

TERRORYZM

studia
analizy
prewencja



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

Zespół redakcyjny

dr Damian Szlachter (redaktor naczelny)
dr Aleksandra Komar (zastępca redaktora naczelnego)
Agnieszka Dębska (sekretarz redakcji, skład)
Aleksandra Dąbała, Izabela Laskus-Rock, Aneta Olkowska, Izabela Paczesna,
Monika Sikora (redakcja, korekta)

Projekt okładki

Aleksandra Bednarczyk

© Copyright by Agencja Bezpieczeństwa Wewnętrznego 2026

ISSN 2720-4383

e-ISSN 2720-6351

Numer zamknięto i oddano do druku w lipcu 2026 r.

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:
<https://ejournals.eu/czasopismo/terroryzm>

**Wersje językowe**

Język polski (wersja drukowana i elektroniczna)
Tłumaczenie na język angielski (wersja elektroniczna)

Zgłaszanie tekstów

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

Kontakt

tel. (+48) 22 58 58 695
e-mail: wydawnictwo@abw.gov.pl

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

Druk

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

Rada naukowa

prof. dr hab. Sebastian Wojciechowski

Uniwersytet im. Adama Mickiewicza w Poznaniu,
Instytut Zachodni w Poznaniu

prof. dr hab. Waldemar Zubrzycki

Akademia Policji w Szczytnie

dr hab. Aleksandra Gasztold, prof. UW

Uniwersytet Warszawski

dr hab. Ryszard Machnikowski, prof. UŁ

Uniwersytet Łódzki

dr hab. Agata Tyburska

Akademia Policji w Szczytnie

dr hab. Barbara Wiśniewska-Paź, prof. UW

Uniwersytet Wrocławski

dr Piotr Burczaniuk

Agencja Bezpieczeństwa Wewnętrznego

ppłk Emilijus Čižas

Centrum Eksperckie Kontrwywiadu NATO w Krakowie
(CI COE)

dr Jarosław Jabłoński

Siły Zbrojne RP

dr Anna Matczak

Uniwersytet Nauk Stosowanych w Hadze

dr Paulina Piasecka

Uniwersytet Civitas w Warszawie

dr Viktorija Rusinaitė

Europejskie Centrum Eksperckie
ds. Zwalczania Zagrożeń Hybrydowych (Hybrid COE)

Recenzenci numeru 9

dr Magdalena Adamczuk

dr Tomasz Białek

dr Łukasz Foryś

dr Tomasz Kijewski

dr Marcin Lipka

dr Katarzyna Maniszewska

dr Michał Piekarski

dr Karolina Wojtasik

SPIS TREŚCI

7 Wstęp

ARTYKUŁY

15 **Cyfrowa rewolucja polityki antyterrorystycznej UE
w nowej Agendzie UE na rzecz zwalczania terroryzmu z 2026 roku**
Piotr Burczaniuk

39 **Terroryzm w Rosji w ujęciu krajowym,
regionalnym i międzynarodowym**
Aleksander Olech

83 **Ochrona przestrzeni publicznych i wydarzeń publicznych
przed atakami z użyciem pojazdu – znaczenie systemów HVM
i barier pojazdowych VSB w kontekście rekomendacji dla Polski**
Jarosław Jaźwiński

VARIA

129 **System ochrony lotnictwa cywilnego jako
przykład wzmocnienia odporności infrastruktury krytycznej**
Karol Dymek

149 **Bezpieczeństwo lotnictwa cywilnego w praktyce –
systemy ochrony, kontrola i odporność operacyjna**
Bohdan Paszukow

163 **Bezpieczniejsza Europa w lepszym świecie.
European High Risk Security Network w latach 2024–2025**
Pedro Nogueira

- 175** Młodzież a bezpieczeństwo państwa.
 Społeczne uwarunkowania podatności na radykalizację
 w świetle raportu „Diagnoza Młodzieży 2026”
 Paweł Rabiej, Konrad Ciesiołkiewicz
- 191** Sprawozdanie z konferencji
 „Nowe uwarunkowania procesu radykalizacji
 młodych ludzi z perspektywy bezpieczeństwa państwa”
 Aleksandra Komar

PRACE KONKURSOWE

- 203** Polityki bezpieczeństwa Francji i Belgii
 w odpowiedzi na zagrożenia terrorystyczne
 na przykładzie zamachów w Paryżu (2015 r.) i Brukseli (2016 r.)
 Nicole Szostak

ARTYKUŁY RECENZYJNE / RECENZJE

- 233** Tomasz Wróblewski,
 Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym
 Tomasz Michalak
- 239** Sprawozdanie z raportu
 „Agencja Bezpieczeństwa Wewnętrznego 2024–2025.
 Wybrane aktywności”
 Aleksandra Komar

Szanowni Państwo!

Przekazujemy w Państwa ręce 9. numer czasopisma ABW „Terroryzm – studia, analizy, prewencja” (T-SAP), które w ciągu kilku lat od startu tego projektu stało się zauważalne również poza Polską, szczególnie w krajach NATO i Unii Europejskiej. Z dumą przyjmujemy, że T-SAP pojawia się w prezentacjach organów ścigania państw europejskich jako materiał ekspercki godny regularnego czytania. Jednocześnie intensywnie pracujemy z całą Redakcją, by spełnić wszystkie wymogi stawiane wysoko punktowanym czasopismom naukowym. Efekty tych zmian mogą Państwo dostrzec zarówno na podstronie wydawnictwa ABW (www.abw.gov.pl/wyd), jak i w składzie Rady Naukowej, do której grona dołączyli ostatnio przedstawiciele The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), The NATO Counter Intelligence Centre of Excellence (CI COE) oraz The NATO Centre of Excellence – Defence Against Terrorism (COE-DAT).

W tym numerze T-SAP dominującym tematem jest brutalny ekstremizm i radykalizacja prowadzące do działań terrorystycznych, dlatego otwiera go tekst poświęcony nowej agendzie UE na rzecz zwalczania terroryzmu i zapobiegania temu zjawisku. To strategiczny dokument przyjęty w lutym 2026 r., który na kilka lat ukształtuje w ramach Unii oraz państw członkowskich podejście do zagrożeń terrorystycznych i brutalnego ekstremizmu. Widać w nim to, co dostrzegamy również w Polsce, czyli stopniowe odchodzenie od klasycznych, fizycznych zagrożeń terrorystycznych na rzecz zagrożeń przyjmujących postać hybrydową lub zachodzących wyłącznie w środowisku cyfrowym. To przekłada się na priorytety walki z terroryzmem w UE, obejmujące przewidywanie zagrożeń, zapobieganie

radikalizacji postaw, ochronę obywateli w internecie, ochronę obywateli przed zamachami fizycznymi, bezpośrednie reagowanie na zagrożenia i ataki oraz współpracę z partnerami międzynarodowymi. Praktyczny wymiar tej współpracy opisujemy na przykładzie osiągnięć portugalskiej prezydencji w jednej z unijnych inicjatyw antyterrorystycznych (AT) – European High Risk Security Network (EU-HRSN). Agencja Bezpieczeństwa Wewnętrznego jest członkiem założycielem tej sieci, zrzeszającej mundurowe formacje specjalne oraz jednostki interwencyjne ds. działań wysokiego ryzyka.

Na łamach T-SAP wielokrotnie podejmowaliśmy tematy trudne, w których dużym ograniczeniem jest brak dostępu do rzetelnych danych, aby poddać je krytycznej analizie i opisać w artykule naukowym. Tym razem przeczytają Państwo o terroryzmie w Rosji, traktowanym jako narzędzie polityczne wykorzystywane przez Kreml w wymiarze krajowym, regionalnym i międzynarodowym. W artykule ukazano m.in., jak Moskwa „montuje” narrację walki z terroryzmem, aby uzasadniać działania militarne, wzmacniać kontrolę społeczną oraz budować swoje wpływy poza granicami państwa – w Azji Centralnej, na Bliskim Wschodzie i w Afryce.

W poprzednim numerze T-SAP poruszyliśmy temat ochrony w Polsce przestrzeni publicznych przed atakami z użyciem pojazdów oraz przedstawiliśmy rekomendacje dla samorządów wydane przez resort spraw wewnętrznych i administracji (opracowali je policyjni eksperci przy współpracy z MSWiA oraz ABW, z uwzględnieniem doświadczeń innych państw). Rekomendacje te zostały wykorzystane w Polsce podczas projektowania zabezpieczeń wybranych jarmarków bożonarodzeniowych zorganizowanych w grudniu 2025 r. W tym numerze na prośbę naszych czytelników poruszamy praktyczny wymiar budowania odporności na tego typu ataki. Omawiamy podatność otwartych przestrzeni publicznych na nie, a także znaczenie analizy ryzyka, rozpoznania dróg dojazdowych, standardów badawczych w odniesieniu do zabezpieczeń antyterrorystycznych oraz interpretacji wyników testów zderzeniowych. Co ważne, wskazujemy najczęstsze błędy popełniane przy projektowaniu, instalacji i eksploatacji barier pojazdowych VSB (ang. *vehicle security barriers*). Nawiażemy do tego tematu po raz kolejny, po przyjęciu

Projektu rozporządzenia Rady Ministrów w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej. Poruszono w nim zagadnienia związane z technicznymi aspektami zabezpieczenia obiektów przed atakiem z wykorzystaniem pojazdu (projekt jest elementem fundamentalnej nowelizacji ustawy o zarządzaniu kryzysowym podpisanej 19 czerwca 2026 r.).

Nasi czytelnicy dopingują nas do publikowania opracowań przygotowywanych przez praktyków krajowych i zagranicznych. Pojawiają się one rzadko w debacie publicznej nad doskonaleniem rozwiązań antyterrorystycznych czy taktyk kontrterrorystycznych. W tym numerze pokazujemy doświadczenia w budowaniu odporności portów lotniczych na współczesne zagrożenia, w tym te o charakterze terrorystycznym, z dwóch perspektyw – krajowej oraz międzynarodowej. Liczymy, że znajdą tam Państwo inspiracje do rozwoju swoich kompetencji czy pasji zawodowych.

W każdej debacie o skuteczności działania krajowych systemów AT w państwach wspólnoty euroatlantyckiej pojawia się pytanie, które państwo ma najbardziej optymalne rozwiązania względem zagrożeń terrorystycznych, z jakimi musi się mierzyć. Na to pytanie nie znajdziemy odpowiedzi, jeśli nie zastosujemy właściwych metod oceny skuteczności przyjętych celów ochrony AT w danym kraju czy regionie. Publikujemy zatem fragment pracy licencjackiej, która została doceniona w tegorocznym konkursie Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych i ekonomicznych. Praca ta jest poświęcona polityce bezpieczeństwa Francji i Belgii w odpowiedzi na zagrożenia terrorystyczne z lat 2015–2016, kiedy to w Paryżu i Brukseli doszło do najtragiczniejszych ataków terrorystycznych w historii Europy. To ważny głos młodej autorki w refleksji nad skutecznością europejskich systemów AT.

W Europie najważniejszym paliwem brutalnego ekstremizmu jest zjawisko radykalizacji poglądów i postaw wśród młodzieży, obserwowane i coraz bardziej szczegółowo badane również w Polsce. Zachęcamy do lektury wniosków

płynących zarówno z raportu *Diagnoza Młodzieży 2026*, jak i z konferencji pt. „Nowe uwarunkowania procesu radykalizacji młodych ludzi z perspektywy bezpieczeństwa państwa” zorganizowanej w kwietniu 2026 r. w ABW. Główną osią problemową rozwoju brutalnego ekstremizmu jest, w opinii badaczy tego zjawiska w Polsce, napięcie między rozwojem technologicznym a bezpieczeństwem psychospołecznym młodych ludzi, ze szczególnym uwzględnieniem mechanizmów prowadzących do radykalizacji, która może skutkować działaniami terrorystycznymi.

Obecnie służby mundurowe poszukują możliwości wykorzystania sztucznej inteligencji na potrzeby zapewnienia porządku publicznego, bezpieczeństwa wewnętrznego, ochrony państwowych granic lądowych, morskich i powietrznych. Zachęcamy do lektury recenzji jednej z najnowszych publikacji na polskim rynku wydawniczym, która porusza temat roli AI w zapobieganiu zagrożeniom terrorystycznym. Tym bardziej że recenzję przygotował ekspert będący międzynarodowym autorytetem w tym obszarze.

W tym numerze T-SAP omawiamy również publikację, która stała się najczęściej cytowanym materiałem ABW na świecie od lat. Mowa o ukazującym się po wieloletniej przerwie raporcie przedstawiającym najważniejsze działania podejmowane przez Agencję w zakresie ochrony bezpieczeństwa wewnętrznego Rzeczypospolitej Polskiej. Obecna edycja obejmuje lata 2024–2025 i opisuje również działalność antyterrorystyczną tej służby, w tym rozpoznawanie brutalnego ekstremizmu i procesów radykalizacji mogących prowadzić do przestępstw o charakterze terrorystycznym, ochronę infrastruktury krytycznej przed sabotażem i dywersją, przeciwdziałanie przedostawaniu się przez granicę polsko-białoruską osób z państw wysokiego ryzyka terrorystycznego oraz prowadzenie postępowań karnych dotyczących aktywności terrorystycznej wymierzonej w obywateli i interesy RP w kraju i za granicą.

Zachęcamy do lektury tekstów pokazujących, jak zmieniają się współczesne zagrożenia i sposób myślenia o bezpieczeństwie. Terroryzm, brutalny ekstremizm, radykalizacja, działania hybrydowe i sabotaż coraz częściej występują obok

siebie albo wzajemnie się przenikają. Właśnie dlatego potrzebne są rzetelne analizy, ostrożne wnioski i stała dyskusja o tym, jak skutecznie rozpoznawać oraz ograniczać zagrożenia, z którymi mierzą się dziś Polska i państwa sojusznicze.

Redaktor naczelny
dr Damian Szlachter

Zastępca redaktora naczelnego
dr Aleksandra Komar



ARTYKUŁY

Cyfrowa rewolucja polityki antyterrorystycznej UE w nowej Agendzie UE na rzecz zwalczania terroryzmu z 2026 roku

Digital revolution of the EU's counter-terrorism policy under the new EU Agenda for Combating Terrorism of 2026

PIOTR BURCZANIUK

Instytut Nauk Prawnych,
Uniwersytet Kardynała Stefana Wyszyńskiego

 <https://orcid.org/0000-0002-6685-8769>

Abstrakt

Komisja Europejska opublikowała 26 lutego 2026 r. w formie komunikatu nową agendę Unii Europejskiej na rzecz zapobiegania terroryzmowi i zwalczania go, zastępując dokument o podobnym charakterze obowiązujący od 9 grudnia 2020 r. Jako główną przyczynę zmian wskazano konieczność realizacji przyjętej 1 kwietnia 2025 r. nowej europejskiej strategii bezpieczeństwa wewnętrznego ProtectEU. Podstawowym celem opracowania jest przybliżenie zakresu treściowego nowej agendy, ze zwróceniem uwagi na zaprezentowane w niej nowe podejście w kwestii zagrożeń terrorystycznych i brutalnego ekstremizmu, odchodzące stopniowo od klasycznych, fizycznych zagrożeń terrorystycznych na rzecz zagrożeń przyjmujących postać hybrydową lub zachodzących wyłącznie w środowisku cyfrowym. W analizie dokumentu skoncentrowano się na przedstawieniu zbudowanej w nim nowej mapy zagrożeń terrorystycznych, opartej na sześciu filarach obejmujących: przewidywanie zagrożeń, zapobieganie radykalizacji postaw, ochronę obywateli w internecie, ochronę obywateli w środowisku fizycznym, reagowanie na zagrożenia i ataki oraz współpracę

z partnerami międzynarodowymi. Omówiono kwestię miejsca tej agendy w systemie źródeł prawa europejskiego i skutku normatywnego, który z niego wynika. Przedstawiono również najważniejsze różnice w podejściu do zjawiska zwalczania terroryzmu i brutalnego ekstremizmu w starej i nowej agendzie.

Słowa kluczowe

terroryzm, brutalny ekstremizm, polityka bezpieczeństwa UE, Agenda UE 2026, ProtectEU, cyfryzacja bezpieczeństwa, nowe technologie w zwalczaniu terroryzmu

Abstract

On 26 February 2026, the European Commission published a new European Union Agenda for Preventing and Combating Terrorism in the form of communication, replacing a similar document that had been in force since 9 December 2020. The need to implement the new European Internal Security Strategy 'Protect EU' adopted on 1 April 2025 was cited as the main reason for the changes. The primary objective of the study is to outline the content of the new Agenda, with particular attention to the new approach presented therein regarding terrorist threats and violent extremism. The approach is gradually shifting away from traditional, physical terrorist threats in favour of threats that take a hybrid form or occur exclusively in the digital environment. The analysis of the document focuses on presenting the new map of terrorist threats outlined therein, based on six pillars encompassing: anticipating threats, preventing radicalisation, protecting citizens online, protecting citizens in the physical environment, responding to threats and attacks, as well as cooperation with international partners. The article pays particular attention to the issue of the Agenda's place within the system of European legal sources and the normative effect that arises from it. The most significant differences in the approach to combating terrorism and violent extremism in the old and new Agendas were also outlined.

Keywords

terrorism, violent extremism, EU security policy, EU Agenda 2026, ProtectEU, digitalisation of security, new technologies in the fight against terrorism

Agenda na rzecz zwalczania terroryzmu jako element strategii ProtectEU

W dniu 26 lutego 2026 r. Komisja Europejska (dalej: Komisja lub KE) opublikowała, w formie komunikatu adresowanego do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, nową agendę Unii Europejskiej pt. *ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska* (dalej: Agenda)¹. Zastąpiła ona wcześniejszą agendę pt. *Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie*, opublikowaną przez KE 9 grudnia 2020 r.²

Zasadniczym celem artykułu jest krytyczna analiza założeń Agendy oraz wskazanie, w jaki sposób redefiniuje ona unijną politykę bezpieczeństwa wewnętrznego, przenosząc środek ciężkości z klasycznego (fizycznego) zwalczania terroryzmu na przeciwdziałanie zagrożeniom hybrydowym i cyfrowym. Główny problem badawczy artykułu można sprowadzić do pytania: w jaki sposób cyfryzacja, rozwój nowych technologii oraz zmiana środowiska geopolitycznego wpłynęły na ewolucję unijnej polityki antyterrorystycznej i czy rozwiązania przyjęte w Agendzie oznaczają trwałe przejście UE od modelu reaktywno-operacyjnego do modelu technologiczno-prewencyjnego?

W artykule połączono kilka podejść badawczych. Oparto się przede wszystkim na: metodzie dogmatyczno-prawnej, która posłużyła do egzegezy aktów prawnych prawa pierwotnego oraz pochodnego UE i orzecznictwa Trybunału Sprawiedliwości UE; metodzie komparatystycznej, wykorzystanej w podsumowaniu artykułu, oraz metodzie systemowo-instytucjonalnej, zastosowanej do opisu architektury bezpieczeństwa UE.

Prace nad Agendą zostały zainicjowane przez KE w ramach realizacji europejskiej strategii bezpieczeństwa wewnętrznego ProtectEU, opublikowanej 1 kwietnia 2025 r. (dalej: Strategia)³. Stanowi ona kompleksową

¹ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. *ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska*, COM(2026) 101 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52026DC0101> [dostęp: 28 IV 2026].

² Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. *Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie*, COM(2020) 795 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0795> [dostęp: 28 IV 2026].

³ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie *ProtectEU: europejska strategia bezpieczeństwa*

aktualizację podejścia UE do bezpieczeństwa wewnętrznego i opiera się na założeniu, że ochrona obywateli oraz stabilność przestrzeni wewnętrznej UE wymagają zintegrowanego i wielopoziomowego działania wszystkich podmiotów – instytucji unijnych, państw członkowskich, krajowych służb bezpieczeństwa i wywiadu, sektora prywatnego oraz społeczeństwa obywatelskiego.

Kluczowym elementem Strategii jest wzmocnienie zdolności UE do przewidywania zagrożeń przez rozwój analiz ryzyka, lepszą wymianę informacji oraz wykorzystanie danych pochodzących od agencji UE, przede wszystkim Europolu. Strategia kładzie nacisk również na zapobieganie zagrożeniom i zwalczanie ich, zwłaszcza terroryzmu, przestępczości zorganizowanej oraz cyberprzestępczości, przez rozbijanie siatek przestępczych, przeciwdziałanie radykalizacji, szczególnie w środowisku internetowym, oraz ograniczanie źródeł finansowania działalności przestępczej. Istotnym filarem Strategii jest także ochrona infrastruktury krytycznej, co ma zwiększyć odporność UE na sabotaż, ataki hybrydowe oraz zakłócenia technologiczne. Duże znaczenie przypisuje się wzmocnieniu cyberbezpieczeństwa i odporności systemów cyfrowych, które coraz częściej są celem działań przestępczych i destabilizacyjnych. W Strategii podkreśla się, że:

(...) poziom zagrożenia terrorystycznego w Europie nadal rośnie. Kryzysy regionalne poza UE wywołują efekt domina, dając podmiotom terrorystycznym z całego spektrum ideologicznego nową motywację do werbowania, mobilizacji lub budowania swoich zdolności. Ich działania w zakresie radykalizacji i werbowania skierowane są w szczególności do najsłabszych grup naszych społeczeństw, a zwłaszcza do niektórych osób młodych. Podżegają do ataków w pojedynkę i powodują gwałtowny wzrost ekstremizmu antysystemowego, którego celem jest zakłócenie demokratycznego porządku prawnego⁴.

Zwalczanie terroryzmu i brutalnego ekstremizmu staje się jednym z filarów Strategii. Poświęcono temu zagadnieniu pkt 6. Zakłada się wprowadzenie kompleksowego planu zwalczania terroryzmu, aby zapobiegać

wewnętrznego, COM(2025) 148 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX%3A52025DC0148> [dostęp: 28 IV 2026].

⁴ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego..., pkt 1.

radikalizacji postaw, zabezpieczać przestrzeń internetową i publiczną, ograniczać kanały finansowania i reagować na ataki, gdy do nich dojdzie.

Strategia, podobnie jak Agenda, nie definiuje pojęcia terroryzmu. Odwołuje się do definicji „przestępstwa terrorystycznego” w rozumieniu art. 3 *Dyrektywy 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*. Zgodnie z nią są to (...) przestępstwa, które ze względu na swój charakter lub kontekst mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej, jeżeli zostają popełnione umyślnie i w tzw. celu terrorystycznym. Do szkód tych zalicza się:

- a) poważne zastraszanie ludności,
- b) bezprawne zmuszenie rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania,
- c) poważną destabilizację lub zniszczenie podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych danego państwa lub danej organizacji międzynarodowej.

Jednocześnie zwraca uwagę, że w regulacjach UE nie została przyjęta żadna prawna definicja brutalnego ekstremizmu. W Agendzie w przypisie dolnym podano jedynie, że (...) *akty brutalnego ekstremizmu to działania, które nie przekraczają progu określonego w definicji przestępstw terrorystycznych, jednak stanowią poważne zagrożenie bezpieczeństwa*⁵.

