresie ochrony osób i mienia. Wskazane jest, aby w przypadku dostępu do informacji niejawnych wykonawca dysponował ważnym Poświadczeniem Bezpieczeństwa Przemysłowego co najmniej III stopnia, z klauzulą dostępu „POUFNE". Spełnienie tego wymogu nie obejmuje obowiązku posiadania kancelarii tajnej.

Pracownicy realizujący czynności w zakresie systemów kontroli dostępu lub ich integracji powinni:

- posiadać osobowe poświadczenie bezpieczeństwa, co najmniej na poziomie „POUFNE";
- figurować na liście kwalifikowanych pracowników zabezpieczenia technicznego, zgodnie z ustawą z dnia 22 sierpnia 1997 r. o ochronie osób imienia (Dz. U. z 2025 r. poz. 532).

Pracownicy wykonujący prace ogólnobudowlane (np. wykopy, instalacje kablowe, montaż urządzeń) nie są zobowiązani do posiadania

poświadczenia bezpieczeństwa osobowego, jednak powinni posiadać aktualne zaświadczenie o niekaralności. Wymogi te dotyczą również podwykonawców, biorących udział w pracach montażowych lub serwisowych.

Dostosowanie rekomendacji do różnych jednostek samorządu terytorialnego

Prezentowane rekomendacje mają charakter ogólny – ich wdrożenie będzie wyglądać inaczej w metropolii, a inaczej w małym miasteczku. Każda jednostka samorządu terytorialnego powinna **przeprowadzić własną analizę potrzeb i możliwości**, biorąc pod uwagę takie czynniki jak: wielkość ruchu turystycznego, liczba wydarzeń o charakterze masowym w roku, ukształtowanie urbanistyczne (np. zabytkowa starówka vs. rozproszone osiedla), posiadany budżet i kadry.

Oto wskazówki, jak dostosować zalecenia do lokalnych warunków:

- **Małe miasta i gminy o ograniczonym budżecie:** Priorytetem powinno być **wytypowanie najbardziej wrażliwych miejsc** (np. główny rynek, deptak przy ratuszu, teren festynu dożynkowego) i zastosowanie tam choćby prostych środków. Jeśli nie stać podmiotu na automatyczne słupki, powinien zacząć od **trwałych słupków lub donic betonowych** – koszt jednostkowy nie jest duży, a można je montować sukcesywnie. Wiele takich gmin już posiada elementy małej architektury, które wystarczy **rozmieszczać strategicznie**. Można też poszukać **sprzętu używanego** – np. pozyskać bariery od większego miasta (po modernizacji) czy z demobilu. Ważne jest również **przeszkolenie strażników gminnych i ochotniczych straży pożarnych** w reagowaniu na tego typu incydenty, bo w małej społeczności to oni będą pierwsi na miejscu.
- **Średnie miasta:** Mające już pewną infrastrukturę i budżet na inwestycje, powinny **systemowo podejść** do tematu. Warto opracować **miejski program poprawy bezpieczeństwa przestrzeni publicznych** na kilka lat, z przypisaniem środków w budżecie. Taki program może np. zakładać: I etap – instalacja zapór na rynku i głównym deptaku, II etap – zakup mobilnych barier dla zabezpieczenia imprez, III etap – utworzenie centrum monitoringu itp.

Istotna jest też **wymiana doświadczeń** – np. poprzez Unie Metropolii Polskich lub inne stowarzyszenia miast, można czerpać z wiedzy liderów (duże miasta często chętnie dzielą się wypracowanymi rozwiązaniami). Średnie miasta powinny też rozważyć **ćwiczenia międzygminne** – zagrożenia terrorystyczne rzadko dotyczą tylko jednej gminy.

- **Duże miasta i metropolie:** Tutaj oczekiwania mieszkańców co do bezpieczeństwa są wysokie, a i potencjalne ryzyko (z uwagi na atrakcyjność celów) większe. Duże miasta powinny inwestować w **najskuteczniejsze dostępne technologie** – np. **systemy zintegrowane** (blokady sprzężone z sygnalizacją świetlną, zdalne sterowanie zaporami z centrum monitoringu, czujniki wykrywające nietypowo szybko jadący pojazd i automatycznie podnoszące zapory). Budżet oczywiście jest barierą, ale duże jednostki mają łatwiejszy dostęp do funduszy zewnętrznych i mogą argumentować swoje potrzeby bezpieczeństwem np. infrastruktury krytycznej czy rangi międzynarodowej (turystyka, siedziby instytucji itp.). Ważne jest utrzymywanie **sieci współpracy** z ekspertami – np. korzystanie z doradców ds. bezpieczeństwa antyterrorystycznego (można konsultować plany z ABW lub policyjnymi specjalistami ds. terroryzmu). Duże miasto powinno również zlecać **audyty zewnętrzne** co pewien czas – świeże spojrzenie eksperta pozwoli wykryć luki, które własnym służbom mogły umknąć.
- **Elastyczność i aktualizacja:** Zagrożenia terrorystyczne ewoluują – pojawiają się nowe techniki (np. w przyszłości potencjalnie zdalne przejmowanie pojazdów autonomicznych), zmieniają się też możliwości techniczne zabezpieczeń. Dlatego niniejsze rekomendacje nie mogą być traktowane jako zamknięty katalog. Przykładowo, Komisja Europejska publikuje wytyczne ochrony przestrzeni publicznych przed atakami (np. poradnik doboru barier antyramowych[16]), a organizacje branżowe prezentują nowe rozwiązania techniczne (konferencje, targi bezpieczeństwa). Warto z tego korzystać. Równie ważna jest **analiza incydentów**, które jednak się wydarzą – jeśli gdziekolwiek dojdzie do ataku wjechania w tłum, należy zadawać pytanie: *czy w danym mieście podobny scenariusz mógłby mieć miejsce? Czy dostępne są środki by temu*

[16] https://ec.europa.eu/newsroom/pps/items/665632/en#:~:text=JRC%20Guideline%20Selecting%20proper%20security,now%20also%20available%20in%20French

zapobiec, a jeśli nie – co należy usprawnić? Wyciąganie wniosków z cudzych doświadczeń jest kluczem do ciągłego doskonalenia zabezpieczeń.

Podsumowanie

Bezpieczna przestrzeń publiczna to taka, w której **ludzie mogą swobodnie przebywać i cieszyć się nią, nie będąc niepotrzebnie niepokojonymi widokiem umocnień**, a jednocześnie **potencjalny agresor napotka ukryte przeszkody** niweczące jego plany. Cel ten osiąga się poprzez **wieloaspektowe działania**: od twardej infrastruktury (zapory, słupki, bariery), przez rozwiązania organizacyjne (plany zabezpieczeń, procedury na czas imprez), po czynnik ludzki (czujność służb i obywateli).

Dobrze zaprojektowane i wdrożone środki mogą realnie **zmniejszyć prawdopodobieństwo udanego zamachu lub ograniczyć jego skutki**. Jak wskazano, nawet proste bariery mogą uratować życie, opóźniając pojazd lub zmieniając jego tor – dając ludziom dodatkowe sekundy na ucieczkę. Ostatecznie jednak żadne środki nie dają 100% gwarancji, dlatego tak ważne jest **całościowe podejście**: łączenie różnych rozwiązań i utrzymywanie gotowości do reagowania na nieprzewidziane sytuacje.

Samorządy w Polsce, korzystając z doświadczeń innych państw europejskich, mogą **skutecznie podnieść poziom bezpieczeństwa** swoich miast i gmin, nie nadwyrężając przy tym budżetu ani nie zakłócając przyjaznego charakteru przestrzeni publicznych. Kluczem jest planowanie z wyprzedzeniem (zanim wydarzy się tragedia), stała współpraca z ekspertami i służbami, a także edukacja społeczności lokalnej. W ten sposób tworzy się miasta odporne na zagrożenia, ale wciąż **otwarte i przyjazne** – miejsca, gdzie bezpieczeństwo staje się naturalnym elementem infrastruktury, niemal niewidocznym dla zwykłego oka przechodnia, lecz czuwającym nad jego spokojem.

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 235–254

https://doi.org/10.4467/27204383TER.25.052.23039

Varia

Terroryści, sabotażyści, szpiedzy przebywający w polskich jednostkach penitencjarnych – rola Służby Więziennej

Andrzej Leńczuk
Autor niezależny
https://orcid.org/0009-0009-0719-6599

Wprowadzenie

Od 2021 r. możemy obserwować w Polsce procesy mające związek ze zmianami w sytuacji międzynarodowej, a w szczególności z wojną w Ukrainie wywołaną przez Rosję i kryzysem migracyjnym na granicy polsko-białoruskiej. Dowiadujemy się o zatrzymaniach na terytorium RP szpiegów, dywersantów, sabotażystów podejmujących różne działania, również dezinformacyjne, w celu wywołania poczucia zagrożenia, strachu i destabilizacji nastrojów społecznych w Polsce. Pożar centrum handlowego przy ulicy Marywilskiej w Warszawie czy aktywność obcych służb wywiadowczych, ukazywana m.in. w komunikatach Agencji Bezpieczeństwa Wewnętrznego czy Prokuratury Krajowej, to tylko niewielka część działań określanych mianem hybrydowych lub nawet wojny hybrydowej.

W związku z tym nasuwa się pytanie, czy SW, realizując powierzone jej zadania, jest przygotowana na nowe wyzwania związane z wojną

hybrydową, której wyrazem jest obecność w zakładach karnych i aresztach śledczych szpiegów, sabotażystów i dywersantów. W celu odpowiedzi na to pytanie zostaną przedstawione podstawowe informacje na temat SW oraz zakładów karnych i aresztów śledczych, funkcje, jakie w nim pełnią funkcjonariusze i pracownicy, oraz dane statystyczne dotyczące obecności w zakładach karnych i aresztach śledczych wskazanych sprawców.

Ramy prawne funkcjonowania Służby Więziennej i jej zadania oraz organizacja zakładów karnych i aresztów śledczych – wybrane aspekty

Funkcjonowanie zakładów karnych i aresztów śledczych oraz zadania funkcjonariuszy SW są opisane w wielu aktach prawnych. Najważniejsze z nich to Kodeks karny wykonawczy[1] (dalej: k.k.w.) oraz *Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej* (dalej: ustawa o SW)[2].

Służba Więzienna w przeciwieństwie do Policji, Straży Granicznej czy Państwowej Straży Pożarnej, ale wzorem wielu innych państw, podlega bezpośrednio Ministrowi Sprawiedliwości. Ten model podległości służby ma ponad 100-letnią tradycję z wyjątkiem okresu 1945–1956, kiedy formacja podlegała najpierw Ministerstwu Bezpieczeństwa Publicznego, a od 1954 r. – Ministerstwu Spraw Wewnętrznych.

Służba Więzienna zatrudnia niemal 30 000 funkcjonariuszy i pracowników i jest trzecią pod względem liczebności formacją mundurową w Polsce[3]. Niezbędnym elementem niemal każdego munduru są stopnie. W SW zachowały one nazewnictwo na wzór wojskowy w czterech korpusach: szeregowych, podoficerów, chorążych, oficerów. Najniższy stopień, od którego rozpoczyna służbę każdy funkcjonariusz, to szeregowy, najwyższy zaś to generał inspektor SW.

Model funkcjonowania SW, obejmujący przypisane jej zadania, zasadę hierarchiczności, jednoosobowe kierownictwo, umundurowanie, stopnie służbowe i wyposażenie w broń palną, sytuuje formację wśród innych grup dyspozycyjnych o charakterze paramilitarnym, pełniących ważną funkcję

[1] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy* (t.j. DzU z 2025 r. poz. 911, ze zm.).

[2] *Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej* (t.j. DzU z 2024 r. poz. 1869, ze zm.).

[3] Służba Więzienna – o nas, https://sw.gov.pl/strona/rekrutacja-o-nas [dostęp: 4 VIII 2025].

w systemie bezpieczeństwa wewnętrznego[4]. Do tej kategorii zalicza się również m.in.: Policję, Straż Graniczną, Państwową Straż Pożarną, Służbę Ochrony Państwa, Agencję Bezpieczeństwa Wewnętrznego, Straż Ochrony Kolei. Są to jednocześnie formacje, z którymi SW współpracuje. Wydarzenia, do których dochodzi na polskiej granicy od jesieni 2021 r., wywołały potrzebę zacieśnienia współpracy SW ze Strażą Graniczną, a także ABW. Straż Graniczna realizuje część swoich zadań ustawowych w bezpośredniej współpracy z SW. Dotyczy to m.in. realizowanych czynności dochodzeniowo-śledczych i postępowań przygotowawczych w rozumieniu przepisów Kodeksu postępowania karnego[5] oraz w określonym zakresie wymiany informacji, np. związanych z wykonywaniem czynności konwojowych z udziałem tymczasowo aresztowanych będących w zainteresowaniu Straży Granicznej. Współpraca obu służb mundurowych służy zarówno zapewnieniu bezpieczeństwa jednostek penitencjarnych, jak i bezpieczeństwa obywateli.

Wysiłki SW na rzecz utrzymania porządku i bezpieczeństwa wewnątrz zakładów karnych i aresztów śledczych oraz ochrony społeczeństwa przed przestępcami są także wspierane na zasadach współpracy przez ABW. Obie służby zawarły 27 października 2021 r. *Porozumienie o współpracy naukowo-dydaktycznej w zakresie przeciwdziałania radykalizacji i zagrożeniom terrorystycznym*. Stworzyło to nowe możliwości współdziałania, obejmujące np. organizowanie szkoleń, konferencji, wymianę doświadczeń. Strategicznym celem porozumienia było jednak (...) *przeciwdziałanie radykalizacji, prowadzącej do brutalnego ekstremizmu i terroryzmu w środowisku penitencjarnym oraz wykluczenie ryzyka nawrotu do radykalnej aktywności po opuszczeniu zakładu karnego. Z tego powodu przedmiotem kooperacji będzie m.in. analiza przypadków radykalizacji w zakładach karnych w celu ustalenia odpowiednich programów resocjalizacji, deradykalizacji, które będą także sprzyjać skutecznej reintegracji społecznej w okresie postpenitencjarnym*[6]. Komórką organizacyjną ABW, która w tym zakresie odgrywała szczególnie ważną rolę, było Centrum Prewencji Terrorystycznej, a obecnie jest to Wydział Prewencji Zagrożeń Centrum Antyterrorystycznego.

---

[4] J. Maciejewski, *Grupy dyspozycyjne. Analiza socjologiczna*, Wrocław 2012, s. 49–53.

[5] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j. DzU z 2025 r. poz. 46, ze zm.).

[6] *Współpraca ABW i SW w zakresie prewencji terrorystycznej*, Terrorism Prevention, https://tpcoe.gov.pl/cpt/wydarzenia/1912,Wspolpraca-ABW-i-SW-w-zakresie-prewencji-terrorystycznej.html [dostęp: 5 VIII 2025].

Podstawowymi jednostkami organizacyjnymi więziennictwa są zakłady karne i areszty śledcze podległe Ministrowi Sprawiedliwości[7], który w drodze zarządzenia tworzy i znosi zakłady karne oraz przekształca je w areszty śledcze, z uwzględnieniem istniejących potrzeb. Zakładem karnym bądź aresztem śledczym kieruje dyrektor. Inni funkcjonariusze i pracownicy zakładu karnego oraz inne osoby w zakresie swoich obowiązków w związku z organizacją pracy czy różnego rodzaju zajęć są natomiast przełożonymi skazanego[8].

Fundamentalnym warunkiem prawidłowego funkcjonowania jednostki penitencjarnej w rozumieniu zapewnienia bezpieczeństwa oraz realizacji celów wykonywania kary pozbawienia wolności i tymczasowego aresztowania, a także ochrony społeczeństwa przed sprawcami przestępstw, jest zapewnienie porządku i dyscypliny w zakładzie karnym czy areszcie śledczym[9]. Powinno się to odbywać z zachowaniem zasad określonych w art. 4 § 1 k.k.w. oraz w innych przepisach dotyczących traktowania osadzonych, zawartych np. w ustawie o SW. W art. 2 ust. 2 tej ustawy są wymienione zadania formacji, do których należą m.in.:

- prowadzenie oddziaływań penitencjarnych i resocjalizacyjnych wobec skazanych na karę pozbawienia wolności,
- wykonywanie tymczasowego aresztowania w sposób zabezpieczający prawidłowy tok postępowania karnego o przestępstwo lub przestępstwo skarbowe,
- zapewnienie skazanym i tymczasowo aresztowanym przestrzegania ich praw, a zwłaszcza humanitarnych warunków bytowych, poszanowania godności, opieki zdrowotnej i religijnej,
- humanitarne traktowanie osób pozbawionych wolności,
- ochrona społeczeństwa przed sprawcami przestępstw lub przestępstw skarbowych osadzonymi w zakładach karnych i aresztach śledczych,
- zapewnienie w zakładach karnych i aresztach śledczych porządku i bezpieczeństwa,
- prowadzenie Centralnej Bazy Danych Osób Pozbawionych Wolności.

W Polsce funkcjonuje 171 jednostek penitencjarnych, w tym: 64 zakłady karne, 39 aresztów śledczych oraz 68 oddziałów zewnętrznych zakładów karnych lub aresztów śledczych, z których część posiada tzw. oddziały

[7] Artykuł 68 i 208 k.k.w.

[8] Artykuł 72 § 1 i 2, 208 § 4 k.k.w.

[9] Artykuł 73 § 1 k.k.w.

aresztowe[10]. W k.k.w. wymieniono cztery rodzaje zakładów karnych dla skazanych[11]: dla młodocianych, odbywających karę po raz pierwszy, recydywistów penitencjarnych oraz odbywających karę aresztu wojskowego. Mogą one być one organizowane jako zakłady karne: zamknięte, półotwarte i otwarte[12]. Poszczególne typy zakładów różnią się (...) *w szczególności stopniem zabezpieczenia, izolacji skazanych oraz wynikającymi z tego ich obowiązkami i uprawnieniami w zakresie poruszania się w zakładzie i poza jego obrębem*[13].

Penitencjarna mapa Polski obrazuje lokalizacje zakładów karnych, aresztów śledczych oraz oddziałów zewnętrznych (rysunek 1):

Rysunek 1. Lokalizacja zakładów karnych, aresztów śledczych oraz oddziałów zewnętrznych w Polsce.

Źródło: dane pochodzące z Biura Ewidencji Centralnego Zarządu Służby Więziennej.

[10] Dane pochodzą z Biura Ewidencji Centralnego Zarządu Służby Więziennej.

[11] Artykuł 69 k.k.w.

[12] Artykuł 70 § 1 k.k.w.

[13] Artykuł 70 § 2 k.k.w.

Według stanu na 30 czerwca 2025 r. w polskich więzieniach przebywało 70 214 osób pozbawionych wolności, w tym: 61 409 skazanych, 7642 tymczasowo aresztowanych oraz 1163 ukaranych[14]. Zaludnienie, czyli liczba osadzonych przebywających w jednostkach penitencjarnych, na poziomie 70 000 osób to ok. 84% możliwości systemu. W populacji osadzonych, tj. skazanych, tymczasowo aresztowanych w polskich jednostkach penitencjarnych, zdecydowanie dominują mężczyźni – jest ich 66 465, tj. 94,6% ogółu. Kobiety stanowią ok. 5,4% tej populacji (3749).

Nowe rodzaje zagrożeń bezpieczeństwa państwa – działania hybrydowe

Od 2021 r. Polska jest szczególnie narażona na różnego rodzaju działania bezpośrednio godzące w bezpieczeństwo państwa i jego obywateli, a znaczna ich część przybiera charakter działań hybrydowych, czego przykładem stał się kryzys migracyjny. Dnia 2 września 2021 r. Prezydent RP na wniosek Rady Ministrów wprowadził 30-dniowy stan wyjątkowy na obszarze części województwa podlaskiego oraz części województwa lubelskiego[15]. W projekcie uchwały Rady Ministrów o skierowaniu do Prezydenta RP wniosku o wprowadzenie stanu wyjątkowego na tych obszarach czytamy, że: (...) *wyjątkowy charakter oraz nadzwyczajna skala presji migracyjnej na granicy polsko-białoruskiej mają swoje źródło w zamierzonych i zaplanowanych działaniach służb białoruskich, ukierunkowanych na destabilizację sytuacji na granicy z Polską oraz innymi państwami członkowskimi Unii Europejskiej, tj. Litwą i Łotwą. Przedmiotowe działania przybierają postać „wojny hybrydowej" prowadzonej przez białoruski reżim*[16].

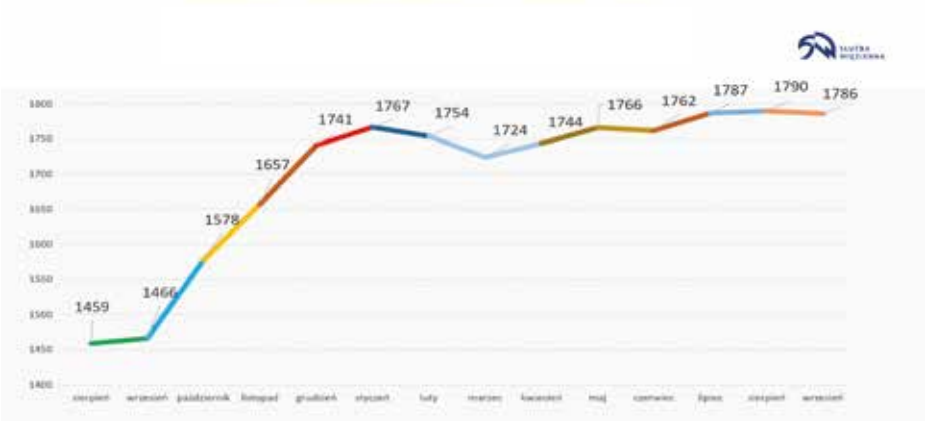
[14] CZSW BIS – statystyka miesięczna – czerwiec 2025. Dane statystyczne są dostępne na stronie: https://www.sw.gov.pl/strona/statystyka.

[15] *Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 2 września 2021 r. w sprawie wprowadzenia stanu wyjątkowego na obszarze części województwa podlaskiego oraz części województwa lubelskiego* (DzU z 2021 r. poz. 1612).

[16] *Projekt uchwały Rady Ministrów o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego na obszarze części województwa podlaskiego oraz części województwa lubelskiego*, Serwis Rzeczypospolitej Polskiej, 31 VIII 2021 r., https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-o-skierowaniu-do-prezydenta-rzeczypospolitej-polskiej-wniosku-o-wprowadzenie-stanu-wyjatkowego-na-obszarze-czesci-wojewodztwa-podlaskiego-oraz-czesci-wojewodztwa-lubelskiego [dostęp: 7 VIII 2025].

Naruszenia bezpieczeństwa polskiej granicy miały nowy charakter i polegały nie tylko na próbach nielegalnego przekroczenia granicy przez tysiące osób różnych narodowości, lecz także na konieczności fizycznej obrony przed grupami imigrantów, którzy niszczyli zabezpieczenia i atakowali funkcjonariuszy Straży Granicznej, Policji, żołnierzy. Skala tych naruszeń była wcześniej niespotykana, co odzwierciedlają dane statystyczne Straży Granicznej. Wystarczy wspomnieć, że o ile w 2020 r. odnotowano 129 przekroczeń granicy państwowej wbrew przepisom na odcinku z Białorusią, to w 2021 r. było ich już 39 697[17].

Kryzys migracyjny spowodował wzrost liczby przestępstw polegających na nielegalnym przekroczeniu granicy RP (art. 264 § 2 Kodeksu karnego, k.k.), pomocy w organizacji takiego procederu (art. 264 § 3 k.k.) oraz czerpaniu korzyści materialnych z tego tytułu (art. 264a § 1 k.k.). Efektem działania służb i prokuratury było zastosowanie wobec niektórych podejrzanych o popełnienie takich czynów środka zapobiegawczego w postaci tymczasowego aresztu. Okres od września do grudnia 2021 r. był czasem wzrostu liczby cudzoziemców przebywających w zakładach karnych i aresztach śledczych (wykres 1)[18].



Wykres 1. Cudzoziemcy w polskich jednostkach penitencjarnych w okresie sierpień 2021 r. – wrzesień 2022 r.

Źródło: dane pochodzące z Biura Ewidencji Centralnego Zarządu Służby Więziennej.

[17] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią w 2021 r.*, Straż Graniczna, 12 I 2022 r., https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [dostęp: 7 VIII 2025].

[18] Służba Więzienna – statystyka, https://www.sw.gov.pl/strona/Statystyka [dostęp: 12 VIII 2025].

Dalszy, nieznaczny wzrost liczby cudzoziemców w polskich więzieniach nastąpił po pełnoskalowym zaatakowaniu Ukrainy przez Rosję w lutym 2022 r. Należy podkreślić, że niektóre osoby zatrzymywane w tym czasie przez polskie służby były wcześniej poszukiwane czerwoną notą Interpolu w związku z podejrzeniem o przynależność do organizacji terrorystycznych w państwach pochodzenia oraz o prowadzenie takiej działalności. Ich obecność wymaga od funkcjonariuszy SW stałych działań o charakterze profilaktycznym, ukierunkowanych na rozpoznanie atmosfery oraz zachowań mogących stanowić zagrożenie bezpieczeństwa w zakładzie karnym. Jest to szczególnie ważne w odniesieniu do tymczasowo aresztowanych, którzy w krajach pochodzenia lub innych organizowali zamachy terrorystyczne lub należeli do Państwa Islamskiego. Ważnym aspektem pozostaje również konieczność przeciwdziałania demoralizacji oraz radykalizacji w więzieniu. Trzeba także pamiętać, że więźniowie lub byli więźniowie pozostają w zainteresowaniu rosyjskich służb wywiadowczych jako potencjalni „agenci jednorazowego użytku", wykorzystywani do przeprowadzania ataków hybrydowych. Raport Międzynarodowego Centrum ds. Zwalczania Terroryzmu (The International Centre for Counter-Terrorism, ICCT) i GLOBSEC wskazuje, że od 2022 r. na terenie Europy doszło do 110 ataków o charakterze hybrydowym powiązanych z Rosją. Służby zidentyfikowały 131 osób mieszkających w Europie i zaangażowanych w takie działania, z których co najmniej 35 miało wcześniej kontakt z przestępczością. Jednocześnie autorzy raportu podkreślają, że więzienia zarówno w Rosji, jak i za granicą pozostają miejscem rekrutacji przestępców, najczęściej młodych mężczyzn (ok. 30 lat), pozostających w trudnej sytuacji materialnej do przeprowadzania aktów sabotażu[19].

Sytuacja na granicy polsko-białoruskiej wciąż jest bardzo trudna, o czym świadczą informacje prezentowane przez Podlaski Oddział Straży Granicznej[20]. Tylko w okresie lipiec – sierpień 2025 r. niemal każdej doby dochodziło do licznych prób nielegalnego przekraczania granicy. Przykładowo, 1 lipca – było 100 prób; 4–6 lipca – 170; 10 lipca – 100; 16 lipca – 210; 18–20 lipca – 340; 25 lipca – 170; 6–7 sierpnia – 280; 12 sierpnia – 170; 13 sierpnia – 130. Do 14 sierpnia 2025 r. Podlaski Oddział Straży Granicznej

[19] *Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe,* https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf, s. 24–31 [dostęp: 10 X 2025].

[20] Straż Graniczna – aktualności, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/.

odnotował 19 500 prób nielegalnego przekroczenia granicy na odcinku polsko-białoruskim[21].

Wspólną cechą większości tego typu zdarzeń jest ich agresywny charakter. Cudzoziemcy, aby dostać się do Polski, często niszczą barierę techniczną za pomocą różnych narzędzi, wykonują podkopy[22], rzucają kamieniami, izolatorami energetycznymi, konarami i kolcami z drutu kolczastego, szklanymi butelkami wypełnionymi piaskiem, kijami zakończonymi ostrym narzędziem w strzegących bezpieczeństwa granicy. W ten sposób niszczą graniczną infrastrukturę techniczną, samochody Straży Granicznej, a co najważniejsze, stwarzają realne i bezpośrednie zagrożenie dla zdrowia i życia funkcjonariuszy i żołnierzy. Tragicznym skutkiem takich działań było zdarzenie z 28 maja 2024 r. kiedy to szer. Mateusz Sitek podczas pełnienia służby został ugodzony nożem przez cudzoziemca próbującego sforsować zabezpieczenia graniczne i po kilku dniach, mimo starań lekarzy, zmarł[23]. Polskie służby szybko ustaliły wizerunek sprawcy i jego pochodzenie. Jednak jego ujęcie nie było możliwe także dlatego, że strona białoruska mimo wystosowanej noty protestacyjnej nie podjęła faktycznej współpracy.

Pomimo wysiłków służb niektórym cudzoziemcom udaje się nielegalnie przekroczyć granicę i są zatrzymywani już na terytorium RP. Podlaski Oddział Straży Granicznej informuje o zatrzymaniach obywateli m.in. Sudanu, Jemenu, Kamerunu, Etiopii, Afganistanu, Indii, Erytrei, Somalii, Bangladeszu i Egiptu. Zatrzymywane są także osoby pomagające w nielegalnym przekroczeniu granicy i organizujące je, wśród których są Ukraińcy, Białorusini, Łotysze, Polacy. Tylko od 1 stycznia do 7 lipca 2025 r. funkcjonariusze Podlaskiego Oddziału Straży Granicznej zatrzymali 95 organizatorów nielegalnego przekroczenia polsko-białoruskiej granicy oraz pomocników w tym przedsięwzięciu[24], z których część zapewne usłyszała zarzuty karne

[21] M. Bura, *Na polsko-białoruskiej granicy*, Podlaski Oddział Straży Granicznej, 14 VIII 2025 r., https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/67321,Na-polsko-bialoruskiej-granicy.html [dostęp: 18 VIII 2025].

[22] M. Bura, *Podkopem (NIE) do Polski*, Podlaski Oddział Straży Granicznej, 10 VII 2025 r., https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/66897,Podkopem-NIE-do-Polski.html [dostęp: 18 VIII 2025].

[23] *Ostatnie pożegnanie śp. szer. Mateusza Sitka*, 1. Warszawska Brygada Pancerna, https://www.wojsko-polskie.pl/1bpanc/articles/aktualnosci-w/ostatnie-pozegnanie-sp-szer-mateusza-sitka [dostęp: 18 VIII 2025].

[24] K. Zdanowicz, *W bagażniku na zachód Europy*, Podlaski Oddział Straży Granicznej, 8 VII 2025 r., https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/66859,W-bagazniku-na-zachod-Europy.html [dostęp: 18 VIII 2025].

skutkujące zastosowaniem aresztu tymczasowego. Warto wspomnieć o trudnościach, z jakimi zmagają się w takich sytuacjach funkcjonariusze SW, takich jak problem z porozumiewaniem się wynikający z nieznajomości języka angielskiego przez aresztowanych oraz ich specyfika kulturowa i religijna.

Innym przykładem zdarzeń niepokojących wielu polskich obywateli są pożary. W przypadku gdy powstają one w wyniku działań człowieka, najprawdopodobniej dochodzi do przestępstwa[25], które może być umyślne, tzn. sprawca chce podjąć i podejmuje działania zabronione albo przewiduje możliwość ich podjęcia i godzi się na to, albo nieumyślne, gdy sprawca nie ma zamiaru popełnić czynu zabronionego, ale dochodzi do niego wskutek nieostrożności sprawcy[26].

Jeszcze inne okoliczności zachodzą, gdy:

a) sprawca lub sprawcy działając, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, dokonują dywersji, sabotażu lub dopuszczają się przestępstwa o charakterze terrorystycznym,
b) sprawca lub sprawcy, działając w zorganizowanej grupie o charakterze zbrojnym, popełniają przestępstwa o charakterze terrorystycznym[27].

Takim zaplanowanym działaniem był pożar z 12 maja 2024 r. w Centrum Handlowym przy ulicy Marywilskiej 44 w Warszawie. Jak wynika z komunikatu Prokuratury Krajowej z 12 maja 2025 r., podpalenie było wynikiem zlecenia wywiadu Federacji Rosyjskiej. W śledztwie ustalono, że obywatel Ukrainy otrzymał od innego obywatela Ukrainy przebywającego w Rosji polecenie nagrania pożaru oraz akcji ratunkowej. W poleceniu była wskazana godzina, o której wybuchnie pożar[28].

Ponadto ustalono, że dwóch obywateli Ukrainy zaangażowanych w wywołanie i dokumentowanie pożaru w CH Marywilska 44 wspólnie z dwoma innymi osobami zaplanowało i przeprowadziło za pomocą urządzeń zapalających w nocy z 8 na 9 maja 2024 r. pożar sklepu wielkopowierzchniowego IKEA w Wilnie.

[25] Artykuł 163 § 1 pkt 1 k.k.

[26] Artykuł 9 k.k.

[27] Artykuł 258 § 2 k.k.

[28] *Zarzuty w związku z pożarem hali przy ul. Marywilskiej 44*, Prokuratura Krajowa, 12 V 2025 r., https://www.gov.pl/web/prokuratura-krajowa/zarzuty-m44 [dostęp: 25 VIII 2025].

W ramach tego samego śledztwa są badane okoliczności pożaru marketu budowlanego w Warszawie, do którego doszło 12 kwietnia 2024 r. Z ustaleń prokuratury wynika, że zdarzenie stanowiło skutek umyślnego działania, a sprawcą był obywatel Białorusi. 31 stycznia 2024 r. funkcjonariusze ABW zatrzymali we Wrocławiu obywatela Ukrainy. Działał on w zorganizowanej grupie przestępczej i na zlecenie rosyjskich służb wywiadowczych przygotowywał się do podjęcia działań dywersyjnych i sabotażowych, polegających na podpaleniu obiektów na terenie Wrocławia, które znajdowały się w bliskiej odległości od elementów infrastruktury o znaczeniu strategicznym[29]. Jak się okazało, 51-letni Ukrainiec (...) *za 4 tysiące dolarów na zlecenie rosyjskich służb miał przygotowywać się do podpalenia centrum farb przy ul. Kwidzyńskiej na Kowalach we Wrocławiu. Działa ono przy fabryce farb należącej do amerykańskiego giganta w tej dziedzinie, jednej z 500 największych amerykańskich firm pod względem przychodów*[30]. Natomiast 23 maja 2024 r. funkcjonariusze ABW zatrzymali Polaka i dwóch Białorusinów podejrzewanych o dokonywanie podpaleń obiektów w różnych częściach kraju i działających na zlecenie rosyjskich służb specjalnych[31].

O skali zagrożenia związanego z działaniami hybrydowymi świadczą również informacje o zatrzymywaniu na terytorium RP osób prowadzących działalnością szpiegowską, sabotażową, terrorystyczną lub inną godzącą bezpośrednio w bezpieczeństwo Polski, prowadzoną na zlecenie obcych służb wywiadowczych. Analizując informacje przekazywane przez ABW w okresie od 1 stycznia 2024 r. do 30 czerwca 2025 r., można znaleźć wiele przykładów świadczących o skuteczności polskich służb w wykrywaniu tego rodzaju zagrożeń. Oto niektóre z nich[32]:

– 9 września 2024 r. – zatrzymanie obywatelki Białorusi pod zarzutem szpiegostwa na rzecz białoruskiej służby specjalnej – Komitetu Bezpieczeństwa Państwowego Republiki Białorusi,

[29] *Funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego zatrzymali mężczyznę działającego na zlecenie rosyjskich służb wywiadowczych*, Serwis Rzeczypospolitej Polskiej, 15 II 2024 r., https://www.gov.pl/web/sluzby-specjalne/funkcjonariusze-agencji-bezpieczenstwa-wewnetrznego-zatrzymali-mezczyzne-dzialajacego-na-zlecenie-rosyjskich-sluzb-wywiadowczych [dostęp: 25 VIII 2025].

[30] *Ukrainiec, który na zlecenie Rosji miał wywołać pożar we Wrocławiu idzie do więzienia. Sąd: „motał i kłamał"*, tuWroclaw.com, 21 II 2025 r., https://tuwroclaw.com/artykul/ukrainiec-ktory-na-n1507326 [dostęp: 25 VIII 2025].

[31] *Komunikat*, ABW, 29 V 2024 r., https://www.abw.gov.pl/pl/informacje/2501,Komunikat.html [dostęp: 25 VIII 2025].

[32] ABW – informacje, https://www.abw.gov.pl/pl/informacje.

- 6 lutego 2024 r. – skierowanie do sądu aktu oskarżenia przeciwko obywatelowi RP podejrzanego o szpiegostwo na rzecz rosyjskich służb specjalnych,
- 19 kwietnia 2024 r. – zatrzymanie obywatela RP podejrzanego o zgłoszenie gotowości do współpracy z rosyjskimi służbami specjalnymi,
- 16 maja 2024 r. – skazanie przez Sąd Okręgowy w Świdnicy obywatela RP na karę 2 lat pozbawienia wolności za udział w zorganizowanej grupie przestępczej o charakterze terrorystycznym oraz planowanie przeprowadzenia zamachu terrorystycznego z wykorzystaniem materiałów wybuchowych – w celu poważnego zastraszenia wielu osób i sprowadzenia zdarzenia zagrażającego życiu lub zdrowiu wielu osób albo mieniu wielkich rozmiarów,
- 13 listopada 2024 r. – zatrzymanie obywatela Białorusi działającego na zlecenie obcych służb specjalnych, podejrzewanego o usiłowanie dokonania podpalenia obiektu zlokalizowanego w Gdańsku,
- 1 kwietnia 2025 r. – zatrzymanie obywatela Ukrainy działającego na rzecz rosyjskiego wywiadu.

Częściowe podsumowanie działań ABW związanych z wykrywaniem zagrożeń wynikających z działań hybrydowych inicjowanych i koordynowanych przez rosyjskie służby specjalne i przeciwdziałaniem tym zagrożeniom, przedstawienie metod działania oraz sposobów rekrutacji do zadań dywersyjnych znajduje się w komunikacie z 25 października 2024 r.[33] Interesujących informacji o niekonwencjonalnych sposobach werbowania osób do prowadzenia działalności o charakterze szpiegowskim i sabotażowym dostarcza także reportaż pt. *Rabota w Polsze*[34].

Opisane działania hybrydowe inspirowane przez obce służby wywiadowcze, najczęściej rosyjskie i białoruskie, mają służyć destabilizacji organów państwa, wywołaniu wśród obywateli poczucia zagrożenia i polaryzacji społeczeństwa, podsycaniu konfliktów narodowościowych, osłabieniu wspólnoty narodowej i kwestionowaniu międzynarodowych sojuszy. Do przeprowadzania ataków często są wykorzystywane przypadkowe osoby działające z chęci zysku. Przedstawione zdarzenia mają wprost przestępczy

[33] *Komunikat dotyczący działalności dywersyjnej FR*, ABW, 25 X 2024 r., https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html [dostęp: 25 VIII 2025].

[34] *Jak działają rosyjscy szpiedzy w Polsce?„Rabota w Polsze" – reportaż Piotra Świerczka*, YouTube, 12 IX 2025 r., https://www.youtube.com/watch?v=44O7Y_yMXGk [dostęp: 12 IX 2025].

charakter, niosą ze sobą bezpośrednie zagrożenie życia i zdrowia obywateli, godzą w bezpieczeństwo i interesy RP oraz są zagrożone wysoką karą, najczęściej na czas nie krótszy niż 5 lat albo karą dożywotniego pozbawienia wolności.

Szpiedzy, sabotażyści i terroryści w polskich więzieniach – dane statystyczne

W każdym przypadku, gdy sąd stosuje najsurowszy środek zapobiegawczy w postaci tymczasowego aresztowania, podejrzani o prowadzenie działalności szpiegowskiej, dywersyjnej lub o charakterze terrorystycznym są umieszczani w aresztach śledczych lub wyznaczonych oddziałach tzw. aresztowych zakładów karnych. Kwalifikacją prawną stosowaną najczęściej wobec tymczasowo aresztowanych, a później skazanych, jest podejrzenie popełnienia przestępstw określonych w art. 130 § 19 k.k. (udział w działalności na rzecz obcego wywiadu) oraz art. 258 § 2 k.k. (udział w zorganizowanej grupie o charakterze zbrojnym mającej na celu popełnienie przestępstwa lub przestępstwa skarbowego o charakterze terrorystycznym). Często, uwzględniając charakter czynów, kwalifikacja prawna łącznie obejmuje wskazane artykuły, a także art. 255a § 2 k.k. (udział w szkoleniu mogącym umożliwić popełnienie przestępstwa o charakterze terrorystycznym lub samodzielnie zapoznawanie się z treściami, które mogą umożliwić popełnienie takiego przestępstwa).

Zgodnie z informacjami statystycznymi przekazanymi autorowi przez Centralny Zarząd Służby Więziennej według stanu na 30 czerwca 2025 r. w polskich zakładach karnych i aresztach śledczych w związku z popełnieniem czynów określonych w art. 130 § 1–9 k.k. przebywało ogółem 34 osadzonych. Spośród wskazanej grupy 18 osób ma status skazanych i 16 – tymczasowo aresztowanych. Wśród skazanych najwięcej było obywateli Ukrainy – 10, a następnie Białorusi – 4, Rosji – 3, Kanady – 1. Wśród tymczasowo aresztowanych także dominowali obywatele Ukrainy – 4, a następnie Polski – 4, Rosji – 4 (w tym 1 kobieta), Białorusi – 3, Litwy – 1.

W badanej grupie zarzut popełnienia przestępstwa szpiegostwa określony w art. 130 § 1 k.k. został przedstawiony łącznie 23 osobom, z których 18 miało status skazanych, a 5 – tymczasowo aresztowanych. Wśród skazanych dominowali Ukraińcy – 10, następnie Białorusini – 4, Rosjanie – 3

i 1 obywatel Kanady. Wśród tymczasowo aresztowanych zarzuty usłyszało 3 Ukraińców, 1 Polak i 1 Rosjanin.

Zarzut popełnienia przestępstwa szpiegostwa określony w art. 130 § 2 k.k. został przedstawiony 6 osobom, z których każda ma status tymczasowo aresztowanej, w tym 2 Polaków, 2 osoby z Rosji (w tym kobieta) oraz 1 osoba z Białorusi i 1 z Litwy. Zarzut zgłoszenia gotowości do działania na rzecz obcego wywiadu przeciwko RP określony w art. 130 § 3 usłyszało 2 tymczasowo aresztowanych. Są to obywatele Polski i Białorusi. Natomiast zarzut podejrzenia popełnienia przestępstwa określonego w art. 130 § 7 polegającego na braniu udziału w działalności obcego wywiadu albo działania na jego rzecz, dokonywaniu dywersji, sabotażu lub dopuszczenia się przestępstwa o charakterze terrorystycznym usłyszało 2 Białorusinów, 1 Rosjanin i 1 Ukrainiec.

Z udostępnionych informacji wynika także, że w areszcie śledczym jako tymczasowo aresztowany przebywa obywatel Ukrainy, któremu postawiono zarzut z art. 255a § 2 k.k.

Wszyscy tymczasowo aresztowani i skazani przebywają w aresztach śledczych i zakładach karnych typu zamkniętego[35], czyli jednostkach penitencjarnych, w których istnieje wysoki poziom zabezpieczeń techniczno-ochronnych. Wspomniana wcześniej grupa 35 osób skazanych i tymczasowo aresztowanych w związku z czynami określonymi w art. 130 § 1–9 oraz art. 255a § 2 k.k. wymaga od funkcjonariuszy SW zwiększonego nadzoru i szczególnie starannego planowania oddziaływań penitencjarnych oraz przedsięwzięć ochronnych, z uwzględnieniem wymogów porządku i dyscypliny będących podstawą bezpieczeństwa zakładu karnego czy aresztu śledczego. Przemawia za tym charakter przestępstw, okoliczności i motywacje ich popełniania, zagrożenie wysoką karą, cechy osobowości osadzonych diagnozowane przez personel więzienny już w początkowym okresie izolacji oraz posiadane przynajmniej w części przypadków umiejętności mogące stanowić zagrożenie dla bezpieczeństwa jednostki penitencjarnej.

Należy podkreślić, że 13 osób z tej grupy, tj. 37%, zostało zakwalifikowanych do kategorii osób stwarzających poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu. W związku z tym są one kierowane do odpowiednich oddziałów dla tzw. więźniów niebezpiecznych, w których zapewnia się wzmożoną ochronę społeczeństwa i bezpieczeństwo zakładu karnego. Oznacza to, że administracja więzienna uznała

[35] Artykuł 88 § 3 k.k.w.

te osoby za stwarzające poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu w rozumieniu przepisów art. 88a § 1 k.k.w. Zakwalifikowanie do tej kategorii wiąże się z wieloma ograniczeniami i najwyższym poziomem reżimu więziennego, rozumianego jako zakres przyznanych uprawnień i przede wszystkim nałożonych obowiązków przewidzianych w polskim prawie[36]. W tym samym czasie we wszystkich oddziałach dla osadzonych stwarzających poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu przebywało łącznie 141 skazanych i tymczasowo aresztowanych.

Według stanu na 31 lipca 2025 r. w związku z popełnieniem przestępstwa określonego w art. 258 § 2 z wyłączeniem czynów określonych w art. 130 k.k. we wszystkich jednostkach penitencjarnych przebywało 239 osób. W tej grupie znajduje się 185 skazanych, w tym 4 kobiety, oraz 54 tymczasowo aresztowanych, w tym 3 kobiety. Zdecydowana większość pozostaje w zakładach karnych typu zamkniętego – 216, w tym 7 osób zostało zakwalifikowanych jako tzw. więźniowie niebezpieczni.

W grupie skazanych zdecydowanie dominują Polacy – 181, w tym 3 kobiety. Są wśród nich również obywatele Łotwy – 2, Ukrainy – 1, Armenii – 1 (kobieta). Także wśród tymczasowo aresztowanych większość stanowią Polacy – 42, w tym 3 kobiety. Następnie są to obywatele Ukrainy – 7, Litwy – 2, Czech – 1, Armenii – 1, Tadżykistanu – 1. W analizowanej grupie ogółem dominują Polacy – 223 osoby. Obywateli Ukrainy jest 8, Litwy – 2, Łotwy – 2, Armenii – 2, Czech – 1, Tadżykistanu – 1.

Ponieważ przestępstwo określone w art. 258 § 2 k.k. może mieć charakter zarówno typowo kryminalny, jak i terrorystyczny, trudno jest jednoznacznie wskazać na podstawie danych statystycznych, ilu skazanych i tymczasowo aresztowanych spośród przebywających w jednostkach penitencjarnych dopuściło się czynów o charakterze terrorystycznym. Wyodrębnienie tej kategorii wymaga przeprowadzenia dodatkowych analiz.

Już teraz można prognozować, że licząca 35 osób grupa szpiegów, dywersantów i sabotażystów o różnym statusie prawnym się zwiększy, ponieważ wiele śledztw ma – jak to określają prokuratorzy – charakter rozwojowy, a aktywność obcych wywiadów jest nadal wysoka, mimo sukcesów polskich służb w wykrywaniu tego typu zagrożeń. Przykładem jest informacja zamieszczona 1 sierpnia 2025 r. na platformie X przez ministra koordynatora służb specjalnych o zatrzymaniu przez ABW obywatela

[36] Artykuł 88b i 88c k.k.w.

jednego z państw azjatyckich, który będąc kadrowym oficerem wywiadu wojskowego, (...) *prowadził działalność wywiadowczą godzącą w bezpieczeństwo RP i wojskowych struktur sojuszniczych. Prokuratura Krajowa przedstawiła mu zarzuty i 1 sierpnia 2025 r. podejrzany został decyzją sądu aresztowany na 3 miesiące*[37].

Dowodzi tego także komunikat ABW z 14 sierpnia 2025 r. o zatrzymaniu 17-letniego obywatela Ukrainy, któremu prokuratura postawiła zarzuty popełnienia wielu przestępstw, w tym określonych w art. 130 § 7 k.k. (działalność sabotażowa na zlecenie obcej służby specjalnej), a sąd zastosował wobec niego tymczasowe aresztowanie na 3 miesiące[38].

Szczególnie ważna z perspektywy funkcjonariuszy SW jest jak największa wiedza o osobie doprowadzonej do aresztu, w tym dotycząca faktycznej tożsamości oraz motywacji do popełnienia przestępstw określonych w art. 130 § 1–9 czy art. 255a § 2 k.k. Działania przestępcze mogą mieć różne podłoże, tzn. być bezpośrednio konsekwencją wykonywanej profesji szpiega, agenta, lub np. ekonomiczne, wynikające z szantażu, narodowościowe, religijne. Wiedza w tym zakresie stanowi dla funkcjonariuszy jedną z przesłanek planowania przedsięwzięć penitencjarno-ochronnych związanych np. z podjęciem decyzji o osadzeniu w konkretnej jednostce penitencjarnej, oddziale, celi pojedynczej lub wieloosobowej, doboru współosadzonych czy objęcia monitoringiem[39]. Równie ważne, zwłaszcza w perspektywie bezpieczeństwa zakładu karnego czy aresztu śledczego, są informacje dotyczące odbytych szkoleń czy posiadanych umiejętności ułatwiających prowadzenie działalności szpiegowskiej czy sabotażowej. Mogą one bowiem być wykorzystywane w czasie pobytu w izolacji np. w celu podjęcia próby ucieczki lub wywołania zagrożenia. Podobne znaczenie mają informacje o osobach, z którymi skazany czy tymczasowo aresztowany zamierza utrzymywać lub utrzymuje kontakt telefoniczny, korespondencyjny, w formie widzeń na terenie więzienia czy udzielanego wsparcia materialnego. Pozyskiwanie rzetelnej wiedzy z zachowaniem wszelkich procedur bezpieczeństwa odbywa się w drodze współpracy SW z innymi

[37] Tomasz Siemoniak, (@TomaszSiemoniak) wpis na portalu X, 1 VIII 2025 r., https://x.com/TomaszSiemoniak/status/1951279798526890013?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E195 [dostęp: 25 VIII 2025].

[38] *Komunikat ABW ws. zatrzymania obywatela Ukrainy*, ABW, 14 VIII 2025 r., https://www.abw.gov.pl/pl/informacje/2668,Komunikat-ABW-ws-zatrzymania-obywatela-Ukrainy.html [dostęp: 25 VIII 2025].

[39] Artykuł 73a k.k.w.

organami, w szczególności prokuraturą, właściwymi służbami mundurowymi oraz sądem.

Podsumowanie

Wybuch wojny w Ukrainie na początku 2022 r. i towarzysząca jej ogromna fala migracyjna stały się podstawą do zastanowienia się nad stanem przygotowań państwa do funkcjonowania w warunkach ekstremalnych. W SW także przeprowadzono taką analizę, dokonując przeglądu obowiązujących w tym zakresie zadań i przepisów obronnych, oceny ich adekwatności, określenia posiadanych zasobów infrastrukturalnych oraz stanu przygotowania formacji. Na podstawie wyników audytu podjęto decyzje związane m.in. z zaopatrzeniem w paliwa, środki łączności, amunicję, żywność oraz przygotowaniem planistycznym zwiększającym zdolności obronne. Już w marcu 2022 r. nawiązano współpracę z Wojskami Obrony Terytorialnej, dzięki czemu w 2022 r. i 2023 r. rozszerzono proces szkolenia funkcjonariuszy SW o zagadnienia typowo wojskowe. Szkolenia te były realizowane także w obiektach podległych Ministerstwu Obrony Narodowej. Podstawą formalną tych działań jest *Porozumienie o współpracy pomiędzy Dowództwem Wojsk Obrony Terytorialnej i Centralnym Zarządem Służby Więziennej* zawarte 21 grudnia 2022 r.

Problematyka zadań obronnych i szerzej roli SW w warunkach stanu wojny pozostaje nie tylko interesującym, lecz przede wszystkim bardzo praktycznym obszarem badań naukowych. Jednocześnie w ocenie autora, ze względu na trwającą wojnę w Ukrainie, imperialną politykę Rosji, działania mające cechy wojny hybrydowej prowadzone na terytorium naszego kraju, a także opinie krajowych i międzynarodowych ekspertów w dziedzinie bezpieczeństwa, niezwykle ważne jest kontynuowanie przez kierownictwo SW prac planistycznych, organizacyjnych, logistycznych i szkoleniowych, pozwalających jak najlepiej przygotować formację na czas kryzysu. Inspiracją w tym zakresie mogą być doświadczenia Państwowej Służby Więziennej Ukrainy (ukr. Державна кримінально-виконавча служба України), która działając w warunkach wojny i realizując działania charakterystyczne dla formacji więziennych, podejmuje wiele dodatkowych zadań, polegających na wsparciu lokalnych społeczności i sił obronnych, zabezpieczeniu pobytu jeńców wojennych i przeprowadzaniu ich wymiany, organizacji systemu rekrutacji do służby wojskowej wśród

wyselekcjonowanych grup skazanych czy usuwaniu skutków ataków rakietowych i dronowych na obiekty penitencjarne.

Współpraca SW z innymi służbami mundurowymi jest szczególnie ważna dla zapewnienia porządku i bezpieczeństwa w zakładach karnych i aresztach śledczych oraz ochrony społeczeństwa przed sprawcami przestępstw pozbawionymi wolności. Z powodu zagrożeń związanych z działaniami o charakterze hybrydowym nowego znaczenia nabiera współpraca z Policją, ABW, Strażą Graniczną oraz Państwową Strażą Pożarną. Za istotne należy uznać podejmowanie, kontynuowanie i intensyfikowanie następujących przedsięwzięć:

1) systematyczne przeprowadzanie ćwiczeń doskonalących współpracę funkcjonariuszy – opartych na scenariuszach uwzględniających realne zagrożenia, także hybrydowe – w zakresie dowodzenia w warunkach kryzysowych, przekazywania informacji, kompatybilności systemów łączności, organizowania ewakuacji,
2) uwzględnianie w przeprowadzanych ćwiczeniach znaczenia komponentu medycznego, tj. udzielania pierwszej pomocy, z elementami medycyny pola walki,
3) systematyczne organizowanie szkoleń, warsztatów z udziałem ekspertów, także zdalnym, poświęconych omówieniu specyfiki określonych zagrożeń oraz możliwości zastosowania procedur profilaktycznych, dotyczących np. prewencji terrorystycznej, radykalizacji, zagrożeń hybrydowych, odmienności kulturowych,
4) stworzenie kanałów szybkiego przekazywania informacji o zagrożeniach i sytuacjach kryzysowych przez m.in. wyznaczenie funkcjonariuszy do współpracy, określenie środków łączności, także alternatywnych, oraz zakresu informacji możliwych do przekazania, z uwzględnieniem przepisów obowiązujących w tym obszarze, a w przypadku zdiagnozowania potrzeby zmiany regulacji prawnych – inicjowanie tego procesu,
5) dokonywanie okresowych ewaluacji współpracy oraz wykorzystywanie w praktyce wyciągniętych wniosków,
6) w razie potrzeby, dokonywanie aktualizacji lub zawieranie nowych dwustronnych porozumień o współpracy, uwzględniających aktualną sytuację i zdiagnozowane potrzeby oraz określających m.in. ich zakres, formę oraz osoby odpowiedzialne,

7) podejmowanie wspólnych projektów naukowo-badawczych i innych, finansowanych również ze źródeł zewnętrznych, zwiększających zdolności formacji do działania w warunkach zagrożeń, także hybrydowych.

W kontekście zapewnienia w zakładach karnych i aresztach śledczych porządku i bezpieczeństwa oraz ochrony społeczeństwa przed sprawcami przestępstw osadzonymi w jednostkach penitencjarnych ważne wydaje się także skonstruowanie formalnych procedur w odniesieniu do osadzonych w związku z popełnieniem przestępstw określonych w art. 130 § 1–9, art. 258 § 2 oraz art. 255a § 2 k.k. Procedury te dotyczyłyby m.in.:

- sposobów monitorowania sytuacji formalno-prawnej i osobistej,
- prowadzenia czynności profilaktycznych, oddziaływań penitencjarnych, w tym profilaktyki radykalizacji,
- systemu pozyskiwania i przekazywania informacji o osobach oraz współpracy w tym zakresie z innymi formacjami i instytucjami, w tym wyznaczenia funkcjonariuszy odpowiedzialnych za realizację tego procesu w ramach struktury SW.

Za podjęciem takich działań przemawia prognozowany przez ekspertów wzrost liczby zdarzeń o charakterze hybrydowym, związany głównie z aktywnością rosyjskich i białoruskich służb wywiadowczych. Należy ponadto uwzględnić poważne zagrożenie dla społeczeństwa oraz dla bezpieczeństwa zakładu karnego czy aresztu śledczego, wynikające z obecności w nich sprawców takich przestępstw. Argumentów dostarcza także wspomniany raport ICCT i GLOBSEC, wskazujący więzienia jako potencjalne miejsca rekrutacji przestępców do przeprowadzania ataków hybrydowych. Racjonalny jest również postulat kontynuowania prac planistycznych, organizacyjnych i szkoleniowych oraz tworzenia algorytmów postępowania uwzględniających skalę i charakter zagrożeń. Ważne są też obowiązki wynikające z zapisów *Zarządzenia Ministra Sprawiedliwości z dnia 5 marca 2024 r. w sprawie organizacji wykonywania zadań w ramach obowiązku obrony* w celu wzmocnienia zdolności obronnych formacji. Wymaga to ścisłej współpracy kierownictwa SW z Ministerstwem Sprawiedliwości i Ministerstwem Obrony Narodowej.

Gen. w st. spocz. Andrzej Leńczuk

Były zastępca Dyrektora Generalnego Służby Więziennej odpowiedzialny za bezpieczeństwo jednostek penitencjarnych oraz realizację działań zwiększających zdolności obronne formacji. Absolwent studiów podyplomowych i kursów specjalistycznych z zakresu bezpieczeństwa, dowodzenia, resocjalizacji i radykalizacji, organizowanych przez Akademię Obrony Narodowej (obecnie Akademia Sztuki Wojennej), Uniwersytet im. Adama Mickiewicza w Poznaniu, Agencję Bezpieczeństwa Wewnętrznego.

Kontakt: and.lenczuk@gmail.com

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 255–269

https://doi.org/10.4467/27204383TER.25.053.23040

Varia

Od phishingu po sabotaż – ewolucja cyberzagrożeń wobec Polski. Wnioski z raportu CSIRT GOV za 2024 rok

Monika Stodolnik
Autorka niezależna
https://orcid.org/0009-0000-5319-7968

Cyberprzestrzeń stanowiąca dziś arenę rywalizacji międzynarodowej podlega dynamicznym przemianom, a ostatnie lata pokazały jej znaczenie w kontekście państwowych działań niemilitarnych. Umożliwia ona prowadzenie operacji o charakterze wywiadowczym, sabotażowym, dezinformacyjnym, a także operacji wpływu. W tej rzeczywistości cyberbezpieczeństwo powinno być integralnym elementem odporności państwa – obok bezpieczeństwa militarnego, energetycznego czy ekonomicznego.

Polska jako członek wspólnot międzynarodowych, a przede wszystkim jako podmiot aktywnie wspierający Ukrainę w obliczu agresji Federacji Rosyjskiej, znajduje się w grupie państw szczególnie narażonych na cyberataki. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP za rok 2024*, opracowany przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV działający w strukturach Agencji Bezpieczeństwa Wewnętrznego, stanowi cenne źródło wiedzy o aktualnych trendach, wektorach ataków oraz poziomie przygotowania administracji publicznej i operatorów infrastruktury krytycznej.

Analiza raportu przedstawiona w artykule pozwala na sformułowanie wniosków dotyczących nie tylko technicznych aspektów ataków, lecz także zagrożeń dla instytucji i społeczeństwa związanych ze współczesnymi zjawiskami w cyberprzestrzeni.

Rola CSIRT GOV w krajowym systemie cyberbezpieczeństwa

Zespół CSIRT GOV pełni funkcję jednego z trzech krajowych zespołów powołanych do życia ustawą o krajowym systemie cyberbezpieczeństwa (dalej: ustawa o KSC)[1], odpowiedzialnych za rozpoznawanie i wykrywanie zagrożeń godzących w systemy administracji publicznej oraz infrastruktury krytycznej i zapobieganie im. CSIRT GOV realizuje zadania nałożone zarówno ustawą o KSC, jak i ustawą o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[2]. Łączy tym samym kompetencje techniczno-operacyjne i analityczne, odpowiadając za monitorowanie cyberprzestrzeni Rzeczypospolitej Polskiej, reagowanie na incydenty i koordynowanie działań w zakresie jej ochrony.

CSIRT GOV jest elementem operacyjnym krajowego systemu cyberbezpieczeństwa i bezpośrednio wspiera realizację zadań państwa w obszarze ochrony informacji, przeciwdziałania zagrożeniom cybernetycznym, będącym główną częścią zagrożeń hybrydowych, oraz zapewnienia ciągłości funkcjonowania infrastruktury krytycznej. Jego umiejscowienie w strukturze ABW pozwala łączyć bieżącą analizę techniczną incydentów z oceną ich szerszego kontekstu, w tym wpływu na bezpieczeństwo narodowe, z uwzględnieniem perspektywy kontrwywiadowczej. Ocena ta obejmuje również aspekt prewencji – dla administracji państwowej i operatorów infrastruktury krytycznej.

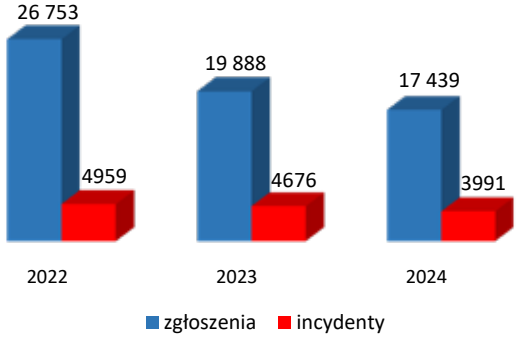
[1] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (t.j. DzU z 2024 r. poz. 1077, ze zm.).

[2] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j. DzU z 2025 r. poz. 902, ze zm.).

Kontekst cyberbezpieczeństwa w 2024 roku

Przez cały rok 2024 obowiązywał podwyższony stopień alarmowy CRP (w styczniu i lutym był to CHARLIE-CRP, a od marca – BRAVO-CRP[3]). Wiązało się to z utrzymywaniem stałej gotowości do reagowania na potencjalne działania o charakterze terrorystycznym, zgodnie z ustawą o działaniach antyterrorystycznych[4]. W szerszym ujęciu oznaczało to stałą gotowość do reagowania na potencjalne incydenty o charakterze hybrydowym i cyberwywiadowczym, ze względu na wspólne wektory ataków wykorzystywane we wszystkich tych przypadkach.

W 2024 r. CSIRT GOV zarejestrował 17 439 zgłoszeń o potencjalnych incydentach, z czego 3991 uznano za faktyczne naruszenia bezpieczeństwa systemów teleinformatycznych (rysunek 1)[5]. Chociaż te liczby wskazują na spadek względem roku 2023, to autorzy raportu zwracają uwagę, że nie wynika to ze zmniejszenia liczby zagrożeń, lecz z poprawy kompetencji i świadomości użytkowników oraz z wdrażania w instytucjach skuteczniejszych mechanizmów ochrony[6].



Rysunek 1. Liczba zgłoszeń i incydentów zarejestrowanych przez CSIRT GOV w latach 2022–2024.

Źródło: CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf, s. 10 [dostęp: 1 X 2025].

[3] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf, s. 5 [dostęp: 1 X 2025].

[4] *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (t.j. DzU z 2025 r. poz. 194).

[5] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 10.

[6] Tamże.

Te dane obrazują zwiększającą się odporność podmiotów będących we właściwości CSIRT GOV. Czynnikami sprzyjającymi wzrostowi tej odporności są:

1) powstrzymywanie ataków na poziomie brzegowym sieci, czyli skuteczne filtrowanie i blokowanie prób naruszeń, zanim dotrą one do właściwych systemów teleinformatycznych. W przypadku ataków socjotechnicznych z wykorzystaniem poczty elektronicznej oznacza to stosowanie zaawansowanych filtrów antyspamowych i mechanizmów reputacyjnych na bramkach pocztowych; w odniesieniu do ataków siłowych – wdrażanie rozwiązań takich jak blokowanie adresów IP (tzw. blacklisting) czy limity prób logowania, a w przypadku zagrożeń wykorzystujących znane podatności – bieżące aktualizowanie oprogramowania i eliminowanie luk bezpieczeństwa;
2) wzrost świadomości użytkowników i pracowników administracji, którzy coraz częściej potrafią rozpoznać i powstrzymać próby ataków, w których wykorzystuje się socjotechnikę (np. phishing, spearphishing, vishing), jeszcze na etapie kontaktu z wiadomością lub podejrzanym linkiem, przed wejściem z nimi w interakcję. To efekt rosnącej liczby szkoleń, komunikatów ostrzegawczych i wewnętrznych procedur reagowania na incydenty. W 2024 r. CSIRT GOV przeprowadził szkolenia i warsztaty dla blisko 1900 osób, co stanowi prawie czterokrotny wzrost w stosunku do roku 2023[7];
3) rozwój wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, takich jak zespoły SOC (Security Operations Center) lub jednostki ds. bezpieczeństwa teleinformatycznego w instytucjach publicznych. Pozwala to na skuteczniejszą obsługę incydentów na poziomie lokalnym, bez konieczności angażowania CSIRT GOV;
4) zacieśnienie współpracy i koordynacji międzyinstytucjonalnej, zarówno w ramach trzech krajowych zespołów CSIRT (GOV, MON, NASK), jak i między administracją publiczną i operatorami infrastruktury krytycznej. Wymiana informacji o zagrożeniach i dystrybucja wskaźników kompromitacji (ang. *indicators of compromise*) umożliwiają wcześniejsze wykrywanie prób ataków oraz szybsze reagowanie na incydenty. Na podstawie zgłoszeń incydentów oraz analizy wskaźników kompromitacji z jednego przypadku

[7] Tamże.

CSIRT GOV opracowuje ostrzeżenia i rekomendacje dla całego swojego obszaru kompetencyjnego, co pozwala zapobiegać rozprzestrzenianiu się zagrożeń[8];

5) wykorzystywanie testów bezpieczeństwa i audytów jako działań proaktywnych, które w sposób bezpieczny i kontrolowany pozwalają na identyfikację słabych punktów systemów, zanim zostaną one wykorzystane przez grupy przestępcze i cyberofensywne. Tego typu działania, prowadzone przez jednostki znajdujące się w strukturze danego podmiotu, zewnętrzne firmy świadczące usługi testów penetracyjnych oraz przez CSIRT GOV, stanowią istotny element prewencji i podnoszenia ogólnej odporności cyfrowej podmiotów administracji publicznej i operatorów infrastruktury krytycznej. W 2024 r. CSIRT GOV przeprowadził serię testów penetracyjnych w instytucjach administracji publicznej. Obejmowały one m.in. ocenę konfiguracji systemów, skuteczności mechanizmów obronnych i jakości zarządzania podatnościami. Wnioski z tych testów posłużyły do opracowania zaleceń dla poszczególnych jednostek[9].

Charakterystyka działań cyberofensywnych w kontekście cyberbezpieczeństwa Rzeczypospolitej Polskiej

Wzrost kompetencji i zdolności podmiotów pozostających we właściwości CSIRT GOV nie eliminuje wszystkich zagrożeń. Analiza incydentów odnotowanych w 2024 r. wskazuje, że mimo zauważalnej poprawy poziomu zabezpieczeń i świadomości użytkowników, cyberprzestrzeń Polski nadal pozostaje miejscem aktywności podmiotów o charakterze przestępczym, wywiadowczym i haktywistycznym[10]. Zdarzenia będące wynikiem działań grup wspieranych przez państwa są jednym z elementów składających się na incydenty dzielone przez CSIRT GOV na dwie kategorie określane jako „socjotechnika" oraz „atak". Pierwsza z kategorii wskazuje głównie na phishing wymierzony w użytkowników organizacji pozostających w zainteresowaniu aktorów, druga dotyczy prób oraz skutecznych incydentów

[8] Tamże, s. 15.

[9] Tamże, s. 96.

[10] Tamże, s. 54.

przełamania zabezpieczeń infrastruktury teleinformatycznej atakowanych podmiotów[11].

W 2024 r. aktywność grup sponsorowanych przez państwa oraz prorosyjskich kolektywów haktywistycznych utrzymywała się na wysokim poziomie. Międzynarodowe raporty umieszczają Polskę wśród czołowych krajów europejskich pod względem liczby ataków sponsorowanych, motywowanych społecznie lub politycznie. Z raportu Microsoftu, firmy z sektora IT, wynika, że w 2024 r. Polska znalazła się w pierwszej trójce w Europie[12]. Z kolei według analityków firmy technologicznej Radware wśród państw Europy Polska zajmowała drugie miejsce, za Ukrainą, pod względem liczby ataków DDoS[13] inicjowanych przez prorosyjskich haktywistów[14]. To potwierdza, że Polska, jako aktywny sojusznik Ukrainy i wschodnia granica NATO i Unii Europejskiej, była szczególnie narażona na działania asymetryczne i hybrydowe w cyberprzestrzeni.

Raport CSIRT GOV wskazuje na dominację ataków z kierunku rosyjskiego, szczególnie przeprowadzanych przez grupę APT28 (stanowiącą jednostkę wojskową nr 26165 w 85. Głównym Centrum Zadań Specjalnych rosyjskiego wywiadu wojskowego GRU[15]) oraz grupę APT2916[16] (podległą Służbie Wywiadu Zagranicznego Federacji Rosyjskiej)[17]. Omawiane przypadki odnotowane w cyberprzestrzeni RP znajdują potwierdzenie także w przywołanych w tym artykule zagranicznych publikacjach, które pokazują szerszy kontekst działalności tych grup.

---

[11] Tamże, s. 12–13.

[12] *Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity*, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf, s. 13 [dostęp: 19 III 2025].

[13] Atak DDoS (ang. *distributed denial of service*, rozproszona odmowa usługi) – skoordynowane przeciążenie zasobów systemu lub usługi poprzez dużą liczbę jednoczesnych żądań pochodzących z różnych urządzeń, co ma uniemożliwić prawidłowe działanie.

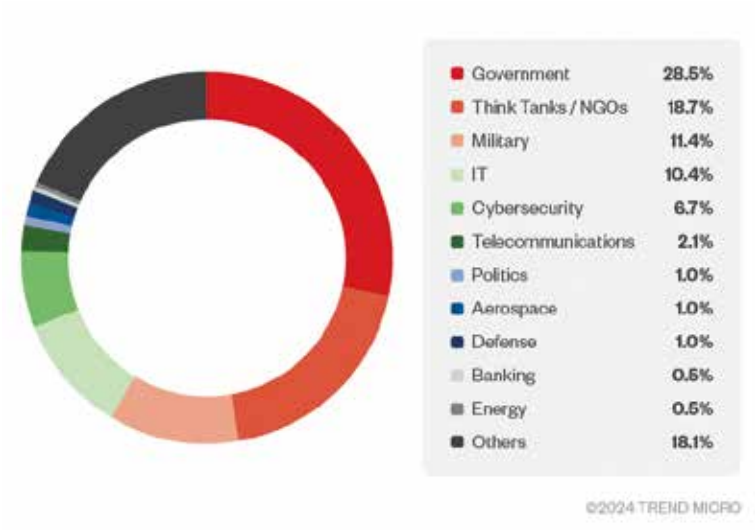
[14] *2024 Global Threat Analysis Report, Executive Summary*, https://www.cisco.com/c/dam/m/en_in/events/security-conclave-2024/radware-threat-report-summary-2024.pdf, s. 9 [dostęp: 2 X 2025].

[15] *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne*, https://www.gov.pl/attachment/e9e86877-2ba0-478e-be36-f20d68474f37, s. 4 [dostęp: 14 X 2025].

[16] APT29, MITRE ATT&CK, https://attack.mitre.org/groups/G0016/ [dostęp: 14 X 2025].

[17] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni…*, s. 56.

Kampania grupy APT29, znanej również jako Earth Koshchei, wykorzystująca pliki konfiguracji połączenia RDP (ang. *remote desktop protocol*), z dużym prawdopodobieństwem (zgodnie z ustaleniami analityków Microsoftu dokonanymi na podstawie nazw zarejestrowanych domen[18]) była adresowana m.in. do podmiotów rządowych państw europejskich, szczególnie do ministerstw spraw zagranicznych i ministerstw obrony, struktur NATO, a także do ukraińskich sektorów: obrony, energii i telekomunikacji (rysunek 2). Wpisuje się to jednoznacznie w kontekst działania służby wywiadowczej państwa prowadzącego wojnę z Ukrainą oraz działalność hybrydową wobec państw NATO, a lista potencjalnych adresatów kampanii pokrywa się z dotychczas notowanymi[19].



Rysunek 2. Odsetek domen zarejestrowanych przez grupę APT29 z podziałem na branże.

Źródło: *Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks*, Trend Micro, 17 XII 2024 r., https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html [dostęp: 14 X 2025].

[18] *Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files*, Microsoft Threat Intelligence, 29 X 2024 r., https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/ [dostęp: 14 X 2025].

[19] *Threat profile: APT29*, https://blackpointcyber.com/wp-content/uploads/2024/06/Threat-Profile-APT29_Blackpoint-Adversary-Pursuit-Group-APG_2024.pdf, s. 4 [dostęp: 2 X 2025].

Wśród zagrożeń ze strony grupy APT28 dominowały ataki socjotechniczne, w tym polegające na wyłudzaniu danych logowania do poczty elektronicznej oraz infekowaniu złośliwym oprogramowaniem wykradającym wrażliwe informacje ze stacji roboczych. Wyróżniono także ataki wykorzystujące różnego rodzaju podatności systemów teleinformatycznych[20]. W kontekście teleinformatyki „podatności" oznaczają słabości systemów, którymi atakujący może się posłużyć do przeprowadzenia skutecznego ataku[21]. Należy jednak podkreślić, że to pojęcie nie odnosi się wyłącznie do błędów oprogramowania zarejestrowanych w bazie CVE (ang. Common Vulnerabilities and Exposures), lecz obejmuje także błędy konfiguracji, zachowania użytkowników oraz niezamierzone cechy oprogramowania, które mogą zostać wykorzystane w sposób sprzeczny z ich przeznaczeniem[22].

Na przykład słabym punktem systemu może być użycie prostych lub powtarzalnych haseł, co bywa wyzyskiwane w atakach siłowych na panele logowania. Brak filtrowania ruchu pochodzącego z anonimizujących sieci VPN[23] lub TOR[24] również stanowi istotną słabość, ułatwiającą atakującemu ukrycie źródła działań. W analizowanych przypadkach odnotowano także wykorzystanie podatności umożliwiających przeprowadzenie ataku DCSync[25], który pozwala na uzyskanie poświadczeń domenowych[26]. Z kolei pewne funkcje systemowe, takie jak mechanizmy nadawania uprawnień do folderów poczty elektronicznej w usłudze Microsoft Exchange, mogą być użyte zgodnie z ich konstrukcją, lecz w sposób złośliwy i służyć eskalacji uprawnień lub eksfiltracji danych[27]. Tak szeroki zakres podatności

[20] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni…*, s. 57–66.

[21] *Vulnerability management, Understanding vulnerabilities*, National Cyber Security Centre, https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities [dostęp: 10 X 2025].

[22] Tamże.

[23] Virtual Private Network – usługa szyfrowanego tunelu pomiędzy urządzeniem użytkownika a serwerem pośredniczącym, maskująca rzeczywisty adres IP i lokalizację użytkownika.

[24] The Onion Router – sieć anonimizująca, przekierowująca ruch sieciowy przez dużą liczbę szyfrowanych węzłów.

[25] Atak DCSync – technika, w której atakujący podszywa się pod kontroler domeny Active Directory i żąda synchronizacji danych, uzyskując w ten sposób skróty kryptograficzne poświadczeń do wszystkich kont w domenie.

[26] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni…*, s. 65.

[27] Tamże.

oznacza, że cyberodporność organizacji zależy nie tylko od bieżącej aktualizacji oprogramowania, lecz także od właściwej konfiguracji środowiska, dyscypliny użytkowników oraz rozumienia, w jaki sposob funkcjami systemowymi może posłużyć się przeciwnik.

Grupa APT28 wykorzystywała te środki w atakach zarówno na podmioty w Polsce, jak i w innych państwach, w tym należących do NATO. W maju 2025 r. zostało to zaraportowane we wspólnym dokumencie służb Stanów Zjednoczonych, Wielkiej Brytanii, Niemiec, Czech, Polski, Australii, Kanady, Danii, Estonii, Francji i Holandii[28]. Dokument ten stanowi rozwinięcie opisu przedstawionej przez CSIRT GOV aktywności GRU wobec podmiotów realizujących zadania na rzecz wsparcia Ukrainy w wojnie z Rosją, a także przedsiębiorstw technologicznych i jednocześnie prezentuje inny – obok działalności sabotażowej[29] – wymiar obecności GRU w państwach zachodnich oraz w Ukrainie (rysunek 3).

Rysunek 3. Lokalizacja geograficzna podmiotów, w które były wymierzone działania GRU.

Źródło: *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/attachment/e9e86877-2ba0-478e-be36-f20d68474f37, s. 7 [dostęp: 14 X 2025].

[28] *Działania rosyjskiej służby specjalnej GRU...*, s. 7.

[29] A. Jawor, *„Agenci jednorazowego użytku" rosyjskiego GRU. „Tajna" kampania sabotażu w Europie*, CyberDefence24, 3 X 2025 r., https://cyberdefence24.pl/armia-i-sluzby/agenci-jednorazowego-uzytku-rosyjskiego-gru-tajna-kampania-sabotazu-w-europie [dostęp: 14 X 2025].

Wśród zagrożeń analizowanych przez CSIRT GOV wskazano również aktywność grup powiązanych z Chińską Republiką Ludową, które w 2024 r. prowadziły działania wywiadowcze wobec państw członkowskich Unii Europejskiej. Koncentrowała się ona na pozyskiwaniu informacji z obszarów: naukowo-technologicznego, energetycznego oraz administracji publicznej. Ataki odnotowane w Polsce zostały przeprowadzone przez dwie grupy – Volt Typhoon[30] oraz APT15[31]. Ponadto zidentyfikowano sieć przejętych przez chińskich cyberprzestępców urządzeń sieciowych firmy TP-Link. Użyto jej do anonimizacji ruchu w atakach na usługi Microsoftu[32]. Działania te wpisują się w długofalową strategię pozyskiwania w sposób ukryty informacji o dużym znaczeniu dla przemysłu i gospodarki, realizowaną w celu wzmocnienia potencjału technologicznego i konkurencyjności Chin na arenie międzynarodowej.

Na uwagę zasługuje także aktywność podmiotów powiązanych z Republiką Białorusi, które z dużym prawdopodobieństwem działają we współpracy ze służbami Federacji Rosyjskiej. W 2024 r. obserwowano działania grupy UNC1151, prowadzącej dwa rodzaje działalności – dezinformacyjną oraz wywiadowczą[33]. Jej kampanie obejmowały wiadomości phishingowe podszywające się pod panele logowania do poczty elektronicznej najpopularniejszych polskich dostawców – Interii, Onetu, Wirtualnej Polski. Chodziło o wyłudzenie danych logowania, przejęcie kont i zbudowanie infrastruktury potrzebnej do akcji dezinformacyjnych. Aby prowadzić działalność szpiegowską, infekowano komputery szkodliwym oprogramowaniem pozwalającym na przejęcie pełnej kontroli nad urządzeniem. Dokonywano tego za pośrednictwem wiadomości e-mail. Aktywność tej grupy jest obserwowana od co najmniej 2017 r.[34], co świadczy o długotrwałym, rozpoznawczym charakterze działań i ukierunkowaniu na destabilizację informacyjną państwa.

[30] Volt Typhoon – grupa o atrybucji wskazującej na Chińską Armię Ludowo-Wyzwoleńczą, atakująca infrastrukturę krytyczną państw zachodnich w celu prowadzenia działań wywiadowczych.

[31] APT15 – grupa cyberofensywna o atrybucji chińskiej, realizująca strategiczne cele wywiadowcze Chin.

[32] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni…*, s. 72–73, 75.

[33] Tamże, s. 69–72.

[34] *Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity*, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, s. 8 [dostęp: 14 X 2025].

W raporcie odnotowano także działania prorosyjskich grup haktywistycznych Beregini i Zarya. Opublikowały one zmanipulowane dane wykradzione z Polskiej Agencji Antydopingowej, aby podważyć wiarygodność polskich sportowców podczas igrzysk olimpijskich w Paryżu[35]. Działania te są określane jako operacje *hack-and-leak*. Łączą one cyberatak z manipulacją informacyjną, której celem jest wywarcie wpływu na opinię publiczną[36].

W przypadku infrastruktury przemysłowej (Operational Technology/Industrial Control Systems) działalność haktywistyczna coraz częściej obejmuje cele związane z instalacjami użyteczności publicznej, takimi jak oczyszczalnie ścieków, sieci wodociągowe czy przepompownie[37]. Jest to trend międzynarodowy, obserwowany także w Stanach Zjednoczonych[38], Holandii, Francji[39] czy Norwegii[40]. W raporcie CSIRT GOV nie podano konkretnych przypadków, wskazano jedynie na nasilenie takich działań. Wśród najbardziej aktywnych kolektywów, pokazujących rezultaty przeprowadzonych ataków na dedykowanych kanałach na platformie Telegram, należy wskazać: Cyber Army of Russia Reborn (CARR), Z-Pentest[41], Sector16 oraz TwoNet[42]. Trzy ostatnie są częścią sojuszu działającego pod przewodnictwem OverFlame (rysunek 4).

[35] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 6.

[36] S. Palczewski, *Kampanie hack-and-leak. Czy namieszają przed wyborami w Polsce?*, Demagog, 17 VIII 2023 r., https://demagog.org.pl/analizy_i_raporty/kampanie-hack-and-leak-czy-namieszaja-przed-wyborami-w-polsce/ [dostęp: 13 X 2025].

[37] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 55.

[38] *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity*, https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf, s. 1 [dostęp: 1 X 2025].

[39] *Cyber Insight, Sector 16 group*, https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Sector16/Sector16Group.pdf, s. 10 [dostęp: 1 X 2025].

[40] M. Bryant, *Russian hackers seized control of Norwegian dam, spy chief says*, The Guardian, 14 VIII 2025 r., https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway [dostęp: 14 X 2025].

[41] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 74.

[42] *Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS*, Forescout, 9 X 2025 r., https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/ [dostęp: 12 X 2025].

Rysunek 4. Grupy haktywistyczne skupione w ramach kolektywu OverFlame.

Źródło: *Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS*, Forescout, 9 X 2025 r., https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/ [dostęp: 12 X 2025].

Aktywność tych kolektywów charakteryzuje się wysoką dynamiką. Dochodzi do częstej dezaktywacji kanałów, powstawania nowych grup i sojuszy, a także konfliktów. Jednocześnie wiele wskazuje na to, że za wieloma kolektywami stoi niewielka grupa tych samych osób, które działają na zlecenie rosyjskich służb. Ukraiński instytut Molfar (Molfar Intelligence Institute) opublikował w styczniu 2025 r. dane administratorów i członków grup NoName057(16) oraz DDoSia, prowadzących ataki DDoS przeciwko stronom i usługom internetowym w państwach sprzeciwiających się polityce Federacji Rosyjskiej[43]. Zidentyfikowana tam Julia Vladimirovna Pankratova wraz z Denisem Olegovichem Dekgtyarenko znaleźli się na liście osób, na które Stany Zjednoczone nałożyły sankcje w związku z rolą, jaką odegrały w atakach grupy hakerskiej CARR na amerykańską infrastrukturę krytyczną[44]. Analitycy Mandiant, amerykańskiej firmy z branży cyberbezpieczeństwa, w swoim raporcie dotyczącym grupy Sandworm

[43] *Russian Cyber Army. Who is it?*, Molfar Intelligence Institute, 23 I 2025 r., https://www.molfar.institute/en/russian-cyber-army/ [dostęp: 12 X 2025].

[44] *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn,* U.S. Department of the Treasury, 19 VII 2024 r., https://home.treasury.gov/news/press-releases/jy2473 [dostęp: 11 X 2025].

(identyfikowanej jako jednostka wojskowa 74455 Centrum Technologii Specjalnych GRU) wskazali na jej powiązania z kolektywami XakNet, Solntsepek oraz CARR[45]. Z dużym prawdopodobieństwem może to oznaczać, że CARR i grupy działające z nią w sojuszu realizują zadania na zlecenie służb Federacji Rosyjskiej, co podaje w wątpliwość oddolny charakter haktywizmu.

Bezpieczeństwo łańcucha dostaw

Jednym z najważniejszych wniosków raportu CSIRT GOV jest zwrócenie uwagi na rosnące ryzyko związane z podmiotami trzecimi – dostawcami usług IT, firmami outsourcingowymi i wykonawcami (w branży IT nazywanymi kontraktorami, z ang. *contractor*). Incydenty dotyczące łańcucha dostaw pokazują, że bezpieczeństwo organizacji jest tak silne jak najsłabsze ogniwo w jej ekosystemie. Restrykcyjne procedury wewnętrzne nie gwarantują bezpieczeństwa, jeśli partnerzy zewnętrzni nie utrzymują odpowiedniego poziomu ochrony[46]. W 2024 r. do incydentów polegających na kompromitacji systemów, eksfiltracji danych i ich publikacji doszło w firmach świadczących usługi z zakresu informatyki i automatyki, np. AIUT Sp. z o.o.[47] czy Atende S.A.[48] W 2025 r. były to EuroCert Sp. z o.o.[49] – dostawca usługi podpisu kwalifikowanego oraz firma ochroniarska Ekotrade Sp. z o.o.[50] Skutkiem tych działań było upublicznienie danych wrażliwych o pracownikach, klientach i umowach.

[45] G. Roncone, D. Black, J. Wolfram, T. McLellan, N. Simonian, R. Hall, A. Prokopenkov, D. Perez, L. Aytes, A. Wahlstrom, *APT44: Unearthing Sandworm*, https://*services*.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf, s. 12–13 [dostęp: 19 III 2025].

[46] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni…*, s. 113.

[47] *Incydent bezpieczeństwa*, Aiut, https://aiut.com/incydent-bezpieczenstwa/ [dostęp: 12 X 2025].

[48] *Komunikat Atende w związku z upublicznieniem ukradzionych danych*, Atende, 22 X 2024 r., https://atende.pl/pl/aktualnosci/komunikat-atende-w-zwiazku-z-upublicznieniem-ukradzionych-danych [dostęp: 12 X 2025].

[49] *Atak na EuroCert – oświadczenie*, EuroCert, 15 I 2025 r., https://eurocert.pl/atak-na-eurocert-oswiadczenie/ [dostęp: 12 X 2025].

[50] *Komunikat dotyczący ataku hakerskiego na infrastrukturę informatyczną Ekotrade Sp. z o.o.*, https://ekotrade.com.pl/img/rodo/KOMUNIKAT-EKOTRADE-dla-pracownikow.pdf [dostęp: 12 X 2025].

W kontekście bezpieczeństwa narodowego oznacza to konieczność traktowania łańcucha dostaw jako integralnej części systemu bezpieczeństwa państwa. Regularne audyty bezpieczeństwa, kontrola dostępu zdalnego, zabezpieczenie danych w ruchu i w spoczynku, weryfikacja umów z dostawcami oraz opracowanie planów ciągłości działania powinny być standardem w instytucjach publicznych i przedsiębiorstwach o znaczeniu strategicznym, w tym wśród operatorów infrastruktury krytycznej[51].

Podsumowanie

Analizując raport CSIRT GOV w szerszym kontekście, należy zauważyć, że cyberataki coraz częściej stanowią element prowadzenia konfliktów poniżej progu wojny, czym wpisują się w rosyjską koncepcję wojny nowej generacji. Służą rozpoznaniu, dezinformacji i destabilizacji bez konieczności użycia siły militarnej. W tym sensie cyberbezpieczeństwo jest już nie tylko domeną technologiczną, lecz także strategiczną i polityczną, stanowi bowiem płaszczyznę, na której przecinają się interesy państw, sektora prywatnego i społeczeństwa. Ataki na administrację państwową, infrastrukturę krytyczną czy media publiczne mają wymiar symboliczny i psychologiczny – podważają zaufanie do instytucji państwa, odsłaniając jego słabości, i wywołują szum medialny. Zdolność do szybkiego reagowania, informowania opinii publicznej zgodnie z przyjętymi scenariuszami komunikacji strategicznej oraz przywracania ciągłości działania organizacji jest jednym z najważniejszych wymiarów obronności.

Raport CSIRT GOV potwierdza, że bezpieczeństwo cybernetyczne RP stanowi dziś integralny element bezpieczeństwa narodowego, a jego utrzymanie wymaga synergii działań technicznych, prawnych i organizacyjnych państwa. Skala zagrożeń dla Polski nie maleje, dlatego tak istotne jest, aby zdolność instytucji do ich identyfikacji, ograniczania skutków i budowania odporności stale rosła. Bardzo ważne są współpraca i wymiana informacji. Stale zmieniający się krajowy system cyberbezpieczeństwa, rozszerzany o sektorowe zespoły CSIRT, wraz z zespołami krajowymi, organami właściwymi do spraw cyberbezpieczeństwa, operatorami usług kluczowych oraz pozostałymi instytucjami, musi stanowić tarczę skutecznie chroniącą przed zagrożeniami o charakterze międzynarodowym. Bezpieczeństwo

[51] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni…*, s. 116.

to proces ciągły, wymagający stałej weryfikacji, audytów i zachowania elastyczności w celu adaptacji do zmieniających się warunków technologicznych i geopolitycznych. Pojawiające się z każdym dniem nowe podatności, techniki ataków, a przede wszystkim rozwój sztucznej inteligencji, która będzie wspierać atakujących w tworzeniu treści phishingowej oraz kolejnych wersji złośliwego oprogramowania, sprawiają, że trzeba zwiększać swoją odporność i zdolność reakcji na pojawiające się zagrożenia. Jest to istotne jak nigdy wcześniej.

Dynamicznie zmieniający się charakter zagrożeń w cyberprzestrzeni unaocznia pilną potrzebę rezygnacji z modelu reaktywnego na rzecz działań ukierunkowanych na budowanie odporności cyberprzestrzeni RP. Powinny one polegać przede wszystkim na wdrażaniu kompleksowych rozwiązań o charakterze systemowym, a także na doskonaleniu wewnętrznych regulacji organizacyjnych. Kierunek ten znajduje odzwierciedlenie w projektowanych zmianach legislacyjnych, zwłaszcza w nowelizacji ustawy o KSC oraz ustawy o zarządzaniu kryzysowym. Ich wejście w życie w 2025 r. ma na celu poprawę koordynacji działań i wymiany informacji, uwzględnienie wrażliwości łańcuchów dostaw oraz podniesienie ogólnej odporności instytucjonalnej państwa na incydenty w cyberprzestrzeni. Skuteczność tych rozwiązań będzie w dużej mierze zależeć od stopnia ich wdrożenia oraz od zdolności do adaptacji w obliczu dalszej ewolucji cyberzagrożeń.

Monika Stodolnik

Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Kontakt: monika.stodolnik@abw.gov.pl

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 271–281

https://doi.org/10.4467/27204383TER.25.054.23041

Varia

Budowanie odporności europejskiego sektora kolejowego na zagrożenia hybrydowe. Polski wkład w dobre praktyki i zwiększenie bezpieczeństwa

Tomasz Lachowicz
Autor niezależny
https://orcid.org/0009-0002-4344-7120

Po serii zamachów terrorystycznych w Europie w latach 2015–2017, wymierzonych również w transport kolejowy, kwestia bezpieczeństwa stała się jednym z priorytetów Unii Europejskiej.

Spotkanie ministerialne państw członkowskich 29 sierpnia 2015 r. w Paryżu i tzw. paryska deklaracja stanowiły polityczne wsparcie dla Komisji Europejskiej, aby podjęła pilne działania podnoszące poziom bezpieczeństwa w UE. Z kolei na spotkaniu Rady UE w Luksemburgu 8 października 2015 r. przyjęto propozycje opracowania wspólnych zasad bezpieczeństwa dla pociągów międzynarodowych i kolei dużych prędkości. Komisja Europejska została tym samym zobligowana do przeanalizowania wpływu szeregu inicjatyw na rzecz poprawy bezpieczeństwa pasażerskiego transportu kolejowego w UE.

W 2017 r. Jean-Claude Juncker, ówczesny przewodniczący Komisji Europejskiej, w przemowie *State of the Union* podkreślił potrzebę silnej i bezpiecznej Unii, a w kolejnych latach zagadnienia związane z bezpieczeństwem transportu lądowego, w tym przede wszystkim bezpieczeństwem

pasażerów i miejsc publicznych, pozostawały priorytetowymi tematami unijnej agendy.

Polska włączyła się w te prace, m.in. przez Przedstawicielstwo Polskich Kolei Państwowych S.A. w Brukseli, odpowiedzialne za współpracę z unijnymi instytucjami oraz międzynarodowymi organizacjami kolejowymi. Efektem wspólnych działań były inicjatywy na rzecz zwiększenia poziomu bezpieczeństwa w UE, w tym w dziedzinie transportu.

Platforma RAILSEC – plan poprawy bezpieczeństwa pasażerów kolei

Z uwagi na rosnące ryzyko zagrożenia terrorystycznego w pasażerskim transporcie kolejowym Dyrekcja Generalna ds. Mobilności i Transportu (Directorate-General for Mobility and Transport, DG MOVE), która odpowiada za politykę transportową w UE, przeprowadziła w latach 2016–2017 publiczne konsultacje skierowane do sektora kolejowego. Zamierzano wysondować, jakie są możliwe unijne inicjatywy legislacyjne i pozalegislacyjne w tym obszarze. W ten proces zaangażowało się Przedstawicielstwo PKP, koordynując wkład spółek PKP oraz wypracowując wspólne stanowisko kolei europejskich w ramach Wspólnoty Kolei Europejskich oraz Zarządców Infrastruktury Kolejowej (Community of European Railways and Infrastructure Managers, CER). Rezultatem konsultacji było opublikowanie przez Komisję Europejską w połowie 2018 r. *Unijnego planu działania na rzecz poprawy bezpieczeństwa pasażerów kolei i personelu kolejowego* (*EU action plan to improve the security of rail passengers and staff*), w którym zainicjowano powołanie unijnej platformy ds. bezpieczeństwa pasażerów w transporcie kolejowym – The EU Rail Passenger Security Platform (RAILSEC). Jej członkami zostali eksperci z państw członkowskich UE oraz z państw należących do Europejskiego Stowarzyszenia Wolnego Handlu (European Free Trade Association, EFTA), wydelegowani do niej z władz i służb krajowych. Pozostali interesariusze, np. organizacje kolejowe takie jak Europejska Agencja Kolejowa (European Railway Agency, ERA), Colpofer, otrzymały status obserwatorów. Spotkania członków platformy miały charakter zamknięty i były prowadzone wspólnie przez DG MOVE oraz Dyrekcję Generalną ds. Migracji i Spraw Wewnętrznych (Directorate-General for Migration and Home Affairs, DG HOME). Prace objęły m.in.:

- zaktualizowanie metodologii oceny ryzyka zagrożenia terrorystycznego w pasażerskim transporcie kolejowym, a także zbioru wytycznych, rekomendacji i najlepszych praktyk, które będą mogły zostać użyte do przeprowadzania oceny ryzyka przez kompetentne podmioty na poziomie krajowym i lokalnym,
- stworzenie listy najbardziej użytecznych technologii do ochrony pociągów i stacji kolejowych (głównie w kontekście wykrywania ładunków wybuchowych, broni). Na jej bazie Komisja Europejska (DG MOVE/DG HOME) stworzyła katalog najlepszych praktyk i najbardziej efektywnych, również pod względem kosztów, rozwiązań,
- opracowanie wytycznych w zakresie zagrożenia wewnętrznego (ang. *insider threat*), w tym listy wrażliwych – z punktu widzenia zagrożenia terrorystycznego – stanowisk pracy, które wymagają specjalnej uwagi ze strony pracodawcy,
- inne działania – m.in. w obszarze cyberbezpieczeństwa, zagrożeń CBRN (chemicznych, biologicznych, radiologicznych, nuklearnych) oraz planów zarządzania bezpieczeństwem na kolei.

Platforma RAILSEC stała się częścią funkcjonującej od lat, większej i szerszej tematycznie eksperckiej platformy państw członkowskich ds. transportu lądowego – Land Transport Security (LANDSEC).

Przedstawicielstwo PKP monitorowało działania RAILSEC, a także brało udział w spotkaniach grup roboczych, przekazując istotne dla Grupy PKP rezultaty prac (wytyczne, rekomendacje itp.). Uczestniczy również w spotkaniach LANDSEC.

Plan działania na rzecz ochrony przestrzeni publicznych

Równolegle z działaniami podejmowanymi w obszarze bezpieczeństwa pasażerów w transporcie kolejowym DG HOME angażowała się w prace związane z bezpieczeństwem przestrzeni publicznych. W październiku 2017 r. został opublikowany unijny *Plan działania na rzecz ochrony przestrzeni publicznej* (*Action Plan to support the protection of public spaces*), w ramach którego powołano unijne forum publicznych i prywatnych operatorów. Jego głównym zadaniem jest wymiana know-how oraz najlepszych praktyk w obszarze ochrony przestrzeni publicznych. Służą temu spotkania tematyczne członków platformy, dotyczące m.in. transportu, organizacji wydarzeń masowych czy ochrony przestrzeni komercyjnych. Forum

opracowało szereg wytycznych i dobrych praktyk w kontekście działań, jakie mogą podejmować operatorzy, aby wzmocnić bezpieczeństwo i ochronę przestrzeni publicznych.

Aktywnym członkiem tego gremium od początku jego powstania jest Przedstawicielstwo PKP, które prezentuje na nim przyjęte w Grupie PKP dobre praktyki i strategie działania z zakresu bezpieczeństwa oraz przekazuje do spółek Grupy PKP informacje ze spotkań, m.in. na temat wypracowanych rozwiązań w obszarze bezpieczeństwa.

ReArm Europe/Gotowość 2030 – plan finansowania obronności Unii Europejskiej

W marcu 2025 r. Komisja Europejska przedstawiła wspólną białą księgę w sprawie gotowości obronnej Europy do 2030 r. – Gotowość 2030 (Readiness 2030). Uzupełnia ją plan ReArm Europe – ambitny pakiet obronny, w ramach którego aż do 800 mld euro (w ramach różnych instrumentów finansowych) zostanie przeznaczonych na inwestycje zwiększające zdolności obronne państw członkowskich. Jako priorytetowe wskazano pakiet na rzecz mobilności wojskowej oraz plan działania UE w zakresie transformacji obronności. W pakiecie tym uwzględniono m.in. wnioski wyciągnięte ze znowelizowanego unijnego planu działania na rzecz mobilności wojskowej 2.0 i zobowiązania do mobilności wojskowej z 2024 r. Opracowano go w ścisłej koordynacji z Europejską Służbą Działań Zewnętrznych (European External Action Service) oraz Europejską Agencją Obrony (European Defence Agency), zapewniając spójność ze standardami i procedurami NATO.

Pakiet składa się z komunikatu na temat mobilności wojskowej i propozycji rozporządzenia w sprawie ustanowienia ram środków ułatwiających transport sprzętu wojskowego, towarów i personelu wojskowego przez Unię[1] (do którego dodano dokument roboczy Komisji Europejskiej), a także wprowadzenia zmian w przepisach UE i lepszego uwzględnienia wymogów dotyczących mobilności wojskowej z perspektywy podwójnego wykorzystania – wojskowego i cywilnego.

[1] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework of measures to facilitate the transport of military equipment, goods and personnel across the Union,* https://eur-lex.europa.eu/resource.html?uri=cellar:b84cfa7d-c619-11f0-8da2-01aa75ed71a1.0001.02/DOC_1&format=PDF.

Komisja Europejska zmierza do stworzenia do 2027 r. wojskowej strefy Schengen i transformacji przemysłu obronnego. Intencją tych działań jest wprowadzenie ułatwień, dzięki którym oddziały, sprzęt i zasoby wojskowe będą mogły być przemieszczane w całej Europie na dużą skalę i z dużą prędkością, w sposób sprawny i skoordynowany. Ma to być możliwe dzięki:

- usunięciu barier regulacyjnych – przez wprowadzenie przepisów dotyczących mobilności wojskowej zharmonizowanych na szczeblu UE oraz określenie zasad i procedur dotyczących transgranicznych przemieszczeń wojskowych, z rozpatrywaniem wniosków w ciągu maksymalnie trzech dni i uproszczonymi formalnościami celnymi;
- powstaniu struktur na wypadek sytuacji nadzwyczajnej – przez powołanie Europejskiego Systemu Wzmocnionej Reakcji w Zakresie Mobilności Wojskowej (European Military Mobility Enhanced Response System, EMERS), aby przyspieszyć procedury i zapewnić priorytetowy dostęp do infrastruktury. EMERS ma wspierać siły zbrojne działające w kontekście UE lub NATO;
- zwiększeniu odporności infrastruktury transportowej – przez dostosowanie kluczowych unijnych korytarzy mobilności wojskowej do norm podwójnego zastosowania oraz ochronę infrastruktury strategicznej za pomocą nowego zestawu narzędzi. Ukierunkowane inwestycje mają wzmocnić cyberbezpieczeństwo, bezpieczeństwo energetyczne i gotowość zarówno w czasie pokoju, jak i kryzysu;
- łączeniu i współdzieleniu zdolności – przez zwiększenie gotowości, solidarności i dostępności zdolności w zakresie mobilności wojskowej dla państw członkowskich. Ma to być możliwe dzięki wprowadzeniu puli solidarnościowej i utworzeniu cyfrowego systemu wymiany informacji na potrzeby mobilności wojskowej;
- wzmocnieniu zarządzania i koordynacji – za wdrażanie zmian i monitorowanie gotowości będą odpowiedzialne nowa unijna Grupa ds. Transportu w ramach Mobilności Wojskowej (Military Mobility Transport Group) oraz wzmocniony Komitet ds. Transeuropejskiej Sieci Transportowej (Trans-European Transport Network, TEN-T). Wspierać ich będą krajowi koordynatorzy ds. transgranicznego transportu wojskowego obecni w każdym państwie członkowskim;
- innowacjom na rzecz gotowości obronnej.

Komisja Europejska zobowiązała się, że w 2026 r. dokona przeglądu rozporządzenia wykonawczego w sprawie przepustowości infrastruktury kolejowej, aby upewnić się, że spełnia ono potrzeby transportu wojskowego.

Uwzględni przy tym wkład wniesiony przez przedstawicieli wojsk. Transport wojskowy ma być zwolniony z ograniczeń ruchu wynikających z efektywności środowiskowej pojazdów, kontroli jakości powietrza czy kontroli poziomu hałasu (w odniesieniu do lotnisk czy portów), a pojazdy kolejowe będą mogły operować bardziej elastycznie. Ponadto w 2026 r. Komisja, przy wsparciu m.in. ERA i zarządców infrastruktury, ma dokonać ponownej oceny fizycznych ograniczeń infrastruktury kolejowej na priorytetowych korytarzach mobilności wojskowej, aby ułatwić transport ładunków ponadgabarytowych. Będzie także pracować, również przy wsparciu ERA, nad wzmocnieniem systemu zarządzania ruchem kolejowym, aby zapewnić ciągłość działania w przypadku sabotażu lub innej awarii systemu. W rozporządzeniu reguluje się m.in. zagadnienia związane z indywidualnymi trasami pociągów dla wojskowego transportu kolejowego, kwestie używania pojazdów kolejowych poza ich określonym obszarem użytkowania czy zagadnienia identyfikacji pojazdów kolejowych do potencjalnego wykorzystania w transporcie wojskowym.

Pakiet ma duże znaczenie dla polskich kolei, a przede wszystkim dla funkcjonowania państwa w sytuacjach kryzysowych. W przypadku konfliktu zbrojnego zdolność kolei do zachowania ciągłości dostaw i wsparcia mobilizacji jest kluczowa dla właściwej reakcji i stabilności kraju. Przewozy kolejowe pozwalają bowiem na skuteczne przemieszczanie sił zbrojnych i sprzętu wojskowego. Kolej i przemysł kolejowy muszą też nadążać za innowacjami i zmianami wynikającymi z zagrożeń hybrydowych. Do tego potrzebne są środki finansowe i budowa odpowiednich kompetencji. Rosyjska agresja na Ukrainę pokazała, jak szybko rozwijają się technologie ofensywne i obronne. Innowacje, takie jak sztuczna inteligencja, systemy kwantowe, drony i technologie kosmiczne, zmieniają oblicze pola walki i działania na nim. Tym istotniejsza jest rola logistyki.

Polski wkład w bezpieczeństwo – aktywność Przedstawicielstwa PKP na poziomie unijnym

Przedstawicielstwo PKP od wielu lat jest zaangażowane w prace związane z poprawą bezpieczeństwa w transporcie kolejowym, aktywnie współpracując z instytucjami unijnymi i uczestnicząc w wielu międzynarodowych platformach eksperckich, inicjatywach i projektach. Ze swojej strony również inicjuje międzynarodowe działania, których zadaniem jest wzmocnienie

bezpieczeństwa na kolei. Jako odpowiedzialne za współpracę i koordynacje działań spółek PKP w ramach największej światowej organizacji kolejowej – Międzynarodowego Związku Kolei (L'Union internationale des chemins de fer, UIC) – Przedstawicielstwo PKP bierze ponadto udział (wraz z Biurem Bezpieczeństwa PKP S.A.) w działaniach i projektach UIC w obszarze bezpieczeństwa kolejowego. Jest to m.in. platforma bezpieczeństwa UIC (wraz z utworzonym w jej ramach hubem UIC ds. bezpieczeństwa), której PKP S.A. przewodziło przez pewien czas. Wspólnie z największymi europejskimi kolejami Przedstawicielstwo PKP zapoczątkowało też kilka projektów międzynarodowych, których koordynację przekazało UIC.

Projekt SHERPA (Shared and Coherent European Railway Protection Approach) – spójne podejście europejskich kolei do ochrony transportu kolejowego[2]

Projekt został zainicjowany na przełomie lat 2017 i 2018 i polegał na opracowaniu spójnego, kompleksowego podejścia europejskich kolei do zapewnienia bezpieczeństwa pasażerów w transporcie kolejowym w kontekście zagrożeń terrorystycznych. Liderem projektu było UIC, a członkami konsorcjum największe koleje europejskie: polskie PKP, niemieckie DB, francuskie SNCF, włoskie FSI oraz belgijskie SNCB. Trwał dwa lata i zakończył się w 2020 r. W 90% został sfinansowany ze środków unijnych.

W ramach tego projektu były analizowane m.in. zagrożenia terrorystyczne wymierzone w stacje kolejowe i pociągi, w tym zamachy i sabotaże bądź próby ich dokonania. To pozwoliło na wypracowanie najlepszych praktyk ochrony wraz z katalogiem potrzeb po stronie kolei, m.in. jednolitego podejścia do oceny i zarządzania ryzykiem związanym z zagrożeniami terrorystycznymi w transporcie kolejowym, wymogów i specyfikacji sprzętu detekcyjnego czy nowych rozwiązań technologicznych. Podczas jego realizacji PKP S.A. zorganizowało w Warszawie warsztaty z udziałem wielu ekspertów z zagranicy, poświęcone poprawie bezpieczeństwa na dworcach i w pociągach.

Dzięki temu projektowi UIC znacznie wzmocniło wspomnianą już platformę bezpieczeństwa i prowadzony w jej ramach hub, zawierający najlepsze praktyki, metodologie i rozwiązania techniczne z zakresu poprawy bezpieczeństwa w transporcie kolejowym.

[2] https://sherpa-rail-project.eu/.

Projekt IMPRESS (IMProving Railway sEcurity through awareneSS and training) – poprawa bezpieczeństwa transportu kolejowego przez podnoszenie świadomości zagrożeń i szkolenia[3]

W 2022 r. Przedstawicielstwo PKP zainicjowało kolejny projekt międzynarodowy, tym razem z udziałem kolei SNCB, FSI i holenderskich NS, a także Niemieckiego Uniwersytetu Policyjnego (Deutsche Hochschule der Polizei) jako strony eksperckiej oraz UIC – jako koordynatora konsorcjum. Był on kontynuacją projektu SHERPA i służył poprawie bezpieczeństwa transportu kolejowego przez podnoszenie świadomości na temat zagrożeń i szkolenia. Budżet projektu wyniósł ponad 1,058 mln euro, a dzięki wysokim ocenom Komisji Europejskiej (DG HOME) w 90% pochodził ze środków UE. Projekt trwał dwa lata i zakończył się w 2025 r.

Jego celem było wzmocnienie systemu bezpieczeństwa kolejowych przestrzeni publicznych (stacji kolejowych, pociągów) przez włączenie w ten system nie tylko personelu kolejowego, służb policyjnych, ochrony kolei i dworców, lecz także innych podmiotów, w tym najemców powierzchni komercyjnych, personelu usługowego na stacjach i w pociągach. Chodziło o podniesienie wśród tych grup, a przede wszystkim wśród tzw. *first responders* (pierwszych reagujących), świadomości na temat zagrożeń terrorystycznych, podejrzanych zachowań czy sytuacji oraz umiejętności prawidłowego reagowania na nie, a także o poprawę współpracy i koordynacji działań między podmiotami publicznymi i prywatnymi w kolejowej przestrzeni publicznej. Jest to ważny, proaktywny element ochrony stacji kolejowych czy pociągów.

Uczestnictwo PKP S.A. w projekcie IMPRESS zaowocowało stworzeniem modułów szkoleniowych i treningowych zwiększających świadomość zarówno pracowników kolei, jak i innych podmiotów będących uczestnikami środowiska kolejowego, a także podniesieniem poziomu wiedzy i wypracowaniem konkretnych rozwiązań z zakresu bezpieczeństwa na stacjach kolejowych. Przyczyniło się także do zacieśnienia współpracy Grupy PKP z największymi kolejami europejskimi i ekspertami w dziedzinie bezpieczeństwa.

[3] https://impress-rail-project.eu/.

Projekt CBNRe4Rail – gotowość CBRNe dla węzłów transportu pasażerskiego[4]

Projekt rozpoczął się w 2025 r. i dotyczy wykrywania zagrożeń chemicznych, biologicznych, radiologicznych, nuklearnych (CBRNe) w transporcie kolejowym, zapobiegania im i reagowania na nie. Jego zadaniem jest zwiększenie świadomości i potencjału interesariuszy sektora kolejowego w zakresie skutecznego reagowania na te zagrożenia na dworcach kolejowych przez udoskonalenie ich planów bezpieczeństwa i przeszkolenie personelu kolejowego. Projekt obejmuje całe spektrum zagrożeń CBRNe, w tym materiały wybuchowe jako środek przenoszenia substancji CBRN. Koncentruje się na dworcach kolejowych jako głównej części składowej infrastruktury kolejowej i kluczowym elemencie podatności na zagrożenia w przestrzeni publicznej. Uwzględniono w nim zarówno przestrzeń publiczną wewnątrz dworców, jak i przestrzeń publiczną w ich pobliżu.

CBNRe4Rail jest finansowany przez Komisję Europejską. Jego inicjatorem jest UIC przy współpracy z Przedstawicielstwem PKP i pozostałymi partnerami.

Mobilne detektory materiałów wybuchowych i chemicznych dzięki współpracy z Komisją Europejską (DG HOME)

W zakresie poprawy bezpieczeństwa na polskiej kolei Przedstawicielstwo PKP ściśle współpracuje z DG HOME, w tym z jednostką ds. zwalczania terroryzmu. Dzięki tej współpracy Komisja Europejska nieodpłatnie udostępniła PKP i służbom (Policji oraz Straży Granicznej operującej na obszarach kolejowych) zaawansowane technologicznie mobilne detektory materiałów wybuchowych i chemicznych IONSCAN 600. Pierwotnie założono, że testy tych urządzeń na obszarach kolejowych w kraju potrwają sześć miesięcy. Pilotaż, który wystartował w listopadzie 2024 r., został jednak przedłużony przez Komisję Europejską do czerwca 2026 r. Ma on na celu zarówno wzmocnienie bezpieczeństwa operacji kolejowych w Polsce (detektory są używane m.in. na dworcach kolejowych, w pociągach, na kolejowych przejściach granicznych, w terminalach cargo, przy nadawaniu przesyłek konduktorskich), jak i określenie przydatności tych urządzeń na obszarach kolejowych.

[4] https://www.cbrne4rail.eu/.

W ramach przygotowań do pilotażu Przedstawicielstwo PKP zorganizowało w Warszawie spotkanie z dyrektorami ds. bezpieczeństwa ze spółek PKP (w tym Służbą Ochrony Kolei), a następnie warsztaty poświęcone zagrożeniom terrorystycznym i sabotażowym w transporcie kolejowym. Wzięli w nich udział eksperci z Komisji Europejskiej, Policji, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego oraz specjaliści ds. bezpieczeństwa w Grupie PKP. Ponadto Przedstawicielstwo PKP wspólnie z Komisją zorganizowało wiele spotkań warsztatowych, na których podsumowywano dotychczasowe doświadczenia polskich służb z wykorzystania detektorów. Do chwili obecnej użytkowanie tego sprzętu przynosi wymierne efekty.

Bezpieczeństwo na kolei w kontekście aktualnej sytuacji geopolitycznej

Ataki na infrastrukturę kolejową, systemy sygnalizacyjne, systemy zasilania są obserwowane od dłuższego czasu w wielu państwach europejskich z rozbudowanym systemem kolejowym. Polska nie jest odosobnionym przypadkiem. Do tego rodzaju zdarzeń doszło wielokrotnie w Niemczech i innych krajach, np. w przeddzień rozpoczęcia igrzysk olimpijskich w Paryżu. Dlatego sektor kolejowy współpracuje ze sobą w ramach kolejowych organizacji międzynarodowych. Cenna jest również kooperacja ze służbami. Warto podkreślić, że od stycznia 2026 r. PKP S.A. jako pierwsza kolej z krajów Europy Środkowo-Wschodniej obejmuje przewodnictwo w CER (The Community of European Railway and Infrastructure Companies)[5]. To efekt zaufania europejskich partnerów, z którymi Przedstawicielstwo PKP współpracuje, i dowód uznania dla jego pracy i zaangażowania w Brukseli. Kwestie dotyczące zwiększenia bezpieczeństwa i odporności europejskiego systemu kolejowego na pewno będą jednym z priorytetów przewodnictwa PKP S.A. w CER.

Wybuch wojny w Ukrainie wiąże się z pojawieniem wielu zagrożeń hybrydowych. Dotyczą one również kolei, ponieważ ten rodzaj transportu pozostaje kluczowy dla mobilności wojskowej. Europa musi wyciągnąć wnioski z doświadczeń Ukrainy – wzmacniać odporność i budować nowy ekosystem obronny, łączący przemysł, innowacje i nowe technologie. Ważne jest także zacieśnienie współpracy instytucji unijnych z NATO.

[5] https://www.cer.be/.

Grupa PKP pozostaje uczestnikiem tego dialogu, zarówno na poziomie unijnym, jak i w sferze doradztwa cywilnego dla Kwatery Głównej NATO.

W 1958 r. brytyjski premier Harold Macmillan powiedział: *Jaw, jaw is better than war, war,* co w swobodnym tłumaczeniu znaczy, że rozmowa jest lepsza od walki. Z pewnością dobrze by było, gdyby problemy rozwiązywano za pomocą dialogu. Wiadomo jednak, że jest to myślenie życzeniowe. Dlatego trzeba działać w sposób odstraszający, przewidywać, dostosowywać się, aktywnie budować odporność systemu kolejowego i łańcucha dostaw. Dotyczy to także innych wymiarów naszego bezpieczeństwa. Potrzebna jest intensywna współpraca na wielu płaszczyznach, oparta na zaufaniu i wspólnej wizji.

Tomasz Lachowicz

Dyrektor Przedstawicielstwa Polskich Kolei Państwowych w Belgii. Doradca cywilny (Senior Transport Advisor) i koordynator NATO Task Group ds. transportu kolejowego.

Ekspert w dziedzinie współpracy międzynarodowej, polityk unijnych, agendy transportowej Unii Europejskiej, lobbingu, kształtowania strategii działań i procesu decyzyjnego w UE. W latach 2021–2025 odpowiadał za przewodnictwo PKP w Międzynarodowym Związku Kolei (UIC) w Paryżu, a od stycznia 2026 r. będzie odpowiedzialny za koordynację przewodnictwa PKP we Wspólnocie Kolei Europejskich oraz Zarządców Infrastruktury Kolejowej (CER) w Brukseli.

Członek Komitetu Doradczego Rail Forum Europe w Parlamencie Europejskim.

Absolwent Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, Wydziału Prawa Uniwersytetu Kardynała Stefana Wyszyńskiego oraz podyplomowych studiów menadżerskich z zarządzania w gospodarce na SGH. Ukończył z wyróżnieniem studia MBA.

Odznaczony medalem Zasłużony dla Transportu RP.

Terroryzm – studia, analizy, prewencja, 2025, nr 8: 283–289

https://doi.org/10.4467/27204383TER.25.055.23042

Varia

Global Internet Forum to Counter Terrorism. Zwalczanie treści terrorystycznych i ekstremistycznych w przestrzeni cyfrowej

Global Internet Forum to Counter Terrorism (GIFCT) to niezależna organizacja non profit utworzona w 2017 r. w Stanach Zjednoczonych. Jej powstanie miało być odpowiedzią na nasilające się wykorzystanie platform internetowych i mediów społecznościowych przez organizacje terrorystyczne i ruchy ekstremistyczne do celów propagandowych, rekrutacyjnych, planowania aktów przemocy oraz do komunikacji operacyjnej. Inicjatorami były cztery wiodące podmioty sektora technologicznego: Meta Platforms, Inc. (dawniej Facebook), Microsoft Corporation, YouTube LLC (spółka zależna Google LLC) oraz X Corp. (dawniej Twitter).

Celem powołania GIFCT było stworzenie ram współpracy między sektorem prywatnym, administracją publiczną, organizacjami pozarządowymi oraz środowiskiem akademickim w zakresie wymiany informacji, opracowywania narzędzi technologicznych i wyznaczania standardów przeciwdziałania wykorzystywaniu przestrzeni cyfrowej do celów terrorystycznych i ekstremistycznych. Nadrzędnym zadaniem GIFCT jest zapobieganie nadużywaniu technologii cyfrowych przez podmioty promujące przemoc polityczną przez ograniczanie ich aktywności w przestrzeni online.

Jednym z kluczowych instrumentów operacyjnych organizacji jest hash-sharing database – wspólna baza danych zawierająca tzw. hashy, czyli cyfrowe odciski plików graficznych i wideo zidentyfikowanych jako materiały o charakterze

terrorystycznym lub ekstremistycznym. Baza ta umożliwia członkom GIFCT szybkie wykrywanie oraz usuwanie tego rodzaju treści z platform cyfrowych.

Kryteria przystąpienia do GIFCT obejmują m.in.:

- posiadanie publicznie dostępnych zasad i regulaminów zakazujących działalności terrorystycznej i ekstremistycznej,
- wdrożenie procedur przyjmowania i analizy zgłoszeń dotyczących naruszeń tych zasad i reagowania na nie,
- zaangażowanie w rozwój innowacyjnych narzędzi technologicznych służących przeciwdziałaniu terroryzmowi w środowisku cyfrowym,
- regularne publikowanie raportów dotyczących transparentności,
- zobowiązanie do poszanowania praw człowieka zgodnie z United Nations Guiding Principles on Business and Human Rights (tj. wytycznymi ONZ dotyczącymi biznesu i praw człowieka),
- wspieranie inicjatyw społeczeństwa obywatelskiego w zakresie zapobiegania terroryzmowi i ekstremizmowi.

Po pozytywnej weryfikacji aplikacji platforma uzyskuje status członka GIFCT. Dzięki temu ma zapewniony m.in. dostęp do bazy hash-sharing, może uczestniczyć w procesach komunikacji kryzysowej, brać udział w briefingu badawczym oraz ma pierwszeństwo w dostępie do warsztatów i seminariów.

Obecnie członkami GIFCT jest ponad 30 podmiotów z sektora technologicznego. Są to m.in. firmy: Meta Platforms, Microsoft, YouTube, X, Airbnb, Discord, Dropbox, LinkedIn, Amazon, Mailchimp, Pinterest, JustPaste.it, Tumblr, WordPress.com oraz Zoom.

Działalność badawczą GIFCT wspiera Global Network on Extremism and Technology (GNET) – projekt realizowany przez konsorcjum instytucji akademickich i think tanków, w tym International Centre for the Study of Radicalisation przy King's College London. Misją GNET jest prowadzenie interdyscyplinarnych badań nad sposobami wykorzystywania technologii przez podmioty terrorystyczne i ekstremistyczne oraz przekładanie wyników badań na rekomendacje polityczne i praktyczne (ang. *policy-relevant outputs*), wspierające sektor technologiczny, administrację publiczną i organizacje społeczeństwa obywatelskiego.

W kwietniu 2025 r. na zaproszenie Ministerstwa Spraw Zagranicznych RP gościła w Warszawie Naureen Chowdhury Fink, dyrektor wykonawcza GIFCT. Wzięła udział w nieformalnym spotkaniu Grupy Roboczej UE ds. Terroryzmu (aspekty międzynarodowe) COTER poświęconemu wyzwaniom i zagrożeniom ekstremistycznym oraz terrorystycznym dla państw Unii Europejskiej. Była to okazja do krótkiej rozmowy na temat organizacji, którą współkieruje.

Damian Szlachter: GIFCT staje się coraz bardziej znaczącą inicjatywą o globalnym zasięgu w działaniach na rzecz zwalczania terroryzmu oraz przemocy ekstremistycznej w sieci. Czy mogłaby Pani omówić formy współpracy, jakie oferujecie instytucjom publicznym i naukowym, szczególnie w krajach, które dopiero zaczynają budować swoje zdolności w tym obszarze, np. takich jak Polska?

Naureen Chowdhury Fink: Współpraca międzysektorowa to sedno naszej działalności. Jeśli chodzi o współpracę z instytucjami publicznymi i naukowymi, jako przykład chciałabym podać dział badań naukowych – GNET. Za pomocą tej sieci aktywnie zachęcamy do nadsyłania materiałów z całego świata[1], aby przygotowywane przez nas raporty, publikacje i analizy odzwierciedlały różne perspektywy i wyczerpująco informowały członków GIFCT o pojawiających się tendencjach i dynamice zmian, również w krajach takich jak Polska.

Inną ważną formą współpracy są regionalne warsztaty[2]. Często współtworzymy je razem z lokalnymi partnerami, aby zapewnić, że działania mające na celu zgromadzenie przedstawicieli rządu, sektora prywatnego oraz społeczeństwa obywatelskiego opierają się na znajomości regionu i jego kontekstu.

Zawsze zapraszamy firmy technologiczne do rozważenia członkostwa w GIFCT, jeśli tylko spełniają ustalone przez nas kryteria. Wszystkie informacje są dostępne online[3]. Chętnie przyjmiemy zgłoszenia od polskich firm technologicznych, które chcą włączyć się w te działania.

Jednym z ważniejszych wyzwań jest skuteczne definiowanie i rozpoznawanie treści terrorystycznych. W jaki sposób GIFCT uwzględnia różnice językowe, kulturowe i kontekstowe w ocenie takich materiałów?

To świetne pytanie. Bierzemy pod uwagę duże różnice kulturowe, kontekstowe, językowe i koncentrujemy się m.in.

[1] Zob. https://gnet-research.org/write-for-us/. Wszystkie przypisy pochodzą od redakcji.

[2] Zob. https://gifct.org/events/.

[3] Zob. https://docs.google.com/forms/d/e/1FAIpQLSfSaduWvuCUmU1P74HhEeAqT7tLu4VLx0863LuA0XWdV93BuQ/viewform.

na informowaniu naszych członków o dynamice w regionie, pojawiających się tendencjach oraz konkretnych zdarzeniach, aby pomóc im lepiej zrozumieć kontekst danej treści. Naszym celem jest zapewnienie członkom dostępu do światowej klasy ekspertów oraz odpowiedniej wiedzy specjalistycznej. Znaczna część tych działań jest realizowana dzięki GNET, a także innym inicjatywom GIFCT. Gdy firmy członkowskie są zainteresowane lepszym poznaniem danego regionu, mogą poprosić o materiały informacyjne dostosowane do ich potrzeb lub treści przygotowane na zamówienie. W takich przypadkach dążymy do tego, aby bezpośrednio połączyć firmy ze specjalistami z różnych dziedzin, którzy mogą pomóc odpowiedzieć na pytania i zapewnić dokładniejszy wgląd w niuanse kulturowe i kontekstowe, z którymi mogą się one spotkać.

GIFCT stworzyło hash-sharing database, czyli bazę danych zaprojektowaną w celu ułatwienia szybkiego usuwania treści terrorystycznych. W jakim stopniu to narzędzie okazało się skuteczne i czy mniejsze platformy cyfrowe są skłonne z niego korzystać?

Hash-sharing database zawiera ok. 2,3 miliona haszy, reprezentujących 408 000 różnych elementów treści[4]. Jesteśmy naprawdę zadowoleni z tego, jak przyjęto tę technologię – to pozytywny znak, że ponad 35 firm członkowskich, w tym wiele platform, korzysta z bazy w istotnym dla nich zakresie. Należy zauważyć, że nie wszystkie firmy członkowskie mają strukturę umożliwiającą bezpośrednie wykorzystanie haszy w swoich usługach. Wartość hash-sharing database wykracza poza samą technologię – sprzyja dialogowi między członkami na temat rodzajów zawartych w niej treści, sposobu ich integracji, a także możliwości wykorzystania tych informacji przez inne firmy. W niektórych przypadkach omawiamy również zasoby, które nie mogą być haszowane, a które mogą wspierać działania w zakresie moderacji treści czy te na rzecz bezpieczeństwa. Jesteśmy bardzo zadowoleni, że wiele firm członkowskich –

[4] Zob. https://gifct.org/hsdb/.

dużych i małych – dołącza do GIFCT i wykorzystuje potencjał tego wspólnego środowiska.

W ostatnich latach toczy się szeroka dyskusja dotycząca wpływu algorytmów na rozpowszechnianie w sieci treści terrorystycznych i ekstremistycznych. Czy GIFCT wdraża środki mające na celu złagodzenie tego wpływu na proces radykalizacji?

Sami nie tworzymy algorytmów, ale upewniamy się, że nasze firmy członkowskie są świadome badań i obaw związanych z tym zagadnieniem. Nasz Niezależny Komitet Doradczy (Independent Advisory Committee[5]) składa się z przedstawicieli z Unii Europejskiej, USA, Wielkiej Brytanii oraz z kilku innych krajów. Każdy z nich ma swoją perspektywę zarządzania systemem cyfrowym, ale wielu z nich podziela obawy dotyczące algorytmów i ich potencjalnego wpływu.

Częścią naszej pracy jest ułatwianie wymiany informacji – pomaganie naszym członkom w zrozumieniu, w jaki sposób pojawiają się te problemy, gdzie znajdują się niektóre proponowane rozwiązania, oraz zapewnienie im dostępu do najnowszych badań. Nie jesteśmy w stanie sami wprowadzić zmian, ale możemy zapewnić firmom członkowskim dostęp do zasobów i wiedzy potrzebnych do podejmowania świadomych decyzji.

Czy występują istotne różnice w podejściu do zwalczania terroryzmu w internecie pomiędzy krajami Europy Środkowej i Europy Wschodniej – takimi jak Polska – a Stanami Zjednoczonymi?

Jeśli chodzi o podejście do wyzwań takich jak zwalczanie treści internetowych, rzeczywiście dostrzegamy różnice w otoczeniu regulacyjnym – szczególnie między USA, Wielką Brytanią oraz Europą. Wiemy, że jest to coś, nad czym firmy technologiczne pracują, dostosowując swoje działania. Myślę, że te różnice widać zarówno w przepisach, jak i w tym, jak różnie

[5] Zob. https://gifct.org/governance/.

zainteresowane strony postrzegają pewne rodzaje treści i gdzie wyznaczają granice. Na przykład w Stanach Zjednoczonych wiele wypowiedzi jest chronionych przez pierwszą poprawkę (do Konstytucji Stanów Zjednoczonych Ameryki – dop. red.) i wiem, że wielu naszych europejskich kolegów ma czasem z tym problem. Zatem tak, różnice zdecydowanie istnieją. Mimo to uważam, że są również podobieństwa – szczególnie w obszarach, gdzie granice są bardziej wyraźne. W takich przypadkach panuje zazwyczaj większy konsensus niż niezgoda i próbujemy koncentrować się na tym pozytywnym aspekcie.

GIFCT to także forum dialogu międzysektorowego. W jaki sposób angażujecie środowiska akademickie oraz specjalistów z różnych dziedzin w opracowywanie skutecznych strategii przeciwdziałania w internecie przemocy o podłożu ekstremistycznym?

Dialog międzysektorowy to kluczowa metoda działania GIFCT. Nasze warsztaty, sieć badawcza oraz bieżąca współpraca z firmami członkowskimi służą temu, aby te odmienne środowiska mogły uczyć się od siebie nawzajem i czerpać korzyści z posiadanych zasobów i wiedzy specjalistycznej. Często obserwujemy w różnych sektorach, że nie zawsze istnieje dogłębne zrozumienie, jak działają inni oraz jakimi narzędziami i zasobami dysponują. Ważną częścią naszych zadań jest łączenie tych społeczności. Niezależnie od tego, czy chodzi o organy ścigania i praktyków czy o naukowców i sektor prywatny, staramy się stwarzać im możliwości bezpośredniego zaangażowania oraz dzielenia się wiedzą.

Polska mierzy się z kampaniami dezinformacyjnymi, a także próbami radykalizacji w przestrzeni internetowej, zwłaszcza w związku z konfliktem za wschodnią granicą. Czy GIFCT analizuje przypadki z tego regionu w ramach badania współczesnych zagrożeń hybrydowych?

Z pewnością postrzegamy zagrożenia hybrydowe jako niebezpieczeństwo dla wielu firm i dlatego współpracujemy z różnymi działami tych firm i z decydentami, inżynierami czy

badaczami. Próbujemy tworzyć wspólną bazę wiedzy dla nich wszystkich.

Dysponujemy raportami[6], w których często są opisywane kwestie związane z zagrożeniami hybrydowymi, w tym w regionie, o którym wspomniałeś. Raporty te pomagają uwidocznić niektóre zjawiska zachodzące w regionie, które są szczególnie istotne w miejscach takich jak Polska. Ponadto, kiedy pojawiają się incydenty, także nasz Ramowy System Reagowania na Incydenty (Incident Response Framework[7]) może pomóc skupić uwagę na wybranych problemach związanych z zagrożeniami hybrydowymi. W ten proces angażujemy nasze firmy członkowskie, aby lepiej zrozumieć zachodzące zjawiska. Tak, jest to kwestia, z którą mamy do czynienia w naszej pracy.

Biorąc pod uwagę rozwijający się sektor technologiczny oraz wykwalifikowanych specjalistów IT w Polsce, proszę powiedzieć, czy nasz kraj ma potencjał, aby zostać regionalnym centrum innowacji w zakresie walki z radykalizacją w sieci i wspierania współpracy z GIFCT?

Z pewnością tak. Zachęcamy polskie firmy technologiczne oraz te powiązane z technologią, aby nawiązywały współpracę z nami i pomagały pogłębiać naszą wiedzę o zagrożeniach i trendach występujących w Polsce oraz aby ubiegały się o członkostwo w GIFCT. Zapraszamy również polskich badaczy, aby współtworzyli sieć GNET, która jest w pełni dostępna online. Dla autorów chcących publikować swoje artykuły są przewidywane mikrodotacje. To pozwala na przedstawienie szerokiego spektrum perspektyw. Jeśli istnieją organizacje powiązane z technologią lub pojawiają się nowe kwestie, o których powinniśmy wiedzieć, chętnie rozważymy możliwość zorganizowania przedsięwzięć czy spotkań, które mogłyby ułatwić dalszy dialog i współpracę.

Rozmawiał: Damian Szlachter

---

[6] Zob. https://gifct.org/gifct-resources-and-publications/.

[7] Zob. https://gifct.org/incident-response/.

TERRORISM

studies
analyses
prevention

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Editorial team Damian Szlachter, PhD (editor-in-chief)
Aleksandra Komar, PhD (deputy editor-in-chief)
Agnieszka Dębska (editorial secretary, layout editor)

Translation Sylwia Kłobuszewska

Cover design Aleksandra Bednarczyk

ISSN 2720-4383
e-ISSN 2720-6351

Material posted in the Articles section and review articles posted in the Review Articles/Reviews section are subject to peer-reviewed

Articles express the views of the authors

Declaration of the original version:
The printed version of the journal is the original version
The online version of the journal is available at www.abw.gov.pl/wyd/

The journal is available on the Jagiellonian University Scientific Journals Portal at: https://www.ejournals.eu/Terroryzm/

Articles for the journal should be submitted through the editorial panel available at: 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, Poland

Contact
phone (+48) 22 58 58 695
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Printed in December 2025

Print
Mazowieckie Centrum Poligrafii Sp. z o.o.
ul. Ciurlionisa 4, 05-270 Marki
mobile: 505 727 782

TABLE OF CONTENTS

297 **Foreword by Editor-in-Chief**

ARTICLES

303 **Bioterrorism in the agri-food sector – underestimated risk and challenges for biosecurity based on selected countries**
Matylda Augustyn-Barwicz

341 **Twenty years since the attacks on London's public transport system. The problem of Islamic terrorism in the United Kingdom**
Krzysztof Izak

389 **Terrorist threats in the European Union in 2024. Analysis of the TE-SAT. European Union Terrorism Situation and Trend Report 2025**
Sebastian Wojciechowski, Artur Wejkszner

411 **The role and significance of Eurojust in countering terrorism**
Dariusz Pożaroszczyk

REVIEW ARTICLES / REVIEWS

439 **Jerzy Trocha,**
Paradigm of railway station security
Jacek Lasota, Małgorzata Lasota

AWARDED THESES

449 **Capabilities of the Armed Forces of the Republic of Poland in the area of decontamination – selected aspects**
Krzysztof Tokarczyk

VARIA

487 **How can local governments protect public spaces from vehicle attacks?**
Mariusz Cichomski

Appendix
Protecting public spaces from vehicle attacks – recommendations for local governments

517 **Terrorists, saboteurs, spies in Polish prisons – the role of the Prison Service**
Andrzej Leńczuk

537 **From phishing to sabotage – the evolution of cyber threats to Poland. Conclusions from CSIRT GOV report for 2024**
Monika Stodolnik

551 **Building resilience of the European railway sector to hybrid threats. Polish contribution to good practices and increased safety**
Tomasz Lachowicz

561 **Global Internet Forum to Counter Terrorism. Combating terrorist and extremist content in the digital space**
Interview with executive director of the GIFCT Naureen Chowdhury Fink

Ladies and Gentlemen!

When we began work on our next issue of the journal "Terrorism – Studies, Analyses, Prevention" (T-SAP) a few months ago, we did not expect this edition to be so relevant in terms of the topics it covers. The materials presented in it are in line with current research and practical needs related to the dynamically changing reality, including in the area of terrorist threats, and the issues addressed concern the vital challenges facing the institutions responsible for security.

Since the outbreak of the war in Ukraine, we have seen an intensification of active operations carried out in European Union countries by Russian special services and their proxies against commercial, water and sewage facilities, and strategic infrastructure in the transport, energy and communications sectors. This has been the subject of numerous analyses. It is worth mentioning a report prepared in 2025 by renowned think tanks – Slovak GLOBCES and Dutch ICCT. It presents clear data on the hybrid activities of the Russian Federation in Europe, including in Poland, carried out, among others, with the support of criminal groups. These activities also include terrorist offences. We publish statistics on the number of people held in penitentiary units, among other things, in connection with activities for foreign intelligence services and crimes of this kind. An example of this are the acts of sabotage targeting Polish railway infrastructure, which took place on 15–17 November 2025 on the strategic transport line from Warsaw to Dorohusk, on the border with Ukraine. In this issue of T-SAP, you will find material – highly relevant in this context – on building the resilience of the European railway sector to hybrid threats and the role of Poland in

this area. Representative Office of PKP S.A. (Polskie Koleje Państwowe) in Brussels is taking many measures at EU level that are effectively improving safety in this sector. It covers many elements, one of the key ones being railway stations. The issue of their protection in Poland is the subject of a unique book published in 2025 by the War Studies University. The monograph entitled *Paradigm of railway station security*, which we are reviewing here, deserves attention not only from security and defence experts, but also from anyone interested in the functioning of the railways as part of the state's critical infrastructure. To conclude the main theme of this issue, namely threats in the transport sector, I encourage you to read an article presenting the history of attacks on London's public transport system in 2005. They were among the most tragic acts of terrorism in Europe. Among the numerous victims were three Polish women. These events have had a significant impact on changing the approach to counter-terrorism at national and EU level.

In T-SAP, we regularly present strategic documents concerning the fight against terrorism. This time the experts discussed this year's most important Europol, Eurojust and CSIRT GOV reports. Their analysis provides a better understanding of the scale and dynamics of changes in the phenomenon of terrorism, identifies challenges and good practices in combating it and highlights the importance of international cooperation.

In the previous issue, we included a comment on the amendment to the Polish Act on anti-terrorist activities in connection with counteracting the dissemination of terrorist content on the internet. Continuing this theme, in this issue we publish an interview with the director of the Global Internet Forum to Counter Terrorism, who talks about combating terrorist and extremist content in the digital space and the role of this body (which brings together over 30 of the world's largest technology companies) in strengthening international security.

We also continue to address the issue of gaps in the actions of European Union countries in the area of counter-terrorism.

One of these gaps is the possibility of using biological agents for terrorist acts against agri-food sector. This risk remains underestimated in the security policies of many countries, especially in terms of assessing the likelihood of its occurrence and potential consequences. The article devoted to the issue of bioterrorism shows how important it is to strengthen the capacity of countries to respond effectively to biological threats. The content presented in it is forward-looking and provides a direction for further analysis and scientific research. The article on the ability of the Armed Forces of the Republic of Poland to eliminate contamination fits into the area of issues related to resistance to biological threats, as well as chemical and radioactive threats. Its author proposes the modernisation of equipment, standardisation of procedures and strengthening of cooperation between the military and non-military entities.

We strive to support projects and initiatives that build and strengthen resilience to terrorist acts. We welcome the creation of guidelines for local governments on protecting public spaces from attacks using vehicles. These were prepared by the Ministry of the Interior and Administration and the National Police Headquarters with the support of other institutions in the counter-terrorism system in Poland. Considering how important these recommendations are, especially during the Christmas and New Year period, when seasonal fairs are organised, attracting large crowds, we asked the co-author of this project to discuss it. It is worth noting that among the expert sources cited in these guidelines are studies published in T-SAP.

We are pleased that our efforts are also recognised abroad. It is a nice touch to receive congratulations from Edward Lucas – a global authority on hybrid activities carried out by the Russian Federation towards NATO countries. He praised the special edition of T-SAP devoted to the protection of critical infrastructure against terrorist and sabotage activities, prepared by the Internal Security Agency and the Government Centre for Security. This is further proof that we are moving in the right direction. This is possible thanks to our authors, reviewers, members of the Academic Editor Board as well as

the efforts of the editorial team, whom I would like to thank for their commitment and professionalism.

Finally, I would like to welcome Aleksandra Komar, PhD, who has become the deputy editor-in-chief and, together with the team, has co-authored this issue of T-SAP. I am convinced that thanks to her support, the journal will develop more intensively, not only in scientific terms.

Editor-in-Chief
Damian Szlachter, PhD

ARTICLES

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 303–340

https://doi.org/10.4467/27204383TER.25.056.23043

Article

Bioterrorism in the agri-food sector – underestimated risk and challenges for biosecurity based on selected countries

MATYLDA AUGUSTYN-BARWICZ https://orcid.org/0009-0006-2882-8311
The Pirbright Institute

Abstract

The aim of this article is to describe bioterrorism threats to the agri-food sector, with particular emphasis on agroterrorism, the risk of which remains underestimated in the security policies of many countries, especially in terms of assessing its likelihood and potential consequences. Achieving this objective involves solving the research problem formulated in the form of a question: What are the bioterrorism threats to the agri-food sector? An attempt to solve this problem was made on the basis of a review of literature and legal acts, using theoretical research methods such as analysis, synthesis, abstraction and inference. Despite the recognition of the food production sector as part of critical infrastructure, there is a lack of scenarios and procedures for responding to intentional contamination. The article describes the definitions of bioterrorism, agroterrorism and agrocrime, as well as the classification of biological threats. It compares biosafety systems in selected countries, emphasises the importance of local entities in early warning systems, and points to the broader context of safety – food protection, animal and human health, which, according to the One Health concept, form an interconnected whole requiring coordinated management. The conclusions emphasise the need to develop interoperable surveillance systems, high-level biosafety

laboratories, education and digitalisation, as well as to include the agri-food sector in national and EU security strategies, thereby strengthening Europe's biological resilience to hybrid threats.

Keywords

bioterrorism, agroterrorism, food security, One Health, biological threats

Introduction

Agri-food sector constitutes an attractive target for hybridtype operations due to its large geographical extent, the complexity of associated logistical processes and a relatively low level of physical security. Biological attacks in this sector are often asymmetric – the aggressor employs cheap, unconventional and hard-to-detect methods, while the defender must incur high costs to protect against them and respond to their effects, yet these attacks remain highly effective. Their consequences may include mass culling of livestock, disruption of supply chains, rising food prices, moral panic and a loss of trust in public institutions[1]. In the face of globalisation and climate change, the risk of transboundary spread of pathogens is increasing, giving such phenomena an international dimension.

In response to these problems, the One Health concept was developed, which links human, animal and environmental health with elements of internal security and promotes an integrated, interdisciplinary approach to effectively prevent such threats. It is being developed by the World Health Organization (WHO), the World Organisation for Animal Health (WOAH) and the Food and Agriculture Organization of the United Nations (FAO).

An analysis of the security strategies of selected EU Member States shows that the risk of agroterrorism threats remains underestimated. Neither Poland nor Germany, France and Italy has developed separate response plans for attacks targeting agri-food sector. A similar gap can be observed in the United Kingdom, where, despite advanced plant biosecurity

[1] J.P. Dudley, M.H. Woodford, *Bioweapons, bioterrorism and biodiversity: potential impacts of biological weapons attacks on agricultural and biological diversity*, "Revue Scientifique et Technique" 2002, no. 21(1), pp. 125–137. http://dx.doi.org/10.20506/rst.21.1.1328.

strategies and analyses of the resilience of the food supply chain, there is no separate, comprehensive plan for responding to agroterrorism attacks.

The aim of the article was to analyse threats to the agri-food sector in selected countries. The research issues were focused around the following questions:

1. In what way does bioterrorism, and especially agroterrorism, pose a threat to agri-food sector in selected countries?
2. Why does the risk of agroterrorism remain underestimated in security policies, and how is the perception of this threat shaped by society and authorities at the local and central levels?
3. What role do farmers, veterinarians and local authorities play in local early warning and operational readiness systems?
4. What systemic actions – institutional, technological and educational – can enhance the biological resilience of the agricultural sector at both national and the EU levels?

Definitions: bioterrorism, agrocrime and agroterrorism

Bioterrorism poses a growing challenge to the internal security, public health and economic stability of states. The WHO and the WOAH define it as a deliberate use of biological agents – pathogenic microorganisms or biological toxins – against people, animals or plants in order to cause social, political or economic harm[2]. The WOAH distinguishes also the term agrocrime, referring to unlawful activities involving animals or products of animal origin that threaten public health, animal welfare or food safety. These include, among others: food product adulteration, i.e. altering their composition or quality to reduce production costs, smuggling, food fraud, i.e. misleading consumers for profit (e.g. false claims about origin or composition), as well as the deliberate release of pathogens. It is worth to emphasise that the range of agrocrime is broader than implied by the definition of the WOAH, which refers exclusively to animals and products of animal origin. These also include crimes involving plants,

[2] *Laboratory Biosafety Manual. Fourth Edition*, WHO, 21 XII 2020, https://www.who.int/publications/i/item/9789240011311 [accessed: 10 VI 2025]; *Terrestrial Animal Health Code*, https://rr-africa.woah.org/app/uploads/2023/09/en_csatvol1-2023.pdf [accessed: 14 VI 2025].

agricultural inputs, food trade, product adulteration and illegal seed trading[3].

Agroterrorism constitutes a specific form of agrocrime motivated by political and ideological factors. Its aim is destabilisation of society through the outbreak of animal or plant diseases. The difference between these categories stems from motivation. In agrocrime, the primary goal is economic, while in agroterrorism, it is political or social[4].

In its strategies, the WOAH has gradually expanded its approach to such threats. The document of 2015 focused on reducing biological risk through biosecurity and international cooperation, while the 2024 strategy formally introduced the concepts of agrocrime and agroterrorism and emphasised prevention, threat detection, and the coordination of veterinary services, law enforcement agencies and security institutions[5].

Although the food production sector has been recognised as an element of critical infrastructure in the Directive (EU) 2022/2557 of the European Parliament and of the Council (commonly referred to by the abbreviation CER Directive, from English: Critical Entities Resilience)[6] and in the plans of the North Atlantic Treaty Organization (NATO)[7], there is still a lack of response plans and consistent implementation of biosecurity principles. The Union perceives bioterrorism as the intentional use of pathogens and toxins to intimidate the population and destabilise state structures, the WOAH defines it as the deliberate introduction of infectious diseases into livestock or wildlife populations, and NATO classifies it within the framework of CBRN (chemical, biological, radiological and nuclear) threats[8]. These definitional and priority discrepancies further complicate

[3] E. Barclay, *A Review of the Literature on Agricultural Crime. Report to the Criminology Research Council,* https://criminology.fsu.edu/sites/g/files/upcbnu3076/files/2021-03/A-Review-of-the-Literature-on-Agricultural-Crime.pdf, pp. 5–18, 46–76 [accessed: 2 XII 2025].

[4] J.P. Dudley, M.H. Woodford, *Bioweapons, bioterrorism and biodiversity*…

[5] *Biological threat reduction strategy. Strengthening global biological security*, https://www.woah.org/app/uploads/2021/03/biothreat-strategy-veng-revised-1st-edition.pdf, pp. 3–12 [accessed: 14 VI 2025]; *Building resilience against agro-crime and agro-terrorism*, https://www.woah.org/app/uploads/2023/02/building-resilience-against-agro-crime-and-agro-terrorism.pdf, pp. 1–10 [accessed: 14 VI 2025].

[6] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*.

[7] *NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy*, NATO, 14 VII 2022, https://www.nato.int/cps/en/natohq/official_texts_197768.htm [accessed: 2 XII 2025].

[8] Ibid.

the development of coherent strategies for preventing and responding to bioterrorism incidents in the agri-food sector[9].

Agri-food sector as a potential target of bioterrorism attack

Agri-food sector constitutes one of the most important elements of the critical infrastructure, and at the same time one of the most vulnerable to bioterrorism activities. The complexity of the food production system – including production, transport, processing, storage and distribution – means that there are many points at which interference can occur, including contamination of raw materials, feed or water. Even incidents of a local nature may lead to a cascading effect resulting in serious health, economic and social consequences[10]. A critical element of the system remains logistics based on the *just-in-time* model. It is cost-effective but limits the ability to respond to sudden disruptions.

The COVID-19 pandemic and changes related to Brexit revealed the vulnerability of food supply chains[11]. The European Commission emphasises the need to increase the resilience of this sector through diversification of supply sources, the creation of strategic reserves, and the strengthening of early warning mechanisms[12]. The European Food Safety Authority (EFSA) studies also indicate that food security should be analysed in the context of health, logistical and political factors, considered together and requiring a collective approach to risk management[13].

[9] *Deliverable D6.5 – Guiding Document on cross-sectoral preparedness and response to biological and/or chemical terror attack. Collaboration between health, civil protection and security*, https://www.jaterror.eu/wp-content/uploads/2024/11/6.5-Guiding-Document.pdf, p. 17, 19–26, 33, 41 [accessed: 8 XII 2025].

[10] *The European Union One Health 2023 Zoonoses Report*, EFSA, 10 XII 2024, https://doi.org/10.2903/j.efsa.2024.9106.

[11] P. Garnett, B. Doherty, T. Heron, *Vulnerability of the United Kingdom's food supply chains exposed by COVID-19*, "Nature Food" 2020, no. 1, pp. 315–318. https://doi.org/10.1038/s43016-020-0097-7.

[12] *Proofing the EU food supply chains against crises: new set of recommendations published*, European Commission, 23 VII 2024, https://agriculture.ec.europa.eu/media/news/proofing-eu-food-supply-chain-against-crises-new-set-recommendations-published-2024-07-23_en [accessed: 14 VI 2025].

[13] *Food Risk Assess Europe*, EFSA, https://www.efsa.europa.eu/en/publications/food-risk-assess-europe [accessed: 13 XII 2025].

In the case of biological threats, crisis logistics is crucial for the effective isolation of infection outbreaks, efficient distribution of vaccines and maintenance of alternative supply channels[14]. Transportation disruptions – resulting from sanitary blocks or border closures – can significantly complicate intervention efforts and amplify negative economic impacts. The psychological dimension of the attacks is equally important. Bioterrorism targeting the agri-food sector can trigger social panic, leading to consumer panic, product boycotts and disinformation – often with consequences more severe than the incident involving biological agents[15].

An example of a bioterrorism attack in the food sector is the mass poisoning of food by members of the Rajneesha cult. The incident occurred in Oregon (the US) in 1984 – bacteria *Salmonella typhimurium* were released in the restaurants, causing over 750 illnesses[16]. Although such attacks are rare, they show the scale of the consequences that intentional food contamination can have.

A bioterrorism attack may also involve infecting livestock with highly contagious pathogens that cause diseases such as anthrax, foot and mouth disease (FMD) or African swine fever (ASF)[17]. This can lead to an epizootic, meaning a mass occurrence of infectious diseases among

[14] W.S. Carus, *Bioterrorism and Biocrimes: the Illicit Use of Biological Arms in the 20th Century*, August 1998, https://wmdcenter.ndu.edu/Publications/Publication-View/Article/626562/bioterrorism-and-biocrimes-the-illicit-use-of-biological-arms-in-the-20th-centu/ [accessed: 14 VI 2025].

[15] *First report on world's animal health reveals changing spread of disease impacting food security, trade and ecosystems*, WOAH, 23 V 2025, https://www.woah.org/en/first-report-on-worlds-animal-health-reveals-changing-spread-of-disease-impacting-food-security-trade-and-ecosystems/ [accessed: 15 VI 2025]; *What past disruptions can teach us about reviving supply chains after COVID-19*, World Economic Forum, 27 III 2020, https://www.weforum.org/stories/2020/03/covid-19-coronavirus-lessons-past-supply-chain-disruptions/ [accessed: 27 V 2025]; D. Ivanov, A. Dolgui, *Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak*, "International Journal of Production Research" 2020, vol. 58, no. 10, pp. 2904–2915. https://doi.org/10.1080/00207543.2020.1750727.

[16] T.J. Török et al., *A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars*, "The Journal of the American Medical Association" 1997, vol. 278, no. 5, pp. 389–393. https://doi.org/10.1001/JAMA.1997.03550050051033.

[17] M. Wheelis, R. Casagrande, L.V. Madden, *Biological Attack on Agriculture: Low-Tech, High-Impact Bioterrorism: Because bioterrorist attack requires relatively little specialized expertise and technology, it is a serious threat to US agriculture and can have very large economic repercussions*, "BioScience" 2002, vol. 52, no. 7, pp. 569–576. https://doi.org/10.1641/0006-3568(2002)052[0569:BAOALT]2.0.CO;2.

animals in a specific area and time, and can result in negative economic consequences. An example is FMD epizootic that occurred in the UK in 2001. During its course, over 2000 disease outbreaks were recorded and more than 6 million farm animals were culled. The economic losses were estimated at around GBP 8 billion, including 3 billion in the agriculture sector and 5 billion in the tourism and recreation sector. This incident was not an act of bioterrorism, but it revealed the economic, social and psychological consequences of the spread of infectious animal diseases and contributed to the reform of the UK's agricultural crisis management system[18].

The deliberate introduction of pathogens into the agri-food sector could cause effects comparable to a natural epizootic. In June 2025, the US authorities accused Chinese scientists – Yunqing Jian and Zunyong Liu – of attempting to smuggle into the US a dangerous plant pathogen – the fungus *Fusarium graminearum*[19]. This species attacks wheat, barley, corn and rice, causing fusarium head blight. It can cause significant crop losses and contaminate the grain with dangerous mycotoxins – primarily deoxynivalenol, which can induce, among other things, vomiting, liver damage, immunosuppression and reproductive disorders in humans and animals. *Fusarium graminearum* is considered an organism that could be used as a weapon in bioterrorism operations due to the ease of obtaining it, its environmental resilience and its ability to spread rapidly within agricultural systems[20]. Local contamination of seeds or planting material alone is enough to introduce it into the food production chain on a regional or international scale[21]. The described incident involving Chinese scientists

[18] D. Thompson et al., *Economic costs of the foot and mouth disease outbreak in the United Kingdom in 2001*, "Revue Scientifique et Technique" 2002, no. 21(3), pp. 675–687. https://doi.org/10.20506/RST.21.3.1353.

[19] *Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory*, United States Attorney's Office, 3 VI 2025, https://www.justice.gov/usao-edmi/pr/chinese-nationals-charged-conspiracy-and-smuggling-dangerous-biological-pathogen-us [accessed: 20 VI 2025].

[20] E. White, *US says it broke up effort to bring toxic fungus to Michigan lab from China*, AP News, 3 VI 2025, https://apnews.com/article/chinese-scientists-charged-toxic-fungus-5ccaba9aff8e5941ebcea71b9b6690b2 [accessed: 20 VI 2025].

[21] A. Ramakrishnan, *What is Fusarium graminearum, the fungus US authorities say was smuggled in from China?*, AP News, 4 VI 2025, https://apnews.com/article/fusarium-graminearum-fungus-head-blight-china-8ce925ae96d9c437b987e58c336cd45f [accessed: 20 VI 2025].

confirms that concerns about biological protection measures and the use of plant pathogens as tools of agroterrorism are justified.

Typologies of biological agents that could be used as weapons against the agri-food sector

To capture the full spectrum of threats arising from the deliberate use of biological agents in the agri-food sector, it is useful to distinguish the main categories of means that may be used in agroterrorism activities.

Animal pathogens

Among the most dangerous epizootics is ASF. The virus that causes it is characterised by nearly 100% mortality in pigs and wild boars, as well as high resistance to adverse environmental conditions. Since 2014, Europe and Asia have suffered significant losses due to it[22]. Equally serious is highly pathogenic avian influenza (HPAI), particularly caused by subtypes of the influenza A virus – H5N1 and H5N8, which leads to mass culling of poultry, export bans and losses amounting to billions of dollars[23]. The effects of an extreme zoonosis were observed in 2001 during the aforementioned FMD epidemic.

Plant pathogens

A similar destabilising potential is exhibited by plant pathogens that could be used to disrupt the production of grains, fruit and vegetables. An attempt to smuggle *Fusarium graminearum* fungal spores into the US was treated as an incident with potential bioterrorism implications. Other high-risk pathogens include: bacteria *Xylella fastidiosa* infecting olive and citrus trees in Southern Europe, the Ug99 strain of wheat stem rust (caused by the fungus *Puccinia graminis forma tritici*)[24] and bacteria *Ralstonia*

[22] *African swine fever*, EFSA, 19 V 2025, https://www.efsa.europa.eu/en/topics/topic/african-swine-fever [accessed: 16 VI 2025].

[23] G. Pavade, *WOAH Updates – Global HPAI situation and current standards and recommendations regarding AI surveillance and vaccination*, https://www.izsvenezie.com/documents/reference-laboratories/avian-influenza/workshops/2022/pavade.pdf [accessed: 16 VI 2025].

[24] *USDA Coordinated Approach to Address New Virulences in Wheat and Barley Stem Rust – Pgt-Ug99*, United States Department of Agriculture, 20 IX 2017, https://www.ars.usda.gov/ug99/ [accessed: 16 VI 2025]; R.P. Singh et al., *The emergence of Ug99 races of the stem rust fungus*

solanacearum attacking potatoes and tomatoes[25]. These pathogens have been included in the national biosecurity strategies of many countries, including the US[26], Australia and Germany[27].

Vector-borne pathogens

Another category consists of vector-borne pathogens transmitted by organisms such as:

- mosquitoes (*Aedes sp., Culex sp.*), which can transmit dengue, Zika, yellow fever and West Nile viruses,
- ticks (*Ixodes spp.*), which can transmit bacteria *Borrelia burgdorferi* (causing Lyme disease), tick-borne encephalitis virus and bacteria *Anaplasma phagocytophilum* (causing anaplasmosis in animals and humans),
- midges (*Culicoides spp.*), which can transmit viruses causing diseases: Bluetongue Disease and African horse sickness[28].

---

is a threat to world wheat production, "Annual Review of Phytopathology" 2011, no. 49, pp. 465–481. https://doi.org/10.1146/annurev-phyto-072910-095423.

[25] *What is EPPO Global Database?*, https://gd.eppo.int/ [accessed: 10 VI 2025].

[26] *National biodefense strategy and implementation plan for countering biological threats, enhancing pandemic preparedness, and achieving global health security*, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf [accessed: 10 VI 2025]; *National Priority Plant Pests (2024)*, Australian Government. Department of Agriculture, Fisheries and Forestry, https://www.agriculture.gov.au/biosecurity-trade/pests-diseases-weeds/plant/national-priority-plant-pests/ [accessed: 10 VI 2025].

[27] *Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy*, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf [accessed: 11 VI 2025].

[28] *Transmission of Zika Virus*, Centers for Disease Control and Prevention, 30 I 2025, https://www.cdc.gov/zika/php/transmission/index.html [accessed: 10 IX 2025]; *Dengue*, World Health Organization, 21 VIII 2025, https://www.who.int/news-room/fact-sheets/detail/dengue-and-severe-dengue [accessed: 10 IX 2025]; *Aedes aegypti – Factsheet for experts*, European Centre for Disease Prevention and Control, 2 I 2023, https://www.ecdc.europa.eu/en/disease-vectors/facts/mosquito-factsheets/aedes-aegypti [accessed: 10 IX 2025]; *West Nile: Causes and How It Spreads*, Centers for Disease Control and Prevention, 19 VIII 2025, https://www.cdc.gov/west-nile-virus/causes/index.html [accessed: 10 IX 2025]; *Tick-Borne Encephalitis*, Centers for Disease Control and Prevention, 23 IV 2025, https://www.cdc.gov/yellow-book/hcp/travel-associated-infections-diseases/tick-borne-encephalitis.html [accessed: 10 IX 2025]; *Factsheet about tick-borne encephalitis (TBE)*, European Centre for Disease Prevention and Control, 22 I 2024, https://www.ecdc.europa.eu/en/tick-borne-encephalitis/facts/factsheet [accessed: 10 IX 2025]; *How Lyme Disease Spreads*, Centers for Disease Control and Prevention, 24 IX 2024, https://www.cdc.gov/lyme/causes/index.html

Pathogens such as bacteria: *Francisella tularensis* (causes tularemia), *Coxiella burnetii* (causes Q fever) and of the genus *Brucella spp.* (cause brucellosis) are recognised by the US Centers for Disease Control and Prevention (CDC) as potential bioterrorism agents due to the ease of their aerosolisation and difficulties in identification, which pose a challenge for surveillance and response systems[29].

Elements of the natural environment as reservoirs of pathogens

Elements of the natural environment are important, though often underestimated, reservoirs of potential biological threats that may affect the agriculture and food production sectors. Unlike classical carriers, the water-soil environment can act as a long-term reservoir for pathogens, enabling their survival and covert spread[30]. In bioterrorism scenarios, water may be deliberately contaminated, for example by introducing pathogens into water reservoirs or irrigation systems. The difficulty in detecting an infection and its delayed symptoms make such actions a particular challenge for early-warning systems, especially in the case of plant epiphytotics such as potato late blight (caused by the oomycete *Phytophthora infestans*), cereal powdery mildew (caused by the fungus *Blumeria graminis*), maize fusariosis (caused by fungi of the genus *Fusarium spp.*), or bacterial rots of fruit trees (caused by bacteria *Erwinia*

[accessed: 10 IX 2025]; *About Anaplasmosis*, Centers for Disease Control and Prevention, 4 IX 2024, https://www.cdc.gov/anaplasmosis/about/index.html [accessed: 10 IX 2025]; *Bluetongue*, World Organisation for Animal Health, https://www.woah.org/en/disease/bluetongue/ [accessed: 10 IX 2025]; *Bluetongue*, U.S. Department of Agriculture, Animal and Plant Health Inspection Service, https://www.aphis.usda.gov/livestock-poultry-disease/cattle/bluetongue [accessed: 10 IX 2025].