W Strategii jako cztery podstawowe elementy zwalczania terroryzmu KE wskazała:

- 1) zapobieganie radykalizacji i ochronę osób w internecie – Komisja zakłada konieczność eliminowania pierwotnych przyczyn, a przede wszystkim zwraca uwagę na wykorzystywanie przez terrorystów i brutalnych ekstremistów platform internetowych do rozpowszechniania (zwłaszcza wśród osób małoletnich) terrorystycznych i innych szkodliwych treści, gromadzenia funduszy i werbowania. Kluczową rolę w przeciwdziałaniu rozprzestrzenianiu się w internecie treści o charakterze terrorystycznym odgrywa *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*,

⁵ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. *ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska...*

- gdyż umożliwia szybkie usuwanie najbardziej odrażających i niebezpiecznych materiałów;
- 2) przeciwdziałanie finansowaniu terroryzmu – Komisja zwraca uwagę, że terroryści pozyskują środki na swoją działalność za pomocą kampanii finansowania społecznościowego, kryptoaktywów, neo-banków lub platform płatności internetowych. Organy ścigania muszą wykrywać i badać te przepływy finansowe, co wymaga odpowiednich środków, narzędzi i wiedzy specjalistycznej;
 - 3) ochrona przed atakami – prócz inwestycji w zapobieganie radykalizacji postaw ważnym elementem ochrony obywateli jest ograniczenie środków, za pomocą których terroryści i przestępcy mogą przeprowadzać ataki. Konieczne są działania zarówno w odniesieniu do narzędzi wykorzystywanych przez terrorystów, jak i ochrony celów zagrożonych atakiem, ze zwróceniem szczególnej uwagi na przestrzeń publiczną. Komisja wskazuje również na coraz większe zagrożenia bezpieczeństwa spowodowane wykorzystywaniem bezzałogowych statków powietrznych do szpiegostwa i ataków;
 - 4) zagraniczni bojownicy terrorystyczni – Komisja wraz z Europolą założyła zacieśnienie współpracy z kluczowymi państwami trzecimi w celu uzyskania danych biograficznych i biometrycznych dotyczących osób mogących stanowić zagrożenie terrorystyczne, w tym zagranicznych bojowników terrorystycznych. Dane te mają być wprowadzone do Systemu Informacyjnego Schengen (Schengen Information System, SIS). Komisja zaznacza, jak ważne jest, aby państwa członkowskie korzystały ze wszystkich istniejących narzędzi, w tym SIS, a także usprawniały kontrole biometryczne i przeprowadzały na granicach zewnętrznych UE obowiązkowe i systematyczne kontrole wszystkich osób.

Jednym z najważniejszych działań w zakresie zwalczania terroryzmu i brutalnego ekstremizmu przewidzianych w Strategii było przyjęcie w 2025 r. nowej unijnej agendy na rzecz zapobiegania terroryzmowi i brutalnemu ekstremizmowi oraz ich zwalczania. Ostatecznie Agendę przyjęło 26 lutego 2026 r.

Miejsce Agendy w systemie źródeł prawnych UE

Podstawę prawną działań UE w zakresie zapobiegania terroryzmowi i zwalczania go stanowią przepisy Traktatu o funkcjonowaniu Unii Europejskiej (dalej: TFUE). W ramach regulacji obszaru przestrzeni wolności, bezpieczeństwa i sprawiedliwości (tytuł V) wskazano w nim wśród obowiązków UE, w art. 67 ust. 3 TFUE, nakaz dokładania (...) *starań, aby zapewnić wysoki poziom bezpieczeństwa za pomocą środków zapobiegających przestępczości, rasizmowi i ksenofobii oraz zwalczających te zjawiska, a także za pomocą środków służących koordynacji i współpracy organów policyjnych i sądowych oraz innych właściwych organów, a także za pomocą wzajemnego uznawania orzeczeń sądowych w sprawach karnych i, w miarę potrzeby, przez zbliżanie przepisów karnych.*

Podstawowym środkiem realizacji tego celu jest art. 83 TFUE. Przyznaje on Parlamentowi Europejskiemu i Radzie prawo stanowienia w drodze dyrektyw (...) *norm minimalnych odnoszących się do określania przestępstw oraz kar w dziedzinach szczególnie poważnej przestępczości o wymiarze transgranicznym, wynikające z rodzaju lub skutków tych przestępstw lub ze szczególnej potrzeby wspólnego ich zwalczania.* Do dziedzin tej przestępczości TFUE zalicza: terroryzm, handel ludźmi oraz seksualne wykorzystywanie kobiet i dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcję, fałszowanie środków płatniczych, przestępczość komputerową i przestępczość zorganizowaną.

Uzupełniając, zgodnie z art. 84 TFUE: *Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, mogą ustanowić środki w celu promowania i wspierania działania Państw Członkowskich w dziedzinie zapobiegania przestępczości, z wyłączeniem jakiejkolwiek harmonizacji przepisów ustawowych i wykonawczych Państw Członkowskich.* To właśnie na tej podstawie Parlament Europejski i Rada mogą przyjmować dokumenty o charakterze strategii i agend, które wyznaczają kierunki polityki, ale nie mają charakteru bezpośrednio wiążącego. Jednocześnie Traktat o Unii Europejskiej (dalej: TUE), w art. 17 TUE, wyznacza KE zadanie wspierania ogólnego interesu UE i podejmowania w tym celu odpowiednich inicjatyw.

Podsumowując, przyjmowanie strategii takich jak Agenda nie opiera się na jednej konkretnej podstawie prawnej, lecz na zespole norm traktatowych. Normy te:

- określają cel UE nakierowany na zapewnienie bezpieczeństwa (art. 67 TFUE),
- przyznają UE kompetencje w zwalczaniu terroryzmu (art. 83 TFUE),

- umożliwiają działania wspierające i strategiczne (art. 84 TFUE),
- nadają Komisji rolę inicjatora polityk UE (art. 17 TUE).

Warto również wskazać, że zgodnie z art. 4 ust. 2 zdanie trzecie TUE: (...) *w szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego*. Oznacza to, że działania UE – w tym strategie antyterrorystyczne – mają charakter wyłącznie koordynacyjny i wspierający, a nie zastępują polityk krajowych.

Na tych podstawach prawnych KE może przyjmować dokumenty strategiczne w postaci m.in. komunikatów COM (COM documents). Zawierają one oficjalne stanowiska, strategie, analizy i zapowiedzi działań legislacyjnych Komisji i odgrywają rolę tzw. *soft law* (prawa miękkiego). Rola i znaczenie takiego prawa wynikają głównie z orzecznictwa Trybunału Sprawiedliwości UE (TSUE). Podkreśla się w nim, że takie prawo nie ma mocy wiążącej, jednak nie może być całkowicie pomijane przy wykładni prawa UE⁶. Może być ono punktem odniesienia interpretacyjnego, szczególnie gdy doprecyzowuje politykę UE⁷, i jednocześnie wiąże ono Komisję w zakresie jej własnej praktyki, chociaż nie jest formalnie wiążące dla państw członkowskich UE⁸.

Mapa zagrożeń terrorystycznych według Agendy

Agendę otwiera wprowadzenie, w którym KE analizuje najważniejsze zagrożenia i podkreśla, że (...) *terroryzm i brutalny ekstremizm pozostają stałym wyzwaniem dla UE i jej państw członkowskich. Coraz silniejsze powiązania między terroryzmem a innymi obszarami przestępczości, elastyczniejsze sieci oraz sprawcy, którzy w mniejszym stopniu kierują się ideologią, a także zacierające się granice działalności on-line i na żywo stanowią szczególne wyzwanie przy definiowaniu i identyfikowaniu przestępstw terrorystycznych*⁹.

⁶ Por. Wyrok Trybunału (druga izba) z dnia 13 XII 1989 r. Salvatore Grimaldi przeciwko Fonds des maladies professionnelles. ECLI: EU:C:1989:646.

⁷ Por. Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

⁸ Por. Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. Dansk Rørindustri and Others v Commission of the European Communities. ECLI:EU:C:2005:408.

⁹ *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska...*, s. 1.

Jak wskazują autorzy tego dokumentu, liczba skoordynowanych i wielokoskalowych zamachów w UE zmniejszyła się w ostatnich latach, ale zagrożenie nie zniknęło, lecz ewoluowało, zarówno w zakresie podmiotowym, jak i ideologicznym. Rośnie liczba sprawców działających w pojedynkę oraz małych kilkuosobowych grup, których trzon stanowią często osoby małoletnie. W aspekcie motywacji ideologicznej podkreśla się, że (...) *podczas gdy terroryzm dżihadystyczny pozostaje najbardziej znaczącym i śmiertelnym zagrożeniem terrorystycznym, terroryści i brutalni ekstremiści kierują się coraz większą liczbą motywacji, nie zawsze związanych z konkretną ideologią, w tym odrzuceniem europejskich wartości demokratycznych, antysemityzmem lub nawiścią antymuzułmańską*¹⁰.

Ponadto KE zwraca uwagę, że na bezpieczeństwo w UE, w tym poziom zagrożeń terrorystycznych, wpływają zmieniające się otoczenie geopolityczne i konflikty zewnętrzne wobec UE, głównie w Strefie Gazy, a także – w kontekście wzrostu liczby działań sabotażowych i hybrydowych – trwająca rosyjska wojna napastnicza przeciwko Ukrainie. Unia Europejska stanęła w obliczu złożonych zagrożeń, których źródłem są zarówno grupy terrorystyczne, jak i zagraniczne podmioty państwowe i niepaństwowe. Podmioty te wzorują się na działaniach tradycyjnie przypisywanych grupom terrorystycznym, np. posługują się improwizowanymi urządzeniami zapalającymi w ładunkach lotniczych, dokonują cyberataków czy sabotażu infrastruktury krytycznej, ale również wykorzystują terrorystów i brutalnych ekstremistów jako popleczników. Powstają i utrzymują się powiązania między terroryzmem, przestępczością zorganizowaną i cyberprzestępczością. Wykorzystuje się w nich modele usług przestępczych oraz wspólne zasoby, głównie w zakresie werbowania, przestępcze platformy handlowe i podziemne sieci bankowe.

Istotnym elementem współczesnego terroryzmu jest jego silne powiązanie ze środowiskiem cyfrowym. Internet, media społecznościowe, platformy do gier online stały się kluczowymi narzędziami wykorzystywanymi przez organizacje o charakterze ekstremistycznym i jednostki o takich postawach do prowadzenia propagandy, rekrutacji nowych członków, a także do wymiany informacji i planowania działań. W Agendzie wskazuje się:

Podmioty terrorystyczne koordynują plany na platformach komunikacyjnych wykorzystujących pełne szyfrowanie transmisji (E2EE) oraz finansują swoje sieci i ataki za pomocą kryptowalut, niewymienialnych

¹⁰ Tamże.

aktywów cyfrowych (NFT) i „cyfrowej hawali”¹¹. Nadużywają generatywnej AI do tworzenia instrukcji przeprowadzania ataków. Technologia druku przestrzennego (np. do produkcji broni palnej) oraz zwiększone wykorzystanie systemów bezzałogowych statków powietrznych (SBSP/dronów) jeszcze bardziej zwiększają zagrożenie¹².

Komisja wskazuje, że opisane zagrożenia mają charakter transgraniczny. To oznacza, że żadne państwo członkowskie nie jest w stanie skutecznie przeciwdziałać im samodzielnie. Konieczne jest zatem wzmocnienie współpracy na poziomie unijnym i międzynarodowym. Nie można jednak przy tym zapominać – co podkreśla Komisja – o konieczności zachowania równowagi między zapewnieniem bezpieczeństwa a ochroną praw podstawowych. Działania antyterrorystyczne muszą być prowadzone zgodnie z wartościami UE, takimi jak demokracja, praworządność oraz poszanowanie praw człowieka. Jest to istotne z punktu widzenia zarówno legalności podejmowanych działań, jak i utrzymania do nich zaufania społecznego.

Sześć filarów walki z terroryzmem i brutalnym ekstremizmem

W punkcie drugim Agendy Komisja przedstawia kompleksową koncepcję przeciwdziałania terroryzmowi i brutalnemu ekstremizmowi opartą na systemie sześciu wzajemnie powiązanych filarów działania. Są to: 1) przewidywanie zagrożeń, 2) zapobieganie radykalizacji postaw, 3) ochrona użytkowników internetu, 4) ochrona ludzi w środowisku fizycznym, 5) reagowanie na zagrożenia i ataki, 6) współpraca z partnerami międzynarodowymi. Podejście to odzwierciedla przekonanie, że skuteczna polityka antyterrorystyczna nie może ograniczać się do reakcji na zdarzenia, lecz musi obejmować pełne spektrum działań – od identyfikacji zagrożeń, przez zapobieganie im, aż po reagowanie i odbudowę po ewentualnych atakach. Współczesne zagrożenia mają charakter dynamiczny, wielowymiarowy i często transgraniczny, co wymaga zintegrowanego podejścia angażującego różne poziomy zarządzania – lokalny, krajowy, unijny i międzynarodowy.

¹¹ Cyfrowa hawala to nieformalny system przekazywania wartości finansowej z wykorzystaniem narzędzi cyfrowych, działający poza tradycyjnym systemem bankowym i oparty na sieci zaufanych pośredników.

¹² *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska...*, s. 3.

Przewidywanie zagrożeń

Komisja podkreśla, że (...) *bezpieczeństwo zaczyna się od skutecznego przewidywania i prognozowania*¹³.

Przewidywanie zagrożeń ma stanowić fundament całej strategii i opierać się na gromadzeniu, analizie i wymianie informacji. Szczególną rolę w tym zakresie odgrywa współpraca między państwami członkowskimi oraz agencjami UE, w tym Single Intelligence Analysis Capacity¹⁴, dostarczającym terminowych ocen zagrożeń, oraz Europol, sporządzającym – na podstawie informacji otrzymanych od organów ścigania – regularne sprawozdania dotyczące tendencji. Dynamiczny i nieprzewidywalny charakter pojawiających się zagrożeń wymaga – zdaniem Komisji – wzmocnienia zdolności organów ścigania do przewidywania, aby móc lepiej określać pojawiające się zagrożenia i podejmować odpowiednie działania polityczne służące zwalczaniu terroryzmu.

Z kolei prognozowanie jest kluczowe z perspektywy identyfikacji zagrożeń i ma się opierać na dwóch elementach. Pierwszy z nich to wykorzystanie potencjału nowych technologii w zakresie egzekwowania prawa. Sztuczna inteligencja (ang. *artificial intelligence*, AI), uczenie maszynowe czy analiza dużych zbiorów danych to potencjał narzędziowy umożliwiający identyfikowanie wzorców zachowań oraz wykrywanie sygnałów ostrzegawczych, które mogą wskazywać na przygotowywanie ataków. Drugim elementem ma być przygotowanie na przeciwdziałanie wykorzystaniu przez terrorystów nowych technologii, takich jak AI, platformy internetowe, metody elektronicznego finansowania, głównie kryptoaktywa, czy stosowanie broni drukowanej w technologii 3D. Działania w ramach prognozowania mają się opierać na pracach Wspólnego Centrum Badawczego Komisji Europejskiej (Joint Research Centre), a podstawą ich finansowania ma być program „Horyzont Europa”.

Analiza założeń tego filaru prowadzi do wniosku o przejściu z dotychczas prezentowanego w UE modelu reaktywnego na model prewencyjny, w którym działania są podejmowane jeszcze przed materializacją zagrożenia.

¹³ Tamże, s. 4.

¹⁴ SIAC – struktura łącząca cywilne EU INTCEN (European Union Intelligence and Situation Centre), czyli cywilną jednostkę wywiadowczą UE będącą częścią Europejskiej Służby Działań Zewnętrznych, z Military Intelligence Directorate (wydziałem wywiadu wojskowego) w ramach Sztabu Wojskowego UE (European Union Military Staff, EUMS).

Zapobieganie radykalizacji postaw

Komisja definiuje zapobieganie radykalizacji postaw jako (...) *zwalczanie jej przyczyn, zanim się one utrwalą*¹⁵. Drugi filar ma się opierać na czterech elementach:

- 1) opracowaniu zestawu narzędzi prewencyjnych z myślą o osobach małoletnich. Narzędzia te mają umożliwić wczesne wykrywanie, wzmacniać czynniki ochronne, budowanie odporności przez edukację i integrację społeczną, przede wszystkim małoletnich, a także wspierać rodziny i społeczności w bezpiecznym korzystaniu z internetu;
- 2) budowaniu odpornych społeczeństw, nakierowanym na ochronę wszystkich wspólnot wyznaniowych przed nienawiścią, dyskryminacją i przemocą. Działania KE będą koncentrować się na usprawnieniu, dzięki wykorzystaniu AI, wykrywania treści ekstremistycznych, tworzeniu wspólnych wskaźników zagrożenia oraz usprawnieniu współpracy między platformami, organami ścigania i naukowcami w celu identyfikacji propagandy generowanej przez AI i skoordynowanych kampanii nakierowanych na radykalizację postaw;
- 3) przeciwdziałaniu radykalizacji postaw w zakładach karnych i wśród osób je opuszczających oraz zarządzaniu powrotami zagranicznych bojowników terrorystycznych i członków ich rodzin. Podstawą ma być opracowanie narzędzi oceny ryzyka i zarządzania nim na etapie poprzedzającym wypuszczenie na wolność oraz wytycznych wspierających krajowe podejścia do zradykalizowanych osób opuszczających zakłady karne oraz osób powracających, połączone ze szkoleniami w zakresie resocjalizacji i reintegracji, ze szczególnym uwzględnieniem ochrony dzieci;
- 4) wsparciu ofiar terroryzmu przez upowszechnienie Europejskiego Dnia Pamięci o Ofiarach Terroryzmu oraz wsparciu stowarzyszeń ofiar przez propagowanie ich aktywnej roli w programach zapobiegania.

Instytucjonalnie działaniami w ramach filaru drugiego zajmuje się powołane w 2024 r. Europejskie Centrum Wiedzy na temat Zapobiegania Radykalizacji (EU Knowledge Hub on Prevention of Radicalisation). Centrum

¹⁵ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. *ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska...*, s. 5.

opracowuje wytyczne, narzędzia, szkolenia i usługi wsparcia dla decydentów i praktyków.

Ochrona użytkowników internetu

Unia Europejska przyjęła najbardziej zaawansowane na świecie ramy regulacyjne ukierunkowane na zwalczanie działalności terrorystycznej w internecie, jednak zagrożenie to nadal się rozwija. W Agendzie wskazuje się: *Sieci ekstremistyczne szybko się dostosowują, wykorzystują powstające technologie oraz przenoszą swoją działalność z otwartych platform do zamkniętych czatów i usług szyfrowanych. Może to stwarzać poważne wyzwania w zakresie wykrywania planów terrorystycznych i zapobiegania ich realizacji, mapowania siatek terrorystycznych i ich zwolenników oraz prowadzenia postępowań przygotowawczych i sądowych w sprawie działalności terrorystycznej*¹⁶.

Zgodnie z założeniem Komisji działania w tym filarze mają się skupiać na trzech zagadnieniach:

- 1) pełnym wykorzystaniu ram regulacyjnych do zwalczania w internecie treści o charakterze ekstremistycznym i terrorystycznym, m.in. przez opracowanie przez Europol europejskiej bazy danych w celu wymiany skrótów kryptograficznych (ang. *hash*), tj. bazy śladów cyfrowych odnoszących się do treści o charakterze terrorystycznym i brutalnych treści ekstremistycznych, co umożliwi państwom członkowskim i dostawcom usług hostingowych bezpieczne oznaczanie, dopasowywanie i usuwanie treści na różnych platformach;
- 2) współpracy z przemysłem, głównie dostawcami usług online, która będzie realizowana za pośrednictwem Forum UE ds. Internetu (European Internet Forum zrzesza ministerstwa państw członkowskich UE, organy ścigania, społeczeństwo obywatelskie i dostawców usług online, w tym platformy mediów społecznościowych) oraz przez działania wspólnie z Europejską Radą ds. Usług Cyfrowych (European Board for Digital Services) w celu zintensyfikowania zwalczania rozpowszechniania treści o charakterze terrorystycznym i brutalnych treści ekstremistycznych;
- 3) zapewnieniu skutecznego i skoordynowanego reagowania kryzysowego w internecie, przy założeniu przekształcenia dotychczasowego unijnego protokołu kryzysowego w unijne ramy reagowania kryzysowego online (włączone do Digital Services Act – unijnego

¹⁶ Tamże, s. 8.

aktu o usługach cyfrowych). Państwa członkowskie będą mogły z nich korzystać w przypadku, gdy incydent prowadzi do zwiększonej aktywności w internecie związanej z atakiem.

Ochrona ludzi w środowisku fizycznym

Czwarty filar opiera się na zmienionym podejściu, zgodnie z którym podstawą jest działanie oparte na odporności. Zastąpiło ono działanie skoncentrowane na ochronie. Nastąpiło to wraz z przyjęciem w 2022 r. *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE* (dalej: dyrektywa CER). Jednocześnie UE zapewnia praktyczne wsparcie, którego podstawą są doradcy UE ds. zapewniania bezpieczeństwa. Ich zadaniem jest pomoc w ocenie podatności na zagrożenia i sugerowanie konkretnych usprawnień. Zgodnie z Agendą działania UE w analizowanym filarze mają się skupić na pięciu zagadnieniach:

- 1) utrudnianiu przemieszczania się terrorystów, głównie przez zapewnienie wysokiego poziomu ochrony granic zewnętrznych UE. Służą temu przede wszystkim wielkoskalowe systemy informatyczne: wjazdu/wyjazdu (Entry/Exit System, EES), informacji o podróży oraz zezwoleń na podróż (European Travel Information and Authorisation System, ETIAS), wizowy system informacyjny (Visa Information System, VIS) oraz ramy interoperacyjności. Dużymi wyzwaniem pozostają współpraca z państwami trzecimi nakierowana na uzyskanie biograficznych i biometrycznych danych osób mogących stanowić zagrożenie terrorystyczne i wprowadzenie tych danych do systemu SIS oraz rozbudowa procedury postępowania w sytuacji uzyskania „trafienia”. Od czerwca 2026 r. ma funkcjonować tzw. kontrola przesiewowa¹⁷. Dzięki niej ma być łatwiejsza identyfikacja obywateli państw trzecich, którzy nielegalnie przekroczyli granice zewnętrzne lub nielegalnie przebywają na terytorium państw członkowskich bez poddania się kontroli wjazdu. Komisja podkreśla, że będzie propagować skuteczne powroty osób stanowiących zagrożenie bezpieczeństwa;

¹⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1356 z dnia 14 maja 2024 r. w sprawie wprowadzenia kontroli przesiewowej obywateli państw trzecich na granicach zewnętrznych oraz zmiany rozporządzeń (WE) nr 767/2008, (UE) 2017/2226, (UE) 2018/1240 i (UE) 2019/817.