[29] *CDC Bioterrorism Agents*, https://biosecurity.fas.org/resource/documents/CDC_Bioterrorism_Agents.pdf [accessed: 10 VI 2025]; *Emergency preparedness, resilience and response concept of operations*, UK Health Security Agency, 15 I 2025, https://www.gov.uk/government/publications/emergency-preparedness-resilience-and-response-concept-of-operations/emergency-preparedness-resilience-and-response-concept-of-operations [accessed: 10 VI 2025]; D.T. Dennis et al., *Tularemia as a biological weapon: medical and public health management*, "The Journal of the American Medical Association" 2001, vol. 285, no. 21, pp. 2763–2773. https://doi.org/10.1001/JAMA.285.21.2763; *Bluetongue*, World Organisation for Animal Health...

[30] *Guidelines for drinking-water quality: fourth edition incorporating the first addendum*, Geneva 2017.

amylovora) – diseases that spread massively within crop plant populations and are difficult to detect in the early warning phase[31]. Water used for irrigation, watering livestock or washing crops, can become a source of contamination with zoonotic and foodborne pathogens such as bacteria: *Escherichia coli*, *Listeria monocytogenes*, of the genus *Salmonella spp.* or noroviruses[32]. The greatest risk concerns products consumed raw, such as leafy vegetables and berries. Sources of contamination may include animal feces, farm runoff and wastewater from treatment plants, but they may also result from bioterrorism activities.

Soil, dust and aerosols can carry bacterial spores such as *Bacillus anthracis*, which remain viable for decades and can cause secondary outbreaks of infection[33]. The negative consequences – both epidemiological and economic – are exacerbated by the spores' ability to survive in the environment[34] for long periods and their potential to trigger sudden, difficult-to-control epidemics[35]. This burdens healthcare systems, destabilises agricultural production and generates significant financial losses[36].

'One Health' concept – integrated framework for protection against bioterrorism threats

In the past decade, there has been a marked shift in the perception of biological threats in Europe. Even before 2020, risk factors associated with biological sabotage were largely underestimated. The public

[31] *Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems*, Geneva 2002.

[32] *Foodborne Disease Outbreaks: Guidelines for Investigation and Control*, Geneva 2008.

[33] J.P. Wood et al., *Environmental Persistence of Bacillus anthracis and Bacillus subtilis Spores*, "PLoS ONE" 2015. https://doi.org/10.1371/journal.pone.0138083.

[34] R. Sinclair et al., *Persistence of Category A Select Agents in the Environment*, "Applied and Environmental Microbiology" 2008, no. 74(3), pp. 555–563. https://doi.org/10.1128/AEM.02167-07.

[35] S. Shadomy et al., *Anthrax Outbreaks: a warning for improved prevention, control and heightened awareness*, "Food and Agriculture Organization of the United Nations" 2016, vol. 37, https://openknowledge.fao.org/server/api/core/bitstreams/59269d58-654e-4790-ac60-a9ea7edd3a99/content [accessed: 16 IV 2025].

[36] S.A. Sarker et al., *An integrated model for anthrax-free zone development*, "Journal of Infection and Public Health" 2023, vol. 16, pp. 141–152. https://doi.org/10.1016/j.jiph.2023.10.024.

debate was dominated by issues related to climate changes, chemical or cybersecurity changes. The COVID-19 pandemic revealed that the consequences of biological threats can be just as far-reaching as economic or climate crises, potentially leading to disruptions in supply chains, destabilisation of healthcare systems and significant social losses[37]. In Europe, attention has also been drawn to the risks associated with zoonotic disease outbreaks, such as SARS-CoV-2 on mink farms in Denmark and the Netherlands, as well as the spread of ASF, which has necessitated the implementation of stricter biosecurity measures in agriculture[38]. An event in 2018, classified as a CBRN threat, was also significant. In Cologne, man suspected of producing biological weapons based on highly toxic ricin was apprehended[39]. The problem lies in the sporadic inclusion of issues related to agroterrorism or crimes involving biological agents in documents concerning the security of EU countries, including Poland, even though international organisations (WHO, WOAH, Interpol) recommend preparing response plans for attacks targeting supply systems for food[40].

The response for the shortcomings was the One Health concept, that links human, animal and environmental health with internal security elements and promotes close cooperation between human, animal and environmental health sectors[41]. Complementing this approach are

[37] *Lessons from the COVID-19 pandemic*, https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-lessons-learned-may-2023.pdf [accessed: 16 IV 2025].

[38] C. Adlhoch et al., *Avian influenza overview February – May 2021*, "EFSA Journal" 2021, vol. 19, no. 12. https://doi.org/10.2903/j.efsa.2021.6951; J.V. Baños et al., *Epidemiological analyses of African swine fever in the European Union*, "EFSA Journal" 2022, vol. 20, no. 5. https://doi.org/10.2903/j.efsa.2022.7290.

[39] *Update: Cologne couple in court over 'biological bomb plot'*, The Local Germany, 7 VI 2019, https://www.thelocal.de/20190607/tunisian-german-couple-in-court-over-ricin-attack-plot [accessed: 16 IV 2025].

[40] *Animal agrocrime and agroterrorism*, Interpol, https://www.interpol.int/Crimes/Terrorism/Bioterrorism/Animal-agrocrime-and-agroterrorism [accessed: 10 VI 2025]; A. Elbers, R. Knutsson, *Agroterrorism Targeting Livestock: A Review with a Focus on Early Detection Systems*, "Biosecurity and Bioterrorism: Biodefense Strategy, Practise, and Science" 2013. https://doi.org/10.1089/bsp.2012.0068; C. Gyles, *Agroterrorism*, https://pmc.ncbi.nlm.nih.gov/articles/PMC2839819/pdf/cvj_04_347.pdf [accessed: 10 VI 2025].

[41] *One health joint plan of action 2022–2026: working together for the health of humans, animals, plants and the environment*, World Health Organization, https://www.who.int/publications/i/item/9789240059139 [accessed: 10 VI 2025].

regulations: the International Plant Protection Convention (IPPC)[42], the Terrestrial Animal Health Code[43] and the Biological Weapons Convention (BWC)[44]. Furthermore, the EU operates early warning systems, such as the Rapid Alert System for Food and Feed (RASFF), the Early Warning and Response System (EWRS) and the Animal Disease Notification System (ADNS), which support biological incident response[45]. At the global level, the Quadripartite One Health Joint Plan of Action 2022–2026 was adopted, outlining, among other things, a common framework for oversight, preparedness and response. Within the EU, the EU4Health programme (2021–2027) formally incorporated the One Health into health action frameworks and funding mechanisms[46]. Legally, a milestone was the *Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU*, which strengthened threat monitoring, early warning and the coordination of reference laboratory activities at the EU level.

In Poland, implementation of the One Health faces barriers such as the lack of a comprehensive legislative and institutional strategy, fragmented databases, limited interoperability and differences in competencies between sectors. These challenges translate into difficulties in integrating passive and active surveillance (the Sentinel Network, i.e. network of veterinarians monitoring field conditions and reporting information to central institutions), which involves farmers, veterinarians, reference laboratories and biological security services. It is recommended to establish central coordination structures that would enable effective

[42] *International Plant Protection Convention (1997)*, Rome 2024, https://openknowledge.fao.org/server/api/core/bitstreams/30cc2e83-a6fd-4e2c-a5ee-312093d5a307/content [accessed: 10 VI 2025].

[43] *Terrestrial Animal Health Code*...

[44] *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*.

[45] *Commission publishes 2023 Annual Report on food safety alerts and agri-food fraud investigations*, European Commission, 16 IX 2024, https://ec.europa.eu/newsroom/sante/items/847722/en [accessed: 14 VI 2025].

[46] *One health joint plan of action (2022–2026): working together for the health of humans, animals, plants and the environment*, Rome 2022; *Regulation (EU) 2021/522 of the European Parliament and of the Council of 24 March 2021 establishing a Programme for the Union's action in the field of health ('EU4Health Programme') for the period 2021-2027, and repealing Regulation (EU) No 282/2014*.

implementation of the integrated approach and the development of modern early warning systems and biomonitoring.

Biosafety systems in Poland and selected countries

Biosafety systems allow for the identification of the key factors influencing the effectiveness of biological threat prevention in the agri-food sector, as well as the detection of and response to such threats.

Poland

In Poland, several key institutions are responsible for carrying out tasks related to biosafety, including the protection of human, animal and plant health, food safety and biological threat prevention, including bioterrorism. These are:

- the State Sanitary Inspection, operating under the Ministry of Health based on the *Act of 14 March 1985 on the State Sanitary Inspection*. Its tasks include, among others, supervision of public health, environmental hygiene, public facilities, water and the safety of non-animal-derived food;
- the Veterinary Inspection operating on the basis of the *Act of 29 January 2004 on the Veterinary Inspection*. It is responsible for animal health protection, oversight of products of animal origin, combating infectious diseases and border control related to the movement of animals and products;
- the State Plant Health and Seed Inspection Service whose tasks arise from the *Act of 18 December 2003 on plant protection* and the *Act of 13 February 2020 on Plant Health and Seed Inspection Service*. It is responsible for the monitoring of plant health, the prevention of the spread of pests and the quality control of seed material;
- the Commercial Quality Inspection of Agricultural and Food Products operating on the basis of the *Act of 21 December 2000 on commercial quality of agri-food products*. It oversees commercial quality, labelling and the compliance of agri-food products with legal requirements;
- the European Food Safety Authority, whose tasks in Poland are carried out by the national contact point in accordance with *Regulation (EC) No 178/2002 of the European Parliament and*

of the Council of 28 January 2002 laying down the general principles and requirements of food law.

The cooperation of these institutions forms the foundation of the national biosafety system, which encompasses the monitoring and detection of biological threats and the response to them, including deliberate contamination of the food chain and epidemics of infectious diseases in humans, animals and plants. This also applies to phenomena of a transboundary nature. Their activities are integrated within national and European information-exchange and early-warning systems, such as the RASFF, the ADNS or the Trade Control and Expert System (TRACES), which enables a rapid and coordinated response to crisis situations[47].

Biosafety supervision in Poland is carried out through cooperation between the Main Sanitary Inspectorate, the Main Veterinary Inspectorate, the State Plant Health and Seed Inspection Service, the Commercial Quality Inspection of Agricultural and Food Products and other institutions of public administration whose competences include the protection of human, animal and environment health. Despite existing legal regulations, such as the *Act of 11 March 2004 on protection of animal health and combating contagious animal diseases* together with executive acts and the *Act of 25 August 2006 on food and nutrition safety*, Poland still lacks – as already mentioned – an integrated strategy covering the coordination of activities in the areas of human and animal health and food safety in accordance with the One Health concept[48].

Laboratories specialising in pathogen diagnostics and threat monitoring play an important role in the biological protection system. In Poland, there are several biosafety level-3 (BSL-3) laboratories[49] operating, among others, in the National Veterinary Institute – the National Research Institute in Puławy. It serves as the national reference laboratory for animal

[47] *Rapid Alert System for Food and Feed (RASFF)*, European Commission, https://food.ec.europa.eu/food-safety/rasff_en [accessed: 10 X 2025].

[48] K.M. Mełgieś, *The Evolution of One Health concept – a European perspective*, "Review of European and Comparative Law" 2024, vol. 57, no. 2. https://doi.org/10.31743/recl.17467; P. Kaczmarek et al., *The One Health Concept: A Holistic Approach to Protect Human and Environmental Health*, "Medycyna Pracy. Workers' Health and Safety" 2024, no. 5, pp. 433–444. https://medpr.imp.lodz.pl/pdf-192557-116180.

[49] K. Chomiczewski, M. Bartoszcze, A. Michalski, *Budowanie nowoczesnego systemu obrony przed bronią biologiczną Sił Zbrojnych RP zgodnego z wymaganiami NATO* (Eng. Building a modern biological weapons defence system for the Polish Armed Forces in line with NATO requirements), "Lekarz Wojskowy" 2019, no. 1, pp. 56–64.

diseases of epizootic and zoonotic importance[50]. Most BSL-3 laboratories, including in the National Institute of Public Health – the National Institute of Hygiene – the National Research Institute and in academic institutions (the University of Gdańsk and the Medical University of Gdańsk) focus on diagnosing human diseases and therefore only contribute indirectly to food safety. At the same time, there is a network of military laboratories, including the Military Institute of Hygiene and Epidemiology, which has BSL-3 laboratories at its disposal[51]. The Military Institute of Hygiene and Epidemiology has the Centre for Diagnosis and Control of Biological Hazards located in Puławy[52], among other places. Military laboratories diagnose biological agents with epidemic and bioterrorism potential as well as support crisis response and international cooperation[53]. BSL-3 laboratories are an essential element of the national biological protection system – they enable early detection and analysis of threats as well as strengthen the state's ability to respond to bioterrorism attacks.

Despite the existence of the above structures and mechanisms, there is still a gap in the ability to quickly detect and respond to intentional contamination of food or feed, both in plant and animal production. There is also a lack of BSL-4 laboratories that enable safe research on the most dangerous pathogens. This limits the state's preparedness for the most serious biological threats, including potential bioterrorism attacks[54].

Germany

Germany has an advanced biosafety infrastructure, coordinated by the Federal Ministry of Agriculture, Food and Regional Identity (Bundesministerium für Landwirtschaft, Ernährung und Heimat). Entities

[50] *Krajowe Laboratoria Referencyjne* (Eng. National reference laboratories), Państwowy Instytut Weterynaryjny – Państwowy Instytut Badawczy, https://www.piwet.pulawy.pl/krajowe-laboratoria-referencyjne/ [accessed: 29 VII 2025].

[51] *Wojskowy Instytut Higieny i Epidemiologii im. Generała Karola Kaczkowskiego*, https://wihe.pl/wihe/o-nas [accessed: 29 VII 2025].

[52] *Ośrodek Diagnostyki i Zwalczania Zagrożeń Biologicznych* (Eng. Centre for Diagnosis and Control of Biological Hazards), Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/zaklady/odizzb/organizacja [accessed: 29 VII 2025].

[53] *Zadania badawczo-rozwojowe* (Eng. Research and development tasks), Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/wihe/zadania [accessed: 29 VII 2025].

[54] K. Goniewicz et al., *Bioterrorism Preparedness and Response in Poland: Prevention, Surveillance and Mitigation Planning*, "Disaster Medicine and Public Health Preparedness" 2021, no. 15(6), pp. 697–702.

such as the Friedrich Loeffler Institute (Friedrich Loeffler Institut, FLI) and the Robert Koch Institute (Robert Koch Institute, RKI) play an important role in the surveillance, investigation and diagnosis of infectious diseases in animals and humans, respectively. The Robert Koch Institute runs the RefBio project at a global level. In this way, it supports an international network of laboratories within the framework of the United Nations Secretary-General's Mechanism to Investigate Suspected Use of Biological Weapons (UNSGM) and organise exercises, workshops and ensures knowledge transfer[55]. The Germans also have laboratories with the highest, biosafety level-4 rating – BSL-4 (including in Berlin)[56]. The crisis management system is based on a federal organisation model, with strong coordination of activities between the federal states. The state's operational readiness is significantly enhanced by regular simulation exercises codenamed LÜKEX. During these exercises, various crisis management scenarios are tested, such as pandemic variants or energy crises and early warning systems[57]. By comparison, in Poland such exercises are conducted less frequently and with a limited agro-bio component. This reinforces the call for a separate agricultural module to be included in them.

France

France integrates sanitary, veterinary and environmental activities through the French Agency for Food, Environmental and Occupational Health & Safety (Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail, ANSES). There is a reference biosafety

[55] *RefBio – German Contribution to Strengthen the Reference Laboratories Bio in the UNSGM*, Robert Koch Institut, 10 V 2019, https://www.rki.de/EN/Institute/International-activities/Biosecurity-Programme/RefBio.html [accessed: 16 VI 2025].

[56] *The Biosafety Level-4 Laboratoty at RKI*, Robet Koch Institut, 31 I 2024, https://www.rki.de/EN/Topics/Research-and-data/Specialised-laboratories/BSL-4-laboratory/bsl-4-laboratory-at-the-robert-koch-institute-node.html [accessed: 16 VI 2025]; *FLI tests mobile One Health laboratory for diagnosing highly pathogenic pathogens*, Friedrich Loeffler Institut, 13 VI 2025, https://www.fli.de/en/press/press-releases/press-singleview/fli-tests-mobile-one-health-laboratory-for-diagnosing-highly-pathogenic-pathogens/ [accessed: 20 VI 2025].

[57] *Germany*, European Commission, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-disaster-management-system/germany_en?utm [accessed: 15 XII 2025]; *Historie der LÜKEX Krisenmanagementübungen*, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Historie/historie_node.html [accessed: 15 XII 2025].

level-4 (BSL-4) laboratory – Laboratoire P4 Inserm Jean Mérieux in Lyon[58]. Despite the existence of a strong institutional base, the reports point to difficulties in cooperation between civil and military services as well as the need for better integration of cross-sectoral data[59].

Italy

In Italy, the biosecurity system is coordinated by the Ministry of Health and regional veterinary services. The network of Zooprophylactic Institutes (Istituti Zooprofilattici Sperimentali) acts as reference laboratories for animal diseases. In Rome, a BSL-4 laboratory operates within the National Institute for Infectious Diseases (Istituto Nazionale per le Malattie Infettive)[60]. Challenges in responding to biological threats include the lack of a central platform for data integration and differences between regions in their ability to respond to these threats[61].

Great Britain

The 2001 FMD epidemic marked a turning point in the UK biosafety policy. After the crisis, a comprehensive biological risk management system was introduced, covering prevention and rapid response. The leading institution is the Animal and Plant Health Agency, which is responsible for surveillance and diagnostics (both routine and in crisis situations), as well as for coordinating actions in the events of threats[62]. The agency cooperates with the Pirbright Institute, which conducts research on viruses that cause diseases in animals[63] and has SAPO-4 laboratory (Specified Animal

---

58 *ANSES Laboratories*, ANSES, 15 II 2013, https://www.anses.fr/en/content/anses-laboratories [accessed: 20 VI 2025].

59 T. Lefrançois et al., *One Health approach at the heart of the French Committee for monitoring and anticipating health risks*, "Natura Communication" 2023, no. 14, p. 9. https://doi.org/10.1038/s41467-023-43089-2.

60 *INMI Lazzaro Spallanzani IRCCS, Istituto Nazionale Malettie Infettive*, https://www.inmi.it/ [accessed: 20 VI 2025].

61 A. Perella, M. Bisogno, *The strength and resilience of Italy's health data system*, "The Lancet Regional Health" 2025, vol. 51. https://doi.org/10.1016/j.lanepe.2025.101255.

62 *Animal and Plant Health Agency framework document*, Department for Environment, Food & Rural Affairs, 7 III 2024, https://www.gov.uk/government/publications/animal-and-plant-health-agency-framework-document/animal-and-plant-health-agency-framework-document [accessed: 20 VI 2025].

63 *Our science*, The Pirbright Institute, https://www.pirbright.ac.uk/our-science [accessed: 20 VI 2025].

Pathogens Order class 4), serving as a reference for the FAO, the WOAH and the EU[64]. The institute conducts research, provides training and develops vaccines.

The government Department for Environment, Food and Rural Affairs (DEFRA) and the UK Health Security Agency (UKHSA) have developed integrated plans for managing zoonotic and phytopathological risks within the framework of the One Health approach[65]. They form the basis of the national preparedness plans in case of outbreaks of non-endemic diseases[66]. After 2001, cooperation between administration, veterinary services, reference laboratories and international partners was developed. Simulation exercises and reports, prepared by the Anderson Report[67] and the National Audit Office[68], among others, have contributed to strengthening analytical and early warning systems. The 2023 biosecurity strategy sets out a framework for protection against natural, accidental and deliberate threats, including bioterrorism threats[69]. It is based on four pillars: understanding, prevention, detection and response, supported by state authorities, scientific and technological development and international cooperation. This strategy aims to be fully operational by 2030 and to establish the National Biosecurity Centre, with a budget of approx. GBP 1 billion. It is expected to reach full operational capacity between 2033 and 2034[70].

---

[64] *Reference Laboratories*, The Pirbright Institute, https://www.pirbright.ac.uk/facilities-and-resources/reference-laboratories [accessed: 17 VI 2025].

[65] *UKHSA Strategic Plan 2023 to 2026*, https://assets.publishing.service.gov.uk/media/650d530e52e73c00139426c1/UKHSA_3_year_strategy.pdf [accessed: 18 VI 2025].

[66] *Contingency plan for exotic notifiable diseases of animals in England*, https://assets.publishing.service.gov.uk/media/691c80cd84a267da57d706da/Defra-contingency-plan-exotic-notifiable-diseases-animals-England.pdf [accessed: 18 VI 2025].

[67] I. Anderson, *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry Report*, London 2002.

[68] *The 2001 Outbreak of Foot and Mouth Disease*, London 2023.

[69] *UK Biological Security Strategy*, Cabinet Office, 12 VI 2023, https://www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html [accessed: 10 VI 2025].

[70] *UK pledges 1 billion pounds to build new biosecurity centre*, Reuters, 24 VI 2025, https://www.reuters.com/business/healthcare-pharmaceuticals/uk-pledges-1-billion-pounds-build-new-biosecurity-centre-2025-06-23 [accessed: 8 VIII 2025]; *Dowden: world-class crisis capabilities deployed to defeat biological threats of tomorrow*, 12 VI 2023, https://www.gov.uk/government/news/dowden-world-class-crisis-capabilities-deployed-to-defeat-biological-threats-of-tomorrow [accessed: 8 VIII 2025].

Research institutions and information tools in the EU

The EU states use shared surveillance networks, such as the RASFF, the TRACES and the EWRS, which support information exchange and coordination of activities[71]. Germany and France have efficient institutional structures in place, including the FLI and the ANSES[72]. In Poland and Italy, there is no unified coordination system linking the veterinary, phytosanitary and public health sectors. Poland has the National Crisis Management Plan, and its framework nature does not ensure operational cross-sector integration. A significant limitation remains the lack of BSL-4 laboratories, which are available in Germany, France, the US and Great Britain[73]. Great Britain has seen effective cooperation between the agriculture, public health, defence and environmental sectors, supported by strategic legal regulations[74].

Despite the existence of community tools, the implementation of the One Health approach within the EU is uneven[75]. The analysis presented in the publication *Countering Agricultural Bioterrorism* emphasises that bioterrorism threats continue to be underestimated in the security policies of the EU states[76]. There is a lack of comprehensive response scenarios, especially regarding responses to acts of agroterrorism, despite the recognition of the food sector as an element of critical infrastructure.

The role of key stakeholders in the early warning system: farmers, veterinarians and local authorities

Effective strengthening of the biosecurity system in the agri-food sector is not possible without the active involvement of farmers, veterinarians and local authorities. These groups are the first line of detection alarming

[71] *One Health: a joint framework for action published by five EU agencies*, European Centre for Disease Prevention and Control, 7 V 2024, https://www.ecdc.europa.eu/en/news-events/one-health-joint-framework-action-published-five-eu-agencies [accessed: 10 VI 2025].

[72] *FLI tests mobile One Health laboratory…*; *ANSES Laboratories…*

[73] *Laboratory Biosafety Manual…*

[74] *UK Biological Security Strategy…*

[75] *One Health: a joint framework for action published…*

[76] *Countering Agricultural Bioterrorism*, Washington 2022. https://doi.org/10.17226/10505.

symptoms and play a decisive role in responding early to biological incidents.

Farmers are the first link in the early notification and warning system. Their daily contact with animals and plants allows them to quickly detect symptoms of ASF, FMD or plant infection caused by bacteria *Xylella fastidiosa*[77]. It is important that farmers know the symptoms and reporting procedures, and that they have confidence in state institutions. This helps to reduce response times. Unfortunately, low awareness, limited access to up-to-date information and fear of administrative consequences often cause delays in implementing procedures[78]. There is also a lack of formal mechanisms to encourage rapid reporting, such as financial support or legal protection for reporting persons.

Veterinarians are a connecting element between local farming communities and the system for monitoring and diagnosing zoonotic threats. Their tasks include not only recognising epizootics, but also educating farmers, providing early warnings and transmitting data to the veterinary services and reference laboratories[79]. Sentinel surveillance operates in many EU states[80].

---

[77] C. Guinat et al., *English Pig Farmers' Knowledge and Behaviour towards African Swine Fever Suspicion and Reporting*, "PLoS ONE" 2016, no. 9. https://doi.org/10.1371/JOURNAL.PONE.0161431; S. Costard et al., *Epidemiology of African swine fever virus*, "Virus Research" 2013, vol. 173, no. 1, pp. 191–197. https://doi.org/10.1016/J.VIRUSRES.2012.10.030.

[78] M.C. Gates, L. Earl, G. Enticott, *Factors influencing the performance of voluntary farmer disease reporting in passive surveillance systems: A scoping review*, "Preventive Veterinary Medicine" 2021, vol. 196, pp. 1–2, 5–7. https://doi.org/10.1016/j.prevetmed.2021.105487; G. Enticott, L. Earl, M.C. Gates, *A systematic review of social research data collection methods used to investigate voluntary animal disease reporting behaviour*, "Transboundary and Emerging Diseases" 2021, no. 5, pp. 2573–2587. https://doi.org/10.1111/tbed.14407; J.C. Mariner et al., *Rift Valley fever action framework*, Italy 2022. https://doi.org/10.4060/cb8653en.

[79] O.A. Hassan, K. de Balogh, A.S. Winkler, *One Health early warning and response system for zoonotic diseases outbreaks: Emphasis on the involvement of grassroots actors*, "Veterinary Medicine and Science" 2023, no. 4, vol. 9, pp. 1881–1889. https://doi.org/10.1002/vms3.1135.

[80] C. Saegerman et al., *Clinical Sentinel Surveillance of Equine West Nile Fever, Spain*, "Transboundary and Emerging Diseases" 2014, vol. 63, no. 2, pp. 161–164. https://doi.org/10.1111/tbed.12243; C. Plaza-Rodriguez et al., *Wildlife as Sentinels of Antimicrobial Resistance in Germany?*, "Frontiers in Veterinary Science" 2021, vol. 7, pp. 1–11. https://doi.org/10.3389/fvets.2020.627821; R. Özçelik et al., *Evaluating 5.5 Years of Equinella: A Veterinary-Based Voluntary Infectious Disease Surveillance System of Equines in Switzerland*, "Frontiers in Veterinary Science" 2020, vol. 7, pp. 1–4. https://doi.org/10.3389/fvets.2020.00327.

In Poland, similar solutions are still developing and are mainly implemented within the National Veterinary Inspection, which coordinates the monitoring of infectious animal diseases on the basis of national and EU surveillance programmes. Digitalisation and integration of systems such as the IRZplus (Identification and Registration of Animals), the TRACES and national databases on animal diseases play an important role. Data exchange and reporting platforms to the Chief Veterinary Officer and European institutions, including the EFSA and the RASFF system, are also becoming increasingly important. However, there are still limitations in terms of full system interoperability and the inclusion of private practitioners in the rapid alert network, which limits the effectiveness of sentinel surveillance compared to solutions used in e.g. Germany or France[81].

Local authorities – provincial, district and municipal – play the most important role in the practical implementation if biosafety principles and biological threat response systems, cooperating with central administration and critical infrastructure operators. Despite the availability of analytical tools such as risk matrices, vulnerability models and predictive scenarios, their effectiveness in practice remains limited due to low awareness and a lack of consistent implementation among the responsible entities.

In Poland, the National Crisis Management Plan and the National System of Contamination Detection and Alarm formally provide for mechanisms for assessing and monitoring threats, including biological ones, but their effectiveness depends not only on the availability of tools, but also on their proper interpretation and use by the administration and critical infrastructure operators.

The role of local institutions should be strengthened through regular training, trust building and ensuring access to digital tools (e.g. e-learning platforms, applications that support monitoring and reporting). Permanent educational programmes, run in cooperation with agricultural chambers, veterinary services and research institutes, should

[81] *Zwalczanie i monitoring wybranych chorób zakaźnych zwierząt* (Eng. Combating and monitoring of selected infectious animal diseases), Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/nadzor-weterynaryjny/programy-zwalczaniamonitorowania-chorob-zakaznych-zwierzat [accessed: 1 IX 2025]; *European Commission*, https://ec.europa.eu [accessed: 1 IX 2025]; *Aplikacja IRZplus* (Eng. The IRZplus app), Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/systemy-informatyczne/cbd-irzgo [accessed: 1 IX 2025]; *EFSA*, https://www.efsa.europa.eu [accessed: 1 IX 2025]; *Rapid Alert System for Food and Feed (RASFF)*...

cover not only the recognition of symptoms of infectious diseases, but also response procedures and inter-institutional cooperation. The educational programmes implemented in Germany and the Netherlands, in which local food producers participate in simulations of crisis situations are a good example[82].

In the context of Poland, the measures described are recommendations rather than binding programmes at national or provincial level. Their aim would be to adapt good practices from the EU level, e.g. initiatives of the EFSA and the European Centre for Disease Prevention and Control (ECDC), in the field of food safety and public health, including educational mechanisms such as the Better Training for Safer Food[83]. The recommended solutions should be implemented within national and regional structures by provincial and district crisis management teams, veterinary services as well as agricultural chambers and closely integrated with local response plans[84]. Such integrated measures should be supplemented by regular simulation exercises[85], which allow for practical verification of the effectiveness of the procedures implemented, and cross-sectoral coordination.

A well-developed logistics infrastructure is crucial for responding to biological threats, however in many countries it remains inadequate. France has advanced cold chains and vaccine reserves, which shortens

[82] *Chemical and biological deliberate events,* World Health Organization, https://openwho.org/emergencymgmt/501116/Chemical+and+biological+deliberate+events [accessed: 1 IX 2025].

[83] *Empowering food safety through enhanced training,* European Commission, 9 IX 2024, https://ec.europa.eu/newsroom/btsf/items/846699/en [accessed: 1 IX 2025].

[84] Ibid.; *Breaking language barriers: translation of training materials on food safety regulations now available,* European Commission, 25 III 2025, https://hadea.ec.europa.eu/news/breaking-language-barriers-translation-training-materials-food-safety-regulations-now-available-2025-03-25_en [accessed: 1 IX 2025]; *HaDEA launches third call for tenders under BTSF,* European Commission, 5 VIII 2022, https://hadea.ec.europa.eu/news/hadea-launches-third-call-tenders-under-btsf-2022-08-05_en?utm [accessed: 1 IX 2025]; *Digitalising the EU agricultural sector,* European Commission, https://digital-strategy.ec.europa.eu/en/policies/digitalisation-agriculture [accessed: 1 IX 2025]; *Transparency solutions for transforming the food system*, EU CAP Network, https://eu-cap-network.ec.europa.eu/projects/transparency-solutions-transforming-food-system_en [accessed: 1 IX 2025].

[85] *Field simulation trainings to support emergency preparedness,* World Organisation for Animal Health, 13 IV 2023, https://www.woah.org/en/article/field-simulation-trainings-to-support-emergency-preparedness/ [accessed: 10 VI 2025].

response times[86]. Poland has modern logistics centres, such as NewCold's warehouses, and systemic reserves of vaccines and diagnostic products maintained by the Government Strategic Reserves Agency[87], however their scope and availability – especially at regional level – are limited. Despite the resilience of the cold chain sector during crises, further investment in digitalisation, interoperability and strategic reserves is necessary[88].

Summary and conclusions

For many years, the security policies of the countries in question reflected a belief that the likelihood of serious biological incidents occurring was low. This assumption led to underestimating risks, limiting investments in preventive measures and a lack of response procedures – particularly in agri-food sector, which resulted in the lowering of the operational readiness. The lack of systemic training, low spending on prevention and neglect of bioterrorism scenarios in local crisis management plans widened the gap between the strategy's provisions and the institutions' actual capacity to act effectively[89].

Over the last decade, there has been a significant change in the perception of biological threats. The COVID-19 pandemic has demonstrated that biological crises can generate effects comparable to economic or climate crises, leading to serious disruptions in supply chains, burdens on health systems and social losses[90]. More attention has also been paid to threats related to zoonotic diseases, such as ASF, SARS-CoV-2, and

[86] Y. He, M. Liu, *Research on sustainable development of agricultural product cold chain logistics under public safety emergencies*, "Frontiers in Sustainable Food Systems" 2023, vol. 7. https://doi.org/10.3389/fsufs.2023.1174221; A. Spitalleri et al., *BioTrak: A Blockchain-based Platform for Food Chain Logistics Traceability*, International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia 2023, pp. 105–110. https://doi.org/10.1109/ICCNS58795.2023.10193341.

[87] *Rezerwy medyczne* (Eng. Medical reserves), Rządowa Agencja Rezerw Strategicznych, https://www.gov.pl/web/rars/rezerwy-medyczne [accessed: 30 IX 2025].

[88] *Poland Cold Chain Logistics et 2025–2034 – Size, Share, Trends, Analysis & Forecast 2025–2034*, MarkWide Research, https://markwideresearch.com/poland-cold-chain-logistics-market/ [accessed: 18 VI 2025].

[89] *Deliberate events*, World Health Organization, 2 IV 2024, https://www.who.int/news-room/fact-sheets/detail/deliberate-events [accessed: 18 VI 2025].

[90] *Lessons from the COVID-19 pandemic*...

incidents classified as CBRN threats[91]. Despite the existence of NewCold's WHO, NewCold's WOAH and Interpol recommendations concerning the need to prepare response plans for intentional contamination of food systems, issues related to agroterrorism continue to be treated marginally in national strategic documents of the EU states, including in Poland[92]. The One Health approach aims to fill this gap by integrating human, animal and environmental health into a single coherent biological threats management system. However, the implementation of this concept is not uniform and faces significant barriers. This hinders the integration of passive and active surveillance and the inclusion of farmers, veterinarians, laboratories and local authorities into the early warning network. The examples from Germany and the Netherlands show that effective One Health implementation requires not only legal tools, but also systemic training, trust building as well as regular simulation exercises, which include local food producers[93]. At the same time, it is necessary to strengthen logistics infrastructure, including cold chains, vaccine reserves, diagnostic materials, and to continue investing in interoperability, digitalisation and the management of strategic reserves.

Given the growing complexity of threats, it is reasonable to consider establishing a specialised EU agrobiosecurity institution, similar to the ECDC[94], but focused on threats for the agri-food sector. Such an institution could conduct strategic research, risk analyses, develop early warning systems and coordinate the activities of food safety, veterinary and sanitary services, reference laboratories and scientific centres. Close cooperation with the Directorate-General for Health & Food Safety[95], the EFSA and the RASFF system would be important in this context. It is also crucial to conduct qualitative and quantitative research among

[91] F. Flade, *The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror*, https://ctc.westpoint.edu/june-2018-cologne-ricin-plot-new-threshold-jihadi-bio-terror/ [accessed: 16 IX 2025].

[92] *Animal agrocrime and agroterrorism...*; *Agro-crime and agro-terrorism*, World Organisation for Animal Health, https://www.woah.org/en/what-we-offer/emergency-preparedness/agro-crime-and-agro-terrorism/ [accessed: 16 IX 2025].

[93] *Field simulation trainings to support emergency preparedness...*

[94] *What We Do*, European Centre for Disease Prevention and Control, https://www.ecdc.europa.eu/en/about-ecdc/what-we-do [accessed: 30 IX 2025].

[95] *Health and Food Safety*, European Commission, https://commission.europa.eu/about/departments-and-executive-agencies/health-and-food-safety_en [accessed: 15 XII 2025].

stakeholders – farmers, veterinarians, laboratories, sanitary services and administration – to identify real operational barriers to the implementation of biosafety procedures and assess readiness for inter-institutional cooperation. At the same time, systemic analyses should be conducted, including mapping of decision-making and communication processes, to detect gaps in coordination and interoperability. The research material gathered would form the basis for the creation of an organisationally and socially effective institution that responds to the real needs of frontline actors and strengthens the ability of the EU and its Member States to respond effectively to biological threats.

In summary, strengthening resilience to bioterrorism attacks requires:

- full integration of activities in the One Health model,
- development of interoperable surveillance systems and laboratories,
- systematic organising trainings and exercises,
- involvement of local actors in sentinel surveillance,
- building efficient logistics in crisis situations,
- taking into account the agri-food sector in national and European security plans.

Implementing these proposals would increase the effectiveness of responses to biological threats – both natural and intentional – and strengthen countries' resilience to hybrid threats.

Bibliography

Adlhoch C., Fusaro A., Gonzales J.L., Kuiken T., Marangon S., Niqueux E., Staubach Ch., Terregino C., Aznar I., Guajardo I.M., Lima E., Baldinelli F., *Avian influenza overview February – May 2021*, "EFSA Journal" 2021, vol. 19, no. 12. https://doi.org/10.2903/j.efsa.2021.6951.

Anderson I., *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry Report*, London 2002.

Baños J.V., Boklund A., Gogin A., Gortázar Ch., Guberti V., Helyes G., Kantere M., Korytarova D., Linden A., Masiulis M., Miteva A., Neghirla I., Oļševskis E., Ostojic S., Petr S., Staubach Ch., Thulke H.H., Viltrop A., Wozniakowski G., Broglia A., Cortiñas J.A., Dhollander S., Mur L., Papanikolaou A., Van der Stede Y., Zancanaro G., Ståhl K., *Epidemiological analyses of African swine fever in the European Union*, "EFSA Journal" 2022, vol. 20, no. 5. https://doi.org/10.2903/j.efsa.2022.7290.

Chomiczewski K., Bartoszcze M., Michalski A., *Budowanie nowoczesnego systemu obrony przed bronią biologiczną Sił Zbrojnych RP zgodnego z wymaganiami NATO* (Eng. Building a modern biological weapons defence system for the Polish Armed Forces in line with NATO requirements), "Lekarz Wojskowy" 2019, no. 1, pp. 56–64.

Costard S., Mur L., Lubroth J., Sanchez-Vizcaino J.M., Pfeiffer D.U., *Epidemiology of African swine fever virus*, "Virus Research" 2013, vol. 173, no. 1, pp. 191–197. https://doi.org/10.1016/J.VIRUSRES.2012.10.030.

Countering Agricultural Bioterrorism, Washington 2022. https://doi.org/10.17226/10505.

Dennis D.T., Inglesby T.V., Henderson D.A., Bartlett J.G., Ascher M.S., Eitzen E., Fine A.D., Friedlander A.M., Hauer J., Layton M., Lillibridge S.R., McDade J.E., Osterholm M.T., O'Toole T., Parker G., Trish M.P., Russell P.K., Tonat K., *Tularemia as a biological weapon: medical and public health management*, "The Journal of the American Medical Association" 2001, vol. 285, no. 21, pp. 2763–2773. https://doi.org/10.1001/JAMA.285.21.2763.

Dudley J.P., Woodford M.H., *Bioweapons, bioterrorism and biodiversity: potential impacts of biological weapons attacks on agricultural and biological diversity*, "Revue Scientifique et Technique" 2002, no. 21(1), pp. 125–137. http://dx.doi.org/10.20506/rst.21.1.1328.

Elbers A., Knutsson R., *Agroterrorism Targeting Livestock: A Review with a Focus on Early Detection Systems*, "Biosecurity and Bioterrorism: Biodefense Strategy, Practise, and Science" 2013. https://doi.org/10.1089/bsp.2012.0068.

Enticott G., Earl L., Gates M.C., *A systematic review of social research data collection methods used to investigate voluntary animal disease reporting behaviour*, "Transboundary and Emerging Diseases" 2021, no. 5, pp. 2573–2587. https://doi.org/10.1111/tbed.14407.

Foodborne Disease Outbreaks: Guidelines for Investigation and Control, Geneva 2008.

Garnett P., Doherty B., Heron T., *Vulnerability of the United Kingdom's food supply chains exposed by COVID-19*, "Nature Food" 2020, no. 1, pp. 315–318. https://doi.org/10.1038/s43016-020-0097-7.

Gates M.C., Earl L., Enticott G., *Factors influencing the performance of voluntary farmer disease reporting in passive surveillance systems: A scoping review*, "Preventive Veterinary Medicine" 2021, vol. 196. https://doi.org/10.1016/j.prevetmed.2021.105487.

Goniewicz K., Osiak B., Pawłowski W., Czerski R., Burkle F.M., Lasota D., Goniewicz M., *Bioterrorism Preparedness and Response in Poland: Prevention, Surveillance and Mitigation Planning*, "Disaster Medicine and Public Health Preparedness" 2021, no. 15(6), pp. 697–702.

Guidelines for drinking-water quality: fourth edition incorporating the first addendum, Geneva 2017.

Guinat C., Wall B., Dixon L., Pfeiffer D.U., *English Pig Farmers' Knowledge and Behaviour towards African Swine Fever Suspicion and Reporting*, "PLoS ONE" 2016, no. 9. https://doi.org/10.1371/JOURNAL.PONE.0161431.

Hassan O.A., Balogh K. de, Winkler A.S., *One Health early warning and response system for zoonotic diseases outbreaks: Emphasis on the involvement of grassroots actors*, "Veterinary Medicine and Science" 2023, no. 4, vol. 9, pp. 1881–1889. https://doi.org/10.1002/vms3.1135.

He Y., Liu M., *Research on sustainable development of agricultural product cold chain logistics under public safety emergencies*, "Frontiers in Sustainable Food Systems" 2023, vol. 7. https://doi.org/10.3389/fsufs.2023.1174221.

Ivanov D., Dolgui A., *Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak*, "International Journal of Production Research" 2020, vol. 58, no. 10, pp. 2904–2915. https://doi.org/10.1080/00207543.2020.1750727.

Kaczmarek P., Wiszniewska M., Słomka S., Walusiak-Skorupa J., *The One Health Concept: A Holistic Approach to Protect Human and Environmental Health*, "Medycyna Pracy. Workers' Health and Safety" 2024, no. 5, pp. 433–444. https://medpr.imp.lodz.pl/pdf-192557-116180.

Lefrançois T., Lina B., Autran B., Caille Y., Carrat F., Cauchemez S., Contenti J., Degrées du Loû A., Druet-Faivre L., Fontenille D., Giraudoux P., Heard M., De Lamballerie X., Lefrançois T., Le Grand R., Lescure F.X., Lina B., Loyer V., Malvy D., Offerle C., Raude J., Saint-Lary O., Slama R., *One Health approach at the heart of the French Committee for monitoring and anticipating health risks*, "Natura Communication" 2023, no. 14, p. 9. https://doi.org/10.1038/s41467-023-43089-2.

Mariner J.C., Raizman E., Pittglio C., Bebay C., Kivaria F., Lubroth J., Makonnen Y., *Rift Valley fever action framework*, Italy 2022. https://doi.org/10.4060/cb8653en.

Mełgieś K.M., *The Evolution of One Health concept – a European perspective*, "Review of European and Comparative Law" 2024, vol. 57, no. 2. https://doi.org/10.31743/recl.17467.

One health joint plan of action (2022–2026): working together for the health of humans, animals, plants and the environment, Rome 2022.

Özçelik R., Graubner C., Remy-Wohlfender F., Dürr S., Faverjon C., *Evaluating 5.5 Years of Equinella: A Veterinary-Based Voluntary Infectious Disease Surveillance System of Equines in Switzerland*, "Frontiers in Veterinary Science" 2020, vol. 7, pp. 1–4. https://doi.org/10.3389/fvets.2020.00327.

Perella A., Bisogno M., *The strength and resilience of Italy's health data system*, "The Lancet Regional Health" 2025, vol. 51. https://doi.org/10.1016/j.lanepe.2025.101255.

Plaza-Rodriguez C., Alt K., Grobbel M., Hammerl J.A., Irrgang A., Szabo I., Stingl K., Schuh E., Wiehle L., Pfefferkorn B., Naumann S., Kaesbohrer A., Tenhagen B.A., *Wildlife as Sentinels of Antimicrobial Resistance in Germany?*, "Frontiers in Veterinary Science" 2021, vol. 7, pp. 1–11. https://doi.org/10.3389/fvets.2020.627821.

Saegerman C., Alba-Casals A., Garcia-Bocanegra I., Dal Pozzo F., Galen G. van, *Clinical Sentinel Surveillance of Equine West Nile Fever, Spain*, "Transboundary and Emerging Diseases" 2014, vol. 63, no. 2, pp. 161–164. https://doi.org/10.1111/tbed.12243.

Sarker S.A., Shahid A.H., Rahman B., Nazir N.H., *An integrated model for anthrax-free zone development*, "Journal of Infection and Public Health" 2023, vol. 16, pp. 141–152. https://doi.org/10.1016/j.jiph.2023.10.024.

Sinclair R., Boone S.A., Greenberg D., Keim P., Gerba C.P., *Persistence of Category A Select Agents in the Environment*, "Applied and Environmental Microbiology" 2008, no. 74(3), pp. 555–563. https://doi.org/10.1128/AEM.02167-07.

Singh R.P., Hodson D.P., Huerta-Espino J., Jin Y., Bhavani S., Njau P., Herrera-Foessel S., Singh P.S., Singh S., Govindan V., *The emergence of Ug99 races of the stem rust fungus is a threat to world wheat production*, "Annual Review of Phytopathology" 2011, no. 49, pp. 465–481. https://doi.org/10.1146/annurev-phyto-072910-095423.

Spitalleri A., Kavasidis I., Cartelli V., Mineo R., Rundo F., Palazzo S., Spampinato C., Giordano D., *BioTrak: A Blockchain-based Platform for Food Chain Logistics Traceability*, International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia 2023, pp. 105–110. https://doi.org/10.1109/ICCNS58795.2023.10193341.

Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems, Geneva 2002.

The 2001 Outbreak of Foot and Mouth Disease, London 2002.

The European Union One Health 2023 Zoonoses Report, EFSA, 10 XII 2024, https://doi.org/10.2903/j.efsa.2024.9106.

Thompson. D., Muriel P., Russell D., Osborne P., Bromley A., Rowland M., Creigh-Tyte S., Brown C., *Economic costs of the foot and mouth disease outbreak in the United Kingdom in 2001*, "Revue Scientifique et Technique" 2002, no. 21(3), pp. 675–687. https://doi.org/10.20506/RST.21.3.1353.

Török T.J., Tauxe R.V., Wise R.P., Livengood J.R., Sokolow R., Mauvais S., Birkness K.A., Skeels M.R., Horan J.M., Foster L.R., *A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars*, "The Journal of the American Medical Association" 1997, vol. 278, no. 5, pp. 389–393. https://doi.org/10.1001/JAMA.1997.03550050051033.

UK Biological Security Strategy, London 2023.

Wheelis M., Casagrande R., Madden L.V., *Biological Attack on Agriculture: Low-Tech, High-Impact Bioterrorism: Because bioterrorist attack requires relatively little specialized expertise and technology, it is a serious threat to US agriculture and can have very large economic repercussions*, "BioScience" 2002, vol. 52, no. 7, pp. 569–576. https://doi.org/10.1641/0006-3568(2002)052[0569:BAOALT]2.0.CO;2.

Wood J.P., Meyer K.M., Kelly T.J., Choi Y.W., Rogers J.V., Riggs K.B., Willenberg Z.J., *Environmental Persistence of Bacillus anthracis and Bacillus subtilis Spores*, "PLoS ONE" 2015. https://doi.org/10.1371/journal.pone.0138083.

Internet sources

About Anaplasmosis, Centers for Disease Control and Prevention, 4 IX 2024, https://www.cdc.gov/anaplasmosis/about/index.html [accessed: 10 IX 2025].

Aedes aegypti – Factsheet for experts, European Centre for Disease Prevention and Control, 2 I 2023, https://www.ecdc.europa.eu/en/disease-vectors/facts/mosquito-factsheets/aedes-aegypti [accessed: 10 IX 2025].

African swine fever, EFSA, 19 V 2025, https://www.efsa.europa.eu/en/topics/topic/african-swine-fever [accessed: 16 VI 2025].

Agro-crime and agro-terrorism, World Organisation for Animal Health, https://www.woah.org/en/what-we-offer/emergency-preparedness/agro-crime-and-agro-terrorism/ [accessed: 16 IX 2025].

Animal agrocrime and agroterrorism, Interpol, https://www.interpol.int/Crimes/Terrorism/Bioterrorism/Animal-agrocrime-and-agroterrorism [accessed: 10 VI 2025].

Animal and Plant Health Agency framework document, Department for Environment, Food & Rural Affairs, 7 III 2024, https://www.gov.uk/government/publications/animal-and-plant-health-agency-framework-document/animal-and-plant-health-agency-framework-document [accessed: 20 VI 2025].

ANSES Laboratories, ANSES, 15 II 2013, https://www.anses.fr/en/content/anses-laboratories [accessed: 20 VI 2025].

Aplikacja IRZplus (Eng. The IRZplus app), Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/systemy-informatyczne/cbd-irzgo [accessed: 1 IX 2025].

Barclay E., *A Review of the Literature on Agricultural Crime. Report to the Criminology Research Council*, https://criminology.fsu.edu/sites/g/files/upcbnu3076/files/2021-03/A-Review-of-the-Literature-on-Agricultural-Crime.pdf [accessed: 2 XII 2025].

Biological threat reduction strategy. Strengthening global biological security, https://www.woah.org/app/uploads/2021/03/biothreat-strategy-veng-revised-1st-edition.pdf [accessed: 14 VI 2025].

Bluetongue, U.S. Department of Agriculture, Animal and Plant Health Inspection Service, https://www.aphis.usda.gov/livestock-poultry-disease/cattle/bluetongue [accessed: 10 IX 2025].

Bluetongue, World Organisation for Animal Health, https://www.woah.org/en/disease/bluetongue/ [accessed: 10 IX 2025].

Breaking language barriers: translation of training materials on food safety regulations now available, European Commission, 25 III 2025, https://hadea.ec.europa.eu/news/breaking-language-barriers-translation-training-materials-food-safety-regulations-now-available-2025-03-25_en [accessed: 1 IX 2025].

Building resilience against agro-crime and agro-terrorism, https://www.woah.org/app/uploads/2023/02/building-resilience-against-agro-crime-and-agro-terrorism.pdf [accessed: 14 VI 2025].

Carus W.S., *Bioterrorism and Biocrimes: the Illicit Use of Biological Arms in the 20th Century*, August 1998, https://wmdcenter.ndu.edu/Publications/Publication-View/Article/626562/bioterrorism-and-biocrimes-the-illicit-use-of-biological-arms-in-the-20th-centu/ [accessed: 14 VI 2025].

CDC Bioterrorism Agents, https://biosecurity.fas.org/resource/documents/CDC_Bioterrorism_Agents.pdf [accessed: 10 VI 2025].

Chemical and biological deliberate events, World Health Organization, https://openwho.org/emergencymgmt/501116/Chemical+and+biological+deliberate+events [accessed: 1 IX 2025].

Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory, United States Attorney's Office, 3 VI 2025, https://www.justice.gov/usao-edmi/pr/chinese-nationals-charged-conspiracy-and-smuggling-dangerous-biological-pathogen-us [accessed: 20 VI 2025].

Commission publishes 2023 Annual Report on food safety alerts and agri-food fraud investigations, European Commission, 16 IX 2024, https://ec.europa.eu/newsroom/sante/items/847722/en [accessed: 14 VI 2025].

Contingency plan for exotic notifiable diseases of animals in England, https://assets.publishing.service.gov.uk/media/691c80cd84a267da57d706da/Defra-contingency-plan-exotic-notifiable-diseases-animals-England.pdf [accessed: 18 VI 2025].

Deliberate events, World Health Organization, 2 IV 2024, https://www.who.int/news-room/fact-sheets/detail/deliberate-events [accessed: 18 VI 2025].

Deliverable D6.5 – Guiding Document on cross-sectoral preparedness and response to biological and/or chemical terror attack. Collaboration between health, civil protection and security, https://www.jaterror.eu/wp-content/uploads/2024/11/6.5-Guiding-Document.pdf [accessed: 8 XII 2025].

Dengue, World Health Organization, 21 VIII 2025, https://www.who.int/news-room/fact-sheets/detail/dengue-and-severe-dengue [accessed: 10 IX 2025].

Digitalising the EU agricultural sector, European Commission, https://digital-strategy.ec.europa.eu/en/policies/digitalisation-agriculture [accessed: 1 IX 2025].

Dowden: world-class crisis capabilities deployed to defeat biological threats of tomorrow, 12 VI 2023, https://www.gov.uk/government/news/dowden-world-class-crisis-capabilities-deployed-to-defeat-biological-threats-of-tomorrow [accessed: 8 VIII 2025].

EFSA, https://www.efsa.europa.eu [accessed: 1 IX 2025].

Emergency preparedness, resilience and response concept of operations, UK Health Security Agency, 15 I 2025, https://www.gov.uk/government/publications/emergency-preparedness-resilience-and-response-concept-of-operations/emergency-preparedness-resilience-and-response-concept-of-operations [accessed: 10 VI 2025].

Empowering food safety through enhanced training, European Commission, 9 IX 2024, https://ec.europa.eu/newsroom/btsf/items/846699/en [accessed: 1 IX 2025].

European Commission, https://ec.europa.eu [accessed: 1 IX 2025].

Factsheet about tick-borne encephalitis (TBE), European Centre for Disease Prevention and Control, 22 I 2024, https://www.ecdc.europa.eu/en/tick-borne-encephalitis/facts/factsheet [accessed: 10 IX 2025].

Field simulation trainings to support emergency preparedness, World Organisation for Animal Health, 13 IV 2023, https://www.woah.org/en/article/field-simulation-trainings-to-support-emergency-preparedness/ [accessed: 10 VI 2025].

First report on world's animal health reveals changing spread of disease impacting food security, trade and ecosystems, WOAH, 23 V 2025, https://www.woah.org/en/first-report-on-worlds-animal-health-reveals-changing-spread-of-disease-impacting-food-security-trade-and-ecosystems/ [accessed: 15 VI 2025].

Flade F., *The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror*, https://ctc.westpoint.edu/june-2018-cologne-ricin-plot-new-threshold-jihadi-bio-terror/ [accessed: 16 IX 2025].

FLI tests mobile One Health laboratory for diagnosing highly pathogenic pathogens, Friedrich Loeffler Institut, 13 VI 2025, https://www.fli.de/en/press/press-releases/press-singleview/fli-tests-mobile-one-health-laboratory-for-diagnosing-highly-pathogenic-pathogens/ [accessed: 20 VI 2025].

Food Risk Assess Europe, EFSA, https://www.efsa.europa.eu/en/publications/food-risk-assess-europe [accessed: 13 XII 2025].

Germany, European Commission, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-disaster-management-system/germany_en?utm [accessed: 15 XII 2025].

Gyles C., *Agroterrorism*, https://pmc.ncbi.nlm.nih.gov/articles/PMC2839819/pdf/cvj_04_347.pdf [accessed: 10 VI 2025].

HaDEA launches third call for tenders under BTSF, European Commission, 5 VIII 2022, https://hadea.ec.europa.eu/news/hadea-launches-third-call-tenders-under-btsf-2022-08-05_en?utm [accessed: 1 IX 2025].

Health and Food Safety, European Commission, https://commission.europa.eu/about/departments-and-executive-agencies/health-and-food-safety_en [accessed: 15 XII 2025].

*Historie der LÜKEX Krisenmanagement*übungen, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Historie/historie_node.html [accessed: 15 XII 2025].

How Lyme Disease Spreads, Centers for Disease Control and Prevention, 24 IX 2024, https://www.cdc.gov/lyme/causes/index.html [accessed: 10 IX 2025].

INMI Lazzaro Spallanzani IRCCS, Istituto Nazionale Malettie Infettive, https://www.inmi.it/ [accessed: 20 VI 2025].

International Plant Protection Convention (1997), Rome 2024, https://openknowledge.fao.org/server/api/core/bitstreams/30cc2e83-a6fd-4e2c-a5ee-312093d5a307/content [accessed: 10 VI 2025].

Krajowe Laboratoria Referencyjne (Eng. National reference laboratories), Państwowy Instytut Weterynaryjny – Państwowy Instytut Badawczy, https://www.piwet.pulawy.pl/krajowe-laboratoria-referencyjne/ [accessed: 29 VII 2025].

Laboratory Biosafety Manual. Fourth Edition, WHO, 21 XII 2020, https://www.who.int/publications/i/item/9789240011311 [accessed: 10 VI 2025].

Lessons from the COVID-19 pandemic, https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-lessons-learned-may-2023.pdf [accessed: 16 IV 2025].

National biodefense strategy and implementation plan for countering biological threats, enhancing pandemic preparedness, and achieving global health security, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf [accessed: 10 VI 2025].

National Priority Plant Pests (2024), Australian Government. Department of Agriculture, Fisheries and Forestry, https://www.agriculture.gov.au/biosecurity-trade/pests-diseases-weeds/plant/national-priority-plant-pests/ [accessed: 10 VI 2025].

NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy, NATO, 14 VII 2022, https://www.nato.int/cps/en/natohq/official_texts_197768.htm [accessed: 2 XII 2025].

One health joint plan of action 2022–2026: working together for the health of humans, animals, plants and the environment, World Health Organization, https://www.who.int/publications/i/item/9789240059139 [accessed: 10 VI 2025].

One Health: a joint framework for action published by five EU agencies, European Centre for Disease Prevention and Control, 7 V 2024, https://www.ecdc.europa.eu/en/news-events/one-health-joint-framework-action-published-five-eu-agencies [accessed: 10 VI 2025].

Ośrodek Diagnostyki i Zwalczania Zagrożeń Biologicznych (Eng. Centre for Diagnosis and Control of Biological Hazards), Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/zaklady/odizzb/organizacja [accessed: 29 VII 2025].

Our science, The Pirbright Institute, https://www.pirbright.ac.uk/our-science [accessed: 20 VI 2025].

Pavade G., *WOAH Updates – Global HPAI situation and current standards and recommendations regarding AI surveillance and vaccination,* https://www.izsvenezie.com/documents/reference-laboratories/avian-influenza/workshops/2022/pavade.pdf [accessed: 16 VI 2025].

Poland Cold Chain Logistics et 2025–2034 – Size, Share, Trends, Analysis & Forecast 2025–2034, MarkWide Research, https://markwideresearch.com/poland-cold-chain-logistics-market/ [accessed: 18 VI 2025].

Proofing the EU food supply chains against crises: new set of recommendations published, European Commission, 23 VII 2024, https://agriculture.ec.europa.eu/media/news/proofing-eu-food-supply-chain-against-crises-new-set-recommendations-published-2024-07-23_en [accessed: 14 VI 2025].

Ramakrishnan A., *What is Fusarium graminearum, the fungus US authorities say was smuggled in from China?,* AP News, 4 VI 2025, https://apnews.com/article/fusarium-graminearum-fungus-head-blight-china-8ce925ae96d9c437b987e58c336cd45f [accessed: 20 VI 2025].

Rapid Alert System for Food and Feed (RASFF), European Commission, https://food.ec.europa.eu/safety/rasff_en [accessed: 10 X 2025].

RefBio – German Contribution to Strengthen the Reference Laboratories Bio in the UNSGM, Robert Koch Institut, 10 V 2019, https://www.rki.de/EN/Institute/International-activities/Biosecurity-Programme/RefBio.html [accessed: 16 VI 2025].

Reference Laboratories, The Pirbright Institute, https://www.pirbright.ac.uk/facilities-and-resources/reference-laboratories [accessed: 17 VI 2025].

Rezerwy medyczne (Eng. Medical reserves), Rządowa Agencja Rezerw Strategicznych, https://www.gov.pl/web/rars/rezerwy-medyczne [accessed: 30 IX 2025].

Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf [accessed: 11 VI 2025].

Shadomy S., Idrissi A.E., Raizman E., Bruni M., Palamara E., Pittglio C., Lubroth J., *Anthrax Outbreaks: a warning for improved prevention, control and heightened awareness*, "Food and Agriculture Organization of the United Nations" 2016, vol. 37, https://openknowledge.fao.org/server/api/core/bitstreams/59269d58-654e-4790-ac60-a9ea7edd3a99/content [accessed: 16 IV 2025].

Terrestrial Animal Health Code, https://rr-africa.woah.org/app/uploads/2023/09/en_csatvol1-2023.pdf [accessed: 14 VI 2025].

The Biosafety Level-4 Laboratoty at RKI, Robet Koch Institut, 31 I 2024, https://www.rki.de/EN/Topics/Research-and-data/Specialised-laboratories/BSL-4-laboratory/bsl-4-laboratory-at-the-robert-koch-institute-node.html [accessed: 16 VI 2025].

Tick-Borne Encephalitis, Centers for Disease Control and Prevention, 23 IV 2025, https://www.cdc.gov/yellow-book/hcp/travel-associated-infections-diseases/tick-borne-encephalitis.html [accessed: 10 IX 2025].

Transmission of Zika Virus, Centers for Disease Control and Prevention, 30 I 2025, https://www.cdc.gov/zika/php/transmission/index.html [accessed: 10 IX 2025].

Transparency solutions for transforming the food system, EU CAP Network, https://eu-cap-network.ec.europa.eu/projects/transparency-solutions-transforming-food-system_en [accessed: 1 IX 2025].

UK Biological Security Strategy, Cabinet Office, 12 VI 2023, https://www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html [accessed: 10 VI 2025].

UK pledges 1 billion pounds to build new biosecurity centre, Reuters, 24 VI 2025, https://www.reuters.com/business/healthcare-pharmaceuticals/uk-pledges-1-billion-pounds-build-new-biosecurity-centre-2025-06-23 [accessed: 8 VIII 2025].

UKHSA Strategic Plan 2023 to 2026, https://assets.publishing.service.gov.uk/media/650d530e52e73c00139426c1/UKHSA_3_year_strategy.pdf [accessed: 18 VI 2025].

Update: Cologne couple in court over 'biological bomb plot', The Local Germany, 7 VI 2019, https://www.thelocal.de/20190607/tunisian-german-couple-in-court-over-ricin-attack-plot [accessed: 16 IV 2025].

USDA Coordinated Approach to Address New Virulences in Wheat and Barley Stem Rust – Pgt-Ug99, United States Department of Agriculture, 20 IX 2017, https://www.ars.usda.gov/ug99/ [accessed: 16 VI 2025].

West Nile: Causes and How It Spreads, Centers for Disease Control and Prevention, 19 VIII 2025, https://www.cdc.gov/west-nile-virus/causes/index.html? [accessed: 10 IX 2025].

What is EPPO Global Database?, https://gd.eppo.int/ [accessed: 10 VI 2025].

What past disruptions can teach us about reviving supply chains after COVID-19, World Economic Forum, 27 III 2020, https://www.weforum.org/stories/2020/03/covid-19-coronavirus-lessons-past-supply-chain-disruptions/ [accessed: 27 V 2025].

What We Do, European Centre for Disease Prevention and Control, https://www.ecdc.europa.eu/en/about-ecdc/what-we-do [accessed: 30 IX 2025].

White E., *US says it broke up effort to bring toxic fungus to Michigan lab from China*, AP News, 3 VI 2025, https://apnews.com/article/chinese-scientists-charged-toxic-fungus-5ccaba9aff8e5941ebcea71b9b6690b2 [accessed: 20 VI 2025].

Wojskowy Instytut Higieny i Epidemiologii im. Generała Karola Kaczkowskiego, https://wihe.pl/wihe/o-nas [accessed: 29 VII 2025].

Zadania badawczo-rozwojowe (Eng. Research and development tasks), Wojskowy Instytut Higieny i Epidemiologii, https://wihe.pl/wihe/zadania [accessed: 29 VII 2025].

Zwalczanie i monitoring wybranych chorób zakaźnych zwierząt (Eng. Combating and monitoring of selected infectious animal diseases), Główny Inspektorat Weterynarii, https://www.wetgiw.gov.pl/nadzor-weterynaryjny/programy-zwalczaniamonitorowania-chorob-zakaznych-zwierzat [accessed: 1 IX 2025].

Legal acts

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (Journal of Laws of 1976 no. 1 item 1).

Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (Official Journal of the EU L 314/26 of 6 XII 2022).

Regulation (EU) 2021/522 of the European Parliament and of the Council of 24 March 2021 establishing a Programme for the Union's action in the field of health ('EU4Health Programme') for the period 2021–2027, and repealing Regulation (EU) No 282/2014 (Official Journal of the EU L 107/1 of 26 III 2021).

Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (Official Journal of the EU L 31/1 of 1 II 2002).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Official Journal of the EU L 333/164 of 27 XII 2022).

Act of 13 February 2020 on the State Plant Health and Seed Inspection Service (consolidated text, Journal of Laws of 2023, item 1992).

Act of 25 August 2006 on food and nutrition safety (consolidated text, Journal of Laws of 2023, item 1448, as amended).

Act of 11 March 2004 on protection of animal health and combating contagious animal diseases (consolidated text, Journal of Laws of 2023, item 1075).

Act of 29 January 2004 on the Veterinary Insection (consolidated text, Journal of Laws of 2024, item 12).

Act of 18 December 2003 on plant protection (consolidated text, Journal of Laws of 2019, item 972, as amended).

Act of 21 December 2000 on commercial quality of agri-food products (consolidated text, Journal of Laws of 2023, item 1980).

Act of 14 March 1985 on the State Sanitary Inspection (consolidated text, Journal of Laws of 2024, item 416).

Matylda Augustyn-Barwicz

Specialist in biotechnology, biosafety and the management of high-containment biological laboratories. She currently serves as the Insectary Manager at Pirbright Institute (Great Britain), where she is responsible for overseeing CL2 laboratories and for operational cooperation with CL3 and SAPO 4 laboratories.

She completed studies in biotechnology and neuroendocrinology at the Jagiellonian Univeristy in Kraków and the Polish Academy of Sciences. Her professional experience includes many years of service in state formations responsible for security and crisis response within the structures of the Ministry of the Interior and Administration as well as the Ministry of National Defence.

Contact: matylda.augustyn@gmail.com

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 341–387

https://doi.org/10.4467/27204383TER.25.057.23044

Article

Twenty years since the attacks on London's public transport system. The problem of Islamic terrorism in the United Kingdom

KRZYSZTOF IZAK

https://orcid.org/0000-0001-9815-6035

Independent author

Abstract

The aim of this article is to describe the terrorist attacks on London's public transport system that took place on 7 July 2005 and terrorist threat in Great Britain, posed by the radicalisation of Muslim communities inspired by spiritual leaders inciting violence. The author discussed the background to these attacks extensively. Then, based on investigation reports, among other sources, he presented profiles of the perpetrators, preparations for the attacks, their course and an attempt to repeat them two weeks later. He pointed out problems in ensuring anti-terrorist security in Great Britain, resulting, among other things, from a policy of tolerance towards Muslim extremists.

Keywords

Al-Muhajirun, Muslim extremism, immigrants, secret services, terrorist threat, attacks

Introduction

Since the beginning of the 21st century, the United Kingdom has been fighting Islamic terrorism, which stems from external factors, including the activities of global Salafi jihadist organisations, London's policies, including the participation of British troops in military operations in Iraq and Afghanistan, the dynamic growth in the number of immigrants from Muslim countries, and the radicalisation of British citizens of immigrant origin who have found favourable living conditions in the United Kingdom. They enjoyed many privileges and brought their relatives to the country. They demanded that local law be adapted to the needs of their minority. They fought for the application of Sharia law in civil matters. The implementation of a multicultural policy in the United Kingdom meant that the threat posed by the uncontrolled spread of radical Islam was not recognised. Dissidents persecuted in their home countries for spreading anti-government propaganda and members of Muslim extremist organisations, including terrorists, could count on asylum in the United Kingdom. In the 1990s, trips to the country of their ancestors became commonplace for young British citizens of Pakistani origin, who constituted the largest Muslim minority. They underwent military training in Taliban and Al-Qaeda camps. There, they were exposed to ideas previously unknown to them and returned with the intention of spreading them in the United Kingdom, including hatred of religions other than Islam and hostility towards Shiites and Ahmadis. Young people of Pakistani origin quickly became radicalised under the influence of slogans preached in mosques by imams and preachers. They became particularly active after the 11 September 2001 attacks in the United States. Although the British security services monitored and arrested individuals suspected of preparing terrorist attacks, jihadist propagandists remained unpunished for a long time. The participation of British forces in military operations in Afghanistan and Iraq led to a sharp increase in the terrorist threat in the United Kingdom.

The attacks of 7 July 2005 on London's public transport system, in which four bombs were detonated (three on London Underground trains and one on a city bus), were the first in a long series of successful attacks and foiled attempts to carry them out. The aim of the article was to describe these attacks and terrorist threat in the United Kingdom related to the radicalisation of Muslim communities inspired by spiritual leaders inciting violence.

Islamic extremism – terrorist threats in the United Kingdom until 2005

Until 2005, the United Kingdom managed to avoid terrorist attacks by Islamic extremists, despite the fact that a large group of radicals openly proclaiming their views lived there. The headquarters of the Tablighi Jamaat (Association for the Propagation of Faith) coordination centre for Europe was established in Dewsbury, West Yorkshire, in northern England. Leicester in central England was chosen as the location for the headquarters of the Federation of Muslim Organisations, which is strongly influenced by the Muslim Brotherhood movement (Al-Ikhwan al-Muslimin, MB), which also influences the Muslim Association of Britain (MAB). One of the founders of MAB, Kamal al-Halbawi, became the official spokesperson for MB in Great Britain in 1995. Leicester is also home to the Islamic Foundation (IF), established by Khurshid Ahmad, an activist of the Pakistani religious party Jamaat-e-Islami[1]. The MB movement operated in the United Kingdom through a network of interconnected organisations of Palestinian, Syrian, Libyan, Somali, Iraqi and Egyptian origin. Apart from IF and MAB, the most significant ones included the Muslim Welfare Trust, the Palestinian Relief and Development Fund (Interpal), the Palestine Return Centre, the Institute for Islamic Political Thought, the Islamic Centre in London, the Muslim Public Affairs Committee and moreover, the media company Mashreq Media Services, which published Hamas' newspaper *Filastin al-Muslimah* (Muslim Palestine) and the pro-Hamas English-language magazine *Palestine Times*[2].

The capital of Great Britain has become an important ideological centre for Muslim extremism and Salafi jihadist networks influencing the entire world. In the 1970s, one Algerian fundamentalist declared: *Here in London, there is freedom. They leave us alone and even help us*[3]. For over 40 years, London was the main base for Islamic extremism, and in the 1980s and 1990s, it was its point of contact. Almost all Muslim movements, from moderate to the most extremist, were located there. London remained

[1] S. Besson, *Islamizacja Zachodu? Historia pewnego spisku* (Eng. The Islamisation of the West? The story of a conspiracy), Warszawa 2006, pp. 125–126, 129.

[2] M. Whine, *The Penetration of Islamist Ideology in Britain*, Hudson Institute, 18 V 2005, https://www.hudson.org/national-security-defense/the-penetration-of-islamist-ideology-in-britain [accessed: 18 XI 2025].

[3] X. Raufer, *Atlas radykalnego islamu* (Eng. Atlas of Radical Islam), Warszawa 2011, p. 87.

a place of recruitment and financing for radical Muslim organisations from various countries around the world. Many volunteers travelling to the jihad front in Afghanistan, Yemen, Chechnya, Bosnia or Kashmir passed through London. The volunteers' trips were organised by well-structured networks benefiting from the financial support of local charities[4].

The city is referred to as 'Londonistan'. The term was first used in 1990 by French counter-terrorism services and the governments of Pakistan and Saudi Arabia[5]. This refers to London as the headquarters of many extremist groups and radical leaders who organise terrorist attacks in other countries. 'Londonistan' became a safe haven for radical Muslim activists such as Omar Bakri Mohammad, one of the founders of the British branch of the Islamic Liberation Party (Hizb ut-Tahrir Islami) and later the Emigrants (Al-Muhajirun) group, who openly supported the attacks in the US on 11 September 2001 and called for the unification of Muslims and the creation of a global caliphate. He was a close friend of Mustafa Kamal Mustafa, better known as Abu Hamza al-Masri, leader of the Ansar al-Sharia organisation and charismatic imam of the Grand Mosque in Finsbury Park, who called for jihad and the destruction of the infidel West. Radical views were also espoused by Omar Mahmud Osman, alias Abu Katada al-Filastini, editor-in-chief of the weekly magazine *Al-Ansar*, which in the 1990s provided propaganda support for the Algerian Armed Islamic Group (Al-Jama'ah al-Islamiyah al-Musallaha) by providing it with media coverage and links to Salafi jihad. Abu Katada also supported Al-Qaeda's activities in Europe[6].

In the 1990s, London became the global centre of the Arab press, including the aforementioned *Filastin al-Muslima* and *Al-Hayat* (Life), *Al-Quds Al-Arabi* (Arab Jerusalem), *Asharq al-Awsat* (Middle East) and *Risalat al-Ichwan* (Message of the Brothers), as well as the Middle East Broadcasting Corporation and many specialist Islamic publications[7]. Some of Osama bin Laden's fatwas were first published in London. In turn, Ayman al-Zawahiri, Osama bin Laden's deputy, published an abridged version

[4] Ibid.

[5] M. Zawadewicz, *Życie codzienne w muzułmańskim Londynie* (Eng. Daily life in Muslim London), Warszawa 2008, p. 134.

[6] K. Izak, *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014, p. 127, 358–359.

[7] M. Phillips, *Londonistan. Jak Wielka Brytania stworzyła państwo terroru* (Eng. Londonistan: How Britain is Creating a Terror State Within), Warszawa 2010, pp. 40–41.

of his manifesto entitled *Fursan tahta rayat an-Nabi* (Knights under the Banner of the Prophet) in *Asharq al-Awsat* in December 2001. In it, he presented Al-Qaeda's strategy, starting with the attacks of 11 September 2001, which were intended to provoke a US attack on Muslims and lead to a global jihad, i.e. a struggle between Islam and its hostile forces, namely the Western powers and Russia[8]. In December 2002, Al-Zawahiri published an article in *Al-Quds al-Arabi* entitled *Al-wala wa-l-bara* (Loyalty and Renunciation or Fidelity and Schism), in which he presented the Koranic definition of Muslim identity. It consists of mutual fidelity among all Muslims and their isolation from Jews and Christians, apostates and heretics[9]. In London, radical groups bringing together immigrants and political refugees from Muslim countries were formed in an Islamist movement with a global reach. At the turn of the 1980s and 1990s, a series of conferences were held in the United Kingdom. They brought together Muslim radicals from around the world, ranging from violent organisations such as Hamas and Hezbollah to Muslim political parties participating in parliamentary elections in Jordan and Malaysia[10].

The United Kingdom provided refuge for radical ideologues of Muslim fundamentalism who were persecuted in their own countries. They were granted political asylum on condition that they did not put their ideas into practice within the territory of the United Kingdom. However, they were free to express them, even in extreme forms, openly calling for jihad against the West. This did not change even after the 11 September attacks. On 14 December 2001, Parliament passed a new anti-terrorism law (the *Anti-terrorism, Crime and Security Act 2001*) allowing for the arrest of foreigners suspected of terrorist activity. However, the activities of extremist organisations, from which terrorists often emerged, were tolerated. Among them were individuals who carried out terrorist

[8] M.B. Shishani, *Salafi-Jihadists Geopolitical Perspective of Central Asia*, Central Asia – Caucasus Analyst, https://www.cacianalyst.org/publications/analytical-articles/item/10050-analytical-articles-caci-analyst-2005-6-29-art-10050.html [accessed: 29 VI 2025]. The full text of the manifesto is included in Laura Mansfield's book, *His Own Words: Translation and Analysis of the Writings of Dr. Ayman Al Zawahiri*, New York 2006.

[9] J. Gilliam, *Why They Hate Us. An Examination of al-wala' wa-l-bara' in Salafi-Jihadist Ideology*, Military Review, 15 II 2018, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Feb/They-Hate/ [accessed: 15 VII 2025].

[10] M. Phillips, *Londonistan*..., p. 42.

operations or attempted attacks in Europe, Asia, Africa and North America[11]. For example, on 30 April 2003, two terrorists carried out a suicide attack on Mikes Place bar on Tel Aviv beach, frequented by Western foreigners. Three people were killed and 65 were injured. The perpetrators were British nationals of Pakistani origin. The first, Asif Mohammad Hanif from London, was killed in the attack. The second, Omar Khan Sharif from Derby, survived, but drowned while attempting to escape. This was the first attack in which Hamas used terrorists who were not native Palestinians. According to British intelligence, the perpetrators were recruited in the United Kingdom and then spent some time in Syria, where they met with Hamas fighters and were trained. In March 2004, Hamas released a video containing the joint will of the attackers and information that the attack was to coincide with the first anniversary of the assassination by Israeli forces of Ibrahim al-Makadma, founder of the Izz ad-Din al-Qassam Brigades[12].

Although London stood alongside Washington in the war on terrorism in 2001, British territory seemed secure against any attempted attack until disturbing signs forced the government to radically change its policy. In 2002, a government strategy known as CONTEST was developed, which combined the activities of all services to reduce the threat of international terrorism[13]. Despite this, no decisive action was taken against manifestations of Islamic extremism and hate speech. On 11 September 2002, on the first anniversary of the attacks in the US, the Al-Muhajiroun organisation held a conference at the Finsbury Park Mosque entitled 'A Great Day in History', during which it presented what it considered to be the positive – according the organisation – aspects of the attack. Al-Masri gave a lecture in which he praised the plane hijackers, and Omar Bakri Mohammad called them 'the magnificent nineteen'[14]. At that time, the Finsbury Park Mosque was

[11] Ibid., p. 44.

[12] M. Levitt, *Hamas. Polityka, dobroczynność i terroryzm w służbie dżihadu* (Eng. Hamas: politics, charity, and terrorism in the service of jihad), Kraków 2008, pp. 293–294.

[13] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c470140f0b62dffde1050/isc_terrorist_attacks_7july_report.pdf, p. 5 [accessed: 18 XI 2025].

[14] *Abu Hamza profile*, BBC News, 9 I 2015, https://www.bbc.com/news/uk-11701269 [accessed: 18 XI 2025]; *"Magnificent 19" risks further outrage*, The Standard, 13 IV 2012, https://www.standard.co.uk/hp/front/magnificent-19-risks-further-outrage-6948639.html [accessed: 18 XI 2025].

one of the most active recruitment centres for Islamic militants in London. Muslim extremists from both the United Kingdom and other countries used to meet there. It was at this mosque that Richard Reid, the famous 'shoe bomber', was recruited. In the late 1990s, he underwent military training in Afghanistan, and after returning to London, he became an active member of an extremist cell centred around Al-Masri. Reid smuggled explosives onto an American Airlines flight from Paris to Miami on 22 December 2001. He was overpowered by passengers while attempting to detonate the explosives[15]. Many other terrorists listened to Al-Masri's militant sermons, including Hanif and Sharif, mentioned above, Kamal Bourgass[16], Zacarias Moussaoui (alleged 20th bomber of 11 September 2001) and three of the four bombers of 7 July 2005 (Mohammad Sidique Khan, Shehzad Tanweer and Jermaine Lindsay)[17].

In November 2002, six people from Morocco and Tunisia were arrested in London. They were accused of planning an attack on the London Underground. They had no permanent address and were unemployed. One of the suspects admitted to having undergone military training in Afghanistan. A month later, four Algerian nationals suspected of planning a terrorist attack were arrested in London and Edinburgh. In January 2003, five Algerians and one Ethiopian who had arrived in the United Kingdom two years earlier and applied for asylum were detained. Traces of ricin were found in their flat in north London[18].

In 2003, the terrorist threat in the United Kingdom increased in connection with the invasion of Iraq by American and British forces. The Finsbury Park Mosque was closed at that time because CS gas, a complete set of protective clothing against chemical and biological

[15] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism. The British Connections*, London 2010, pp. 308–309.

[16] An Algerian man who killed Detective Stephen Oake in Manchester in January 2003 while attempting to resist arrest by British police, suspected of attempting to carry out a terrorist attack in the United Kingdom using ricin, a powerful poison. See: *Terror Watch: What Ricin?*, Newsweek, 12 IV 2005, https://www.newsweek.com/terror-watch-what-ricin-116577 [accessed: 18 IX 2025].

[17] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism...*, pp. 46–48, 213, 216, 220, 342, 384, 386; C. Marsden, *Britain: Why did it take so long to bring Abu Hamza to trial?*, World Socialist Web Site, 16 II 2006, https://www.wsws.org/en/articles/2006/02/hamz-f16.html [accessed: 16 VII 2025]; D. Strieff, *Terror-tinged U.K. mosque gets a makeover*, NBC News, 5 VII 2006, https://www.nbcnews.com/id/wbna13501930 [accessed: 18 IX 2025].

[18] X. Raufer, *Atlas radykalnego islamu...*, p. 92.

weapons, poison, handcuffs, gas weapons and many blank British passports, driving licences and credit cards, as well as the famous 11-volume encyclopaedia of Afghan jihad, a handbook on terrorism, were found there. Seven people were arrested at the time on suspicion of possessing ricin[19]. Al-Masri remained at large. The closure of the mosque did not prevent the preacher from delivering sermons on the street in front of the building and in other mosques in central England. However, no action was taken to stop his activities, even after he issued a fatwa stating that the United Kingdom's active involvement in the invasion and occupation of Iraq made it a legitimate target for attack. According to, among others, *The Guardian* newspaper, security service agents and police officers were opposed to his arrest, hoping that he would provide information about attempts to carry out terrorist attacks in the United Kingdom[20].

In May 2003, six Islamic extremists were arrested in Nottinghamshire, central England, as part of an investigation into a suicide bombing in Tel Aviv[21]. Scotland Yard officers estimated at the time that around 50 highly trained fighters out of 200 British nationals trained in Afghanistan had returned to the United Kingdom and formed operational terrorist groups[22]. In June, the Joint Terrorism Analysis Centre (JTAC) was established under MI5 to assess and analyse the terrorist threat in the United Kingdom.

[19] W. Hoge, *Threats and Responses: Terror Suspects, Mosque Raid in London Results in 7 Arrests in Connection With Discovery of Poison*, The New York Times, 21 I 2003, https://www.nytimes.com/2003/01/21/world/threats-responses-terror-suspects-mosque-raid-london-results-7-arrests.html [accessed: 18 IX 2025].

[20] P. Owen, *Clarke rejects Hamza inquiry calls*, The Guardian, 9 II 2006, https://www.theguardian.com/uk/2006/feb/09/terrorism.politics [accessed: 18 IX 2025]; E.F. Vencat, *'Bleed the Enemy'*, Newsweek, 11 I 2006, https://www.newsweek.com/bleed-enemy-108227 [accessed: 11 VII 2025]. In May 2004, Abu Hamza al-Masri was arrested at the request of the United States, which sought his extradition. In October 2004, the British judiciary brought 15 charges against Al-Masri, including incitement to kill infidels and possession of propaganda material encouraging terrorist activities. In February 2006, Al-Masri was found guilty of 11 of the 15 charges against him and sentenced to seven years in prison. In October 2012, after an eight-year legal battle, he was extradited from the UK to the US. There, in May 2014, he was found guilty on 11 counts of terrorism. On 9 January 2015, he was sentenced to life imprisonment without the possibility of parole. See: X. Raufer, *Atlas radykalnego islamu…*, p. 92; *Radical cleric Abu Hamza jailed for life by US court*, BBC News, 9 I 2015, https://www.bbc.com/news/world-us-canada-30754959 [accessed: 18 IX 2025].

[21] X. Raufer, *Atlas radykalnego islamu…*, p. 92.

[22] Ibid.

Five threat levels were identified: low, moderate, substantial, severe and critical[23].

In November 2003, during President George W. Bush's visit to London, attacks took place in Istanbul, in which Muslim terrorists targeted the British bank HSBC and the British consulate[24]. In December of the same year, Afghan veteran Andrew Rowe, who was linked to French jihadist Lionel Dumont, a member of the so-called Roubaix gang, was arrested[25]. In March 2004, 600 kg of potassium nitrate used in the production of explosives was discovered in the suburbs of London. Eight British citizens of Pakistani origin, aged between 17 and 32, were arrested. One of them, Mohammed Babar, who was associated with Omar Khyam, testified that the group intended to carry out attacks on a London nightclub, a shopping centre in Kent, and energy and gas infrastructure[26]. In 2004, the Al-Muhajiroun organisation was banned. It recruited Muslim students from British universities for ideological and military training in Pakistan, Afghanistan, Yemen and Sudan. However, Al-Muhajiroun was replaced by two cooperating groups: the Salvation Sect (Firkat an-Naja) and Al-Ghuraba (The Strangers). Both groups were united not only by the idea of moral purity and the promotion of orthodox Islam in the spirit of the first Muslims, but also by the person of Anjem Choudary, a close associate of Omar Bakri Mohammad[27]. The leaders of the new groups avoided making aggressive statements and officially distanced themselves from extremist propaganda. They removed hostile slogans from their websites registered in the British Isles, but kept links to websites based in Muslim countries, including Indonesia and Bangladesh, which contained random links to

[23] *Terrorism threat levels*, Security Service MI5, https://www.mi5.gov.uk/threats-and-advice/terrorism-threat-levels [accessed: 23 VI 2025].

[24] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism*..., p. 18.

[25] Ibid.

[26] X. Raufer, *Atlas radykalnego islamu*..., p. 92; R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism*..., p. 18.

[27] In 2005, after twenty years in the United Kingdom, Omar Bakri Mohammad voluntarily left for Lebanon, where he was informed by the British authorities that he was banned from returning to the United Kingdom for life. However, he did not cease his activities and participated remotely in meetings and conferences organised by Islamic extremists in London. See: K. Izak, *Leksykon organizacji*..., p. 359.

extremist content, devoid of keywords typical for propaganda of radical Muslim circles[28].

In 2004, British security services increased their interest in groups composed mainly of British citizens of Pakistani origin. This was the result of the discovery of a cache of potassium nitrate and the case of an Afghan veteran who refused to carry out a suicide mission similar to Reid's[29]. On 3 August 2004, a group directly linked to Al-Qaeda and led by Dhiren Barot, alias Abu Musa al-Hindi, a veteran of the war in Afghanistan, was arrested[30]. At the same time, an attempt was made to change the British political doctrine of multiculturalism. This change concerned support for the separate cultural development of individual ethnic and religious groups of foreign origin, valuing the differences between them and their specific signs of identity. At the same time, it entrusted community leaders with the task of enforcing public order – they were to command social peace from the mosques[31]. On 3 April 2004, Mark Trevor Phillips, chairman of the British Parliamentary Commission for Racial Equality, which had made multiculturalism a key element of social policy, criticised it for the first time, declaring in a press interview that multiculturalism was a term that (...) *has lost its meaning* (...). *Multiculturalism suggests separation*. (...) *We should therefore rather talk about how to move from it to an integrated society in which everyone is equal before the law and common values prevail: democracy rather than violence, the common use of the English language and subordination to the culture of the British Isles*[32]. This statement was poorly received by followers of Islam. During a demonstration organised in London in support of young British men of Pakistani descent imprisoned, they burned the British flag while shouting 'Allah Akbar'[33]. This event raised questions about the significance of integration and multicultural policies, factors determining their success or failure[34].

---

[28] Ibid., p. 358, 360.

[29] G. Chaliand, A. Blin. *Historia terroryzmu. Od starożytności do Da'isz* (Eng. The history of terrorism. From antiquity to Daesh), Warszawa 2020, p. 393.

[30] Ibid.; *Al-Qaeda plotter jailed for life*, BBC News, 7 XI 2006, http://news.bbc.co.uk/2/hi/uk_news/6123236.stm [accessed: 7 VIII 2025].

[31] Ibid.

[32] G. Kepel, *Fitna, wojna w sercu islamu* (Eng. Fitna, war in the heart of Islam), Warszawa 2006, p. 222.

[33] Ibid.

[34] Intelligence and Security Committee, *Report into the London Terrorist Attacks...*, p. 17.

The perpetrators of the attack

The suicide attack in London was carried out by four men aged between 18 and 30. Three of them: Mohammad Sidique Khan (30), Shehzad Tanweer (22) and Hasib Hussain (18) were born in the United Kingdom. Their parents had arrived there many years earlier and settled in Beeston and Holbeck, suburbs of Leeds. They found work there and obtained British citizenship. Each of them came from large families. They all attended local schools and mosques. The fourth bomber, Jermaine Lindsay (19), was from Jamaica[35].

Khan, the eldest of them, later identified as the leader of the terrorist cell, was remembered as a diligent, quiet student who never caused any trouble. After graduating from school, he worked for a local aid agency and then for the Department of Trade and Industry[36]. In 1996, he began studying business at Leeds Metropolitan University. While still a student, he began working with young people, and after graduating in 2001, he was employed as a teacher at a school in Beeston, an educational institution for children with language and behavioural difficulties[37]. He was highly regarded by teachers and parents. In 2002, he gave an interview to the *Times Educational Supplement*, in which he spoke passionately about his work[38]. At the same time, he became known as a devout Muslim. He prayed regularly at work and mosque. He said that he did not have a peaceful youth, easily getting into fights, drinking alcohol and taking drugs. He was also involved in drug dealing and had several conflicts with the police, including warnings for assault and handling stolen goods. He broke with that life and turned to religion. According to those around him, he was not aggressive, radical or politicised in the way he spoke about religion to his charges[39]. However, this turned out to be an illusion, as Khan was leading a double life. On the one hand, he was extremely socially engaged, and on the other, he was conducting covert jihadist activities.

In July 2001, Khan and his close friend Wahid Ali travelled to the Manser training camp in the Pakistan-controlled part of Kashmir. The camp was

[35] *Report of the Official Account of the Bombings in London on 7th July 2005*, https://assets.publishing.service.gov.uk/media/5a7c7bc840f0b626628ac62e/1087.pdf, pp. 15–16 [accessed: 7 VII 2025].

[36] Ibid., p. 13.

[37] Ibid.

[38] *Report of the Official Account...*, p. 14, 16.

[39] Ibid., p. 14.

run by the Mujahideen Movement (Harakat ul-Mujahideen). From there, they travelled to north-eastern Afghanistan and reached the front line between the Taliban and the Northern Alliance. They returned home a few days before the attacks of 11 September 2001. At school, Khan officially spoke out against these attacks[40]. According to Artur Wejkszner, citing Simon Elegant's article entitled *A London Bomber's Asia Tour*, published in *The Time* on 26 September 2005, after completing military training at the Manser camp, Khan moved to a Taliban camp near Bagram, not far from Kabul. After American forces entered Afghanistan on 7 October 2001 and provided support to the Northern Alliance, he actively defended the Taliban regime. He then went on a reconnaissance mission to Malaysia, where he met with Riduan Isamuddin, alias Hambali, a member of the Indonesian Muslim Community (Jemaah Islamiyah). Khan's main task was to find out how much money the organisation needed for its terrorist activities. During his visit to Borneo, Khan met with Nasir Abbas, a high-ranking member of Jemaah Islamiyah, with whom he travelled to the organisation's base on the Philippine island of Mindanao. There, he was to meet with Azhari Husin, who was responsible for preparing most of the explosives used by Jemaah Islamiyah terrorists[41]. According to a report by the special services prepared for the House of Commons, media reports concerning Khan's visit to Malaysia and the Philippines were investigated and deemed to be unfounded[42].

At the turn of 2001 and 2002, Khan began regularly attending the Finsbury Park Mosque in London, where he made contact with Al-Masri and his close associate Harun Rashid Aswat, who had undergone military training in Pakistan and Afghanistan. After returning to London, he was responsible for recruiting new members. Khan personally supported, and may also have been responsible for recruiting, Omar Sharif and Asif Hanifa, who carried out a suicide attack in Tel Aviv in April 2003. Khan is believed to have visited Israel in February 2003, probably to conduct reconnaissance prior to the attack[43].

---

[40] Ibid.; *Profile: Mohammad Sidique Khan,* BBC News, 2 III 2011, https://www.bbc.com/news/uk-12621381 [accessed: 2 VI 2025].

[41] A. Wejkszner, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu* (Eng. The evolution of religiously motivated terrorism as exemplified by the Salafi global jihad movement), Poznań 2010, pp. 346–347.

[42] *Report of the Official Account…*, p. 20.

[43] A. Wejkszner, *Ewolucja terroryzmu…*, p. 346; R. Simcox, H, Stuart, H. Ahmed, *Islamist Terrorism…*, p. 213.

Khan's official social life revolved around youth clubs, a Muslim bookshop and a gym. Until 2003, he sat on the management committee of one such club. Khan's community work allowed him to establish close ties with Tanweer and Hussain, for whom Khan, whom they called 'Sidi,' was a mentor.

Working with young people began to give way to establishing contacts with Islamic radicals[44]. In 2003, Khan met Omar Khyam, a British citizen of Pakistani origin who had previously travelled to northern Pakistan, where he underwent training in the manufacture of fertiliser bombs at a camp in the Malakand district. That same year, the two travelled to Pakistan with a group of British jihadists, probably also to Malakand. After their return, they planned another trip, but Khan postponed it due to his wife's pregnancy. In February and March 2004, Khan met several times with Khyam, who was already under surveillance by MI5. In April 2004, Khyam was arrested on charges of leading a conspiracy to detonate a high-powered explosive device in London. Khan was not a suspect in this case[45]. However, he was dismissed from his job. The school administration decided that his sick leave from 20 September to 19 November 2004 was unjustified. On 19 November, Khan left for Pakistan[46].

Tanweer also lived in Beeston. He came from a well-off family and was a good student and a talented sportsman. From an early age, he took religion seriously, but showed no signs of extremism. At school, he was remembered as calm, modest and popular among his peers. At the age of 16, he became very religious. He developed his sporting interests at Leeds Metropolitan University, where he received a Higher National Diploma after two years of study. In 2003, he left the university and did not continue his studies. During his studies, he turned even more towards religion, to which he devoted more and more time. This was probably the reason why he dropped out of university. While still a student, he attended a religious school in Dewsbury. However, there were no signs that this had turned into religious fanaticism, even though he repeatedly visited the Finsbury Park Mosque in the company of Khan[47]. In April 2004, he received a warning for indecent behaviour, but otherwise had no trouble with the police.

[44] Ibid., p. 16.

[45] R. Simcox, H, Stuart, H. Ahmed, *Islamist Terrorism...*, pp. 24–26.

[46] *Profile: Mohammad Sidique Khan...*

[47] A. Wejkszner, *Ewolucja terroryzmu...*, p. 346.

On 19 November 2004, he travelled to Pakistan with Khan, and after returning to Leeds, he did not work and was supported by his family.

Hussain lived in the Holbeck district. He was not an outstanding student. He was quiet at school and did not have many friends. He became involved in racial protests, but did not attract attention with aggressive behaviour[48]. At the beginning of 2002, he went on a traditional pilgrimage to Mecca (hajj) with his family. After returning to his country, he began to manifest his religiosity. He wore traditional Muslim clothing and praised Al-Qaeda, calling the 11 September 2001 attackers martyrs. He told his teacher that he wanted to become an imam after finishing his studies. In 2004, he was punished for shoplifting, but apart from that incident, he had no problems with the police. In 2005, he obtained a vocational diploma in business from South Leeds College[49].

Lindsay was an outsider among the group of attackers. He was born in Jamaica in 1985, his father quickly abandoned them. The following year, his mother, son and another man moved to the United Kingdom. They settled in Huddersfield, England. Jermaine attended local schools. He was popular among his peers, intelligent, artistically, musically and athletically gifted. He trained in kickboxing and martial arts[50]. In 2000, Lindsay's mother converted to Islam, and he followed suit shortly afterwards, taking the name Djamal. His conversion to Islam was accompanied by a change in the environment in which he often spent time. He spent more and more time at the mosque. In Huddersfield and neighbouring Dewsbury, he was admired for the speed with which he became proficient in Arabic and memorised large sections of the Koran. He was 15 years old at the time. Despite his young age, he showed maturity and seriousness. He regularly wore a long Arabic robe (jellabiya)[51]. It is believed that Lindsay was greatly influenced by the radical preacher Abdullah al-Faisal, also of Jamaican origin, a colleague of Al-Masri, convicted in 2003 and then deported to Jamaica for dissemination of propaganda materials of an extremist nature, inciting racial hatred and urging the killing of 'infidels'[52]. Jermaine was punished for distributing leaflets supporting Al-Qaeda at school. In 2002, his mother

[48] *Report of the Official Account…*, p. 15.

[49] Ibid.

[50] Ibid., p. 17.

[51] Ibid., p. 18.

[52] Ibid.; R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism…*, pp. 14–15.

moved to the US to live with her third partner, leaving the boy alone in the family home. This event was a traumatic experience for him. He dropped out of school and lived on benefits. He also did odd jobs, including selling mobile phones and books about Islam[53]. He met Samantha Lewthwaite, a British woman who had converted to Islam, online, and they participated in the 'Stop the War' march organised in London on 30 October 2002. They married and settled in Huddersfield. After the closure of the Finsbury Park Mosque in 2003, Lindsay and Tanweer visited Al-Masri when gatherings with his participation were organised in front of the temple[54]. In September 2003, Lindsay moved with his wife to Aylesbury, but they spent a lot of time in Huddersfield. It was probably in the second half of 2004, in Huddersfield or Dewsbury, that Lindsay met Khan[55].

The preparations for the attack

The turning point in the preparations for the terrorist attacks in London was Khan and Tanweer's trip to Pakistan. It took place on 19 November 2004 and lasted until 8 February 2005. Previously, Khan had travelled there alone or with other people, and his trips were not for the purpose of visiting family. Tanweer informed his family and friends that he was going to Pakistan to broaden his religious knowledge. Khan's friends, on the other hand, believed that he was going to Pakistan to cross the border into Afghanistan, where he had previously stayed. In Pakistan, the two men went their separate ways. Tanweer stayed with his uncle in Faisalabad. After a week, Khan came to pick him up and they both headed north. Tanweer informed his family that they were going to the Lahore area to visit one of the religious schools[56]. It is possible that both men travelled to one of the training camps in Malakand, where Khan may have established contacts with Al-Qaeda during an earlier trip. One of its representatives in the United Kingdom was Mohammed Kayyum Khan, who in July 2003 organised Khan's trip to the training camp in Malakand. Tanweer, in turn, established contacts with the Army of Muhammad (Jaish-e Mohammed)

[53] *Report of the Official Account...*, p. 18.

[54] A. Wejkszner, *Ewolucja terroryzmu...*, p. 347.

[55] *Report of the Official Account...*, p. 18.

[56] Ibid., p. 20.

organisation[57]. It is also mentioned that both underwent training in the manufacture of explosives. This training was organised for them by Rashid Rauf, a British citizen living in Pakistan. The training took place in a rented house in Islamabad, where Khan and Tanweer made a film about martyrdom, which was to be released after their deaths[58]. The decision to carry out an attack in London was therefore made in Pakistan. Tanweer claimed that he had not found a suitable school to study Islam[59].

After returning to the country, Khan and Tanweer began to implement key elements of the attack plan. Both resigned from their jobs. They involved Hussain and Lindsay in their activities. From April 2005 onwards, the men spent a lot of time together. In May, they rented a modern flat at 18 Alexandra Grove. This put them far away from the Beeston area, where they were well known. They did not attract attention in their new location, as the neighbourhood was mainly inhabited by students renting flats. The Grand Mosque was located nearby. The flat was rented to them by an Egyptian, Magdy Elnashar, whom Lindsay met at the mosque in November 2004. Elnashar obtained his PhD in chemistry from Leeds Metropolitan University in May 2005 and left for a holiday in his home country in June, intending to return to the UK to continue his research work[60].

In a rented flat, the bombers began constructing explosives using readily available and inexpensive chemicals. To avoid arousing suspicion, they bought them in batches. They made their first purchase on 31 March 2005[61]. It can therefore be assumed that before they rented the flat, they already had a significant amount of chemicals in their possession. These included acetone (solvent) and hydrogen peroxide (bleach or hydrogen peroxide), sulphuric or hydrochloric acid and distilled water combined in appropriate proportions. This produces an explosive material in the form

[57] R. Simcox, H. Stuart, H. Ahmed, *Islamist Terrorism…*, p. 213, 456.

[58] *Shehzad Tanweer*, Counter Extremism Project, https://www.counterextremism.com/extremists/shehzad-tanweer [accessed: 27 VI 2025].

[59] *Report of the Official Account…*, p. 20.

[60] *Chemistry student held in Cairo*, The Guardian, 15 VII 2005, https://www.theguardian.com/uk/2005/jul/15/july7.uksecurity10 [accessed: 15 VII 2025]. A week after the attacks, Magdy Elnashar was arrested in Cairo. Initially, he was considered to be the mastermind and instigator of the London bombings, or the founder of the group of bombers. Ultimately, the Egyptian authorities cleared him of charges and released him in August 2005. See: X. Raufer, *Atlas radykalnego islamu…*, p. 93.

[61] *Report of the Official Account…*, p. 23.

of powder or crystals called acetone peroxide, abbreviated as TATP, from the English name: *triacetone triperoxide* (trimeric acetone peroxide). It is a highly unstable substance with a powerful explosive force, not much less than TNT. TATP, commonly used by terrorists, is also known as the 'mother of Satan'. The aforementioned Reid attempted to detonate it[62]. Due to the release of suffocating chemical vapours, Tanweer and Lindsay had to use face masks and open windows. The escaping gas caused the tops of the plants outside to die and lightened the hair on Tanweer and Hussain's heads, which their families noticed a few weeks before the attack. The men explained to them that this was the effect of chlorine in the swimming pool where they regularly swam with Khan. The explosive material produced was divided into four portions weighing an estimated 2 to 5 kg and placed in rucksacks. It is very likely that the group carried out a test explosion, although it is not known where and when it took place[63].

It is estimated that the cost of preparing for the attacks amounted to no less than GBP 8000, including travel, car and flat hire, and the purchase of chemicals[64]. It appears that Khan provided most of the funds. He worked for three years and opened several bank accounts, into which he deposited small amounts for long periods of time, and had a good credit rating. This enabled him to take out a loan of GBP 10 000, but from March 2005 onwards, he fell behind with his repayments and had overdrafts on his accounts. Lindsay, on the other hand, made several purchases using cheques that the sellers were unable to cash[65].

On 28 June, three participants in the plot (excluding Hussain) travelled to London via the same route as on the day of the attack. They probably made a similar trip in mid-March. It is believed that they acted in a methodical and disciplined manner, using mobile phones cautiously and

[62] G. Vince, *Explosives linked to London bombings identified*, New Scientist, 15 VII 2005, https://www.newscientist.com/article/dn7682-explosives-linked-to-london-bombings-identified/ [accessed: 15 VII 2025]; P. Szymczak, *TATP, materiał wybuchowy zwany matką szatana. Czy można go wykryć?* (Eng. TATP, an explosive known as the mother of Satan. Can it be detected?), Focus.pl, 23 IX 2019, https://www.focus.pl/artykul/czy-tatp-materia-wybuchowy-zwany-matk-szatana-mona-wykry [accessed: 23 VI 2025].

[63] *Report of the Official Account...*, p. 23.

[64] Ibid.

[65] Ibid.

travelling in rented cars. It was assumed that Khan may have suspected that he was under surveillance, which increased his vigilance[66].

During the period of preparation for the attacks, Lindsay's behaviour changed. He became less religious, did not pray with his wife, shaved his beard and wore Western clothes. He had an affair, but maintained relationships with other women. He established contacts with petty criminals[67]. On 27 May, he participated in a robbery in Luton, near London, during which a car registered in his name was used. Lindsay was not questioned by the police in connection with this case[68]. He spent money on various purchases, which he exchanged online for materials needed to make explosives. He spent less and less time at home, and when he was there, he locked himself in his room with his computer. Shortly before the attack, his wife confronted him with text messages from a girl she had discovered on his phone. She asked him to leave the house, which he did[69].

In the days leading up to the attack, Hussain often left the house. On 4 July, he told his mother that he would be travelling to London in the coming days. Two days later, he said that his trip to the capital had been postponed due to a car breakdown, but that he had to leave that evening for another destination. At around 3.30 p.m., his sister-in-law noticed that he was getting ready to leave. That was the last time his family saw him[70].

On 4 July, Tanweer went to visit his old school friends. The next day, he asked his mother to pack a bag for him because he wanted to go to Manchester to visit a Muslim school. On 6 July, he played cricket in a local park until late in the evening. When he returned home, he said he had lost his mobile phone. He was last seen at home shortly after 11 p.m. It is believed that he left shortly afterwards[71].

66 Ibid., p. 24.

67 Ibid.

68 Intelligence and Security Committee, *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c153540f0b61a825d6582/7-7_attacks_intelligence.pdf, p. 17 [accessed: 23 VI 2025].

69 Ibid., pp. 24–25.

70 Ibid., p. 25.

71 Ibid.

The course of the attack

On 7 July 2005, at 5.07 a.m., Lindsay arrived in Luton from Leeds in Fiat Brava. He parked in the car park at the railway station. He went inside and checked the timetable. He then moved his car several times. At 6.49 a.m., Nissan Micra pulled up next to Lindsay's car, and Khan, Tanweer and Hussain got out. The men put on large backpacks and went to the station. They looked like tourists going on a trip. At 7.15 a.m., they entered the station and headed for the ticket gates. They had already purchased their tickets. They went to the platform, where they waited about 20 minutes for the train to King's Cross station. They were clearly relaxed. The train departed from the platform at 7.40 a.m. The train arrived at King's Cross at 8.23 a.m. Seven minutes later, the men were seen in the station concourse hugging each other before parting. Each of them went to the underground[72]. Tanweer boarded train no. 204 on the Circle Line heading east, Khan boarded a train on the same line heading in the opposite direction, and Lindsay boarded a train on the Piccadilly Line heading south. Hussain was heading to a tube station on the same line. At 8.50 a.m., the train Tanweer was travelling on stopped at the crowded platform at Liverpool Street station. The terrorist was sitting in the second carriage at the front. His rucksack was on the floor at his feet. A few seconds after leaving the platform for Aldgate station, an explosion occurred. Eight people were killed, including the perpetrator, and 171 were injured[73]. Within a minute, a bomb exploded in the second carriage of train no. 216, which was travelling from Edgware Road station to Paddington station, and on which Khan was travelling. Seven people were killed and 163 were injured. The third bomb exploded about two minutes after the first, as train no. 311 on the Piccadilly Line, on which Lindsay was travelling, approached Russell Square station. The bomb exploded in the crowded first carriage, resulting in the highest number of casualties. Twenty-seven people were killed and 340 were injured[74].

[72] *Report of the Official Account...*, pp. 2–4.

[73] Ibid., p. 5.

[74] Ibid.

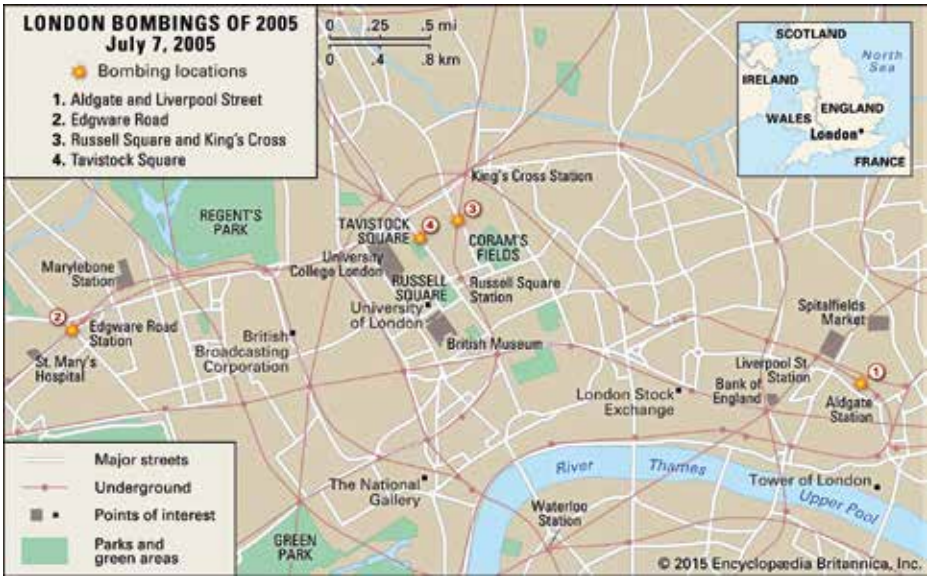


Figure 1. Location of the terrorist attacks on 7 July 2005 in London.

Source: M. Ray, *London bombings of 2005*, Britannica, https://www.britannica.com/event/London-bombings-of-2005 [accessed: 12 VII 2025].

At 8.55 a.m., Hussain got off the Piccadilly Line underground train at Euston Road station, where he spent several minutes unsuccessfully trying to contact the other bombers on his mobile phone. He then returned to King's Cross station, where he bought a 9V battery, possibly to detonate the explosive device. At 9.06 a.m., he entered the McDonald's restaurant on Euston Road, which he left after about 10 minutes. At 9.19 a.m., he was seen on the 91 bus travelling from King's Cross to Euston Station. This time, clearly nervous, he squeezed his way through the passengers. At Euston Station, he changed to the number 30 bus travelling east from Marble Arch. The vehicle was crowded due to the closure of the underground following the earlier attacks. He took a seat at the back of the upper deck and placed his rucksack on the floor between his feet, where he was seen 'fiddling' with something inside it. At 9.47 a.m., when the bus was at Tavistock Square, he detonated the bomb, killing 14 people, including himself, and injuring more than 110 (Figure 1)[75].

[75] Ibid., pp. 5–6.

The explosion occurred near the headquarters of the British Medical Association, from which doctors rushed out to rescue the injured. It is not known why the terrorist did not detonate the device at 8.50 a.m., like the other perpetrators. Perhaps the reason was a faulty battery, which he had to replace[76]. The attack in London took place at a time when the G8 summit was being held at the Gleneagles Hotel in Scotland and the day after the International Olympic Committee's decision to award London the 2012 Summer Olympics[77].

At 8.51 a.m., the first report was made to the 999 emergency number by a tube worker at Aldgate station. At the same time, the London Ambulance Service received a report and sent an ambulance to Liverpool Street station. The first fire engine arrived at Aldgate at 9.00 a.m., and at the same time, additional fire and rescue teams were dispatched. Officers from the British Transport Police took action and requested assistance from the Metropolitan Police Service. However, the situation was very difficult. After the explosions, passengers were plunged into total darkness. The interior lights of the carriages went out and internal communication between the driver and passengers ceased to function. Smoke was coming out of the underground. Information about the explosions and power loss on some sections of the underground initially led the London Underground Network Control Centre to conclude that there had been power surges in the network, and they began to respond to this scenario. Shortly afterwards, the centre received a call informing them that there had been an accident at Edgware Road station. It was suspected at the time that the train had hit a tunnel wall and that there was a passenger on the tracks[78]. At 9.15 a.m., it became clear that an explosion had occurred, although the cause and exact location remained unknown. In the early stages, the emergency services and police acted chaotically because it was not clear what had happened. Passengers were unable to contact train drivers, and drivers were unable to contact headquarters, as communications were down for the first half hour after the attack. Initially, emergency services were called to seven locations. For a time, it was believed that there had been five separate incidents in

[76] Ibid., p. 6.; *Report of the 7 July Review Committee,* https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/archives/assembly-reports-7july-report.pdf, p. 37 [accessed: 20 VI 2025].

[77] M. Phythian, *Intelligence, Policy-Making and the 7 July 2005 London Bombings*, "Crime, Law & Social Change" 2005, vol. 44, no. 4–5, p. 362. https://doi.org/10.1007/s10611-006-9027-3.

[78] *Report of the 7 July Review Committee*..., p. 12, 25.

the underground. Despite conflicting information, the Metropolitan Police considered the situation to be serious, without specifying the causes[79]. At 9.30 a.m., the national crisis centre was activated. Half an hour later, Home Secretary Charles Clarke chaired a meeting. The possibility of a terrorist attack was considered, which was confirmed at 10.55 a.m. by the head of the Home Office. He informed the representatives of the services that the explosions had caused many casualties and the suspension of public transport. At the same briefing, Ian Blair, Commissioner of the London Metropolitan Police, stated that the situation was very confusing but was now under control[80].

To provide immediate assistance, 101 ambulances and 25 rapid response medical teams were sent to the scene of the attacks. However, communication with the Royal London Hospital, where the injured were being transported, failed because all telephone networks were overloaded.

Fifty-six people were killed, including four attackers. Fifty-three people died immediately as a result of the explosions, one on the way to hospital and two in hospital. A total of 775 people were injured. The hospital admitted 27 seriously injured and 167 people who were able to move on their own. Seventeen patients underwent surgery. Some of the people were taken to other hospitals[81]. Among the victims were three Polish women: Monika Suchocka (23), Karolina Glueck (29) and Anna Brandt (43). Three other Polish nationals suffered minor injuries[82].

At 11.15 a.m., during the first press conference of the day, Commissioner Blair announced that there had been six explosions[83]. At noon, Prime Minister Tony Blair, who was attending the G8 summit in Scotland, issued a statement saying that a series of terrorist attacks had taken place in London, and the leaders of the G8 expressed their condemnation of the perpetrators. At 12.55 p.m., the Home Secretary made a statement in Parliament informing that there had been four explosions. He listed their locations and stated that the perpetrators remained unknown and would be identified by the investigation that had been launched. He added that the false information

[79] Ibid., p. 13.

[80] *Report of the Official Account…*, p. 7.

[81] K.L. Koenig, *Medical Consequences of the 2005 London Terrorist Bombings*, NEJM Journal Watch, 25 I 2007, https://www.jwatch.org/em200701260000006/2007/01/26/medical-consequences-2005-london-terrorist [accessed: 26 VI 2025].

[82] B. Hołyst, *Terroryzm. Tom 1* (Eng. Terrorism. Volume 1), Warszawa 2009, p. 708.

[83] *Report of the 7 July Review Committee…*, p. 13.

that had been reported earlier was due to the fact that the explosions occurred on trains between stations, causing passengers to leave both underground stations. This gave the impression that an incident had occurred at each of them. At the same time as Minister Clarke was speaking in Parliament, a statement was published on the internet in which responsibility for the attack was claimed by The Secret Organisation of Al-Qaida in Europe. It also threatened the governments of other countries that had sent troops to Afghanistan and Iraq[84]. At 5.30 p.m., Prime Minister Blair, who had returned to London, went to a meeting of the national crisis centre held in the Cabinet Office Briefing Rooms and made a statement announcing the most intensive police and security service operations to bring those responsible to justice. Before midnight, gym membership cards belonging to Khan and Tanweer were found at Aldgate underground station[85]. A painstaking investigation into the perpetrators of the attack began.

The investigation into the attack and the attempted repeat attack

Investigators analysed footage from over 2500 CCTV cameras monitoring the London Underground. The breakthrough in the investigation came when footage from King's Cross station was found showing four men walking together with large rucksacks. The same individuals were seen on CCTV footage from Luton railway station. The Nissan Micra and Fiat Brava cars used by the terrorists were found in the car park in front of the station. The first car contained several small explosive devices, the purpose of which could not be determined, while a pistol was found in the second car[86]. The investigation uncovered various recordings, one of which contained a statement by Khan: *We are at war and I am a soldier.*

[84] *Report of the Official Account...*, pp. 7–8. On 9 July, the Abu Hafs al-Masri Brigades, an organisation linked to Al-Qaeda, claimed responsibility for the attack in London. This was the same organisation that claimed responsibility for the attack in Madrid on 11 March 2004. See: C. Johnston, *Tube blasts 'almost simultaneous'*, The Guardian, 9 VII 2005, https://www.theguardian.com/uk/2005/jul/09/july7.uksecurity12 [accessed: 9 VII 2025].

[85] *Report of the Official Account...*, p. 8.

[86] B. Hołyst, *Terroryzm...*, p. 708; B. Levitt, *The True Story Behind Attack on London: Hunting the 7/7 Bombers*, Time, 1 VII 2025, https://time.com/7299329/attack-on-london-netflix-true-story/ [accessed: 1 VII 2025].

Now you too will taste the reality of this situation[87]. The investigation revealed that on the day of the attack, the terrorists made calls to a mobile phone belonging to Harun Rashid Aswat, one of Al-Masri's closest associates, who is believed to have been the mastermind behind the 7 July attacks. Aswat was arrested on 20 July 2005 in Zambia[88]. On the same day, the British press published information about the identification of all victims of the attack in London. In response to Prime Minister Blair's proposal to organise an international conference on combating Islamic extremism, British Muslim leaders demanded an independent judicial inquiry into the motives of the four 'local' suicide bombers who attacked London. They also warned that the Muslim community alone was not capable of eliminating extremism[89].

On 21 July 2005, another series of attacks was attempted. Four bombers: Yassin Omar, Mukhtar Ibrahim, Ramzi Mohammad and Hussain Osman attempted to detonate bombs at three London Underground stations (Oval, Shepherd's Bush and Warren Street) and on a bus on Hackney Road. None of them exploded. In two cases, only the detonators worked, but the explosives did not detonate, and the third was not activated. One person was injured. The bombers fled the scene[90].

The following day, at Stockwell underground station, police officers shot and killed Jean Charles de Menezes (27), a Brazilian citizen who had been living in the United Kingdom for three years. He was pursued by plainclothes police officers, but did not stop and ran into the underground station, where he was overpowered by two officers, while a third fired seven shots at the man lying on the floor. He was not a terrorist, nor did he have any connection to the 21 July attack.

After the events of 7 July, police guidelines on how to deal with individuals suspected of planning a suicide attack were changed. Officers were instructed to shoot them in the head to prevent the possibility of the wounded terrorist detonating a bomb. The whole affair had a negative

[87] B. Levitt, *The True Story*...

[88] A. Wejkszner, *Ewolucja terroryzmu*..., p. 346, 348.

[89] *All 56 dead identified in July 7 attacks*, NBC News, 20 VII 2005, https://www.nbcnews.com/id/wbna8642326 [accessed: 20 VII 2025].

[90] A. Wejkszner, *Ewolucja terroryzmu*..., p. 349; X. Raufer, *Atlas radykalnego islamu*..., p. 93.

impact on the image of the British police, and the head of the Metropolitan Police, Ian Blair, resigned[91].

At the end of July, Mohammad and Ibrahim were arrested in London. The third bomber, Omar, was arrested in Birmingham (dressed in a burqa), while Osman was arrested in Rome and sent back to the United Kingdom[92]. The attackers were immigrants from the Horn of Africa (two from Somalia, one from Ethiopia and one from Eritrea). They arrived in the United Kingdom in the 1990s and were awaiting citizenship. They did not establish contact with Pakistani jihadists.

It was also not possible to confirm any links between the terrorist groups involved in the 7 and 21 July attacks. The terrorists involved in the 21 July attacks had insufficient knowledge of how to manufacture explosives, but they were just as determined as their predecessors and had a similar motivation of 'martyrdom'. This was in response to the presence of Western troops, including those from the United Kingdom, in Afghanistan and Iraq[93]. The bombers were convicted of participating in a conspiracy to commit mass murder, and each received a sentence of at least 40 years in prison[94].

On 2 August 2005, in a speech broadcast on Qatar's Al-Jazeera channel, Osama bin Laden's deputy, Ayman al-Zawahiri, said that the 7 July attacks were a response to the prolonged presence of Western forces in Iraq and Afghanistan as well as the beginning of a major confrontation that would remind Americans of a second Vietnam[95]. He also offered Western countries a ceasefire if they withdrew from the Middle East and forced Israel to make peace with the Palestinians. On 1 September, in a recording broadcast by the same television station, he justified the attacks in London, stating: *Our targets are the lands and interests of countries that are involved in aggression against Palestine, Iraq and Afghanistan*[96]. On 25 September, Al-Zawahiri unequivocally confirmed Al-Qaeda's responsibility for the attacks in London:

[91] *Policja nie odpowie za śmierć w metrze* (Eng. The police will not be held responsible for the death in the underground), TVN24, 13 II 2009, https://tvn24.pl/swiat/policja-nie-odpowie-za-smierc-w-metrze-ra85753-ls3724956 [accessed: 13 VII 2025].

[92] A. Wejkszner, *Ewolucja terroryzmu...*, p. 350.

[93] A. Wejkszner, *Ewolucja terroryzmu...*, p. 350; X. Raufer, *Atlas radykalnego islamu...*, pp. 93–94.

[94] B. Levitt, *The True Story...*

[95] A. Wejkszner, *Ewolucja terroryzmu...*, p. 350.

[96] X. Raufer, *Atlas radykalnego islamu...*, p. 95.

> Brothers, knights of unity and heroes of the London operation, may Allah place you in his heavenly gardens and accept your good deeds. Their wills contain important lessons for Muslims in Pakistan and the West regarding the rejection of taghut [idols] and the determination of the mujahideen of Islam [...] to take revenge on the crusaders and Jews for the crimes they have committed with their hands drenched in the blood of the Muslim people. The blessed attack on London is one of a series of attacks that Al-Qaeda has had the honour of carrying out against the arrogance of the British crusaders in response to more than a century of British aggression against the Muslim nation, the historical crime of the creation of Israel, and the ongoing crimes of the British against Muslims in Afghanistan and Iraq[97].

On 6 July 2006, before the first anniversary of the London bombings, Al-Jazeera broadcast Tanweer's posthumous will. The terrorist declared that the operation (...) *was only the beginning of attacks that would continue and grow stronger until you withdrew your troops from Afghanistan and Iraq*. The video recording was accompanied by a message from Al-Zawahiri, who stated that Khan and Tanweer had been trained in Al-Qaeda camps[98].

On 22 March 2007, Mohammad Shakil and Waheed Ali were arrested in London while attempting to travel to Pakistan. On the same day, Sadeer Saleem was arrested in Leeds. They were charged with participating in a conspiracy to prepare the attacks of 7 July 2005[99]. The arrested individuals knew the perpetrators of the attack well, but their involvement in Khan's terrorist cell was not proven. In April 2009, they were sentenced to seven years in prison for participating in military training in Pakistan and attempting to travel there for further training[100].

[97] Ibid., p. 96.

[98] Ibid.

[99] A. Wejkszner, *Ewolucja terroryzmu...*, p. 351.

[100] *British 7/7 suspects jailed for terrorism camp plans*, Reuters, 29 IV 2009, https://www.reuters.com/article/world/british-7-7-suspects-jailed-for-terrorism-camp-plans-idUSTRE53S5SV/ [accessed: 29 VI 2025].

The UK's counter-terrorism security issues

The terrorist attack in London undermined the effectiveness of MI5. British security services did not fully take into account the threat posed by Muslim extremists, as they assumed that these circles had been effectively infiltrated. Three weeks before the attacks on 7 July, the terrorist threat alert level was lowered from severe to substantial (from 4 to 3 on a five-point scale), and the heads of the services assured that they had the situation under control, except that the two bombers from 7 July, Khan and Tanweer, and one of the bombers from 21 July had already been of interest to the British services in 2004. However, it was concluded that they did not pose a serious threat. The determination and operational commitment of Khan's cell was underestimated[101]. Renowned British security institutions with vast experience in combating Northern Irish terrorism, reinforced financially after 11 September 2001, were unable, despite their personnel and organisational resources, not only to stop the bombers, as evidenced by the July attacks, but also to correctly assess the scale of the threat[102]. Within two weeks, a second, independent group of terrorists could have adopted a similar modus operandi, and only the lack of professionalism of its members in the production of explosive devices prevented numerous casualties among London residents.

The events of 2005 influenced anti-Muslim sentiments among the British and led to an unprecedented increase in the sense of terrorist threat. Although leaders of the British Muslim community immediately condemned the actions of the bombers (several leaders even issued fatwas – theological rulings stating that the attacks were contrary to Islam), there was an increase in the number of hate crimes. The victims included both Muslims and people whom the attackers wrongly identified as followers of Islam[103]. There have been several attacks on mosques,

[101] F. Eliott, S. Goodchild, *7/7 one year on: Why did it happen? The big questions still need answers*, The Independent, 2 VII 2006, https://www.independent.co.uk/news/uk/crime/7-7-one-year-on-why-did-it-happen-the-big-questions-still-need-answers-406351.html [accessed: 2 VII 2025]; B. Levitt, *The True Story*...

[102] Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world*, https://www.statewatch.org/media/documents/news/2010/oct/uk-national-security-strategy-2008.pdf, pp. 4–5, [accessed: 14 VI 2025].

[103] *20 lat temu zamachowcy Al Kaidy dokonali zamachów bombowych w londyńskim metrze* (Eng. Twenty years ago, Al-Qaeda bombers carried out attacks on the London Underground), PAP, 7 VII 2025, https://www.pap.pl/aktualnosci/20-rocznica-zamachow-bombowych-w

including in London, Glasgow, Manchester, Birmingham, South-on-Sea and Exeter[104]. Islamophobia, propagated mainly by far-right organisations and parties, intensified. The increased terrorist threat led to the inclusion of the Prevent programme in the government's CONTEST strategy. Its aim was to prevent attacks by identifying individuals expressing extremist views. The programme was constantly expanded, and individuals deemed dangerous were referred to a part of the programme called Channel. Although Prevent was applied to all extremists, including the far right, it was criticised from the outset by Muslim organisations for stigmatising their communities. Some even expressed the opinion that it was deeply Islamophobic. The most controversial part of the programme was the obligation imposed on schools, the police, the health service, local government organisations and other public institutions to report individuals suspected of harbouring radical views that could lead to terrorism[105]. In April 2006, a new anti-terrorism law (*The Terrorism Act 2006*) came into force, defining and mandating the prosecution of crimes such as glorifying terrorism (praising terrorist acts in the hope of encouraging others to commit them), participating in or organising terrorist training, planning and preparing a terrorist act, and disseminating publications with terrorist content[106]. The government proposed the initiative to criminalise the glorification of terrorism shortly after the London bombings. It was to be one of a package of measures targeting Muslim preachers such as Al-Masri, whom Prime Minister Blair considered to be inciting hatred. The new law was intended to give the police the power to detain a terrorism suspect for up to 28 days instead of the previous 14 (the government initially proposed 90 days). The provision came into force on 25 July 2006. The law was protested by human rights activists, who claimed that the new

londynie#:~:text=7%20lipca%202005%20r.,ofiar%20zamachu%20wynosi%C5%82%2034%20lata [accessed: 7 VII 2025].

[104] M. Zawadewicz, *Życie codzienne…*, p. 138.

[105] *About Prevent*, Prevent Watch, https://www.preventwatch.org/about-prevent/ [accessed: 23 VII 2025]; A. Safdar, *Prevent: UK anti-terror plan "harms children's rights"*, AlJazeera, 13 VII 2016, https://www.aljazeera.com/features/2016/7/13/prevent-uk-anti-terror-plan-harms-childrens-rights [accessed: 13 VII 2025].

[106] It was the fourth anti-terrorism law after: *Terrorism Act 2000*, *The Anti-Terrorism, Crime and Security Act 2001* and *The Prevention of Terrorism Act 2005*. See: A. Kalicki, *Aspekty prawne w brytyjskim systemie zwalczania terroryzmu* (Eng. Legal aspects of the British counter-terrorism system), in: *Terroryzm. Materia ustawowa?*, K. Indecki, P. Potejko (eds.), Warszawa 2009, pp. 92–100.

law would restrict freedom of speech and the freedom of action of non-governmental organisations[107].

The new law did not stop Islamic extremists from carrying out hostile activities. After the Ministry of the Interior banned one group, a new one was established under a different name. For example, after the aforementioned Firkat an-Naja and Al-Ghuraba were banned in July 2006, Choudary established an online organisation called Islam4UK. It continued the ideological message of Al-Muhajiroun, motivating young Islamic radicals to travel to Pakistan for training. On 6 August 2006, the police announced that they had uncovered a terrorist plot to blow up aeroplanes flying from the United Kingdom to the United States. Twenty British citizens of Pakistani origin were arrested, eight of whom were charged with preparing a terrorist plot. They had undergone training on the Afghan-Pakistani border. It was there that the plan for the attacks was hatched, and the group's leader, Abdullah Ahmed Ali, received detailed instructions on how to carry them out. The attackers intended to blow up the planes over the Atlantic using liquid explosives hidden in soft drink bottles. Since the plans for these attacks were revealed, stricter security measures have been introduced at airports, prohibiting liquids from being brought on board aeroplanes[108]. In November 2006, MI5 director general Eliza Manningham-Buller stated that the services were monitoring 200 groups comprising over 1600 individuals (mainly British citizens of foreign origin) involved in planning or supporting terrorist attacks in the United Kingdom or abroad[109].

Terrorist organisations managed to maintain their operational capabilities despite decisive action by the British authorities after 2005 aimed at dismantling these structures. This was confirmed by the attack on Glasgow Airport on 30 June 2007. Shortly before that, in January 2007, the British police managed to prevent the kidnapping and killing of a British soldier[110]. Anti-terrorist measures taken by British authorities have forced

[107] *W. Brytania: Nowa ustawa antyterrorystyczna weszła w życie* (Eng. United Kingdom: New anti-terrorism law comes into force), Wirtualna Polska, 13 IV 2006, https://www.money.pl/archiwum/wiadomosciagencyjne/pap/artykul/w;brytania;nowa;ustawa;antyterrorystyczna;weszla;w;zycie,28,0,152348.html [accessed: 13 IV 2006]; A. Kalicki, *Aspekty prawne w brytyjskim systemie...*, p. 95.

[108] K. Izak, *Leksykon organizacji...*, p. 361.

[109] X. Raufer, *Atlas radykalnego islamu...*, p. 96.

[110] A. Wejkszner, *Ewolucja terroryzmu...*, p. 351.

a number of terrorist cells to go into hiding[111]. However, the propaganda activities of jihadist ideologues continued to be tolerated. In September 2008, on the seventh anniversary of the terrorist attacks in the US, Islam4UK announced in the media a conference entitled 'Caliphate for Britain – God's Alternative'. Invitations and posters advertising the meeting featured a map of the United Kingdom with the black flag of Islam flying over it and the inscription 'Caliphate'. During the gathering, attended by over 100 people, Choudary stated that seven years earlier Osama bin Laden had taught the Americans a lesson, but the 'crusaders' had learned nothing, so another 11 September would occur in the British Isles. Another 7 July could also come. The leader of Islam4UK then declared: *We do not integrate into Christianity. We will ensure that one day you will integrate into the Sharia Islamic law. Our eyes are on Downing Street. That is why the British are so afraid. It would be easy for us to declare Jihad in Britain and each one of us could become a time-bomb waiting to go off.*[112]. Another person who delivered a speech filled with hatred was Saiful Islam, head of the Salafi Youth for Islamic Propagation. He praised Bin Laden for his courage and warned against a repeat of the events of seven years ago, stating, among other things, that: *The American government and no one else is to blame for the 11 September attacks. They are the terrorists. Sheikh Osama repeatedly warned America, all because of their arrogance, because they thought they were a superpower and no one could threaten them, so Osama bin Laden taught the US a lesson that they still have not learned*[113]. Referring to the situation in Iraq and Afghanistan, he warned the United States and the United Kingdom: *Wake up. Withdraw. You must stop the violence, otherwise the next 11 September will take place in the United Kingdom, and the next 7 July may also happen here*[114].

The activities of Muslim extremists contributed to the establishment of the anti-Muslim organisation English Defence League (EDL) in Luton in 2009. The city is inhabited mainly by descendants of immigrants, mostly

[111] Ibid.

[112] R. Watson, *Al-Muhajiroun and the long tail of UK terror*, The New Statesman, 22 II 2020, https://www.newstatesman.com/long-reads/2020/02/al-muhajiroun-and-long-tail-uk-terror [accessed: 22 VII 2025].

[113] *"Have more babies and Muslims can take over the UK" hate fanatic says, as warning comes that "next 9/11 will be in UK"*, Daily Mail, 13 IX 2008, https://www.dailymail.co.uk/news/article-1054909/Have-babies-Muslims-UK-hate-fanatic-says-warning-comes-9-11-UK.html [accessed: 13 VII 2025].

[114] Ibid.

from Muslim countries, who form a parallel society and live according to Sharia law. The immediate cause of the EDL's formation was an attempt by Choudary's supporters to attack participants in a ceremony in Luton welcoming soldiers of the Royal Anglican Regiment returning from Afghanistan[115]. The organisation was established within the football hooligan subculture. It became a permanent feature of British political life. It organised regular demonstrations that attracted between several hundred and several thousand participants. Its membership was estimated at 25 000–30 000, making it one of the largest street protest movements in the United Kingdom[116]. Unlike traditional British far-right parties (such as the National Front or the British National Party), the EDL did not refer to anti-immigrant and racist ideology in its official statements, but claimed that it was only opposed to Islam. The League viewed Islam not so much as one of the religions of British society, but rather as an aggressive and expansionist political ideology that threatened human rights and democracy. It considered it its duty to morally support British troops in the Middle East. Against this backdrop, there were frequent clashes with Muslims protesting against the presence of British soldiers in Iraq and Afghanistan[117].

In January 2010, Islam4UK announced that it would organise a march of 'empty coffins' through the streets of Royal Wootton Bassett, where the bodies of British soldiers killed in Afghanistan were brought. Relatives, friends of the fallen and residents lined the streets as the flag-draped coffins of the fallen were carried on catafalques. Choudary accused the soldiers of murder and posted an open letter online entitled *To the families of British soldiers who have died or are currently in Afghanistan*, explaining the reasons for organising the march. His announcement sparked a wave of protests[118]. This forced the authorities to ban Islam4UK. The decision came into force on 14 January 2010[119]. The threat of imprisonment did not change

[115] J. Barlett, M. Littler, *Inside the EDL: Populist Politics in a Digital Age*, https://demos.co.uk/wp-content/uploads/2011/10/Inside_the_edl_WEB.pdf, p. 10 [accessed: 10 IX 2025].

[116] K. Jaskułowski, *Głośni i dumni: etnografia Angielskiej Ligi Obrony* (Eng. Loud and proud: an ethnography of the English Defence League), "Prace Etnograficzne" 2017, vol. 45, n. 1, p. 117.

[117] Ibid.

[118] *Fury over British Muslim cleric's anti-war march threat*, CNN, 5 I 2010, https://edition.cnn.com/2010/WORLD/europe/01/04/britain.afghanistan.demo/index.html [accessed: 5 I 2010].

[119] D. Orr, *Is the Islam4UK ban a blow against democracy?*, The Guardian, 14 I 2010, https://www.theguardian.com/commentisfree/2010/jan/14/deborah-orr-islam4uk [accessed: 14 VII 2025].

the nature of Choudary's statements, as he consistently preached extremist propaganda. He founded the website Muslims Against Crusades (MAC). This name was also used to refer to his supporters. Taking advantage of his access to social media, Choudary was able to reach a wide audience of Muslims with his views, thereby influencing the level of their radicalisation[120]. On 11 September 2011, MAC supporters organised a demonstration next to the US Embassy in London to mark the 10th anniversary of the attacks in the US. Clashes with the EDL ensued[121]. On the same day, 11 British Muslims were arrested in Birmingham for preparing a terrorist attack in that city using eight bombs placed in rucksacks. Some of them had undergone training in Al-Qaeda camps on the Afghan-Pakistani border. The terrorists intended to turn Birmingham into a zone of small-scale warfare. All of them were sentenced to imprisonment. The leader of the group, Irfan Naseer (31), was sentenced to life imprisonment, and his two closest associates, Irfan Khalid (28) and Ashik Ali (28), received sentences of 23 and 20 years' imprisonment, respectively. The members of the group were under the ideological influence of Choudary[122].

On 10 November 2011, the British Home Office decided to ban the MAC. It was the 48th extremist organisation banned in the United Kingdom under the anti-terrorist Act and the Act prohibiting the glorification of terrorism. The ban on the group's activities meant that the authorities had the right to seize its assets and that membership in the organisation was punishable by up to 10 years' imprisonment. In a statement, Choudary described the banning of the MAC as a manifestation of the British government's hatred of Muslims[123]. The MAC was replaced by the United Ummah organisation, which organised a demonstration in London on 2 December 2011 against American drone strikes on Muslim countries[124].

[120] C. Gammell, *Muslims Against Crusades earn notoriety in less than a year*, The Telegraph, 21 IV 2011, https://www.telegraph.co.uk/news/8461436/Muslims-Against-Crusades-earn-notoriety-in-less-than-a-year.html [accessed: 21 VI 2025].

[121] D. Casciani, *Muslims Against Crusades banned by Theresa May*, BBC News, 10 XI 2011, https://www.bbc.com/news/uk-15678275 [accessed: 10 XI 2025].

[122] *Wielka Brytania: 11 skazanych za planowanie zamachów w Birmingham* (Eng. United Kingdom: 11 convicted for planning attacks in Birmingham), Wirtualna Polska, 26 IV 2013, https://wiadomosci.wp.pl/wielka-brytania-11-skazanych-za-planowanie-zamachow-w-birmingham-6082107866088065a [accessed: 26 VII 2025].

[123] D. Casciani, *Muslims Against Crusades*...

[124] K. Izak, *Leksykon organizacji*..., p. 365.

On 22 May 2013, two British men of Nigerian descent, Michael Adebolayo (28) and Michael Adebowale (22), killed British soldier Lee Rigby in the London borough of Woolwich. The man, who was crossing the street, was first hit by a car, and then the perpetrators attempted to cut off his head with a meat cleaver, shouting 'Allah Akbar'. They dragged his body into the middle of the street so that passers-by could see it. The perpetrators did not flee the scene of the crime, but talked to bystanders while waiting for the police. They tried to explain their views to them, with Adebolayo shouting, among other things: *We swear by the almighty Allah we will never stop fighting you. The only reason we have killed this man today is because Muslims are dying daily by British soldiers. It's an eye for an eye and a tooth for a tooth.*[125]. When the police arrived, the men tried to attack them. Both hoped to be killed on the spot and become martyrs. However, they were only wounded. Adebolayo and Adebowale came from Catholic families of Nigerian immigrants, but converted to Islam and became radicalised in the United Kingdom[126]. This murder led to social mobilisation that spread across almost the entire country. It was the largest such mobilisation in over 30 years. Anti-Muslim demonstrations took place in many cities. In response to these events, Prime Minister David Cameron declared war on radicalisation and extremism, but he directed even stronger words at the EDL and BNP, stating that he would not tolerate right-wing Islamophobia. He also announced the creation of a special task force, TERFOR, whose aim was to combat extremists[127]. These promises were not fulfilled. The crackdown on the far right was intensified, but Islamic extremists and Muslim activists accusing the British of Islamophobia and racism were tolerated.

Meanwhile, there were growing opinions that the special services could have prevented the attack on 22 May 2013, just as they could have prevented the attacks in London eight years earlier. Adebolayo was already known to the services in 2010, when he intended to join the armed organisation Harakat al-Shabab al-Mujahideen (Young Mujahideen Movement) in Somalia. However, he was arrested in Kenya and sent back to the United

[125] *Dożywocie i 45 lat więzienia dla „rzeźników z Londynu" za zabójstwo żołnierza* (Eng. Life imprisonment and 45 years in prison for the 'London butchers' for the murder of a soldier), TVN24, 26 II 2014, https://tvn24.pl/swiat/dozywocie-i-45-lat-wiezienia-dla-rzeznikow-z-londynu-za-zabojstwo-zolnierza-ra402449-ls3352033 [accessed: 26 VII 2025].

[126] Ibid.

[127] G. Kayzer, *Radykałowie na celowniku* (Eng. Radicals in the crosshairs), "Gazeta Polska Codziennie", 29 V 2013.

Kingdom[128]. The British authorities did not place him under surveillance or bring him to trial, as they should have done under the 2006 Act, which criminalised travelling or intending to travel abroad with the intention of joining a terrorist organisation or carrying out an attack. The situation was similar with Adebowale, who had previously been under surveillance. It also turned out that both terrorists were guided by the teachings of Choudary, who remained at large and continued to preach hate speech with impunity[129]. The decision to arrest him was only made after he pledged allegiance to Islamic State in July 2014. Two years later, he was sentenced to 5.5 years in prison, instead of the 10 years he faced. The guilty verdict was preceded by an investigation that cost millions of pounds. It showed that his name had been linked to most terrorist attacks in the UK. He is believed to have inspired more than 100 UK citizens to carry out terrorist attacks, and it is likely that one in four of the more than 900 British jihadists who left to fight for Islamic State were influenced by their mentor's teachings[130]. Other statistical data is included in a report by the non-profit organisation Counter Extremism Project (CEP) entitled *Anjem Choudary's Ties to Extremists*. It lists 33 organisations and 112 individuals whom Choudary influenced or communicated with during his career. Of these, 20 carried out terrorist attacks, 50 attempted to do so, 19 joined or attempted to join Islamic State in Syria, and others promoted jihadist content and recruited for terrorist organisations[131].

---

[128] Ibid.

[129] Ibid.; P. Falkowski, *Niespokojny Londyn* (Eng. Restless London), "Nasz Dziennik", 3 VI 2013.

[130] M.R. Chehab, *Kim jest Anjem Choudary, mentor ostatniego zamachowca z Londynu?* (Eng. Who is Anjem Choudary, the mentor of the latest London bomber?), Newsweek, 8 XII 2019, https://www.newsweek.pl/swiat/po-zamachu-w-londynie-kim-jest-anjem-choudary/n0plx7f [accessed: 8 XI 2025].

[131] *Anjem Choudary's Ties to Extremists*, Counter Extremism Project, https://www.counterextremism.com/anjem-choudary-ties-to-extremists [accessed: 23 X 2025]. Choudary served less than half of his sentence, with the remainder to be served under strict supervision, but he continued his propaganda and agitation activities nonetheless. In 2019, he initiated the revival of the Al-Muhajiroun organisation. He used social media to teach his followers in the US and Canada. He became involved in the activities of the Islamic Thinkers Society, an organisation promoting radical ideas. Al-Muhajiroun was operating under this name. His close associate in Canada was Khaled Hussain, representing a new generation of Choudary's students, promoting him in North America. On 17 July 2023, after Hussain arrived in London to meet with Choudary, both men were arrested. On 30 July 2024, Choudary was sentenced to life imprisonment with the possibility of release after 28 years, while Khaled Hussein received a 5-year prison sentence. See: *International counter terrorism*

The Islamic State continued the activities of jihadist networks in the United Kingdom. It intended to carry out an attack to commemorate its predecessors who were responsible for the 2005 bombings. One such plot was uncovered in 2015, another the following year, and three in 2017[132]. Unfortunately, it was a year marked by three terrorist attacks: in London on 22 March (6 people killed and at least 49 injured)[133] and 3 June (8 people killed and over 40 injured)[134], and the deadliest suicide bombing in Manchester on 22 May (22 people were killed and 118 were injured). The perpetrator of the latter was Salman Ramadan Abedi, who detonated a bomb placed in his rucksack as concert-goers were leaving the venue shortly after American singer Ariana Grande had finished performing[135].

On 29 November 2019, Usman Khan (28), born in the United Kingdom, attacked passers-by with a knife near London Bridge. He killed two people and injured three others. Witnesses to the incident, including Łukasz Koczocik from Poland, who was also injured, tried to stop the attacker. The terrorist was shot dead by the police. His idol and mentor was Choudary. Islamic State claimed responsibility for the attack. In 2010, Khan, operating under the pseudonym Abu Saif, was arrested along with eight other extremists[136]. They were preparing a series of attacks, including on Parliament, the London Stock Exchange, the US Embassy, the flat of the then Mayor of London Boris Johnson, and St Paul's Cathedral[137]. In 2012, Khan was sentenced to 16 years in prison. He was released on parole. The day after the attack, Prime Minister Boris Johnson criticised the practice of releasing terrorists on parole, saying that if Khan had not

investigation leads to Anjem Choudary conviction, Counter Terrorism Policing, 23 VII 2024, https://www.counterterrorism.police.uk/historic-met-and-international-police-counter-terrorism-investigation-leads-to-anjem-choudary-terror-conviction/ [accessed: 23 VII 2025]; *CPS statement: Convictions of Anjem Choudary and Khaled Hussein,* Crown Prosecution Service, 31 VII 2024, https://www.cps.gov.uk/cps/news/cps-statement-convictions-anjem-choudary-and-khaled-hussein [accessed: 31 VII 2025].

[132] A. Wejkszner, *Europejska armia kalifatu. Tom I. Centrum supersieci* (Eng. The European Army of the Caliphate. Volume I. The centre of the supernetwork), Warszawa 2020, pp. 234–235.

[133] Ibid., p. 237.

[134] Ibid., p. 246.

[135] Ibid., p. 240, 243.

[136] M.R. Chehab, *Kim jest Anjem Choudary...*

[137] Ibid.

been released early, he would not have carried out the attack. He also reported that 74 people convicted of terrorism are currently on parole[138].

On 15 October 2021, British citizen Ali Harbi Ali (26) stabbed Conservative politician David Amess to death in London. The killer was under Choudary's influence. Experts criticised the Prevent programme, which had cost millions of pounds to implement but had failed to achieve its objectives. They pointed out that the reasons for the programme's failure included its paralysis by Muslim clerics and social activists as well as its constant criticism by opposition representatives[139].

On 29 July 2024, Axel Rudakubana (17), a British citizen of Rwandan descent, stabbed three girls attending a dance class to death. He also injured nine other children and one adult before being apprehended. The attack took place in the town of Southport, near Liverpool. After the incident, several days of anti-immigrant and anti-Muslim protests and riots broke out in many British cities. There were clashes with police officers, and a police station as well as a hotel for illegal immigrants awaiting asylum were attacked[140].

Summary

After the Al-Qaeda terrorist attack in London on 7 July 2005, Tony Blair's government took measures to improve internal security and protect citizens from extremist attacks. However, these measures were limited due to opposition from Muslim organisations and human rights activists. Supporters of a hard line against Islamic extremism criticised the British practice of so-called vigilant tolerance, which allowed many radical imams

[138] *"Przygotowywał działalność terrorystyczną". Mężczyzna zatrzymany* (Eng. "He was preparing terrorist activities". Man detained), TVN24, 2 XII 2019, https://tvn24.pl/swiat/wielka-brytania-policja-zatrzymala-mezczyzne-podejrzanego-o-terroryzm-ra989867-ls2508450 [accessed: 2 X 2025].

[139] V. Dodd, *Ali Harbi Ali guilty of murdering MP David Amess in terrorist attack*, The Guardian, 11 IV 2022, https://www.theguardian.com/uk-news/2022/apr/11/david-amess-verdict-terrorist-attack-ali-harbi-ali-guilty [accessed: 11 VI 2025].

[140] M. Czarnecki, *Po ataku nożownika w Southport rozruchy rozlały się na kolejne brytyjskie miasta. Aresztowano ponad 90 osób* (Eng. After the knife attack in Southport, riots spread to other British cities. Over 90 people were arrested), wyborcza.pl, 4 VIII 2024, https://wyborcza.pl/7,75399,31200497,po-ataku-nozownika-w-southport-rozruchy-rozlaly-sie-na-kolejne.html [accessed: 4 VIII 2025].

to incite hatred and violence. The British authorities emphasised, however, that the strategy of focusing on surveillance and control measures for individuals suspected of terrorist activity yielded better results than imprisoning them, as it allowed for the gathering of intelligence[141]. According to some experts, the source of placing the rights of criminals above the safety of British citizens was the *Human Rights Act*, which in 1998 incorporated the provisions of the European Convention on Human Rights into British law. Literally interpreted, the provisions allowed foreigners prosecuted in their countries for crimes to be granted asylum in the UK because they could be exposed to 'inhuman or degrading treatment' there[142]. On the basis of this law and Resolution A/HRC/22/L.40 of the UN Human Rights Council, adopted in March 2013, even the slightest criticism of Muslim minorities, including the term 'Islamic terrorism', may be considered punishable Islamophobia[143].

This strategy failed, and the authorities were eventually forced to arrest the so-called hate preachers. However, it took several more years before they were successfully deported from the country. Al-Masri was not extradited to the US until October 2012[144], Abu Katada was handed over to Jordan in July 2013. However, Amman had to assure that Abu Katada,

---

[141] G. Wilk-Jakubowski, *Sytuacja społeczna muzułmanów w Wielkiej Brytanii* (Eng. The social situation of Muslims in the United Kingdom), Kraków 2013, p. 153.

[142] A. Pearson, *Allison Pearson: We must get rid of the dreadful Human Rights Act*, The Telegraph, 13 V 2015, https://www.telegraph.co.uk/news/uknews/law-and-order/11602222/Allison-Pearson-We-must-get-rid-of-the-dreadful-Human-Rights-Act.html [accessed: 13 VI 2025].

[143] The resolution states that terrorism in all its forms and manifestations cannot be associated with any religion, nationality or ethnic group. This would mean that there is no such thing as Palestinian, Basque, Corsican, Tamil, Muslim and dozens of other forms of terrorism. However, most terrorist organisations have had and continue to have references to ethnic, national and religious terms in their names. The EU representative to the UN condemned the provisions contained in the document, while referring to international support for freedom of speech: "(...) America is still the last bastion of freedom of speech, but it is clear that even here we are sliding down a slippery slope towards the demise of free speech. This is sad and frightening. I hope that people will wake up, because this freedom is being quietly taken away from them, while many of them live in the belief that they will always have it". See: D. Weiss, *If You Criticize Islam, You Will Suffer Consequences*, Citizen Times, 13 VII 2014, http://www.citizentimes.eu/2013/06/13/if-you-criticize-islam-you-will-suffer-consequences/ [accessed: 13 VIII 2024].

[144] *Ekstradycja Abu Hamzy do USA wstrzymana przez apelację* (Eng. Abu Hamza's extradition to the US halted by appeal), Wirtualna Polska, 26 IX 2012, https://wiadomosci.wp.pl/ekstradycja-abu-hamzy-do-usa-wstrzymana-przez-apelacje-6082120547132033a [accessed: 26 IX 2025].

who had previously been sentenced in absentia to life imprisonment for his involvement in the preparation of two attacks in the country's capital in 1999 and 2000, would not be tortured to extract a confession. After hearing the unfavourable verdicts, both men appealed to higher courts and the European Court of Human Rights[145]. International humanitarian organisations defended them, even though they incited hatred and Al-Masri organised terrorist attacks in Yemen.

In Great Britain, however, a policy of concessions and privileges continued to be applied to Muslims. They were given special rights at the expense of other social groups. This special status exempted Muslims from complying with norms, the violation of which by members of other social groups is punishable by sanctions. The application of Sharia law in civil matters was permitted (including marriage and inheritance issues). The multiculturalism programme was intended to curb discontent among newcomers, primarily from Muslim countries, and weaken their critical attitude towards their new homeland. These calculations failed completely, and the friendly policies of successive governments led to a rise in Islamic extremism[146]. This situation worsened after the large wave of migration in 2015. The British police concealed crimes committed by Muslim minorities from the public. Fear of being accused of racism paralysed the actions of the security services. In the UK, Muslim gangs sexually abused around 1400 British girls over a period of 10 years, and the police did not make this information public. When the case came to light, a report stated, among other things, that the reason for the inaction, silencing and downplaying of the crimes was the fear of law enforcement agencies of accusations of racism and the political consequences of turning native Britons against ethnic minorities[147].

---

[145] *Wydalony z Wielkiej Brytanii Abu Katada, oskarżony o terroryzm* (Eng. Abu Katada, accused of terrorism, expelled from the United Kingdom), Wirtualna Polska, 7 VII 2013, https://wiadomosci.wp.pl/wydalony-z-wielkiej-brytanii-abu-katada-oskarzony-o-terroryzm-6031568274154113a [accessed: 7 VII 2025]. In September 2014, a military court in Jordan finally acquitted Abu Katada of charges of terrorist activity, allegedly involving plans to attack Americans and Israelis. The radical preacher was released. See: *Oskarżony o planowanie masakry niewinny. Abu Katada na wolności* (Eng. Man accused of planning massacre found not guilty. Abu Katada released), TVN24, 24 IX 2014, https://tvn24.pl/swiat/oskarzony-o-planowanie-masakry-niewinny-abu-katada-na-wolnosci-ra471293-ls3412841 [accessed: 24 IX 2025].

[146] G. Wilk-Jakubowski, *Sytuacja społeczna muzułmanów…*, pp. 152–153.

[147] G. Drymer, *Afery seksualne w Wielkiej Brytanii. Gwałty muzułmańskich gangów* (Eng. Sex scandals in the United Kingdom. Rape by Muslim gangs), Rzeczpospolita, 1 X 2017,

The effectiveness of deradicalisation programmes seems questionable due to the inability to realistically assess whether someone has softened their views. Such a person's claim that they have abandoned their ideas may be considered a lie. It is also difficult to predict their future behaviour. They very often feign a change in behaviour in order to divert the attention of the security services. An example of this is Usman Khan, the terrorist of 29 November 2019, who, prior to his conditional release from prison, assured that he was a good Muslim and a good British citizen and that his involvement in planning attacks was immaturity[148]. After his release, he joined the Learning Together programme, which aims to eliminate prejudice against other people. Khan's victims, who were fatally stabbed, were the programme coordinator and a volunteer. Mandatory deradicalisation programmes for terrorists leaving prison have proved to be a failure. In private conversations, they admitted that they had not changed their beliefs and that for them, the fight for an Islamic state was still ongoing[149].

On 8 October 2024, MI5 chief Ken McCallum announced in a rare public statement that since 2017, his agency and the police had foiled 43 different terrorist attacks[150]. The terrorist threat in the United Kingdom remains at level three (substantial) on a five-point scale, which means that an attack is likely. According to government assessments, the threat to the United Kingdom is 'persistent and evolving' and, at the same time, 'less predictable and more difficult to detect and investigate'[151]. This is accompanied by public unrest. Furthermore, three quarters of the British public believe that Muslim extremists pose the greatest threat to the country[152].

https://www.rp.pl/spoleczenstwo/art2411491-afery-seksualne-w-wielkiej-brytanii-gwalty-muzulmanskich-gangow [accessed: 8 X 2025].

148 M.R. Chehab, *Kim jest Anjem Choudary*...

149 Ibid.

150 *Director General Ken McCallum gives latest threat update,* Security Service MI5, 8 X 2024, https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update [accessed: 8 X 2025].

151 Ibid.

152 M. Smith, *Which extremists do Britons see as threats in 2024?*, YouGov, 29 II 2024, https://yougov.co.uk/politics/articles/48784-which-extremists-do-britons-see-as-threats-in-2024 [accessed: 29 VII 2025].

Bibliography

Besson S., *Islamizacja Zachodu? Historia pewnego spisku* (Eng. Islamisation of the West? The story of a conspiracy), Warszawa 2006.

Chaliand G., Blin A., *Historia terroryzmu. Od starożytności do Da'isz* (Eng. The history of terrorism. From antiquity to Daesh), Warszawa 2020.

Falkowski P., *Niespokojny Londyn* (Eng. Restless London), "Nasz Dziennik", 3 VI 2013.

Hołyst B., *Terroryzm. Tom 1* (Eng. Terrorism. Volume 1), Warszawa 2009.

Izak K., *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014.

Jaskułowski K., *Głośni i dumni: etnografia Angielskiej Ligi Obrony* (Eng. Loud and proud: an ethnography of the English Defence League), "Prace Etnograficzne" 2017, vol. 45, n. 1, pp. 117–121.

Kalicki A., *Aspekty prawne w brytyjskim systemie zwalczania terroryzmu* (Eng. Legal aspects of the British counter-terrorism system), in: *Terroryzm. Materia ustawowa?*, K. Indecki, P. Potejko (eds.), Warszawa 2009, pp. 92–100.

Kayzer G., *Radykałowie na celowniku* (Eng. Radicals in the crosshairs), "Gazeta Polska Codziennie", 29 V 2013.

Kepel G., *Fitna, wojna w sercu islamu* (Eng. Fitna, war in the heart of Islam), Warszawa 2006.

Levitt M., *Hamas. Polityka, dobroczynność i terroryzm w służbie dżihadu* (Eng. Hamas: Politics, Charity and Terrorism in the Service of Jihad), Kraków 2008.

Mansfield L., *His Own Words: Translation and Analysis of the Writings of Dr. Ayman Al Zawahiri*, New York 2006.

Phillips M., *Londonistan. Jak Wielka Brytania stworzyła państwo terror* (Eng. Londonistan: How Britain Created a State of Terror), Warszawa 2010.

Phythian M., *Intelligence, Policy-Making and the 7 July 2005 London Bombings*, "Crime, Law & Social Change" 2005, vol. 44, no. 4–5, pp. 361–385. https://doi.org/10.1007/s10611-006-9027-3.

Raufer X., *Atlas radykalnego islamu* (Eng. Atlas of Radical Islam), Warszawa 2011.

Simcox R., Stuart H., Ahmed H., *Islamist Terrorism. The British Connections*, London 2010.

Wejkszner A., *Europejska armia kalifatu. Tom I. Centrum supersieci* (Eng. The European Army of the Caliphate. Volume I. The centre of the supernetwork), Warszawa 2020.

Wejkszner A., *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu* (Eng. The evolution of religiously motivated terrorism as exemplified by the Salafi global jihad movement), Poznań 2010.

Wilk-Jakubowski G., *Sytuacja społeczna muzułmanów w Wielkiej Brytanii* (Eng. The social situation of Muslims in the United Kingdom), Kraków 2013.

Zawadewicz M., *Życie codzienne w muzułmańskim Londynie* (Eng. Daily life in Muslim London), Warszawa 2008.

Internet sources

20 lat temu zamachowcy Al Kaidy dokonali zamachów bombowych w londyńskim metrze (Eng. Twenty years ago, Al-Qaeda bombers carried out attacks on the London Underground), PAP, 7 VII 2025, https://www.pap.pl/aktualnosci/20-rocznica-zamachow-bombowych-w-londynie#:~:text=7%20lipca%202005%20r.,ofiar%20zamachu%20 wynosi%C5%82%2034%20lata [accessed: 7 VII 2025].

About Prevent, Prevent Watch, https://www.preventwatch.org/about-prevent/ [accessed: 23 VII 2025].

Abu Hamza profile, BBC News, 9 I 2015, https://www.bbc.com/news/uk-11701269 [accessed: 18 XI 2025].

Al-Qaeda plotter jailed for life, BBC News, 7 XI 2006, http://news.bbc.co.uk/2/hi/uk_news/6123236.stm [accessed: 7 VIII 2025].

All 56 dead identified in July 7 attacks, NBC News, 20 VII 2005, https://www.nbcnews.com/id/wbna8642326 [accessed: 20 VII 2025].

Anjem Choudary's Ties to Extremists, Counter Extremism Project, https://www.counterextremism.com/anjem-choudary-ties-to-extremists [accessed: 23 X 2025].

Barlett J., Littler M., *Inside the EDL: Populist Politics in a Digital Age*, https://demos.co.uk/wp-content/uploads/2011/10/Inside_the_edl_WEB.pdf [accessed: 10 IX 2025].

British 7/7 suspects jailed for terrorism camp plans, Reuters, 29 IV 2009, https://www.reuters.com/article/world/british-7-7-suspects-jailed-for-terrorism-camp-plans-idUSTRE53S5SV/ [accessed: 29 VI 2025].

Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world*, https://www.statewatch.org/media/documents/news/2010/oct/uk-national-security-strategy-2008.pdf [accessed: 14 VI 2025].

Casciani D., *Muslims Against Crusades banned by Theresa May*, BBC News, 10 XI 2011, https://www.bbc.com/news/uk-15678275 [accessed: 10 XI 2025].

Chehab M.R., *Kim jest Anjem Choudary, mentor ostatniego zamachowca z Londynu?* (Eng. Who is Anjem Choudary, the mentor of the latest London bomber?), Newsweek, 8 XII 2019, https://www.newsweek.pl/swiat/po-zamachu-w-londynie-kim-jest-anjem-choudary/n0plx7f [accessed: 8 XI 2025].

Chemistry student held in Cairo, The Guardian, 15 VII 2005, https://www.theguardian.com/uk/2005/jul/15/july7.uksecurity10 [accessed: 15 VII 2025].

CPS statement: Convictions of Anjem Choudary and Khaled Hussein, Crown Prosecution Service, 31 VII 2024, https://www.cps.gov.uk/cps/news/cps-statement-convictions-anjem-choudary-and-khaled-hussein [accessed: 31 VII 2025].

Czarnecki M., *Po ataku nożownika w Southport rozruchy rozlały się na kolejne brytyjskie miasta. Aresztowano ponad 90 osób* (Eng. After the knife attack in Southport, riots spread to other British cities. Over 90 people were arrested), wyborcza.pl, 4 VIII 2024, https://wyborcza.pl/7,75399,31200497,po-ataku-nozownika-w-southport-rozruchy-rozlaly-sie-na-kolejne.html [accessed: 4 VIII 2025].

Director General Ken McCallum gives latest threat update, Security Service MI5, 8 X 2024, https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update [accessed: 8 X 2025].

Dodd V., *Ali Harbi Ali guilty of murdering MP David Amess in terrorist attack*, The Guardian, 11 IV 2022, https://www.theguardian.com/uk-news/2022/apr/11/david-amess-verdict-terrorist-attack-ali-harbi-ali-guilty [accessed: 11 VI 2025].