- 2) ograniczeniu dostępu do środków wykorzystywanych do przeprowadzania ataków przez harmonizację przepisów dotyczących kryminalizacji nielegalnego handlu bronią palną i innych przestępstw związanych z tą bronią, w tym nielegalnego tworzenia, posiadania i rozpowszechniania projektów na potrzeby wytwarzania broni palnej drukowanej w technologii 3D. Agenda zakłada również dokonanie przeglądu *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1148 z dnia 20 czerwca 2019 r. w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, zmieniającego rozporządzenie (WE) nr 1907/2006 i uchylającego rozporządzenie (UE) nr 98/2013* oraz przedstawienie w 2026 r. nowego planu działania na rzecz gotowości i reagowania w zakresie zagrożeń chemicznych, biologicznych, radiologicznych i nuklearnych (CBRN);
- 3) przeciwdziałaniu zagrożeniu stwarzanemu przez drony. Komisja podkreśla znaczenie zagrożenia związanego z wykorzystaniem nowych i powstających technologii, głównie dronów, przez podmioty terrorystyczne. Zwalczanie ma się opierać na strategii dotyczącej dronów 2.0¹⁸ oraz planie działania UE w zakresie bezpieczeństwa dronów i zabezpieczeń antydronowych przedstawionym 11 lutego 2026 r.¹⁹;
- 4) ochronie przestrzeni publicznej w Europie, przy czym jest konieczne uwzględnianie wymogów bezpieczeństwa już na etapie projektowania obszarów miejskich, przestrzeni publicznych i miejsc kultu. Powinno to znaleźć odzwierciedlenie w odpowiednich zobowiązaniach dla podmiotów eksploatujących przestrzeń publiczną, aby wdrażały środki bezpieczeństwa wynikające z analiz ryzyka. Organizacyjnie to zadanie zostaje powierzone wzmocnieniu Forum UE ds. Ochrony Przestrzeni Publicznych (EU Forum on the Protection of Public Spaces);

¹⁸ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. „Strategia dotycząca dronów 2.0 na rzecz inteligentnego i zrównoważonego ekosystemu bezzałogowych statków powietrznych w Europie, COM(2022) 652 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52022DC0652> [dostęp: 28 IV 2026].

¹⁹ Plan działania na rzecz ochrony przed dronami i zwalczania dronów, Komisja Europejska, <https://digital-strategy.ec.europa.eu/pl/policies/drone-security> [dostęp: 28 IV 2026].

- 5) odporności podmiotów krytycznych oraz bezpieczeństwa transportu i łańcucha dostaw. Wiąże się to z rosnącymi obawami dotyczącymi możliwych incydentów w postaci kampanii hybrydowych i aktów sabotażu ze strony wrogich podmiotów państwowych i ich popleczników. W celu poprawy bezpieczeństwa KE rekomenduje pilne wdrożenie wspomnianej wcześniej dyrektywy CER oraz *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS2)*.

Reagowanie na zagrożenia i ataki

Piąty filar ma się opierać na szybkiej i skoordynowanej reakcji zapewnianej przez, wymagające wzmocnienia, organy ścigania i organy sądowe przy wsparciu Europolu i Eurojustu. Komisja zwraca uwagę także na konieczność podejmowania dalszych działań nakierowanych na wyeliminowanie luk w systemie zapobiegania finansowaniu terroryzmu.

Działania w ramach tego filaru mają się skoncentrować na trzech zagadnieniach:

- 1) zwalczaniu finansowania terroryzmu i brutalnego ekstremizmu. Komisja podkreśla, że globalny charakter usług finansowych wymaga aktywnej reakcji całej Europy na problem jego wykorzystywania do finansowania terroryzmu. Ma to istotne znaczenie również ze względu na nowe źródła finansowania, takie jak kryptoaktywa czy cyfrowa hawala (oraz internetowe usługi płatnicze). Za fundament prawny walki z finansowaniem terroryzmu Komisja uznaje pełne wdrożenie, przyjętego 30 maja 2024 r., pakietu UE dotyczącego przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (ang. *anti-money laundering and countering the financing of terrorism*, AML/CFT), obejmującego *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy i finansowania terroryzmu* (wejdzie w życie 10 lipca 2027 r.) oraz *Dyrektywę Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania*

terroryzmu, zmieniającą dyrektywę (UE) 2019/1937 oraz zmieniającą i uchylającą dyrektywę (UE) 2015/849. Komisja planuje też podjęcie prac nad stworzeniem ogólnounijnego systemu umożliwiającego wyszukiwanie danych finansowych w celu śledzenia środków finansowych należących do terrorystów i korzyści z przestępczości zorganizowanej. System miałby powstać do 2030 r. i obejmować transakcje wewnątrzunijne i transakcje w ramach jednolitego obszaru płatności w euro (ang. *single euro payments area*, SEPA), transfery kryptoaktywów, płatności online i elektroniczne transfery środków pieniężnych;

- 2) usprawnieniu działań organów ścigania przez wzmacnianie mandatu Europolu, zwłaszcza jego Europejskiego Centrum ds. Zwalczania Terroryzmu (European Counter Terrorism Centre, ECTC), jako głównego centrum informacji, technologii i innowacji dla organów ścigania;
- 3) zacieśnieniu współpracy sądowej przez pełne wdrożenie, przyjętego komunikatem Komisji z 24 czerwca 2025 r., planu działania na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych²⁰. Decydującego znaczenia nabiera możliwość zabezpieczania i pozyskiwania dowodów bezpośrednio od usługodawców oferujących swoje usługi w UE, na mocy znajdującego zastosowanie od 18 sierpnia 2026 r. *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności*. Komisja zwraca uwagę na istotę firmowanego przez UE projektu SIRIUS, będącego unijnym systemem wsparcia dla organów ścigania w zdobywaniu ponad granicami państw dowodów z internetu²¹.

²⁰ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan działania na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych, COM(2025) 349 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52025DC0349> [dostęp: 29 IV 2026].

²¹ SIRIUS project, Europol, 21 I 2026 r., <https://www.europol.europa.eu/how-we-work/sirius-project> [dostęp: 29 IV 2026].

Współpraca z partnerami międzynarodowymi

Ostatni filar zakłada konieczność zacieśnienia współpracy międzynarodowej, głównie przez działania Wysokiego Przedstawiciela i koordynatora UE ds. zwalczania terroryzmu.

Działania w ramach tego filaru mają się skoncentrować na czterech zagadnieniach:

- 1) środkach ograniczających służących zwalczaniu terroryzmu, przy czym podstawowe narzędzie rozbijania siatek terrorystycznych stanowi tzw. unijna lista terrorystów²²;
- 2) postępie w zakresie zawierania umów międzynarodowych, dla których największym wyzwaniem pozostaje nowy protokół zmieniający definicję przestępstw terrorystycznych w Konwencji Rady Europy o zapobieganiu terroryzmowi²³. Po wejściu w życie ma on zapewnić dla ponad 40 państw ogólnoeuropejską definicję przestępstw terrorystycznych;
- 3) zacieśnianiu współpracy dwustronnej i regionalnej, a zwłaszcza wzmacnianiu współpracy z partnerami objętymi procesem rozszerzenia UE, a także na działaniach prowadzonych wobec konkretnych regionów, ze zwróceniem szczególnej uwagi na Bałkany Zachodnie, Bliski Wschód, w tym Syrię, oraz państwa afrykańskie;
- 4) wzmocnieniu roli UE przez koordynację i działania na forach wielostronnych Wysokiego Przedstawiciela, Komisji oraz koordynatora UE ds. zwalczania terroryzmu. Utrzymana ma zostać współpraca tematyczna z Radą Europy, Grupą Specjalną ds. Przeciwdziałania Praniu Pieniędzy (Financial Action Task Force), Interpolem i NATO.

²² Oficjalny wykaz osób, grup i podmiotów uznanych przez UE za zaangażowane w działalność terrorystyczną formalnie funkcjonuje na mocy *Wspólnego stanowiska Rady z dnia 27 grudnia 2001 r. w sprawie zastosowania szczególnych środków w celu zwalczania terroryzmu (2001/931/WPZiB)*.

²³ Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), [https://search.coe.int/cm/eng#{%22CoEIdentifier%22:\[%220912594880264105%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/eng#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}) [dostęp: 14 V 2026].

Agenda z 2026 roku a agenda z 2020 roku

Agenda z 2026 r., która została opracowana w celu realizacji nowej strategii bezpieczeństwa wewnętrznego ProtectEU opublikowanej 1 kwietnia 2025 r., czyni motywem przewodnim dostosowanie unijnej strategii walki z terroryzmem i brutalnym ekstremizmem do aktualnych zagrożeń. Ich charakter uległ, co podkreśla Komisja, zauważalnej zmianie – z klasycznych, fizycznych zagrożeń terrorystycznych na zagrożenia przyjmujące postać hybrydową lub występujące wyłącznie w środowisku cyfrowym. Podejście reaktywno-operacyjne zostaje więc zastąpione podejściem skupionym na działaniach proaktywnych, systemowych, w sferze cyfrowej.

Agenda z 2020 r. ujmowała zagrożenia terrorystyczne w sposób tradycyjny, jako działalność zorganizowanych grup, inspirowaną ideologicznie i realizowaną głównie „offline”. Internet pojawiał się w niej wyłącznie jako jedno z narzędzi i nie stanowił centralnego pola zainteresowania. Nowa Agenda traktuje przestrzeń cyfrową jako główne środowisko występowania zagrożeń. Radykalizacja, rekrutacja, propaganda czy finansowanie coraz częściej odbywają się bowiem wyłącznie w środowisku wirtualnym, co powoduje, że zagrożenia są bardziej rozproszone, trudniejsze do wykrycia na wczesnym etapie oraz silnie powiązane z dezinformacją i manipulacją informacyjną. Agenda zakłada konieczność przejścia z podejścia skoncentrowanego na zwalczaniu konkretnej organizacji na podejście oscylujące wokół zarządzania dynamicznym, głównie cyfrowym, ekosystemem zagrożeń.

Zmieniło się również podejście do sposobu prowadzenia działań prewencyjnych. Poprzednia agenda koncentrowała się na przeciwdziałaniu radykalizacji m.in. za pomocą programów społecznych, monitorowania środowisk ryzyka oraz współpracy służb. W Agendzie z 2026 r. prewencja zostaje przeniesiona w dużej mierze do internetu, z naciskiem na wczesne wykrywanie treści ekstremistycznych, przeciwdziałanie ich algorytmicznemu wzmacnianiu, szybkie usuwanie oraz ograniczanie ich zasięgu. W ten sposób prewencja staje się bardziej technologiczna i zautomatyzowana, a w mniejszym stopniu opiera się na działaniach społecznych.

W poprzedniej agendzie technologie cyfrowe były narzędziem wyłącznie wspierającym działania (np. analizy danych, wymiany informacji). W nowej Agendzie technologie te stają się centralnym elementem strategii, nakierowanym głównie na wykorzystanie AI do identyfikacji zagrożeń, analizy dużych zbiorów danych (big data), automatyzacji procesów bezpieczeństwa czy rozwoju narzędzi predykcyjnych. Różnica polega więc na przejściu od poziomu wsparcia technologicznego do strategii opartej na technologii.

W obu dokumentach podkreśla się znaczenie współpracy, jednak w poprzedniej agendzie skupiono się wyłącznie na współpracy między państwami członkowskimi i agencjami UE, a w nowej rozszerzono ją o sektor prywatny, podmioty technologiczne oraz współpracę globalną. Współpraca ta staje się sieciowa i wielopoziomowa. W dokumencie z 2020 r. sektor prywatny (zwłaszcza platformy internetowe) był partnerem wspierającym działania państw. W Agendzie z 2026 r. rola tego sektora wyraźnie wzrasta. Platformy społecznościowe stają się współodpowiedzialne za bezpieczeństwo. Komisja oczekuje od nich aktywnego wykrywania i usuwania treści oraz wprowadzenia systemowych mechanizmów współpracy i nadzoru. Następuje przesunięcie z modelu dobrowolnej współpracy w stronę modelu współodpowiedzialności regulacyjnej.

Zauważalna jest również zmiana w podejściu do budowania odporności społeczeństwa. W strategii z 2020 r. ta odporność była ważna, ale traktowana raczej jako element uzupełniający. W nowej Agendzie stała się ona jednym z najważniejszych filarów, głównie w zakresie walki z dezinformacją, budowania świadomości cyfrowej oraz ograniczania w sieci podatności na radykalizację. Bezpieczeństwo nie dotyczy już tylko konkretnej instytucji, ale całego społeczeństwa jako systemu.

Podsumowując, trzeba pamiętać, że przyjęta Agenda stanowi de facto dokument o charakterze wyłącznie programowym. Realizacja zawartych w nim założeń ma być osiągnięta dzięki projektowanym lub już wdrażanym aktom prawnym UE oraz działaniom zorientowanym głównie na rozwijanie współpracy organów ścigania państw członkowskich UE oraz państw trzecich, w swoistej koordynacji wzmacnianego organizacyjnie, mającego realne funkcje wykonawcze, Europolu.

Bibliografia

Źródła internetowe

Plan działania na rzecz ochrony przed dronami i zwalczania dronów, Komisja Europejska, <https://digital-strategy.ec.europa.eu/pl/policies/drone-security> [dostęp: 28 IV 2026].

SIRIUS project, Europol, 21 I 2026 r., <https://www.europol.europa.eu/how-we-work/sirius-project> [dostęp: 29 IV 2026].

Akty prawne

Traktat o funkcjonowaniu Unii Europejskiej (DzU z 2004 r. nr 90 poz. 864).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy i finansowania terroryzmu (Dz. Urz. UE L 1624 z 19 VI 2024 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1356 z dnia 14 maja 2024 r. w sprawie wprowadzenia kontroli przesiewowej obywateli państw trzecich na granicach zewnętrznych oraz zmiany rozporządzeń (WE) nr 767/2008, (UE) 2017/2226, (UE) 2018/1240 i (UE) 2019/817 (Dz. Urz. UE L 1356 z 22 V 2024 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz. Urz. UE L 191/118 z 28 VII 2023 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172/79 z 17 V 2021 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1148 z dnia 20 czerwca 2019 r. w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, zmieniające rozporządzenie (WE) nr 1907/2006 i uchylające rozporządzenie (UE) nr 98/2013 (Dz. Urz. UE L 186/1 z 11 VII 2019 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca dyrektywę (UE) 2019/1937 oraz zmieniająca i uchylająca dyrektywę (UE) 2015/849 (Dz. Urz. UE L 1640 z 19 VI 2024 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.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333/80 z 27 XII 2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88/6 z 31 III 2017 r.).

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie, COM(2020) 795 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0795> [dostęp: 28 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan działania na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych, COM(2025) 349 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52025DC0349> [dostęp: 29 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska, COM(2026) 101 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52026DC0101> [dostęp: 28 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. „Strategia dotycząca dronów 2.0 na rzecz inteligentnego i zrównoważonego ekosystemu bezzałogowych statków powietrznych w Europie”, COM(2022) 652 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52022DC0652> [dostęp: 28 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego, COM(2025) 148 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX%3A52025DC0148> [dostęp: 28 IV 2026].

Wspólne stanowisko Rady z dnia 27 grudnia 2001 r. w sprawie zastosowania szczególnych środków w celu zwalczania terroryzmu (2001/931/WPZiB) – (Dz. Urz. UE L 344/93 z 28 XII 2001 r.).

Orzecznictwo

Wyrok Trybunału (druga izba) z 13 XII 1989 r. Salvatore Grimaldi przeciwko Fonds des maladies professionnelles. ECLI: EU:C:1989:646.

Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. Dansk Rørindustri and Others v Commission of the European Communities. ECLI: EU:C:2005:408.

Inne dokumenty

Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), [https://search.coe.int/cm/eng#{%22CoEIdentifier%22:\[%220912594880264105%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/eng#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}) [dostęp: 14 V 2026].

Dr Piotr Burczaniuk

Doktor nauk prawnych, adiunkt w Katedrze Teorii i Filozofii Prawa na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie; radca prawny, członek Okręgowej Izby Radców Prawnych w Warszawie; legislator, członek Polskiego Towarzystwa Legislacji; ekspert ds. legislacji. Autor publikacji z zakresu teorii i filozofii prawa, prawa konstytucyjnego oraz prawa gospodarczego.

Kontakt: p.burczaniuk@uksw.edu.pl

Terroryzm w Rosji w ujęciu krajowym, regionalnym i międzynarodowym

Terrorism in Russia at national, regional and international level

ALEKSANDER OLECH

Defence24



<https://orcid.org/0000-0002-3793-5913>

Abstrakt

Terroryzm w Rosji należy analizować nie tylko jako zagrożenie dla bezpieczeństwa państwa, lecz także jako narzędzie polityczne wykorzystywane przez Kreml w wymiarze krajowym, regionalnym i międzynarodowym. Przedstawiona ewolucja zagrożeń terrorystycznych w Federacji Rosyjskiej, od Kaukazu Północnego i Emiratu Kaukaskiego, przez wzrost znaczenia tzw. Państwa Islamskiego, po działalność Państwa Islamskiego Prowincji Chorasán i zamach w Crocus City Hall ukazuje, jak wiele wyzwań stoi przed służbami bezpieczeństwa. Autor analizuje rosyjskie ustawodawstwo antyterrorystyczne, a także wybrane regulacje dotyczące ekstremizmu, które w praktyce państwa rosyjskiego są wykorzystywane jako element szerszego systemu kontroli i definiowania zagrożeń. W artykule omówiono również współpracę przeciwko terroryzmowi w Organizacji Układu o Bezpieczeństwie Zbiorowym. Autor wykazuje, że Moskwa wykorzystuje narrację walki z terroryzmem do uzasadniania działań militarnych, wzmacniania kontroli społecznej oraz budowania wpływów poza granicami państwa, m.in. w Azji Centralnej, na Bliskim Wschodzie i w Afryce. Rosyjski model antyterrorystyczny coraz mniej bazuje na prewencji, a coraz bardziej na politycznym definiowaniu przeciwników, co prowadzi do błędnego zarządzania percepcją zagrożeń i w efekcie – do kolejnych ataków terrorystycznych.

Słowa kluczowe

Rosja, terroryzm, ekstremizm, ISIS, Azja, OUBZ, antyterroryzm, Kreml

Abstract

Terrorism in Russia should be analysed not only as a threat to national security, but also as a political tool used by the Kremlin at the national, regional and international level. The evolution of threats in the Russian Federation, from the North Caucasus and the Caucasus Emirate, through the growing significance of the so-called Islamic State, to the activities of the Islamic State – Khorasan Province and the attack at the Crocus City Hall, illustrates the many challenges facing the security services. The author analyses Russian anti-terrorist legislation and selected regulations concerning extremism, which, in practice, are used by the Russian state as part of a broader system of control and threat assessment. The article also discusses cooperation in the fight against terrorism in the Collective Security Treaty Organisation. The author demonstrates that Moscow uses the narrative of the fight against terrorism to justify military action, strengthen social control and build influence beyond the country's borders, including in Central Asia, the Middle East and Africa. The Russian anti-terrorist model is based less and less on prevention and more and more on political definition of opponents, which leads to incorrect management of threat perception and, as a result, to further terrorist attacks.

Keywords

Russia, terrorism, extremism, ISIS, Asia, CSTO, anti-terrorism, the Kremlin

Wprowadzenie

Terroryzm należy do pojęć szeroko używanych, lecz trudnych do jednoznacznego zdefiniowania. Zjawisko terroryzmu jest bowiem dynamiczne, zależne od kontekstu prawnego i politycznego, a także od definiujących je podmiotów: państwa, organizacji międzynarodowej czy badacza. W literaturze funkcjonują setki ujęć, od opisów akcentujących przemoc wobec cywilów i efekt psychologiczny, po podejścia traktujące terroryzm jako metodę walki służącą wymuszeniu zmian politycznych lub ideologicznych. Alex P. Schmid określa terroryzm jako metodę powtarzających się aktów przemocy stosowanych przez częściowo tajnych aktorów indywidualnych, grupowych lub państwowych, motywowanych politycznie, kryminalnie lub idiosynkratycznie. W jego ujęciu bezpośrednie ofiary przemocy nie są głównym adresatem działania, ale służą jako narzędzie komunikatu kierowanego do wybranej grupy, władz lub społeczeństwa¹. Bruce Hoffman

¹ A.P. Schmid, *Defining Terrorism*, https://icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf [dostęp: 20 III 2026]; zob. także: A.P. Schmid, A.J. Jongman,

definiuje terroryzm jako celowe wzbudzanie strachu przez przemoc lub groźbę jej użycia i wykorzystywanie tego w dążeniu do zmiany politycznej. Podkreśla, że terroryzm ma wywoływać skutki psychologiczne wykraczające poza bezpośrednie ofiary ataku, ponieważ jego rzeczywistym adresatem jest szersza publiczność: społeczeństwo, rząd, opinia publiczna albo określona grupa polityczna, etniczna lub religijna².

W polskim ujęciu Krzysztof Liedel i Paulina Piasecka definiują terroryzm jako bezprawne użycie siły lub przemocy wobec osób albo mienia w celu zastraszenia lub wywarcia przymusu na rządzie albo ludności cywilnej. Głównym założeniem takich działań jest osiągnięcie celów politycznych lub społecznych³.

Global Terrorism Index nie przedstawia autorskiej definicji terroryzmu, ale na podstawie raportu z 2026 r. można przyjąć, że jest to (...) *groźba użycia lub faktyczne użycie nielegalnej siły i przemocy przez aktora niepaństwowego w celu osiągnięcia celu politycznego, ekonomicznego, religijnego lub społecznego poprzez zastraszenie, przymus lub wywołanie strachu*⁴. Dodatkowo, w źródle tym następuje rozróżnienie między pojęciami terror i terroryzm, a także kwestionuje się granicę między terroryzmem a oporem czy wojną partyzancką, bo to, co dla jednych jest zamachem, dla innych bywa narracją w walce o wolność⁵.

Trzeba podkreślić, że w artykule pojęcie ekstremizmu nie jest traktowane jako synonim terroryzmu. Ekstremizm oznacza szerszą kategorię ideologiczną, organizacyjną i polityczną, związaną ze skrajnymi poglądami, radykalizacją, propagandą lub działalnością środowisk uznawanych za zagrożenie. Może prowadzić do przemocy lub działalności terrorystycznej, ale nie musi być z nią tożsamy. Terroryzm odnosi się natomiast przede wszystkim do stosowania przemocy lub groźby jej użycia w celu politycznym,

Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature, Amsterdam 1988.

² *Database Scope*, RAND National Security Research Division, <https://www.rand.org/nsrd/projects/terrorism-incidents/about/definitions.html> [dostęp: 20 III 2026].

³ K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej*, Warszawa 2008, s. 46–47.

⁴ *Global Terrorism Index 2026*, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf>, s. 6–7 [dostęp: 13 IV 2026]. Tłumaczenia w tekście pochodzą od autora (dop. red.).

⁵ A.P. Schmid, *Defining Terrorism...*; L. Weinberg, A. Pedahzur, S. Hirsch-Hoefler, *The Challenges of Conceptualizing Terrorism*, „Terrorism and Political Violence” 2004, t. 16, nr 4, s. 777–794. <https://doi.org/10.1080/095465590899768>.

ideologicznym, religijnym albo społecznym. W rosyjskim systemie prawnym ekstremizm i terroryzm funkcjonują jako powiązane, ale nietożsame kategorie prawne. Widać to m.in. w art. 282.2 Kodeksu karnego Federacji Rosyjskiej, który dotyczy organizacji ekstremistycznej, ale wyraźnie wyłącza organizacje uznane zgodnie z prawem rosyjskim za terrorystyczne. Organizacje terrorystyczne są objęte odrębnymi regulacjami, w szczególności art. 205.5 Kodeksu karnego Federacji Rosyjskiej dotyczącym organizowania działalności organizacji terrorystycznej i udziału w niej. Jednocześnie w praktyce rosyjskiego aparatu bezpieczeństwa pojęcia ekstremizmu i terroryzmu bywają wykorzystywane równolegle jako instrumenty kontroli społecznej i politycznego definiowania zagrożeń. Dlatego w tekście termin „terroryzm” odnosi się przede wszystkim do aktów przemocy, zamachów i działalności organizacji terrorystycznych, „ekstremizm” natomiast pojawia się tam, gdzie są omawiane rosyjskie regulacje prawne, radykalizacja, propaganda oraz szersze mechanizmy politycznego definiowania przeciwników.

Dla władz Moskwy kluczowe jest osiągnięcie celów, dlatego wykorzystują własną i zależną od kontekstu definicję terroryzmu⁶. Z jednej strony, jak wskazują rosyjscy politycy, żaden kraj nie jest odporny na ataki terrorystyczne⁷. Z drugiej strony, terroryzm w ujęciu rosyjskim jest powiązany z polityką państwa, a nie tylko z zagrożeniem dla bezpieczeństwa. To oznacza, że Rosja może wykorzystywać szeroką definicję terroryzmu do nadawania działaniom przeciwników, w tym podmiotom zewnętrznym (organizacjom, państwom oraz grupom), charakteru terrorystycznego jako element ochrony swoich interesów, również poza granicami. Rosyjskie rozumienie terroryzmu różni się od ujęć przyjmowanych w państwach Zachodu, w tym w Polsce, zarówno na poziomie prawnym, jak i politycznym⁸.

⁶ W rosyjskim ustawodawstwie zdefiniowano akt terrorystyczny jako dokonanie eksplozji, podpalenia lub innych działań wywołujących strach wśród ludności oraz stwarzających zagrożenie dla życia, powodujących znaczne szkody materialne lub inne poważne konsekwencje, podejmowanych w celu destabilizacji działalności organów władzy lub organizacji międzynarodowych. Więcej w podrozdziale: *Rosyjskie ustawodawstwo wobec terroryzmu i ekstremizmu*.

⁷ G. Faulconbridge, *Russian security failure? Kremlin says no country is immune to terrorism*, Reuters, 25 III 2024 r., <https://www.reuters.com/world/europe/russian-security-failure-kremlin-says-no-country-is-immune-terrorism-2024-03-25/> [dostęp: 20 III 2026].

⁸ A. Olech, *Terroryzm – określenie definicji zjawiska w polskich i zagranicznych badaniach*, „Studia Bezpieczeństwa Narodowego” 2020, t. 18, nr 2, s. 121–138. <https://doi.org/10.37055/sbn/145302>.

W artykule autor przedstawił zagrożenia terrorystyczne, z jakimi przez lata zmagala się FR. Opisał także najważniejsze ugrupowania terrorystyczne oraz prowadzone przez nie działania na terytorium Rosji, przede wszystkim na Kaukazie Północnym. Ponadto podkreślił rolę współpracy międzynarodowej Moskwy oraz jej operacje zagraniczne, ze szczególnym naciskiem na zwalczanie terroryzmu. Omówił działania kontrterrorystyczne, strategię Organizacji Układu o Bezpieczeństwie Zbiorowym (dalej: OUBZ)⁹ w walce z terroryzmem oraz krajowe ustawodawstwo dotyczące terroryzmu i wybranych regulacji związanych z ekstremizmem.

Ramy objętościowe artykułu i przyjęty cel badawczy nie pozwalają na szczegółowe omówienie wszystkich aspektów rosyjskiej polityki wewnętrznej. Nie uwzględniono w nim upolitycznionych skazań na kary pozbawienia wolności oraz pełnej analizy instytucji uczestniczących zarówno w działaniach antyterrorystycznych, jak i w funkcjonowaniu aparatu represji. Te kwestie wymagają odrębnego opracowania.

Od początku pełnoskalowej inwazji FR na Ukrainę terroryzm w Rosji przestał być wyłącznie jednym z zagrożeń dla bezpieczeństwa, a stał się elementem polityki krajowej i międzynarodowej, narzędziem wykorzystywanym do wspierania działań politycznych i militarnych. Kolejne zamachy w Rosji po 2022 r. wykazały znaczne luki w działaniu aparatu bezpieczeństwa i brak efektywnej reakcji. Nie zmieniło to paradygmatu polityki Moskwy w stosunku do zagrożeń terrorystycznych. Przeciwnie – wzmacniana jest narracja przypisująca odpowiedzialność za ataki przeciwko FR przede wszystkim Ukrainie i państwom Zachodu¹⁰. W efekcie rosyjski model antyterrorystyczny coraz bardziej opiera się na zarządzaniu percepcją społeczeństwa i politycznym definiowaniu przeciwników, a nie na prewencji. Przez to kraj staje się podatny na kolejne ataki ze strony różnych grup¹¹.

Współczesna strategia Rosji w Europie opiera się na systemowym wykorzystywaniu środowisk przestępczych jako narzędzia wojny hybrydowej.

⁹ Organizację Układu o Bezpieczeństwie Zbiorowym tworzą: Federacja Rosyjska, Białoruś, Armenia, Kazachstan, Kirgistan i Tadżykistan, przy czym Armenia formalnie pozostaje członkiem organizacji, ale od lutego 2024 r. nie bierze udziału w jej pracach.

¹⁰ K. Hird i in., *Russian Offensive Campaign Assessment, March 25, 2024*, Critical Threats, 25 III 2024 r., <https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-march-25-2024> [dostęp: 20 III 2026].

¹¹ E. Ferris, *How Russia's War in Ukraine is Creating Domestic Security Gaps*, Royal United Services Institute, 23 IX 2025 r., <https://www.rusi.org/explore-our-research/publications/insights-papers/how-russias-war-ukraine-creating-domestic-security-gaps> [dostęp: 21 III 2026].

Rosyjskie służby rekrutują osoby o przeszłości kryminalnej, często znajdujące się w trudnej sytuacji ekonomicznej i wywodzące się ze środowisk rosyjskojęzycznych, do prowadzenia działań sabotażowych, takich jak uszkadzanie infrastruktury i akty wandalizmu¹². Mechanizm ten pozwala Rosji działać poniżej progu otwartego konfliktu, ograniczać ryzyko jednoznacznego przypisania jej odpowiedzialności oraz zmniejszać koszty operacyjne.

Rosyjskie ustawodawstwo wobec terroryzmu i ekstremizmu

Rosyjskie ustawodawstwo, w tym art. 205 Kodeksu karnego Federacji Rosyjskiej, definiuje akt terrorystyczny jako dokonanie eksplozji, podpalenia lub innych działań wywołujących strach wśród ludności oraz stwarzających zagrożenie dla życia, powodujących znaczne szkody materialne lub inne poważne konsekwencje, podejmowanych w celu destabilizacji działalności organów władzy lub organizacji międzynarodowych bądź wywarcia wpływu na ich decyzje. Przepis obejmuje również samą groźbę przeprowadzenia takich działań. W przypadku czynów popełnionych przez zorganizowaną grupę lub skutkujących poważnymi konsekwencjami przewidziano zastrzone kary, działania związane z wykorzystaniem materiałów jądrowych, substancji chemicznych lub biologicznych bądź prowadzące do śmierci człowieka mogą natomiast skutkować karą dożywotniego pozbawienia wolności. Jednocześnie przepisy przewidują możliwość zwolnienia z odpowiedzialności karnej osób, które przyczyniły się do zapobieżenia zamachowi¹³.

Rosyjskie ustawodawstwo, w szczególności federalna ustawa „O przeciwdziałaniu terroryzmowi”¹⁴, definiuje terroryzm jako ideologię

¹² K. Rekawek, J. Lanchès, M. Zotova, *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 VI 2026].

¹³ Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 205. Террористический акт (Ugołownyj Kodeks Rossijskoj Fiedieracyi ot 13.06.1996 No 63-FZ. Stat'ja 205. Tierroristiczeskij akt), https://www.consultant.ru/document/cons_doc_LAW_10699/43942021d9206af7a0c78b6f65ba3665db940264/ [dostęp: 20 III 2026].

¹⁴ Федеральный закон Российской Федерации от 06.03.2006 No 35-ФЗ „О противодействии терроризму”. Статья 3. Основные понятия (Fiedieralnyj zakon Rossijskoj Fiedieracyi ot 06.03.2006, No 35-FZ. „O protiwodiejstwii tierrorizmu”. Stat'ja 3. Osnownyje poniatija), https://www.consultant.ru/document/cons_doc_LAW_58840/4fdc493704d123d418c32ed-33872ca5b3fb16936/ [dostęp: 20 III 2026].

przemocy oraz praktykę wywierania wpływu na decyzje organów władzy lub organizacji międzynarodowych przez zastraszanie ludności lub inne formy bezprawnych działań z zastosowaniem przemocy. Ustawa wprowadza jednocześnie szerokie rozumienie działalności terrorystycznej, obejmujące przeprowadzanie zamachów, ich planowanie, finansowanie, podżeganie, tworzenie nielegalnych struktur zbrojnych, rekrutację i szkolenie sprawców, oraz działania informacyjne i propagandę. Zakres działalności terrorystycznej może być bardzo szeroki, biorąc pod uwagę również aktywność o charakterze informacyjnym i politycznym. Regulacje związane z przeciwdziałaniem terroryzmowi obejmują nie tylko prewencję, wykrywanie i zwalczanie zagrożeń, lecz także minimalizowanie ich skutków, prowadzenie operacji kontrterrorystycznych oraz zapewnienie ochrony obiektów i miejsc o szczególnym znaczeniu¹⁵. Rozszerzenie kategorii dotyczącej przestrzeni publicznej daje państwu znaczną swobodę interpretacyjną w kwalifikowaniu określonych aktywności jako działań terrorystycznych¹⁶.

Narodowy Komitet Antyterrorystyczny stanowi centralny organ koordynujący działania FR w zakresie przeciwdziałania terroryzmowi, integruje aktywność struktur federalnych, regionalnych i lokalnych pod przewodnictwem Federalnej Służby Bezpieczeństwa (FSB). Odpowiada za planowanie operacji kontrterrorystycznych, kształtowanie polityki państwa w tym obszarze oraz zarządzanie komunikacją dotyczącą zagrożeń¹⁷. To pokazuje centralizację rosyjskiego systemu bezpieczeństwa oraz istotną rolę Kremla w definiowaniu zagrożeń i zwalczaniu terroryzmu.

Rosja definiuje zjawisko tzw. terroryzmu międzynarodowego w sposób bardzo szeroki i powiązany bezpośrednio z własnymi interesami.

¹⁵ Operacja kontrterrorystyczna – zespół specjalnych, operacyjno-bojowych, wojskowych oraz innych działań z użyciem sprzętu bojowego, broni i środków specjalnych, mających na celu powstrzymanie aktu terrorystycznego, neutralizację terrorystów, zapewnienie bezpieczeństwa osobom fizycznym, organizacjom i instytucjom, a także minimalizację skutków aktu terrorystycznego. Rosyjskie ustawodawstwo odróżnia szeroko rozumianą działalność antyterrorystyczną (systemową) od operacji kontrterrorystycznej (konkretnego użycia siły), przy czym oba pojęcia są skonstruowane w taki sposób, że umożliwiają ich elastyczne – także polityczne – zastosowanie. Przeciwdziałanie terroryzmowi to działalność organów państwowych, organów władzy publicznej terytoriów federalnych i organów samorządu terytorialnego oraz osób fizycznych. Za: *Федеральный закон Российской Федерации от 06.03.2006 No 35-ФЗ...*

¹⁶ Tamże.

¹⁷ *National Antiterrorism Committee: goals and objectives*, National Antiterrorism Committee, <https://en.nac.gov.ru/home> [dostęp: 21 III 2026].

Artykuł 361 Kodeksu karnego obejmuje nie tylko klasyczne akty przemocy, takie jak zamachy czy podpalenia, lecz także wszelkie działania uznane za wymierzone przeciwko interesom FR lub zakłócające „pokoju współistnienie państw”. W praktyce oznacza to, że kategoria terroryzmu może być stosowana znacznie szerzej niż tylko wobec zagrożeń bezpieczeństwa w kraju. Co ważne, karze dożywotniego pozbawienia wolności mogą podlegać również osoby finansujące, werbujące lub szkolące sprawców takich ataków. Przepisy przewidują najwyższe kary w przypadku ataków, które doprowadziły do ofiar śmiertelnych¹⁸. Całość wpisuje się w ogólną tendencję rosyjskiego aparatu do maksymalnego zaostrzania odpowiedzialności karnej, przy jednoczesnym pozostawieniu przestrzeni do interpretacji.

Rosyjskie przepisy dotyczące działalności ekstremistycznej i terrorystycznej wskazują, że państwo traktuje te kategorie bardzo szeroko i przede wszystkim jako narzędzie kontroli. Artykuł 282.2 Kodeksu karnego przewiduje surowe kary (nawet 10–12 lat pozbawienia wolności w przypadku wykorzystania stanowiska służbowego) zarówno za organizowanie struktur uznanych za ekstremistyczne, jak i za samo uczestnictwo w nich czy werbunek. To oznacza, że granica między realnym zagrożeniem a działalnością uznaniowo określaną jako ekstremistyczna jest bardzo płynna. Co ważne, przepis ten dotyczy organizacji uznanych za ekstremistyczne¹⁹, z wyłączeniem organizacji, które zgodnie z ustawodawstwem FR zostały uznane za terrorystyczne²⁰. W praktyce pokazuje to, że ekstremizm

¹⁸ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Статья 361. Акт международного терроризма (Ugolownyj Kodeks Rossijskoj Fiedieracyi ot 13.06.1996. Stat'ja 361. Akt mieżdunarodnogo tierrorizma), https://www.consultant.ru/document/cons_doc_LAW_10699/0994b72ccab34fae773ced2c837691518a3e3dca/ [dostęp: 20 III 2026].

¹⁹ Lista organizacji uznanych za ekstremistyczne zgodnie z ustawodawstwem Federacji Rosyjskiej zob. Перечень организаций, признанных в соответствии с законодательством Российской Федерации экстремистскими, Министерство юстиции Российской Федерации (Pierieczien' organizacyj, priznannych w sootwietstwiu s zakonodatelstwom Rossijskoj Fiedieracyi ekstriemists, Ministerstwo justycyi Rossijskoj Fiedieracyi), <https://minjust.gov.ru/ru/documents/7822/> [dostęp: 20 IV 2026].

²⁰ Jednolita federalna lista organizacji (obejmująca organizacje zagraniczne i międzynarodowe) uznanych za terrorystyczne zgodnie z ustawodawstwem Federacji Rosyjskiej zob. Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими (на 4 апреля 2026 г.), Федеральная служба безопасности Российской Федерации (Jedynyj fiedieralnyj spisok organizacyj, w tom czisle inostrannyh i mieżdunarodnyh organizacyj, priznannych w sootwietstwiu s zakonodatelstwom Rossijskoj Fiedieracyi tierroristiczeskimi (na 4 apriela 2026 g.), Fiedieralnaja

i terroryzm funkcjonują w rosyjskim prawie jako powiązane, ale nietożsame kategorie. Jednocześnie jest możliwe uniknięcie odpowiedzialności przez dobrowolne zaprzestanie działalności, ale w praktyce ostateczna decyzja należy do aparatu bezpieczeństwa, który decyduje, czy dana osoba rzeczywiście przestała działać i czy powinna ponieść konsekwencje.

Zagrożenia terrorystyczne dotyczące Federacji Rosyjskiej

Wśród państw należących do OUBZ Rosja stanowi główny rejon zagrożeń o charakterze terrorystycznym w przestrzeni postsowieckiej, a zarazem jest państwem oskarżanym o działania o charakterze terrorystycznym w wymiarze wewnętrznym i zewnętrznym. Kreml, aby osiągnąć własne cele, w sposób demonstracyjny sięga w polityce wewnętrznej po działania, które wpisują się w definicję terroryzmu. Równolegle FR rozwija strategię antyterrorystyczną, którą wykorzystuje do podporządkowywania sobie regionów, społeczności i uzasadniania działań militarnych. Przez dziesięciolecia Rosja udowodniła, że bardzo sprawnie wykorzystuje „zagrożenie terroryzmem”, żeby osiągać swoje cele. Tak jest w przypadku obszaru Kaukazu, działań na kontynencie afrykańskim i względem Ukrainy²¹. Jednocześnie FR wielokrotnie ponosi konsekwencje swojej działalności antyterrorystycznej²², gdyż staje się celem grup terrorystycznych²³.

Po rozpadzie Związku Radzieckiego największą koncentrację ataków terrorystycznych na terytorium FR odnotowywano na Kaukazie Północnym, zwłaszcza w Czeczenii, Dagestanie i Inguszetii. Obszary te od lat stanowią główne ogniska działalności ugrupowań islamistycznych i separatystycznych. Choć Osetia Północna była miejscem jednego z najtragiczniejszych

służba bieżącej ochrony Rosji (Fiedieracy), <http://www.fsb.ru/fsb/npd/terror.htm> [dostęp: 20 IV 2026].

²¹ A. Wilk, W. Konończuk, *Wojna ukraińsko-rosyjska pod szyldem operacji antyterrorystycznej*, Ośrodek Studiów Wschodnich, 6 VIII 2014 r., <https://www.osw.waw.pl/pl/publikacje/analizy/2014-08-06/wojna-ukrainsko-rosyjska-pod-szyldem-operacji-antyterrorystycznej> [dostęp: 19 I 2026].

²² J. Flanagan, *Bloodshed and retreat from Mozambique for Putin's private army the Wagner Group*, The Times, 25 XI 2019 r., <https://www.thetimes.com/uk/politics/article/bloodshed-and-retreat-from-mozambique-for-putin-s-private-army-the-wagner-group-696tnpzqh> [dostęp: 19 I 2026].

²³ *The Deadliest Attacks In Russia*, Radio Free Europe/Radio Liberty, <https://www.rferl.org/a/russia-timeline-terror-attacks/28410225.html> [dostęp: 19 I 2026].

zamachów terrorystycznych w historii Rosji, to jej znaczenie we współczesnej statystyce ataków jest mniejsze niż pozostałych republik kaukaskich²⁴. Jeszcze w 2012 r., przed serią zamachów w Europie Zachodniej m.in. we Francji, Wielkiej Brytanii, Belgii i Niemczech, konflikt o charakterze terrorystycznym na Kaukazie Północnym uchodził za najbrutalniejszy tego typu konflikt w Europie. W starciach między siłami FR a bojownikami określonymi przez rosyjskie władze mianem terrorystów ginęło w tym okresie ok. 700–800 osób rocznie²⁵. Co więcej, w latach 1992–2011 na terytorium Rosji odnotowano 1415 ataków terrorystycznych powiązanych z ugrupowaniami działającymi na Kaukazie Północnym. Do największej liczby incydentów doszło w Czeczenii, Dagestanie i Inguszetii, co potwierdza koncentrację zagrożenia terrorystycznego w tym regionie. Część zamachów była przeprowadzana również m.in. w Moskwie oraz Sankt Petersburgu.

Doświadczenia FR z terroryzmem islamistycznym mają charakter długotrwały i systemowy. Od wojny w Afganistanie (1979–1989), przez konflikty czeczeńskie, aż po zaangażowanie w Syrii, Moskwa pozostaje jednym z głównych przeciwników środowisk dżihadystycznych. W efekcie Rosja wielokrotnie była celem zamachów, a kulminacją były ataki przeprowadzone w teatrze na Dubrowce (2002 r.), w szkole w Biesłanie (2004 r.), a także w sali koncertowej Crocus City Hall (2024 r.). Jednocześnie należy podkreślić, że mimo świadomości zagrożenia, rosyjski aparat bezpieczeństwa ma ograniczone możliwości jego skutecznego neutralizowania²⁶, zwłaszcza w warunkach przeciążenia wojną przeciwko Ukrainie.

²⁴ IntelBrief: *Radicalization and Extremism in Russia's North Caucasus Region*, The Soufan Center, 12 IV 2024 r., <https://thesoufancenter.org/intelbrief-2024-april-12/> [dostęp: 26 X 2025]; M. Bartosiewicz, *Postępująca radykalizacja. Ataki terrorystyczne w Dagestanie*, Ośrodek Studiów Wschodnich, 25 VI 2024 r., <https://www.osw.waw.pl/pl/publikacje/analizy/2024-06-25/postepujaca-radykalizacja-ataki-terrorystyczne-w-dagestanie> [dostęp: 26 X 2025]; T. Grabowski, *Terroryzm północnokaukaski: przejawy zjawiska*, „Res Polticae” 2014, t. VI, s. 59–78. <http://dx.doi.org/10.16926/rp.2014.06.04>; M. Johns, *Terrorism and the North Caucasus: An Overview*, „START Background Report”, National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, April 2013, s. 1–5, https://www.academia.edu/8490735/Terrorism_and_the_North_Caucasus_An_Overview [dostęp: 16 VI 2026].

²⁵ T.W. Grabowski, *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku*, Kraków 2017, s. 7.

²⁶ J. de Gliniasty, *Moscow Attack: Russia Confronts Islamist Terrorism*, Institut de Relations Internationales et Stratégiques, 26 III 2024 r., <https://www.iris-france.org/en/184928-moscow-attack-russia-confronts-islamist-terrorism/> [dostęp: 21 III 2026].

Rosyjska „wojna z terroryzmem” w Czeczenii od lat 90. XX w. nie była wyłącznie operacją o charakterze wewnętrznym, ale elementem strategii polityki zagranicznej. Po zamachach z 11 września 2001 r. FR dążyła do wpisania swoich działań na Kaukazie w narrację globalnej walki z terroryzmem, wykorzystując chwilową zbieżność interesów ze Stanami Zjednoczonymi, zwłaszcza w kontekście operacji w Afganistanie oraz amerykańskiej obecności wojskowej w Azji Centralnej²⁷. Relacje Rosji z Europą pozostawały napięte z uwagi na krytykę naruszeń praw człowieka w Czeczenii, odmowy ekstradycji podejrzanych oraz oskarżenia o ingerencję w krajach byłego ZSRR, co stopniowo zmniejszało pole do współpracy. Rosja instrumentalizowała narrację dotyczącą antyterroryzmu, podporządkowując ją interesom politycznym. Sprzeciwiała się wzrostowi wpływów USA w wielu regionach świata. Jednocześnie wskazywała na rozbieżność między deklarowaną przez Waszyngton potrzebą konsekwentnego zwalczania terroryzmu a zróżnicowanym podejściem Stanów Zjednoczonych do poszczególnych państw i organizacji, m.in. w kontekście Afganistanu, Iranu, Syrii, Hezbollahu i Hamasu. W rosyjskiej narracji miało to potwierdzać tezę o podwójnych standardach USA, polegających na tym, że kwalifikacja danego podmiotu jako terrorystycznego lub jako partnera politycznego zależała nie tylko od jego metod działania, lecz także od bieżących interesów Stanów Zjednoczonych i ich sojuszników. To pozwalało Moskwie podważać wiarygodność USA i osłabiać rzeczywisty wymiar współpracy z Zachodem w walce z terroryzmem. W latach 2001–2022 Rosja konsekwentnie łączyła krytykę zachodnich „podwójnych standardów” w walce z terroryzmem z próbami legitymizowania własnej polityki bezpieczeństwa, w tym działań prowadzonych na Kaukazie Północnym, w Syrii oraz w innych regionach uznawanych przez Moskwę za istotne dla jej interesów²⁸. Obecnie nadal próbuje lawirować między działaniami na poziomie politycznym w kontekście polityki antyterrorystycznej oraz zaangażowaniem wojskowym w operacje antyterrorystyczne w Rosji i na całym świecie.