Dożywocie i 45 lat więzienia dla „rzeźników z Londynu" za zabójstwo żołnierza (Eng. Life imprisonment and 45 years in prison for the 'London butchers' for the murder of a soldier), TVN24, 26 II 2014, https://tvn24.pl/swiat/dozywocie-i-45-lat-wiezienia-dla-rzeznikow-z-londynu-za-zabojstwo-zolnierza-ra402449-ls3352033 [accessed: 26 VII 2025].

Drymer G., *Afery seksualne w Wielkiej Brytanii. Gwałty muzułmańskich gangów* (Eng. Sex scandals in the United Kingdom. Rape by Muslim gangs), Rzeczpospolita, 1 X 2017, https://www.rp.pl/spoleczenstwo/art2411491-afery-seksualne-w-wielkiej-brytanii-gwalty-muzulmanskich-gangow [accessed: 8 X 2025].

Ekstradycja Abu Hamzy do USA wstrzymana przez apelację (Eng. Abu Hamza's extradition to the US halted by appeal), Wirtualna Polska, 26 IX 2012, https://wiadomosci.wp.pl/ekstradycja-abu-hamzy-do-usa-wstrzymana-przez-apelacje-6082120547132033a [accessed: 26 IX 2025].

Eliott F., Goodchild S., *7/7 one year on: Why did it happen? The big questions still need answers*, The Independent, 2 VII 2006, https://www.independent.co.uk/news/uk/crime/7-7-one-year-on-why-did-it-happen-the-big-questions-still-need-answers-406351.html [accessed: 2 VII 2025].

Fury over British Muslim cleric's anti-war march threat, CNN, 5 I 2010, https://edition.cnn.com/2010/WORLD/europe/01/04/britain.afghanistan.demo/index.html [accessed: 5 I 2010].

Gammell C., *Muslims Against Crusades earn notoriety in less than a year*, The Telegraph, 21 IV 2011, https://www.telegraph.co.uk/news/8461436/Muslims-Against-Crusades-earn-notoriety-in-less-than-a-year.html [accessed: 21 VI 2025].

Gilliam J., *Why They Hate Us. An Examination of al-wala' wa-l-bara' in Salafi-Jihadist Ideology*, Military Review, 15 II 2018, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Feb/They-Hate/ [accessed: 15 VII 2025].

'Have more babies and Muslims can take over the UK' hate fanatic says, as warning comes that 'next 9/11 will be in UK', Daily Mail, 13 IX 2008, https://www.dailymail.co.uk/news/article-1054909/Have-babies-Muslims-UK-hate-fanatic-says-warning-comes-9-11-UK.html [accessed: 13 VII 2025].

Hoge W., *Threats and Responses: Terror Suspects, Mosque Raid in London Results in 7 Arrests in Connection With Discovery of Poison*, The New York Times, 21 I 2003, https://www.nytimes.com/2003/01/21/world/threats-responses-terror-suspects-mosque-raid-london-results-7-arrests.html [accessed: 18 IX 2025].

Intelligence and Security Committee, *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c153540f0b61a825d6582/7-7_attacks_intelligence.pdf [accessed: 23 VI 2025].

Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, https://assets.publishing.service.gov.uk/media/5a7c470140f0b62dffde1050/isc_terrorist_ attacks_7july_ report. pdf [accessed: 18 XI 2025].

International counter terrorism investigation leads to Anjem Choudary conviction, Counter Terrorism Policing, 23 VII 2024, https://www.counterterrorism.police.uk/historic-met-and-international-police-counter-terrorism-investigation-leads-to--anjem-choudary-terror-conviction/ [accessed: 23 VII 2024].

Johnston C., *Tube blasts 'almost simultaneous'*, The Guardian, 9 VII 2005, https://www.theguardian.com/uk/2005/jul/09/july7.uksecurity12 [accessed: 9 VII 2025].

Koenig K.L., *Medical Consequences of the 2005 London Terrorist Bombings*, NEJM Journal Watch, 25 I 2007, https://www.jwatch.org/em200701260000006/2007/01/26/medical-consequences-2005-london-terrorist [accessed: 26 VI 2025].

Levitt B., *The True Story Behind Attack on London: Hunting the 7/7 Bombers*, Time, 1 VII 2025, https://time.com/7299329/attack-on-london-netflix-true-story/ [accessed: 1 VII 2025].

"Magnificent 19" risks further outrage, The Standard, 13 IV 2012, https://www.standard.co.uk/hp/front/magnificent-19-risks-further-outrage-6948639.html [accessed: 18 XI 2025].

Marsden C., *Britain: Why did it take so long to bring Abu Hamza to trial?*, World Socialist Web Site, 16 II 2006, https://www.wsws.org/en/articles/2006/02/hamz-f16.html [accessed: 16 VII 2025].

Orr D., *Is the Islam4UK ban a blow against democracy?*, The Guardian, 14 I 2010, https://www.theguardian.com/commentisfree/2010/jan/14/deborah-orr-islam4uk [accessed: 14 VII 2025].

Oskarżony o planowanie masakry niewinny. Abu Katada na wolności (Eng. Man accused of planning massacre found not guilty. Abu Katada released), TVN24, 24 IX 2014, https://tvn24.pl/swiat/oskarzony-o-planowanie-masakry-niewinny-abu-katada-na-wolnosci-ra471293-ls3412841 [accessed: 24 IX 2025].

Owen P., *Clarke rejects Hamza inquiry calls*, The Guardian, 9 II 2006, https://www.theguardian.com/uk/2006/feb/09/terrorism.politics [accessed: 18 IX 2025].

Pearson A., *Allison Pearson: We must get rid of the dreadful Human Rights Act*, The Telegraph, 13 V 2015, https://www.telegraph.co.uk/news/uknews/law-and-order/11602222/Allison-Pearson-We-must-get-rid-of-the-dreadful-Human-Rights-Act.html [accessed: 13 VI 2025].

Policja nie odpowie za śmierć w *metrze* (Eng. The police will not be held responsible for the death in the underground), TVN24, 13 II 2009, https://tvn24.pl/swiat/policja-nie-odpowie-za-smierc-w-metrze-ra85753-ls3724956 [accessed: 13 VII 2025].

Profile: Mohammad Sidique Khan, BBC News, 2 III 2011, https://www.bbc.com/news/uk-12621381 [accessed: 2 VI 2025].

"Przygotowywał działalność terrorystyczną". Mężczyzna zatrzymany (Eng. 'He was preparing terrorist activities.' Man detained), TVN24, 2 XII 2019, https://tvn24.pl/swiat/wielka-brytania-policja-zatrzymala-mezczyzne-podejrzanego-o-terroryzm--ra989867-ls2508450 [accessed: 2 X 2025].

Radical cleric Abu Hamza jailed for life by US court, BBC News, 9 I 2015, https://www.bbc.com/news/world-us-canada-30754959 [accessed: 18 IX 2025].

Ray M., *London bombings of 2005*, Britannica, https://www.britannica.com/event/London-bombings-of-2005 [accessed: 12 VII 2025].

Report of the 7 July Review Committee, https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/archives/assembly-reports-7july-report.pdf [accessed: 20 VI 2025].

Report of the Official Account of the Bombings in London on 7th July 2005, https://assets.publishing.service.gov.uk/media/5a7c7bc840f0b626628ac62e/1087.pdf [accessed: 7 VII 2025].

Safdar A., *Prevent: UK anti-terror plan "harms children's rights"*, AlJazeera, 13 VII 2016, https://www.aljazeera.com/features/2016/7/13/prevent-uk-anti-terror-plan--harms-childrens-rights [accessed: 13 VII 2025].

Shehzad Tanweer, Counter Extremism Project, https://www.counterextremism.com/extremists/shehzad-tanweer [accessed: 27 VI 2025].

Shishani M.B., *Salafi-Jihadists Geopolitical Perspective of Central Asia*, Central Asia – Caucasus Analyst, https://www.cacianalyst.org/publications/analytical-articles/item/10050-analytical-articles-caci-analyst-2005-6-29-art.-10050.html [accessed: 29 VI 2025].

Smith M., *Which extremists do Britons see as threats in 2024?*, YouGov, 29 II 2024, https://yougov.co.uk/politics/articles/48784-which-extremists-do-britons-see-as--threats-in-2024 [accessed: 29 VII 2025].

Strieff D., *Terror-tinged U.K. mosque gets a makeover*, NBC News, 5 VII 2006, https://www.nbcnews.com/id/wbna13501930 [accessed: 18 IX 2025].

Szymczak P., *TATP, materiał wybuchowy zwany matką szatana. Czy można go wykryć?* (Eng. TATP, an explosive known as the mother of Satan. Can it be detected?), Focus.pl, 23 IX 2019, https://www.focus.pl/artykul/czy-tatp-materia-wybuchowy-zwany-matk-szatana-mona-wykry [accessed: 23 VI 2025].

Terror Watch: What Ricin?, Newsweek, 12 IV 2005, https://www.newsweek.com/terror-watch-what-ricin-116577 [accessed: 18 IX 2025].

Terrorism threat levels, Security Service MI5, https://www.mi5.gov.uk/threats-and-advice/terrorism-threat-levels [accessed: 23 VI 2025].

Vencat E.F., *'Bleed the Enemy'*, Newsweek, 11 I 2006, https://www.newsweek. com/bleed-enemy-108227 [accessed: 11 VII 2025].

Vince G., *Explosives linked to London bombings identified*, New Scientist, 15 VII 2005, https://www.newscientist.com/article/dn7682-explosives-linked-to-london-bombings-identified/ [accessed: 15 VII 2025].

W. Brytania: Nowa ustawa antyterrorystyczna weszła w życie (Eng. United Kingdom: New anti-terrorism law comes into force), Wirtualna Polska, 13 IV 2006, https://www.money.pl/archiwum/wiadomosciagencyjne/pap/artykul/w;brytania;nowa;ustawa;antyterrorystyczna;weszla;w;zycie,28,0,152348.html [accessed: 13 IV 2006].

Watson R., *Al-Muhajiroun and the long tail of UK terror*, The New Statesman, 22 II 2020, https://www.newstatesman.com/long-reads/2020/02/al-muhajiroun-and-long-tail-uk-terror [accessed: 22 VII 2025].

Weiss D., *If You Criticize Islam, You Will Suffer Consequences*, Citizen Times, 13 VII 2014, http://www.citizentimes.eu/2013/06/13/if-you-criticize-islam-you-will-suffer-consequences/ [accessed: 13 VIII 2024].

Whine M., *The Penetration of Islamist Ideology in Britain*, Hudson Institute, 18 V 2005, https://www.hudson.org/national-security-defense/the-penetration-of-islamist-ideology-in-britain [accessed: 18 XI 2025].

Wielka Brytania: 11 skazanych za planowanie zamachów w Birmingham (Eng. United Kingdom: 11 convicted for planning attacks in Birmingham), Wirtualna Polska, 26 IV 2013, https://wiadomosci.wp.pl/wielka-brytania-11-skazanych-za-planowanie-zamachow-w-birmingham-6082107866088065a [accessed: 26 VII 2025].

Wydalony z Wielkiej Brytanii Abu Katada, oskarżony o terroryzm (Eng. Abu Katada, accused of terrorism, expelled from the United Kingdom), Wirtualna Polska,

7 VII 2013, https://wiadomosci.wp.pl/wydalony-z-wielkiej-brytanii-abu-katada-oskarzony-o-terroryzm-6031568274154113a [accessed: 7 VII 2025].

The article expresses the view of the author and does not represent the position of the Internal Security Agency.

Krzysztof Izak

Retired officer of the Internal Security Agency, who served, inter alia, in divisions carrying out tasks in the field of counteracting terrorist threats. Author of more than 20 articles on terrorism, which were published in many scientific journals. Creator of *Lexicon of Islamist organisations and movements* published by the Internal Security Agency.

Contact: lizior3@wp.pl

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 389–410

https://doi.org/10.4467/27204383TER.25.058.23045

Article

Terrorist threats in the European Union in 2024. Analysis of the TE-SAT. European Union Terrorism Situation and Trend Report 2025

SEBASTIAN WOJCIECHOWSKI https://orcid.org/0000-0002-7972-6618
Adam Mickiewicz University in Poznań
Institute for Western Affairs in Poznań

ARTUR WEJKSZNER https://orcid.org/0000-0002-7638-9708
Adam Mickiewicz University in Poznań

Abstract

The authors of the article analysed the terrorist threats in the European Union in 2024 based on the data contained in the Europol report entitled *TE-SAT. European Union Terrorism Situation and Trend Report 2025* and characterised them with reference to data concerning individual EU Member States. The authors described both the objective aspect of the threats (from jihadist, right-wing, left-wing and anarchist, ethno-nationalist and separatist groups, and others) and the quantitative aspect (e.g. the number of attacks and people arrested for terrorism). Data from the report indicate that in 2024, the number of terrorist attacks in the EU decreased compared to 2023 (from 120 to 58), but at the same time, the number of EU Member States experiencing attacks increased (from 7 to 14). The number of jihadist attacks has also escalated (from 14 to 24). An increase in the number of people arrested for terrorism-related crimes was also recorded (from 426 to 449). Furthermore, it is evident that the age of terrorists is gradually decreasing. New technological solutions,

such as drones, 3D printing and artificial intelligence, are being used in terrorist activities. Of particular concern are the growing links between terrorists and criminal groups and the intelligence services of hostile states. All the above evidence demonstrates the constant changes in the nature of terrorist threats in the EU.

Keywords

terrorism, European Union, security, Europol, TE-SAT Report

Introduction

The changes taking place in contemporary terrorism occur on many levels and affect different parts of the world[1]. These include changes in the profile of perpetrators (e.g. increasingly younger age), terrorist tactics and strategies, and their use of new technologies (e.g. artificial intelligence, 3D printing, drones, Starlink systems[2]). This can be confirmed by the example of the European Union. In the article, the authors analysed the latest Europol report entitled *TE-SAT. European Union Terrorism Situation and Trend Report 2025*[3] (hereinafter: TE-SAT 2025 report) and characterised terrorist threats, taking into account data on individual EU Member States. They discussed both the substantive aspect of the threat (from jihadist, right-wing, left-wing and anarchist, ethno-nationalist

[1] On the evolution of the terrorist threat in the EU between 2021 and 2024, see, for example: S. Wojciechowski, *The hybrid dimension of contemporary terrorism and critical infrastructure. Analysis of Europol's TE-SAT reports from 2021–2024*, "Terrorism – Studies, Analyses, Prevention" 2025, special edition: *Terrorist and sabotage threats to critical infrastructure*. https://doi.org/10.4467/27204383TER.25.020.21523; S. Wojciechowski, *Terrorism – old wine in new bottles*, Defence24, 21 VII 2025, https://defence24.com/geopolitics/terrorism-old-wine-in-new-bottles [accessed: 25 VII 2025].

[2] The UN Security Council Counter-Terrorism Committee has identified unmanned aerial systems as one of the main terrorist threats. This is due to both the growing logistical and financial capabilities of terrorist structures and the rapid development of the commercial and military drone market. See: *Wojny dronów: jak to się robi w Afryce [ANALIZA]* (Eng. Drone wars: how it's done in Africa [ANALYSIS]), Defence24, 31 V 2025, https://defence24.pl/technologie/wojny-dronow-jak-to-sie-robi-w-afryce-analiza#goog_rewarded [accessed: 18 VII 2025].

[3] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf [accessed: 20 VII 2025]. https://doi.org/10.2813/5425593.

and separatist groups, among others) and the quantitative aspect (e.g. the number of attacks and people arrested for terrorism).

The international context of the terrorist threat in the European Union

An analysis of the terrorist threat in the EU requires consideration of the broader context. This threat is greatly influenced by the conflict in the Gaza Strip, which has been accompanied by numerous attacks and calls for violence spread by fundamentalists, including on the internet. Attention should also be paid to the success of the opposition in Syria, especially its Islamist factions, which jihadists continue to exploit for propaganda and military purposes[4]. In the context of analysing the threat in the EU, it is also important to note that groups linked to Islamic State and Al-Qaeda have greatly strengthened their position in Africa, mainly in the Sahel. According to Europol, the target of militias trained in Africa is Europe, and these groups are transforming the Sahel countries (especially Mali, Burkina Faso and Niger) into a centre of global terrorism. This has a direct impact on security in the EU. The Sahel has become a base for a growing number of foreign terrorists who are looking for new fronts to fight on after withdrawing from Syria or Iraq, for example. What is more, the groups operating there – e.g. those linked to Al-Qaeda: the Islamic and Muslim Support Group (Jama'at Nusrat ul-Islam wa al-Muslimin, JNIM), Al-Shabaab (Harakat al-Shabaab al-Mujahideen, HSM), the Islamic State West Africa Province (ISWAP) and the Islamic State Sahel Province (ISSP) – are expanding their influence. They now also threaten countries on the Gulf of Guinea, including Togo, Benin, Ghana and Côte d'Ivoire. One consequence of this situation is the dramatic increase in the number of fatalities caused by terrorist activities worldwide. In 2024, more than half of these people (51%) were killed in the Sahel region (in 2023, it was 48%)[5].

[4] One example is the ISIS attack on American soldiers in Syria on 13 December 2025. See: E. Kourdi, N. Bertrand, *Trump pledges retaliation after two US soldiers, one civilian interpreter killed in Syria*, CNN, https://edition.cnn.com/2025/12/13/politics/two-us-army-soldiers-killed-in-syria [accessed: 17 XII 2025].

[5] *Europol: Afryka jest problemem dla bezpieczeństwa Unii Europejskiej* (Eng. Europol: Africa is a problem for the security of the European Union), Onet, 26 VI 2025, https://wiadomosci.

As already mentioned, fundamentalists in Africa spread propaganda via digital platforms. It is disseminated in many languages and also targets young Europeans. Another serious problem is the use of Starlink systems by terrorists, both for communication and armed combat. These systems are particularly useful in the vast areas of West Africa, which lack traditional communication infrastructure. This is highlighted in a report by the Global Initiative against Transnational Organized Crime[6]. Europol is therefore calling on European countries to strengthen their cooperation with African entities and to anticipate the risks associated with potential threats, including the influx of trained Islamic terrorists into Europe[7].

Another serious challenge to the security of EU Member States is state terrorism supported or directly carried out by Russia and its allies. This manifests itself not only in cyberattacks and acts of terror, but also in the recruitment of foreigners, including via the Telegram messaging app, to organise sabotage in Europe. This has been noted by both European intelligence services and, for example, the Organized Crime and Corruption Reporting Project, an American non-governmental organisation involved in investigative journalism[8]. This is also directly referenced in the report *Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe*[9].

onet.pl/swiat/europol-afryka-jest-problemem-dla-bezpieczenstwa-unii-europejskiej/f6pm9xl [accessed: 20 VII 2025].

[6] *Observatory of Illicit Economies in West Africa*, https://riskbulletins.globalinitiative.net/download/wea-obs-012-screen-pdf.pdf [accessed: 10 VII 2025].

[7] See e.g.: A. Wejkszner, *Europejska armia kalifatu*. Tom 1. *Centrum supersieci* (Eng. The European Army of the Caliphate. Volume 1. The centre of the supernetwork), Warszawa 2020; A. Wejkszner, *Europejska armia kalifatu.* Tom 2. *Peryferie supersieci* (Eng. The European Army of the Caliphate. Volume 2. The Peripheries of the Supernetwork), Warszawa 2023.

[8] *'Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder*, Organized Crime and Corruption Reporting Project, 26 IX 2024, https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder [accessed: 20 VII 2025]; *How crime is accelerated by AI*, Europol, https://www.europol.europa.eu/media-press/europol-podcast/episode-21-how-crime-is-accelerated-by-ai [accessed: 21 VII 2025].

[9] *Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe*, https://icct.nl/sites/default/files/2025-09/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool.pdf [accessed: 16 XII 2025].

Terrorist threats in the European Union in 2024 compared to data from 2022–2023

Presenting data from 2024 against previous years will enable us to track the dynamics of changes occurring in the phenomena discussed.

Terrorist attacks – general characteristics

According to the TE-SAT 2025 report, in 2024 Europol recorded a total of 58 terrorist attacks (including 34 carried out, 5 unsuccessful and 19 foiled) in 14 EU Member States. The highest number of attacks took place in Italy (20), followed by France (14), Germany (6), Austria and Greece (3 each), the Czech Republic, Denmark, Lithuania (2 each), and Belgium, Ireland, the Netherlands, Slovakia, Spain and Malta (1 each). Jihadist terrorists were attributed 24 attacks, left-wing and anarchist terrorists – 21. Eight attacks were classified as other forms of terrorist threat, 4 were separatist in nature and 1 was right-wing (Table 1).

Although the number of attacks fell significantly in 2024 (there were 120 in 2023[10], and 58 in 2024), the data contained in the Europol report does not inspire optimism. The number of EU Member States affected by attacks rose from 7 to 14. This is particularly evident in the case of the jihadist threat. In 2023, 14 attacks of this nature were recorded in 4 countries, while in 2024 there were 24 attacks in 7 countries. Jihadist attacks caused the highest number of fatalities compared to other types of terrorist attacks. In 2024, they resulted in 5 deaths and 18 injuries in the EU.

In 2024, most attacks (12) were directed at civilians. Eight attacks were carried out by jihadists, three by perpetrators linked to ethno-nationalist or separatist terrorism, and one was classified as another form of terrorism. The second most frequently attacked target was the industrial (state-owned) sector, with nine incidents. All attacks were organised by left-wing and anarchist terrorists. Other popular targets included private companies (5), religious entities/symbols (5), critical infrastructure (4), political entities (4) and law enforcement agencies (4). The attacks took place mainly in cities (45), with significantly fewer in rural areas (13).

[10] See e.g.: S. Wojciechowski, A. Wejkszner, *The new face of terrorist threat in the European Union. Analysis of the EU Terrorism Situation and Trend Report 2024 (TE-SAT) and other sources*, "Terrorism – Studies, Analyses, Prevention" 2025, no. 7, pp. 307–326. https://doi.org/10.4467/27204383TER.25.035.21812.

Table 1. Number of terrorist attacks in EU countries in 2024, broken down by ideological motivations of perpetrators (figures include attacks carried out, failed and foiled).

COUNTRY	TERRORISM TYPE					TOTAL
	JIHADIST	RIGHT-WING	LEFT-WING AND ANARCHIST	ETHNO-NATIONALIST AND SEPARATIST	OTHER	
Austria	3					**3**
Belgium	1					**1**
Czechia					2	**2**
Denmark					2	**2**
France	11			3		**14**
Greece			3			**3**
Spain	1					**1**
Netherlands	1					**1**
Ireland	1					**1**
Lithuania					2	**2**
Malta					1	**1**
Germany	6					**6**
Slovakia					1	**1**
Italy		1	18	1		**20**
TOTAL	**24**	**1**	**21**	**4**	**8**	**58**

Source: own elaboration based on: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, p. 62 [accessed: 20 VII 2025].

The most common form of terrorist activity was arson (used in 22 attacks). This was followed by bombings (11 attacks), stabbings (8), the use of firearms (6), destruction of property (6) and kidnappings (1). In most attacks (15), escalators of fire were used. They were used primarily by left-wing and anarchist terrorists (11 attacks). Improvised explosive devices were used in 10 cases, bladed weapons also in 10 (attacks carried out by jihadists), and improvised incendiary devices in 6.

Arrests for terrorist offences

It should be emphasised that the overall number of persons arrested for terrorist offences has increased[11]. In 2023, there were 426 such persons, and in 2024 – 449 (Figure 1) in 20 EU Member States. Those detained were mainly men – 405 persons. The highest number of arrests was made in Spain (90 persons), followed by France (69), Italy (62) and Germany (55). In Poland, 13 arrests were recorded, with 1 case involving jihadist terrorist activities and 12 unclassified incidents.

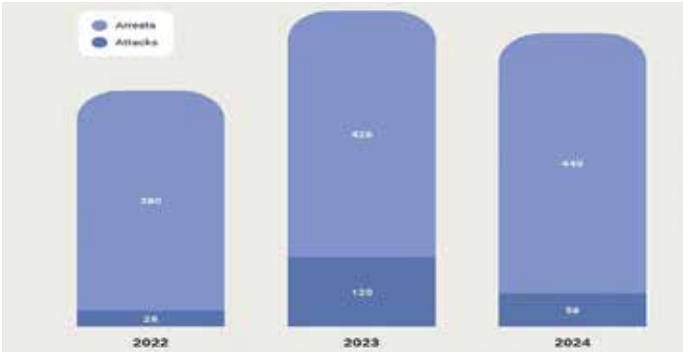


Figure 1. Number of terrorist attacks and number of persons arrested for terrorist activities in the EU between 2022 and 2024 (the figures presented for attacks include attacks that were carried out, failed and foiled).

Source: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, p. 13 [accessed: 20 VII 2025].

[11] In *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*, a 'terrorist offence' is defined as a criminal act committed with the aim of seriously intimidating the population, unduly compelling a government or an international organisation or destabilising the fundamental structures of a State. This Directive establishes a common framework for definitions, but the internal provisions of EU Member States differ in detail.

In the EU, most arrests in 2024 concerned perpetrators of jihadist terrorism (289). Compared to the previous year, this number decreased from 334 (Figure 2).

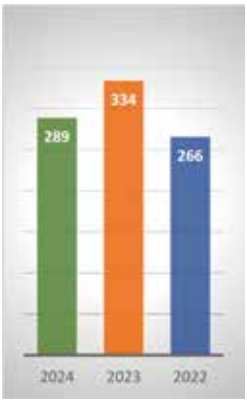


Figure 2. Number of arrests of persons suspected of jihadist terrorist offences in EU Member States between 2022 and 2024.

Source: own elaboration based on: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, p. 26 [accessed: 20 VII 2025].

Almost half (136) of the 289 people arrested were detained in two countries – France and Spain. The vast majority (88%) of those arrested were men. Most of them were teenagers or men under the age of 27. Less than half of those arrested were charged with belonging to a terrorist organisation or distributing jihadist propaganda on the internet[12].

In the case of other forms of terrorism, there has been an increase in the number of arrests. This applies in particular to perpetrators of: extreme right-wing, extreme left-wing and anarchist terrorism, as well as unclassified forms of terrorism[13].

[12] Europol, *TE-SAT*..., pp. 26–27.

[13] This group includes, for example, acts of sabotage reported by Poland and Spain and carried out on behalf of foreign services. During the period analysed, 9 people recruited by Russian agents were detained in these countries. As Jacek Dobrzyński, spokesperson for the Minister-Coordinator of Special Services, announced on 29 July 2025: 'Officers of the Internal Security Agency have determined that a 27-year-old Colombian acting on behalf of Russian intelligence was behind two arson attacks that took place in Poland in 2024. The incidents occurred on 23 May last year in Warsaw and a week later, on 30 May,

In 2024, almost twice as many people were arrested in EU Member States on suspicion of terrorist activity motivated by far-right ideology than in the previous year (47 and 26 respectively). Those arrested were exclusively men aged between 12 and 76 with EU citizenship.

In the case of terrorist activities motivated by extreme left-wing and anarchist ideology, however, the police arrested a relatively small number of people associated with this type of activity, considering the number of such activities. There were 28 people in total, 20 of whom were arrested in Greece. Among those arrested, there were almost five times more men than women, and their ages ranged from 26 to 78. Their terrorist affiliations were not disclosed, indicating that they belonged to independent cells operating autonomously. However, Greek investigators managed to identify at least three terrorist groups, to which a total of ten detainees belonged. These were: 'Partnership of Revenge', 'Conspiracy of Revenge' and 'Armed Response'.

In connection with suspicions of extremism motivated by ethno-nationalist ideology, 27 people were detained in EU Member States in 2024. More than half of them belonged to the Kurdistan Workers' Party (Partiya Karkerên Kurdistanê). They were accused of preparing a terrorist attack, membership of a terrorist organisation, financing its activities and spreading terrorist propaganda[14].

The most common terrorism-related offences were: membership of a terrorist organisation (110), planning or preparing an attack (107) and creating and/or disseminating terrorist propaganda (90)[15].

It is very worrying that in 2024, the number of minors and young people involved in terrorist and extremist activities in the EU increased. Of the 449 people arrested in 2024, 133 were aged between 12 and 20, accounting for over 29% of all arrests for terrorist offences. The youngest suspect was 12 years old and was arrested for planning an attack. The vast majority of juvenile offenders were linked to jihadist terrorism. The charges against them most often concerned: participation in attacks, creating and

in Radom'. See: *Pożary w Polsce. Kolumbijczyk miał działać na zlecenie Rosji. Ustalenia ABW* (Eng. Fires in Poland. Colombian man allegedly acting on behalf of Russia. Findings of the ABW), Rzeczpospolita, 29 VII 2025, https://www.rp.pl/przestepczosc/art42769991-pozary-w-polsce-kolumbijczyk-mial-dzialac-na-zlecenie-rosji-ustalenia-abw [accessed: 30 VII 2025].

[14] Europol, *TE-SAT*..., pp. 50–51.

[15] Ibid., p. 14.

disseminating radical content, and membership of a terrorist or extremist group. The juvenile terrorists were mostly males who were radicalised online and operated independently of any organisational structures[16].

Terrorism motivated by jihadist ideology

In 2024, terrorism motivated by jihadist ideology[17] posed a significant challenge to the security of EU countries. This is evidenced by data on both successful and unsuccessful terrorist attacks. Jihadists carried out two attacks both in France and Germany and one each in Ireland and the Netherlands. As a result, five people were killed and 18 were injured[18]. There were three times as many failed attacks (Figure 3).

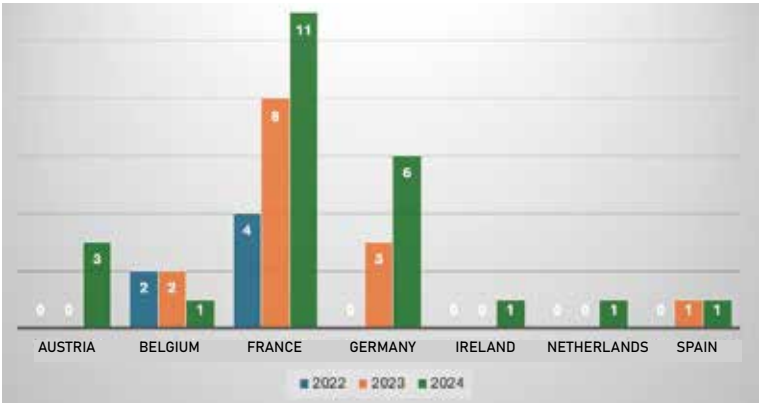


Figure 3. Number of terrorist attacks motivated by jihadist ideology in EU Member States between 2022 and 2024 (the figures presented include attacks that were carried out, failed and foiled).

Source: own elaboration based on: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, p. 24 [accessed: 20 VII 2025].

[16] Ibid., p. 10.

[17] According to the authors of the report, jihadism is defined as a radical branch of Salafism (a Sunni Muslim revivalist movement). Its supporters reject modern democracy because, in their view, man-made laws contradict God's status as the sole lawgiver. Jihadists seek to create an Islamic state governed exclusively by Islamic law (Sharia). Unlike other Salafi movements, jihadists legitimise the use of violence by referring to classical Islamic doctrines of jihad (the term literally means 'striving' or 'effort', but jihadists understand it as religiously sanctioned warfare). All those who oppose jihadist interpretations of Islamic law are considered enemies of Islam and therefore legitimate targets for attack. Some jihadists also view Shiites and other Muslims as enemies. See ibid., p. 23.

[18] Ibid.

The modus operandi of jihadist terrorists should be considered characteristic of this group of religious extremists. It involved only the activities of individual jihadist terrorists[19]. In at least two cases (Germany and France), the perpetrators were suspected or confirmed to have links to Islamic State[20]. Their targets were primarily mass events, including football matches and other sporting events in France, and a concert in Austria. In addition, attempts were made to attack places of worship (mainly synagogues) and targets related to the justice system. The attackers most often used primitive weapons, mainly knives. One example of this tactic is the attack carried out on 2 March 2024 in Zurich by a 15-year-old boy. He attacked a 50-year-old Orthodox Jew. Shortly before, he had posted an oath of allegiance to the Caliph of the Islamic State on social media and called for attacks on Jews and Christians. The radicalisation process of the attacker (a Swiss citizen with immigrant roots) began in Tunisia, where he stayed between 2017 and 2021[21]. What was unique about this incident was that it was broadcast live, which, according to the perpetrator, was intended to have a propaganda effect. Another example of the use of this tactic is the attack in Solingen, Germany, on 23 August 2024. The attacker used a knife to attack random participants at a city festival, killing 3 people[22]. Just before the attack, he contacted a representative of Islamic State via instant messaging, who encouraged him to document his intentions so that the material could later be used for propaganda purposes[23]. A similar tactic was used during the terrorist attacks carried out on 15 August 2024 in Galway, Ireland, and on 19 September 2024 in Rotterdam, the Netherlands. The perpetrators were young men aged 16 and 22[24].

---

[19] On the subject of so-called individual jihadist terrorism, see: A. Wejkszner, *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej* (Eng. Lone wolves of the caliphate? The Islamic State and individual jihadist terrorism in Western Europe), Warszawa 2018, pp. 27–47.

[20] Europol, *TE-SAT*..., p. 23.

[21] *Anti-Semitism: Zurich attacker radicalised in Tunisia and online,* swissinfo.ch, 25 III 2024, https://www.swissinfo.ch/eng/swiss-politics/zurich-stabber-radicalized-in-tunisia-and-online/74284770 [accessed: 20 VII 2025].

[22] *Anklage gegen ein mutmaßliches Mitglied der ausländischen terroristischen Vereinigung "Islamischer Staat (IS)" wegen des Messerangriffs in Solingen erhoben,* Der Generalbundesanwalt beim Bundesgerichtshof, 27 II 2025, https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2025/Pressemitteilung-vom-27-02-2025.html [accessed: 20 VII 2025].

[23] Ibid.

[24] Europol, *TE-SAT*..., p. 25.

The events discussed above indicate that the threat of jihadist terrorism persisted in the EU (or, more broadly, in Western Europe) during the period under review. This is also confirmed by the number of people arrested on suspicion of involvement in such activities.

One of the main drivers of jihadist radicalisation in the EU during the period under review, including attacks on Jewish targets and targets associated with the State of Israel, were the events in the Gaza Strip in 2024, triggered by Hamas terrorist attacks on targets in Israel in October 2023. Al-Qaeda and Islamic State propagandists used anti-Israeli and anti-Christian narratives, drawing on images of the effects of Israel's retaliatory actions in the Gaza Strip[25].

Terrorism motivated by extreme right-wing ideology

In 2024, terrorism perpetrated by far-right groups[26] posed a significantly lower threat to the EU than jihadist terrorism. During this period, there was only one attack motivated by this ideology (Figure 4).

The attack covered in the Europol report took place in Montello, Italy, on 18 March 2024. The alleged attacker attempted to set fire to the entrance of the Islamic Centre. However, the classification of this case seems questionable, as neither the perpetrator's political agenda nor his terrorist affiliation has been disclosed. The targets of attacks motivated by far-right ideology were to be people of non-white races, far-left activists and unidentified 'enemies and traitors'[27].

[25] Ibid., pp. 29–30.

[26] The authors of the report understand the term 'far-right terrorism' to mean the use of violence to transform the contemporary political, social and economic system into an authoritarian model in which democratic values and institutions would be rejected. Right-wing ideologies that refer to this model use aggressive narratives focused on nationalism, racism, xenophobia and other forms of intolerance. The basic concept of right-wing extremism is the supremacy of a nation or race. In practice, this means that a common element characterising a given group of people makes them superior to others and they consider domination over the rest of the population to be their natural right. In addition, right-wing extremist ideologies also promote ideas that oppose social diversity and equal rights for minorities, such as misogyny, hostility towards the LGBTQ+ community, and anti-immigration attitudes. See ibid., p. 34.

[27] Ibid., pp. 36–37.

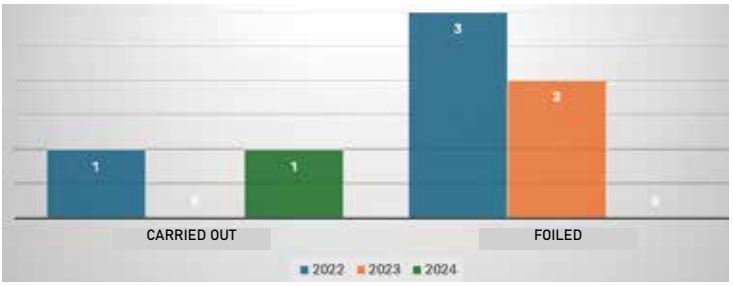


Figure 4. Number of terrorist attacks motivated by far-right ideology in EU Member States between 2022 and 2024.

Source: own elaboration based on: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, p. 36 [accessed: 20 VII 2025].

In order to intensify the recruitment of new extremists and encourage them to use violence, supporters of this ideology used online tools. Their efforts were primarily directed at representatives of socially and economically dysfunctional communities, dominated by a cult of strength and opposition to current social processes (e.g. legal and illegal migration). In this context, neo-Nazi circles were particularly dangerous, as their network structure (reminiscent of that created by jihadists) made it difficult for the police and the judiciary to effectively penetrate them. It is worth noting that representatives of these circles gained experience in the use of various types of weapons during the Russian-Ukrainian conflict, fighting on both sides of the conflict[28].

Terrorism motivated by extreme left-wing and anarchist ideology

In 2024, far-left and anarchist groups in the EU were noticeably more active than in the two cases discussed above[29]. They were responsible for a total of 21 terrorist attacks – 17 successful and 4 unsuccessful (Figure 5). These attacks were mainly carried out in Italy and Greece.

[28] Ibid., p. 38.

[29] In the report, terrorist activity by extreme left-wing groups is understood as activity involving the use of violence and aimed at provoking a revolution motivated by Marxist-Leninist ideology, directed against the democratic state. The aim of such activities is to establish socialism, communism or a classless society. Anarchist terrorism, in turn, is a form of political violence aimed at destroying the current model of political power and replacing it with an anti-discriminatory and anti-capitalist model that promotes equality, freedom and social justice. See ibid., p. 42.

Figure 5. Number of terrorist attacks motivated by extreme left-wing and anarchist ideology in EU Member States between 2022 and 2024.

Source: own elaboration based on: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, p. 42 [accessed: 20 VII 2025].

The perpetrators' modus operandi did not change significantly compared to previous years. The attacks were mainly directed at critical infrastructure, including properties belonging to state institutions. From a tactical point of view, arson attacks were the most effective. Of the 13 cases in which this tactic was used, 2 involved the use of improvised incendiary devices and 4 involved improvised explosive devices. The perpetrators claimed political responsibility for 10 terrorist attacks, in most cases by posting a statement on the internet. The most frequently cited reasons for such activity were opposition to government policy (mainly migration policy) and anti-war and anti-capitalist views. To a lesser extent, emphasis was placed on the fight for animal rights or solidarity with comrades repressed by the justice system. The Europol report cites the attack on a photovoltaic farm in Tuili, Italy, on 10 September 2024 as an example of a terrorist attack of this type. The arson attack destroyed approx. 2000 panels belonging to the Portuguese company Greenvolt Power, causing losses of at least EUR 1 million[30]. The perpetrators have not been identified. Therefore, attributing this criminal activity to the indicated group of terrorist attacks solely on the basis of the perpetrators' modus operandi should be considered methodologically questionable.

[30] *Attack in Tuili during the night: hundreds of photovoltaic panels destroyed*, L'Unione Sarda.it, 10 IX 2024, https://www.unionesarda.it/en/sardinia/attack-in-tuili-during-the-night-hundreds-of-photovoltaic-panels-destroyed-nuyrob0o [accessed: 20 VII 2025].

Among the main propaganda themes promoted by members of extreme left-wing and anarchist groups were anti-fascist, anti-imperialist, anti-colonial, anti-war and anti-authoritarian slogans. Slogans of solidarity with persecuted Palestinians and Kurds were also proclaimed, and NATO and the EU were criticised[31].

Terrorism motivated by ethno-nationalist ideology

Terrorists motivated by ethno-nationalist ideology[32] carried out relatively few terrorist acts in 2024 compared to the perpetrators with other motivations described above. They were responsible for only 4 attacks, which is a significant decrease compared to the previous year (70 attacks). Three of these attacks took place in France and one in Italy[33] (Figure 6). According to the French police, the attacks in France were carried out by the National Liberation Front of Corsica (Front de libération nationale corse) and the Secret Corsican Youth (Ghjuventù Clandestina Corsa). The tactics used in the attacks (arson attacks on property) remained unchanged.

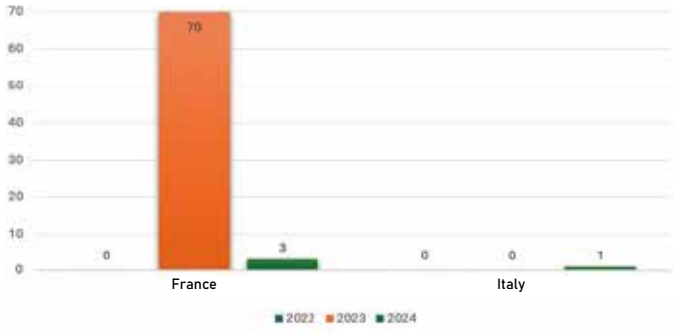


Figure 6. Number of terrorist attacks motivated by ethno-nationalist and separatist ideology in the EU between 2022 and 2024 (the figures presented include attacks that were carried out, failed and foiled).

Source: own elaboration based on: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf, p. 50 [accessed: 20 VII 2025].

[31] Europol, *TE-SAT*..., pp. 46–47.

[32] The concept of ethno-nationalist or separatist terrorist groups includes groups whose members refer to nationalist ideologies or ethnic or national affiliation as part of their political agenda. The strategic goal of these groups is to separate a territory from an existing state and/or to annex a territory to another state. See ibid., p. 49.

[33] Ibid., p. 50.

The TE-SAT 2025 report also contains information on activities undertaken by Irish terrorists linked to groups that do not support the peace process in Northern Ireland (the New IRA, the Continuity IRA). However, during the period analysed, no members of either group returned to terrorist activity[34].

Other forms of terrorist activity

The TE-SAT 2025 report also mentions 8 other cases of terrorist activity, but does not specify the affiliation of the perpetrators. The most well-known example is the attempted assassination of Prime Minister Robert Fico on 15 May 2024 in Handlova, Slovakia. The perpetrator, Juraj Cintula, had been planning the attack since at least April[35]. However, there was no manifesto published shortly before the attack, which is characteristic of individual terrorist attacks, in which the attacker would indicate the motives for the use of violence. Political motivations for his criminal actions were attributed a posteriori by the Slovak authorities investigating the case[36]. Equally controversial is the attack mentioned in the report, which took place on 30 May 2024 in Malta. Near the Labour Party office, an 18-year-old criminal detonated TATP (trimeric peroxide acetone) explosives. According to the authorities investigating the case, the perpetrator was insane at the time of the attack. This makes it impossible to classify his act as terrorism[37]. It is difficult to agree with the decision to classify a criminal act as terrorist activity when it is impossible to reconstruct the political agenda or confirm the declared terrorist affiliation of a person suspected of such activity. The inclusion of such terrorist activity in the report should therefore be considered debatable. This is all the more so given that, in the context of arrests of persons suspected of links to terrorism, we are talking about members of organised criminal groups whose activities resemble typical criminal activities (illegal accumulation of weapons

[34] Ibid., p. 53.

[35] J. Zadražilová, *Atentátník se k činu rozhodl hned po prezidentských volbách*, Novinky.cz, 15 V 2024, https://www.novinky.cz/clanek/zahranicni-atentatnik-se-k-cinu-rozhodl-hned-po-prezidentskych-volbach-rekl-ministr-40471949 [accessed: 20 VII 2025].

[36] B. Szandelszky, P.D. Josek, P. Jenne, *Slovak authorities charge 'lone wolf' with assassination attempt on the prime minister*, AP, 16 V 2024, https://apnews.com/article/slovakia-prime-minister-shooting-fico-23faba11c0f371ef0f69a34861337ae0 [accessed: 20 VII 2025].

[37] Europol, *TE-SAT*..., p. 56.

and explosives, sabotage, disinformation activities) or, ultimately, hybrid activities undertaken by third countries hostile to EU Member States.

Use of networks for terrorist activities

A rapidly growing problem is the increasing number of various online platforms used, for example, to recruit minors for terrorist activities or to commit acts of violence. Groups associated with such online activity often advocate the breakdown of democratic structures by introducing chaos or using terror. Many of them represent ideological views associated with jihadist terrorism, the extreme right, the extreme left, but also Satanism and the occult.

In 2024, the number of new services in cyberspace using new technologies, including artificial intelligence, to create and disseminate propaganda or hate speech reached a record high. This applies particularly to far-right terrorism, but also affects, to varying degrees, far-left and anarchist terrorist groups. One example is the anarchist terrorist organisation Partnership of Revenge. Most of its members did not declare any ideological affiliation. They were mainly motivated by financial gain, which indicates a break with the traditional practices used so far by anarchist-motivated terrorists[38].

Throughout 2024, Al-Qaeda and Islamic State propaganda was very active, using, as already mentioned, events in the Gaza Strip, among other things. Several coordinated jihadist propaganda campaigns were aimed at inciting their supporters to carry out attacks. Representatives of other terrorist groups also engaged in such activities[39].

Combating terrorism in the European Union

The European Union is constantly taking measures to prevent and combat terrorism. Examples of such measures include: 'Referral Action Days' – a campaign to quickly report and remove terrorist content from the internet, the creation of task forces dealing with, for example, cryptocurrencies and updating the list of foreign fighters, and the use of mobile laboratories

[38] Ibid., p. 8.

[39] See e.g.: *Steal, deal and repeat: How cybercriminals trade and exploit your data*, Europol, https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data [accessed: 15 VII 2025].

to analyse improvised explosive devices. However, these measures should be considered insufficient. The EU needs a new, comprehensive approach to terrorism. This is important due to the escalation and evolution of this threat, including, among others: mass arms smuggling from the Balkans and Ukraine, the use of modern solutions by terrorists, e.g. drones, 3D-printed weapons, artificial intelligence, cryptocurrencies. It is also necessary to combat terrorist activities in cyberspace and links between terrorists and criminal groups and state secret services. This applies in particular to the policies of Russia and its partners, targeting, among others, Poland, the Czech Republic, Romania, Spain and the Baltic states.

Effective counter-terrorism measures must be implemented not only through enhanced cooperation (in terms of intelligence, logistics, legal and political matters) between all EU Member States, but also through expanded cooperation with NATO and other allies in various parts of the world, e.g. in the Middle East or Africa. The aim is to build multi-faceted resilience both externally and internally. The effective implementation of counter-terrorism plans may be threatened by the particular interests of individual EU Member States, the ongoing political crisis in some of them, discord in transatlantic relations, a lack of financial resources and the increasingly frequent predictions of economic collapse.

Conclusions

1. The changes in terrorism indicated in the TE-SAT 2025 report include, among others, a gradual decrease in the age of terrorists, as well as the use of increasingly newer technological solutions by perpetrators of attacks, such as drones, 3D printing and artificial intelligence.
2. A particularly worrying phenomenon is the increasingly strong links between terrorists and criminal groups and state secret services. This is manifested, among other things, in frequent cases of terrorism and sabotage in EU Member States.
3. Although the number of terrorist attacks fell significantly in 2024, it should be noted that the number of EU Member States affected by attacks increased. The number of people arrested for terrorism and the scale of international links between terrorist structures also increased.

4. Two types of terrorism: jihadist as well as extreme left-wing and anarchist, posed the most serious security challenge in many EU Member States (due, among other things, to the number of incidents). Only the terrorist incidents in Italy had a much broader ideological basis.
5. The European Union needs a new comprehensive approach to terrorism-related threats. This is important due to the intensity and evolution of the threat under analysis. Effective counter-terrorism must be pursued not only through deeper cooperation between EU Member States, but also through broader cooperation with other allies.

Bibliography

Wejkszner A., *Europejska armia kalifatu. Tom 1. Centrum supersieci* (Eng. The European Army of the Caliphate. Volume 1. The Supernetwork Centre), Warszawa 2020.

Wejkszner A., *Europejska armia kalifatu. Tom 2. Peryferie supersieci* (Eng. The European Army of the Caliphate. Volume 2. The Peripheries of the Supernetwork), Warszawa 2023.

Wejkszner A., *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej* (Eng. Lone wolves of the caliphate? The Islamic State and individual jihadist terrorism in Western Europe), Warszawa 2018.

Wojciechowski S., *The hybrid dimension of contemporary terrorism and critical infrastructure. Analysis of Europol's TE-SAT reports from 2021–2024*, "Terrorism – Studies, Analyses, Prevention" 2025, special edition: *Terrorist and sabotage threats to critical infrastructure*. https://doi.org/10.4467/27204383TER.25.020.21523.

Wojciechowski S., Wejkszner A., *The new face of terrorist threat in the European Union. Analysis of the EU Terrorism Situation and Trend Report 2024 (TE-SAT) and other sources*, "Terrorism – Studies, Analyses, Prevention" 2025, no. 7, pp. 307–326. https://doi.org/10.4467/27204383TER.25.035.21812.

Internet sources

Anklage gegen ein mutmaßliches Mitglied der ausländischen terroristischen Vereinigung "Islamischer Staat (IS)" wegen des Messerangriffs in Solingen erhoben,

Der Generalbundesanwalt beim Bundesgerichtshof, 27 II 2025, https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2025/Pressemitteilung-vom-27-02-2025.html [accessed: 20 VII 2025].

Anti-Semitism: Zurich attacker radicalised in Tunisia and online, swissinfo.ch, 25 III 2024, https://www.swissinfo.ch/eng/swiss-politics/zurich-stabber-radicalized-in-tunisia-and-online/74284770 [accessed: 20 VII 2025].

Attack in Tuili during the night: hundreds of photovoltaic panels destroyed, L'Unione Sarda.it, 10 IX 2024, https://www.unionesarda.it/en/sardinia/attack-in-tuili-during-the-night-hundreds-of-photovoltaic-panels-destroyed-nuyrob0o [accessed: 20 VII 2025].

Europol: Afryka jest problemem dla bezpieczeństwa Unii Europejskiej (Eng. Europol: Africa is a problem for the security of the European Union), Onet, 26 VI 2025, https://wiadomosci.onet.pl/swiat/europol-afryka-jest-problemem-dla-bezpieczenstwa-unii-europejskiej/f6pm9xl [accessed: 20 VII 2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2025*, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf [accessed: 20 VII 2025]. https://doi.org/10.2813/5425593.

How crime is accelerated by AI, Europol, https://www.europol.europa.eu/media-press/europol-podcast/episode-21-how-crime-is-accelerated-by-ai [accessed: 21 VII 2025].

Kourdi E., Bertrand N., *Trump pledges retaliation after two US soldiers, one civilian interpreter killed in Syria*, CNN, https://edition.cnn.com/2025/12/13/politics/two-us-army-soldiers-killed-in-syria [accessed: 17 XII 2025].

'Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder, Organized Crime and Corruption Reporting Project, 26 IX 2024, https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder [accessed: 20 VII 2025].

Observatory of Illicit Economies in West Africa, https://riskbulletins.globalinitiative.net/download/wea-obs-012-screen-pdf.pdf [accessed: 10 VII 2025].

Pożary w Polsce. Kolumbijczyk miał działać na zlecenie Rosji. Ustalenia ABW (Eng. Fires in Poland. Colombian man allegedly acting on behalf of Russia. Findings of the ABW), Rzeczpospolita, 29 VII 2025, https://www.rp.pl/przestepczosc/art42769991-pozary-w-polsce-kolumbijczyk-mial-dzialac-na-zlecenie-rosji-ustalenia-abw [accessed: 30 VII 2025].

Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe, https://icct.nl/sites/default/files/2025-09/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool.pdf [accessed: 16 XII 2025].

Steal, deal and repeat: How cybercriminals trade and exploit your data, Europol, https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data [accessed: 15 VII 2025].

Szandelszky B., Josek P.D., Jenne P., *Slovak authorities charge 'lone wolf' with assassination attempt on the prime minister*, AP, 16 V 2024, https://apnews.com/article/slovakia-prime-minister-shooting-fico-23faba11c0f371ef0f69a34861337ae0 [accessed: 20 VII 2025].

Wojciechowski S., *Terrorism – old wine in new bottles*, Defence24, 21 VII 2025, https://defence24.com/geopolitics/terrorism-old-wine-in-new-bottles [accessed: 25 VII 2025].

Wojny dronów: jak to się robi w Afryce [ANALIZA] (Eng. Drone wars: how it's done in Africa [ANALYSIS]), Defence24, 31 V 2025, https://defence24.pl/technologie/wojny-dronow-jak-to-sie-robi-w-afryce-analiza#goog_rewarded [accessed: 18 VII 2025].

Zadražilová J., *Atentátník se k činu rozhodl hned po prezidentských volbách*, Novinky.cz, 15 V 2024, https://www.novinky.cz/clanek/zahranicni-atentatnik-se-k-cinu-rozhodl-hned-po-prezidentskych-volbach-rekl-ministr-40471949 [accessed: 20 VII 2025].

Legal acts

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal of the EU L 88 of 31 March 2017).

Sebastian Wojciechowski, Professor

Head of the Department of Strategic Studies and International Security at the Faculty of Political Science and Journalism of Adam Mickiewicz University in Poznań. Chief analyst at the Institute for Western Affairs in Poznań. Expert on security issues, including

terrorism, of the Organization for Security and Cooperation in Europe. Editor-in chief of "Przegląd Strategiczny".

Recipient of two scholarships from the Foundation for Polish Science and the US State Department. Winner of the scientific award of the Prime Minister of the Republic of Poland and the scientific award funded by the European Union. Member of, among others: the Commission on Balkan Studies of the Polish Academy of Sciences, the Scientific Board of the Terrorism Research Center at Collegium Civitas.

Author of many expert opinions and analyses prepared for Polish and foreign institutions, as well as publications in the field of international relations and internal and international security. He is also NATO DEEP eAcademy security expert.

Contact: sebastian.wojciechowski@amu.edu.pl

Assoc. Prof. Artur Wejkszner, Professor at the Adam Mickiewicz University

Political scientist, professor in the Department of Strategic Studies and International Security at the Faculty of Political Science and Journalism of Adam Mickiewicz University in Poznań. Author of dozens of publications on contemporary international relations and the issues of international terrorism and Islamic radicalism, including a two-volume monograph entitled *Europejska armia kalifatu* (Eng. The European Army of the Caliphate).

Contact: artur.wejkszner@amu.edu.pl

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 411–436

https://doi.org/10.4467/27204383TER.25.059.23046

Article

The role and significance of Eurojust in countering terrorism

DARIUSZ POŻAROSZCZYK
https://orcid.org/0000-0003-0435-0529
Internal Security Agency

Abstract

The text presents the development of the European Union Agency for Criminal Justice Cooperation (Eurojust) and discusses the legal institutions at its disposal for the performance of its tasks. Then, data was cited concerning terrorist cases in which Eurojust had provided assistance. The number of cases in which Eurojust was involved and the related data were compared, on the one hand, with data from previous years and, on the other hand, with data on terrorism contained in Europol's TE-SAT reports (European Union Terrorism Situation and Trend Report). This procedure led to the confirmation of the research hypothesis that Eurojust is an important element of a complex legal and institutional system aimed at combating terrorism, but its role is not sufficiently reflected in its reports. The summary attempts to answer the following questions: 1. Why do Eurojust reports not fully reflect its position in the counter-terrorism system? 2. What is the value of Eurojust reports in the context of recognising the phenomenon of terrorism? 3. What should be done to increase the practical significance and substantive quality of these reports?

Keywords

Eurojust, Eurojust Annual Report, Europol, terrorism, judicial cooperation in criminal cases, cross-border investigations

Introduction

The article presents the Annual Report of the European Union Agency for Criminal Justice Cooperation (Eurojust) and analyses its significance as a source of knowledge about the terrorist threats in the European Union. This aims to verify the hypothesis that, while Eurojust constitutes an important element of a complex legal and institutional system focused on combating terrorism, this role is not sufficiently reflected in the aforementioned report.

The selection of the research topic and the accompanying research hypothesis stems from the fact that Eurojust plays a significant role in coordinating and supporting cross-border criminal proceedings and thus constitutes an important forum enabling the exchange of information on ongoing criminal proceedings[1]. This activity is carried out with the support of numerous institutions and organisational solutions, which are described in the later part of the article. As a result, a large amount of information is collected concerning cross-border criminal proceedings, including cases related to terrorism. The information collected and processed by Eurojust is of significant importance for supporting specific proceedings. Furthermore, the aforementioned data allows for presenting a broader picture of the activities carried out by Eurojust, which could be reflected in the analysed report. However, this does not occur. Answering the question of why this is the case requires identifying which of the pieces of information collected by Eurojust are presented in the report in question and what is the reason for providing the selected data. The article explains how, despite undeniable limitations, Eurojust report allows for better understanding of a complex phenomenon of terrorism, which is interconnected with multiple issues. The article also discusses the tasks of Eurojust, as well as forms, institutions and practices used to carry them out. From a comparative perspective, it presents data on terrorism-related cases in which Eurojust provided assistance. On one hand, the years 2022–2023 served as a reference point, on the other, the data on terrorism and the way it was presented by Europol in the European Union Terrorism Situation and Trend Report[2] (hereinafter: TE-SAT). For this purpose, Eurojust reports from 2022–2024 and Europol reports from 2023–2025 were

[1] *Eurojust Annual Report 2024*, Luxembourg 2025, p. 3. https://doi.org/10.2812/2312311.

[2] This is an annual report prepared by Europol, presenting the situation and trends concerning terrorism in the European Union countries in the previous year.

used, with particular attention paid to the type, source and level of detail of the data contained in both reports. Presenting this data allowed for a comparison of the two reports.

In addition to the comparative method, the text employs document analysis, including reports, informational materials issued by Eurojust and relevant scientific literature.

The conclusion attempts to answer the research questions: 1. Why do Eurojust reports not fully reflect its position in the counter-terrorism system? 2. What is the value of Eurojust reports in the context of recognising the phenomenon of terrorism? 3. What should be done to increase the practical significance and substantive quality of these reports?

The development of Eurojust

The origins of Eurojust are linked to the progress of European integration, initially aimed at strengthening economic cooperation. In the 1970s and 1980s, as integration deepened, the conviction grew that the development of economic cooperation required ensuring broadly understood security. The Maastricht Treaty[3] was signed, on the basis of which the European Union was established, built on three pillars[4]. The third pillar created at that time was called 'Cooperation in the fields of justice and home affairs'[5]. Its creation was intended to deepen cooperation among EU Member States in the area of crime-related issues. The detailed substantive scope

[3] Treaty on the European Union signed in Maastricht on 7 February 1992.

[4] On this matter Krystian Bartosz wrote: 'Until the Maastricht Treaty came into force, Community law primarily covered provisions concerning the economy. It recognised cooperation in criminal matters solely as a sovereign element of a Member State's internal policy. The Maastricht Treaty, established in 1991, was in a way a response to the growing problem of international crime, as well as the increasing strength of terrorist organisations that could pose a real threat to Europe's security'. See in more detail: K. Bartosz, *Prawne aspekty walki z terroryzmem* (Eng. Legal aspects of fighting terrorism), "Security, Economy & Law" 2018, no. 1, p. 20. https://doi.org/10.24356/SEL/18/1.

[5] The beginnings of the third pillar can be traced back to the establishment of an internal security group created by the European Council in Rome in 1975, known as TREVI (French: Terrorisme, Radicalisme, Extrémisme, Violence Internationale). Already in 1976, within TREVI, two subgroups emerged: TREVI I and TREVI II. The tasks of TREVI I, whose establishment was linked to the increased activity of terrorist organisations as the IRA, the Black September and the RAF, were to streamline the flow of information about terrorist organisations and to jointly analyse the threats they generated.

of the third pillar was defined by Article K.1, included in Title VI of the then Treaty on European Union, which specified matters considered to be of 'common interest', namely:

1) asylum policy,
2) rules governing the crossing by persons of the external borders of the Member States and the exercise of controls thereon,
3) immigration policy and policy regarding nationals of third countries,
4) combatting drug addiction,
5) combatting fraud on an international scale,
6) judicial cooperation in civil matters,
7) judicial cooperation in criminal matters,
8) customs cooperation,
9) police cooperation for the purposes of preventing and combatting terrorism, unlawful drug trafficking and other serious forms of international crime, including if necessary certain aspects of customs cooperation, in connection with the organisation of a Union-wide system for exchanging information within a European Police Office (Europol).

An analysis of Article K.1 indicates that the primary motivation for cooperation in the fields of justice and home affairs was to ensure the free movement of persons. A detailed interpretation of the specified 'matters of common interests' shows that the greatest threats to be addressed within the third pillar were considered to be illegal immigration, organised crime and terrorism[6].

In the following years, European integration gained momentum. Based on the Treaty of Amsterdam[7], the name of the third pillar was changed to 'Police and Judicial Cooperation in Criminal Matters', and cooperation in the field of security was strengthened, including by transferring some issues from the third pillar to the Community-based first pillar.

[6] These phenomena, as well as cybercrime and human trafficking as major threats arising from globalisation, are also highlighted by Marek Fałdowski. See: M. Fałdowski, *Międzynarodowa Organizacja Policji Kryminalnych – Interpol w zwalczaniu wybranych zagrożeń XXI w.* (Eng. International Organisation of Criminal Police – Interpol in fighting selected threats of the 21st century), "Wiedza Obronna" 2023, vol. 282, no. 1, p. 198. https://doi.org/10.34752/2023-i282.

[7] *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts.*

Another significant stage of development was a special meeting of the European Council, which took place on 15–16 October 1999, in the Finnish city of Tampere. The meeting was dedicated to creating an area of freedom, security and justice within the EU. Plans were discussed to establish a judicial body aimed at strengthening cooperation among national authorities in combating serious cross-border organised crime[8]. In March 2001, in Brussels, based on Council Decision 2000/799/JHA of 14 December 2000, the Provisional Judicial Cooperation Unit began its operations, also known as Pro-Eurojust. The terrorist attacks in the US on 11 September 2001, were another factor implying the need to strengthen international cooperation, which resulted in an acceleration of efforts to establish Eurojust[9]. This body was officially established by Council Decision 2002/187/JHA of 28 February 2002[10] as the European Judicial Cooperation Unit. The objectives of Eurojust were defined in Art. 3 of the aforementioned decision. They included stimulating and improving coordination and cooperation between national investigative and law enforcement authorities, as well as supporting, in other ways, the competent authorities of the Member States to streamline the investigation and prosecution of serious crime, particularly organised crime, involving two or more Member States. At this point, it should be noted that the limitation of Eurojust's competencies at that time, which has remained in place to this day, to actions concerning crimes involving more than one EU Member State, significantly affects the scope of data collected by this body. Unlike the data collected by Europol and presented in TE-SAT reports, Eurojust reports provide only information on cases related to transnational terrorism in which Eurojust was involved in prosecution[11].

[8] *Eurojust: European Union Agency for Criminal Justice Cooperation*, The Hague 2020, p. 2. https://doi.org/10.2812/556790. In point 46 of the conclusions from the European Council meeting in Tampere, it was stated: 'To reinforce the fight against serious organised crime, the European Council has agreed that a unit (Eurojust) should be set up composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to its legal system. Eurojust should have the task of facilitating the proper coordination of national prosecuting authorities and of supporting criminal investigations in organised crime cases, notably based on Europol's analysis, as well as of co-operating closely with the European Judicial Network (...)'.

[9] *Eurojust: European Union Agency for Criminal...*, p. 2.

[10] *Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime.*

[11] This issue will be discussed in greater detail in the following sections of the article.

In the following years, both the functioning of Eurojust and its normative foundations and political assumptions underwent further changes. On 16 December 2008, the EU Council adopted Decision 2009/426/JHA amending Decision 2002/187/JHA[12], which led to the strengthening of Eurojust's coordinating role. The reform carried out at that time envisaged the creation of the Eurojust National Coordination System (ENCS) whose tasks were to streamline the flow of information between Eurojust and the Member States, as well as to improve case management, including by assisting in determining whether a case should be referred to Eurojust or the European Judicial Network, and identifying the competent authorities responsible for implementing requests and decisions related to international cooperation in criminal matters. The ENCS operates in every EU Member State. It is managed by national Eurojust correspondents and relies on contact points that function under separate regulations[13].

Following the signing of the Treaty of Lisbon[14], the current normative foundations of Eurojust in primary law are set out in Art. 85 of the Treaty on the Functioning of the European Union, according to which: *Eurojust's mission shall be to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime* ***affecting two or more Member States***[15] *or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by Europol*. The most important tasks of Eurojust, described in Art. 85 of the TFEU, include:

a) initiation of criminal investigations, as well as proposing the initiation of prosecutions conducted by competent national authorities, particularly those relating to offences against the financial interests of the Union,
b) coordination of investigations and prosecutions referred to in point (a),

[12] *Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*.

[13] G. Stronikowska, *Prokuratura Europejska jako instytucja ochrony interesów finansowych Unii Europejskiej* (Eng. The European Public Prosecutor's Office as an institution protecting the financial interests of the European Union), Warszawa 2020, p. 231.

[14] *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*.

[15] The emphasis is by the author (editor's note).

c) strengthening of judicial cooperation, including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network.

The evolution of Eurojust resulted in two legal acts. The first is Regulation (EU) 2018/1727[16] adopted on 14 November 2018, implementing the provisions of the Lisbon Treaty[17], which, as of 12 December 2019, replaced Decision 2002/187/JHA. On this basis, the European Union Agency for Criminal Justice Cooperation became the legal successor of Eurojust, established under Council Decision 2002/187/JHA[18]. Grażyna Stronikowska notes that: *The purpose of Regulation (EU) 2018/1727 is to align Eurojust with the requirements of Art. 85 TFEU by introducing a mechanism for evaluating its activities by the European Parliament and national parliaments, replacing the decision with a regulation, and adapting the agency for cooperation with the newly established EP*[19]. Stronikowska emphasises that Regulation (EU) 2018/1727 did not introduce radical changes regarding the functioning of Eurojust and the tasks it performs, it rather played an organisational and clarifying role[20]. It should be noted that, due to the abandonment of the formal linkage of Eurojust's subject-matter competence with the subject-matter jurisdiction of Europol, Eurojust's competence was defined by reference to the types of serious crime listed in the annex to Regulation (EU) 2018/1727[21].

[16] See: G. Stronikowska, *Prokuratura Europejska jako instytucja…*, p. 250.

[17] *Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA*.

[18] Stronikowska notes that the succession established under Regulation (EU) 2018/1727 also covers all agreements and other obligations undertaken by Eurojust under Council Decision 2002/187/JHA. See: G. Stronikowska, *Prokuratura Europejska jako Instytucja…*, p. 251.

[19] European Public Prosecutor's Office (EPPO) is an independent body operating on the basis of *Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation (Articles 20 TEU and 329 TFEU) on the establishment of the European Public Prosecutor's Office*. The material and functional competence of the European Public Prosecutor's Office includes conducting preparatory proceedings and bringing or supporting indictments against perpetrators of crimes affecting the financial interests of the European Union.

[20] G. Stronikowska, *Prokuratura Europejska jako instytucja…*, p. 251.

[21] Among the forms of serious crime for which Eurojust has competence to take action, the mentioned annex lists terrorism.

The second act is Regulation (EU) 2023/2131 of 4 October 2023[22], concerning the digital information exchange, which aims to streamline the operation of Eurojust's Counter-Terrorism Register (hereinafter: CTR)[23] established in 2019. This database is used to collect information on judicial proceedings related to terrorism. It contains, inter alia, data on the identity of persons suspected of terrorism-related offences and their links to terrorist networks, as well as other detailed information concerning ongoing proceedings. Due to the sensitive nature of the collected information, there is no public access to the CTR, which means that these data are not presented or discussed in the annual Eurojust reports.

Forms of operation and cooperation of Eurojust

An analysis of regulations governing the functioning of Eurojust, including the changes that have occurred over the years, leads to the conclusion that it has been steadily gaining a stronger institutional position within the EU legal system[24], and that the scope of its powers has been expanding. Nevertheless, it is still not an autonomous body conducting independent preparatory proceedings, but rather a supporting body. The four most important forms of support provided by Eurojust in connection with preparatory proceedings conducted by the competent authorities of the Member States and the EPPO are[25]:

[22] *Regulation (EU) 2023/2131 of the European Parliament and of the Council of 4 October 2023 amending Regulation (EU) 2018/1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA, as regards digital information exchange in terrorism cases.*

[23] CTR is a special database established by Eurojust to strengthen the response – particularly through the processing of relevant information – to terrorist threats in the EU Member States. The legal basis for CTR is *Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences*. However, CTR was launched only on 1 IX 2019, in response to the terrorist attacks of 13 X 2015 in Paris. See in more detail: *Launch of Judicial Counter-Terrorism Register at Eurojust*, Eurojust, 5 IX 2019, https://www.eurojust.europa.eu/news/launch-judicial-counter-terrorism-register-eurojust [accessed: 9 VIII 2025].

[24] Eurojust currently operates on the basis of a regulation rather than a decision.

[25] *Eurojust: European Union Agency for Criminal…*, pp. 6–7.

– support for joint investigation teams[26],
– assistance in the use of EU judicial cooperation instruments, in particular the European Arrest Warrant[27] and the European Investigation Order[28],
– support in organising coordination meetings[29],
– serving as coordination centres[30].

When discussing the competencies and capabilities of Eurojust regarding information collection, it should be noted that increasing globalisation translates into a systematic rise in human mobility. This results, among other things, in criminals increasingly crossing both internal

[26] Joint Investigation Teams (JIT) are established on the basis of an agreement between law enforcement and judicial authorities of two or more states – most often EU Member States – for the purpose of conducting a joint criminal investigation. Their aim is to coordinate activities and enable the direct exchange of information and evidence. The legal basis for establishing the JIT is *Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams*. The details of JIT operations involving Polish authorities have been specified in the Code of Criminal Procedure, Articles 589b – 589f. See in more detail: K. Leśniewski, *Słów kilka o instytucji wspólnych zespołów śledczych w pryzmacie polskiej procedury karnej* (Eng. A few words about joint investigation teams from the perspective of Polish criminal procedure), "Przegląd Prawno-Ekonomiczny" 2019, no. 2(47), pp. 177–186.

[27] European Arrest Warrant is a simplified form of extradition existing between EU Member States, established under *2002/584/JHA*: *Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States*. This issue is regulated in Chapters 65a and 65b of the Code of Criminal Procedure.

[28] European Investigation Order (EIO) is based on a ruling issued by the competent judicial or law enforcement authority of an EU Member State. The aim of EIO is to carry out specified procedural actions in another EU country aimed at obtaining evidence. The legal basis for the operation of EIO is *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters*. This issue is regulated in Chapters 62c and 62d of the Code of Criminal Procedure.

[29] Coordination meetings are a form of cooperation that enables contact between judicial and law enforcement authorities from EU Member States and, in some cases, from third countries. During these meetings, participants have the opportunity to exchange information, discuss, and resolve legal issues typical of cross-border cooperation, most often concerning jurisdictional conflicts and matters related to the assumption or transfer of ongoing criminal proceedings. Coordination meetings also provide an opportunity to develop plans for the further conduct of criminal proceedings, including discussing the potential need to establish JIT. See in more detail: *Eurojust: European Union Agency for Criminal…*, p. 7.

[30] Eurojust coordination centres constitute a special form of cooperation, organised to manage in real time coordinated operations targeting organised crime groups or terrorist networks. See in more detail: *Eurojust: European Union Agency for Criminal…*, p. 7.

and external borders of Member States. Consequently, there is an increasing need to support the fight against serious cross-border crime extending beyond the EU, which in Eurojust's practice is reflected in a steady rise in the number of supported proceedings initiated in non-EU countries[31]. This trend makes it necessary to develop, including the institutionalisation of cooperation with countries outside of the united Europe. This particularly concerns the fight against complex crimes in the areas of illegal migration, smuggling and counter-terrorism. In March 2024, Eurojust adopted the *Strategy on cooperation with international partners 2024–2027*, outlining actions aimed at strengthening its role in cooperation with law enforcement authorities both within the EU and beyond its borders.

In the context of Eurojust's cooperation with third countries, it should be noted that it currently has contact points in over 70 countries and in three international organisations. Furthermore, this network is continually being expanded – in 2024, a contact point was established in the United Arab Emirates, and the activities of similar points were resumed in Nigeria and Mongolia[32]. Twelve third countries have delegated their liaison prosecutors (LPs) to Eurojust – these are: Albania, Georgia, Iceland, Moldova, Montenegro, North Macedonia, Norway, Serbia, Switzerland, Ukraine, the United Kingdom and the United States. Eurojust has signed agreements with the above-mentioned countries and additionally with Liechtenstein, which enable cooperation in the exchange of information including evidentiary materials and personal data. Eurojust has concluded working agreements with nine additional countries: Nigeria, Panama, Costa Rica, Bolivia, Chile, Ecuador, Peru, Egypt and South Korea, enabling strategic cooperation in the exchange of information, including sharing

[31] Ibid., p. 10.

[32] *Eurojust Annual Report…*, p. 14. It is worth noting that Nigeria has been grappling for years with Islamic terrorism, primarily propagated by the Boko Haram organisation. See in more detail: A. Wejkszner, *Boko Haram – the evolution of jihad activity in Nigeria 2015–2019,* "Przegląd Strategiczny" 2020, no. 13, p. 349. https://doi.org/10.14746/ps.2020.1.21. It should also be added that, according to the annual *Global Terrorism Index* (GTI) report prepared by the Institute for Economics and Peace (IEP), Nigeria moved from 8th to 6th place in 2025 among the countries most affected by terrorism. At the same time, the country is an important economic partner of the EU, and its increasing destabilisation threatens to undermine the situation across the Sahel region, which could result in a sharp rise in unwanted immigration to the EU. Therefore, developing all forms of cooperation with this country aimed at identifying and combating terrorism should be considered highly beneficial.

best practices, but without sharing operational information. Eurojust also signed a working agreement with the Ibero-American Association of Public Prosecutors Offices (AIAMP)[33].

Eurojust is also involved in many additional activities or initiatives that enable, or at least create, conditions for the exchange of information relevant to combating international crime. In October 2024, its representatives participated in the first Summit of the Heads of Prosecution Services of G20 Members, hosted by the Federal Prosecutor's Office of Brazil. Participation in this event was used to organise bilateral meetings with representatives of Argentina, Australia, Brazil, Chile, Egypt, India, Nigeria, Saudi Arabia, South Africa, the United Arab Emirates and the United Kingdom, which may lead to the development of future cooperation with these countries[34]. It should be emphasised that good cooperation with some of the above-mentioned countries, such as Nigeria[35], Saudi Arabia[36] and the United Kingdom[37], may be particularly important in preventing and combating terrorism. Similar positive effects may result from the co-organisation by Eurojust of study visits for representatives of the general prosecutor's offices of Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan[38], as well as from the participation of Eurojust representatives in workshops organised in Baghdad that were devoted to issues of cooperation between judicial authorities.

[33] *Eurojust Annual Report*..., p. 15.

[34] Ibid., p. 13.

[35] See: footnote 32.

[36] It is worth paying attention to analyses concerning the involvement of the Wahhabi movement – supported and playing a major role in the Saudi state – in the development of Islamic terrorism, as contained in the thesis of Michał Harkot. See: M. Harkot, *Wpływ wahabizmu na pozycję społeczno-polityczną Arabii Saudyjskiej* (Eng. Impact of Wahhabism on the socio-political position of Saudi Arabia), "Annales Universitatis Mariae Curie-Skłodowska Lublin – Polonia" 2020, no. 1, vol. 27, pp. 97–110. https://doi.org/10.17951/k.2020.27.1.97-110.

[37] The importance of cooperation with the United Kingdom in combating terrorism stems from the fact that the country has repeatedly faced terrorism motivated by various factors, which has translated into extensive experience on the part of British services in countering this threat.

[38] The significant involvement of Central Asian residents in jihadist terrorism is indicated, for example, by Krzysztof Strachota. See: K. Strachota, *Islamic State-Khorasan: global jihad's new front*, Ośrodek Studiow Wschodnich, 29 III 2024, https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-03-29/islamic-state-khorasan-global-jihads-new-front [accessed: 15 VIII 2025].

In addition to organising one-off meetings with certain countries, more permanent forms of cooperation are also being developed. An example is the EuroMed Justice Project, whose aim is to strengthen cross-border cooperation in criminal matters between EU countries and states such as: Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine and Tunisia. As part of the indicated programme, among other things, 18 working meetings were organised[39]. It is also worth mentioning the Western Balkans Criminal Justice Project, under which Eurojust has been strengthening cooperation with Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, Montenegro and Serbia and has so far supported 25 cross-border proceedings, including those concerning money laundering and arms trafficking. Among the specific forms of support, it is worth noting, inter alia, assistance in the establishment of three new joint investigation teams and two so-called action days[40].

In addition to cooperation with foreign states or entities, Eurojust also cooperates with the law enforcement authorities of the Member States as well as with other EU agencies established to combat crime, i.e. Europol, the European Public Prosecutor's Office and the European Anti-Fraud Office[41].

Figures concerning Eurojust's activities

The steadily expanding network of entities with which Eurojust cooperates to prevent and combat crime translates into a systematic year-on-year increase in the number of cases in which it provides assistance. In 2019, there were approx. 8000 such cases. By 2024, this number had reached nearly 13 000, representing an increase of almost 60%[42]. These were cases

[39] *Eurojust Annual Report…*, p. 16.

[40] Action days are days on which complex procedural operations are carried out simultaneously in multiple countries, the coordination and real-time management of which may be supported by Eurojust coordination centres.

[41] The European Anti-Fraud Office, known as OLAF (French: L'Office europeen de lutte antifraude), was established on the basis of *Commission Decision of 28 April 1999 establishing the European Anti-fraud Office (OLAF).*

[42] *Eurojust Annual Report…*, p. 7. At the same time, it should be noted that the number of criminal proceedings in which Eurojust does not provide assistance is many times higher – in 2024 in Poland alone, the Police conducted 440 269 preparatory proceedings. See: *Zwalczanie przestępczości kryminalnej* (Eng. Combating criminal offences),

covering 14 categories of serious cross-border crime, including drug-related crime, money laundering, financial crimes/fraud, facilitating illegal migration and intellectual property theft[43]. The first three categories accounted for the majority of the crime combated by Eurojust. In 2024, it was involved in over 4000 proceedings concerning financial fraud and approx. 2000 cases related to drug trafficking and money laundering. Altogether, these three categories accounted for more than two-thirds of the cases in which Eurojust provided assistance[44].

With regard to the above data, it should be noted that although many terrorist organisations operate simultaneously in multiple countries, and the use of modern technologies facilitates the easy dissemination of content promoting and enabling terrorism[45], the number of terrorism-related proceedings in which Eurojust was involved in 2024 is significantly lower than those concerning the aforementioned types of crime with a typical criminal and economic character. This situation appears to result from at least two reasons. Firstly, the overall number of terrorist offences is considerably smaller than the number of typical criminal offences. Secondly, despite global spread of propaganda calling for violence and glorifying acts of terror, a significant portion of terrorist offences is committed by individuals acting alone, who have no real connections with organisations such as ISIS or Al-Qaeda, and are at most influenced by materials produced by them[46]. Only the virtual contact of perpetrators of many terrorist offences with these organisations and their members –

Informacyjny Serwis Policyjny, 9 I 2025, https://isp.policja.pl/isp/aktualnosci/18325, Zwalczanie-przestepczosci-kryminalnej.html [accessed: 2 XI 2025].

[43] *Eurojust Annual Report…*, p. 19.

[44] Ibid.

[45] It is worth emphasising that in many countries, the mere dissemination of content promoting terrorism already constitutes a criminal offence. For instance, in Poland, this is penalised under Art. 255a of the Criminal Code, in Germany – in Art. 86 StGB (Strafgesetzbuch – the German Criminal Code), and in Austria in Art. 282a öStGB (Österreichische Strafgesetzbuch – the Austrian Criminal Code).