Przez wiele lat czeczeńscy separatyści byli przedstawiani przez rosyjskie władze jako najpoważniejsze źródło zagrożenia terrorystycznego dla FR. W części literatury anglojęzycznej określano ich m.in. jako Chechen

²⁷ M. McFaul, *U.S. Russia Relations After September 11, 2001*, Carnegie Endowment for International Peace, 24 X 2001 r., <https://carnegieendowment.org/posts/2001/10/us-russia-relations-after-september-11-2001?lang=en> [dostęp: 21 III 2026].

²⁸ I. Oldberg, *The War on Terrorism in Russian Foreign Policy*, FOI – Swedish Defence Research Agency, Defence Analysis, Stockholm 2006.

Rebels lub Chechen Separatist Movement²⁹. W latach 1999–2013 struktury wywodzące się z tego ruchu odpowiadały za większość zamachów terrorystycznych przeprowadzonych na terytorium FR, jednak z czasem ich aktywność znacznie się zmniejszyła. Nową fazę terroryzmu północnokaukaskiego zapoczątkowało powstanie 31 października 2007 r. kolejnej organizacji terrorystycznej, założonej przez Doku Umarowa, jednego z przywódców północnokaukaskich rebeliantów. Zrzekł się on funkcji prezydenta Czecheńskiej Republiki Iczkerii i ogłosił utworzenie Emiratu Kaukaskiego (Caucasus Emirate)³⁰ – islamistycznej, samowłańczej struktury organizacyjnej, stanowiącej przez lata główne zaplecze terrorystyczne w regionie Kaukazu Północnego.

Proces formowania struktur zbrojnych o charakterze terrorystycznym na Kaukazie Północnym rozpoczął się już w 1999 r. Funkcjonujące wówczas lokalne dżamaaty w Dagestanie, Inguszetii, Kabardo-Bałkarii, Karaczajo-Czerkiesji oraz Osetii Północnej stały się w kolejnych latach zapleczem organizacyjnym i kadrowym dla Emiratu Kaukaskiego, ogłoszonego formalnie w 2007 r.³¹ W grudniu 2009 r. Sąd Najwyższy Federacji Rosyjskiej zakazał działalności Emiratu Kaukaskiego, uznając go za organizację terrorystyczną. Od tego momentu Emirat Kaukaski stał się jednym z głównych źródeł zagrożenia terrorystycznego związanego z Kaukazem Północnym oraz jednym z istotnych wyzwań dla rosyjskiego systemu antyterrorystycznego³².

²⁹ P. Bhattacharji, *Chechen Terrorism (Russia, Chechnya, Separatist)*, Council on Foreign Relations, 8 IV 2010 r., <https://www.cfr.org/backgrounders/chechen-terrorism-russia-chechnya-separatist> [dostęp: 20 III 2026]; T. Grabowski, *Terroryzm północnokaukaski: przejawy zjawiska...*

³⁰ *The North Caucasus: The Challenges of Integration (II), Islam, the Insurgency and Counter-Insurgency*, Europe Report N°221, 19 X 2012 r.; *Caucasus Emirate*, START – National Consortium for the Study of Terrorism and Responses to Terrorism, January 2015, <https://www.start.umd.edu/baad/narratives/caucasus-emirate.html> [dostęp: 19 I 2026]; B. Roggio, *Doku Umarov declares Islamic Caucasus Emirate*, Long War Journal, 26 XI 2007 r., https://www.longwarjournal.org/archives/2007/11/doku_umarov_declares.php [dostęp: 19 I 2026].

³¹ T.W. Grabowski, *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku...*, s. 159.

³² J. Sinai, *The Terrorist Threats Against Russia and its Counterterrorism Response Measures*, „Connections: The Quarterly Journal” 2015, t. 14, nr 4, s. 95–101. <http://dx.doi.org/10.11610/Connections.14.4.08>; M. Falkowski, *Państwo Islamskie na Kaukazie – cui bono?*, Ośrodek Studiów Wschodnich, 14 I 2015 r., <https://www.osw.waw.pl/pl/publikacje/analizy/2015-01-14/panstwo-islamskie-na-kaukazie-cui-bono> [dostęp: 12 III 2026]; M. Youngman, C. Moore, *Guide: The Caucasus Emirate*, Radicalisation Research, 9 XI 2017 r., <https://radicalisationresearch.org/research/youngman-guide-caucasus-emirate/> [dostęp: 12 III 2026].

Wzrost znaczenia tzw. Państwa Islamskiego (Islamic State of Iraq and Syria, ISIS) wywarł bezpośredni wpływ na sytuację bezpieczeństwa na rosyjskim Kaukazie Północnym. ISIS należy w tym kontekście traktować przede wszystkim jako organizację terrorystyczną, choć jej działalność była oparta na ekstremistycznej ideologii, radykalnej propagandzie oraz międzynarodowych mechanizmach prowadzenia rekrutacji. Region opuściły setki bojowników, aby dołączyć do działań zbrojnych w Syrii i Iraku, a wśród cudzoziemców walczących w szeregach ISIS i innych ugrupowaniach dżihadystycznych znaczną grupę stanowili obywatele FR, w dużej mierze pochodzący właśnie z Kaukazu Północnego. Ten proces osłabił Emirat Kaukaski i ograniczył jego możliwości rekrutacyjne. Doprowadziło to do fragmentacji tej organizacji, ponieważ część dowódców i bojowników złożyła przysięgę wierności ISIS, a część kontynuowała działalność w regionie już pod jego szyldem³³. W konsekwencji na Kaukazie Północnym zaczęły współistnieć – często w warunkach rywalizacji – resztki struktur Emiratu Kaukaskiego oraz nowe formacje związane z Państwem Islamskim, co oznaczało przesunięcie ciężaru zagrożenia z lokalnej, kaukaskiej perspektywy na wymiar transnarodowy.

Po 2014 r. struktury Emiratu Kaukaskiego się rozpadły. Była to konsekwencja zarówno nasilonych działań rosyjskich służb bezpieczeństwa, jak i głębokich podziałów wewnętrznych w środowisku kaukaskich ugrupowań dżihadystycznych. Ważnym czynnikiem osłabiającym pozycję grupy terrorystycznej była nielojalność części jej dowódców i bojowników, którzy w latach 2014–2015 złożyli przysięgę wierności ISIS. Doprowadziło to do podporządkowania części kaukaskich struktur Państwu Islamskiemu. ISIS stopniowo przejęło rolę dominującego ośrodka ideologicznego i organizacyjnego dla radykalnych środowisk wywodzących się z Kaukazu Północnego³⁴. W rezultacie Emirat Kaukaski utracił zdolność do niezależnego wyznaczania kierunków działalności i koordynowania działań na znaczną skalę w Rosji i republikach autonomicznych. Ustąpił miejsca silniejszej organizacji powiązanej z ISIS.

To właśnie w kolejnych latach istotną rolę w krajobrazie zagrożeń terrorystycznych w Rosji odegrała utworzona w czerwcu 2015 r. Prowincja

³³ M. Ter, *The Caucasus Emirate, the Other Russian Front*, https://www.cidob.org/sites/default/files/2024-07/NOTES%20129_TER_ANG.pdf [dostęp: 16 VI 2026].

³⁴ *The North Caucasus Insurgency and Syria: An Exported Jihad?*, International Crisis Group, 16 III 2016 r., <https://www.crisisgroup.org/europe-central-asia/russia-internal-syria/238-north-caucasus-insurgency-and-syria-exported-jihad> [dostęp: 19 I 2026].

Kaukaska Państwa Islamskiego (Wilayat al-Qawqaz, Islamic State Caucasus Province), która przejęła część kadr oraz zaplecza organizacyjnego dawnego Emiratu Kaukaskiego. Była to konsekwencja masowego składania przysięg wierności Państwu Islamskiemu przez przywódców lokalnych dżamaatów. Proces ten doprowadził do wchłonięcia przez struktury ISIS znacznej liczby dotychczasowych zwolenników Emiratu, a jednocześnie do wewnętrznej fragmentacji środowiska zbrojnego na Kaukazie Północnym. Skutkiem było czasowe osłabienie aktywności operacyjnej ugrupowań dżihadystycznych oraz spadek liczby ataków w latach 2014–2015 w takich republikach jak Dagestan i Inguszetia. Szacuje się, że w okresie konfliktu syryjskiego ok. 2800 bojowników z państw byłego Związku Radzieckiego dołączyło do działań zbrojnych w szeregach ISIS³⁵, w tym osoby pochodzące z regionu Kaukazu Północnego oraz państw Azji Centralnej. Oznaczało to stopniowy rozpad Emiratu Kaukaskiego i przejęcie jego kadr oraz zaplecza przez struktury ISIS, przede wszystkim Prowincję Kaukaską Państwa Islamskiego³⁶, która od 2015 r. stała się głównym ogniwem dżihadystycznej aktywności na Kaukazie Północnym.

Tym samym to aktywność ISIS od lat stanowi jedno z największych wyzwań dla rosyjskiego aparatu bezpieczeństwa, przede wszystkim ze względu na podatność części regionów Kaukazu Północnego na rozwój terroryzmu. Idee globalnego dżihadu i budowy kalifatu znajdowały tam zwolenników jeszcze przed formalnym pojawieniem się struktur ISIS. Momentem przełomowym był rok 2015, gdy organizacja otwarcie ogłosiła dżihad przeciw FR. Taka decyzja była bezpośrednio związana z militarnym zaangażowaniem rosyjskich wojsk w Syrii po stronie reżimu Baszara al-Asada, a przez to uznano Rosję za priorytetowy cel ISIS. Towarzyszyły temu liczne działania propagandowe, rekrutacyjne oraz terrorystyczne.

Kreml odpowiadał wzmacnianiem kompetencji aparatu bezpieczeństwa, co z jednej strony zwiększało kontrolę państwa, a z drugiej mogło pogłębiać napięcia społeczne i polityczne³⁷.

³⁵ F. Hanoush, *Fighters from the Caucasus Join ISIS to Fight Russia*, Atlantic Council, 14 IX 2016 r., <https://www.atlanticcouncil.org/blogs/syriasource/fighters-from-the-caucasus-join-isis-to-fight-russia/> [dostęp: 21 III 2026].

³⁶ M. Vatchagaev, *Caucasus Emirate and Islamic State Split Slows Militant Activities in North Caucasus*, Jamestown, 14 II 2015 r., <https://jamestown.org/program/caucasus-emirate-and-islamic-state-split-slows-militant-activities-in-north-caucasus-2/> [dostęp: 20 I 2026].

³⁷ A.M. Dyner, *Zamach w Moskwie*, Polski Instytut Spraw Międzynarodowych, 25 III 2024 r., <https://www.pism.pl/publikacje/zamach-w-moskwie> [dostęp: 19 I 2026].

W 2015 r. zagrożenie terroryzmem w Rosji znacznie wzrosło nie tylko ze strony bojowników pochodzenia czeczeńskiego, dagestańskiego i szerzej północnokaukaskiego walczących o niepodległość, lecz także ze strony innych organizacji terrorystycznych. Gdy we wrześniu 2015 r. Rosja rozpoczęła ofensywę wojskową przeciwko rebeliantom w Syrii, zareagował odłām Al-Kaidy – organizacja Front al-Nusra (Jabhat al-Nusra)³⁸. Przywódca grupy terrorystycznej Abu Muhammad al-Julani wezwał wówczas do ataków odwetowych na rosyjskich obywateli w Syrii. Reakcja osób popierających organizację terrorystyczną była prawie natychmiastowa – 13 października 2015 r. dwie rakiety uderzyły w ambasadę Rosji w Damaszku³⁹. Tym samym ugrupowania terrorystyczne funkcjonujące dotychczas w Afryce i na Bliskim Wschodzie zintensyfikowały działania przeciwko FR⁴⁰.

Warto zwrócić uwagę, że według szacunków z grudnia 2015 r. obywatele Rosji stanowili ok. 8% ogółu zagranicznych bojowników, którzy podczas konfliktu syryjskiego wyjechali do Syrii i Iraku, aby dołączyć do ISIS oraz innych ugrupowań dżihadystycznych. Liczba rosyjskich ochotników wynosiła ok. 2400 osób (stan na wrzesień 2015 r.), podczas gdy łączną skalę zjawiska oceniano na 27 000–31 000 wyjazdów z co najmniej 86 państw⁴¹. Potwierdza to istotny udział Rosjan wśród zagranicznych bojowników.

Kolejnym przykładem eskalacji działań terrorystycznych przeciwko FR po rozpoczęciu jej interwencji wojskowej w Syrii był zamach na rosyjski samolot pasażerski lecący z Szarm el-Szejk do Petersburga. W dniu 31 października 2015 r. na pokładzie samolotu linii Metrojet doszło do eksplozji ładunku wybuchowego, w wyniku której zginęły łącznie 224 osoby (217 pasażerów i 7 członków załogi). Wśród ofiar większość stanowili Rosjanie, z wyjątkiem trzech pasażerów Ukrainy i jednego z Białorusi. Odpowiedzialność

³⁸ J. Beslin, M. Ignjatijevic, *Balkan foreign fighters: from Syria to Ukraine*, „Brief” 2017, nr 20, s. 1–4.

³⁹ *Al-Qaeda in Syria calls for revenge attacks on Russia*, The Washington Post, 13 X 2015 r., https://www.washingtonpost.com/world/middle-east/al-qaeda-in-syria-calls-for-revenge-attacks-on-russia/2015/10/13/b7f7dfdf-a0a4-451d-bd2e-180f2f4882f5_story.html [dostęp: 16 V 2026]; *Syria crisis: Rockets hit Russian embassy compound in Damascus, reports say*, ABC News, 13 X 2015 r., <https://www.abc.net.au/news/2015-10-13/rockets-hit-russian-embassy-compound-in-damascus-reports/6851968> [dostęp: 16 V 2026].

⁴⁰ A.K. Olech, *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku*, „Nowa Polityka Wschodnia” 2019, nr 4, s. 110–115. <https://doi.org/10.15804/NPW20192306>.

⁴¹ *Foreign Fighters. An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq*, December 2015, https://thesoufancenter.org/wp-content/uploads/2017/05/TSG_Foreign-FightersUpdate_format-for-print-120915-REBRAND-031317.pdf [dostęp: 21 I 2026].

za atak wzięły na siebie struktury ISIS, wskazując zamach jako bezpośredni odwet za rosyjską interwencję zbrojną w Syrii⁴². To pokazuje, że rosyjskie zaangażowanie militarne na Bliskim Wschodzie skutkowało intensyfikacją zagrożenia terrorystycznego poza obszar Kaukazu Północnego, a obywatele FR byli celem ataków również poza krajem.

Prowincja Kaukaska Państwa Islamskiego przypisała sobie atak na rosyjski obiekt wojskowy w południowym Dagestanie dokonany 2 września 2015 r., jednak informacja o tym zdarzeniu nie została niezależnie potwierdzona. W nagraniu opublikowanym przez rosyjskojęzyczny środek przekazu ISIS przywódca dagestańskich struktur Prowincji Kaukaskiej Furat Media Abu Mukhammad Kadarsky (Rustam Asildarov) wezwał zwolenników organizacji do prowadzenia walki na Kaukazie zamiast wyjazdu do Syrii⁴³. Przekonywał, że podejmowanie działań w regionie będzie skuteczniejsze niż wyjazd na Bliski Wschód w celu wspierania struktur ISIS w Iraku i Syrii. Był to przykład propagandy ukierunkowanej na mobilizowanie zwolenników do podejmowania działań w kraju zamieszkania, bez konieczności przemieszczania się na obszary konfliktów zbrojnych.

Innym ugrupowaniem działającym przeciwko FR był powiązany z Al-Kaidą Batalion Imama Szamila (Katibat Imam Shamil), określający się mianem Rycerzy Islamu. Grupa przypisała sobie samobójczy zamach przeprowadzony 3 kwietnia 2017 r. w metrze w Petersburgu, między stacjami Siennaja Płoszczad' i Technologiczeskij Institut. W wyniku ataku zginęło 15 osób, a kilkadziesiąt zostało rannych. Drugie urządzenie wybuchowe odnaleziono i rozbrojono na innej stacji metra. Rosyjskie władze w związku z zamachem zatrzymały 11 osób pochodzących z Azji Centralnej⁴⁴. Te wydarzenia pokazują znaczenie transnarodowych środowisk dżihadystycznych oraz ich zdolność do prowadzenia i inspirowania działań terrorystycznych na terytorium FR.

⁴² Z. Gold, *Wilayat Sinai Risks Backlash After Metrojet Bombing*, <https://ctc.westpoint.edu/wp-content/uploads/2015/12/CTCSentinel-Vol8Iss118.pdf>, s. 19–22 [dostęp: 19 I 2026]; D. Costa-Roberts, *Questions swirl over Russian plane crash in Egypt that killed 224*, PBS News, 1 XI 2015 r., <https://www.pbs.org/newshour/world/details-emerge-case-downed-russian-jet> [dostęp: 20 I 2026].

⁴³ J. Paraszczuk, *IS's North Caucasus Affiliate Calls for Recruits to Join It in Daghestan*, Radio Free Europe/Radio Liberty, 3 X 2015 r., <https://www.rferl.org/a/islamic-state-north-caucasus-affiliate-call-for-recruits-daghestan/27285024.html> [dostęp: 16 V 2026].

⁴⁴ A.K. Olech, *Ataki terrorystyczne...*, s. 109–129.

W latach 2015–2022 Rosja mierzyła się z zagrożeniem zamachami terrorystycznymi skoncentrowanym na Kaukazie Północnym. Odpowiadały za nie głównie grupy dżihadystyczne powiązane z Prowincją Kaukaską Państwa Islamskiego, które przejęły część kadr i struktur dawnego Emiratu Kaukaskiego. Ataki miały najczęściej charakter wycelowanych uderzeń i, co ważne, były wymierzone w funkcjonariuszy służb bezpieczeństwa, lokalnych przedstawicieli władz oraz instytucje religijne⁴⁵.

Język rosyjski stał się trzecim najpopularniejszym językiem propagandy ISIS (po arabskim i angielskim), a rosyjska interwencja w Syrii była czynnikiem, który mógł dodatkowo wzmocnić oddziaływanie ugrupowań radykalnych w Rosji – zarówno samego ISIS, jak i innych środowisk radykalnych oraz dżihadystycznych⁴⁶. Można z tego wnioskować, że język rosyjski, ze względu na wzmożoną aktywność organizacji terrorystycznych i środowisk radykalnych na terytorium Rosji oraz w krajach sąsiadujących, zyskał istotne znaczenie w ponadnarodowej komunikacji propagandowej i rekrutacyjnej środowisk dżihadystycznych.

Od 2020 r. w Rosji coraz większe znaczenie zyskiwała działalność Państwa Islamskiego Prowincji Chorasán (Islamic State Khorasan Province, ISIS-K), czyli regionalnej struktury ISIS aktywnej przede wszystkim w Afganistanie i Azji Centralnej. Organizacja stopniowo przejmowała inicjatywę w planowaniu oraz inspirowaniu zamachów wymierzonych w Rosję. Ta grupa realizuje operacje inaczej niż wcześniejsze ugrupowania północnokaukaskie. Dotyczy to zarówno sposobu działania, jak i rekrutacji, która w dużej mierze opiera się na migrantach zarobkowych z Tadżykistanu, Uzbekistanu i Kirgistanu, funkcjonujących na marginesie rosyjskiego społeczeństwa. To właśnie te środowiska stały się dla organizacji zapleczem rekrutacyjnym. Są one podatne na radykalizację w warunkach dyskryminacji, represji i dezinformacji w Rosji. Tym samym w FR działają także struktury międzynarodowe, a nawet globalne organizacje terrorystyczne⁴⁷. W takim ujęciu nie da się neutralizować zagrożenia wyłącznie przy użyciu

⁴⁵ M.S. Stempień, *The evolution of terrorism in Russia in the years 2015–2022. Quantitative analysis of the phenomenon*, „Przegląd Wschodnioeuropejski” 2023, nr 14, s. 185–199. <https://doi.org/10.31648/pw.9711>.

⁴⁶ A. Borshchevskaya, *Russian Officials Inadvertently Aid Radical Islamists in Russia*, The Washington Institute for Near East Policy, 31 XII 2015 r., <https://www.washingtoninstitute.org/policy-analysis/russian-officials-inadvertently-aid-radical-islamists-russia> [dostęp: 22 I 2026].

⁴⁷ IntelBrief: *Radicalization and Extremism in Russia's...*

brutalnych metod lub zaangażowania wyspecjalizowanych grup kontrterrorystycznych, czyli procedur stosowanych dotychczas przez Kreml.

Należy zwrócić uwagę, że w kontekście całego regionu Azji Centralnej i w Afganistanie aktywność ISIS-K rosła stopniowo od 2020 r., a kulminacją działań terrorystycznych w Rosji był zamach 22 marca 2024 r., w którym zginęły 144 osoby, a 551 zostało rannych. Był to nie tylko jeden z największych pokazów zdolności ISIS-K w Rosji⁴⁸, lecz także jeden z największych ataków terrorystycznych w skali globalnej. ISIS-K przeprowadziło atak w Crocus City Hall, w rejonie Krasnogorska w obwodzie moskiewskim. Już dzień po zamachu Narodowy Komitet Antyterrorystyczny poinformował o zatrzymaniu 11 podejrzanych⁴⁹. Wśród istotnych motywów działania sprawców należy wymienić to, że działania ISIS-K stanowiły reakcję na zacieśnioną współpracę Rosji z Talibami⁵⁰ oraz aktywność rosyjskich wojsk w Syrii i Sahele przeciwko Państwu Islamskiemu⁵¹.

W kontekście zamachu na Crocus City Hall trzeba odnotować, że Rosja miała otrzymać informacje o planowanych zamachach w halach koncertowych w Moskwie od służb z innych państw, tych zaprzyjaźnionych (Iran) i tych wrogich (USA⁵²). Ograniczona reakcja rosyjskich władz może wskazywać, że nie dysponowały one wystarczającą wiedzą o zagrożeniu albo nie nadały sygnałom ostrzegawczym odpowiedniej wagi. Rosyjskie służby bezpieczeństwa mogły zatem nie tyle całkowicie wykluczyć możliwość wystąpienia zagrożenia, ile błędnie ocenić jego prawdopodobieństwo, skalę lub pilność. Możliwe również, że ich uwaga w tym czasie była

⁴⁸ K. Strachota, *Państwo Islamskie Chorasanu – nowa odsłona światowego dżihadu*, 29 III 2024 r., Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-03-29/panstwo-islamskie-chorasanu-nowa-odslona-swiatowego-dzihadu> [dostęp: 20 I 2026].

⁴⁹ *Global Terrorism Index 2025*, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf> [dostęp: 22 I 2026]; A.M. Dyner, *Zamach w Moskwie...*

⁵⁰ M.N. Katz, *No, Putin, the ISIS-K attack in Moscow wasn't about Ukraine*, Atlantic Council, 29 III 2024 r., <https://www.atlanticcouncil.org/blogs/menasource/isis-k-putin-moscow-al-qaeda/> [dostęp: 20 I 2026].

⁵¹ A. Olech, *Grupa Wagnera w Afryce. Pozorowana walka rosyjskich najemników z terroryzmem*, „Terroryzm – studia, analizy, prewencja” 2024, nr 5, s. 53–89. <https://doi.org/10.4467/27204383TER.24.002.19390>.

⁵² *On the Terrorist Attack at the Crocus City Hall in Moscow*, U.S. Mission to the Organization for Security and Cooperation in Europe, 11 IV 2024 r., <https://osce.usmission.gov/on-the-terrorist-attack-at-the-crocus-city-hall-in-moscow/> [dostęp: 20 III 2026].

skoncentrowana na innych priorytetach, w tym na działaniach prowadzonych poza granicami kraju.

Z opracowania Royal United Services Institute wynika, że aparat państwowy, na czele z FSB, na pierwszym miejscu stawiał wyzwania o charakterze politycznym i społecznym względem rosyjskiej operacji przeciwko Ukrainie. Terroryzm nie był priorytetem. Nawet po samym zamachu od razu założono, że są za niego odpowiedzialne zachodnie służby (na czele z amerykańskimi i brytyjskimi) oraz Ukraina. Innym ważnym aspektem jest radykalizacja w samej Rosji, także wśród migrantów z Tadżykistanu i Uzbekistanu. W 2024 r. w Rosji doszło do pięciu zamachów i żaden nie został wcześniej wykryty⁵³. Jak na kraj, który od dziesięcioleci zmagają się z terroryzmem, tak duże uchybienia świadczą o braku zdolności do reagowania, niedoborze zasobów (w tym wyspecjalizowanych oficerów), nie traktowaniu terroryzmu jako priorytetu oraz znacznej koncentracji na wojnie w Ukrainie.

Również w 2024 r. na terytorium Rosji doszło do zamachu terrorystycznego w Dagestanie, gdzie uzbrojeni napastnicy przeprowadzili skoordynowane ataki na prawosławne cerkwie, synagogi oraz posterunek policji w miastach Derbent i Machaczka⁵⁴. W wyniku tych zamachów, nazwanych przez władze atakami terrorystycznymi, zginęło co najmniej 20 osób, w tym funkcjonariusze służb bezpieczeństwa i duchowni, a ponad 40 zostało rannych. Rosyjskie służby nie potwierdziły, kim byli sprawcy. Część informacji wskazuje, że współpracowali z organizacjami powiązanymi z ISIS, w tym z Prowincją Kaukaską Państwa Islamskiego, ale wsparcie medialne dało również ISIS-K. Co ważne, rosyjskie władze budowały narrację o udziale zachodnich lub ukraińskich struktur wywiadowczych w inspirowaniu i wspieraniu ataków terrorystycznych.

Obecnie FSB publikuje „Jednolity federalny wykaz organizacji, w tym zagranicznych i międzynarodowych, uznanych zgodnie z ustawodawstwem Federacji Rosyjskiej za terrorystyczne”. Obejmuje on 70 podmiotów, w tym organizacje zagraniczne i międzynarodowe, a także struktury o charakterze lokalnym i regionalnym⁵⁵ działające na terytorium FR.

Mimo że Centralny Duchowny Zarząd Muzułmanów Rosji, jedna z ogólnorosyjskich struktur reprezentujących społeczność muzułmańskie

⁵³ E. Ferris, *How Russia's War in Ukraine...*

⁵⁴ M. Bartosiewicz, *Postępująca radykalizacja. Ataki terrorystyczne w Dagestanie...*

⁵⁵ *Единый федеральный список организаций...*

w FR, wielokrotnie publicznie potępiał terroryzm oraz ideologie ekstremistyczne jako sprzeczne z zasadami islamu, na terytorium FR dochodziło do aktów przemocy dokonywanych przez osoby odwołujące się do tej religii. W odpowiedzi na zamachy terrorystyczne w moskiewskim metrze w 2010 r. najwyższy mufti Rosji, Tałgat Tadžuddin, podkreślił, że społeczności muzułmańskie w Rosji jednoznacznie potępiają sprawców ataków terrorystycznych. Wskazał, że tego rodzaju czyny nie mają uzasadnienia religijnego i pozostają w sprzeczności z nauczaniem islamu⁵⁶. W kolejnych latach oficjalne instytucje muzułmańskie w FR podtrzymywały krytyczne stanowisko wobec terroryzmu i przemocy motywowanej religijnie, podkreślając, że działań terrorystycznych nie należy utożsamiać ze wspólnotami muzułmańskimi⁵⁷.

Ze względu na zaangażowanie FR na świecie należy także uwzględnić zagrożenia terrorystyczne w Afryce. Rosja deklaruje prowadzenie działań antyterrorystycznych przede wszystkim w państwach Sahelu, zwłaszcza w Mali, gdzie walka z terroryzmem stanowi jedno z głównych uzasadnień obecności rosyjskich sił i najemników. W praktyce aktywność ta służy jednak również realizacji celów politycznych, gospodarczych i wojskowych, w tym utrzymaniu wpływów oraz dostępu do surowców.

Rosyjska polityka antyterrorystyczna w Afryce jest przedstawiana jako odpowiedź na aktywność wielu ugrupowań dżihadystycznych działających na kontynencie. Należą do nich m.in. Grupa Wsparcia Islamu i Muzułmanów (Jama'at Nusrat al-Islam wal-Muslimin, JNIM), Państwo Islamskie w Sahelu (Islamic State Sahel Province, IS Sahel, ISSP), Prowincja Afryki Zachodniej Państwa Islamskiego (Islamic State West Africa Province, ISWAP), a także struktury Państwa Islamskiego w Mozambiku, określane również jako Ansar al-Sunna/Ahl al-Sunna. W kontekście Afryki Środkowej należy wskazać także Sojusznicze Siły Demokratyczne (Allied Democratic Forces, ADF) oraz struktury Państwa Islamskiego w Demokratycznej Republice Konga (ISIS-DRC), powiązane z Prowincją Afryki Centralnej Państwa Islamskiego (Islamic State Central Africa Province, ISCAP). W rosyjskiej narracji bezpieczeństwa są one przedstawiane jako zagrożenie uzasadniające

⁵⁶ *Peaceful Muslims have no relation to extremists – supreme mufti of Russia*, Pravmir, 30 XII 2013 r., <https://www.pravmir.com/peaceful-muslims-have-no-relation-to-extremists-supreme-mufti-of-russia/> [dostęp: 21 I 2026].

⁵⁷ B. Vitkine, *Russia faces wave of Islamophobia after Moscow attacks*, Le Monde, 30 III 2024 r., https://www.lemonde.fr/en/international/article/2024/03/30/russia-faces-wave-of-islamophobia-after-moscow-attacks_6666864_4.html [dostęp: 20 I 2026].

dalszą obecność wojskową i polityczną Moskwy w wybranych państwach afrykańskich⁵⁸.

Tym samym ze szczególną uwagą należy analizować działania podejmowane przez terrorystów przeciwko Rosji, zwłaszcza w Mali, Burkinie Faso, Nigrze, Mozambiku, Libii czy Republice Środkowoafrykańskiej. Jeżeli Rosja zdecydowałaby się na budowę swoich baz w którymkolwiek z tych państw oraz dalej rozwijała obecność Grupy Wagnera⁵⁹ lub Korpusu Afrykańskiego⁶⁰, a także próbowała utrzymać infrastrukturę w Syrii i rozpoczęła budowę kolejnych baz, to z pewnością będzie musiała zaangażować dodatkowe wojska i środki do zwalczania terroryzmu zarówno w Rosji i na Kaukazie, jak i w Afryce oraz na Bliskim Wschodzie. Będzie się to wiązało z dodatkowymi, nieplanowymi i znacznymi inwestycjami oraz przeniesieniem środków, np. z tych przeznaczonych na prowadzenie wojny w Ukrainie.

Kreml będzie musiał podjąć decyzję, jak ważne jest organizowanie nowych ośrodków wojskowych na kontynencie afrykańskim w kontekście kolejnych walk z terrorystami i utrudnień związanych z prowadzeniem operacji i szkoleń. Dotychczas rosyjscy najemnicy w Afryce – będący przecież najczęściej etatowymi żołnierzami rosyjskiej armii – przegrywają rywalizację z terrorystami i nie są w stanie się im przeciwstawić. Taki scenariusz zaistniał w Mozambiku, Republice Środkowoafrykańskiej, a teraz w Mali i Burkinie Faso. Rosja ze względu na trudności w walce z ugrupowaniami terrorystycznymi nie pozwoli sobie na budowę baz wojskowych, ponieważ stałyby się one automatycznie celami ugrupowań terrorystycznych, w tym dżihadystycznych. Dlatego bardzo ostrożnie i w ścisłej współpracy z rządami państw Afryki musi wybierać lokalizacje dla nowych inwestycji.

⁵⁸ A. Olech, *Grupa Wagnera w Afryce...*

⁵⁹ A. Olech, *Rosyjscy najemnicy – raport z działalności w Afryce*, Defence24, 8 IV 2024 r., <https://defence24.pl/geopolityka/rosyjscy-najemnicy-raport-z-dzialalnosci-w-afryce> [dostęp: 22 I 2026].

⁶⁰ Po śmierci Jewgienija Prigożyna w 2023 r. rosyjska obecność paramilitarna/najemników w Afryce była stopniowo reorganizowana i podporządkowywana strukturom kontrolowanym przez państwo, przede wszystkim Korpusowi Afrykańskiemu, powiązanemu z rosyjskim Ministerstwem Obrony. W praktyce oznaczało to częściowe przejęcie lub zastąpienie funkcji pełnionych wcześniej przez Grupę Wagnera w państwach takich jak Mali, Burkina Faso, Niger, Libia czy Republika Środkowoafrykańska. Zob. F. Bryjka, J. Czerep, *Korpus Afrykański – nowa odsłona starej obecności wojskowej Rosji w Afryce*, Polski Instytut Spraw Międzynarodowych, 29 V 2024 r., <https://www.pism.pl/publikacje/korpus-afrykanski-nowa-odslona-starej-obecnosci-wojskowej-rocji-w-afryce> [dostęp: 22 I 2026].

Federacja Rosyjska, w kontekście obecnych wyzwań dla bezpieczeństwa, dokonanych zamachów oraz wpływu terroryzmu na funkcjonowanie państwa, pozostaje wśród państw szczególnie narażonych na zagrożenie terrorystyczne. W raporcie *Global Terrorism Index 2025* Rosja została sklasyfikowana na 17. miejscu na świecie (przesunięcie o 20 pozycji w górę względem raportu z 2024 r.), a w raporcie *Global Terrorism Index 2026* – na 16. miejscu. Wzrost pozycji w rankingu w 2025 r. i utrzymanie w pierwszej dwudziestce w 2026 r. jest konsekwencją nasilonej aktywności terrorystycznej na terytorium państwa, w tym skutecznych zamachów o dużym oddziaływaniu społecznym. Rosja, prowadząc pełnoskalową operację wojskową przeciwko Ukrainie oraz angażując się militarnie w Afryce pod hasłem walki z terroryzmem, jednocześnie zwiększa swoją podatność na tego typu zagrożenia i staje się celem działań odwetowych ze strony ugrupowań terrorystycznych⁶¹.

Przedstawione w tabeli 1 zestawienie pokazuje, że wysoki poziom oddziaływania terroryzmu w latach 2020–2025 w państwach takich jak Somalia, Syria, Mali, Burkina Faso, Niger, Mozambik, Libia, Republika Środkowoafrykańska oraz Sudan utrzymuje się pomimo obecności lub zaangażowania FR. Jednocześnie w państwach współpracujących z Moskwą na poziomie polityczno-wojskowym, takich jak Egipt, Algieria, Serbia oraz Erytrea, nie obserwuje się wyraźnej poprawy sytuacji bezpieczeństwa. W praktyce oznacza to, że rosyjska aktywność – zarówno w państwach Sahelu, jak i w Libii, Republice Środkowoafrykańskiej, Mozambiku czy Sudanie – nie prowadzi do zwalczania terroryzmu, ale raczej wpisuje się w mechanizm utrzymywania środowiska niestabilności, umożliwiającego uzależnianie rządów lub junt od wsparcia zewnętrznego⁶². W efekcie Rosja funkcjonuje jako beneficjent długotrwałego chaosu, w którym terroryzm pozostaje elementem współpracy umożliwiającym i uzasadniającym jej dalszą obecność, a nie problemem, który Moskwa systemowo rozwiąże.

⁶¹ *Global Terrorism Index 2025...*; *Global Terrorism Index 2026...*

⁶² Wpisuje się to w szerszy model rosyjskich operacji bezpieczeństwa w Afryce, w którym Moskwa oferuje wsparcie wojskowe, ochronę reżimów oraz pomoc w operacjach przeciwko partyzantom, przedstawianych często jako walka z terroryzmem, w zamian za wynagrodzenie, dostęp do surowców lub wpływy polityczne. Zob. A. Arieff i in., *Russia's Security Operations in Africa*, Congressional Research Service, 8 IV 2026 r., <https://www.congress.gov/crs-product/IF12389> [dostęp: 12 IV 2026].

Tabela 1. Miejsce wybranych państw w latach 2021–2025 pod względem wpływu zagrożeń terrorystycznych na ich funkcjonowanie według Global Terrorism Index (1 – największy wpływ, 100 – najmniejszy wpływ).

Państwo	Miejsce na świecie				
	2021 r.	2022 r.	2023 r.	2024 r.	2025 r.
Egipt	15	16	20	29	32
Erytrea	93*	93*	89*	100*	100*
Mozambik	13	12	15	17	15
Republika Środkowoafrykańska	93*	55	59	71	76
Somalia	3	3	7	7	7
Sudan	86	93*	89*	100* (pochłonięty wojną)	100* (pochłonięty wojną)
Syria	5	5	5	3	6
Mali	7	4	3	4	5
Burkina Faso	4	2	1	1	2
Niger	8	10	10	5	3
Libia	26	32	39	53	59
Algieria	39	37	44	42	47
Serbia	93	93	89	82	66

* Ostatnie miejsce w raporcie

Źródło: opracowanie własne na podstawie: *Global Terrorism Index 2022*, <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf>, s. 8–9 [dostęp: 22 I 2026]; *Global Terrorism Index 2023*, <https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf>, s. 8–9 [dostęp: 22 I 2026]; *Global Terrorism Index 2024*, <https://www.economic-sandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf>, s. 6–7 [dostęp: 22 I 2026]; *Global Terrorism Index 2025*, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>, s. 6–7 [dostęp: 22 I 2026]; *Global Terrorism Index 2026*, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf>, s. 6–7 [dostęp: 13 IV 2026].

Zagrożenia terrorystyczne dla państw Organizacji Układu o Bezpieczeństwie Zbiorowym

Istnieje niebezpieczeństwo, że organizacje terrorystyczne z Kaukazu będą próbowały przeprowadzać ataki terrorystyczne nie tylko w Rosji, lecz także w państwach członkowskich OUBZ. Działania organizacji terrorystycznych mają również charakter kryminalny, ponieważ stale współpracują one z grupami przestępczymi. Aby pozyskać fundusze na prowadzenie swojej działalności, organizacje te angażują się m.in. w międzynarodowy handel narkotykami, porwania czy sprzedaż broni. Dlatego wykorzystanie terytoriów państw członkowskich OUBZ do prowadzenia nielegalnych działań, np. przez stworzenie szlaku handlowego Europa-Azja, stanowi ogromne zagrożenie dla bezpieczeństwa w regionie. Ponadto stałe prowadzenie działań w Syrii oraz nieustabilizowana sytuacja na południu kraju powodują, że FR musi monitorować regiony konfliktów zbrojnych i jednocześnie nie zaniedbywać bezpieczeństwa na granicach państw OUBZ.

Należy zwrócić uwagę na zagrożenie ze strony Afganistanu. Graniczący z nim Tadżykistan, państwo członkowskie OUBZ, zgłaszał niebezpieczeństwa związane z terroryzmem od strony południowej granicy. Wynikało to z niestabilnej sytuacji w Afganistanie, a także braku zabezpieczenia przejść granicznych. Trzeba dodać, że kraje Azji Centralnej po 2022 r. zdecydowanie zmieniły swoją politykę względem Kabulu. Z jednej strony dostrzegane są zagrożenia, ale z drugiej głównym czynnikiem wpływającym na rozwinięcie relacji Afganistanu z Kazachstanem, Uzbekistanem, Turkmenistanem, Tadżykistanem i Kirgistanem jest właśnie Rosja. Oprócz powyższego Moskwa dąży do nadzorowania współpracy oraz projektów realizowanych przez państwa Azji Centralnej, aby nie dopuścić do wzmocnienia ich niezależności, a jednocześnie przedstawia się jako gwarant bezpieczeństwa⁶³, choć mierzy się z największymi wyzwaniami w kontekście walki z terroryzmem (tabela 2).

⁶³ D. Zielińska, *Pragmatyzm ponad podziałami. Państwa Azji Centralnej wobec Afganistanu*, Ośrodek Studiów Wschodnich, 7 XI 2025 r., <https://www.osw.waw.pl/pl/publikacje/analizy/2025-11-07/pragmatyzm-ponad-podzialami-panstwa-azji-centralnej-wobec-afganistanu> [dostęp: 12 I 2026].

Tabela 2. Miejsce wybranych państw OUBZ oraz Afganistanu w latach 2021–2025 pod względem wpływu zagrożeń terrorystycznych na ich funkcjonowanie według Global Terrorism Index (1 – największy wpływ, 100 – najmniejszy wpływ).

Państwo	Miejsce na świecie				
	2021 r.	2022 r.	2023 r.	2024 r.	2025 r.
Armenia	93*	93*	76	79	81
Białoruś	93*	93*	89*	90	94
Kazachstan	93*	93*	89*	100*	100*
Kirgistan	93*	93*	89*	100*	100*
Rosja	44	45	35	16	17
Tadżykistan	47	50	69	70	41
Afganistan	1	1	6	9	11

* Ostatnie miejsce w raporcie

Źródło: opracowanie własne na podstawie: *Global Terrorism Index 2022*, <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf>, s. 8–9 [dostęp: 22 I 2026]; *Global Terrorism Index 2023*, <https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf>, s. 8–9 [dostęp: 22 I 2026]; *Global Terrorism Index 2024*, <https://www.economic-sandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf>, s. 6–7 [dostęp: 22 I 2026]; *Global Terrorism Index 2025*, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>, s. 6–7 [dostęp: 22 I 2026]; *Global Terrorism Index 2026*, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf>, s. 6–7 [dostęp: 13 IV 2026].

Potencjalne zagrożenie stwarzane przez samotnych sprawców (ang. *lone actors*) lub osoby samodzielnie deklarujące przynależność bądź lojalność wobec organizacji terrorystycznych⁶⁴ może stanowić współcześnie jedno z najpoważniejszych wyzwań dla rosyjskiego rządu oraz państw OUBZ. Jest to związane z masowymi wyjazdami obywateli rosyjskich na Bliski Wschód, ich indoktrynacją, a następnie powrotem do Rosji i podejmowaniem przez nich działań o charakterze terrorystycznym. Dokładna liczba takich osób nie jest znana, jednak zagrożenie związane z powracającymi bojownikami oraz osobami radykalizującymi się indywidualnie

⁶⁴ B.M. Jenkins, *Stray Dogs and Virtual Armies. Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11*, RAND, 31 VIII 2011 r., https://www.rand.org/pubs/occasional_papers/OP343.html [dostęp: 22 IV 2026].

było wielokrotnie wskazywane jako jeden z problemów rosyjskiego systemu bezpieczeństwa. Najważniejsze w tym aspekcie jest ustalenie, w jaki sposób (środki, narzędzia) oraz gdzie może zostać dokonany zamach. Jednym z głównych sposobów kontaktowania się terrorystów i omawiania poszczególnych celów są internetowe sieci społecznościowe oraz platformy do gier. Są w nich udostępniane materiały szkoleniowe, a także materiały zachęcające i mobilizujące do ataków. Dzięki temu indoktrynowani terroryści mają stały kontakt ze swoimi zwierzchnikami w Afryce lub na Bliskim Wschodzie. Z tego powodu weryfikacja wszystkich poszlak oraz źródeł wymaga stałego zaangażowania rosyjskich służb. Rosyjski rząd bierze również pod uwagę podobne zagrożenia wynikające z ciągłej migracji i rozwoju cyberterroryzmu.

Od lat rosyjskie służby bezpieczeństwa prowadzą działania profilaktyczne w największych miastach kraju, ukierunkowane przede wszystkim na ochronę transportu publicznego, miejsc o dużym natężeniu ruchu oraz imprez masowych. Wiąże się to z oddelegowaniem policji i żołnierzy do patrolowania ulic, a także z wydzielaniem stref wzmożonych kontroli, które umożliwią utrzymanie bezpieczeństwa w krytycznych rejonach miast. Ważnymi elementami są również kontrola na granicy oraz współpraca międzynarodowa. Dotychczasowe doświadczenia związane z atakami terrorystycznymi na terytorium Rosji oraz powtarzające się groźby terrorystów są podstawą do intensyfikacji ochrony. Jest to spowodowane głównie tym, że organizacje terrorystyczne, np. Al-Kaida i ISIS, wciąż wzywają w swoich oświadczeniach do przeprowadzania ataków na terytorium Rosji, nawołują do indywidualnych zamachów⁶⁵. W związku z powyższym niezbędne jest międzynarodowe zaangażowanie państw OUBZ, aby każdy z członków wdrożył podobne metody i środki w celu zwalczania terroryzmu. Wspólne inicjatywy militarne oraz reagowanie na zagrożenia powinny polegać na prowadzeniu symultanicznych działań i stosowaniu podobnej strategii w realizowaniu czynności antyterrorystycznych.

⁶⁵ A. Aji, B. Mroue, *Russian Embassy shelled in Syria as insurgents hit back*, Associated Press, 13 X 2015 r., <https://apnews.com/article/991656eab57d4aa79fbd5458af62b60e> [dostęp: 21 III 2026]; T. Joscelyn, *Head of al Qaeda's Syrian branch threatens Russia in audio message*, Long War Journal, 13 X 2015 r., <https://www.longwarjournal.org/archives/2015/10/head-of-al-qedas-syrian-branch-threatens-russia-in-audio-message.php> [dostęp: 21 III 2026]; *ISIS video threatens attacks in Russia, Moscow*, Ahram Online, 12 XI 2015 r., <https://english.ahram.org.eg/News/165409.aspx> [dostęp: 21 III 2026]; *Why is ISIS targeting Russia?*, Vision of Humanity, 25 III 2024 r., <https://www.visionofhumanity.org/why-is-isis-targeting-russia/> [dostęp: 21 III 2026].