[46] Andrzej Czop proposes to refer to such individuals as 'solo terrorists'. Meanwhile, he defines a 'lone wolf' as 'a perpetrator who carries out acts of terror alone, completely isolated and devoid of any direct or indirect connections with terrorist groups, and lacking any form of command structure'. See in more detail: A. Czop, *Nowe trendy terroryzmu i możliwości podniesienia efektywności jego zwalczania* (Eng. New trends in terrorism and ways to increase the effectiveness of combating them), "Studia de Securitate" 2023, no. 13(2), p. 161. https://doi.org/10.24917/26578549.13.2.9.

who are most often located in countries (or areas) that do not provide international legal assistance – makes seeking support offered by Eurojust irrelevant. It also sometimes happens that even if international assistance in criminal matters is theoretically justified and possible, the proceedings are so straightforward that there is no need to involve Eurojust. An example of such investigations are those in which only a few evidentiary actions need to be carried out abroad[47]. There is also a group of terrorist offences of a strictly local nature – their effects are limited to a single country and, importantly, they are committed by groups whose area of activity is also narrowly defined. This category includes Corsican groups that were particularly active in 2023.

In 2024, with regard to criminal proceedings related to terrorism cases, Eurojust provided support in 191 cases (63 new cases and 128 ongoing cases). In connection with these cases, 10 joint investigation teams were active (including two new ones established in 2024). Thirty two coordination meetings and one coordination centre were organised[48]. Eurojust also provided support in the application of the European investigation order for mutual legal assistance requests and assisted in the execution of European arrest warrants. It continuously collected information in the CTR from national authorities regarding ongoing and completed criminal proceedings related to terrorism, thereby expanding its existing database on crime, particularly concerning individuals involved in it[49].

The majority of cases referred to Eurojust were initiated by Italy, France, Spain and Germany. The largest number of requests for assistance in terrorism-related cases, however, was sent via Eurojust to the Netherlands and France. Among non-EU countries, the United Kingdom and Norway most frequently submitted cases to Eurojust. Meanwhile, the highest number of assistance requests was directed to Ukraine and the United Kingdom[50].

Based on the data presented, it can be observed that participation in international forms of cooperation in criminal matters is related to the level of terrorist threat in a given country. States in which many terrorist

[47] Kamil Leśniewski emphasises the need to analyse each time whether it is necessary to establish a joint investigation team. See in more detail: K. Leśniewski, *Słów kilka o instytucji…*, p. 181.

[48] *Eurojust Annual Report…*, p. 20.

[49] Ibid.

[50] Ibid.

offences occur, and consequently have a higher number of individuals involved in these offences who may benefit from EU freedom of movement, are more likely to be compelled to conduct cross-border proceedings, for which they seek assistance from Eurojust. The report does not provide specific data or more detailed information on the cases mentioned, limiting itself to a rather brief reference to the number and nature of individual acts. In this latter regard, it is generally indicated that the cases supported by Eurojust concerned terrorist offences inspired by various ideologies and included criminal acts such as: the preparation of terrorist attacks, participation in terrorist organisations, financing of terrorism, recruitment into terrorist organisations and incitement to commit terrorist offences. In the report under discussion (also without providing specific data), it was stated that in some cases the proceedings concerning terrorist offences also included acts of a typically criminal nature: killings/murders, deprivation of liberty (including hostage taking), the illegal trafficking of weapons, explosives and ammunition[51].

For comparison, in 2023 Eurojust was involved in 205 cases related to terrorism (70 new and 135 carried over from previous years). In connection with these cases, it supported 9 joint investigation teams (3 new and 6 initiated in previous years) and organised 22 coordination meetings. The 2023 report, unlike the 2024 report, does not include additional details, such as specifying the countries that initiated the largest number of cases or those to which requests for assistance were most frequently directed[52].

In 2022, Eurojust provided assistance in 203 cases (53 new and 150 initiated in previous years). In 2022, it was involved in supporting 8 joint investigation teams, of which 3 were initiated in 2022. During the period under review, 21 coordination meetings were organised[53].

Data from Europol's TE-SAT reports

According to Europol reports, compiled based on qualitative and quantitative data provided by Member States concerning terrorist attacks, arrests, convictions and penalties for terrorist offences, in 2024 there were

[51] Ibid.

[52] *Eurojust Annual Report 2023*, Luxembourg 2024, p. 27. https://doi.org/10.2812/356222.

[53] *Eurojust Annual Report 2022*, Luxembourg 2023, p. 52. https://doi.org/10.2812/022275.

58 terrorist attacks recorded (34 carried out, 5 unsuccessful and 19 foiled) in 14 Member States[54]. Among them, 24 were related to jihadist terrorism[55], indicating an increase in this type of attacks, 21 attacks were motivated by anarchism and left-wing ideology[56], 4 were ethnonationalist/separatist in nature[57], 1 was driven by right-wing ideology[58], and 8 were classified as not linked to any specific ideology. The deadliest form of terrorism was that motivated by jihadist ideology, which resulted in 5 deaths and 18 injuries. In 20 Member States, 449 individuals were arrested for offences related to terrorism. The majority of arrests concerned jihadist terrorism (289), followed by right-wing terrorism (47), left-wing and anarchist terrorism (28) as well as ethnonationalist and separatist terrorism (27). For terrorist offences related to other or unspecified forms of terrorism, 8 individuals were arrested[59]. The highest number of arrests took place in Spain (90), France (69), Italy (62) and Germany (55)[60].

In 2023, as many as 120 terrorist attacks were recorded in the EU, including 98 carried out, 9 unsuccessful and 13 foiled. The majority

[54] *European Union terrorism situation and trend report 2025,* Luxembourg 2025, p. 13. https://doi.org/10.2813/5425593.

[55] TE-SAT defines jihadism as a violent sub-set of Salafism, a revivalist Sunni Muslim movement that rejects democracy and elected parliaments, arguing that human legislation is at odds with God's status as the sole lawgiver. See in more detail: *European Union terrorism situation and trend report 2025*..., p. 23.

[56] According to Europol, left-wing terrorist groups seek to provoke a violent revolution against the political, social and economic system of the state in order to establish socialism and, ultimately, a communist and classless society. Their ideology is often Marxist-Leninist. Anarchist terrorism is a term used to describe acts of violence carried out by groups or individuals promoting the absence of authority as a social model. Anarchists pursue a revolutionary, anti-capitalist and anti-authoritarian agenda. See in more detail: *European Union terrorism situation and trend report 2025*..., p. 34.

[57] According to TE-SAT, ethnonationalist and separatist terrorist groups are motivated by nationalism, ethnic identity, and/or religion. Separatist groups seek to carve out a state for themselves from a larger country or to annex the territory of one country to another. See in more detail: *European Union terrorism situation and trend report 2025*..., p. 49.

[58] According TE-SAT, right-wing terrorism is associated with aggressive right-wing actors (groups or individuals) who seek to use violence to transform the entire political, social, and economic system into an authoritarian model, rejecting the democratic order, values, and fundamental rights. Aggressive right-wing ideologies employ narratives centred on exclusionary nationalism, racism, xenophobia and/or intolerance. See in more detail: *European Union terrorism situation and trend report 2025*..., p. 42.

[59] Ibid., p. 8.

[60] Ibid., p. 14.

of attacks were motivated by ethnonationalist and separatist ideologies (70)[61], with fewer driven by anarchist and left-wing views (32). During the period in question, there were 14 jihadist attacks and 2 attacks linked to far-right ideology. 426 people were arrested on charges related to terrorism. The highest number of arrests was recorded in Spain (84), France (78) and Belgium (75)[62]. In fourth place, but with significantly fewer arrests, was Germany (51). With regard to the type of terrorism in 2023, most arrests (334) were related to jihadist terrorism, 26 people were arrested for right-wing terrorism, and 14 for left-wing and anarchist terrorism. Terrorist activity related to separatist and ethno-nationalist terrorism resulted in 25 arrests, of which 18 arrests in terrorist cases were linked to other forms of terrorism and 9 were classified as unspecified[63].

In 2022, there were 28 attacks recorded, 16 of which were considered successful. This year, most attacks were left-wing and anarchist (18, including 13 successful ones), 6 attacks were jihadist (including 2 successful ones) and 4 were right-wing (1 successful and 3 unsuccessful). A total of 380 people were arrested. Of this number, 266 arrests were for jihadist crimes, with the highest number of arrests made in France (93),

[61] All attacks of this nature took place in Corsica, as many as 34 of them were carried out on the night of 8–9 October 2022 and are assessed as a reaction to the visit of French President Emmanuel Macron to the island. The attacks involved the detonation of small explosive devices placed in holiday homes and at construction sites. They did not cause serious damage or casualties. See in more detail: *France's Corsica rocked by blasts claimed by separatist group*, RFI, 9 X 2023, https://www.rfi.fr/en/france/20231009-france-s-corsica-rocked-by-blasts-claimed-by-separatist-group [accessed: 10 VIII 2025].

[62] It is worth noting that the Belgian capital has a district called Molenbeek, inhabited by a very large number of Muslims. Many of them have become radicalised and left for Syria and Iraq to support ISIS. Available data for the years 2011–2017 indicate that as many as 47 people living in Molenbeek left for areas controlled by the so-called Islamic State. See: *Molenbeek. Fabryka terrorystów w stolicy Europy* (Eng. Molenbeek. A terrorist factory in the capital of Europe), Magazyn TVN24, https://archiwum.tvn24.pl/magazyn-tvn24/14/tvn24.pl/magazyn-tvn24/molenbeek-przystan-dzihadystow-w-sercu-europy%2c14%2c296.html [accessed: 10 VIII 2025]. The article also points out that it was among Belgian citizens that ISIS recruited the most foreign fighters. Similar information confirming that Belgium had the highest *per capita* rate of departures to ISIS in Europe in the second decade of the 21st century is cited by Matthew Levitt. See: M. Levitt, *My Journey Through Brussels' Terrorist Safe Haven,* The Washington Institute for Near East Policy, https://www.washingtoninstitute.org/policy-analysis/my-journey-through-brussels-terrorist-safe-haven [accessed: 10 VIII 2025].

[63] *European Union terrorism situation and trend report 2024*, Luxembourg 2024, pp. 11–13. https://doi.org/10.2813/4435152.

Spain (46), Germany (30), Belgium (22), Italy (21) and the Netherlands (21). The number of arrests for right-wing terrorism was 45. There were also 18 arrests for ethno-nationalist and separatist terrorism and 19 for left-wing and anarchist terrorism. Twenty-six people were arrested for other types of terrorism. In the case of 6 arrests, the type of terrorism with which they could be linked was not specified[64].

In addition to the information indicated, Europol reports on terrorist offences contain a wealth of other data (although the scope of their presentation may vary depending on the edition), such as the country where the crime was committed, sometimes the number of victims broken down into those killed and injured, and some details about the perpetrators, such as their age, gender and nationality. TE-SAT reports also provide data on the modus operandi of the perpetrators, including information on the tools used, indicating whether the attack was carried out with a knife, an improvised explosive device, a drone, a firearm, etc. In some cases, the communication channels and technologies used are described. Europol data also provides information on judgments handed down in cases related to terrorism. Their important and cognitively valuable elements include the presentation of a larger number (than in the case of Eurojust reports) of actual cases and an in-depth analysis of trends in terrorist crime. While maintaining a distinction between types of terrorism, information is presented on the communities associated with them, the structures of individual groups or organisations, recruitment methods, including among persons deprived of liberty, the characteristics of the propaganda used, with an emphasis on social and political events that are used to recruit new supporters and methods of financing. TE-SAT also identifies and analyses events that may have a particular impact on the level of terrorist crime. For example, the 2023 report on 2022 discussed, among other things, the possible impact of the war in Ukraine on terrorism[65]. In TE-SAT 2024[66] attention was focused, among other things, on the conflict in Gaza in the context of its impact on the rise of radicalisation leading to terrorism. TE-SAT 2025 again addressed the implications of Israeli actions in the Gaza Strip and the effects of the weakening of the Syrian regime

[64] *European Union terrorism situation and trend report 2023*, Luxembourg 2023, p. 10. https://doi.org/10.2813/302117.

[65] Ibid., p. 17.

[66] *European Union terrorism situation and trend report 2024*, p. 7.

on the situation in the region[67]. The development of modern technologies in the context of facilitating terrorist activities was also mentioned, including the increasingly serious threat posed by the development of 3D printing, which makes it increasingly easy to obtain firearms[68].

Comparison of Eurojust and Europol reports

The information presented shows that the data contained in TE-SAT is much more detailed and thus provides a more complete picture of terrorism in the EU[69]. This is undoubtedly a result of the fact that the aim of Europol reports is to provide an accurate description of the terrorist threat situation in EU countries. The wide range of information used and issues addressed implies the comprehensiveness of the documents in question – for example, TE-SAT 2025 is 75 pages long. By comparison, terrorism issues are covered in 2 pages in the latest Eurojust report.

Table 1 presents some of the differences between the annual reports of Eurojust and Europol's TE-SAT.

Table 1. Differences between the annual reports of Eurojust and Europol's TE-SAT.

Criterion	Eurojust's reports	Europol's TE-SAT reports
Aim	Presentation of cooperation and coordination activities related to combating cross-border crime. Presentation of Eurojust's activities in this area and their effects	Monitoring terrorist threats, their scale and development trends in order to provide decision-makers and those involved in combating terrorism with a precise and detailed picture of this threat

[67] The report was written before Bashar al-Assad's government fell in December 2024.

[68] *European Union terrorism situation and trend report 2025*, pp. 9–12.

[69] Sebastian Wojciechowski and Artur Wejkszner also point out that TE-SAT takes the broader context into account. See: S. Wojciechowski, A. Wejkszner, *The new face of terrorist threat in the European Union. Analysis of the EU Terrorism Situation and Trend Report 2024 (TE-SAT) and other sources*, "Terrorism – Studies, Analyses, Prevention" 2025, no. 7, p. 310. https://doi.org/10.4467/27204383TER.25.035.21812.

Criterion	Eurojust's reports	Europol's TE-SAT reports
Subject area	Eurojust's tasks, detailed forms of their implementation in the field of combating the most serious cross-border crime and their results	The phenomenon of terrorism in the European Union. Its scale, manifestations, evolutionary trends and etiological factors
Level of detail	General data on various forms of serious crime (financial crime, drug-related crime, money laundering, human trafficking, cross-border crime, cybercrime, terrorist offences). Data on the main forms of support provided by Eurojust in relation to specific types of crime. Figures broken down by specific types of crime, indicating the countries that most frequently requested assistance from Eurojust and vice versa	Detailed and in-depth data, supplemented with additional analyses concerning terrorist offences. Descriptions and analyses of selected terrorist offences. Discussion of specific phenomena contributing to an increased terrorist threat (e.g. Israel's attack on the Gaza Strip, aggression by the Russian Federation against Ukraine) and changes in the way terrorist crimes are committed (e.g. the development of 3D printing as a factor influencing the ease of access to firearms)
Data type	Information on cases involving cross-border crime in which Eurojust was involved in the investigation. Information on the tools/forms of support (joint investigation teams, assistance in using EAW and EIO, assistance in organising meetings and coordination centres) provided by Eurojust. Information on other forms of cooperation between Eurojust and its international partners (third countries, international organisations)	Very detailed data on terrorist acts – number of attacks, nature (broken down into jihadist, right-wing, left-wing, ethno-nationalist and separatist terrorism, and other), outcome (attacks successful, unsuccessful and foiled). Additionally, data on the number of arrests, convictions and sentences imposed in connection with terrorist offences. Information on the locations of the attacks, the number of victims, the nature of the targets (civilian facilities, public facilities, facilities related to critical infrastructure), modus operandi

Criterion	Eurojust's reports	Europol's TE-SAT reports
Data sources	Prosecutors, courts, law enforcement agencies of Member States, foreign partners, OLAF, Interpol, Europol. No sensitive/classified operational data collected in CTR	Law enforcement and security/special services of Member States, Eurojust, Europol's own materials, primarily of an analytical nature. No sensitive/classified operational data used in Europol's core business.

Source: own elaboration.

Summary

A comparison of Eurojust and Europol reports and the established detail of the latter, combined with the growing role of Eurojust and the tools at its disposal, confirm the hypothesis put forward at the outset. In response to the research questions, it should be noted that the modest catalogue of data in Eurojust's reports on terrorism and other types of crime is due to the fact that its reports are designed to present only a certain aspect related to terrorism, namely the form, scale and development trends of law enforcement cooperation in preventing and combating this phenomenon, rather than presenting it in its entirety[70]. Unlike the data contained in TE-SAT, which includes detailed qualitative and quantitative statistics on terrorist attacks along with an in-depth analysis of specific types of terrorism, the data in the Eurojust's report only illustrates the development and forms of cooperation in cross-border criminal proceedings. In its reports, Eurojust also does not include detailed operational data obtained from entities to which it provides assistance and which is collected in CTR. This restriction, which also applies to Europol's reports, stems from the fact that information about persons suspected of terrorism cannot be made publicly available for both legal and praxeological reasons.

Although the data contained in Eurojust's reports does not provide a direct picture of terrorist crime, by presenting the scale of cooperation

[70] More comprehensive data enabling the development of a picture of terrorist crime is presented by Eurojust in other materials it publishes. See, for example, the brochure *Eurojust Meeting on Counter-Terrorism. 27–28 November 2024. Outcome report*, The Hague 2025. https://doi.org/10.2812/4325013.

between law enforcement agencies in the field of international crime, they create an additional perspective that can be adopted in the analysis of the phenomenon of terrorism. First and foremost, it allows us to identify and examine development trends in cross-border cooperation in the prosecution of terrorist offences. In this regard, data indicating a systematic increase in the number of cases involving Eurojust, accompanied by an intensification in the frequency and diversity of legal instruments used, in the absence of a radical increase in terrorist crime, can be seen as an argument in favour of a growing understanding of the benefits offered by Eurojust. Assuming that over time skills in using the tools and solutions offered by Eurojust will also develop, it can be assumed that in the coming years it will become an increasingly important element of an extensive legal and organisational system aimed at preventing various crimes and prosecuting them, including those of a terrorist nature. In this context, it can be suggested that in future Eurojust's reports, more detailed statistical data be published, for example in the form of an annex. The value of the reports would be enhanced by the presentation of additional information concerning, for example, the average response time and the processing of requests for assistance, so that the effectiveness of cooperation could be assessed. It would also be highly informative to cite data relating to the results of proceedings, e.g. in how many cases convictions were secured, funds were frozen, or criminal networks were uncovered. The presentation of such information would certainly allow for more in-depth assessments of the effectiveness and extent of international cooperation in criminal matters and Eurojust's participation therein. The significance of its reports in the context of combating terrorism would also be positively influenced by the presentation of a larger number of case studies and more extensive considerations concerning the basic scope of Eurojust's activities, i.e. analyses of problems in cross-border cooperation. Detailed discussion of the difficulties encountered in international investigations, including legal barriers and restrictions, as well as the procedures and good practices developed to overcome them, would most likely lead to the gradual elimination of the identified obstacles. Such an effect of the reports would be not only cognitive but also practical.

Bibliography

Bartosz K., *Prawne aspekty walki z terroryzmem* (Eng. Legal aspects of fighting terrorism), "Security, Economy & Law" 2018, no. 1, pp. 18–39. https://doi.org/10.24356/SEL/18/1.

Czop A., *Nowe trendy terroryzmu i możliwości podniesienia efektywności jego zwalczania* (Eng. New trends in terrorism and ways to increase the effectiveness of combating them), "Studia de Securitate" 2023, no. 13(2), pp. 153–169. https://doi.org/ 10.24917/26578549.13.2.9.

Fałdowski M., *Międzynarodowa Organizacja Policji Kryminalnych – Interpol w zwalczaniu wybranych zagrożeń XXI wieku* (Eng. International Organisation of Criminal Police – Interpol in fighting selected threats of the 21st century), "Wiedza Obronna" 2023, vol. 282, no. 1, pp. 193–210. https://doi.org/10.34752/2023-i282.

Harkot M., *Wpływ wahabizmu na pozycję społeczno-polityczną Arabii Saudyjskiej* (Eng. Impact of Wahhabism on the socio-political position of Saudi Arabia), "Annales Universitatis Mariae Curie-Skłodowska Lublin – Polonia" 2020, vol. 27, no. 1, pp. 97–110. https://doi.org/10.17951/k.2020.27.1.97-110.

Leśniewski K., *Słów kilka o instytucji wspólnych zespołów śledczych w pryzmacie polskiej procedury karnej* (Eng. A few words about joint investigation teams from the perspective of Polish criminal procedure), "Przegląd Prawno-Ekonomiczny" 2019, no. 2(47), pp. 173–193.

Stronikowska G., *Prokuratura Europejska jako instytucja ochrony interesów finansowych Unii Europejskiej* (Eng. The European Public Prosecutor's Office as an institution protecting the financial interests of the European Union), Warszawa 2020.

Wejkszner A., *Boko Haram – the evolution of jihad activity in Nigeria 2015–2019*, "Przegląd Strategiczny" 2020, no. 13, pp. 349–360. https://doi.org/10.14746/ps.2020.1.21.

Wojciechowski S., Wejkszner A., *The new face of terrorist threat in the European Union. Analysis of the EU Terrorism Situation and Trend Report 2024 (TE-SAT) and other sources*, „Terrorism – Studies, Analyses, Prevention" 2025, no. 7, pp. 307–326. https://doi.org/10.4467/27204383TER.25.035.21812.

Internet sources

France's Corsica rocked by blasts claimed by separatist group, RFI, 9 X 2023, https://www.rfi.fr/en/france/20231009-france-s-corsica-rocked-by-blasts-claimed-by-separatist-group [accessed: 10 VIII 2025].

Launch of Judicial Counter-Terrorism Register at Eurojust, Eurojust, 5 IX 2019, https://www.eurojust.europa.eu/news/launch-judicial-counter-terrorism-register-eurojust [accessed: 9 VIII 2025].

Levitt M., *My Journey Through Brussels' Terrorist Safe Haven*, The Washington Institute for Near East Policy, 27 III 2016, https://www.washingtoninstitute.org/policy-analysis/my-journey-through-brussels-terrorist-safe-haven [accessed: 10 VIII 2025].

Molenbeek. Fabryka terrorystów w stolicy Europy (Eng. Molenbeek. A terrorist factory in the capital of Europe), Magazyn TVN24, https://archiwum.tvn24.pl/magazyn-tvn24/14/tvn24.pl/magazyn-tvn24/molenbeek-przystan-dzihadystow-w-sercu-europy%2c14%2c296.html [accessed: 10 VIII 2025].

Strachota K., *Islamic State-Khorasan: global jihad's new front*, Ośrodek Studiow Wschodnich, 29 III 2024, https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-03-29/islamic-state-khorasan-global-jihads-new-front [accessed: 15 VIII 2025].

Zwalczanie przestępczości kryminalnej (Eng. Combating criminal offences), Informacyjny Serwis Policyjny, 9 I 2025, https://isp.policja.pl/isp/aktualnosci/18325,Zwalczanie-przestepczosci-kryminalnej.html [accessed: 2 XI 2025].

Other documents

Eurojust: European Union Agency for Criminal Justice Cooperation, The Hague 2020, pp. 1–12. https://doi.org/10.2812/556790.

Eurojust Annual Report 2022, Luxembourg 2023, pp. 1–78. https://doi.org/10.2812/022275.

Eurojust Annual Report 2023, Luxembourg 2024, pp. 1–96. https://doi.org/10.2812/356222.

Eurojust Annual Report 2024, Luxembourg 2025, pp. 1–52. https://doi.org/10.2812/2312311.

Eurojust Meeting on Counter-Terrorism, 27–28 November 2024, Outcome report, The Hague 2025, pp. 1–14. https://doi.org/10.2812/4325013.

European Union terrorism situation and trend report 2023, Luxembourg 2023, pp. 1–94. https://doi.org/10.2813/302117.

European Union terrorism situation and trend report 2024, Luxembourg 2024, pp. 1–74. https://doi.org/10.2813/4435152.

European Union terrorism situation and trend report 2025, Luxembourg 2025, pp. 1–75. https://doi.org/10.2813/5425593.

Legal acts

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (Journal of Laws of 2009, item 1569).

Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts (Official Journal of the EU C 340/1 of 10 XI 1997).

Treaty on the Functioning of the European Union (consolidated version) – (Official Journal of the EU C 202/47 of 7 VI 2016).

Treaty on the European Union (Official Journal of the EU C 191/1 of 29 VII 1992).

Regulation (EU) 2023/2131 of the European Parliament and of the Council of 4 October 2023 amending Regulation (EU) 2018/1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA, as regards digital information exchange in terrorism cases (Official Journal of the EU L 2023/2131 of 11 X 2023).

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (Official Journal of the EU L 295/138 of 21 XI 2018).

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (Official Journal of the EU L 283/1 of 10 I 2021).

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (Official Journal of the EU L 130/1 of 3 IV 2014).

Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (Official Journal of the EU L 138/14 of 4 VI 2009).

Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences (Official Journal of the EU L 253/22 of 20 IX 2005).

2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States – Statements made by certain Member States on the adoption of the Framework Decision (Official Journal of the EU L 190/1 of 18 VII 2002).

Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams (Official Journal of the EU L 162/1 of 20 VI 2002).

Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (Official Journal of the EU L 63/1 of 6 III 2002).

Commission Decision of 28 April 1999 establishing the European Anti-fraud Office (OLAF) – (Official Journal of the EU L 136/20 of 31 V 1999).

The article expresses the view of the author and does not represent the position of the Internal Security Agency.

Dariusz Pożaroszczyk, PhD

Lawyer, Internal Security Agency officer.

REVIEW ARTICLES / REVIEWS

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 439–445

https://doi.org/10.4467/27204383TER.25.060.23047

Review

Jerzy Trocha, Paradigm of railway station security[1]

Jacek Lasota
War Studies University
https://orcid.org/0000-0002-1136-9829

Małgorzata Lasota
War Studies University
https://orcid.org/0000-0001-7254-5593

James Watt's invention of the steam engine in 1763 changed the face of the world. Nearly 200 years ago, the world's first steam railway traction was created, and over 180 years ago, the first railway line was inaugurated on Polish soil. This mode of transport primarily 'made the world smaller' and became the driving force behind the development of civilisation. Railway lines quickly became strategic arteries serving the military purposes. The military first used rail transport in 1839 in the United

[1] J. Trocha, *Paradygmat bezpieczeństwa dworców kolejowych* (Eng. Paradigm of railway station security), Warszawa 2025, Akademia Sztuki Wojennej, 200 p.

Kingdom on the Liverpool–Manchester route, but this was only a one-off event. In 1836, a short text by Prussian General Helmuth von Moltke entitled *Über die militärische Benutzung der Eisenbahn* (Eng. On the military use of the railway) was published. Thirteen years later, at the request of Emperor Franz Joseph, the Russians used this means of transport to move a 15 000-strong division from Kraków via Koźle to Uherské Hradiště to fight Hungarian insurgents. Many later experiences were gained also from the American Civil War, the Austro-Prussian War, the Franco-Prussian War, the Boer War and, above all, World War I and World War II. Today, railway plays an important role in the hostilities in Ukraine.

There is a lot of talk about airports and stadiums, while railway stations – places that people use every day – remain in the shadows. Yet in an era of terrorist threats, growing passenger and freight traffic, safety at railway stations is a topic that should be the focus of attention. However, it is rarely discussed in the Polish scientific literature. Until now, there has been no comprehensive, in-depth treatment of this issue. Jerzy Trocha's publication entitled *Paradigm of railway station security* undoubtedly fills the gap and deserves the attention not only of security and defence experts, but also of anyone interested in the functioning of railways as part of a country's critical infrastructure. This is all the more so because the author approaches the subject with great expertise.

Trocha co-authors publications on public safety and crisis management, and his earlier works, including those on civil protection, have attracted the attention of academic and expert circles. He is an author with a solid academic and practical background. He does not write 'from behind the desk', but from the position of a person who knows the functioning of security structures from the inside. He belongs to a rare group of authors who are able to integrate three perspectives: that of systems analyst, that of an officer responsible for safety, and that of a citizen. This combination means that his book is not merely an academic intellectual exercise, but has a strong implementation potential.

What can we find between the covers

Trocha's book is a solid academic monograph. Its structure has been carefully thought out to allow the reader to be gradually introduced to the subject, and the language remains understandable even to those

outside the expert community. This is not a textbook or a collection of legal provisions, but an analytical story about railway stations, places so familiar that we cease to notice them.

The book is divided into four parts, which form a logical structure: from the historical and structural characteristics of railway stations in Poland, to an analysis of the typology of threats, to a description of security systems and a set of recommendations aimed at improving the current situation.

The first chapter is introductory and contextual in nature. In it, the author reviews the origins of rail transport in Poland, placing the development of the railways in the context of the historical, economic and political conditions of particular eras. He pays particular attention to the impact of the partitions on the development of the railway infrastructure and the processes of its reconstruction and development after regaining independence in 1918. Later on, he presents the contemporary legal conditions governing the operation of railway stations in Poland, including issues related to their ownership and organisational structure. He also classifies types of railway stations according to their functions and the scale of passenger traffic they handle.

The second chapter provides a critical analysis of factors threatening the safety of users and station infrastructure. Trocha identifies and describes in detail both intentional threats (such as terrorist activities, crimes and offences), as well as random threats, including fires, technical failures and other emergencies. The author emphasises the specific nature of railway stations as places with a high concentration of users, which, combined with their public character, significantly increases their vulnerability to crisis incidents. In the context of contemporary threats, the author discusses of the impact of the migration crisis related to the armed conflict in Ukraine on the level of security in railway areas, which is particularly important.

In the third chapter, which is systemic and descriptive in nature, Trocha focuses on institutional and technical mechanisms for ensuring railway station safety. He discusses primarily the role of physical protection, technical security systems as well as specialised entities and services, including the Railway Station Safety Centre, the Railway Security Guard, the Police, as well as forms of cooperation between them. He also analyses the functioning of crisis management structures in the railway sector as well as the importance of international standards and supranational

organisations for shaping practices in the area of critical infrastructure protection.

The fourth chapter includes summary, conclusions and recommendations. The author identifies the most important problems and shortcomings in the current station infrastructure security system in Poland and presents proposals for modernisation and implementation measures aimed at improving security level at the design stage and during the operation of railway station facilities. Of particular value is the list of author's recommendations concerning organisational, legal and technical changes. According to Trocha, the solutions described allow the railway station security system to be adapted to contemporary threats and social expectations.

Each of the chapters serves a separate but complementary function: from outlining the context, to analysing threats and protective measures, to recommending systemic changes. As a result, the book provides a comprehensive overview of the subject and can serve as both a source of academic knowledge and a practical guide for those involved in the security of critical infrastructure.

The publication *Paradigm of railway station security* includes interesting iconographic material – the charts and tables complement the author's reflections and allow the reader to better understand the content. The monograph has clear typography and a legible layout. This makes the text easier to work with, which is a significant added value in this type of publication. In other words, the structure of the book was planned in a manner that enables a smooth transition from the diagnosis of the actual state and risk analysis, through the assessment of available protective mechanisms, to the formulation of proposals for changes aimed at improving public safety at railway stations. Such an arrangement of content allows for an in-depth understanding of the issue and, at the same time, provides a starting point for further scientific research and practical considerations in this area.

Strengths and weaknesses of the publication – subjective reflections

The greatest strength of the publication is its interdisciplinary nature, as it combines knowledge in the fields of security, history, law and management.

Reliable bibliography, up-to-date information and the author's experience build the reader's trust in the proposed conclusions.

One of the shortcomings may be the occasional use of specialised language, which makes some passages difficult to understand for readers who are less familiar with the subject matter. There is also a lack of in-depth comparisons with solutions used abroad, which could broaden the perspective of the publication. It seems that the main shortcoming of book, is the lack of explanation of the term 'paradigm' – how the author understands this and what the paradigms of railway station security are. This expression appears only once – in the title. The lack of definition of a key concept constitutes an understatement that may hinder the classification of the book within the established discourse of security sciences. According to the reviewers, setting a clearly defined research problem would have allowed this mistake to be avoided. Taking into account the broader scientific apparatus specific to security studies would further enhance the scientific value of this monograph.

Summary – who is this book for

Paradigm of railway station security is a publication which defies simple categorisation. It is not a typical academic monograph, although it meets all scientific requirements. Nor is it a practical guide, although it can certainly serve as a guide for infrastructure managers or officers. It is more like a well-thought-out analytical and social project and diagnosis of the current situation, as well as an appeal for sensible and responsible planning of public space.

The way the author shows railway station is particularly interesting. It is not only a physical facility, but also, a place where different social groups, interests, cultures and, unfortunately, also threats meet. It is a space, where security ceases to be an abstraction and becomes part of everyday experience.

There is no intrusive didacticism here, but neither is there any tolerance for mediocrity. Trocha writes with responsibility that spreads to a reader. After reading this book, it is difficult to view the railway station as just a place to change trains.

The reviewed publication deserves careful reading. It was written with specialists in mind, but it is also understandable to a wider audience,

including people who are not professionally involved in security issues. We recommend it especially to:

- students and lecturers in fields related to security, defence, transport and public administration,
- employees of structures responsible for protection of the critical infrastructure,
- local government officials and spatial planners,
- as well as all citizens who wish to consciously participate in shaping safety public space.

The reviewed monograph[2] is a rare example of a book that successfully combines expert knowledge with a sense of social responsibility. The book not only diagnoses the problem but also inspires further reflection and action. We need more publications like this in times of growing uncertainty.

Col. (Ret.) Associate Professor Jacek Lasota,
Professor of the War Studies University

Certified officer, graduate of the Officer School of Armoured Forces in Poznań, of diploma studies and third-cycle studies at the Academy of National Defence. After graduating in 1993, he served in 9 pz, 6 BKPanc, 34 BKPanc and 2 BOT. He participated in activities of the 8th rotation of the Polish Military Contingent in Iraq in 2007. Since 2008, he has been associated with the AON (since 2016 – the War Studies University). He is currently the Director of the Institute of History and Polemology at the War Studies University. His reasearch interests include issues related to: theory and history of the art of war, polemology, military security.

Contact: j.lasota@akademia.mil.pl

[2] We encourage readers to get acquainted with another review of this monograph. The review was published in issue 33 of the journal "Przegląd Bezpieczeństwa Wewnętrznego" published by the Internal Security Agency (editor's note). See: E. Jakubiak, *Jerzy Trocha, Paradygmat bezpieczeństwa dworców kolejowych*, "Przegląd Bezpieczeństwa Wewnętrznego" 2025, no. 33, pp. 217-221. https://doi.org/10.4467/20801335PBW.25.027.22644.

Małgorzata Lasota, PhD

Doctor of social sciences in the discipline of security sciences, assistant professor at the Department of Security Management in Civil Aviation of the Institute of Civil Aviation Management, the War Studies University. She has many years of professional experience gained in Polish and foreign airlines, where she served as a cabin crew instructor. Her research interests focus on safety management in civil aviation as well as training, preparation and operational procedures, with particular emphasis on issues related to flight safety.

Contact: m.lasota@akademia.mil.pl

AWARDED THESES

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 449–483

https://doi.org/10.4467/27204383TER.25.061.23048

Article

Capabilities of the Armed Forces of the Republic of Poland in the area of decontamination – selected aspects[1]

Krzysztof Tokarczyk

Independent author

https://orcid.org/0009-0004-4484-6179

Abstract

This article analyses the capabilities of the decontamination subsystem of the Polish Armed Forces in the context of contemporary security challenges, with particular emphasis on chemical, biological and radioactive (CBRN) threats. The author characterised the decontamination subsystem, discussed its structure and operating conditions, and compared it with the subsystems in Germany and the US. The results of the analysis indicate technological, organisational, and doctrinal limitations that impact the subsystem's effectiveness. Proposed solutions include equipment modernisation, procedure standardisation and strengthening cooperation between armed forces and non-military entities. The author emphasises the need to adapt the subsystem to NATO requirements and contemporary hybrid threats.

[1] The article is based on a doctoral dissertation entitled *Zdolność podsystemu likwidacji skażeń Sił Zbrojnych Rzeczpospolitej Polskiej do podjęcia działań* (Eng. The ability of the decontamination subsystem of the Armed Forces of the Republic of Poland to take action), defended at the War Studies University. The dissertation was awarded in the 14th edition of the Head of the Internal Security Agency competition for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats.

Keywords

decontamination, Polish Armed Forces, CBRN, operational capabilities, security

Introduction

The hazards associated with the use of weapons of mass destruction (WMD) remain one of the significant challenges to national security in the context of both potential terrorist acts and armed conflicts. This is evidenced by incidents of this type recorded over the last 30 years:

- 1995 – the Aum Shinrikyo cult carried out an attack in the Tokyo subway, spraying sarin, which killed 13 people and poisoned several thousand[2];
- 2006 – in London, Alexander Litvinenko, a former officer of the Russian Federal Security Service (FSB), was poisoned with the radioactive substance polonium-210 administered in tea, which led to his death from radiation sickness within three weeks[3];
- 2015 and 2017 – Russian politician and journalist Vladimir Kara-Murza, known for his criticism of the Kremlin, has twice been the victim of suspicious poisonings, which led to multiple organ failure and coma. In both cases, Russian hospitals and foreign tests confirmed poisoning with an unidentified chemical substance[4];
- 2018 – in Salisbury, Great Britain, the chemical agent Novichok was used in an attempt to poison Sergei Skripal, a former Russian military intelligence officer, and his daughter Yulia. The substance,

[2] *Rozproszenie gazu sarin w Tokio* (Eng. The sarin gas attack in Tokyo), Terroryzm!com, 26 XII 2006, http://www.terroryzm.com/rozproszenie-gazu-sarin-w-tokio/ [accessed: 25 VII 2025]; K. Pletcher, *Tokyo subway attack of 1995*, Britannica, 8 V 2025, https://www.britannica.com/event/Tokyo-subway-attack-of-1995 [accessed: 25 VII 2025]; T. Okumara et al., *Report on 640 Victims of the Tokyo Subway Sarin Attack*, "Annals of Emergency Medicine" 1996, vol. 26, no. 2, pp. 129–135. https://doi.org/10.1016/S0196-0644(96)70052-5.

[3] *Alexander Litvinenko: Profile of murdered Russian spy*, BBC News, 21 I 2016, https://www.bbc.com/news/uk-19647226 [accessed: 26 VII 2025].

[4] *Vladimir Kara-Murza Tailed by Members of FSB Squad Prior to Suspected Poisonings*, Bellingcat, 11 II 2021, https://www.bellingcat.com/news/2021/02/11/vladimir-kara-murza-tailed-by-members-of-fsb-squad-prior-to-suspected-poisonings/ [accessed: 1 VIII 2025].

which was applied to the door handle of their home, led to the serious poisoning of the Skripals and police officer Nick Bailey, as well as the death of Dawn Sturgess, who had accidental contact with an abandoned vial containing the poison[5];

– 2020 – Russian opposition leader Alexei Navalny was poisoned with the chemical agent Novichok during a flight from Tomsk to Moscow, which led to his hospitalisation. The poison was applied to his clothing (probably his underwear). The presence of the substance was confirmed by five laboratories certified by the Organisation for the Prohibition of Chemical Weapons (OPCW)[6];
– 2017 – Kim Jong-nam, the brother of North Korea's leader, was attacked at Kuala Lumpur airport with the paralytic-convulsive agent VX, which was applied to his face by two women[7].

Incidents involving the poisoning of Russian citizens are attributed to the FSB unit specialising in toxic substances and are linked to the activities of the Russian secret services aimed at eliminating Vladimir Putin's political opponents[8].

Due to their deliberate nature and the use of prohibited substances against civilians, these events can be classified as acts of terrorism. The use of chemical weapons in contemporary armed conflicts was of a different nature, despite the existence of the Chemical Weapons Convention[9]:

---

[5] S. Morris, *UK believes Putin personally authorized Salisbury novichok attack, inquiry told*, The Guardian, 14 X 2024, https://www.theguardian.com/uk-news/2024/oct/14/salisbury-novichok-poisonings-inquiry-sergei-skripal-vladmir-putin [accessed: 25 VII 2025].

[6] F. Gardner, *Navalny 'Novichok poisoning' a test for the West,* BBC News, 2 IX 2020, https://www.bbc.com/news/world-europe-54003014 [accessed: 1 VIII 2025]; *OPCW Issues Report on Technical Assistance Requested by Germany*, OPCW, 6 X 2020, https://www.opcw.org/media-centre/news/2020/10/opcw-issues-report-technical-assistance-requested-germany [accessed: 1 VIII 2025]; D. Steindl et al., *Novichok nerve agent poisoning*, "The Lancet" 2021, vol. 397, no. 10270, pp. 249–252. https://doi.org/10.1016/S0140-6736(20)32644-1.

[7] *Kim Jong-nam killing: 'VX nerve agent' found on his face*, BBC News, 24 II 2017, https://www.bbc.com/news/world-asia-39073389 [accessed: 26 VII 2025].

[8] *The Lab: How FSB chemical weapons experts tried to poison Alexei Navalny*, The Insider, 14 XII 2020, https://theins.ru/en/politics/262611 [accessed: 1 VIII 2025]; *Zabójstwo Aleksandra Litwinienki* (Eng. The murder of Alexander Litvinenko), in: Konsorcjum Mall-CBRN, *Podręcznik zapobiegania i reagowania na zdarzenia CBRNE w centrach handlowych*, https://www.uni.lodz.pl/fileadmin/Projekty/MALL-CBRN/Materials_available_for_download_/Mall-CBRN-Handbook-PL-1.0.pdf, pp. 24–25 [accessed: 2 VIII 2025].

[9] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, drawn up in Paris on 13 January 1993.* Compliance

– between 2013 and 2018 in Syria, the OPCW confirmed at least 85 cases of chemical weapons use[10], mainly sarin and chlorine. These actions are unofficially attributed to Bashar al-Assad's regime[11]. The use of dangerous substances resulted in hundreds of deaths and thousands of casualties[12];
– since February 2022 in Ukraine, the OPCW has recorded reports of more than 3000 cases of the use of toxic substances, including chloropicrin. OPCW technical inspections during site visits have gathered evidence of the use of these substances and secured relevant traces. However, from a procedural point of view, the evidence is insufficient and requires further investigation to conclusively determine that these incidents were caused by Russian forces[13].

The use of WMD by an adversary (state, organisation, assassin) poses a serious operational hazard to military operations, and a significant security threat to state authorities in the context of crisis management in the broad sense, but also to civilians who are unprepared for such attacks.

An analysis of the events mentioned above highlights the enormous costs that must be incurred in order to eliminate or at least minimise the negative effects of contamination resulting from the use of chemical,

with the provisions of the Convention is monitored by the OPCW, based in The Hague, as the executive body.

[10] A report by the public broadcaster BBC indicated that between September 2013 and spring 2018, there were 106 cases of chemical weapons use in Syria. Neither this report nor any of the official reports of the United Nations or the OPCW explicitly identified the perpetrator of the use of prohibited substances. See: *Syria: BBC Investigation Reveals Widespread Chemical Weapons Use*, BBC, https://www.bbc.co.uk/programmes/w172w25d6yyjrc0 [accessed: 25 X 2018].

[11] Inspections conducted by the OPCW in Syria confirmed the use of prohibited toxic agents, but the evidence gathered and secured did not allow for a clear identification of the entity responsible for their use. At the same time, given that the victims of the attacks were so-called rebels and the community supporting them, it is highly likely that the agents were used by forces loyal to the President's regime.

[12] *Syria: BBC Investigation Reveals*...

[13] The use of prohibited weapons in the Russian-Ukrainian war resembles the actions in Syria. A common feature in both cases is the lack of evidence enabling the perpetrator of the use of WMD to be clearly identified. See: *OPCW issues report on third Technical Assistance Visit to Ukraine following an incident of alleged use of toxic chemicals as a weapon*, OPCW, 26 VI 2025, https://www.opcw.org/media-centre/news/2025/06/opcw-issues-report-third-technical-assistance-visit-ukraine-following [accessed: 26 VI 2025].

biological, radiological and nuclear (CBRN) agents[14]. This includes the need to possess and develop the ability to carry out broadly understood decontamination, both internal (when contaminants have entered the human body through the skin or digestive system) which is carried out by qualified health care units, as well as external (surface) contamination, which is neutralised by other services, most often forces detached from the resources of the State Fire Service (PSP) or the Armed Forces of the Republic of Poland (SZ RP).

The decontamination capabilities achieved by individual services must be sufficient to remove (or destroy) contamination resulting from both terrorist acts and military operations. In this context, it is necessary to take into account, above all, human resources and procedures that are as unified as possible, as well as the specific nature of potential tasks, the time and place of activities, infrastructure and logistics. It seems reasonable to have a coherent system at the national level for the interoperability and cooperation of individual services, depending on the operation being conducted.

The article presents selected aspects of the capability of the Polish Armed Forces' decontamination subsystem as part of the defence system against weapons of mass destruction (OPBMR)[15] in the process of achieving the capability to take action. The subsystem comprises the indicated organisational structures of the Polish Armed Forces, equipment and gear appropriate for the specific nature of the tasks, proven operating procedures, as well as relations between the management structures, those carrying out decontamination measures and the troops undergoing this process. This subsystem can also be seen as a set of unique capabilities. Achieving them affects the potential capabilities of individual subunits, troops, organisational structures or entire systems.

[14] In the United Kingdom, nearly 800 soldiers from the chemical regiment were involved in the operation to identify contamination, take multiple samples and, above all, decontaminate buildings and land after the attempted poisoning of Sergei Skripal and his daughter in 2018. The operations, which resulted in the infrastructure being declared fit for use again, lasted almost a year and cost millions of pounds. See: *Salisbury declared decontaminated after Novichok poisoning*, BBC, 1 III 2019, https://www.bbc.com/news/uk-england-wiltshire-47412390 [accessed: 10 III 2019].

[15] This system is part of the functional system for the survival and protection of troops, which, like other functional systems, was established on the basis of Decision No. 56/Org./P5 of the Minister of National Defence of 24 December 2013 on the Organisers of Functional Systems of the Polish Armed Forces (unpublished).

This article aims to present the capabilities of the Polish Armed Forces' decontamination subsystem, identify its weaknesses and indicate directions for development. The analysis is based on the literature on the subject, NATO doctrinal documents, the author's research forming the basis of his dissertation, and examples. The dissertation sought to identify the factors that determine the capabilities of the Polish Armed Forces' decontamination subsystem and ways to improve it in the face of contemporary CBRN threats[16]. An interdisciplinary approach was used, combining historical, comparative and systemic analysis. The analysis of existing and desired capabilities was carried out in accordance with the DOTMLPFI criteria[17] adopted by NATO, as a fully functional capability must take into account not only technical and technological aspects[18], but also all other factors that influence it.

The article may serve as a starting point for discussion and further research on the need for a coherent, inter-ministerial decontamination system at the national level, capable of responding to both terrorist incidents and the combat use of prohibited weapons.

Structure and role of the Polish Armed Forces decontamination subsystem

The decontamination subsystem[19] in the Polish Armed Forces is one of the key subsystems of the OPBMR system. Contamination elimination, also referred to as decontamination, aims to ensure the safety of people, facilities or areas. It involves the sorption, destruction, neutralisation, rendering harmless or removal of chemical or biological contaminants, or the removal of radioactive substances from them or their surroundings.

[16] The research question in the dissertation was: 'What requirements should the Polish Armed Forces' decontamination subsystem meet and what capabilities must it achieve in functional and structural terms in order to be fully ready to perform its tasks, and how should it be organised in times of peace and war?'.

[17] DOTMLPFI is an acronym formed from the first letters of each component of capability: doctrine, organisation, training, material, leader, personnel, facilities, interoperability. This type of analysis allows for a holistic view of capability.

[18] Equipment and technical ability to use it.

[19] See: *NATO Glossary of Terms and Definitions* AAP-6(2014), p. 129; *NATO Glossary of Terms and Definitions for Chemical, Biological, Radiological and Nuclear Threats* AAP-21(B), p. 18; NO-01-A006:2010 *Defence against weapons of mass destruction. Terminology*, p. 17.

General characteristics of the subsystem

The main tasks of the decontamination subsystem in the Polish Armed Forces include:

- neutralisation of chemical, biological and radiological contamination in order to protect personnel and equipment,
- multi-level decontamination of personnel, uniforms, equipment, including sensitive equipment (SE), and the area,
- support for military and civil operations in crisis situations, such as terrorist incidents or industrial and natural disasters.

A soldier's ability to carry out decontamination procedures is developed as early as the basic training stage, as one of the skills enabling survival (saving one's own life or that of another soldier) and creating conditions for the continuation of the assigned task. Decontamination is therefore present and perfected at every organisational level (from the soldier to the Armed Forces component – Figure 1), and thus at every organisational level – from tactical to strategic.

The broadest scope of activities in this area has been assigned to soldiers from decontamination units that are part of the chemical forces, and they have the best training in this regard. Until recently, decontamination was even considered at the political and strategic level in civilian state structures[20]. The higher the organisational or command level, the broader the scope of tasks performed, which in military doctrine is generally described as (...) *creating conditions for the armed forces to perform their tasks in situations of contamination and contamination threats*[21].

In any case, as part of the task, operation or mission planning process, the appropriate scope of decontamination is taken into account, which is a function of variables such as:

- organisational level,
- command level,

[20] Paragraph 16(8)(f) of the repealed *Regulation of the Council of Ministers of 27 April 2004 on the preparation of the national security management system* indicated that the preparation of command posts for individual public authorities included the preparation of **points for special measures**. Meanwhile, the *Regulation of the Council of Ministers of 25 March 2025 on the preparation of the national security management system*, which repealed the previous executive act, generally specified that protective and rescue measures are carried out in relation to the main command post, without specifying the contractor or the scope of these measures.

[21] *Defence against weapons of mass destruction in combined operations* DD/3.8(A), Training 869/2013, p. 14.

– task, operation or mission,
– theatre of operations, taking into account terrain conditions and even climate zones,
– availability of terrain infrastructure in the area of operations,
– logistics system,
– degree of detail of reconnaissance preparation of the battlefield,
– the enemy, its CBRN[22] capabilities and potential impact,
– CBRN threat level,
– forces and resources allocated to the task/operation/mission,
– meteorological conditions.

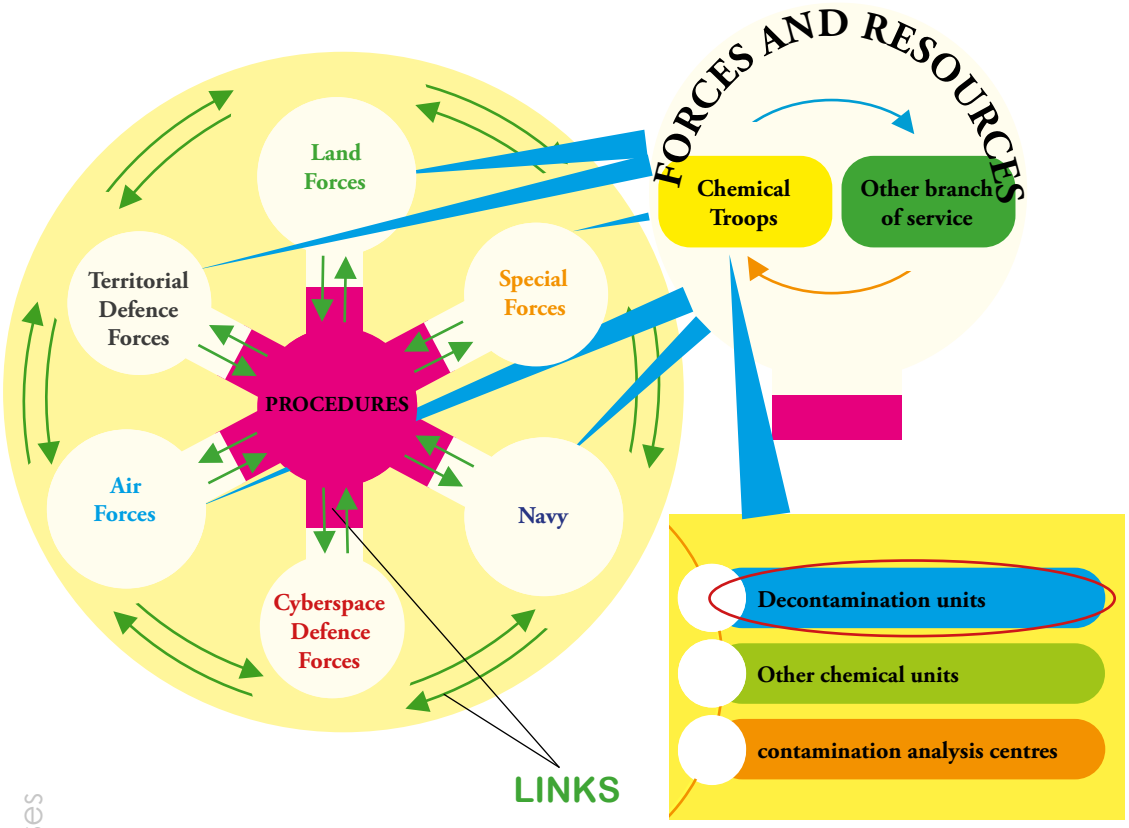


Figure 1. General structure of the Polish Armed Forces decontamination subsystem.

Source: own elaboration.

[22] OPBMR issues outside Poland have been described as 'CBRN' - (translator's note).

The last factor plays a particularly important role, which is why the impact of natural forces on contamination without human intervention has been treated as a form of contamination remediation (so-called passive decontamination)[23]. The weather, or more precisely selected meteorological parameters, is taken into account in the planning process. Since humans have no influence on these conditions, only human-dependent issues can be considered when modelling or optimising the functioning of the system. In the Polish Armed Forces, these are treated as active contamination removal.

Contamination removal carried out by the Polish Armed Forces for the military includes classification based on:

1) the agent causing contamination:
   – decontamination – exposure to chemical agents (C),
   – deactivation – action against radioactive agents (R, N),
   – disinfection – action against biological agents (B),
2) the entity affected (for which decontamination is carried out):
   – people – both those who are contaminated but still able to perform tasks after treatment, and those who are injured, for whom treatment is a preliminary stage allowing for further treatment and rehabilitation,
   – individual soldier equipment,
   – combat equipment (land, aircraft and ships) and armaments,
   – electronic, optical and optoelectronic equipment considered sensitive (SE),
   – facilities,
   – terrain.

Mechanical, physical and chemical methods are used in the decontamination process[24]. The choice of method depends on the contaminant and the time elapsed since contamination. Chemical contaminants should be removed as quickly as possible using the best

[23] Passive decontamination, known as natural decontamination or weathering, is a natural process of decontamination that does not require the use of forces or resources. Objects left for passive decontamination should be isolated and marked as hazardous. See: *Defence against weapons of mass destruction in combined operations* DD/3.8(A)..., p. 50.

[24] Various approaches to this issue can be found in the literature on the subject. This article adopts the most commonly used nomenclature contained in the manual *Special treatments for terrain and field defensive structures*, Ref. No. 1984 Chem. 321, Warszawa 1985, and in: A. Leosz, S. Sawczak, *Sprzęt likwidacji skażeń* (Eng. Decontamination equipment), WSO–TK internal 57/96.

available methods. The principle of 'as quickly as possible' is crucial in OPBMR.

Subsystem structure

The decontamination subsystem consists of (Figure 2):

- **organisational structures** (some OPBMR projects are carried out by all soldiers, and therefore each soldier is part of the subsystem),
- **equipment** used to carry out tasks,
- **measures** directly affecting contamination,
- **procedures** and **relationships** defining the performance of tasks and rules of cooperation.

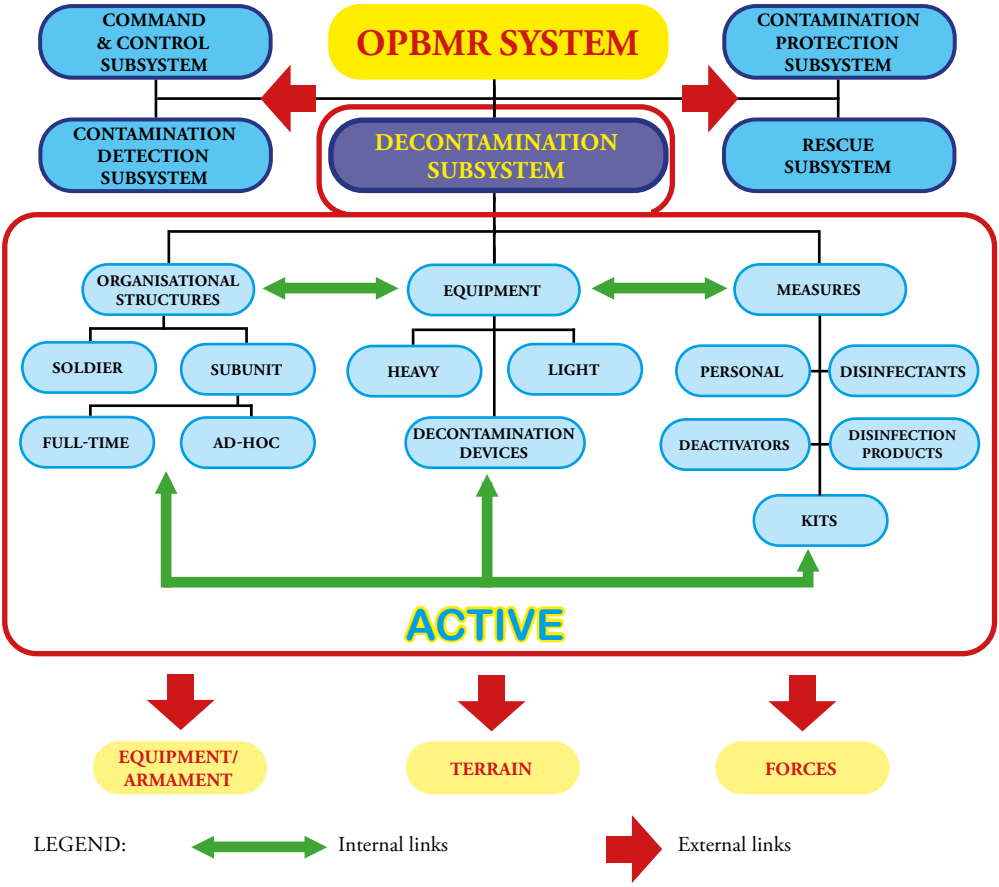


Figure 2. Components of the Polish Armed Forces decontamination subsystem.

Source: own elaboration.

Although only chemical decontamination subunits are capable of performing the full range of tasks related to this subject area[25], it is vital for every soldier to take immediate and appropriate remedial action after potential contact with a contaminant. The selection of equipment and gear is also related to the scope of assigned tasks. Soldiers of decontamination subunits have specialised devices and means for decontamination, while soldiers of other types of troops are equipped with the equipment and means necessary to carry out immediate[26] and/or operational[27] decontamination, depending on the organisational level, needs and capabilities.

Capability requirements for the subsystem

The concept of operational capability in the Polish Armed Forces was introduced by Decision No. 95/MON of the Minister of National Defence of 27 February 2007 on guidelines for the Operational Requirements Review[28]. In 2014, the decision was amended to include the DOTMLPFI model. These capabilities are described in the Catalogue of Capabilities of the Polish Armed Forces[29], in area P – survival and protection of troops, in which the decontamination subsystem is a key element of the OPBMR

[25] Decontamination subunits perform Level III tasks, i.e. thorough decontamination, mainly at decontamination points (PLSk). PLSks perform a full range of tasks, i.e. in relation to contaminated people and combat equipment. In the case of decontamination carried out in military formations (in areas where troops are deployed), the procedures mainly concern equipment. The decontamination of people takes time and is too sensitive a process to be carried out close to the line of contact between troops (within range of the enemy's basic firepower).

[26] Each soldier undertakes immediate decontamination as soon as contamination is detected. The procedures for which they use their individual protective kit, mainly the IPP-95 individual anti-chemical kit and the IPLS-1 individual decontamination kit, are applied to exposed parts of the body, uniforms, and parts of weapons and equipment essential for further use.

[27] These procedures are primarily performed by decontamination teams from OPBMR units at the company level (equivalent sub-unit) and full-time personnel operating combat equipment such as tanks, combat vehicles and motor vehicles. The procedures are carried out using PZLS-1 contamination decontamination kits and instruments included in the combat equipment, e.g. the DK-4 ejector kit, ZOd-2, ZO-E, ZO-1 or ZO-2 decontamination kits.

[28] *Decision No. 95/MON of the Minister of National Defence of 27 February 2007 on the introduction of the 'Guidelines for Conducting an Operational Needs Review'*.

[29] Classified document. The catalogue is one of the tools for planning the development of the Polish Armed Forces.

system. The author has identified four main capabilities for decontaminating people (personnel), equipment, facilities and terrain (Figure 3).

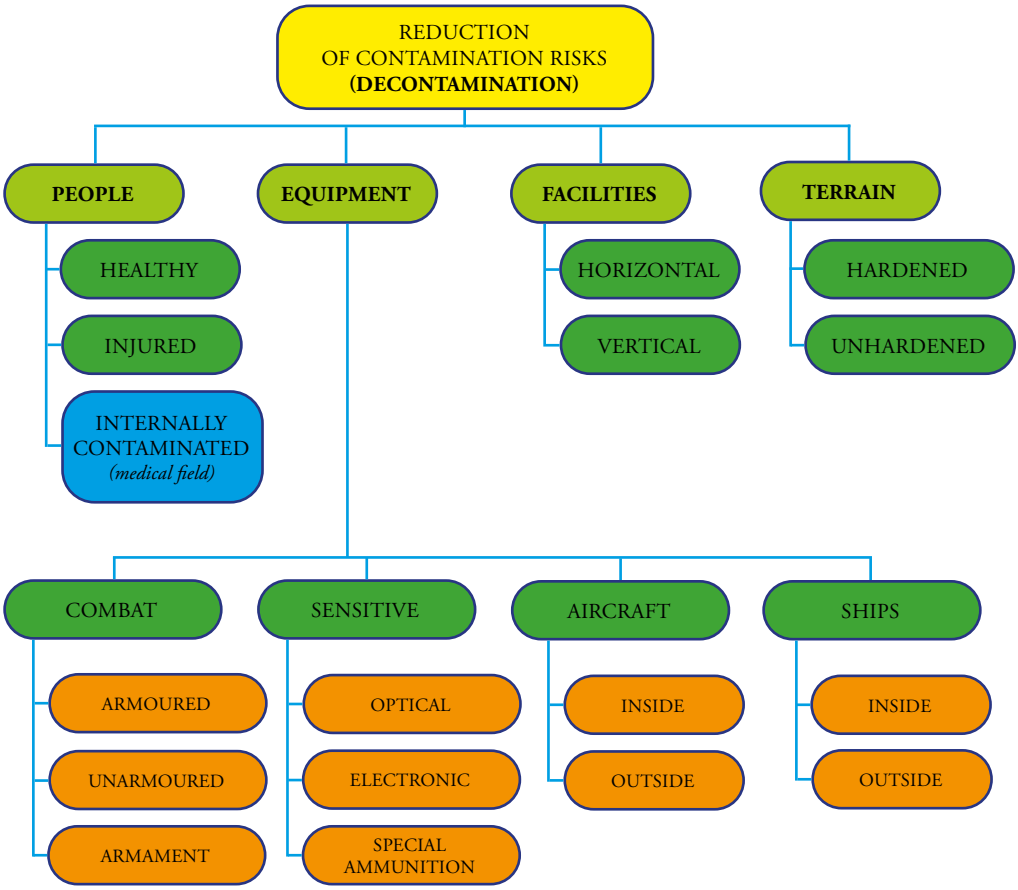


Figure 3. Capabilities of the OPBMR system decontamination subsystem.

Source: own elaboration based on the Catalogue of Capabilities of the Polish Armed Forces.

The ability to decontaminate people includes procedures for soldiers and civilians, with wartime and peacetime procedures, including support during possible contamination during mass events (inspired by the security measures taken during EURO 2012), being unified[30].

[30] The planning, organisation and conduct of decontamination in the Polish Armed Forces, including the decontamination of people, are essentially defined by the following documents: *Regulations for chemical forces of the land forces*, DWLąd. Internal 183/2011 and *Sanitary and special treatments of weapons and combat equipment*, Chem. Instruction 278/79.

Systems for decontaminating people can be field-based (in tents, containers, vehicles) or stationary, while meeting the following requirements: specific throughput (number of people/hour depending on the level), communication routes eliminating contact between contaminated and clean persons, separation of clean and dirty zones, securing water and decontamination agents, water heating, collection of contaminated waste generated after treatment, contamination control, medical stations and separate routes for women and men.

The ability to treat people who have been internally contaminated by chemical or radioactive agents goes beyond the competence of chemical warfare units and has been assigned to health protection services. However, such patients require preliminary decontamination before they can be admitted to hospital.

Within the decontamination subsystem, the equipment undergoing this process is divided into the following groups: combat, sensitive, ships (external and internal treatments, at sea or in port) and aircraft (external and internal treatments). The methods used vary depending on the design and purpose of the equipment, taking into account its different surfaces.

The ability to decontaminate facilities includes buildings up to 15 metres high, stationary infrastructure (offices, schools) after floods or pandemics, as well as paved surfaces, roads and squares.

In accordance with NATO requirements, the ability to decontaminate the area requires subunits to be self-sufficient for three days and to maintain the capacity to transport 90 m^3 of water and purify 240 m^3/day[31].

Conditions for the functioning of the Polish Armed Forces decontamination subsystem

The functioning of the Polish Armed Forces' decontamination subsystem is determined by operational, doctrinal, technological, financial, organisational and training conditions.

[31] *BI-SC Capability Codes and Capability Statements*, 26 I 2016, https://www.scribd.com/document/382349178/Capability-Codes-and-Capability-Statements-2016-Bi-sc-Nu0083, p. 304 [accessed: 2 VIII 2025].

Operational conditions

The operational conditions of the decontamination subsystem in the Polish Armed Forces determine its organisation and functioning, taking into account anticipated threats, the type of mission and the balance of forces in national and allied operations. At the same time, the modern battlefield has become an extremely complex and demanding area of operation due to the integration of systems used in cyberspace and robotics using artificial intelligence. There is more and more electronics in the equipment, which forces the search for increasingly advanced decontamination technologies (e.g. the use of vacuum, vaporised hydrogen peroxide, nanosorbents, enzymes or cold plasma) and their replacement with universal equipment. The Polish Armed Forces must be able to respond skilfully to various scenarios involving CBRN threats, both at home (during armed conflict or terrorist incidents) and abroad. The analysis of threats converted into scenarios influences the planning of countermeasures appropriate to the situation, which often involves the acquisition of newer equipment and technologies. These are, of course, examined and verified during testing, but reality verifies the correctness of the implemented solutions and exposes any shortcomings and errors. The incident in Salisbury in 2018, in which the chemical agent Novichok was used, revealed shortcomings in the capabilities of civil services and the military, such as difficulties in decontaminating the civilian environment and the need for them to work together. It took almost a year to restore the contaminated area to public use, as the procedures carried out there were at the highest i.e. level IV clearance decontamination[32]. At the time of writing, no such procedures were in place in the Polish Armed Forces. Furthermore, the decontamination agents used by the Polish military had not been tested for their effectiveness against Novichok-type agents.

Furthermore, while the interoperability of the Polish Armed Forces with Alliance forces is achieved at various levels of integration[33], as well

[32] Level IV treatments involve the elimination of contamination to achieve complete safety from CBRN contamination. See: *Defence against weapons of mass destruction in combined operations* DD/3.8(A)...

[33] Interoperability, as defined by NATO, is the ability to operate coherently, effectively and efficiently to achieve Alliance objectives. Its level depends on the degree to which different systems and forces can work together. There are three levels of interoperability: commonality – when all forces involved in a joint operation use the same doctrines, procedures and equipment; interchangeability – the ability to use a specific product, process or service in place of another to meet the same requirements; compatibility –

as at the equipment, organisational, doctrinal, procedural and training levels[34], it is difficult to speak of common standards of conduct between the Polish Armed Forces and civil services in the area of decontamination. Interoperability is one of the challenges in building the readiness of the decontamination subsystem to perform specialised tasks.

Doctrinal considerations

The doctrinal conditions of the decontamination subsystem in the Polish Armed Forces are shaped by a hierarchical system of operational standardisation documents, including:

- doctrines (as level 1 documents),
- doctrinal documents (level 2),
- supplementary documents (level 3).

Issues related to OPBMR, and thus the decontamination subsystem, are addressed in dozens of publications. The most important of these is the periodically updated doctrinal document *Defence against weapons of mass destruction in combined operations* DD/3.8[35], which in its current version (B) introduces a three-pillar approach to CBRN defence, comprising prevention, protection and recovery. This document standardises the planning, execution and support of operations in conditions of WMD threat or use. The changes introduced in version (B) reflect, among other things, an active threat response model inspired by American solutions[36].

The following documents are also important from the point of view of creating a decontamination subsystem: the DD/3.14 *Protection of military*

the suitability of products, processes or services for use in specific conditions to meet requirements without causing unacceptable interactions between them.

[34] Requirements in this area have been specified in standardisation documents (STANAGs), planning documents (e.g. *BI-SC Capability Codes and Capability Statements*...), training documents, doctrines and regulations.

[35] *Defence against weapons of mass destruction in combined operations* DD/3.8(A)... is the equivalent of a document: NATO Standard AJP-3.8 *Allied joint doctrine for chemical, biological, radiological, and nuclear defence,* Edition A Version 1, 2012 https://assets.publishing.service.gov.uk/media/5bf40787ed915d18301589b4/archive_doctrine_nato_cbrn_defence_ajp_3_8.pdf [accessed: 2 VIII 2025]. During the research, version DD/3.8 (A) was in force, and since 2018 – version DD/3.8 (B).

[36] M.F. Kelly, *United States Army Chemical, Biological, Radiological and Nuclear Corps Capability for Combating the Contemporary Weapons of Mass Destruction Threat*, Master's Thesis, Fort Leavenworth, Kansas 2012, https://apps.dtic.mil/sti/tr/pdf/ADA563129.pdf, pp. 67–69 [accessed: 2 VIII 2025].

forces doctrine document[37], which specifies the rules for protecting personnel, equipment, infrastructure and operational capabilities in combined and multinational operations, treating OPBMR as a component of protection; *The combat systems integration manual* DD/7.1.2[38], which sets out the rules for integrating the decontamination subsystem during training and exercises, and the *Regulations for chemical forces of the land forces*[39], which standardises the planning and implementation of tasks, including support in various forms of combat operations.

In NATO, medical aspects of CBRN defence are regulated by CBRN Medical Publications: AJMedP-7 (medical support in CBRN operations),[40], AMedP-7.1[41] (CBRN casualty management) and AMedP-7.3[42] (CBRN medical training), which focus on decontaminating casualties.

The procedures for decontamination in the Polish Armed Forces are generally consistent with NATO standards, with the exception of clearance decontamination.

Technological constraints

The technological conditions of the subsystem have implications resulting from Poland's membership in NATO, such as allied standards, meeting the requirements of the armed forces' objectives, and achieving full interoperability in tactical and operational activities, procedures, and technology. Meanwhile, equipment designed in the 1970s and 1980s and used by the Polish Armed Forces is unable to meet certain requirements and limits the subsystem's capabilities in terms of neutralising contamination from CBRN agents. The lack of modern technologies in this area is compensated for by the Alliance's capabilities in allied operations. However, it is necessary to consider what the consequences of these

[37] DD-3.14 (A) *Military protection*, Training 915/2015.

[38] Classified document.

[39] *Regulations for chemical forces of the land forces*...

[40] NATO Standard AJMedP-7 *Allied Joint Chemical, Biological, Radiological and Nuclear (CBRN) Medical Support Doctrine*, Edition B Version 1, 2022, https://www.coemed.org/files/stanags/02_AJMEDP/AJMedP-7_EDB_V1_E_2596.pdf [accessed: 28 VII 2025].

[41] NATO Standard AMedP-7.1 *Medical Management of CBRN Casualties*, Edition A Version 1, 2018, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.1_EDA_V1_E_2461.pdf [accessed: 28 VII 2025].

[42] NATO Standard AJMedP-7.3 *Training of Medical Personnel for Chemical, Biological, Radiological, and Nuclear (CBRN) Defence*, Edition A Version 1, 2016, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.3_EDA_V1_E_2954.pdf [accessed: 28 VII 2025].

shortcomings will be in the case of national operations or crisis response activities.

The development of modern technologies, including optoelectronic systems and equipment packed with electronics, requires innovative decontamination methods that exclude traditional wet methods, which can damage the decontaminated equipment and reduce its combat capability. Contemporary solutions in the field of decontamination are replacing older technologies to enable the treatment of modern equipment[43]. Technological trends are therefore influencing the need for organisational changes, tactics and operating procedures, forcing the restructuring of specialist subunits and the acquisition of new capabilities.

Financial and organisational conditions

The global trend of increasing defence spending is mainly due to the implementation of modern technologies. This also applies to Poland. Meanwhile, the funds allocated to the development of the Polish Armed Forces' decontamination subsystem are far from sufficient and mainly concern the maintenance of decontamination supplies. Expenditure on technological development remains close to zero[44]. In the area of acquiring new OPBMR technologies, the scale of this expenditure will not change significantly until 2026[45].

---

[43] NATO, Science and Technology Organization, *TR-HFM-233, Sensitive Equipment Decontamination*, 2017, https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-233/$$TR-HFM-233-ALL.pdf [accessed: 2 VIII 2025].

[44] The technical modernisation plans of the Polish Armed Forces (PMT) are classified documents, but their implementation is subject to control. One such control was carried out by the Supreme Audit Office (NIK) in 2017 in the area of the implementation of the state budget in 2016 in the part concerning national defence. See: Supreme Audit Office, Department of National Defence, *Information on the results of the audit of the implementation of the state budget in 2016 in part 29 – National Defence and the implementation of the financial plans of the Armed Forces Modernisation Fund and the Military Property Agency*, https://www.nik.gov.pl/plik/id,14141.pdf [accessed: 20 VII 2025]. The data from this report indicate that the level of funding for the entire area of Survival and Protection of Troops is 0.07% of the budget allocated for technical modernisation (item 11.1.5. Survival and Protection Capability, p. 33). This area includes purchases of equipment for the entire OPBMR system, which includes the decontamination subsystem. The data for 2016 in this regard does not differ significantly from the data for the years preceding and following the report.

[45] The modernisation priorities adopted by the Ministry of National Defence are publicly available. See: Ministry of National Defence, *Technical Modernisation Plan until 2026. Selected*

A report by the Ministry of National Defence from 2010–2011 emphasised the need to strengthen decontamination capabilities as an element of survival and protection of troops, and provided for improvements in equipment by 2018[46].

An analysis of the organisational conditions of the subsystem showed that while there were periods of prosperity during the years of transformation in the Polish Armed Forces, in most cases the chemical forces were subject to reductions.

An analogy can be found in planning processes. While in the 2009 Defence Strategy of the Republic of Poland, developed on the basis of the National Security Strategy of the Republic of Poland 2007, OPBMR was identified as one of the main functional systems[47], in 2011, in the Strategic Defence Review[48] OPBMR was classified as an element of survival and protection of the armed forces. On the basis of the 2012 Concept of Functional System Organisers and Decision No. 56/MON of 2013[49] responsibility for the OPBMR system was divided among various organisational entities of the Polish Armed Forces, without simultaneously indicating mechanisms for preparing personnel for the needs of the system[50]. This introduced organisational chaos, which hindered the development of the system, technology and integrated training.

---

issues, https://www.wojsko-polskie.pl/u/e1/aa/e1aa4b89-1045-4d1c-8a5c-7ffd4026e8d5/plan_modernizacji_technicznej_do_2026_r.pdf [accessed: 28 VII 2025]. The description refers to the period of the research. Since then, expenditure on technical modernisation has increased significantly, but this has not translated into technological development of the analysed subsystem.

[46] Ministry of National Defence, *Strategic Defence Review. Professional Armed Forces of the Republic of Poland in a modern state. Report*, Warszawa 2011, https://gdziewojsko.wordpress.com/wp-content/uploads/2011/05/raport_spo_14042011.pdf, p. 15 [accessed: 2 VIII 2025].

[47] *National Security Strategy of the Republic of Poland 2007*, https://www.bbn.gov.pl/ftp/dokumenty/SBN_RP.pdf [accessed: 2 VIII 2025]; Ministry of National Defence, *Defence Strategy of the Republic of Poland. Sectoral strategy for the National Security Strategy*, https://mkuliczkowski.pl/static/pdf/strategia_obronnosci.pdf, point 94, p. 19 [accessed: 2 VIII 2025].

[48] Ministry of National Defence, *Strategic Defence Review* ..., p. 93.

[49] General Staff of the Polish Armed Forces, Concept for the Establishment of Functional System Organisers approved by the Minister of National Defence on 19 October 2012 (unpublished); *Decision No. 56/Org./P5 of the Minister of National Defence of 24 December 2013 on Functional System Organisers of the Armed Forces of the Republic of Poland* (unpublished).

[50] General Staff of the Polish Army, Concept for establishing Organisers..., pp. 22–23.

In addition, the last decade has seen a growing trend towards the creation of expeditionary and multifunctional structures, such as task forces and chemical companies. In the case of the latter, this has not increased their existing specialist capabilities, but rather had a negative impact on the combat capabilities of the subunits.

Comparison of the Polish Armed Forces decontamination subsystem with NATO solutions

A comparison of the capabilities of the Polish Armed Forces' decontamination subsystem with similar subsystems of the armed forces of selected NATO countries reveals differences in technological, organisational and doctrinal approaches, as well as in the ability to cooperate with civil services in crisis response.

Germany

The main effort of the army

The Bundeswehr's efforts focus on providing comprehensive defence against CBRN threats in allied (NATO, European Union) and national operations, with an emphasis on crisis response, civil protection and support in stabilisation missions.

The ABC-Abwehrkommando der Bundeswehr, the command responsible for the OPBMR system in the German army, focuses on rapid detection, decontamination and neutralisation of threats, including asymmetric ones such as terrorism or industrial incidents. This reflects the resilience and interoperability emphasised in Germany's national defence strategy. The army supports authorities at the municipal, district, city, state and federal levels[51] in CBRN emergencies by integrating military capabilities with civilian structures.

Similarities between the German and Polish decontamination systems

The similarities stem from NATO membership, which requires compliance with the standards set out in the CBRN doctrine, i.e. a three-pillar approach

[51] See: H. Wyligała, *Uwarunkowania systemu zarządzania kryzysowego w Republice Federalnej Niemiec* (Eng. Conditions of the crisis management system in the Federal Republic of Germany), "Rocznik Bezpieczeństwa Międzynarodowego" 2011, vol. 5, pp. 133–154. https://doi.org/10.34862/rbm.2011.9.

and a focus on protecting personnel and equipment. In both countries, the decontamination subsystem is part of OPBMR, with an emphasis on the ability to secure troops in combined operations. Decontamination points are being developed in both armies. Although there are differences in the tactics used to develop them, the role of training troops in the procedures involved is emphasised, particularly at levels I and II, i.e. immediate and operational decontamination.

Differences between the German and Polish decontamination systems

- Organisational and functional – ABC-Abwehrkommando der Bundeswehr has centralised command in the area of OPBMR, which enables effective management of subordinate forces and development of the system[52]. Germany divides OPBMR capabilities into seven sub-areas[53], within which individual tasks are carried out at three levels of advancement: I – basic, II – advanced, III – qualified or specialised.
- Technological – Germany uses advanced decontamination systems, some of which integrate robotics and system automation.
- Doctrinal – in the German doctrine HDv 330/100[54], the OPBMR area has been integrated with civil protection, taking into account an active approach to decontamination (three phases: preliminary, operational, in-depth), and NATO guidelines (AJMedP-7) on the treatment of contaminated and infected casualties have been implemented.

Ability to cooperate with civil services

The cooperation between the Bundeswehr and civil services is based on constitutional provisions (German: *Grundgesetz für die Bundesrepublik*

[52] ABC-Abwehrkommando der Bundeswehr, https://www.bundeswehr.de/de/organisation/unterstuetzungsbereich/abc-abwehr-bundeswehr/abc-abwehrkommando-der-bundeswehr-in-bruchsal [accessed: 2 VIII 2025].

[53] These are: 1) individual protection, 2) collective protection, 3) medical defence against WMD, 4) contamination detection, 5) contamination removal (active), 6) specialist advice on OPBMR, 7) OPBMR technology compatibility.

[54] This is the equivalent of the Polish doctrine/regulations in the area of chemical forces command. See: *HDv 330/100 (zE) VS-NfD Führung der ABC-Abwehrtruppe*, 1999, https://www.scribd.com/document/58550605/HDv-330-100-Fuhrung-ABC-Abwehrtruppe [accessed: 3 VIII 2025].