Grupa Robocza ds. Walki z Terroryzmem i Ekstremizmem OUBZ

W ramach OUBZ została powołana specjalna struktura organizacyjna – Grupa Robocza ds. Walki z Terroryzmem i Ekstremizmem / Robocza Grupa Ekspertów ds. Walki z Terroryzmem i Ekstremizmem (ros. *Рабочая группа экспертов по вопросам борьбы с терроризмом и экстремизмом*) działająca pod auspicjami Komitetu Sekretarzy Rad Bezpieczeństwa OUBZ. Do jej podstawowych zadań należy koordynacja działań państw członkowskich w zakresie zwalczania terroryzmu i ekstremizmu, identyfikacja oraz analiza aktualnych i potencjalnych zagrożeń bezpieczeństwa, a także formułowanie rekomendacji dotyczących wspólnych działań prewencyjnych i operacyjnych. Grupa pełni funkcję ekspercko-doradczą, wspiera wypracowywanie wspólnej polityki bezpieczeństwa OUBZ, w tym przez inicjowanie harmonizacji rozwiązań prawnych oraz współpracy instytucjonalnej państw członkowskich w obszarze przeciwdziałania zagrożeniom terrorystycznym i ekstremistycznym⁶⁶.

Już w 2015 r. państwa OUBZ wskazywały na wzrost zagrożeń bezpieczeństwa związanych z aktywnością tzw. Państwa Islamskiego i Al-Kaidy, zwłaszcza w kontekście niestabilnej sytuacji w Afganistanie⁶⁷. Szczególne znaczenie przypisywano ochronie południowych granic państw członkowskich, przede wszystkim pogranicza tadżycko-afgańskiego, uznawanego za jeden z najbardziej wrażliwych odcinków pod względem zagrożeń terrorystycznych, ekstremistycznych i narkotykowych. Współpraca państw OUBZ w tym zakresie miała służyć wzmocnieniu bezpieczeństwa

⁶⁶ Меры по противодействию международному терроризму и экстремизму рассмотрены на заседании Комитета секретарей советов безопасности стран ОДКБ, Национальный правовой Интернет-портал Республики Беларусь (*Miery po protivodejstwiu miedzunarodnomu tierrorizmu i ekstriemizmu rassmotrieny na zasiedanii Komitietia siekrietaryj sowietow bezopasnosti stran ODKB, Nacyonalnyj prawowoj Intierniet-portal Riespubliki Bielarus*), 24 V 2018 r., <https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2018/may/28997/> [dostęp: 22 I 2026].

⁶⁷ Заявление глав государств-членов Организации Договора о Коллективной Безопасности о противодействии международному терроризму, 21 декабря 2015 года, г. Москва, Организация Договора о коллективной безопасности (*Zajawlenije glav gosudarstw-czlenow Organizacyi Dogowora o Kollektiwnoj Biezopasnosti o protivodejstwiu miedzunarodnomu tierrorizmu, 21 diekabria 2015 goda, g. Moskwa, Organizacyja Dogowora o kolektiwnoj biezopasnosti*), 21 XII 2015 r., https://odkb-csto.org/documents/documents/zayavlenie_glav_gosudarstv_chlenov_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_o_protivodeystv/?sphrase_id=66457 [dostęp: 10 III 2026].

granic, koordynacji działań oraz rozwojowi zdolności systemu kolektywnego bezpieczeństwa⁶⁸.

Według przedstawicieli OUBZ to właśnie terroryzm znacznie zwiększa prawdopodobieństwo wybuchu konfliktów w różnych regionach świata, utrudnia rozwijanie działalności wojskowej, w tym na granicach strefy odpowiedzialności OUBZ, przez co wymaga wszechstronnej i dogłębnej analizy oraz wspólnych wysiłków w celu przeciwdziałania zagrożeniom. Konsolidacja działań na rzecz bezpieczeństwa globalnego i regionalnego, w tym wymiana informacji, wspólne ćwiczenia oraz zbieżne priorytety w sferze bezpieczeństwa, stanowi jeden z priorytetów OUBZ⁶⁹.

Podczas regularnych spotkań Grupa Robocza ds. Walki z Terroryzmem i Ekstremizmem opracowuje propozycje usprawnienia współdziałania przy organizowaniu wspólnych operacji zwalczania terroryzmu i ekstremizmu. Na bieżąco aktualizuje listę organizacji uznawanych za terrorystyczne i ekstremistyczne w państwach członkowskich OUBZ. Prowadzi również działania mające na celu usprawnienie szkolenia operacyjnego i bojowego jednostek sił specjalnych OUBZ.

W latach 2024–2025 w ramach OUBZ utrzymano i rozwinięto dotychczasowe priorytety Grupy Roboczej, dostosowano je do zmieniającego się środowiska bezpieczeństwa. Szczególny nacisk położono na przeciwdziałanie działalności terrorystycznej i ekstremistycznej z wykorzystaniem dezinformacji oraz nowych technologii, w tym propagandy i rekrutacji prowadzonej w cyberprzestrzeni, zwalczanie transnarodowych grup terrorystycznych powiązanych z komórkami w Afganistanie, wzmocnienie ochrony granic zewnętrznych państw członkowskich (zwłaszcza na odcinku tadżycko-afgańskim), intensyfikację wspólnych ćwiczeń antyterrorystycznych oraz pogłębienie współpracy informacyjnej i prawnej między państwami OUBZ. Równolegle podkreślano znaczenie działań prewencyjnych, w tym

⁶⁸ В Астане состоялась сессия СКБ ОДКБ, Организация Договора о коллективной безопасности (W Astanie sostojałas' siessija SKB ODKB, Organizacyja Dogowora o kolektywnej biezopasnosti), 28 XI 2024 r., https://odkb-csto.org/news/news_odkb/v-astane-sostoyalas-sessiya-skb-odkb/ [dostęp: 22 I 2026].

⁶⁹ Генеральный секретарь ОДКБ Станислав Зась 4 сентября выступил на совместном заседании министров обороны СНГ, ШОС и ОДКБ, Организация Договора о коллективной безопасности (Gienieralnyj siekrietar' ODKB Stanisław Zas' 4 sientjabria wystąpił na sowmiestnom zasiedanii ministrow oborony SNG, SZOS i ODKB, Organizacyja Dogowora o kolektywnej biezopasnosti), https://odkb-csto.org/news/news_odkb/generalnyy-sekretar-odkb-stanislav-zas-4-sentyabrya-vystupil-na-sovmestnom-zasedanii-ministrov-oboro/?sphrase_id=66458 [dostęp: 11 III 2026].

programów edukacyjnych i przeciwdziałania radykalizacji, jako integralnego elementu regionalnego wzmacniania bezpieczeństwa zbiorowego⁷⁰.

Ważną kwestią w zwalczaniu terroryzmu w ramach OUBZ pozostaje rola Rosji, której strategia antyterrorystyczna opiera się na budowaniu współpracy zarówno z państwami członkowskimi organizacji, jak i z wybranymi partnerami zewnętrznymi. Federację Rosyjską w działaniach antyterrorystycznych wspierały m.in. ONZ oraz Chiny⁷¹. To oznacza, że Moskwa będzie dążyć do rozwijania współpracy antyterrorystycznej zarówno w ramach OUBZ, jak i poza nią. Może się też okazać, że po zakończeniu wojny w Ukrainie narracja walki z terroryzmem stanie się jednym z instrumentów umożliwiających Rosji częściowy powrót do aktywności na arenie międzynarodowej.

Jednocześnie priorytetem nadal są działania na rzecz ochrony interesów FR, które będą przez Kreml podejmowane jako działania kontrterrorystyczne, także w ramach szerszej jurysdykcji, tj. na terytorium wszystkich państw należących do OUBZ. To daje Rosji możliwość utrzymywania

⁷⁰ O. Keskin, *Лидеры стран ОДКБ выразили глубокую озабоченность эскалацией в зоне израильско-палестинского конфликта* (Lidery stran ODKB wyrazili głubokuju ozaboczennost' eskalacii w zonie izraillsko-palestinskogo konflikta), Anadolu Agency, 28 XI 2024 r., <https://www.aa.com.tr/ru/мир/лидеры-стран-одкб-выразили-глубокую-озабоченность-эскалацией-в-зоне-израильско-палестинского-конфликта/3407532> [dostęp: 22 I 2026]; *МИД стран-членов ОДКБ сделали заявление о положении в Афганистане* (MID stran-czlenow ODKB sdialali zajavlenije o položenii w Afganistanie), KazTAG, 28 XI 2024 r., <https://kaztag.kz/ru/news/mid-stran-chlenov-odkb-sdelali-zayavlenie-o-polozhenii-v-afganistanie> [dostęp: 22 I 2026]; *Касым-Жомарт Токаев принял участие в сессии Совета коллективной безопасности ОДКБ в узком составе*, Официальный сайт Президента Республики Казахстан (Kasym-Zomart Tokajew prinił uczaście w siessii Sowjeta kollektiwnoj biezopasnosti ODKB w uzkom sostawie, Oficjalnyj sajt Priezidenta Riestpubliki Kazachstan), 28 XI 2024 r., <https://www.akorda.kz/ru/kasym-zhomart-tokaev-prinyal-uchastie-v-sessii-soveta-kollektivnoy-bezopasnosti-odkb-v-uzkom-sostave-2810955> [dostęp: 22 I 2026]; *Организация Договора о коллективной безопасности (ОДКБ)*, Министерство иностранных дел Российской Федерации (Organizacyja Dogowora o kollektiwnoj biezopasnosti (ODKB), Ministierstwo inostrannykh diel Rossijskoj Fiedieracyi), https://mid.ru/ru/foreign_policy/integracii-struktury-prostranstva-sng/odkb/ [dostęp: 22 I 2026].

⁷¹ В Москве прошла Международная конференция «О роли и характере взаимодействия международных и региональных организаций в борьбе с международным терроризмом», организованная Секретариатом ОДКБ при участии ОБСЕ, Организация Договора о коллективной безопасности (W Moskwie proszła Mieždunarodnaja konfieriencyja «O roli i charakterie wzaimodiejstwija mieždunarodnykh i regionalnykh organizacij w bor'bie s mieždunarodnym tierrorizmom», organizowannaja Siekrietariatom ODKB pri uczaščii OBSIE, Organizacyja Dogowora o kollektiwnoj biezopasnosti), 30 X 2019 r., https://odkb-cs-to.org/news/news_odkb/v-moskve-proshla-mezhdunarodnaya-konferentsiya-o-rol-i-kharaktere-vzaimodeystviya-mezhdunarodnykh-i/?sphrase_id=66458 [dostęp: 16 I 2026].

wpływów w państwach członkowskich OUBZ za pośrednictwem współpracy służb bezpieczeństwa, wymiany informacji, szkoleń oraz wspólnych działań prowadzonych pod hasłem przeciwdziałania terroryzmowi. Walka z terroryzmem w rozumieniu Kremla, co wybrzmiewało w wielu oświadczeniach⁷², ma zupełnie inny wymiar niż z perspektywy Zachodu.

Istnieje wiele obszarów współpracy między OUBZ i ONZ dotyczących międzynarodowej walki z terroryzmem. Podstawą wspólnej aktywności są porozumienia zawarte między Sekretariatem OUBZ a wybranymi jednostkami organizacyjnymi ONZ, a przede wszystkim protokół ustaleń z Komitetem Antyterrorystycznym Rady Bezpieczeństwa ONZ (Counter-Terrorism Committee, CTC) i porozumienie o współpracy pomiędzy Sekretariatem OUBZ a Biurem Narodów Zjednoczonych ds. Zwalczania Terroryzmu (United Nations Office of Counter-Terrorism, UNOCT). Nie bez znaczenia jest również współpraca z partnerami – Wspólnotą Niepodległych Państw oraz Szanghajską Organizacją Współpracy. Należy zauważyć, że od powstania UNOCT w 2017 r. funkcję kierowniczą w Biurze sprawują przedstawiciele FR⁷³, co z perspektywy politycznej i instytucjonalnej mogło sprzyjać utrzymywaniu aktywnych relacji pomiędzy ONZ a OUBZ w zakresie przeciwdziałania terroryzmowi.

Wojna Rosji przeciw Ukrainie obnażyła słabość OUBZ jako mechanizmu bezpieczeństwa zbiorowego, czyli zamiast konsolidacji i współpracy pojawiło się zdystansowanie, a większość członków – poza Białorusią – unika otwartego poparcia Moskwy. Łączy to dwa sprzeczne podejścia z perspektywy Rosji. Większość członków nie chce legitymizować agresji ani ryzykować utraty zysków w relacjach z Zachodem. Jednocześnie Kreml wciąż próbuje rozwijać swoją politykę regionalną, odwołując się do narracji o stałych potrzebach walki z terroryzmem i utrzymywania operacji specjalnej na Ukrainie, co ma uzasadniać zdecydowane działania w regionie oraz budować wpływy w formatach takich jak OUBZ czy Szanghajska Organizacja Współpracy. Problem w tym, że bez zdolności Rosji do interwencji i narzucania rozstrzygnięć konfliktów (np. Armenia – Azerbejdżan lub Kirgistan – Tadżykistan) OUBZ jako organizacja staje się bezsilna, a państwa regionu coraz

⁷² *Putin Accuses Ukraine of Wanting Ceasefire to Rearm and Prepare 'Terrorist Attacks'*, The Moscow Times, 4 VI 2025 r., <https://www.themoscowtimes.com/2025/06/04/putin-say-sukraine-wants-ceasefire-to-rearm-and-prepare-terrorist-attacks-a89340> [dostęp: 22 I 2026].

⁷³ *Leadership*, United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en/leadership> [dostęp: 14 III 2026].

częściej poszukują alternatywnych projektów współpracy, m.in. z Chinami oraz Turcją, a także szukają kooperacji z Unią Europejską⁷⁴.

Podsumowanie

Władze w Moskwie budują wizerunek Rosji jako kluczowego aktora w międzynarodowej walce z terroryzmem, podkreślając potrzebę braku podwójnych standardów oraz budowy szerokiej koalicji przeciw terroryzmowi i ekstremizmowi. Traktują kontrterroryzm jako narzędzie polityki państwowej. Promują narrację, w której priorytetem jest eliminacja istniejących zagrożeń (a nie prewencja). Całkowicie kontrolują przestrzeń informacyjną i marginalizują znaczenie praw człowieka. To wszystko ma służyć legitymizacji represyjnych metod wewnątrz kraju oraz zwiększaniu wpływów za granicą⁷⁵. Jednocześnie nawiązanie współpracy z rządem Talibów czy instrumentalne używanie „antyterrorystycznych” operacji do działań w Syrii, Sahelu i Ukrainie podważa wiarygodność tej narracji. To pokazuje, że chodzi o pogłębienie rywalizacji z państwami zachodnimi nie tyle w zakresie samego zwalczania terroryzmu, ile w sposobie definiowania zagrożeń, budowania narracji o bezpieczeństwie oraz legitymizowania pod hasłem antyterroryzmu własnych działań. Rosja wykorzystuje tę kategorię jako instrument polityczny, przedstawia własne podejście jako alternatywę wobec modelu zachodniego i jako uzasadnienie dla działań podejmowanych zarówno wewnątrz kraju, jak i poza jego granicami.

Federacja Rosyjska od lat głosi opinię, że walka z terroryzmem powinna być prowadzona bez podwójnych standardów i często wykorzystuje ją do wykazywania błędów Zachodu⁷⁶. Władze Moskwy oskarżają

⁷⁴ P. Filkowska, *Pierwsze reakcje państw członkowskich Organizacji Układu o Bezpieczeństwie Zbiorowym na inwazję Federacji Rosyjskiej na Ukrainę, „Wschód Europy”* 2024, t. 10, nr 1. <https://doi.org/10.17951/we.2024.10.1.113-128>; A.M. Dyner, *OUBZ wobec wojny na Ukrainie i wyzwań regionalnych*, Polski Instytut Spraw Międzynarodowych, 27 III 2023 r., <https://www.pism.pl/publikacje/oubz-wobec-wojny-na-ukrainie-i-wyzwan-regionalnych> [dostęp: 12 I 2026].

⁷⁵ Zob. więcej: J. Hedenskog, *Russia and International Cooperation on Counter-Terrorism. From the Chechen Wars to the Syria Campaign*, FOI, March 2020, <https://foi.se/rest-api/report/FOI-R-4916--SE> [dostęp: 12 I 2026].

⁷⁶ *Russia accuses West of double standards regarding Daesh*, Middle East Monitor, 29 VIII 2019 r., <https://www.middleeastmonitor.com/20190829-russia-accuses-west-of-double-standards-regarding-daesh/> [dostęp: 12 I 2026].

państwa zachodnie o selektywne podejście do ISIS (m.in. w kontekście Afganistanu), sugerując, że część państw traktuje ugrupowania terrorystyczne instrumentalnie, jako narzędzie do realizacji własnych celów politycznych, zamiast konsekwentnie je zwalczać. Ponadto może w ten sposób obarczać inne podmioty odpowiedzialnością za zamachy⁷⁷.

Jednocześnie doświadczenia z Kaukazu Północnego oraz udział obywateli FR w konfliktach zagranicznych pokazują, że zagrożenie terrorystyczne ma charakter długofalowy i będzie się rozwijać. Szacuje się, że w szczytowym okresie działalności ISIS w walkach w Syrii i Iraku brało udział ok. 2300 obywateli Rosji oraz ok. 4700 bojowników z byłych republik radzieckich. Część z nich mogła wrócić do Rosji lub państw sąsiednich, wzmacniając lokalne sieci radykalne i terrorystyczne⁷⁸. Powracający terroryści dysponują doświadczeniem bojowym, kontaktami oraz funduszami, co ułatwia rekrutację kolejnych osób oraz realizowanie operacji, a to przekłada się na rosnący poziom zagrożenia terrorystycznego. Ze względu na rosyjski system kontrterrorystyczny, oparty głównie na działaniach służb specjalnych i operacjach wojskowych, kształtują się warunki sprzyjające dalszej radykalizacji i przemocy.

Agresja Rosji na Ukrainę w 2022 r. obnażyła poważne słabości rosyjskich służb specjalnych, które przez lata budowały wizerunek skutecznego aparatu bezpieczeństwa⁷⁹. Piony analityczne nie tylko nie korygowały politycznych założeń Kremla, lecz także mogły je wzmacniać, dostosowując ocenę sytuacji do oczekiwań decydentów skupionych wokół Władimira Putina. W efekcie rosyjskie służby, w tym FSB, zamiast pełnić funkcje gwarantujące bezpieczeństwo, stały się elementem systemu potwierdzającego błędne tezy, co miało bezpośrednie konsekwencje w działaniach prowadzonych w Ukrainie. Podobny charakter działań służb dotyczy walki z terroryzmem w FR.

Koncentracja rosyjskiego aparatu bezpieczeństwa na wojnie przeciwko Ukrainie oraz rywalizacji z Zachodem ograniczyła zdolności państwa do skutecznego wykrywania i neutralizacji części zagrożeń terrorystycznych.

⁷⁷ A. Koziół, *Walka z terroryzmem jako element propagandy wojennej Rosji*, Polski Instytut Spraw Międzynarodowych, 18 X 2024 r., <https://www.pism.pl/publikacje/walka-z-terroryzmem-jako-element-propagandy-wojennej-rosji> [dostęp: 19 III 2026].

⁷⁸ D. Nicolson, *Foreign Terrorist Fighters from the North Caucasus: Understanding Islamic State Influence in the Region*, „Connections: The Quarterly Journal” 2017, t. 16, nr 4. <https://doi.org/10.11610/Connections.16.4.04>.

⁷⁹ J.M. Raubo, *Ukraina 2022. Historyczna rysa na propagandowym obrazie rosyjskich służb specjalnych*, InfoSecurity24, 12 III 2022 r., <https://infosecurity24.pl/sluzby-specjalne/ukraina-2022-historyczna-rysa-na-propagandowym-obrazie-rosyjskich-sluzb-specjalnych> [dostęp: 19 I 2026].

Wydarzenia z 2024 r., w tym zamach w Crocus City Hall czy ataki w Dagestanie, pokazały nie tylko skalę wyzwań w domenie terroryzmu, lecz także luki w systemie reagowania, mimo wcześniejszych ostrzeżeń ze strony innych państw. Jednocześnie reakcja Kremla koncentrowała się w dużej mierze na zarządzaniu narracją, represjami, zwiększaniu uprawnień dla służb oraz przypisywaniu odpowiedzialności wybranym grupom terrorystycznym oraz przeciwnikom, czyli w szczególności Ukrainie i państwom Zachodu⁸⁰. To wszystko jest spójne z założeniami wykorzystywania terroryzmu jako elementu polityki wewnętrznej i narzędzia do mobilizacji społecznej na rzecz utrzymania kontroli, choć wciąż dochodzi do zamachów w Rosji i regionie.

Trzeba podkreślić, że to właśnie zamach na Crocus City Hall pokazał, że mimo wieloletnich działań pacyfikacyjnych Rosja nie wyeliminowała źródeł zagrożenia terrorystycznego, a przyczyna problemu nadal tkwi na Kaukazie Północnym. Choć w ostatnich latach skala ataków wewnątrz kraju była mała, to radykalizacja w republikach takich jak Czeczenia, Dagestan i Inguszetia pozostaje trwałym zjawiskiem, szczególnie wśród młodego pokolenia. Struktury dżihadystyczne – zarówno powiązane z Państwem Islamskim, jak i z reaktywującym się Emiratem Kaukaskim – koncentrują się na działaniach przeciwko służbom czy instytucjom państwowym⁸¹. Coraz większe znaczenie ma wymiar międzynarodowy, gdzie zamachów mogą dokonywać osoby z Rosji i z całego regionu Kaukazu.

Omówione uwarunkowania i zagrożenia nie wskazują na znaczny wzrost skali terroryzmu w FR, ale pokazują istnienie trwałych czynników, które nie mogą zostać w pełni wyeliminowane, nawet przez autorytarny aparat rosyjski. Lekceważenie wczesnych sygnałów radykalizacji oraz utrzymujący się i postępujący terror oraz uprzywilejowanie rosyjskich służb, zarówno w wymiarze lokalnym, jak i regionalnym, doprowadziły do błędnych ocen zagrożenia i opóźnionej reakcji państwa. Doświadczenia związane z niedoszacowaniem wcześniejszych ataków w Rosji, w tym wpływu czeczeńskiego, działalności Al-Kaidy oraz ISIS⁸², wskazują,

⁸⁰ A. Koziół, *Walka z terroryzmem jako element propagandy wojennej Rosji...*; P. Sonne, E. Schmitt, M. Schwirtz, *Why Russia's Vast Security Services Fell Short on Deadly Attack*, The New York Times, 28 III 2024 r., <https://www.nytimes.com/2024/03/28/world/europe/russia-concert-attack-security-failures.html> [dostęp: 21 III 2026].

⁸¹ *IntelBrief: Radicalization and Extremism in Russia's...*

⁸² L. Aron, *The Expansion of Russia's Radical Islamism Outside the North Caucasus*, American Enterprise Institute, 30 IX 2015 r., <https://www.aei.org/research-products/testimony/the-expansion-of-russias-radical-islamism-outside-the-north-caucasus/> [dostęp: 22 I 2026].