Deutschland, GG)[55], which allows the use of the armed forces in crisis situations, e.g. during disasters, acts of terrorism, CBRN incidents, natural disasters, at the request of the federal authorities or the authorities of a given federal state. The military can carry out tasks such as decontamination (of people, vehicles and infrastructure), delivery of water and/or disinfectants, and medical and logistical support. In the Bundeswehr, interoperability is at a high level in terms of documentation, procedures (joint exercises) and equipment (compatible Kärcher equipment used by the military and civil services.

United States

The main effort of the army

The US military's efforts to combat WMD focus on global operations, expeditionary missions, counterterrorism, and support for civil authorities and services in their tasks (Defense Support of Civil Authorities, DSCA), with an emphasis on actively countering the proliferation of WMD outside the country, in accordance with the *National Security Strategy*[56].

The US 20th CBRNE Command integrates CBRN systems into joint operations, supporting the U.S. Army Forces Command (FORSCOM) and the U.S. Northern Command (USNORTHCOM)[57] in their activities.

Similarities between the American and Polish decontamination systems

Similarities include a three-pillar approach and a focus on protecting personnel and equipment. In both countries, joint operations place great emphasis on decontamination. The US Army, like the Polish Army, develops decontamination points in the field (as part of thorough decontamination) and conducts operational decontamination within six hours of contamination. It is extremely important for the military to decontaminate exposed skin (body) within one minute of contamination,

[55] See: Article 35(2) and (3) of the *Basic Law for the Federal Republic of Germany of 23 May 1949* (Grundgesetz für die Bundesrepublik Deutschland), https://biblioteka.sejm.gov.pl/wp-content/uploads/2016/02/Niemcy_pol_010711.pdf [accessed: 3 VIII 2025].

[56] *A New National Security Strategy for a New Era*, U.S. Embassy and Consulate in Poland, https://pl.usembassy.gov/pl/nss_pl/ [accessed: 11 XII 2019].

[57] USNORTHCOM is the primary military authority responsible for the defence of the continental United States, Alaska, Canada, Mexico, Cuba, the Bahamas, and adjacent waters. The command also provides support to civilian authorities within the United States. See: U.S. Northern Command, https://www.northcom.mil/ [accessed: 2 VIII 2025].

and other contaminated surfaces (e.g. weapons, personal equipment) within no more than 15 minutes[58].

Differences between the American and Polish decontamination systems

- Organisational and functional – The United States has a centralised command system in the area of CBRNE. The 20th CBRNE Command commands forces divided into the active army, reserves and National Guard. This allows for the flexible creation of task forces for expeditionary missions.

  Depending on the type of service, individual chemical warfare units and CBRN defence personnel are trained to varying degrees. The tasks of active army subunits include supporting the military in passive CBRN defence in assigned areas of responsibility (in areas of operations) and active operations to counter the proliferation of weapons of mass destruction (counterproliferation, CP[59]) and combat them (World Mass Destruction-elimination, WMD-E)[60]. In the Reserve Army, CBRNE forces are primarily prepared to carry out passive CBRN defence tasks, although they can also support operations to counter the proliferation of WMD or advise civilian services in the event of an incident involving WMD[61]. In turn, the forces comprising the National Guard are trained – like the entire armed forces – to carry out passive CBRN defence tasks, but since their main purpose is to serve within the country, this primarily involves crisis response in the broad sense. They support civil authorities within the country during events such as:
  – use or threat of use of WMD,
  – terrorist attack or threat of terrorist attack,

[58] See: FM 3-11 *Chemical, Biological, Radiological, and Nuclear Operations*, May 2019, https://irp.fas.org/doddir/army/fm3_11.pdf, p. Chapter 3 3-24 [accessed: 2 VIII 2025]; *FM 3-5, MCWP 3-37.3, NBC Decontamination*, 2000, https://www.globalsecurity.org/wmd/library/policy/army/fm/3-5/fm3-5.pdf, p. Introduction 1-3 [accessed: 2 VIII 2025].

[59] Joint Publication 3-40, *Joint Countering Weapons of Mass Destruction*, 2019, https://irp.fas.org/doddir/dod/jp3_40.pdf, p. GL-5 [accessed: 2 VIII 2025].

[60] M.F. Kelly, *United States Army Chemical, Biological…*

[61] This is handled, for example, by the 773rd Civil Support Team stationed in Kaiserslautern, Germany. See: *Army Reserve Component CBRN Units*, https://home.army.mil/wood/application/files/7315/9352/6705/UnitLocations.pdf [accessed: 2 VII 2025]; D. Friedberg, *U.S. Army North certifies the only Civil Support Team in Europe*, U.S. Army, 16 IX 2017, https://www.army.mil/article/193991/u_s_army_north_certifies_the_only_civil_support_team_in_europe [accessed: 2 VII 2025].

  - intentional or unintentional release of CBRN agents (including toxic industrial agents),
  - natural or man-made disasters that result or may result in catastrophe, loss of life or property.

  In the USA, level IV decontamination – clearance decontamination – is very well prepared in terms of planning and organisation.
- Technological – services in the USA use both older, proven technologies and modern ones, including those capable of decontaminating sensitive equipment. To this end, they use nanosorbents, enzymatic decontaminants and modern modular decontamination systems, including technology developed by Kärcher, such as the Kärcher Multipurpose Power Driven System (MPDS).

Ability to cooperate with civil services

Cooperation between the military and relevant services in the event of CBRN incidents, terrorist attacks, industrial toxic substance releases (TSP) and natural disasters involves decontamination, medical support, evacuation and logistical support (e.g. delivery of personal protective equipment). In the US, the army demonstrates a high degree of interoperability with civilian services, both in terms of documentation, procedures and equipment.

Conclusions from the comparison

Compared to Germany and the United States, the Polish Armed Forces lag behind in terms of technology, organisation and interoperability. Poland does not have integrated structures at the CBRNE command level, and its IRS-2 equipment does not meet the requirements of modern operations. The lack of regular exercises and insufficient cooperation with the civilian sector limit the capabilities of the subsystem.

Table 1. Comparison of the decontamination capabilities of Poland, Germany and the United States.

Country	Command structure/ responsibility for the system	Dominant technology	Interoperability	Cooperation with the civil sector
Poland	scattered	IRS-2, UG, Millagro	limited	weak
Germany	centralised (ABC-Abwehrkommando)	mobile kits (Kärcher Futuretech)	high	good
USA	centralised (20th CBRNE Command)	mobile kits (foam systems, unmanned vehicles)	high	very good

Source: own elaboration.

SWOT analysis of the Polish Armed Forces decontamination subsystem

SWOT analysis provides a concise overview of the strengths and weaknesses of the Polish Armed Forces' decontamination subsystem, as well as the opportunities and threats to its development. Table 2 illustrates the current capabilities and shortcomings.

Strengths

- well-educated and experienced personnel capable of cooperating in the development of modern CBRN technologies, including in the area of decontamination. Poland has, among other things, well-trained personnel in key chemical units – the Chemical Troops are well regarded among NATO partners. In this respect, Poland is one of the main pillars of NATO's CBRN defence system,
- existing infrastructure that can be adapted as stationary decontamination points (PLSk) in major garrisons,
- NATO membership, which provides access to allied experience and standards, which in turn helps to achieve interoperability, supports problem solving within the Lessons Learned system, forces the development of new capabilities, and indicates directions for the development of new technologies;

Weaknesses

- equipment and technology – outdated equipment with significant deficiencies in the required capabilities for decontaminating sensitive equipment, high-infrastructure facilities, aircraft interiors, external surfaces of large C-130 aircraft, ship interiors, contaminated casualties,
- organisational, technological and tactical inconsistencies with officially applicable manuals and instructions,
- lack of research confirming the ability of the technology used to decontaminate new-generation agents,
- lack of full compliance with NATO procedures and standards, particularly in the area of clearance decontamination,
- limited financial resources for the modernisation and development of decontamination technology,
- dispersion of the authorities responsible for the functioning and development of the OPBMR system, including the decontamination subsystem – lack of centralised command, a substantive system creator, and a decision-maker in the field of implemented and developed technologies.

Opportunities

- ability to focus efforts on acquiring key capabilities that determine the readiness of forces to take action, based on identified gaps and shortcomings,
- possibility of obtaining funds (including those from the EU) for the development and modernisation of equipment, technology and infrastructure in the area of decontamination,
- international cooperation within NATO, including participation in exercises, missions and exchange of experience in the area of technologies and tactics used,
- development of cooperation with the National Rescue and Firefighting System (KSRG) and civil services (formations) in the area of decontamination (hazard removal) in order to increase the effectiveness of response – development of solutions, including uniform standards to enable joint implementation of tasks in military operations (national and allied) and in crisis response, which will allow for the development and use of dual-use technologies and more effective management of allocated financial resources, while increasing rescue capabilities in both peacetime and wartime.

Threats

- increased hybrid threats, including the use of new-generation chemical and biological agents,
- slower pace of modernisation compared to other NATO countries in the area of decontamination,
- potential staff shortages resulting from insufficient training and inappropriate personnel policy in the chemical forces.

Table 2. Capabilities and shortcomings of the Polish Armed Forces decontamination subsystem – summary.

Survival and protection of troops Defence against WMD Contamination elimination					
Classification			**Yes**	**Yes, but with restrictions**	**No**
PEOPLE	**healthy contaminated**			– no possibility of collecting waste after procedures, – disinfectants for equipment and personal equipment do not meet environmental protection requirements	
	injured contaminated				X
EQUIPMENT	**combat**	**armoured**		– disinfectants do not meet environmental protection requirements, – inability to eliminate contamination inside the equipment	
		unarmoured		– disinfectants do not meet environmental protection requirements, – inability to eliminate contamination inside the equipment	
		weaponry		– disinfectants do not meet environmental protection requirements, – inability to eliminate contamination inside the equipment	
	sensitive	**optical**			X
		electronic			X
		special ammunition			X

Survival and protection of troops Defence against WMD Contamination elimination					
Classification			**Yes**	**Yes, but with restrictions**	**No**
EQUIPMENT	**ships**	**inside**			X
		outside		disinfectants do not meet environmental protection requirements	
	aircraft	**inside**			X
		outside		– lack of appropriate decontaminants, – lack of capacity to decontaminate large aircraft	
FACILITIES	**vertical**				X
	horizontal			disinfectants do not meet environmental protection requirements	
TERRAIN	**hardened**			disinfectants do not meet environmental protection requirements	
	unhardened				
WATER SUPPLY				no tanks with filling equipment and water pre-treatment system	
CHEMICAL RESCUE	**contamination reduction**		X		

Source: own elaboration.

Areas for improvement of the Polish Armed Forces decontamination subsystem

Based on literature, comparative analysis and examples, the author proposes the following directions for change.

1. **Technical modernisation**
   1) immediate acquisition and implementation of modern decontamination technologies in the armed forces, including for:
      – sensitive equipment,
      – aircraft,
      – ship interiors,
      – vertical facilities,
      – casualties,
   2) increasing the capacity to decontaminate personnel and essential combat equipment,
   3) introducing robotisation in the area of decontamination in order to increase personnel safety.
2. **Operational standardisation**
   1) aligning all procedures with NATO standards, including introducing clearance decontamination as an operational standard,
   2) continuously updating doctrines and doctrinal documents to include the area of OPBMR,
   3) integrating chemical warfare units into an integrated battlefield system that ensures the ability to respond to incidents in real time.
3. **Development of training programmes**
   1) implementation of regular, interdisciplinary exercises involving chemical units, civil services and NATO allies,
   2) development of specialist courses on the operation of modern decontamination systems and response to CBRN incidents in cooperation with civilian formations.
4. **Integration with the non-military system**
   1) strengthening cooperation with the National Firefighting and Rescue System, the Police, the Border Guard and other services, including the Internal Security Agency, in order to develop common standards and procedures for responding to CBRN incidents in the civilian environment and securing

NATO forces in a potential allied operation on the territory of the country,

2) establishing joint crisis response teams comprising subunits of the Polish Armed Forces (including chemical troops) and civilian formations capable of responding to incidents involving CBRN agents.

5. **Centralisation of organisational structures**
   1) creating a central command/ organisational unit to manage OPBMR, modelled on the American 20th CBRNE Command or the German ABC-Abwehrkommando der Bundeswehr, which would have the capacity to identify operational needs for the entire Polish Armed Forces, coordinate the development of the OPBMR system, including the decontamination subsystem, and the activities of chemical units in the Polish Armed Forces,
   2) optimising the deployment of infrastructure capable of functioning as stationary and mobile PLSk, to increase operational flexibility.
6. **Increasing funding**
   1) involving EU and national funds in modernisation programmes, including the purchase of new equipment and decontamination technologies, and the development of infrastructure in the field of OPBMR,
   2) prioritising the decontamination subsystem in defence budgets in order to overcome the technological slump.

Perspectives for further development

Further research on the Polish Armed Forces decontamination subsystem should focus on the following areas:

- development of technologies to neutralise new-generation chemical and biological agents, such as Novichok or modified pathogens,
- optimisation of organisational models, including the impact of centralised command on the effectiveness of operations,
- expansion of international cooperation, e.g. through joint research projects with NATO or the EU,

– analysis of the impact of climate change and local armed conflicts on potential CBRN threats, e.g. the impact of migration on the increase in biological threats.

Summary and conclusions

The Polish Armed Forces' decontamination subsystem plays an important role in countering chemical, biological and radioactive threats, but its effectiveness is limited. Factors that contribute to this and require urgent corrective action include outdated equipment, lack of full interoperability with NATO, insufficient training and limited cooperation with the civilian sector. This points to the need for comprehensive change, including:

– introduction of modern decontamination technologies,
– achievement of full interoperability with NATO forces and civil services,
– development of training programmes and cross-sector cooperation,
– centralisation of organisational structures and increased funding.

The implementation of these solutions should create conditions for increasing the operational readiness of the Polish Armed Forces, strengthening national security and more effective cooperation with allies within NATO.

Bibliography

NATO Glossary of Terms and Definitions AAP-6(2014) – (item available after logging into the NATO Standardization Office system).

NATO Glossary of Terms and Definitions for Chemical, Biological, Radiological and Nuclear Threats AAP-21(B) – (item available after logging into the NATO Standardization Office system).

Okumara T., Takasu N., Ishimatsu S., Kumada K., Tanaka K., Hinohara S., *Report on 640 Victims of the Tokyo Subway Sarin Attack*, "Annals of Emergency Medicine" 1996, vol. 26, no. 2, pp. 129–135. https://doi.org/10.1016/S0196-0644(96)70052-5.

Steindl D., Boehmerle W., Korner R., Preager D., Haug M., Nee J., Schreiber A., Scheibe F., Demin K., Jacoby P., Tauber R., Hartwig S., Endres M., Eckardt K-U.,

Novichok nerve agent poisoning, "The Lancet" 2021, vol. 397, no. 10270, pp. 249–252. https://doi.org/10.1016/S0140-6736(20)32644-1.

Wyligała H., *Uwarunkowania systemu zarządzania kryzysowego w Republice Federalnej Niemiec* (Eng. Conditions of the crisis management system in the Federal Republic of Germany), "Rocznik Bezpieczeństwa Międzynarodowego" 2011, vol. 5, pp. 133–154. https://doi.org/10.34862/rbm.2011.9.

Internet sources

A New National Security Strategy for a New Era, U.S. Embassy and Consulate in Poland, https://pl.usembassy.gov/pl/nss_pl/ [accessed: 11 XII 2019].

ABC-Abwehrkommando der Bundeswehr, https://www.bundeswehr.de/de/organisation/unterstuetzungsbereich/abc-abwehr-bundeswehr/abc-abwehrkommando-der-bundeswehr-in-bruchsal [accessed: 2 VIII 2025].

Alexander Litvinenko: Profile of murdered Russian spy, BBC News, 21 I 2016, https://www.bbc.com/news/uk-19647226 [accessed: 26 VII 2025].

Army Reserve Component CBRN Units, https://home.army.mil/wood/application/files/7315/9352/6705/UnitLocations.pdf [accessed: 25 IX 2019].

BI-SC Capability Codes and Capability Statements, 26 I 2016, https://www.scribd.com/document/382349178/Capability-Codes-and-Capability-Statements-2016-Bi-sc-Nu0083 [accessed: 2 VIII 2025].

FM 3-11 *Chemical, Biological, Radiological, and Nuclear Operations*, May 2019, https://irp.fas.org/doddir/army/fm3_11.pdf [accessed: 2 VIII 2025].

FM 3-5, *MCWP 3-37.3, NBC Decontamination Operations*, 2000, https://www.globalsecurity.org/wmd/library/policy/army/fm/3-5/fm3-5.pdf [accessed: 2 VIII 2025].

Friedberg D., *U.S. Army North certifies the only Civil Support Team in Europe*, U.S. Army, 16 IX 2017, https://www.army.mil/article/193991/u_s_army_north_certifies_the_only_civil_support_team_in_europe [accessed: 2 VII 2025].

Gardner F., *Navalny 'Novichok poisoning' a test for the West,* BBC News, 2 IX 2020, https://www.bbc.com/news/world-europe-54003014 [accessed: 1 VIII 2025].

Joint Publication 3-40, Joint Countering Weapons of Mass Destruction, 2019, https://irp.fas.org/doddir/dod/jp3_40.pdf [accessed: 2 VIII 2025].

Kelly M.F., *United States Army Chemical, Biological, Radiological and Nuclear Corps Capability for Combating the Contemporary Weapons of Mass Destruction Threat*,

Master's Thesis, Fort Leavenworth, Kansas 2012, https://apps.dtic.mil/sti/tr/pdf/ADA563129.pdf [accessed: 2 VII 2025].

Kim Jong-nam killing: 'VX nerve agent' found on his face, BBC News, 24 II 2017, https://www.bbc.com/news/world-asia-39073389 [accessed: 26 VII 2025].

Ministry of National Defence, *Technical Modernisation Plan until 2026. Selected issues*, https://www.wojsko-polskie.pl/u/e1/aa/e1aa4b89-1045-4d1c-8a5c-7ffd4026e8d5/plan_modernizacji_technicznej_do_2026_r.pdf [accessed: 28 VII 2025]

Ministry of National Defence, *Strategic Defence Review. Professional Armed Forces of the Republic of Poland in a modern state. Report*, Warszawa 2011, https://gdziewojsko.wordpress.com/wp-content/uploads/2011/05/raport_spo_14042011.pdf [accessed: 2 VIII 2025].

Morris S., *UK believes Putin personally authorized Salisbury novichok attack, inquiry told*, The Guardian, 14 X 2024, https://www.theguardian.com/uk-news/2024/oct/14/salisbury-novichok-poisonings-inquiry-sergei-skripal-vladmir-putin [accessed: 25 VII 2025].

NATO Standard AJMedP-7 *Allied Joint Chemical, Biological, Radiological and Nuclear (CBRN) Medical Support Doctrine*, Edition B Version 1, 2022 https://www.coemed.org/files/stanags/02_AJMEDP/AJMedP-7_EDB_V1_E_2596.pdf [accessed: 3 VIII 2025].

NATO Standard AJMedP-7.1 *Medical Management of CBRN Casualties*, Edition A Version 1, 2018, NATO Standard AJMedP-7 https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.1_EDA_V1_E_2461.pdf [accessed: 3 VIII 2025].

NATO Standard AJMedP-7.3 *Training of Medical Personnel for Chemical, Biological, Radiological, and Nuclear (CBRN) Defence*, Edition A Version 1, 2016, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-7.3_EDA_V1_E_2954.pdf [accessed: 3 VIII 2025].

NATO Standard AJP-3.8 *Allied joint doctrine for chemical, biological, radiological, and nuclear defence*, Edition A Version 1, 2012 https://assets.publishing.service.gov.uk/media/5bf40787ed915d18301589b4/archive_doctrine_nato_cbrn_defence_ajp_3_8.pdf [accessed: 3 VIII 2025].

NATO, Science and Technology Organization, *TR-HFM-233, Sensitive Equipment Decontamination*, 2017, https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-233/$$TR-HFM-233-ALL.pdf [accessed: 2 VIII 2025].

OPCW Issues Report on Technical Assistance Requested by Germany, OPCW, 6 X 2020, https://www.opcw.org/media-centre/news/2020/10/opcw-issues-report-technical-assistance-requested-germany [accessed: 1 VIII 2025];

OPCW issues report on third Technical Assistance Visit to Ukraine following an incident of alleged use of toxic chemicals as a weapon, OPCW, 26 I 2025, https://www.opcw.org/media-centre/news/2025/06/opcw-issues-report-third-technical-assistance-visit-ukraine-following [accessed: 26 VI 2025].

Pletcher K., *Tokyo subway attack of 1995*, Britannica, 8 V 2025, https://www.britannica.com/event/Tokyo-subway-attack-of-1995 [accessed: 25 VII 2025].

Rozproszenie gazu sarin w Tokio (Eng. The sarin gas attack in Tokyo), Terroryzm!com, 26 XII 2006, http://www.terroryzm.com/rozproszenie-gazu-sarin-w-tokio/ [accessed: 25 VII 2025].

Salisbury declared decontaminated after Novichok poisoning, BBC, 1 III 2019, https://www.bbc.com/news/uk-england-wiltshire-47412390 [accessed: 10 III 2019].

Supreme Audit Office, Department of National Defence, *Information on the results of the audit of the implementation of the state budget in 2016 in part 29 – National Defence and the implementation of the financial plans of the Armed Forces Modernisation Fund and the Military Property Agency*, https://www.nik.gov.pl/plik/id,14141.pdf [accessed: 20 VII 2025].

Syria: BBC Investigation Reveals Widespread Chemical Weapons Use, BBC,https://www.bbc.co.uk/programmes/w172w25d6yyjrc0 [accessed: 25 X 2018].

The Lab: How FSB chemical weapons experts tried to poison Alexei Navalny, The Insider, 14 XII 2020, https://theins.ru/en/politics/262611 [accessed: 1 VIII 2025].

U.S. Northern Command, https://www.northcom.mil/ [accessed: 2 VIII 2025].

Vladimir Kara-Murza Tailed by Members of FSB Squad Prior to Suspected Poisonings, Bellingcat, 11 II 2021, https://www.bellingcat.com/news/2021/02/11/vladimir-kara-murza-tailed-by-members-of-fsb-squad-prior-to-suspected-poisonings/ [accessed: 1 VIII 2025].

Zabójstwo Aleksandra Litwinienki (Eng. The murder of Alexander Litvinenko), in: Konsorcjum Mall-CBRN, *Podręcznik zapobiegania i reagowania na zdarzenia CBRNE w centrach handlowych*, https://www.uni.lodz.pl/fileadmin/Projekty/MALL-CBRN/Materials_available_for_download_/Mall-CBRN-Handbook-PL-1.0.pdf, pp. 24–25 [accessed: 2 VIII 2025].

Legal acts

Basic Law for the Federal Republic of Germany of 23 May 1949 (*Grundgesetz für die Bundesrepublik Deutschland*), https://biblioteka.sejm.gov.pl/wp-content/uploads/2016/02/Niemcy_pol_010711.pdf [accessed: 3 VIII 2025].

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, drafted in Paris on 13 January 1993 (Journal of Laws of 1999, No. 63, item 703).

Regulation of the Council of Ministers of 25 March 2025 on the preparation of the national security management system (Journal of Laws of 2025, item 407).

Regulation of the Council of Ministers of 27 April 2004 on the preparation of the national security management system (Journal of Laws of 2004, No. 98, item 978).

Other documents

DD-3.14 (A) *Military protection*, Training. 915/2015.

Decision No. 56/MON of the Minister of National Defence of 8 March 2013 amending the decision on the introduction of a methodology for supplying professional soldiers with uniforms and equipment, calculating cash equivalents for these items, and monitoring the prices of these items and services (Journal of Laws of the Ministry of National Defence of 2013, item 64).

Decision No. 56/Org./P5 of the Minister of National Defence of 24 December 2013 on the Organisers of Functional Systems of the Polish Armed Forces (unpublished).

Decision No. 95/MON of the Minister of National Defence of 27 February 2007 on the introduction of the 'Guidelines for Conducting an Operational Needs Review' (Journal of Laws of the Ministry of National Defence of 2007, No. 5, item 67).

Defence against weapons of mass destruction in combined operations DD/3.8(A), training. 869/2013 (item made available by the Ministry of National Defence).

General Staff of the Polish Armed Forces, Concept for the establishment of Functional System Organisers approved by the Minister of National Defence on 19 October 2012 (item made available by the Ministry of National Defence).

HDv 330/100 (zE) VS-NfD Führung der ABC-Abwehrtruppe, 1999, https://www.scribd.com/document/58550605/HDv-330-100-Fuhrung-ABC-Abwehrtruppe [accessed: 3 VIII 2025].

Leosz A., Sawczak S., *Sprzęt likwidacji skażeń* (Eng. Decontamination equipment), WSO–TK internal 57/96 (in the archives of the Land Forces Academy, item made available by the Ministry of National Defence).

Ministry of National Defence, *Defence Strategy of the Republic of Poland. Sectoral strategy for the National Security Strategy*, https://mkuliczkowski.pl/static/pdf/strategia_obronnosci.pdf [accessed: 2 VIII 2025].

National Security Strategy of the Republic of Poland 2007, https://www.bbn.gov.pl/ftp/dokumenty/SBN_RP.pdf [accessed: 2 VIII 2025].

NO-01-A006:2010 Defence against weapons of mass destruction. Terminology (document at the Military Centre for Standardisation, Quality and Codification).

Regulations for chemical forces of the land forces, DWLąd. Internal 183/2011.

Sanitary procedures and special procedures for weapons and combat equipment, Chemical Manual 278/79 (item made available by the Ministry of National Defence).

Special treatments for terrain and field defence structures, Ref. No. 1984 Chem. 321, Warszawa 1985 (item made available by the Ministry of National Defence).

Colonel (ret.) Krzysztof Tokarczyk, PhD

Colonel retired, Doctor of Social Sciences in the field of security studies. Expert at the Stratpoints Foundation. Former officer of the chemical forces, ending his service in the Polish Armed Forces as chief of division – deputy chief of the operations directorate of the General Command of the Armed Forces. He specialises in the field of decontamination. Author of several guides for the Armed Forces, developed as part of the Lessons Learned System, and co-author of several manuals and handbooks on defence against weapons of mass destruction.

Contact: ktokarczyk1@wp.pl

VARIA

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 487–516

https://doi.org/10.4467/27204383TER.25.062.23049

Varia

How can local governments protect public spaces from vehicle attacks?

Mariusz Cichomski

Ministry of the Interior and Administration

https://orcid.org/0000-0003-3707-7856

Since 16 April 2022, alert BRAVO[1], the second level on a four-level scale, has been in force throughout Poland. Alert levels are introduced on the basis of the *Act of 10 June 2016 on anti-terrorist activities* in the event of a threat of a terrorist incident or the occurrence of such an incident. The second alert level is introduced in the event of an increased and predictable threat of a terrorist incident, but where no specific target has been identified[2].

The introduction of the BRAVO alert was a preventive measure. It was caused by the geopolitical situation in the region related to various activities typical of a hybrid attack carried out by the Russian Federation

[1] The BRAVO alert from 6 October 2022 also applies to Polish energy infrastructure located outside of the borders of the Republic of Poland. From 19 November 2025, a third alert level (CHARLIE) was introduced on railway lines managed by PKP PLK and PKP LHS. In addition, a second alert level for cyber threats (BRAVO-CRP) has been introduced, effective as of 1 March 2024. Previously, i.e. from 21 February 2022 to 29 February 2024, the third alert level CHARLIE-CRP was in force, and from 15 February 2022 to 21 February 2022, the first alert level ALFA-CRP was in force.

[2] Article 15(4) of the *Act of 10 June 2016 on anti-terrorist activities*.

and Belarus against Poland and other European Union countries, as well as the consequences of Russia's armed attack on Ukraine. As the Ministry of the Interior and Administration points out, (...) *alert levels are primarily a signal to security services and the entire public administration to remain particularly vigilant*[3].

The legal instrument of introducing alert levels had been used before, but in 2022 both the reasons for and the effects of this measure differed from previous cases. This time, the alert levels were not introduced in connection with the organisation of a specific event, such as state ceremonies, international meetings or elections, but as a consequence of events beyond the control of the Polish authorities and in response to direct intentional actions by other states. The first element of the aforementioned hybrid attack was the migration crisis on the Polish-Belarusian border, which is also the external border of the EU. It was artificially caused by the Belarusian authorities in cooperation with the authorities of the Russian Federation. Over time, hybrid activities began to take other forms, such as testing the resilience of Polish critical infrastructure, setting fire to shops and warehouses or cyber attacks and attacks on railway infrastructure, posing a direct threat to human life and health.

Another significant difference from previous cases of alert levels being declared is their duration. Previously, they were introduced for a short period of time in response to a specific event. This time, they have been in force continuously for over three years, and it is difficult to assess when they will be lifted[4]. As a result, the relevant services, public administration bodies and other entities whose work is affected by alert levels are required to maintain a heightened state of readiness for a long period of time and to implement specific measures in this regard. This is also an opportunity to verify the correctness and adequacy of existing regulations and procedures, as well as a key moment for implementing mechanisms to prevent threats or minimise their effects.

[3] *Stopnie alarmowe BRAVO i BRAVO-CRP na terenie całego kraju wciąż obowiązują* (Eng. BRAVO and BRAVO-CRP alert levels still in force throughout the country), Serwis Rzeczypospolitej Polskiej, 29 VIII 2025, https://www.gov.pl/web/mswia/stopnie-alarmowe-bravo-i-bravocrp-na-terenie-calego-kraju-wciaz-obowiazuja3 [accessed: 11 X 2025].

[4] M. Cichomski, I. Idzikowska-Ślęzak, *Alert levels – practical and legal dimensions of their use*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 245–251. https://doi.org/10.4467/27204383TER.22.025.16345.

Regardless of the reasons for introducing alert levels in Poland, it remains necessary to continuously analyse terrorist attacks that have occurred in other countries, and identify on this basis potential targets for such attacks. This analysis cannot be limited to threats specific to hybrid activities, but should take into account a broader context not only related to regional conditions.

In the current circumstances, it is important to take measures aimed at preventing terrorist incidents or minimising their effects should they occur. Pursuant to Art.3(2) of the Act on anti-terrorist activities: *the minister competent for internal affairs is responsible for preparing to take control of terrorist incidents through planned measures, responding to such incidents when they occur, and restoring the resources used to respond to them*. It should be emphasised that these measures do not have to be implemented directly by the minister responsible for internal affairs. It remains important to initiate them or support other authorities that undertake the responsibility of preparing for threats of a terrorist nature.

The minister responsible for internal affairs chairs the Interministerial Team for Terrorist Threats. The team's tasks include initiating, coordinating and monitoring activities undertaken by the relevant government authorities in the field of preparedness for preventing terrorist incidents, taking control of them through planned measures and responding to them[5]. The role of the chairperson is therefore linked to statutory responsibility for the preparation phase for terrorist incidents, as well as being part of the overall responsibility for security and public order.

One of the methods of terrorist attacks already used in various countries, including the states of the European Union, is the use

[5] See: § 2(2) point 3 of the *Ordinance No. 162 of the Prime Minister of 25 October 2006 on creation of the Interministerial Team for Terrorist Threats*. Current legal status: *Order No. 162 of the Prime Minister of 25 October 2006 on the creation of the Interministerial Team for Terrorist Threats*, amended by Order No. 95 of the Prime Minister of 4 September 2008, Order No. 74 of the Prime Minister of 21 September 2009, Order No. 18 of the Prime Minister of 3 April 2014, Order No. 84 of the Prime Minister of 18 September 2015, Order No. 86 of the Prime Minister of 5 July 2016, Order No. 32 of the Prime Minister of 27 April 2017, Order No. 160 of the Prime Minister of 9 November 2017, Order No. 92 of the Prime Minister of 7 June 2018 and Order No. 37 of the Prime Minister of 8 April 2021. Cf. M. Cichomski, I. Idzikowska-Ślęzak, *Strategic level of the Polish anti-terrorist system – 15 years of the Interministerial Team for Terrorist Threats*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 1, pp. 297–319. DOI: 10.4467/27204383TER.22.011.15427.

of a ramming vehicle. The use of a vehicle to attack people in urban spaces is one of the most serious threats in urban spaces, if only because of the high availability of this tool. Preventing such incidents is not solely the responsibility of services. In the case of open and mass events organised in public spaces, responsible for their security, especially in terms of infrastructure, which can be used to increase the security level of a given undertaking, is primarily the responsibility of local authorities.

Therefore, a document entitled: *Protecting public spaces from vehicle attacks – recommendations for local authorities* was prepared on the initiative of the Minister of the Interior and Administration. It was developed by police experts in cooperation with the Ministry of the Interior and Administration as well as the Internal Security Agency, drawing on the experiences of other states. Recommendations are intended to be helpful both in planning investments aimed at ensuring the security of public spaces, e.g. automatic anti-terrorist barriers or other fixed structures, and in the improvement of technical and architectural solutions already in use. The document was prepared in September 2025 and forwarded to provincial city mayors and provincial governors for further distribution to local authorities.

As indicated in the recommendations many technical and architectural solutions are currently available on the market, ranging from parking bollards and obstacles in the form of street furniture elements to certified road barrier systems that can minimise or even eliminate the risks associated with the use of a ramming vehicle. The effectiveness of these measures usually increases with the cost of their purchase and maintenance. Therefore, decisions in these matters must serve to ensure the highest possible level of protection within the available resources, including the effective use of law enforcement services, and must be adequate to the threats.

Recommendations include, among other things, the characteristics of threats involving the use of ramming vehicle, a description of the process of planning security measures for various public spaces, infrastructural and architectural protective measures, as well as possible forms of integrating security measures into urban architecture or the possibility of using temporary security measures and other existing architectural elements as barriers. The document also describes the role of local law enforcement services (municipal and communal guards)

as well as formal safety requirements for contractors and employees performing activities related to anti-terrorist barrier access control systems or their integration.

It is worth noting that recommendations include various types of public spaces that may become targets for vehicle-borne terrorist attacks, such as marketplaces and town squares, pedestrian zones and promenades, venues for mass events, as well as public spaces of a universal nature.

The document is not normative in nature, and therefore its use will depend on the willingness and capabilities of local authorities. The guidelines contained therein can be adapted to local conditions[6].

Mariusz Cichomski

Lawyer, sociologist. He works on issues related to terrorism, organised crime, oversight of service activities, security legislation and issues related to the application of national restrictive measures. He is the author of more than 30 publications on security, particularly in the legal dimension, and on sociology.

[6] We publish the document on the following pages as an attachement to the text (editor's note).

Protecting public spaces from vehicle attacks – recommendations for local governments[1]

Introduction

The threat posed by attacks using vehicles, so-called vehicle-ramming attacks to run people over, is currently one of the reasons for the growing number of incidents of a terrorist nature. Attacks of this kind have been carried out in Europe and around the world for many years, and recently there has been an increase in their frequency and in the number of fatalities. An example is the incident that took place in Nice in July 2016 during the celebrations of the national holiday of France, when a truck driven by an attacker rammed through barriers and drove into people on the promenade, killing 87 people and injuring another 434. Similar attacks were carried out in other major cities in Europe and America, including in Berlin, Barcelona, London, Stockholm, New York, Toronto. Poland is a safe country, but terrorist incidents are also possible in our country, which is why it is necessary to take preventive measures or measures to minimise the effects of possible attacks.

It should be noted that a vehicle-ramming attack is a relatively easily accessible tool. Even an ordinary passenger vehicle can cause numerous casualties and trigger mass panic. On the other hand, this type of threat has led to the development of numerous architectural and technical solutions. These include various types of security measures, ranging from simple parking posts considered to be order maintenance measures, through small architecture obstacles capable of stopping vehicles, to certified road barrier systems offering the highest level of security. Due to the variety of available solutions, choosing the right one is not a simple matter. On the one hand, it depends on the type of facilities or the layout of the space that would be protected, and on the other hand, it often depends on the size of the budget allocated for this purpose.

[1] The Polish version is the original version of the document. Only changes to the graphic layout of the table were made. Translation provided by the editorial team (editor's note).

In summary, the use of a vehicle as a means of carrying out a terrorist attack is becoming a phenomenon that is part of the current picture of urban threats, if only because of the relatively simple mechanism of action of their perpetrators. The openness and accessibility of urban spaces make it impossible to completely eliminate the risk of vehicle attacks, but proper infrastructure planning can significantly hinder their execution and minimise their impact. In particular, this refers to infrastructure that can be used in such situations to increase the security level of a given public project, as well as being appropriately integrated into the resources of law enforcement services, including, for example, municipal guards.

These recommendations have been developed by the Police, in cooperation with the Ministry of the Interior and Administration and the Internal Security Agency, with concern for the safety of Polish cities and towns, and are intended to serve as a practical guide based on expert experience and international best practices (including those from the United Kingdom, Germany and the Netherlands). They are based on proven solutions used in other countries and specialist knowledge, without referring to detailed local risk analyses. The aim of this study is to present universal principles that every municipality, regardless of its size and budget, will be able to adapt to its own conditions in order to prevent or mitigate the effects of a vehicle attack.

The purpose of addressing this document to city and municipality authorities is that its contents will prove useful in making often difficult decisions regarding ways to protect public spaces, both in terms of future investment processes and in the context of developing existing resources.

Scope and application of recommendations

Recommendations include various types of **public spaces** that could become targets for attacks using speeding vehicles. This applies in particular to:

- **market squares and town squares** – central gathering places (e.g. market square, squares in front of town halls), often used for fairs, gatherings or special events,
- **pedestrian zones and areas** – streets closed to traffic, where pedestrians gather every day (shopping streets, promenades),

- **places of mass events** – areas where concerts, festivals, sporting events, etc. take place, both permanent (stadiums, esplanades) and temporarily arranged (e.g. streets closed for the duration of a street race),
- **public spaces of a universal nature** – e.g. parks, squares, boulevards, recreational and tourist areas, which are open by nature and can accommodate large groups of people.

For each of the above categories of space, typical **threats and challenges** as well as **appropriate countermeasures** have been identified. The document focuses on **infrastructural and architectural protective solutions** – such as physical barriers (fixed and automatic), posts, guardrails or specially designed elements of street furniture that serve a protective function. Furthermore, **methods of temporarily securing** spaces during periods of increased risk (e.g. during mass events) using portable barriers and other available means were discussed. Recommendations also define **the tasks of local security services** (municipal/communal guards) in supporting these security measures and address **legal and organisational aspects** necessary for the effective implementation of measures (division of responsibilities, cooperation with private entities, compliance with regulations).

Note: Recommendations should be treated as a starting point – they should be adapted to local conditions (urban layout, scale of risk, available financial resources). Where possible, a range of solutions has been indicated, from simple and low-cost to advanced and more costly, in order to facilitate their implementation in different municipalities.

Characteristics of a vehicle attack

Before we move on to solutions, it is worth understanding the specific nature of the threat:

- **Element of surprise:** A vehicle attack can occur **suddenly and without warning**, anywhere where there is a crowd. The perpetrator may use a passenger car, van or lorry – including a rented or stolen vehicle – which makes it difficult to detect their intentions in advance[2].

[2] https://www.rand.org/randeurope/research/projects/2022/preventing-and-mitigating-terrorism-attacks-using-vehicles.html#:~:text=The%20frequency%20of%20vehicle,such%20attacks%20in%20the%20future

- **High destructive power:** A vehicle travelling at high speed (even a medium-sized one) can cause serious casualties. A lorry weighing several tonnes travelling at high speed can ram obstacles and victims over a distance of several dozen metres[3].
- **Multiple potential targets:** There are many places where people gather, from shopping streets to outdoor events. It is impossible to secure literally every place at all times, so efforts are focused on **the most vulnerable locations** (city centres, pedestrian zones, public facilities) and **events that attract large crowds**.
- **Technical measures limitations:** Available security measures can **hinder or prevent** an attack, but they do not guarantee complete protection. Even solid barriers have their limits, and an attacker may find a vulnerability (e.g. an unsecured entrance). During crash tests, one of the parameters taken into account when checking the effectiveness of a security measure is the so-called penetration, which determines how far beyond the barrier line a vehicle can travel. Once this parameter is known, it must be taken into account when designing the distance between the barrier and the protected objects or pedestrian and vehicle routes. That is why it is important to have **a well-thought-out plan for the placement** of barriers – decisions on where to place them leave no room for error[4].
- **Psychological impact:** The presence of security measures affects the sense of safety of residents and visitors. Efforts should be made **to mitigate the 'bunker syndrome'**, i.e. avoid transforming the city into a visible fortress, which could cause anxiety. The solutions should be **discreetly integrated** into the urban space so that people can feel at ease, without even realising that they are being protected. As experts emphasise, **maintaining the open character of the city** is important – we do not want fear to dictate the appearance of our streets.

When determining the types of risk for a specific location, both the threat and the potential consequences of an incident should be taken

[3] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrier

[4] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=helped%20prevent%20Saturday%27s%20attack%20because,among%20those%20to%20be%20protected

into account, as well as the vulnerability of the location to an attack using a vehicle as a means of carrying it out[5].

Knowing these conditions, local governments can approach the problem realistically: **risk reduction instead of total elimination**. The aim is to transform and manage public spaces in such a way that a potential attacker encounters **physical barriers that delay or prevent** them from achieving their goal, and that the services have a chance to react before the greatest damage is done. Below are specific recommendations on how to achieve this.

Planning security measures in various public spaces

The nature and layout of a space influence the choice of security measures. Below are descriptions of key types of locations and recommended approaches to securing them against the entry of dangerous vehicles:

- **Markets and town squares:** Open squares are often surrounded by streets from which vehicles can potentially enter. **Fixed barriers around the perimeter of the square** (e.g. rows of posts, low walls, heavy planters) form the first line of defence, protecting people in the centre. Attention should be paid to securing the main **entrances to the square** – it is worth installing **fixed or automatic barriers** there to prevent unauthorised vehicles from entering. If the square is occasionally used as a car park or delivery point, **retractable bollards** can be used, which are opened to allow authorised vehicles to pass. When planning new squares, it is recommended to **design access roads with safety in mind** – e.g. using curves, narrowings or changes in surface levels to prevent vehicles from gaining high speed in front of the square. When organising mass events in the square, it is advisable to add **additional temporary barriers** for the duration of the event (details later in this document).
- **Pedestrian zones and areas:** Permanent pedestrian zones (streets closed to traffic) require security measures mainly **at the beginning and end of the zone** – where the pedestrian area normally begins. It is standard practice to install **fixed**

[5] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, p. 369.

bollards or **automatic barriers** at the entrances to streets leading to the pedestrian zone so that no vehicle can enter without permission. Many European cities (i.e. in France) use a combination of **fixed and retractable bollards** – fixed bollards block entry most of the time, while automatic bollards can be lowered for emergency vehicles or deliveries at specific times[6]. It is important to maintain **continuity of safety measures** – e.g. if a pedestrian zone crosses a street where traffic is not completely closed, consider **shielding the pedestrian route with barriers or solid elements of street furniture** at the intersection. An additional solution to improve safety is to **'naturally' slow down traffic** around the pedestrian zone: traffic islands dividing lanes, chicanes or raised crossings, which force drivers to drive slowly and make it difficult to suddenly steer a vehicle into a crowd.

- **Areas of mass events:** in the case of events attracting large crowds (concerts, street festivals, seasonal fairs) organised in open spaces, **temporary security measures around the perimeter of the event are particularly important**. All possible routes that a vehicle could use to enter the area should be identified and blocked in advance. **Access roads should be closed** at a sufficient distance from the crowd so that a speeding vehicle would not be able to reach it. In practice, a combination of measures is used: **heavy physical barriers (concrete or steel)** placed across streets, **special mobile anti-terrorist barriers** (modules placed on the road) or **service vehicles as blockades**. For instance, in Germany, following the attack on the Christmas market in Berlin, routine security measures were introduced for large events – during festivals in Stuttgart and other cities, multi-tonne lorries were placed on access roads, creating a barrier against any potential attack[7]. Efforts should also be made to ensure that service vehicles used as roadblocks have sufficient weight to serve as effective security measures (a vehicle weighing 1.5 or even 3.5 tonnes may not constitute an effective barrier, so,

[6] Ibid.

[7] https://www.dw.com/pl/niemieckie-miasta-reaguj%C4%85-na-zamach-w-barcelonie/a-40160693#:~:text=W%20STUTTGARCIE%20i%20innych%20miastach,kampanii%20wyborczej%20oraz%20na%20festynach

where possible, security measures should be implemented using heavy goods vehicles weighing over 12 tonnes, treated, of course, only as a temporary measure). Organisers should cooperate with the Police and local government to ensure that **the event security plan (required by the Act on the safety of mass events) takes into account the scenario of an attack using a vehicle**, including procedures for the rapid closure of roads and readiness to use available barriers.

- **Universal public spaces (parks, boulevards, etc.):** in open spaces, it is difficult to install physical barriers around the entire perimeter, but it is worth assessing **where a vehicle could potentially enter at high speed** (e.g. a long straight section of an alley leading into a park, a boulevard along a river with technical access). In such critical areas, it is recommended to **install obstacles in specific locations:** e.g. narrowing the entrance to the park with posts or decorative boulders, setting up **roadblock restricting entry** (barriers, guardrails) on side access roads used only by services. **Street furniture** can play a role here – benches, planters and bicycle racks placed in a row can prevent vehicles from speeding along the park path. It is important to strike a balance between accessibility for residents (e.g. not closing park entrances unnecessarily) and security – often, **simply making entry more difficult and introducing an element of surprise** is enough to deter potential perpetrators.

Regardless of the type of space, a **layered approach** is key: the more successive barriers and obstacles a vehicle encounters, the greater the chance of stopping or slowing it down, giving people time to escape and emergency services time to respond. Specific engineering and organisational solutions that can be implemented are described below.

Before installing anti-terrorist barriers, it is necessary to conduct an appropriate risk analysis and reconnaissance, taking into account the terrain and urban layout of the areas where such an investment is planned. It should be noted that the terrain itself or the layout of streets in urban agglomerations (e.g. winding, narrow roads preventing vehicles from accelerating) may determine that there is no need to install such barriers, or may indicate an increased likelihood of an effective terrorist attack using a vehicle ram in a given location (e.g. a wide pedestrian zone located near the city's main transport

routes, a square located near a slope allowing vehicles to quickly pick up speed, etc.).

Infrastructural and architectural protective solutions

This section presents the available **technical solutions** for protecting public spaces against vehicle intrusion. These include both **fixed infrastructure elements** that become part of the urban landscape, as well as **automatic devices** and **mobile equipment**. It is important to understand the capabilities and limitations of each measure in order to select the combination that best suits local needs. The table below summarises the basic types of barriers and their characteristics, while the following description presents their role and examples of their use.

Table 1. Overview of types of antiterrorist barriers and their characteristics.

Fixed posts and barriers (steel, concrete)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
Medium (one-time installation)	**High against passenger cars**; when using certified posts – also against heavier vehicles at moderate speeds. Certified models can even stop trucks (7.5 t at ~80 kph). They are also effective as everyday access control.	They require earthworks (foundations) and a design that fits into the space. After installation – minimal maintenance costs.	Fixed fencing of pedestrian zones, surrounding squares, protecting pavements from vehicles. Aesthetically, it can be adapted (e.g. stylised posts). They hinder access for emergency services if there are no gaps or removable elements[8].

[8] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a-43300057#:~:text=The%20highest%20security,worth%20their%20often%20enormous%20cost

Automatic retractable barriers (retractable bollards, hydraulic barriers)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
High (purchase and infrastructure)	**Very high** (certified models can even stop trucks ~7.5 t at ~80 kph). They are also effective as everyday access control.	They require a power supply and control system, as well as solid installation (although shallow mounting systems are available). Technical servicing is necessary.	Entrances to restricted areas (old towns, important facilities). They allow authorised vehicles (e.g. public transport, supplies at designated times) to enter. In the event of a breakdown, they must have an emergency exit procedure[9].
Massive elements of small architecture (conrete flowerpots, blocking benches, low walls)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
Low to medium (often part of the space design)	**Average** – well-designed ones can stop or deflect lighter vehicles; **limited effectiveness against lorries** (which can push them aside or ram them). Certified models can even stop trucks (7.5 t at ~80 kph). They are also effective as everyday access control.	Installation as part of site arrangement (flower pots/benches may need to be anchored to the ground for stability). Maintenance is required as with ordinary street furniture.	They can serve a dual purpose: aesthetic and protective. Used in old towns, on public buildings (e.g. rows of reinforced concrete planters in front of the office can stop a heavy vehicle). They should be **arranged so as not to leave wide gaps**. It is worth combining them into groups or with additional steel elements to enhance the effect.
Temporary road barriers (partitions, concrete road barriers of a Jersey type)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
Low (often already owned by road services or easy to hire)	**Low to medium** – standard lightweight metal barriers do not constitute an obstacle for vehicles (only a visual signal).	Easy to use – simply place it in a desired location. Concrete blocks require transport equipment (crane, forklift).	Temporary closure of streets for the duration of the event, designation of a safety zone.

[9] Ibid.

Temporary road barriers (partitions, concrete road barriers of a Jersey type)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
	Heavy concrete blocks **slow down and hinder** entry, but **will not stop a speeding truck** (DEKRA tests: a truck travelling at 50 kph smashed through concrete blocks, only coming to a halt 80 m further on).	The arrangement should allow for a pedestrian crossing.	It is recommended to **connect the blocks in a row** (e.g. with steel cable or modular connectors), which increases their effectiveness. Lightweight barriers should only be used as an auxiliary measure (to fence off an area or regulate traffic), never as the main vehicle barrier[10]. They are a supplement to antivehicle barriers. Their use – for example in the form of chicanes – can effectively reduce the speed of an approaching vehicle. Therefore, it is possible to use certified barriers with lower impact resistance, as lower vehicle speed and weight mean lower forces acting during a collision. This may also reduce the costs of installing certified barriers, while maintaining their effectiveness in appropriately prepared conditions.
Mobile anti-terrorist barriers (blocking modules)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
Medium (cost of purchasing or renting a set)	**High** – certified steel modules can stop a speeding vehicle	They require little time to set up by trained personnel.	The best **temporary** protection in case of increased risk or events.

[10] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a--43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrier

Mobile anti-terrorist barriers (blocking modules)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
	(available designs tested on lorries). Effectiveness depends on the model and configuration of the modules.	They do not need fixed installation – they are placed on the surface, often wedged in place by their own weight and friction. Storage space, transport to the site and assistance with unfolding are required.	Modules allow pedestrians and cyclists to move freely while protecting the area from vehicles ramming into it. They are easy to remove after the event. Recommended for protecting procession routes, public gatherings, VIP visits, etc. – wherever there are no fixed barriers and the risk is temporarily increased.
The use of vehicles as roadblocks (e.g. trucks, city buses)			
Approximate cost	**Effectiveness**	**Installation requirements**	**Example applications/ comments**
Low (use of own resources, fuel and possible overtime for drivers)	**High for passenger cars and medium for lorries** – properly positioned heavy vehicle (sand spreader, bus) is a very difficult barrier to overcome. However, **it is not anchored**, so a speeding lorry can move it or partially push it aside. Service vehicles used as roadblocks should have sufficient weight to serve as effective barriers. A car weighing 1.5 or even 3.5 t may not be an effective barrier, so where possible, barriers should be created using heavy goods vehicles weighing over 12 t. They should be treated only as temporary measures.	This requires the availability of heavy vehicles and drivers, as well as coordination with the services (e.g. the Police). Vehicles should be positioned at the correct angle (preferably sideways to the direction of a potential attack) and secured (brakes, wheel chocks).	A makeshift method used, for example, by German cities to secure mass events. Good as **a last line of defence** or emergency measure – e.g. placing vehicles at the end of a pedestrian zone during a large Christmas market. Barricade vehicles require constant readiness to be moved if necessary (e.g. to let an ambulance through), so they should be parked with the driver nearby or with the possibility of quick departure.

Approximate cost: "low" – low-cost or existing solution (to be used within current resources), "medium" – moderate purchase/installation cost, "high" – significant investment and maintenance cost.

Effectiveness: relative assessment against attacks – the actual ability to stop a vehicle depends on the weight and speed of the vehicle and the specifications of the barrier.

Installation requirements: key technical, logistical or formal requirements for implementing a given measure.

Commentary to the above solutions: It should be emphasised that the **advantage of the best systems** (certified barriers) is their **predictable effectiveness** – they have undergone standardised crash tests (e.g. in accordance with PAS 68, IWA 14-1 or ASTM F2656, DOS (K4, K8, K12) or ISO 22343 standards), which means that it is known what mass and speed the vehicles are capable of stopping. In practice, however, local governments often have to resort to makeshift or lower-standard solutions (for budgetary or aesthetic reasons). Even these can **reduce the risk**: the presence of even partial barriers may discourage the perpetrator, who will assess their chances of success as lower[11]. However, one should be aware of the limitations – e.g. **ordinary road barriers or loosely placed concrete blocks will not stop a speeding lorry**[12]. Therefore, whenever possible, **choose proven and certified solutions** or those that increase the effectiveness of simple measures (e.g. by connecting blocks in a row, using double rows of barriers, utilising the natural terrain such as kerbs, trees, lampposts, etc. as additional obstacles).

Integrating security measures into urban architecture

In order to secure public spaces, it is worth using **"Security by design"** approach, i.e. incorporating protective elements into urban and architectural design. This allows the city to be safe **without**

[11] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, p. 372.

[12] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrie%20r

compromising its charm and functionality. Here are some good practices for such integration:

- **Decorative elements with a protective function:** Many physical barriers can be turned into visually appealing installations. The example is Emirates Stadium in London, where **big concrete letters forming the word "ARSENAL" serve as a vehicle barrier** protecting the entrance to the building. Similarly, **concrete benches and sculptures** can block access roads while looking like part of the street furniture. Such 'ram-proof landscape features' have been successfully used around government buildings in London (e.g. discreetly built-in barriers on Whitehall street).
- **Flowerbeds and urban greenery: Massive planters** arranged in rows are a popular way to block a vehicle's potential path. They are aesthetically pleasing and, when properly constructed (made of reinforced concrete or steel and filled with soil), they form a solid obstacle. Experts point out that **even innocent-looking flowerbeds can stop a lorry if they have an anti-ramming structure inside**. Such flower pots are used, for example, in France in front of government buildings and in the United Kingdom at shopping centres. These types of products, i.e. flowerbeds and planters can also be certified.
- **Designing streets with safety in mind:** Landscape architects recommend that the **layout of communication routes should not allow vehicles to accelerate for long distances in a straight line towards crowds**. This can be achieved through **bends, roundabouts, chicanes, narrowings** – anything that forces a potential vehicle to slow down or manoeuvre. For example, a pedestrian zone can be designed with a slight meander instead of a perfectly straight line, and a town square can have a **buffer zone** around it with trees, lampposts and benches positioned to make it difficult for a vehicle to gain speed.
- **Resistance standards and certifications:** If possible, **use products that have been certified** as effective in stopping vehicles. International standards have been adopted, such as the British **PAS 68** or international **IWA 14-1**, ISO 22343, classifying barriers according to the weight and speed of the vehicle they can stop. In practice, this means, for example, that a certified post can withstand the impact of a 7.5 t lorry travelling at 50 kph, while an uncertified element of similar appearance can be broken by

a passenger car. **Ordinary road barriers should not be confused with anti-terrorist barriers** – the former are designed to limit the effects of accidents, not deliberate attacks[13]. Therefore, for example, **grey concrete road separators** used on roads (so-called "New Jersey") do not guarantee that a lorry will be stopped and should only be treated as an auxiliary measure.

- **Avoiding installation errors:** Even the best barrier will not work if it is poorly installed. **Unanchored, poorly chosen barriers can be moved by a vehicle**, causing more damage – a barricade pushed by a lorry can fall into a crowd instead of protecting it[14]. Therefore, when planning the installation, attention should be paid to the **technical requirements for assembly** (whether a given element should be fixed to the ground, how deep the foundation needs to be, and how far away from the protected object it should be placed). If concrete blocks are used temporarily, try to **connect them to each other** or to other structures (e.g. place them behind a lamppost or tree) to increase their resistance. In turn, when opting for automatic bollards, make sure that they have an **emergency power supply system** or can be lowered manually in the event of a power failure, so that emergency services do not get stuck in front of their own barriers in a critical situation.

Temporary safeguards and use of existing barriers

Local government units often face the challenge of securing one-off or recurring events (e.g. annual festivals, street marathons) without having a permanent, extensive anti-terrorist infrastructure in place. In such situations, it is crucial to **make effective use of the temporary measures available**. Recommendations in this regard are described below.

- **Road barriers in a new role:** typical barriers used in traffic management (steel spans, bollards, road barriers) **will not stop an attack on their own**, but they can be used as an auxiliary

[13] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, p. 362.

[14] https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr3/10_-_artykul_-_J__Jazwinski.pdf, p. 367.

measure. For example, **a series of road barriers** can be used to create an obstacle course, forcing a vehicle to slalom and preventing it from accelerating straight into a crowd. Metal barriers can also be used to separate pedestrian areas from the road, maintaining distance. **However, on their own, they only provide partial protection**. If concrete segments are available (e.g. from road repairs), they can be placed behind such a line of barriers as physical reinforcement. **Water and sand** – filling containers – this will improve the weight of the barrier, but its effectiveness will still be limited with larger vehicles[15].

- **Renting or sharing mobile barriers:** More and more companies are offering mobile **anti-terrorist barriers for hire**. Local governments in the region may consider **jointly purchasing** such equipment for use in securing various events. Alternatively, it is worth establishing cooperation with private companies that own such barriers (e.g. by renting them for large municipal events). It is important to practise assembly in advance – ensure that employees or municipal guards are trained in the quick assembly and disassembly of modules. Mobile barriers should be **strategically placed**: for instance, instead of placing a single row of barriers directly in front of the concert stage, it is better to place two rows several metres apart on the access roads to the venue (creating a buffer zone). We should also remember that **techniques can be combined** – mobile barriers can be supplemented with service vehicles, warning tapes and even natural elements of the environment (e.g. blocking the entrance between buildings with a heavy rubbish container or concrete municipal bins).
- **Use of municipal and service vehicles:** According to the data presented in the table, the use of heavy vehicles as blockades is a proven temporary measure. **The crisis management plan for a mass event** should specify where such vehicles can be obtained if necessary – whether from the municipal fleet (rubbish trucks, sand spreaders, buses) or from partners (construction companies, public transport). It is worth **establishing a procedure**: who

[15] https://www.dw.com/en/do-bollards-offer-protection-against-vehicle-attacks/a43300057#:~:text=The%20barriers%20most%20commonly%20used,80%20meters%20behind%20the%20barrie%20r

decides on the provision of vehicles, where exactly they should be stationed, who is in charge. It is good practice to keep vehicles on standby on the outskirts of the event. For example, during the Christmas market, two street spreaders can be placed around the corner, ready to block the main entrance when signalled. It is important to ensure that **priority signals are visible** – a vehicle used as a barrier should have its warning lights (flashing lights) so that it is clearly visible and unambiguously associated with the activities of the services, which prevents panic and facilitates communication (people and drivers should see that the blockade is intentional and not, for example, the result of an accident).

- **Temporary infrastructure modifications:** If a given location is regularly used for events (e.g. a town square for a New Year's Eve concert every year), **permanent mounting points** for temporary barriers may be considered. These could be, for example, **anchors in the pavement** covered with decorative caps on a daily basis, into which additional posts/barriers can be inserted if necessary. Another idea is to have **chain barrier segments** that fit fixed elements – for example, if the square is surrounded by fixed posts, you can have chains or beams that can be quickly attached between them to create a continuous barrier. These are simple solutions, but they can save valuable time when securing the area.

In summary, in special situations, **one should make creative use of what is available to a given local government**. Even a makeshift barrier can save lives if used wisely. However, whenever only temporary measures are planned, it is essential to have a **plan B** – what to do if they fail. This is why the role of security services during secured events is so important, as discussed below.

The role of local security services (municipal/communal police)

The municipal or communal police, as a formation subordinate to local government, plays an important role in supporting architectural and organisational security measures against terrorist threats. Its tasks and competences in this context include:

- **Supervision of public spaces:** City guards patrolling the streets can **monitor the condition of security measures** – check whether

fixed barriers have been damaged or deliberately removed, ensure that automatic bollards are not left down unnecessarily, and check for unauthorised vehicle traffic in protected areas. They are the 'eyes and ears' of the local government in the field, so their observations can quickly identify potential weak points (e.g. an open roadblock, a broken barrier mechanism, a detour that allows entry from another side).

- **Enforcement of traffic restrictions:** Most architectural solutions work in conjunction with regulations – e.g. no-entry signs in vehicle-free zones, delivery hours, etc. The municipal police have the authority to enforce these local regulations (issuing fines for entering a prohibited zone, removing incorrectly parked vehicles). **Removing illegally parked vehicles** from pavements or pedestrian zones is not only a matter of order, but also of safety – a parked car could be used as a means of committing a terrorist attack or hinder the operation of barriers (e.g. someone could drive around a bollard on the pavement). Therefore, guards should emphasise **keeping protective zones free of vehicles**.
- **Support in closing roads and organising events:** During temporary road closures (e.g. for demonstrations, street races, concert) in the anti-terrorist context, guards may **set up and guard barricades**, e.g. station themselves at the entrance to a closed street with a police car across the road to physically stop any attempts to enter if necessary (the police car can also act as a barrier in an emergency, although the lives of officers are obviously the priority here). Guards may also direct authorised vehicles to take detours so that they do not drive into the crowd.
- **Operation of security devices:** Many local governments entrust municipal police with the administration of access control systems – for example, **the remote control for lowering automatic bollards** is often at the disposal of patrols or the police officer on duty. Guards may be tasked with opening barriers for municipal service vehicles, closing them after deliveries, etc. It is important to have clear procedures in place: who decides when to raise/lower the bollard, so that unauthorised entry does not occur due to a communication error. It is good practice to equip the security control centre with CCTV monitoring (city surveillance) of entrances to protected areas – the guard can

remotely verify the need for entry and unlock the barrier, while also having a recording of the event.

- **Monitoring and rapid response:** Many local governments have access to **urban video surveillance systems**, often operated by municipal police. Camera operators should be trained to pay attention to unusual vehicle behaviour in pedestrian areas, such as a car speeding towards a closed street or a van repeatedly circling near a gathering. **Early detection of a threat** will allow the municipal police or police to respond (set up an additional roadblock, stop the driver before they enter the crowd). Municipal guards, as the first on the scene, can attempt **to redirect traffic** or **evacuate people** if they notice a speeding vehicle.
- **Cooperation with the Police and other services:** in a terrorist threat situation, the main role falls to the Police (primarily Police counter-terrorist units), but the municipal/communal police may perform auxiliary functions, such as securing the surrounding area, directing people to safe areas and providing information to the crisis management team. It is good to establish communication channels and division of tasks in advance (e.g. the guard immediately closes traffic on neighbouring streets so that emergency services have free access). **It is also worth involving guards in anti-crisis training and exercises** related to terrorist attacks – their knowledge of the city's topography and experience in working with residents can significantly improve the course of action.
- **Education and awareness raising:** Municipal police can conduct **information activities concerning** appropriate behaviour in emergency situations on the street. This includes, for example, providing advice on '**what to do if you see a car speeding into a crowd**' – run sideways, hide behind the nearest obstacle (wall, tree, lamppost), warn others. Conscious and alert citizens are an additional element of the security system, and guards can shape this alertness by teaching people to recognise danger signals and respond appropriately.

In summary, municipal/communal police provides a natural support in the implementation of the activities described in these recommendations. In order to fully exploit its potential, **the local government should clarify the scope of its competences** (e.g. include tasks related to anti-terrorist security in the regulations governing

the municipal/communal police) and **provide appropriate training** in this area. Good cooperation between the municipal/communal police, the Police, road administrators and event organisers will translate into more efficient and effective security at the local level.

Legal and organisational aspects

Implementation of the described solutions requires consideration of a number of legal and organisational issues. The most important ones that local authorities should bear in mind are discussed below:

- **Administrative responsibility:** The safety of public spaces is the responsibility of local government and state administration bodies. In practice, **the city president/mayor/commune head** is responsible for public order tasks in their area, cooperating with the provincial governor and state services. The installation of fixed safety measures (posts, barriers) on municipal roads requires a decision by the road administrator (often the municipal road authority, subordinate to the president) – hence, the local government must ensure formal approval of traffic organisation projects that take into account the new barriers. It is worth appointing a **public space safety coordinator** within municipal structures – a person or unit responsible for planning and supervising the implementation of these measures. This may be part of the municipal crisis management team or a separate presidential representative for security. It is important to clearly define who maintains and monitors individual devices (e.g. whether the investment department, road administration or an external company is responsible for servicing automatic bollards).
- **Coordination with owners and managers of private public spaces:** in cities, many **formally private** spaces serve a de facto public function – e.g. shopping centre arcades, squares between office buildings, private university campuses, supermarket car parks, etc. The local government cannot unilaterally impose its installations there, but **cooperation is crucial**. It is recommended to invite the managers of such facilities to **joint meetings** within the framework of a safety committee or crisis management team. It is worth developing **minimum security standards** for such

places – e.g. encouraging (or requiring in administrative decisions, if possible) the installation of bollards in front of shopping centre entrances and the installation of barriers at driveways to passageways. A **safety audit** can be used here: municipal services (e.g. the State Fire Service, Police, municipal police) in cooperation with the owner inspect the facility and suggest improvements. **Practical exercises** (e.g. simulation of an attack or evacuation in a shopping centre) involving the services and facility staff will also reveal shortcomings and allow procedures to be developed. Legally speaking, the owner of the site is responsible for ensuring the safety of users – the municipality may therefore argue that **implementing security measures is also in their interest (limiting civil liability)**. In the case of large public facilities (stadiums, shopping centres), a security plan agreed with the Police is often required – it is worth ensuring that it also takes into account the **threat posed by vehicles**.

- **Compliance with building regulations and technical regulations:** Installation of fixed anti-terrorist barriers may be subject to building regulations. Some elements (e.g. walls, foundations for barriers) will require a building design and a building permit or notification of construction works. It is necessary to ensure that the design is prepared by a person with the appropriate qualifications. **The placement of barriers on public roads** must comply with traffic regulations – approval of the new traffic organisation (signs, traffic safety devices) is required. In addition, **health and safety as well as fire regulations** require that safety measures do not impede the evacuation of people and access for emergency services. This means, for example, that **pedestrian walkways next to posts must remain passable** (ensuring a minimum passage width), and if a street is closed, it must be possible to quickly remove the barrier in case the fire brigade needs to enter. In areas under the supervision of a conservation officer (e.g. old towns), **the choice of security measures** should be agreed with the conservation officer – sometimes concrete blocks cannot be placed freely because they spoil the historical layout, so alternative solutions must be sought (e.g. stylised posts that fit in with the aesthetics of the place).
- **The Act on crisis management and planning documents:** Pursuant to the Act on crisis management, each municipality

should have a **Crisis Management Plan** that identifies potential threats (including terrorist threats) and defines response procedures. In the context of vehicle attacks, it is advisable for this plan to:

- include a **scenario for such an attack** (risk analysis, identification of the most vulnerable locations in the municipality),
- specify the **forces and means** of counteraction – i.e. an inventory of available security measures (e.g. a list of locations where there are fixed barriers; a warehouse of mobile barriers; available trucks and vehicles for blocking roads, together with contact details for the operators),
- assign **roles and responsibilities** – e.g. who decides to raise the security level in the event of an increased alert (BRAVO/CHARLIE/DELTA), who is responsible for physically setting up barriers in the event of a threat, etc.,
- include **cooperation with other entities**, e.g. with the administrators of national roads running through the city (if it is necessary to block the exit from such a road to the event site), with neighbouring municipalities (when the event has a wider impact), with the provincial crisis management centre (reporting). Regular updates to the plan and exercises (even at the level of decision-making games) will help maintain readiness. In addition to the crisis plan, **local spatial development plans** for sensitive areas may also include safety guidelines (e.g. a requirement to design shopping malls with elements that block entry).

- **Financing safety investments:** The purchase and installation of professional anti-terrorist systems can be costly. Local governments should seek **available sources of external financing**, such as European funds (the EU Internal Security Fund provides funds for the protection of public spaces). It is worth preparing **projects justifying the need** (e.g. when applying for funding for the installation of automatic barriers in the old town, refer to risk analyses and good practices from other cities). Furthermore, involving private entities (e.g. shopping centres) in joint initiatives, costs can be shared – for example, the city builds the infrastructure for automatic locks, and the shopping centre provides the devices themselves. **Maintenance costs** should also

be planned for: servicing, repairs, periodic crash tests (if required by the manufacturer). It is better to invest in a certified solution than to be responsible for a faulty half- measure that will fail – this awareness should guide decision-makers when allocating funds.

Formal safety requirements for contractors and employees performing activities related to anti-terrorist barrier access control systems or their integration

It is reasonable to check whether the contractor has a licence from the Ministry of the Interior and Administration to conduct activities in the field of personal and property protection. In the case of access to classified information, it is advisable that the contractor has a valid Facility Security Clearance up to the 'CONFIDENTIAL' level without safeguarding capacity. Compliance with this requirement does not include the obligation to have a registry.

Employees performing activities related to access control systems or their integration should:

- hold a personal security clearance of at least 'CONFIDENTIAL' level;
- be included in the list of qualified technical security personnel, according to the Act of 22 August 1997 on the protection of persons and property (Journal of Laws of 2025, item 532).

Employees performing general construction work (e.g. excavation, cable installation, equipment assembly) are not required to have personal security clearance, however, they should have a current certificate of no criminal record. These requirements also apply to subcontractors involved in installation or maintenance work.

Adaptation of recommendations to different local government units

The recommendations presented are of a general nature – their implementation will look different in a metropolis than in a small town. Each local government unit should **conduct its own analysis of needs and possibilities**, taking into account factors such as: the volume

of tourist traffic, the number of mass events per year, urban layout (e.g. historic old town vs. scattered housing estates), budget and staff.

Here are some tips on how to adapt the recommendations to local conditions:

- **Small towns and municipalities with limited budgets**: The priority should be to **identify the most vulnerable locations** (e.g. the main market square, the pedestrian zone near the town hall, the harvest festival grounds) and implement even simple measures there. If an entity cannot afford automatic bollards, it should start with **fixed posts or concrete planters** – the unit cost is not high, and they can be installed gradually. Many such municipalities already have street furniture elements that only need to be **strategically placed**. You can also look for **used equipment** – e.g. obtain barriers from a larger town (after modernisation) or from demobilisation. It is also important to **train municipal guards and volunteer fire brigades** in responding to such incidents, because in a small community they will be the first on the scene.
- **Medium-sized towns:** Already having some infrastructure and a budget for investments, they should take a **systematic approach** to the issue. It is worth to develop a **municipal programme to improve the safety of public spaces** over several years, with funds allocated in the budget. Such a programme could, for example, include: stage I – installation of barriers in the market square and main pedestrian zone, stage II – purchase of mobile barriers to secure events, stage III – creation of a monitoring centre, etc. It is also important to exchange the experience – for example, through the Union of Polish Metropolises or other city associations, it is possible to draw on the knowledge of leaders (large cities are often willing to share the solutions they have developed). Medium-sized cities should also consider **inter-municipal exercises** – terrorist threats rarely affect only one municipality.
- **Large cities and metropolises:** Here, residents' expectations regarding security are high, and the potential risk (due to the attractiveness of the targets) is greater. Large cities should invest in **the most effective technologies available**, such as **integrated systems** (barriers linked to traffic lights, remote control of barriers from a monitoring centre, sensors that detect

unusually fast-moving vehicles and automatically raise barriers). Budget is obviously a barrier, but large entities have easier access to external funding and can justify their needs on security grounds, for example critical infrastructure or of international importance (tourism, institution headquarters, etc.). It is important to maintain a **network of cooperation** with experts – e.g. using anti-terrorist security advisers (plans can be consulted with the Internal Security Agency or police terrorism specialists). A large city should also commission **external audits** from time to time – a fresh expert perspective will help identify gaps that its own services may have overlooked.

- **Flexibility and updating:** Terrorist threats evolve – new techniques emerge (e.g. in the future, potentially remote takeover of autonomous vehicles), and the technical capabilities of security measures also change. Therefore, these recommendations cannot be regarded as an exhaustive list. For instance, the European Commission publishes guidelines for protecting public spaces from attacks (e.g. The guideline to selecting barrier solutions against vehicle-ramming attacks[16]), and industry organisations present new technical solutions (conferences, security fairs). It is worth taking advantage of this. It is equally important to **analyse incidents** that do occur – if a vehicle-ramming attack takes place anywhere, the question must be asked: *could a similar scenario occur in a given city? Are there measures in place to prevent this, and if not, what needs to be improved?* Learning from the experiences of others is the key to continuous improvement in security.

Summary

A safe public space is one where **people can freely gather and enjoy themselves without being unnecessarily disturbed by the sight of fortifications**, while at the same time **potential aggressors encounter hidden obstacles** that thwart their plans. This goal is achieved through **multifaceted measures**: from fixed infrastructure (barriers, posts, railings), through organisational solutions (security

[16] https://ec.europa.eu/newsroom/pps/items/665632/en#:~:text=JRC%20Guideline%20Selecting%20proper%20security,now%20also%20available%20in%20French

plans and procedures during events), to the human factor (vigilance of services and citizens).

Well-designed and implemented measures can significantly **reduce the likelihood of a successful attack or limit its impact**. As indicated, even simple barriers can save lives by delaying a vehicle or changing its trajectory, giving people extra seconds to escape. Ultimately, however, no measures can provide a 100% guarantee, which is why a **comprehensive approach** is so important: combining different solutions and maintaining readiness to respond to unforeseen situations.

Local governments in Poland, drawing on the experiences of other European countries, can **effectively improve the safety** of their towns and municipalities without straining their budgets or disrupting the friendly nature of public spaces. The key is to plan ahead (before a tragedy occurs), to cooperate continuously with experts and services, as well as to educate the local community. This is how cities that are resilient to threats but still **open and friendly** are created – places where safety becomes a natural part of the infrastructure, almost invisible to the casual passer-by, but ensuring their peace of mind.

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 517–535

https://doi.org/10.4467/27204383TER.25.063.23050

Varia

Terrorists, saboteurs, spies in Polish prisons – the role of the Prison Service

Andrzej Leńczuk

Independent author

https://orcid.org/0009-0009-0719-6599

Introduction

Since 2021, we have been able to observe in Poland processes that are clearly connected to the international situation, in particular the war in Ukraine triggered by Russia and the migration crisis on the Polish – Belarusian border. We learn about the detention on Polish territory of spies, diversion agents, saboteurs carrying out various activities, including disinformation, with the aim of creating a sense of threat, fear and destabilising social mood in Poland. The fire at the shopping centre at Marywilska Street in Warsaw or the activities of foreign intelligence services shown, among other things, in statements of the Internal Security Agency (ABW) or the National Prosecutor's Office are only a fragment of the processes described as hybrid events or even hybrid war.

This raises the question of whether the Prison Service, in carrying out its tasks, is prepared for the new challenges posed by hybrid warfare, which manifests itself in the presence of spies, saboteurs and diversionists

in prisons and remand centres. In order to answer this question, basic information will be presented on the Prison Service as well as prisons and remand centres, the functions performed by officers and employees, and statistical data on the presence of the indicated perpetrators in prisons and remand centres.

The legal framework for the functioning of the Prison Service and its tasks, and the organisation of prisons and remand centres – selected aspects

Operation of the prisons and remand centres as well as tasks of the Prison Service officers are described in many legal acts. The most important of these are the Penal Enforcement Code[1] and the *Act of 9 April 2010 on the Prison Service*[2].

The Prison Service, unlike the Police, the Border Guard or the State Fire Service but following the example of many countries, reports directly to the Minister of Justice. This model of service subordination has a tradition of over 100 years, except for the period between 1945 and 1956, when the formation was first subordinate to the Ministry of Public Security, and from 1954 to the Ministry of the Interior.

The Prison Service employs nearly 30 000 officers and employees, and is the third-largest uniformed formation in Poland in terms of personnel[3]. Rank insignia are an essential element of almost every uniform. In the Prison Service, they have retained military-style nomenclature in four corps: privates, non-commissioned officers, warrant officers and officers. The lowest rank, from which every officer begins their service, is private, while the highest is inspector general of the Prison Service.

The model of the Prison Service's functioning, taking into account its assigned tasks, principle of hierarchy, single-person management, uniform, service ranks and armament with firearms, positions the formation among other paramilitary-type operational groups performing an important role

[1] *Act of 6 June 1997 – the Penal Enforcement Code* (consolidated text, Journal of Laws of 2025, item 911, as amended).

[2] *Act of 9 April 2010 on the Prison Service* (consolidated text, Journal of Laws of 2024, item 1869, as amended).

[3] Służba Więzienna – o nas (Eng. The Prison Service – about us), https://sw.gov.pl/strona/rekrutacja-o-nas [accessed: 4 VIII 2025].

in the internal security system[4]. This category includes, among others: the Police, the Border Guard, the State Fire Service, the State Protection Service, the Internal Security Agency, the Railway Security Guard. These are also the formations with which the Prison Service cooperates. The events that have been taking place on the Polish border since autumn 2021 have necessitated closer cooperation between the Prison Service and the Border Guard, as well as the Internal Security Agency. The Border Guard carries out part of its statutory tasks in direct cooperation with the Prison Service. This applies, among other things, to ongoing investigative and preparatory proceedings within the meaning of the Code of Criminal Procedure[5], as well as to the exchange of information within a specific scope, e.g. related to the transport of remand prisoners of interest to the Border Guard. Cooperation between the two uniformed services serves to ensure both the security of penitentiary units and the safety of citizens.

The Prison Service's efforts to maintain order and security within prisons and remand centres as well as to protect the public from criminals are also supported on a cooperative basis by the Internal Security Agency. On 27 October 2021, both services concluded the *Agreement on scientific and educational cooperation in the field of countering radicalisation and terrorist threats*. This created new opportunities for cooperation, including the organisation of training courses, conferences and exchange of experiences. However, the strategic objective of the agreement was (...) *to counteract radicalisation leading to violent extremism and terrorism in the prison environment and to eliminate the risk of a return to radical activity after release from prison. For this reason, the cooperation will include, among other things, the analysis of cases of radicalisation in prisons in order to establish appropriate rehabilitation and deradicalisation programmes, which will also promote effective social reintegration in the post-penitentiary period*[6]. The organisational unit of the Internal Security Agency that played

[4] J. Maciejewski, *Grupy dyspozycyjne. Analiza socjologiczna* (Eng. Dispositional groups. Sociological analysis), Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2012, pp. 49–53.

[5] *Act of 6 June 1997 – the Code of Criminal Procedure* (consolidated text, Journal of Laws of 2005, item 46, as amended).

[6] *Współpraca ABW i SW w zakresie prewencji terrorystycznej* (Eng. Cooperation of the Internal Security Agency and the Prison Service in the field of counter-terrorism), Terrorism Prevention, https://tpcoe.gov.pl/cpt/wydarzenia/1912,Wspolpraca-ABW-i-SW-w-zakresie-prewencji-terrorystycznej.html [accessed: 5 VIII 2025].

a particularly important role in this area was the Terrorism Prevention Centre of Excellence, now the Terrorism Prevention Unit.

The basic organisational units of the prison system are prisons and remand centres subordinated to the Minister of Justice[7], who, by way of an order, establishes and abolishes prisons and transforms them into remand centres, taking into account existing needs. A prison or remand centre is managed by a director, while other officers and employees of the prison and other persons within the scope of their duties in relation to the organisation of work or various types of activities are the convict's superiors[8].

A fundamental condition for the proper functioning of a penitentiary unit – understood as ensuring security and achieving the objectives of enforcing imprisonment and pre-trial detention, as well as protecting society from offenders – is the maintenance of order and discipline in the prison or remand centre[9]. This process should be carried out with the principles set out in Art. 4 § 1 of the Penal Enforcement Code and in other regulations concerning the treatment of inmates contained in the Act on the Prison Service. Article 2(2) of this Act lists the tasks of the formation, which include, among others:

- conducting penitentiary and rehabilitative interventions for persons sentenced to imprisonment,
- carrying out pre-trial detention in a manner that ensures the proper course of criminal or fiscal proceedings,
- ensuring that convicted and pre-trial detainees have their rights respected, particularly with respect to humane living conditions, respect for dignity, health and religious care,
- humane treatment of persons deprived of liberty,
- protecting society from offenders of crimes or fiscal offenses held in prisons and remand centres,
- maintaining order and security in prisons and remand centres,
- managing the Central Database of Persons Deprived of Liberty.

There are 171 penitentiary units operating in Poland, including: 64 prisons, 39 remand centres and 68 external branches of prisons or

[7] Articles 68 and 208 of the Penal Enforcement Code.

[8] Articles 72 § 1 and 2, 208 § 4 of the Penal Enforcement Code.

[9] Article 73 § 1 of the Penal Enforcement Code.

remand centres, some of which have so-called detention wards[10]. The Penal Enforcement Code lists four types of prisons for convicts[11]: for juveniles, first-time offenders, repeat offenders and those serving military detention. They may be organised as prisons: closed, semi-open and open[12]. Various types of penitentiary facilities differ (...) *in particular in the degree of security, the level of inmate isolation, and the resulting obligations and entitlements regarding their movement within the facility and outside its premises*[13].

The penitentiary map of Poland shows the locations of prisons, remand centres and external wards (Figure 1):

Figure 1. The locations of prisons, remand centres and external wards in Poland.

Source: data from the Registry Office of the Central Prison Service Administration.

[10] Data from the Registry Office of the Central Prison Service Administration.

[11] Article 69 of the Penal Enforcement Code.

[12] Article 70 § 1 of the Penal Enforcement Code.

[13] Article 70 § 2 of the Penal Enforcement Code.

As of 30 June 2025, there were 70 214 persons deprived of liberty in Polish prisons, including: 61 409 convicted persons, 7642 persons in pre-trial detention and 1163 persons serving sentences[14]. Population, i.e. the number of inmates in penitentiary facilities, at 70 000 persons, is approx. 84% of the system's capacity. In the prison population, i.e. those convicted, remanded in custody in Polish penitentiary units, male definitely dominate – 66 465, i.e. 94.6% of the total. Women constitute approx. 5.4% of this population (3749).

New types of threats to state security – hybrid activities

Since 2021, Poland has been particularly vulnerable to various types of activities that directly threaten the security of the state and its citizens, a significant part of them take the form of hybrid activities, as exemplified by the migration crisis. On 2 September 2021, at the request of the Council of Ministers, the President of the Republic of Poland introduced a 30-day state of emergency in parts of the Podlaskie and Lubelskie provinces[15]. The draft resolution of the Council of Ministers on submitting a request to the President of the Republic of Poland to introduce a state of emergency in these areas states, among other things, that: (...) *the unique nature and extraordinary scale of migratory pressure on the Polish-Belarusian border stem from deliberate and planned actions by the Belarusian authorities aimed at destabilising the situation on the border with Poland and other European Union Member States, i.e. Lithuania and Latvia. These actions take the form of a 'hybrid war' waged by the Belarusian regime*[16].

[14] CZSW BIS (Eng. The Information and Statistics Office of the Central Prison Service Administration) – monthly statistics – June 2025. Statistical data is available on the website: https://www.sw.gov.pl/strona/statystyka.

[15] *Regulation of the President of the Republic of Poland of 2 September 2021 on the introduction of a state of emergency in parts of the Podlaskie and Lubelskie provinces* (Journal of Laws of 2021, item 1612).

[16] *Draft resolution of the Council of Ministers to submit to the President of the Republic of Poland a request to declare a state of emergency in parts of the Podlaskie and Lubelskie provinces*, Serwis Rzeczypospolitej Polskiej, 31 VIII 2021, https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-o-skierowaniu-do-prezydenta-rzeczypospolitej-polskiej-wniosku-o-wprowadzenie-stanu-wyjatkowego-na-obszarze-czesci-wojewodztwa-podlaskiego-oraz-czesci-wojewodztwa-lubelskiego [accessed: 7 VIII 2025].

The Polish border security breaches were of a new nature and consisted not only of attempts by thousands of people of various nationalities to cross the border illegally, but also of the need to physically defend against groups of immigrants who destroyed security measures and attacked officers of the Border Guard, the Police, soldiers. The scale of these violations was unprecedented, as reflected in the Border Guard statistics. Suffice it to say that while in 2020 there were 129 illegal border crossings from Belarus, in 2021 there were already 39 697[17].

The migration crisis has led to an increase in the number of crimes involving illegal border crossings into Poland (Art. 264 § 2 of the Criminal Code), assistance in organising such activities (Art. 264 § 3 of the Criminal Code) and deriving material benefits from them (Art. 264a § 1 of the Criminal Code). As a result of the actions of the services and the public prosecutor's office, some of the suspects were placed in pre-trial detention. The period from September to December 2021 was a time of increase in the number of foreigners in prisons and remand centres (Chart 1)[18].

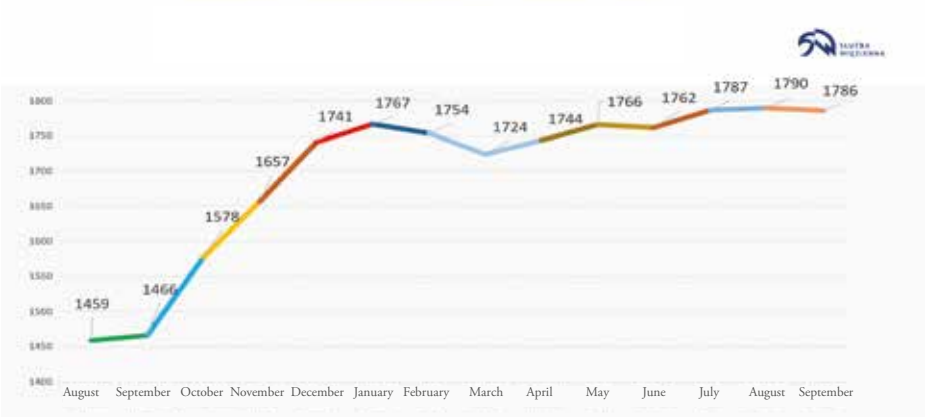


Chart 1. Foreign nationals in Polish prisons between August 2021 – September 2022.

Source: data from the Registry Office of the Central Prison Service Administration.

[17] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią w 2021 r.* (Eng. Illegal border crossings from Belarus in 2021), Straż Graniczna, 12 I 2022, https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [accessed: 7 VIII 2025].

[18] Służba Więzienna – statystyka (Eng. The Prison Service – statistics), https://www.sw.gov.pl/strona/Statystyka [accessed: 12 VIII 2025].

A further slight increase in the number of foreigners in Polish prisons occurred after Russia's full-scale attack on Ukraine in February 2022. It should be emphasised, that some of the individuals detained by the Polish authorities at that time had previously been wanted by Interpol on suspicion of belonging to terrorist organisations in their countries of origin and conducting such activities. Their presence requires the Prison Service officers to take constant preventive measures aimed at identifying any atmosphere or behaviour that could pose a threat to security in prison. This is particularly important in relation to remand prisoners who have organised terrorist attacks in their countries of origin or elsewhere, or who have belonged to Islamic State. Another important aspect is the need to counteract demoralisation and radicalisation in prison. It should also be remembered that prisoners or former prisoners remain of interest to Russian intelligence services as potential 'disposable agents' used to carry out hybrid attacks. The Report of the International Centre for Counter Terrorism (ICCT) and GLOBSEC points out that since 2022, there have been 110 hybrid attacks in Europe linked to Russia. The services identified 131 individuals residing in Europe and involved in such activities, at least 35 of whom had previous contact with crime. At the same time, the authors of the report emphasise that prisons both in Russia and abroad remain a place of recruitment for criminals, most often young men (around 30 years old) who are in a difficult financial situation, to carry out an act of sabotage[19].

The situation on the Polish-Belarusian border is still very difficult, as evidenced by information presented by the Podlaski Border Guard Regional Unit[20]. Only in the period from July to August 2025, numerous attempts to cross the border illegally occurred almost daily. For example: 1 July – there were 100 attempts; 4–6 July – 170; 10 July – 100; 16 July – 210; 18–20 July – 340; 25 July – 170; 6–7 August – 280; 12 August – 170; 13 August – 130. By 14 August 2025, the Podlaski Border Guard Regional Unit recorded 19 500 attempts to cross the Polish-Belarusian border illegally[21].

[19] *Russia's Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe*, https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf, pp. 24–31 [accessed: 10 X 2025].

[20] Straż Graniczna – aktualności (Eng. The Border Guard – News), https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/.

[21] M. Bura, *Na polsko-białoruskiej granicy* (Eng. On the Polish-Belarusian border), Podlaski Oddział Straży Granicznej, 14 VIII 2025, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/67321,Na-polsko-bialoruskiej-granicy.html [accessed: 18 VIII 2025].

A common feature of most of these events is their aggressive nature. Foreigners, attempting to enter Poland, very often destroy technical barriers using various tools, dig tunnels[22], and throw stones, power insulators, tree branches, barbed wire spikes, glass bottles filled with sand and sticks tipped with sharp tools at those guarding the border. In this way, they damage border infrastructure, vehicles of the Border Guard, and, most importantly, create a real and direct threat to health and life of officers and soldiers. A tragic consequence of such actions was the incident on 28 May 2024, when Private Mateusz Sitek, while on duty, was stabbed by a foreigner attempting to breach the border security measures and, despite the efforts of doctors, died a few days later[23]. Polish authorities were relatively quick to establish the perpetrator's appearance and origin. However, his capture was not possible, also because the Belarusian side, despite a formal note of protest, did not cooperate effectively.

Despite the efforts of the services, some foreigners manage to cross the border illegally and are detained once already on the territory of Poland. The Podlaski Border Guard Regional Unit reports the detention of citizens of, among others, Sudan, Yemen, Cameroon, Ethiopia, Afghanistan, India, Eritrea, Somalia, Bangladesh and Egypt. People who assist in illegal border crossings and organise them are also detained, including Ukrainians, Belarusians, Latvians and Poles. Only between 1 January and 7 July 2025 alone, officers of the Podlaski Border Guard Regional Unit detained 95 accomplices and organisers involved in illegal crossings of the Polish-Belarusian border[24], some of whom were probably charged with criminal offences resulting in pre-trial detention. It is worth mentioning the difficulties faced by the Prison Service officers in such situations, such as communication problems resulting from the arrested persons' lack of knowledge of English and their cultural and religious specificities.

[22] M. Bura, *Podkopem (NIE) do Polski* (Eng. A tunnel (NOT) to Poland), Podlaski Oddział Straży Granicznej, 10 VII 2025, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/66897,Podkopem-NIE-do-Polski.html [accessed: 18 VIII 2025].

[23] *Ostatnie pożegnanie śp. szer. Mateusza Sitka* (Eng. The final farewell to the late Private Mateusz Sitek), 1. Warszawska Brygada Pancerna, https://www.wojsko-polskie.pl/1bpanc/articles/aktualnosci-w/ostatnie-pozegnanie-sp-szer-mateusza-sitka [accessed: 18 VIII 2025].

[24] K. Zdanowicz, *W bagażniku na zachód Europy* (Eng. In the boot to Western Europe), Podlaski Oddział Straży Granicznej, 8 VII 2025, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/66859,W-bagazniku-na-zachod-Europy.html [accessed: 18 VIII 2025].

Another example of events that are currently causing concern among many Polish citizens are fires. If it is caused by human activity, it is most likely a crime[25], which may be intentional, i.e. the perpetrator wants to and takes prohibited actions or anticipates the possibility of taking them and accepts it, or unintentional, when the perpetrator does not intend to commit a prohibited act but it occurs as a result of the perpetrator's carelessness[26].

Other circumstances arise when:

a) participating in foreign intelligence activities or acting on its behalf, perpetrator or perpetrators commit acts of diversion, sabotage or terrorist offences,
b) acting in an organised armed group, perpetrator or perpetrators commit terrorist offences[27].

One such planned action was the fire on 12 May 2024 at the shopping centre at Marywilska 44 Street in Warsaw. According to a statement issued by the National Prosecutor's Office on 12 May 2025, the arson attack was ordered by the Russian Federation's intelligence services. The investigation established that a Ukrainian citizen received instructions from another Ukrainian citizen residing in Russia to record the fire and the actions of the rescue services. The order specified the time at which the fire would break out[28].

Furthermore, the investigation established that two Ukrainian citizens involved in starting and documenting the fire at the Marywilska 44 shopping centre, together with two other individuals, planned and carried out, using incendiary devices, on the night of 8 to 9 May 2024, a fire at IKEA large-scale store in Vilnius.

As part of the same investigation, the circumstances of the fire at the building supply store in Warsaw on 12 April 2024 are being investigated. According to the findings of the prosecutor's office, the incident was the result of deliberate action, and the perpetrator was a Belarusian citizen. On 31 January 2024, the officers of the Internal Security Agency detained a citizen of Ukraine in Wrocław. He was acting in an organised criminal group and on behalf of Russian intelligence services, was preparing to carry

[25] Article 163 § 1 point 1 of the Criminal Code.

[26] Article 9 of the Criminal Code.

[27] Article 258 § 2 of the Criminal Code.

[28] *Zarzuty w związku z pożarem hali przy ul. Marywilskiej 44* (Eng. Allegations in connection with the fire at the market hall at Marywilska 44), Prokuratura Krajowa, 12 V 2025, https://www.gov.pl/web/prokuratura-krajowa/zarzuty-m44 [accessed: 25 VIII 2025].

out acts of sabotage and diversion, consisting in particular of setting fire to buildings in Wrocław, located in close proximity to elements of strategic infrastructure[29]. As the investigation revealed, a 51-year-old Ukrainian man (...) *was paid USD 4000 by Russian intelligence services to prepare to set fire to a paint centre on Kwidzyńska Street in Kowale, Wrocław. It operates at a paint factory owned by the US giant in this field, one of the 500 largest US companies in terms of revenue*[30]. On 23 May 2024, the officers of the Internal Security Agency arrested a Polish man and two Belarusians suspected of setting fire to buildings in various parts of the country and acting on behalf of Russian secret service[31].

The scale of the threat posed by hybrid activities is also evidenced by information about the detention in Poland of persons conducting espionage, sabotage, terrorist or other activities directly threatening the security of our country on behalf of foreign intelligence services. An analysis of information provided by the Internal Security Agency between 1 January 2024 and 30 June 2025 reveals a number of examples demonstrating the effectiveness of the Polish services in detecting such threats. Here are some of them[32]:

- 9 September 2024 – arrest of a Belarusian woman on charges of spying for Belarusian secret service – the State Security Committee of the Republic of Belarus,
- 6 February 2024 – referral to court of an indictment against a Polish citizen suspected of spying for Russian secret service,
- 19 April 2024 – arrest of a Polish citizen suspected of reporting willingness to cooperate with Russian secret services,

[29] *Funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego zatrzymali mężczyznę działającego na zlecenie rosyjskich służb wywiadowczych* (Eng. The officers of the Internal Security Agency arrested a man acting on behalf of the Russian intelligence services), Serwis Rzeczypospolitej Polskiej, 15 II 2024, https://www.gov.pl/web/sluzby-specjalne/funkcjonariusze-agencji-bezpieczenstwa-wewnetrznego-zatrzymali-mezczyzne-dzialajacego-na-zlecenie-rosyjskich-sluzb-wywiadowczych [accessed: 25 VIII 2025].

[30] *Ukrainiec, który na zlecenie Rosji miał wywołać pożar we Wrocławiu idzie do więzienia. Sąd: „motał i kłamał"* (Eng. The Ukrainian man who was commissioned by Russia to start a fire in Wrocław is going to prison. Court: 'He was confused and lied'), tuWroclaw.com, 21 II 2025, https://tuwroclaw.com/artykul/ukrainiec-ktory-na-n1507326 [accessed: 25 VIII 2025].

[31] *Statement*, ABW, 29 V 2024, https://www.abw.gov.pl/pl/informacje/2501,Komunikat.html. [accessed: 25 VIII 2025].

[32] ABW (the Internal Security Agency) – information, https://www.abw.gov.pl/pl/informacje.

– 16 May 2024 – sentencing by the District Court in Świdnica of a Polish citizen to 2 years imprisonment for participating in an organised criminal group of a terrorist nature and planning to carry out a terrorist attack using explosives – with the aim of seriously intimidating many people and causing an event threatening the life or health of many people or property of great value,
– 13 November 2024 – arrest of a Belarusian citizen acting on behalf of foreign secret services, suspected of attempting to set fire to a building located in Gdańsk,
– 1 April 2025 – arrest of a Ukrainian citizen acting on behalf of the Russian intelligence.

A partial summary of the Internal Security Agency activities related to detecting threats resulting from hybrid activities initiated and coordinated by Russian secret services and counteracting them, presentation of methods of operation and ways of recruiting for diversionary tasks can be found in the statement dated 25 October 2024[33]. Interesting information about unconventional methods of recruiting people to carry out espionage and sabotage activities is also provided in the aforementioned report entitled *Rabota w Polsze*[34].

The described hybrid activities inspired by foreign intelligence services, most often Russian and Belarusian, serve to destabilise state authorities, creating a sense of threat among citizens and polarising society, fuelling ethnic conflicts, weakening the national community and questioning international alliances. Random individuals acting out of greed are often used to carry out attacks. The events presented are clearly criminal in nature, pose a direct threat to the life and health of citizens, undermine the security and interests of the Republic of Poland, and are punishable by severe penalties, most often for a period of not less than 5 years or life imprisonment.

[33] *The statement concerning diversionary activities of the RF*, ABW, 25 X 2024, https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html [accessed: 25 VIII 2025].

[34] *Jak działają rosyjscy szpiedzy w Polsce? "Rabota w Polsze" – reportaż Piotra Świerczka* (Eng. How do Russian spies operate in Poland? 'Rabota w Polsze' – a report by Piotr Świerczek), YouTube, 12 IX 2025, https://www.youtube.com/watch?v=44O7Y_yMXGk [accessed: 12 IX 2025].

Spies, saboteurs and terrorists in Polish prisons – statistical data

In every case where the court applies the most severe preventive measure in the form of pre-trial detention, suspects of espionage, sabotage or terrorist activities are placed in remand centres or designated units, known as detention prisons. The legal classification most commonly applied to persons remanded in custody and subsequently convicted is suspicion of committing offences specified in Art. 130 § 19 of the Criminal Code (participation in activities for foreign intelligence service) and Art. 258 § 2 of the Criminal Code (participation in an organised armed group with the aim of committing a crime or a fiscal offence of a terrorist nature). Often, considering the nature of the acts, the legal classification includes the indicated articles as well as Art. 255a § 2 of the Criminal Code (participation in training that could enable the commission of a terrorist offence, or independently familiarising oneself with content that could enable the commission of such an offence).

According to statistic information provided by the Central Prison Service Administration, as of 30 June 2025, a total of 34 inmates were being held in Polish prisons and remand centres in connection with the offences specified in Art. 130 § 1–9 of the Criminal Code. Of the indicated group, 18 persons have been convicted and 16 are in pre-trial detention. Among those convicted, the largest group were citizens of Ukraine – 10, followed by Belarus – 4, Russia – 3, and Canada – 1. Among those in pre-trial detention, citizens of Ukraine also predominated – 4, followed by Poland – 4, Russia – 4 (including 1 woman), Belarus – 3, Lithuania – 1.

In the group under study, a total of 23 persons were charged with the crime of espionage specified in Art. 130 § 1 of the Criminal Code, of whom 18 were convicted and 5 were in pre-trial detention. Among those convicted, the majority were Ukrainians – 10, followed by Belarusians – 4, Russians – 3 and 1 citizen of Canada. Among those temporarily detained, charges were brought against 3 Ukrainians, 1 Pole and 1 Russian.

The charge of espionage under Art. 130 § 2 of the Criminal Code was brought against 6 persons, each of whom is currently in pre-trial detention, including 2 Poles, 2 persons from Russia (including a woman) as well as 1 person from Belarus and 1 from Lithuania. The charge of declaring readiness to act on behalf of foreign intelligence services against the Republic of Poland, as specified in Art. 130 § 3 of the Criminal Code, was heard by 2 persons in pre-trial detention. They are citizens of Poland and Belarus.

However, the charge of suspicion of committing the offence specified in Art. 130 § 7, consisting of participating in the activities of a foreign intelligence service or acting on its behalf, committing diversion, sabotage or committing a terrorist offence, was heard by 2 Belarusians, 1 Russian and 1 Ukrainian.

The information provided indicates that a Ukrainian citizen is being held in remand centre as a remand prisoner, charged under Art. 255a § 2 of the Criminal Code.

Those in pre-trial detention and those who have been convicted are held in remand centres and closed prisons[35], i.e. penitentiary facilities with a high level of technical and security measures. The aforementioned group of 35 persons convicted and remanded in custody in connection with the acts referred to in Art. 130 § 1–9 and Art. 255a § 2 of the Criminal Code requires increased supervision by the Prison Service officers and particularly careful planning of penitentiary measures and security measures, taking into account the requirements of order and discipline that are the basis for the security of a prison or remand centre. This is supported by the nature of the crimes, the circumstances and motivations for committing them, the threat of severe punishment, the personality traits of inmates diagnosed by prison staff already in the initial period of isolation, and, at least in some cases, skills that may pose a threat to the security of the penitentiary unit.

It should be emphasised that 13 people from this group, i.e. 37%, were classified as persons posing a serious threat to society or a serious threat to the security of the facility. Therefore, they are directed to special units for so-called dangerous prisoners, where increased protection of the public and security of the prison are ensured. This means that the prison administration has deemed these individuals to pose a serious threat to society or to the security of the facility within the meaning of the provisions of Art. 88a § 1 of the Penal Enforcement Code. Qualification for this category entails a number of restrictions and the highest level of the prison regime, understood as the scope of rights granted and, above all, the obligations imposed by Polish law[36]. At the same time, a total of 141 convicted prisoners and detainees were held in all units

[35] Article 88 § 3 of the Penal Enforcement Code.

[36] Articles 88b and 88c of the Penal Enforcement Code.

for inmates posing a serious social threat or a serious threat to the security of the facility.

As of 31 July 2025, a total of 239 persons were detained in all penitentiary facilities for committing an offence specified in Art. 258 § 2, excluding acts specified in Art. 130 of the Criminal Code. This group include 185 convicted prisoners, including 4 women and 54 remand prisoners, including 3 women. The vast majority are held in closed prisons – 216. Seven of them have been classified as dangerous prisoners.

Poles definitely dominate the group of convicts – 181, including 3 women. Among them are citizens of Latvia – 2, Ukraine – 1, Armenia – 1 (woman). The majority of those temporarily detained are also Poles – 42, including 3 women. Followed by citizens of Ukraine – 7, Lithuania – 2, the Czech Republic – 1, Armenia – 1, Tajikistan – 1. The analysed group is dominated by Poles – 223 persons. Followed by Ukrainians – 8 and citizens of Lithuania – 2, Latvia – 2, Armenia – 2, the Czech Republic – 1, Tajikistan – 1.

Since the offence referred to in Art. 258 § 2 of the Criminal Code may be both criminal and terrorist in nature, it is difficult to determine unequivocally on the basis of statistical data how many convicted and remand prisoners in penitentiary facilities have committed acts of a terrorist nature. Separating this category requires additional analysis.

It can already be predicted that the group of spies, diversionists and saboteurs of various legal statuses, numbering 35 people, will grow, because many investigations, as prosecutors say, are ongoing, and the activity of foreign intelligence services remains high, despite the successes of the Polish services in detecting such threats. An example of this is the information posted on 1 August 2025 on the X platform by the Minister Coordinator of Special Services about the arrest by the Internal Security Agency of a citizen of one of the Asian countries who, as a staff officer of the military intelligence service (...) *was conducting intelligence activities detrimental to the security of the Republic of Poland and allied military structures. The National Prosecutor's Office presented him with charges, and on 1 August 2025, the suspect was remanded in custody for 3 months by court order*[37].

This is also confirmed by another announcement of the Internal Security Agency from 14 August 2025 regarding the arrest of a 17-year-old

[37] Tomasz Siemoniak, post on the X portal, 1 VIII 2025, https://x.com/TomaszSiemoniak/status/1951279798526890013?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E195 [accessed: 25 VIII 2025].

Ukrainian citizen who has been charged by the prosecutor's office with multiple offences, including those specified in Art. 130 § 7 of the Criminal Code (sabotage activities on behalf of a foreign secret service), and who has been remanded in custody for 3 months by the court[38].

Particularly important from the perspective of the Prison Service officers is to have as much information as possible about the person brought into custody, including their actual identity and motivation for committing the offences specified in Art. 130 § 1–9 or Art. 255a § 2 of the Criminal Code. The criminal activity may have various origins, i.e. it may be a direct consequence of the profession of a spy, agent or e.g. economic, resulting from blackmail, national or religious. Knowledge in this area is one of the prerequisites for officers when planning penitentiary and security measures related to, for example, decisions on placement in a specific penitentiary unit, ward, single or shared cell, selection of fellow inmates or monitoring[39]. Equally important, especially from the perspective of prison or remand centre security, is information about training courses completed or skills acquired that could facilitate espionage or sabotage activities. Such skills could be used during periods of isolation, e.g. to attempt an escape or cause danger. Information about persons with whom a convicted or remand prisoner intends to maintain or maintains contact by telephone, correspondence, visits to the prison or material support is of similar importance. Reliable information is obtained in accordance with all security procedures through cooperation between the Prison Service and other authorities, in particular the public prosecutor's office, the relevant uniformed services and the courts.

Summary

The outbreak of war in Ukraine at the beginning of 2022 and the accompanying huge wave of migration provided an opportunity to reflect on the state of the country's preparedness to function in extreme conditions. The Prison Service also conducted such an analysis, reviewing

[38] *Komunikat ABW ws. zatrzymania obywatela Ukrainy* (Eng. Statement of the ABW on the detention of a Ukrainian citizen), ABW, 14 VIII 2025, https://www.abw.gov.pl/pl/informacje/2668,Komunikat-ABW-ws-zatrzymania-obywatela-Ukrainy.html [accessed: 25 VIII 2025].

[39] Article 73a of the Penal Enforcement Code.

the tasks and defence regulations in force in this area, assessing their adequacy, determining the infrastructure resources available and the state of preparedness of the formation. Based on the audit results, a number of important decisions were made, including those related to the supply of fuel, communications equipment, ammunition, food and planning preparations to increase defence capabilities. Already in March 2022, a cooperation was established with Territorial Defence Forces, thanks to which in 2022 and 2023 the training process for the Prison Service officers was expanded to include typically military issues. The trainings were also carried out in facilities subordinate to the Ministry of Defence. The formal basis of this activities is the *Cooperation agreement between the command of the Territorial Defence Forces and the Central Prison Service Administration* concluded on 21 December 2022.

The issue of defence tasks and, more broadly, the role of the Prison Service in wartime remains not only an interesting but, above all, a very practical area of scientific research. At the same time, in the author's opinion, taking into account the ongoing war in Ukraine, Russia's imperial policy, hybrid warfare activities already underway on our territory, and the opinions of national and international security experts, it is extremely important for the management of the Prison Service to continue its planning, organisational, logistical and training efforts to prepare the formation as well as possible for a crisis. The experiences of the Ukrainian Prison Service (Ukrainian: Державна кримінально-виконавча служба України) operating in wartime conditions and carrying out activities characteristic of prison formation, which undertake a number of additional tasks, including supporting local communities and defence forces, securing the stay of prisoners of war and carrying out their exchange, organising a system of recruitment for military service among selected groups of convicts, and removing the effects of missile and drone attacks on penitentiary facilities.

The cooperation between the Prison Service and other uniformed services is particularly important for ensuring order and security in prisons and remand centres and for protecting the public from offenders who are deprived of their liberty. Due to the risks associated with activities of hybrid nature, cooperation with the Police, the Internal Security Agency, the Border Guard and the State Fire Service takes a new significance. The following measures should be considered essential: initiating, continuing and intensifying the following projects:

1) systematic conduct of exercises to improve cooperation between officers, based on scenarios that take into account real threats, including hybrid threats, in the areas of crisis command, information transfer, communication system compatibility and organising evacuation,
2) taking into account the importance of the medical component, i.e. first aid with elements of battlefield medicine, in the exercises carried out,
3) systematically organise, including remotely, training courses and workshops with experts to discuss the specific nature of certain threats and the possibility of applying preventive procedures, e.g. terrorism prevention, radicalisation, hybrid threats, cultural differences,
4) creating channels for the rapid transmission of information about threats and crisis situations, including appointing officers for cooperation, determining means of communication, including alternative ones, and the scope of information that can be transmitted, taking into account the applicable regulations in this area. If a need to change legal regulations is identified, initiating this process,
5) conducting periodic evaluations of cooperation and implementing conclusions directly into practice,
6) if necessary, updating or concluding new bilateral cooperation agreements that take into account the current situation and identified needs and specify, among other things, their scope, form and responsible persons,
7) undertaking joint scientific research and other projects, also financed from external sources, increasing the formation's ability to operate in conditions of threat, including hybrid threats.

In the context of ensuring order and security in prisons and remand centres as well as protecting society from offenders imprisoned in penitentiary facilities, it also seems important to develop formal procedures for prisoners who have committed offences specified in Art. 130 § 1–9, Art. 258 § 2 and Art. 255a § 2 of the Criminal Code. These may include, among other things:

– methods of monitoring formal, legal and personal situation,
– carrying out preventive measures, penitentiary measures, including the prevention of radicalisation,

– system of obtaining and transmitting information about individuals and cooperation in this area with other formations and institutions, including the appointment of officers responsible for implementing this process within the Prison Service structure.

One of the arguments in favour of taking such measures is the possible increase in the number of hybrid incidents predicted by experts, mainly generated by the activities of the Russian and Belarusian intelligence services. Furthermore, the serious threat for society and the security of prisons and remand centres resulting from the presence of perpetrators of such crimes in these places should be taken into account. Arguments are also provided by the aforementioned Report of the International Centre for Counter Terrorism (ICCT) and GLOBSEC, which identifies prisons as potential places for recruiting criminals to carry out hybrid attacks. It is also reasonable to continue planning, organisational and training work, as well as to develop algorithms for action that take into account the scale and nature of threats. The obligations arising from the provisions of the *Ordinance of the Minister of Justice of 5 March 2024 on the organisation of tasks within the framework of defence obligations* are also important in order to strengthen the defence capabilities of the formations. This requires close cooperation between the management of the Prison Service with the Ministry of Justice and the Ministry of National Defence.

Gen. (Ret.) Andrzej Leńczuk

Former Deputy Director General of the Prison Service responsible for the security of penitentiary units and the implementation of measures to increase the defence capabilities of the formation. Graduate of postgraduate studies and specialist courses in security, command, rehabilitation and radicalisation organised by the National Defence Academy (currently the War Studies University), the Adam Mickiewicz University in Poznań, the Internal Security Agency.

Contact: and.lenczuk@gmail.com

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 537–550

https://doi.org/10.4467/27204383TER.25.064.23051

Varia

From phishing to sabotage – the evolution of cyber threats to Poland. Conclusions from CSIRT GOV report for 2024

Monika Stodolnik

Independent author

https://orcid.org/0009-0000-5319-7968

Cyberspace, which is nowadays an arena of international competition, is undergoing dynamic changes, and recent years have demonstrated its importance in the context of state non-military activities. It enables operations of an intelligence, sabotage, disinformation nature, as well as influence operations. In this reality, cybersecurity should be an integral part of national resilience – alongside military, energy or economic security.

Poland as a member of international communities and, above all, as an entity actively supporting Ukraine in the face of the aggression from the Russian Federation, is among the countries particularly vulnerable to cyber attacks. *Report on the state of Poland's cybersecurity in 2024*, prepared by the Computer Security Incident Response Team CSIRT GOV operating within the structures of the Internal Security Agency (ABW), provides a valuable source of knowledge about current trends, attack vectors and the level of preparedness of public administration and critical infrastructure operators.

The analysis of the report presented in the article allows conclusions to be drawn not only about the technical aspects of the attacks, but also about

the threats to institutions and society in connection with contemporary phenomena in cyber space.

The role of the CSIRT GOV in the national cybersecurity system

The CSIRT GOV team serves as one of three national teams established by the Act on the national cybersecurity system[1], responsible for recognising and detecting of threats to public administration systems and critical infrastructure as well as preventing them. The CSIRT GOV carries out tasks imposed by both the Act on the national cybersecurity system and the Act on the Internal Security Agency and the Foreign Intelligence Agency[2]. It thus combines technical, operational and analytical competences, and is responsible for monitoring the cyberspace of the Republic of Poland, responding to incidents and coordinating activities in the field of its protection.

The CSIRT GOV is an operational element of the national cybersecurity system, directly supporting implementation of state tasks in the area of information protection, counteracting cyber threats, which is a key element of hybrid threats, and ensuring continuity of critical infrastructure operation. Its position within the ABW structure allows for combining ongoing technical analysis of incidents with an assessment of their broader context, including their impact on national security, taking into account the counterintelligence perspective. This assessment also covers the aspect of prevention – for state administration and operators of critical infrastructure.

Cybersecurity context in 2024

Throughout 2024, an elevated CRP alert level was maintained (in January and February – CHARLIE-CRP, and from March onwards – BRAVO-CRP[3] level). This involved maintaining constant readiness to respond to potential

[1] *Act of 5 July 2018 on the national cybersecurity system* (Journal of Laws of 2024, item 1077, as amended).

[2] *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (consolidated text, Journal of Laws of 2025, item 902, as amended).

[3] CSIRT GOV, *Report on the state of Poland's cybersecurity in 2024*, https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf, p. 5 [accessed: 1 X 2025].

terrorist activities, in accordance with the Act on anti-terrorist activities[4]. In a broader sense, this means constant readiness to respond to potential incidents of hybrid and cyber intelligence nature, due to the common attack vectors used in all these cases.

In 2024, the CSIRT GOV registered 17 439 reports on potential incidents, of which 3991 were considered to be actual breaches of the security of ICT systems (Figure 1)[5]. Although these figures indicate a decline compared to 2023, the authors of the report point out that this is not so much due to a reduction in the number of threats as to an improvement in the competence and awareness of users as well as the implementation of more effective protection mechanisms in institutions[6].

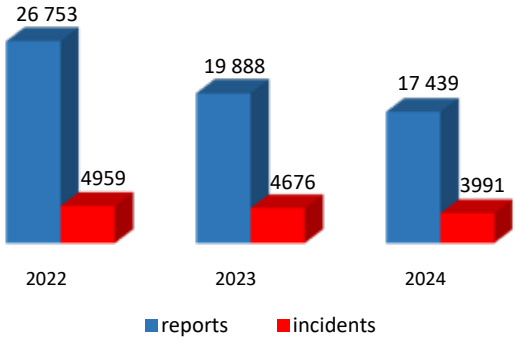


Figure 1. Number of reports and incidents recorded by the CSIRT GOV between 2022 and 2024.

Source: CSIRT GOV, *Report on the state of Poland's cybersecurity in 2024*, https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf, p. 10 [accessed: 1 X 2025].

The above data illustrates the increasing resilience of entities within the competence of the CSIRT GOV. Factors contributing to this increased resilience include:

1) preventing attacks at the network edge, i.e. effectively filtering and blocking intrusion attempts before they reach the right ICT systems. In the case of social engineering attacks using e-mail,

[4] *Act of 10 June 2016 on anti-terrorist activities* (consolidated text, Journal of Laws of 2025, item 194).

[5] CSIRT GOV, *Report on the state of Poland's cybersecurity...*, p. 10.

[6] Ibid.

this means using advanced anti-spam filters and reputation mechanisms on mail gateways; in the case of force attacks – implementing solutions such as IP address blocking (so-called blacklisting) or login attempt limits, and in the case of threats exploiting known vulnerabilities – keeping software up to date and eliminating security gaps;

2) increased awareness among users and administration employees, who are increasingly able to recognise and stop social engineering attempts (e.g. phishing, spearphishing, vishing) at the stage of contact with a message or suspicious link, before interacting with them. This is the result of an increasing number of training courses, warning messages and internal incidents response procedures. In 2024, the CSIRT GOV conducted training courses and workshops for nearly 1900 people, which is almost four times more than in 2023[7];
3) development of internal structures responsible for cybersecurity, such as SOC (Security Operations Center) teams or IT security units in public institutions. This allows for more effective handling of incidents at the local level, without the need to involve the CSIRT GOV each time;
4) strengthening interinstitutional cooperation and coordination, both within the three national CSIRT teams (GOV, MON, NASK) and between public administration and critical infrastructure operators. The exchange of threat intelligence and distribution of indicators of compromise (IoC) enable earlier detection of attack attempts and faster response to incidents. Based on incident reports and analysis of indicators of compromise from a single case, the CSIRT GOV develops warnings and recommendations for its entire area of competence, which helps prevent the spread of threats[8];
5) using security tests and audits as proactive measures that allow for the safe and controlled identification of system vulnerabilities before they are exploited by criminal and cyber offensive groups. Such activities, carried out by units within the structure of a given entity, external companies providing penetration testing services

[7] Ibid.

[8] Ibid., p. 15.

or the CSIRT GOV are an important element of prevention and improving the overall digital resilience of public administration entities and critical infrastructure operators. In 2024, the CSIRT GOV conducted a series of penetration tests in public administration institutions. These included, among other things, an assessment of system configurations, the effectiveness of defence mechanisms and the quality of vulnerability management. The conclusions from these tests were used to develop recommendations for specific entities[9].

Characteristics of cyber offensive activities in the context of cybersecurity in the Republic of Poland

The increase in the competence and capabilities of entities falling within the remit of the CSIRT GOV does not eliminate all threats. The analysis of incidents recorded in 2024 indicates that despite a noticeable improvement in security levels and user awareness, Polish cyberspace remains a place of activity for criminal, intelligence and hacktivist entities[10]. Events resulting from the actions of state-sponsored groups are one of the elements that make up incidents divided by the CSIRT GOV into two categories referred to as 'social engineering' and 'attack'. The first category mainly refers to phishing targeting users of organisations of interest to the actors, while the second concerns attempts and successful incidents of breaching the security of the ICT infrastructure of the attacked entities[11].

In 2024, the activity of state-sponsored groups and pro-Russian hacktivist collectives remained high. International reports place Poland among the leading European countries in terms of the number of socially and politically motivated, sponsored attacks. A report by Microsoft, an IT company, shows that in 2024 Poland was among the top three countries in Europe[12]. In turn, according to analysts from technology company,

[9] Ibid., p. 96.

[10] Ibid., p. 54.

[11] Ibid., pp. 12–13.

[12] *Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity*, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf, p. 13 [accessed: 19 III 2025].

Radware, Poland ranked second among European countries, behind Ukraine, in terms of the number of DDoS attacks[13] initiated by pro-Russian hacktivists[14]. This confirms that Poland, as an active ally of Ukraine and the eastern border of NATO and the European Union, was particularly vulnerable to asymmetric and hybrid actions in a cyberspace.

The CSIRT GOV report points to the predominance of attacks from the Russian direction, particularly those carried out by APT28 group (military unit no. 26165 within the 85th Main Special Service Centre of the General Staff Main Intelligence Directorate GRU[15]) and APT29 group[16] (subordinate to the Foreign Intelligence Service of the Russian Federation)[17]. The cases discussed, recorded in the cyberspace of the Republic of Poland, are also confirmed in the foreign publications cited in the article, which show the broader context of the activities of these groups.

The campaign by APT29 group, also known as Earth Koshchei, using RDP (remote desktop protocol) connection configuration files, was most likely (according to Microsoft analysts' findings based on registered domain names[18]) targeted, among others, at European government entities, particularly foreign and defence ministries, NATO structures, as well as the Ukrainian defence, energy and telecommunications sectors (Figure 2). This clearly fits into the context of the activities of the intelligence service of the state waging war against Ukraine and hybrid activities against NATO

[13] DDoS (distributed denial of service) attack – coordinated overload of system or service resources through a large number of simultaneous requests from different devices, intended to prevent proper operation.

[14] *2024 Global Threat Analysis Report, Executive Summary*, https://www.cisco.com/c/dam/m/en_in/events/security-conclave-2024/radware-threat-report-summary-2024.pdf, p. 9 [accessed: 2 X 2025].

[15] *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne* (Eng. Actions by the Russian GRU special service targeting Western logistics entities and technology companies), https://www.gov.pl/attachment/e9e86877-2ba0-478e-be36-f20d68474f37, p. 4 [accessed: 14 X 2025].

[16] APT29, MITRE ATT&CK, https://attack.mitre.org/groups/G0016/ [accessed: 14 X 2025].

[17] CSIRT GOV, *Report on the state of Poland's cybersecurity…*, p. 56.

[18] *Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files*, Microsoft Threat Intelligence, 29 X 2024, https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/ [accessed: 14 X 2025].

states, and the list of potential recipients of the campaign coincides with those previously recorded[19].

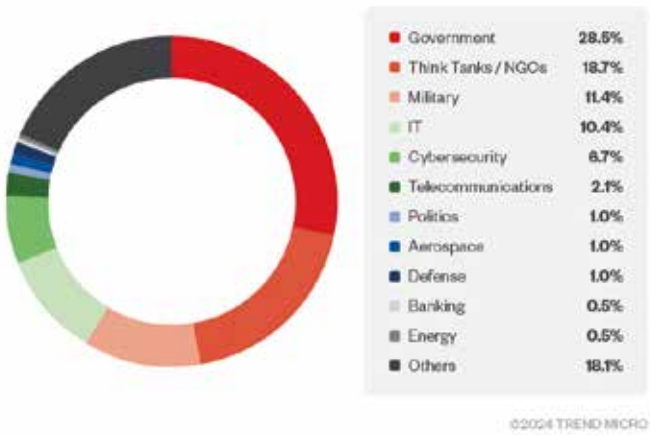


Figure 2. Percentage of domains registered by APT29 group, divided into economic sectors.

Source: *Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks*, Trend Micro, 17 XII 2024, https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html [accessed: 14 X 2025].

Among the threats posed by APT28 group, social engineering attacks predominated, including those involving the theft of e-mail login details and the infection of workstations with malware designed to steal sensitive information. Attacks exploiting various types of ICT system vulnerabilities were also identified[20]. In the context of ICT, 'vulnerabilities' refer to weaknesses in systems that that an attacker may use to carry out an effective attack[21]. However, it should be emphasised that this term does not refer exclusively to software errors recorded in the CVE (Common Vulnerabilities and Exposures) database, but also includes configuration errors, user behaviour and unintended software features that may be exploited in a manner contrary to their intended purpose[22].

[19] *Threat profile: APT29*, https://blackpointcyber.com/wp-content/uploads/2024/06/Threat-Profile-APT29_Blackpoint-Adversary-Pursuit-Group-APG_2024.pdf, p. 4 [accessed: 2 X 2025].

[20] CSIRT GOV, *Report on the state of Poland's cybersecurity...*, p. 57–66.

[21] *Vulnerability management, Understanding vulnerabilities*, National Cyber Security Centre, https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities [accessed: 10 X 2025].

[22] Ibid.

For example, a weak point in the system may be the use of simple or repetitive passwords, which is sometimes exploited in brute force attacks on login panels. The lack of filtering of traffic originating from anonymising VPN[23] or TOR[24] networks is also a significant weakness, making it easier for attackers to conceal the source of their activities. The analysed cases also noted the use of vulnerabilities enabling DCSync attacks[25] that allow domain credentials to be obtained[26]. In turn, certain system functions, such as mechanisms for granting permissions to email folders in Microsoft Exchange service, may be used in accordance with their design, but in a malicious manner to escalate privileges or exfiltrate data[27]. Such a broad range of vulnerability means that an organisation's cyber resilience depends not only on keeping its software up to date, but also on proper configuration of the environment, user discipline, and understanding how an adversary may exploit system functions.

The APT28 group used these funds to attack both entities in Poland, and in other countries, including those belonging to NATO. In May 2025, this was reported in a joint document by the services of the United States, the United Kingdom, Germany, the Czech Republic, Poland, Australia, Canada, Denmark, Estonia, France and the Netherlands[28]. This document provides a detailed description of the GRU's activities, as presented by the CSIRT GOV, towards entities carrying out tasks to support Ukraine in the war with Russia, as well as technology companies, and at the same time presents another dimension of the GRU's presence in Western countries and Ukraine, apart from its sabotage activities[29] (Figure 3).

[23] Virtual Private Network – encrypted tunnel service between the user's device and an intermediary server, masking the user's actual IP address and location.

[24] The Onion Router – anonymising network that redirects network traffic through a large number of encrypted nodes.

[25] DCSync attack – technique in which an attacker impersonates Active Directory domain controller and requests data synchronisation, thereby obtaining cryptographic hashes of credentials for all accounts in the domain.

[26] CSIRT GOV, *Report on the state of Poland's cybersecurity…*, p. 65.

[27] Ibid.

[28] *Działania rosyjskiej służby specjalnej GRU…*, p. 7.

[29] A. Jawor, *"Agenci jednorazowego użytku" rosyjskiego GRU. "Tajna" kampania sabotażu w Europie* (Eng. "Disposable agents" of the Russian GRU. "Secret" sabotage campaign in Europe), CyberDefence24, 3 X 2025, https://cyberdefence24.pl/armia-i-sluzby/agenci-jednorazowego-uzytku-rosyjskiego-gru-tajna-kampania-sabotazu-w-europie [accessed: 14 X 2025].

Figure 3. Geographical location of entities targeted by the GRU actions.

Source: *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne* (Eng. Actions by the Russian GRU special service targeting Western logistics entities and technology companies), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/attachment/e9e86877-2ba0-478e-be36-f20d68474f37, p. 7 [accessed: 14 X 2025].

Among the threats analysed by the CSIRT GOV, the activity of groups linked to the People's Republic of China, which in 2024 conducted intelligence operations against the Member States of the European Union, was identified. It focused on gathering information in the following areas: science and technology, energy and public administration. The attacks reported in Poland were carried out by two groups – Volt Typhoon[30] and APT15[31]. Furthermore, the network of TP-Link devices hijacked by Chinese cybercriminals has been identified. It was used to anonymise traffic in attacks on Microsoft services[32]. These activities are part of a long-term strategy to covertly obtain information of great importance to industry and the economy in order to strengthen China's technological potential and competitiveness on the international stage.

Also noteworthy is the activity of entities associated with the Republic of Belarus, which are highly likely to be working in cooperation with

[30] Volt Typhoon – the group attributed to the People's Liberation Army, attacking the critical infrastructure of Western countries in order to conduct intelligence operations.

[31] APT15 – cyber offensive group attributed to China, pursuing China's strategic intelligence objectives.

[32] CSIRT GOV, *Report on the state of Poland's cybersecurity...*, pp. 72–73, 75.

the services of the Russian Federation. In 2024, the activities of UNC1151 group, which conducts two types of activities – disinformation and intelligence, were observed[33]. Its campaigns included phishing messages impersonating login panels for the most popular Polish e-mail services – Interia, Onet, Wirtualna Polska. The aim was to obtain login details, take over accounts and build the infrastructure needed for disinformation campaigns. In order to carry out espionage activities, computers were infected with malware that allowed full control of the devices to be taken over. This was done via email. The group's activity has been observed since at least 2017[34], which indicates the long-term, reconnaissance nature of their activities and their focus on destabilising the state through information warfare.

The report also noted the activities of pro-Russian hacktivist groups: Beregini and Zarya. The groups published manipulated data stolen from the Polish Anti-Doping Agency to undermine the credibility of Polish athletes during the Olympic Games in Paris[35]. These activities are referred to as *hack-and-leak* operations. They combine a cyber attack with information manipulation aimed at influencing public opinion[36].

In the case of industrial infrastructure (Operational Technology/ Industrial Control Systems), the hacktivist activity increasingly involves targets related to public utility installations, such as sewage treatment plants, water supply networks and pumping stations[37]. This is international trend observed in the United States[38], the Netherlands, France[39] and

[33] Ibid., pp. 69–72.

[34] *Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity*, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, p. 8 [accessed: 14 X 2025].

[35] CSIRT GOV, *Report on the state of Poland's cybersecurity*..., p. 6.

[36] S. Palczewski, *Kampanie hack-and-leak. Czy namieszają przed wyborami w Polsce?* (Eng. Hack-and-leak campaigns. Will they stir things up before the elections in Poland?), Demagog, 17 VIII 2023, https://demagog.org.pl/analizy_i_raporty/kampanie-hack-and-leak-czy-namieszaja-przed-wyborami-w-polsce/ [accessed: 13 X 2025].

[37] CSIRT GOV, *Report on the state of Poland's cybersecurity*..., p. 55.

[38] *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity*, https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf, p. 1 [accessed: 1 X 2025].

[39] *Cyber Insight, Sector 16 group*, https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Sector16/Sector16Group.pdf, p. 10 [accessed: 1 X 2025].

Norway[40]. The CSIRT GOV report does not specify any particular cases, but only points to the intensification of such activities. Among the most active collectives showing the results of attacks carried out on dedicated channels on the Telegram platform, the following should be noted: Cyber Army of Russia Reborn (CARR), Z-Pentest[41], Sector16 and TwoNet[42]. The latter three are part of an alliance operating under the leadership of the OverFlame (Figure 4).

Figure 4. Hacktivist groups focused within OverFlame collective.

Source: *Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS*, Forescout, 9 X 2025, https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/ [accessed: 12 X 2025].

The activity of these collectives is characterised by high dynamics. Channels are frequently deactivated, new groups and alliances as well as conflicts are formed. At the same time, there are many indications that behind many collectives there is a small group of the same people who

[40] M. Bryant, *Russian hackers seized control of Norwegian dam, spy chief says*, The Guardian, 14 VIII 2025, https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway [accessed: 14 X 2025].

[41] CSIRT GOV, *Report on the state of Poland's cybersecurity*..., p. 74.

[42] *Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS*, Forescout, 9 X 2025, https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/ [accessed: 12 X 2025].

act on behalf of the Russian services. In January 2025, the Ukrainian Molfar Intelligence Institute published data on administrators and members of NoName057(16) and DDoSia groups carrying out DDoS attacks against websites and online services in countries opposed to the policy of the Russian Federation[43]. Julia Vladimirovna Pankratova, who was identified there, and Denis Olegovich Dekgtyarenko were included on the list of individuals sanctioned by the United States for their role in attacks by the CARR hacker group on the US critical infrastructure[44]. Analysts at Mandiant, the US cybersecurity company, pointed out in their report on the Sandworm group (identified as the military unit 74455 within the Main Centre for Special Technologies of the GRU) its links to XakNet, Solntsepek and CARR collectives[45]. This most likely means that the CARR and the groups working in alliance with it carry out tasks on behalf of the Russian Federation, which calls into question the grassroots nature of hacktivism.

Supply chain security

One of the most important conclusions of the CSIRT GOV report is to draw attention to the growing risk associated with third parties – IT service providers, outsourcing companies and contractors. Supply chain incidents show that organisation's security is only as strong as the weakest link in its ecosystem. Restrictive internal procedures do not guarantee security if external partners do not maintain an adequate level of protection[46]. In 2024, incidents involving system compromises, data exfiltration and publication occurred in companies providing IT and automation services,

[43] *Russian Cyber Army. Who is it?*, Molfar Intelligence Institute, 23 I 2025, https://www.molfar.institute/en/russian-cyber-army/ [accessed: 12 X 2025].

[44] *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn,* U.S. Department of the Treasury, 19 VII 2024, https://home.treasury.gov/news/press-releases/jy2473 [accessed: 11 X 2025].

[45] G. Roncone, D. Black, J. Wolfram, T. McLellan, N. Simonian, R. Hall, A. Prokopenkov, D. Perez, L. Aytes, A. Wahlstrom, *APT44: Unearthing Sandworm*, https://*services*.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf, pp. 12–13 [accessed: 19 III 2025].

[46] CSIRT GOV, *Report on the state of Poland's cybersecurity*..., p. 113.

e.g. AIUT Sp. z o.o.[47] and Atende S.A.[48] In 2025, these were EuroCert Sp. z o.o.[49], a provider of qualified signature services, and the security company Ekotrade Sp. z o.o.[50]. These actions resulted in the disclosure of sensitive data about employees, customers and contracts.

In the context of national security, this means that the supply chain must be treated as an integral part of the state's security system. Regular security audits, remote access control, data protection in transit and at rest, verification of contracts with suppliers, and the development of business continuity plans should be standard practice in public institutions and strategically important enterprises, including among critical infrastructure operators[51].

Summary

When analysing the CSIRT GOV report in a broader context, it should be noted that cyber attacks are increasingly becoming part of conflicts below the threshold of war, which fits in with Russia's concept of new-generation warfare. They serve to gather intelligence, spread disinformation and destabilise without the need to use military force. In this sense, cybersecurity is no longer just a technological domain, but also a strategic and political one, as it is an area where the interests of states, the private sector and society intersect. Attacks on public administration, critical infrastructure and public media have symbolic and psychological dimensions – they undermine trust in state institutions by exposing their weaknesses and generate media hype. The ability to respond quickly, inform

[47] *Incydent bezpieczeństwa* (Eng. Security incydent), Aiut, https://aiut.com/incydent-bezpieczenstwa/ [accessed: 12 X 2025].

[48] *Komunikat Atende w związku z upublicznieniem ukradzionych danych* (Eng. Atende statement regarding the disclosure of stolen data), Atende, 22 X 2024, https://atende.pl/pl/aktualnosci/komunikat-atende-w-zwiazku-z-upublicznieniem-ukradzionych-danych [accessed: 12 X 2025].

[49] *Atak na EuroCert – oświadczenie* (Eng. The attack on EuroCert – statement), EuroCert, 15 I 2025, https://eurocert.pl/atak-na-eurocert-oswiadczenie/ [accessed: 12 X 2025].

[50] *Komunikat dotyczący ataku hakerskiego na infrastrukturę informatyczną Ekotrade Sp. z o.o.* (Eng. Statement regarding the cyber attack on the IT infrastructure of Ekotrade Sp. z o.o.), https://ekotrade.com.pl/img/rodo/KOMUNIKAT-EKOTRADE-dla-pracownikow.pdf [accessed: 12 X 2025].

[51] CSIRT GOV, *Report on the state of Poland's cybersecurity*..., p. 116.

public opinion in accordance with established strategic communication scenarios, and restore organisation continuity is one of the most important aspects of defence.

The CSIRT GOV report confirms that the cybersecurity of the Republic of Poland is now an integral part of national security, and its maintaining requires synergy between the technical, legal and organisational activities of the state. The scale of threats to Poland is not diminishing, which is why it is so important that the ability of institutions to identify them, mitigate their effects and build resilience continues to grow. Cooperation and information exchange are very important. The constantly evolving national cybersecurity system, expanded to include sectoral CSIRT teams, together with national teams, competent cybersecurity authorities, operators of essential services and other institutions, must constitute an effective shield against threats of international nature. Security is a continuous process that requires constant verification, audits and flexibility in order to adapt to changing technological and geopolitical conditions. New vulnerabilities and attack techniques emerging every day, and above all, the development of artificial intelligence, which will support attackers in creating phishing content and new versions of malware, mean that it is necessary to increase one's resilience and ability to respond to emerging threats. This is more important than ever before.

The dynamically changing nature of threats in cyberspace highlights the urgent need to abandon the reactive model in favour of actions aimed at building Poland's cyberspace resilience. They should consist primarily of implementing comprehensive, system-level solutions, as well as improving internal organisational regulations. This direction is reflected in the proposed legislative changes, particularly in the amendment to the Act on national cybersecurity system and the Act on crisis management. Their implementation in 2025 aims to improve coordination of actions and exchange of information, take into account the vulnerability of supply chains, and increase the overall institutional resilience of the state to incidents in the cyberspace. The effectiveness of these solutions will largely depend on the extent to which they are implemented and on the ability to adapt in the face of further evolution of cyber threats.

Monika Stodolnik

Officer of the Internal Security Agency.

Contact: monika.stodolnik@abw.gov.pl

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 551–560

https://doi.org/10.4467/27204383TER.25.065.23052

Varia

Building resilience of the European railway sector to hybrid threats. Polish contribution to good practices and increased safety

Tomasz Lachowicz

Independent author

https://orcid.org/0009-0002-4344-7120

Following a series of terrorist attacks in Europe in 2015–2017, which also targeted rail transport, the issue of safety became one of the European Union's priorities.

The ministerial meeting of Member States on 29 August 2015 in Paris and the so-called Paris Declaration provided political support for the European Commission to take urgent action to improve safety in the EU. In turn, at the EU Council meeting in Luxembourg on 8 October 2015, proposals to develop common safety rules for international trains and high-speed railways were adopted. The European Commission was thus obliged to analyse the impact of a number of initiatives to improve passenger rail transport safety in the EU.

In 2017, Jean-Claude Juncker, the then President of the European Commission, emphasised the need for a strong and secure Union in his *State of the Union* address, and in the following years, issues related to land transport safety, including the safety of passenger and public places in particular, remained priority topics on the EU agenda.

Poland was involved in this work, including through the Representative Office of the Polish State Railways (PKP S.A.) in Brussels, responsible for cooperation with EU institutions and international railway organisations. These joint efforts resulted in initiatives to increase security in the EU, including in the field of transport.

RAILSEC platform – plan to improve rail passenger safety

In view of the growing risk of terrorist attacks on passenger rail transport, the Directorate-General for Mobility and Transport (DG MOVE) responsible for transport policy in the EU conducted a public consultation with the rail sector in 2016–2017. The aim was to explore possible EU legislative and non-legislative initiatives in this area. The Representative Office of PKP was involved in this process, coordinating the contribution of the PKP companies and developing a common position of European railways within the Community of European Railways and Infrastructure Managers (CER). The consultation resulted in the European Commission publishing the *EU action plan to improve the security of rail passengers and staff* in mid-2018, which initiated the establishment of the EU Rail Passenger Security Platform (RAILSEC). Its members included experts from the EU Member States and from countries belonging to the European Free Trade Association (EFTA), delegated to it from national authorities and services. Other stakeholders, for instance railway organisations such as the European Railway Agency (ERA), Colpofer, were granted observer status. The platform members' meetings were closed-door and were chaired jointly by the DG MOVE and the Directorate-General for Migration and Home Affairs (DG HOME). The work covered, among other things:

- updating the methodology for assessing the risk of terrorist threats in passenger rail transport, as well as a set of guidelines, recommendations and best practices that can be used to conduct risk assessments by competent entities at national and local level,
- creating a list of the most useful technologies for protecting trains and railway stations (mainly in the context of detecting explosives and weapons). On this basis, the European Commission (DG MOVE/DG HOME) developed a catalogue of best practices and the most effective technologies, including in terms of cost and solutions,

- developing guidelines on insider threat, including a list of workplaces that are vulnerable to terrorist threats and require special attention from employers,
- other activities – including in the areas of cybersecurity, CBRN (chemical, biological, radiological, nuclear) threats and railway safety management plans.

RAILSEC platform has become part of the larger and broader thematic expert platform of Member States on land transport – the Land Transport Security (LANDSEC), which has been operating for years.

The Representative Office of PKP monitored the activities of RAILSEC and participated in working group meetings, communicating the results of its work (guidelines, recommendations, etc.) that were relevant to the PKP Group. It also participates in LANDSEC meetings.

Action plan for the protection of public spaces

In parallel with activities undertaken in the area of passenger safety in rail transport, DG HOME was involved in work related to the protection of public spaces. In October 2017, the *Action Plan to support the protection of public spaces* was published, establishing EU forum of public and private operators. Its main task is to exchange know-how and best practices in the field of public spaces safety. This is achieved through thematic meetings of platform members, concerning, among other things, transport, the organisation of mass events and the protection of commercial spaces. The forum has developed a number of guidelines and good practices in the context of actions that operators can take to strengthen the security and protection of public spaces.

The Representative Office of PKP has been an active member of this body since its inception. It presents the good practices and strategies adopted by the PKP Group in the field of safety and provides PKP Group companies with information from meetings, including on solutions developed in the area of safety.

ReArm Europe/Readiness 2030 – the European Union defence financing plan

In March 2025, the European Commission presented joint White Paper on European Defence Readiness 2030. It is complemented by Plan ReArm Europe, an ambitious defence package under which up to EUR 800 billion (through various financial instruments) will be allocated to investments that increase defence capabilities of the Member States. The military mobility package and EU's defence transformation action plan were identified as priorities. The package includes, among other things, conclusions drawn from the revised EU military mobility action plan 2.0 and the 2024 military mobility commitments. It was developed in close coordination with the European External Action Service and the European Defence Agency, ensuring consistency with NATO standards and procedures.

The package consists of a communication on military mobility and a proposal for a regulation establishing a framework for measures to facilitate the transport of military equipment, goods and personnel by the EU[1] (to which a European Commission working document has been added), and introducing changes to the EU regulations and better taking into account the requirements of the military mobility from a dual-use perspective – military and civilian.

The European Commission aims to establish by 2027 a military Schengen zone and transform the defence industry. The intention of these measures is to introduce facilitations that will enable military units, equipment and resources to be moved across Europe on a large scale and at high speed, in an efficient and coordinated manner. This is to be achieved by:

- removing regulatory barriers – by introducing rules on harmonised military mobility at EU level and setting out rules and procedures on cross-border military movements, with applications processed within a maximum of three days and simplified customs formalities;
- establishment of structures in case of an emergency – by appointing the European Military Mobility Enhanced Response System (EMERS) to speed up procedures and ensure priority access to

[1] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework of measures to facilitate the transport of military equipment, goods and personnel across the Union*, https://eur-lex.europa.eu/resource.html?uri=cellar:b84cfa7d-c619-11f0-8da2-01aa75ed71a1.0001.02/DOC_1&format=PDF.

the infrastructure. EMERS shall support the armed forces operating in the context of the EU and NATO;

- increasing the resilience of transport infrastructure – by adapting key EU military mobility corridors to dual-use standards and protecting strategic infrastructure with a new set of tools. Targeted investments are intended to strengthen cybersecurity, energy security and readiness both in times of peace and crisis;
- pooling and sharing capabilities – by increasing the readiness, solidarity and availability of military mobility capabilities for the Member States. This is to be achieved through the introduction of a solidarity pool and the creation of a digital information exchange system for the purposes of military mobility;
- strengthening governance and coordination – the implementation of changes and the monitoring of readiness will be the responsibility of a new EU Military Mobility Transport Group and a reinforced Trans-European Transport Network (TEN-T). They will be supported by national coordinators for cross-border military transport operating in each Member State;
- innovations for defence readiness.

The European Commission has committed to reviewing, in 2026, the implementing regulation on railway infrastructure capacity in order to ensure that it meets the needs of military transport, taking into account input from military representatives. Military transport is to be exempt from traffic restrictions resulting from vehicle environmental efficiency requirements, air-quality controls or noise-level controls (with regard to airports or ports), and railway vehicles will be able to operate with greater flexibility. Furthermore, in 2026, the Commission with the support of, inter alia, the ERA and infrastructure managers, is to carry out a reassessment of the physical constraints of railway infrastructure on priority military mobility corridors in order to facilitate the transport of oversized cargo. It will also work, with the support of the ERA as well, on strengthening the railway traffic management system in order to ensure continuity of operations in the event of sabotage or another system failure. The regulation also addresses, inter alia, issues related to individual train paths for military rail transport, the use of railway vehicles outside their designated area of operation, and the identification of railway vehicles for potential use in military transport.

The package is of great importance for Polish railways and, above all, for the functioning of the state in crisis situations. In the event of an armed

conflict, the ability of the railway system to maintain continuity of supplies and support mobilisation is crucial for an effective response and the country's stability. Rail transport enables the efficient movement of armed forces and military equipment. The railway sector and the rail industry must also keep pace with innovations and changes resulting from hybrid threats. This requires financial resources and the development of appropriate competencies. The Russian aggression against Ukraine has shown how rapidly offensive and defensive technologies are developing. Innovations such as artificial intelligence, quantum systems, drones and space technologies are changing the nature of the battlefield and operations conducted on it. This makes the role of logistics all the more important.

Polish contribution to security – activity of the PKP Representative Office at the EU level

For many years, the PKP Representative Office has been engaged in efforts to improve security in rail transport, actively cooperating with EU institutions and participating in numerous international expert platforms, initiatives and projects. It also initiates international actions aimed at strengthening railway security. As the body responsible for cooperation and coordination of the PKP companies within the world's largest railway organisation – the International Union of Railways (L'Union internationale des chemins de fer, UIC) – the PKP Representative Office additionally takes part, together with the PKP S.A. Security Office, in UIC activities and projects in the field of railway security. This is, among others, the UIC Security Platform (together with the UIC Security Hub established within it), which was chaired by the PKP S.A. for a period of time. Together with the largest European railways, the PKP Representative Office also initiated several international projects, the coordination of which was later handed over to the UIC.

The SHERPA project (Shared and Coherent European Railway Protection Approach)[2]

The project was initiated at the turn of 2017 and 2018 and involved developing a coherent, comprehensive approach by European railways to ensuring passenger safety in rail transport in the context of terrorist

[2] https://sherpa-rail-project.eu/.

threats. The project was led by the UIC, with the consortium members being the largest European railways: Polish PKP, German DB, French SNCF, Italian FSI and Belgian SNCB. It lasted two years and concluded in 2020 with 90% of its funding provided by the EU.

Within the framework of this project, terrorist threats targeting railway stations and trains were analysed, including attacks and acts of sabotage or attempts thereof. This allowed for the development of best protection practices along with a catalogue of railway needs, including a unified approach to assessing and managing risks related to terrorist threats in rail transport, requirements and specifications for detection equipment, and new technological solutions. During its implementation, the PKP S.A. organised in Warsaw workshops involving numerous international experts, focused on improving safety at stations and on trains.

Due to this project, the UIC significantly strengthened the aforementioned security platform and the hub operating within it, which contains best practices, methodologies and technological solutions for improving security in rail transport.

The IMPRESS project (IMProving Railway sEcurity through awareneSS and training)[3]

In 2022, the PKP Representative Office initiated another international project, this time with the participation of the SNCB Railway, FSI Railway and the Dutch NS Railway, as well as the German Police University (Deutsche Hochschule der Polizei) as the expert party and the UIC as the consortium coordinator. It was a continuation of the SHERPA project and aimed to improve rail transport security by raising awareness of threats and providing training. The project budget amounted to over EUR 1.058 million, and due to high evaluations by the European Commission (DG HOME), 90% of it was funded by the EU. The project lasted two years and concluded in 2025.

Its objective was to strengthen the security system of railway public spaces (train stations, trains) by involving not only railway staff, police services, railway and station security, but also other entities, including commercial tenants, station and train service personnel. The aim was to raise awareness among these groups, and especially among the so-called first respondents, about terrorist threats, suspicious behaviour and situations, and how to respond appropriately, as well as to improve cooperation and

[3] https://impress-rail-project.eu/.

coordination between public and private entities within the public railway environment. This is very important, proactive component of railway and train security.

The PKP S.A. participation in the IMPRESS project resulted in the development of educational and training modules that increased awareness among both railway employees and other entities operating within the railway environment, as well as in the enhancement of knowledge and the creation of specific security solutions for train stations. It also contributed to strengthening cooperation of the PKP Group with the largest European railway companies, as well as security experts.

The CBRNe4Rail project – CBRNe preparedness for passenger transport hubs[4]

The project started in 2025 and focuses on the detection of chemical, biological, radiological and nuclear (CBRNe) threats in railway transport, as well as on their prevention and response. Its objective is to increase awareness and the capacity of railway sector stakeholders to respond effectively to these threats at railway stations by improving their security plans and providing training to railway personnel. The project includes the full spectrum of CBRNe threats, including explosives as a means of delivering CBRN substances. It focuses on railway stations as a primary component of railway infrastructure and a key element of vulnerability to threats in public spaces. It includes both the public spaces inside stations and the public areas in their vicinity.

The CBRNe4Rail project is funded by the European Commission. Its initiator is the UIC, in cooperation with the PKP Representative Office and other partners.

Mobile detectors for explosives and chemical substances, provided in cooperation with the European Commission (DG HOME)

In the area of improving security on the Polish railway, the PKP Representative Office works closely with the DG HOME, including its counter-terrorism unit. Thanks to this cooperation, the European Commission has provided the PKP and the services (the Police and

[4] https://www.cbrne4rail.eu/.

the Border Guard operating in railway areas) with advanced mobile detectors for explosives and chemical substances (IONSCAN 600) free of charge. Initially, it was assumed that testing these devices in railway areas within the country would last six months. However, the pilot, which started in November 2024, was extended by the European Commission until June 2026. Its aim is both to strengthen the security of railway operations in Poland (the detectors are used, among others, at railway stations, on trains, at railway border crossings, in cargo terminals, and during sending conductor parcels) and to assess the usefulness of these devices in railway areas.

As part of the preparations for the pilot, the PKP Representative Office organised a meeting in Warsaw with security directors from the PKP companies (including the Railway Security Guard), followed by workshops dedicated to terrorist and sabotage threats in railway transport. The workshops were attended by experts from the European Commission, the Police, the Border Guard, the Internal Security Agency and security specialists from the PKP Group. Furthermore, the PKP Representative Office, together with the Commission, organised numerous workshop meetings to review the experiences of the services in using detectors gained so far. To date, the use of this equipment has brought tangible results.

Railway safety in the context of the current geopolitical situation

Attacks on railway infrastructure, signaling systems, and power supply systems have been observed for a long time in many European countries with well-developed railway networks. Poland is not an isolated case. Such incidents have occurred repeatedly in Germany and other countries, for example, on the eve of the Olympic Games in Paris. For this reason, the railway sector cooperates closely within international railway organisations. Cooperation with the services is also valuable. It is worth to emphasise, that from January 2026, the PKP S.A. is the first railway from the Central and Eastern European countries to assume leadership in the CER (The Community of European Railway and Infrastructure Companies)[5]. This is the result of the trust of the European partners with whom the PKP Representative Office cooperates, and a recognition

[5] https://www.cer.be/.

of its work and commitment in Brussels. Issues related to enhancing the security and resilience of the European railway system will certainly be one of the priorities of the PKP S.A. leadership in the CER.

The outbreak of war in Ukraine is associated with the emergence of many hybrid threats. They also concern railways, as this type of transport remains crucial for military mobility. Europe must draw lessons from Ukraine's experiences – strengthening resilience and building a new defence ecosystem that combines industry, innovations and new technologies. It is also important to strengthen cooperation between the EU institutions and NATO. The PKP Group remains a participant in this dialogue, both at the EU level and in the sphere of civilian advisory services for NATO Headquarters.

In 1958, the British Prime Minister Harold Macmillan said: *Jaw, jaw is better than war, war*, which loosely translated means that discussion is better than conflict. It would certainly be preferable if problems were resolved through dialogue. However, it is clear that this is wishful thinking. Therefore, it is necessary to act in a deterrent manner, anticipate, adapt, and actively build the resilience of the railway system and the supply chain. This also applies to other dimensions of our security. What is needed is intensive cooperation on multiple levels, based on trust and a common vision.

Tomasz Lachowicz

The Head of Representative Office of PKP in Brussels. He is Senior Transport Advisor and the Rail Coordinator for the NATO Task Group responsible for rail transport.

Expert in international cooperation, EU policies, the European Union's transport agenda, lobbying, strategy development and decision-making processes in the EU. In 2021–2025, he was responsible for chairing PKP in the International Union of Railways (UIC) in Paris, and since January 2026 he will be responsible for coordinating the leadership of PKP in the Community of European Railway and Infrastructure Companies (CER) in Brussels.

He is a member the Rail Forum Europe (RFE) Advisory Committee in the European Parliament.

Graduate of the Faculty of Law and Administration, University of Warsaw, Faculty of Law, Cardinal Stefan Wyszyński University in Warsaw and postgraduate management studies in economics at the SGH Warsaw School of Economics. He graduated with honours from an MBA programme.

He was awarded the Medal of Meritorious for Transport of the Republic of Poland.

Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 561–567

https://doi.org/10.4467/27204383TER.25.066.23053

Varia

Global Internet Forum to Counter Terrorism. Combating terrorist and extremist content in the digital space

The Global Internet Forum to Counter Terrorism (GIFCT) is independent non-profit organisation established in 2017 in the US. Its creation was intended as a response to the increasing use of online platforms and social media by terrorist organisations and extremist movements for propaganda, recruitment, planning acts of violence and operational communication. The initiators were four leading entities in the technology sector: Meta Platforms, Inc. (formerly Facebook), Microsoft Corporation, YouTube LLC (a subsidiary of Google LLC) and X Corp. (formerly Twitter).

The aim of establishing the GIFCT was to create a framework for cooperation between the private sector, public administration, non-governmental organisations and academia in the field of information exchange, development of technological tools and setting standards for counteracting the use of digital space for terrorist and extremist purposes. The primary task of the GIFCT is to prevent the abuse of digital technologies by entities promoting political violence by limiting their activity in the online space.

One of the organisation's key operational instruments is hash-sharing database – a shared database containing so-called hashes, i.e. digital fingerprints of image and video files identified as terrorist and extremist materials. This database enables the GIFCT members to quickly detect and remove such content from digital platforms.

The criteria for joining the GIFCT include, among others:

- having publicly available rules and regulations prohibiting terrorist and extremist activities,
- implementation of procedures for receiving and analysing reports of violations of these rules and responding to them,
- commitment to developing innovative technological tools for countering terrorism in the digital environment,
- regular publication of transparency reports,
- commitment to respect human rights according to the United Nations Guiding Principles on Business and Human Rights,
- supporting civil society initiatives in the field of terrorism and extremism prevention.

After positive verification of the application, the platform obtains the GIFCT member status. This ensures the platform, among other things, the access to hash-sharing database, allows to participate in crisis communication processes and research briefings as well as gives them priority access to workshops and seminars.

Currently, the GIFCT has over 30 members from technology sector. These include the following companies: Meta Platforms, Microsoft, YouTube, X, Airbnb, Discord, Dropbox, LinkedIn, Amazon, Mailchimp, Pinterest, JustPaste.it, Tumblr, WordPress.com and Zoom.

Research activities of the GIFCT are supported by the Global Network on Extremism and Technology (GNET) – a project carried out by a consortium of academic institutions and think tanks, including the International Centre for the Study of Radicalisation at King's College London. The mission of the GNET is conducting interdisciplinary research on how terrorist and extremist entities use technology as well as translating research findings into policy-relevant outputs, supporting technology sector, public administration and civil society organisations.

In April 2025, Naureen Chowdhury Fink, executive director of the GIFCT, visited Warsaw at the invitation of the Ministry of Foreign Affairs of the Republic of Poland. She took part in an informal meeting of the Working Party on Terrorism COTER, devoted to challenges as well as extremist and terrorist threats facing the EU countries. It was an opportunity for a brief discussion about the organisation she co-leads.

Damian Szlachter: the GIFCT is becoming an increasingly significant global initiative in the ongoing effort to combat terrorism and violent extremism online. Could you elaborate on the forms of cooperation you offer to public and scientific institutions, particularly in countries which are just beginning to build their capabilities in this area, e.g. such as Poland?

Naureen Chowdhury Fink: Cooperation across sectors is at the heart of what we do. When it comes to collaboration with public and scientific institutions, one example I would highlight is our academic research arm – the GNET. Through this network, we actively invite contributions from around the world[1] to ensure that the reports we prepare, publications as well as insights reflect diverse perspectives and can meaningfully inform the GIFCT member companies about emerging trends and dynamics – including those in countries like Poland.

Our regional workshops are another important form of cooperation[2]. We often co-develop these workshops with local partners to ensure that efforts to convene government, the private sector and civil society are grounded in regional knowledge and context.

We always welcome tech companies to consider joining the GIFCT as members if they meet our established criteria. All the information is available online[3]. We would very much welcome interest from Polish tech companies who want to be part of this work.

One notable challenge is effectively defining and identifying terrorist content. How does the GIFCT address linguistic, cultural and contextual differences when evaluating such materials?

That's a great question. Given the wide range of cultural, contextual, linguistic differences, one of the key things we

[1] See: https://gnet-research.org/write-for-us/. All the footnotes come from the editors.

[2] See: https://gifct.org/events/.

[3] See: https://docs.google.com/forms/d/e/1FAIpQLSfSaduWvuCUmU1P74HhEeAqT7tLu4VLx0863LuA0XWdV93BuQ/viewform.

focus on is keeping our member companies informed about regional dynamics, emerging trends and specific incidents so it helps them identify context for content. Our aim is to ensure that members have access to global experts and relevant expertise. A significant part of this effort is supported through the GNET, as well as other GIFCT activities. When member companies are interested in better understanding a particular region, they can request tailored informational materials or bespoke resources. In those cases, we work to connect them directly with subject-matter experts who can help answer their questions and provide deeper insight into the cultural and contextual nuances they may be encountering.

The GIFCT has established a hash-sharing database designed to facilitate the rapid removal of terrorist content. To what extent has this tool demonstrated effectiveness, and are smaller digital platforms receptive to utilising it?

Hash-sharing database currently contains approximately 2.3 million hashes, representing around 408 000 distinct pieces of content[4]. We are really encouraged by the level of adoption – it is a positive sign that over 35 member companies, including a range of platforms, are engaged with the database to varying degrees of integration. It is important to note that not all member companies are structured in a way that makes direct use of hashes relevant to their services. The value of the hash-sharing database extends beyond the technology itself – it fosters dialogue among members about what types of content are included, how they are integrated and how different companies can make use of the information. In some cases, we also discuss non-hashable resources that can support content moderation and safety efforts. We are very pleased to see that so many member companies – large and small – are joining the GIFCT and finding value in this shared environment.

[4] See: https://gifct.org/hsdb/.

Recent years have seen considerable discussion regarding the influence of algorithms in spreading radical content. Does the GIFCT implement measures to mitigate their impact on the process of radicalisation?

We do not produce algorithms, but what we do is make sure our member companies are aware of the research and the concerns that exist around this issue. Our Independent Advisory Committee[5] includes representatives from the EU, the US, the United Kingdom and several other countries – each with different perspectives on managing the digital ecosystem, but many of them share concerns about algorithms and their potential impact.

Part of our role is to facilitate information sharing – helping our members understand how these concerns are emerging, where some of the proposed solutions lie, and making sure they are aware of the latest research. We are not in a position to implement changes ourselves, but we can ensure that member companies have access to the resources and insights they need to make informed decisions.

Are there noticeable differences in the approaches to countering terrorism online between Central and Eastern European countries – such as Poland – and the United States?

Certainly in terms of approaching the challenge of combating online content, we do see differences in the regulatory environment – particularly between the US, the United Kingdom and Europe. We know this is something tech companies are working to address in how they operate. I think those differences are reflected both in regulation and in how various stakeholders feel about certain types of content and where the boundaries are. In the US, for example, there is a lot of speech that is protected under the First Amendment (to the Constitution of the United States – editor's note), and I know that many of our European colleagues sometimes struggle with that. So there is definitely a difference. However,

[5] See: https://gifct.org/governance/.

I think there is also some commonality – especially in areas where there is a clearer line. There tends to be more consensus than disagreement in those cases and we try to focus on that positive aspect.

The GIFCT also serves as a forum for cross-sectoral dialogue. In what ways do you engage academic communities and subject matter experts in developing effective strategies to address online violent extremism?

Cross-sectoral dialogue is a key working method for the GIFCT. Through our workshops, our research network and our daily engagement with member companies, we work to make sure they can learn from one another and benefit from each other's resources and expertise. One of the things we often find across sectors is that there is not always a strong understanding of how others operate or what tools and resources they have. A big part of our role is bringing those different communities together. So whether it is law enforcement and practitioners or academics and the private sector, we try to create opportunities for them to engage directly and share knowledge.

Poland has been facing disinformation campaigns and radicalisation attempts online, particularly concerning the conflict on its eastern border. Does the GIFCT analyse cases from this region as part of its examination of contemporary hybrid threats?

We certainly see hybrid threats as a concern for many companies, and as a result, we are working with different parts of those companies – policymakers, engineers or investigators. We try to build shared knowledge across all of them.

We have our reports[6], which frequently highlight issues related to hybrid threats in the region you mentioned. These reports help surface some of the regional dynamics that are especially relevant in places like Poland. In addition, when

[6] See: https://gifct.org/gifct-resources-and-publications/.

incidents arise, our Incident Response Framework[7] may also bring some of these hybrid threat issues into focus. Through that process, we engage our member companies to better understand the dynamics at play. So yes, this is something that definitely comes up in our work.

With Poland's expanding technology sector and its highly skilled IT professionals, do you see potential for the country to emerge as a regional innovation hub for combating online radicalisation and fostering cooperation with the GIFCT?

We certainly would. We very much welcome Polish tech companies and tech-adjacent companies to engage with us and help deepen our understanding of the threats and trends specific to Poland. We encourage tech companies in Poland to apply for membership with the GIFCT. We also invite Polish researchers to contribute to the GNET, which is fully accessible online. There are microgrants available for authors who wish to contribute articles. This allows for a wide range of perspectives. If there are tech-adjacent organisations or emerging issues we should be aware of, we are happy to explore opportunities for events or meetings that could help facilitate further dialogue and collaboration.

Interviewed by: Damian Szlachter

[7] See: https://gifct.org/incident-response/.