że Rosja nie jest w stanie, i nigdy nie będzie, w pełni zwalczyć zagrożenia terrorystycznego, zarówno w kraju, jak i za granicą.

Bibliografia

Beslin J., Ignjatijevic M., *Balkan foreign fighters: from Syria to Ukraine*, „Brief” 2017, nr 20, s. 1–4.

Filkowska P., *Pierwsze reakcje państw członkowskich Organizacji Układu o Bezpieczeństwie Zbiorowym na inwazję Federacji Rosyjskiej na Ukrainę*, „Wschód Europy” 2024, t. 10, nr 1. <https://doi.org/10.17951/we.2024.10.1.113-128>.

Grabowski T., *Terroryzm północnokaukaski: przejawy zjawiska*, „Res Polticae” 2014, t. VI, s. 59–78. <http://dx.doi.org/10.16926/rp.2014.06.04>.

Grabowski T.W., *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku*, Kraków 2017.

Liedel K., Piasecka P., *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej*, Warszawa 2008.

Nicolson D., *Foreign Terrorist Fighters from the North Caucasus: Understanding Islamic State Influence in the Region*, „Connections: The Quarterly Journal” 2017, t. 16, nr 4. <https://doi.org/10.11610/Connections.16.4.04>.

Oldberg I., *The War on Terrorism in Russian Foreign Policy*, FOI – Swedish Defence Research Agency, Defence Analysis, Stockholm 2006.

Olech A., *Grupa Wagnera w Afryce. Pozorowana walka rosyjskich najemników z terroryzmem*, „Terroryzm – studia, analizy, prewencja” 2024, nr 5, s. 53–89. <https://doi.org/10.4467/27204383TER.24.002.19390>.

Olech A., *Terroryzm – określenie definicji zjawiska w polskich i zagranicznych badaniach*, „Studia Bezpieczeństwa Narodowego” 2020, t. 18, nr 2, s. 121–138. <https://doi.org/10.37055/sbn/145302>.

Olech A.K., *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku*, „Nowa Polityka Wschodnia” 2019, nr 4, s. 110–115. <https://doi.org/10.15804/NPW20192306>.

Schmid A.P., Jongman A.J., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Amsterdam 1988.

Sinai J., *The Terrorist Threats Against Russia and its Counterterrorism Response Measures*, „Connections: The Quarterly Journal” 2015, t. 14, nr 4, s. 95–101. <http://dx.doi.org/10.11610/Connections.14.4.08>.

Stempień M.S., *The evolution of terrorism in Russia in the years 2015–2022. Quantitative analysis of the phenomenon*, „Przegląd Wschodnioeuropejski” 2023, nr 14, s. 185–199. <https://doi.org/10.31648/pw.9711>.

The North Caucasus: The Challenges of Integration (II), Islam, the Insurgency and Counter-Insurgency, Europe Report N°221, 19 X 2012 r.

Weinberg L., Pedahzur A., Hirsch-Hoefler S., *The Challenges of Conceptualizing Terrorism*, „Terrorism and Political Violence” 2004, t. 16, nr 4, s. 777–794. <https://doi.org/10.1080/095465590899768>.

Źródła internetowe

Aji A., Mroue B., *Russian Embassy shelled in Syria as insurgents hit back*, Associated Press, 13 X 2015 r., <https://apnews.com/article/991656eab57d4aa79fbd5458af62b60e> [dostęp: 21 III 2026].

Al-Qaeda in Syria calls for revenge attacks on Russia, The Washington Post, 13 X 2015 r., https://www.washingtonpost.com/world/middle_east/al-qaeda-in-syria-calls-for-revenge-attacks-on-russia/2015/10/13/b7f7dfdf-a0a4-451d-bd2e-180f2f4882f5_story.html [dostęp: 16 V 2026].

Arief A., Blanchard L.P., Collins S.R., Husted T.F., *Russia's Security Operations in Africa*, Congressional Research Service, 8 IV 2026 r., <https://www.congress.gov/crs-product/IF12389> [dostęp: 12 IV 2026].

Aron L., *The Expansion of Russia's Radical Islamism Outside the North Caucasus*, American Enterprise Institute, 30 IX 2015 r., <https://www.aei.org/research-products/testimony/the-expansion-of-russias-radical-islamism-outside-the-north-caucasus/> [dostęp: 22 I 2026].

Bartosiewicz M., *Postępująca radykalizacja. Ataki terrorystyczne w Dagestanie*, Ośrodek Studiów Wschodnich, 25 VI 2024 r., <https://www.oswawaw.pl/pl/publikacje/analizy/2024-06-25/postepujaca-radykalizacja-ataki-terrorystyczne-w-dagestanie> [dostęp: 26 X 2025].

Bhattacharji P., *Chechen Terrorism (Russia, Chechnya, Separatist)*, Council on Foreign Relations, 8 IV 2010 r., <https://www.cfr.org/backgrounders/chechen-terrorism-russia-chechnya-separatist> [dostęp: 20 III 2026].

Borshchevskaya A., *Russian Officials Inadvertently Aid Radical Islamists in Russia*, The Washington Institute for Near East Policy, 31 XII 2015 r., <https://www.washingtoninstitute.org/policy-analysis/russian-officials-inadvertently-aid-radical-islamists-russia> [dostęp: 22 I 2026].

Bryjka F., Czerep J., *Korpus Afrykański – nowa odsłona starej obecności wojskowej Rosji w Afryce*, Polski Instytut Spraw Międzynarodowych, 29 V 2024 r., <https://www.pism.pl/publikacje/korpus-afrykanski-nowa-odslona-starej-obecnosci-wojskowej-rosji-w-afryce> [dostęp: 22 I 2026].

Caucasus Emirate, START – National Consortium for the Study of Terrorism and Responses to Terrorism, January 2015, <https://www.start.umd.edu/baad/narratives/caucasus-emirate.html> [dostęp: 19 I 2026].

Costa-Roberts D., *Questions swirl over Russian plane crash in Egypt that killed 224*, PBS News, 1 XI 2015 r., <https://www.pbs.org/newshour/world/details-emerge-case-downed-russian-jet> [dostęp: 20 I 2026].

Database Scope, RAND National Security Research Division, <https://www.rand.org/nsrd/projects/terrorism-incidents/about/definitions.html> [dostęp: 20 III 2026].

Dyner A.M., *OUBZ wobec wojny na Ukrainie i wyzwań regionalnych*, Polski Instytut Spraw Międzynarodowych, 27 III 2023 r., <https://www.pism.pl/publikacje/oubz-wobec-wojny-na-ukrainie-i-wyzwan-regionalnych> [dostęp: 12 I 2026].

Dyner A.M., *Zamach w Moskwie*, Polski Instytut Spraw Międzynarodowych, 25 III 2024 r., <https://www.pism.pl/publikacje/zamach-w-moskwie> [dostęp: 19 I 2026].

Falkowski M., *Państwo Islamskie na Kaukazie – cui bono?*, Ośrodek Studiów Wschodnich, 14 I 2015 r., <https://www.osw.waw.pl/pl/publikacje/analizy/2015-01-14/panstwo-islamskie-na-kaukazie-cui-bono> [dostęp: 12 III 2026].

Faulconbridge G., *Russian security failure? Kremlin says no country is immune to terrorism*, Reuters, 25 III 2024 r., <https://www.reuters.com/world/europe/russian-security-failure-kremlin-says-no-country-is-immune-terrorism-2024-03-25/> [dostęp: 20 III 2026].

Ferris E., *How Russia's War in Ukraine is Creating Domestic Security Gaps*, Royal United Services Institute, 23 IX 2025 r., <https://www.rusi.org/explore-our-research/publications/insights-papers/how-russias-war-ukraine-creating-domestic-security-gaps> [dostęp: 21 III 2026].

Flanagan J., *Bloodshed and retreat from Mozambique for Putin's private army the Wagner Group*, The Times, 25 XI 2019 r., <https://www.thetimes.com/uk/politics/article/bloodshed-and-retreat-from-mozambique-for-putin-s-private-army-the-wagner-group-696tnpzqh> [dostęp: 19 I 2026].

Foreign Fighters. An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq, December 2015, https://thesoufancenter.org/wp-content/uploads/2017/05/TSG_ForeignFightersUpdate_format-for-print-120915-REBRAND-031317.pdf [dostęp: 21 I 2026].

Gliniasty J. de, *Moscow Attack: Russia Confronts Islamist Terrorism*, Institut de Relations Internationales et Stratégiques, 26 III 2024 r., <https://www.iris-france.org/en/184928-moscow-attack-russia-confronts-islamist-terrorism/> [dostęp: 21 III 2026].

Global Terrorism Index 2022, <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf> [dostęp: 22 I 2026].

Global Terrorism Index 2023, <https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf> [dostęp: 22 I 2026].

Global Terrorism Index 2024, <https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf> [dostęp: 22 I 2026].

Global Terrorism Index 2025, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf> [dostęp: 22 I 2026].

Global Terrorism Index 2026, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf> [dostęp: 13 IV 2026].

Gold Z., *Wilayat Sinai Risks Backlash After Metrojet Bombing*, <https://ctc westpoint.edu/wp-content/uploads/2015/12/CTCSentinel-Vol8Iss118.pdf> [dostęp: 19 I 2026].

Hanoush F., *Fighters from the Caucasus Join ISIS to Fight Russia*, Atlantic Council, 14 IX 2016 r., <https://www.atlanticcouncil.org/blogs/syriasource/fighters-from-the-caucasus-join-isis-to-fight-russia/> [dostęp: 21 III 2026].

Hedenskog J., *Russia and International Cooperation on Counter-Terrorism. From the Chechen Wars to the Syria Campaign*, FOI, March 2020, <https://foi.se/rest-api/report/FOI-R--4916--SE> [dostęp: 12 I 2026].

Hird K., Mappes G., Wolkov N., Harward Ch., Evans A., Kagan F.W., *Russian Offensive Campaign Assessment, March 25, 2024*, Critical Threats, 25 III 2024 r., <https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-march-25-2024> [dostęp: 20 III 2026].

IntelBrief: Radicalization and Extremism in Russia's North Caucasus Region, The Soufan Center, 12 IV 2024 r., <https://thesoufancenter.org/intelbrief-2024-april-12/> [dostęp: 26 X 2025].

ISIS video threatens attacks in Russia, Moscow, Ahram Online, 12 XI 2015 r., <https://english.ahram.org.eg/News/165409.aspx> [dostęp: 21 III 2026].

Jenkins B.M., *Stray Dogs and Virtual Armies. Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11*, RAND, 31 VIII 2011 r., https://www.rand.org/pubs/occasional_papers/OP343.html [dostęp: 22 IV 2026].

Johns M., *Terrorism and the North Caucasus: An Overview*, „START Background Report”, National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, April 2013, https://www.academia.edu/8490735/Terrorism_and_the_North_Caucasus_An_Overview [dostęp: 16 VI 2026].

Joscelyn T., *Head of al Qaeda's Syrian branch threatens Russia in audio message*, Long War Journal, 13 X 2015 r., <https://www.longwarjournal.org/archives/2015/10/head-of-al-qaedas-syrian-branch-threatens-russia-in-audio-message.php> [dostęp: 21 III 2026].

Katz M.N., *No, Putin, the ISIS-K attack in Moscow wasn't about Ukraine*, Atlantic Council, 29 III 2024 r., <https://www.atlanticcouncil.org/blogs/menasource/isis-k-putin-moscow-al-qaeda/> [dostęp: 20 I 2026].

Kozioł A., *Walka z terroryzmem jako element propagandy wojennej Rosji*, Polski Instytut Spraw Międzynarodowych, 18 X 2024 r., <https://www.pism.pl/publikacje/walka-z-terroryzmem-jako-element-propagandy-wojennej-rosji> [dostęp: 19 III 2026].

Leadership, United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en/leadership> [dostęp: 14 III 2026].

McFaul M., *U.S. Russia Relations After September 11, 2001*, Carnegie Endowment for International Peace, 24 X 2001 r., <https://carnegieendowment.org/posts/2001/10/us-russia-relations-after-september-11-2001?lang=en> [dostęp: 21 III 2026].

National Antiterrorism Committee: goals and objectives, National Antiterrorism Committee, <https://en.nac.gov.ru/home> [dostęp: 21 III 2026].

Olech A., *Rosyjscy najemnicy – raport z działalności w Afryce*, Defence24, 8 IV 2024 r., <https://defence24.pl/geopolityka/rosyjscy-najemnicy-raport-z-dzialalnosci-w-afryce> [dostęp: 22 I 2026].

On the Terrorist Attack at the Crocus City Hall in Moscow, U.S. Mission to the Organization for Security and Cooperation in Europe, 11 IV 2024 r., <https://osce.usmission.gov/on-the-terrorist-attack-at-the-crocus-city-hall-in-moscow/> [dostęp: 20 III 2026].

Paraszczyk J., *IS's North Caucasus Affiliate Calls for Recruits to Join It in Daghestan*, Radio Free Europe/Radio Liberty, 3 X 2015 r., <https://www.rferl.org/a/islamic-state-north-caucasus-affiliate-call-for-recruits-daghestan/27285024.html> [dostęp: 16 V 2026].

Peaceful Muslims have no relation to extremists – supreme mufti of Russia, Pravmir, 30 XII 2013 r., <https://www.pravmir.com/peaceful-muslims-have-no-relation-to-extremists-supreme-mufti-of-russia/> [dostęp: 21 I 2026].

Putin Accuses Ukraine of Wanting Ceasefire to Rearm and Prepare 'Terrorist Attacks', The Moscow Times, 4 VI 2025 r., <https://www.themoscowtimes.com/2025/06/04/putin-says-ukraine-wants-ceasefire-to-rearm-and-prepare-terrorist-attacks-a89340> [dostęp: 22 I 2026].

Raubo J.M., *Ukraina 2022. Historyczna rysa na propagandowym obrazie rosyjskich służb specjalnych*, InfoSecurity24, 12 III 2022 r., <https://infosecurity24.pl/sluzby-specjalne/ukraina-2022-historyczna-rysa-na-propagandowym-obrazie-rosyjskich-sluzb-specjalnych> [dostęp: 19 I 2026].

Rekawek K., Lanchès J., Zotova M., *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 VI 2026].

Roggio B., *Doku Umarov declares Islamic Caucasus Emirate*, Long War Journal, 26 XI 2007 r., https://www.longwarjournal.org/archives/2007/11/doku_umarov_declares.php [dostęp: 19 I 2026].

Russia accuses West of double standards regarding Daesh, Middle East Monitor, 29 VIII 2019 r., <https://www.middleeastmonitor.com/20190829-russia-accuses-west-of-double-standards-regarding-daesh/> [dostęp: 12 I 2026].

Schmid A.P., *Defining Terrorism*, https://icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf [dostęp: 20 III 2026].

Sonne P., Schmitt E., Schwirtz M., *Why Russia's Vast Security Services Fell Short on Deadly Attack*, The New York Times, 28 III 2024 r., <https://www.nytimes.com/2024/03/28/world/europe/russia-concert-attack-security-failures.html> [dostęp: 21 III 2026].

Strachota K., *Państwo Islamskie Chorasanu – nowa odsłona światowego dżihadu*, 29 III 2024 r., Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-03-29/panstwo-islamskie-chorasanu-nowa-odslona-swiatowego-dzihadu> [dostęp: 20 I 2026].

Syria crisis: Rockets hit Russian embassy compound in Damascus, reports say, ABC News, 13 X 2015 r., <https://www.abc.net.au/news/2015-10-13/rockets-hit-russian-embassy-compound-in-damascus-reports/6851968> [dostęp: 16 V 2026].

Ter M., *The Caucasus Emirate, the Other Russian Front*, https://www.cidob.org/sites/default/files/2024-07/NOTES%20129_TER_ANG.pdf [dostęp: 16 VI 2026].

The Deadliest Attacks In Russia, Radio Free Europe/Radio Liberty, <https://www.rferl.org/a/russia-timeline-terror-attacks/28410225.html> [dostęp: 19 I 2026].

The North Caucasus Insurgency and Syria: An Exported Jihad?, International Crisis Group, 16 III 2016 r., <https://www.crisisgroup.org/europe-central-asia/russia-internal-syria/238-north-caucasus-insurgency-and-syria-exported-jihad> [dostęp: 19 I 2026].

Vatchagaev M., *Caucasus Emirate and Islamic State Split Slows Militant Activities in North Caucasus*, Jamestown, 14 II 2015 r., <https://jamestown.org/program/caucasus-emirate-and-islamic-state-split-slows-militant-activities-in-north-caucasus-2/> [dostęp: 20 I 2026].

Vitkine B., *Russia faces wave of Islamophobia after Moscow attacks*, Le Monde, 30 III 2024 r., https://www.lemonde.fr/en/international/article/2024/03/30/russia-faces-wave-of-islamophobia-after-moscow-attacks_6666864_4.html [dostęp: 20 I 2026].

Why is ISIS targeting Russia?, Vision of Humanity, 25 III 2024 r., <https://www.vision-ofhumanity.org/why-is-isis-targeting-russia/> [dostęp: 21 III 2026].

Wilk A., Konończuk W., *Wojna ukraińsko-rosyjska pod szyldem operacji antyterrorystycznej*, Ośrodek Studiów Wschodnich, 6 VIII 2014 r., <https://www.osw.waw.pl/pl/publikacje/analizy/2014-08-06/wojna-ukrainsko-rosyjska-pod-szyldem-operacji-antyterrorystycznej> [dostęp: 19 I 2026].

Youngman M., Moore C., *Guide: The Caucasus Emirate*, Radicalisation Research, 9 XI 2017 r., <https://radicalisationresearch.org/research/youngman-guide-caucasus-emirate/> [dostęp: 12 III 2026].

Zielińska D., *Pragmatyzm ponad podziałami. Państwa Azji Centralnej wobec Afganistanu*, Ośrodek Studiów Wschodnich, 7 XI 2025 r., <https://www.osw.waw.pl/pl/publikacje/analizy/2025-11-07/pragmatyzm-ponad-podzialami-panstwa-azji-centralnej-wobec-afganistanu> [dostęp: 12 I 2026].

Rosyjskie i białoruskie źródła internetowe

Keskin O., *Лидеры стран ОДКБ выразили глубокую озабоченность эскалацией в зоне израильско-палестинского конфликта* (*Lidery stran ODKB wyrazili glubokuju ozaboczennost' eskalacyye w zonie izrailsko-palestinskogo konflikta*), Anadolu Agency, 28 XI 2024 r., <https://www.aa.com.tr/ru/мир/лидеры-стран-одкб-выразили-глубокую-озабоченность-эскалацией-в-зоне-израильско-палестинского-конflikta/3407532> [dostęp: 22 I 2026].

В Астане состоялась сессия СКБ ОДКБ, Организация Договора о коллективной безопасности (*W Astanie sostojałas' siessija SKB ODKB*, Organizacja Dogowora o kollektiwnoj biezopasnosti), 28 XI 2024 r., https://odkb-csto.org/news/news_odkb/v-astane-sostoyalas-sessiya-skb-odkb/ [dostęp: 22 I 2026].

В Москве прошла Международная конференция «О роли и характере взаимодействия международных и региональных организаций в борьбе с международным терроризмом», организованная Секретариатом ОДКБ при участии ОБСЕ, Организация Договора о коллективной безопасности (*W Moskwie proszła Mieždunarodnaja konfierencyja «O roli i charakterie wzaimodiejstwiya mieždunarodnykh i regionalnykh organizacyj w bor'bie s mieždunarodnym tierrorizmom»*, organizowannaja Siekrietariatom ODKB pri uczastii OBSIE, Organizacja Dogowora o kollektiwnoj biezopasnosti), 30 X 2019 r., https://odkb-csto.org/news/news_odkb/v-moskve-proshla-mezhdunarodnaya-konferentsiya-o-rol-i-kharaktere-vzaimodeystviya-mezhdunarodnykh-i/?sphrase_id=66458 [dostęp: 16 I 2026].

Генеральный секретарь ОДКБ Станислав Зась 4 сентября выступил на совместном заседании министров обороны СНГ, ШОС и ОДКБ, Организация Договора о коллективной безопасности (*Gienieralnyj siekrietar' ODKB Stanisław Zas' 4 sentiabria wystupił na sowmiesnom zasiedanii ministrow oborony SNG, SZOS i ODKB*, Organizacja Dogowora o kollektiwnoj biezopasnosti), https://odkb-csto.org/news/news_odkb/generalnyy-sekretar-odkb-stanislav-zas-4-sentyabrya-vystupil-na-sovmestnom-zasedanii-ministrov-oboro-/?sphrase_id=66458 [dostęp: 11 III 2026].

Заявление глав государств-членов Организации Договора о Коллективной Безопасности о противодействии международному терроризму, 21 декабря 2015 года, г. Москва, Организация Договора о коллективной безопасности (Zajawlenije gław gosudarstw-czlenow Organizacyi Dogowora o Kollektivnoy Biezopasnosti o protivodejstwiu mieżdunarodnomu tierrorizmu, 21 diekabria 2015 goda, g. Moskwa, Organizacyja Dogowora o kolektivnoy biezopasnosti), 21 XII 2015 r., https://odkb-csto.org/documents/documents/zayavlenie_glav_gosudarstv_chlenov_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_o_protivodeystv/?sphrase_id=66457 [dostęp: 10 III 2026].

Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими (на 4 апреля 2026 г.), Федеральная служба безопасности Российской Федерации (Jedynyj fiedieralnyj spisok organizacyj, w tom czisle inostrannyh i mieżdunarodnyh organizacyj, priznannyh w sootwietstwiu s zakonodatelstwom Rossijskoj Fiedieracyi tierroristycznymi (na 4 apriela 2026 g.), Fiedieralnaja służba biezopasnosti Rossijskoj Fiedieracyi), <http://www.fsb.ru/fsb/npd/terror.htm> [dostęp: 20 IV 2026].

Касым-Жомарт Токаев принял участие в сессии Совета коллективной безопасности ОДКБ в узком составе, Официальный сайт Президента Республики Казахстан (Kasym-Žomart Tokajew priniął uczastije w siessii Sowieta kolektivnoy biezopasnosti ODKB w uzkom sostawie, Oficjalnyj sajł Priezidenta Riespubliki Kazachstan), 28 XI 2024 r., <https://www.akorda.kz/ru/kasym-zhomart-tokaev-prinyal-uchastie-v-sessii-soveta-kollektivnoy-bezopasnosti-odkb-v-uzkom-sostave-2810955> [dostęp: 22 I 2026].

Меры по противодействию международному терроризму и экстремизму рассмотрены на заседании Комитета секретарей советов безопасности стран ОДКБ, Национальный правовой Интернет-портал Республики Беларусь (Miery po protivodejstwiu mieżdunarodnomu tierrorizmu i ekstremizmu rassmotrieny na zasiedanii Komiteta siekrietariej sowietow biezopasnosti stran ODKB, Nacyonalnyj prawowoj Intierniet-portał Riespubliki Biełarus'), 24 V 2018 r., <https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2018/may/28997/> [dostęp: 22 I 2026].

МИД стран-членов ОДКБ сделали заявление о положении в Афганистане (MID stran-czlenow ODKB sdělali zajawlenije o położenii w Afganistanie), KazTAG, 28 XI 2024 r., <https://kaztag.kz/ru/news/mid-stran-chlenov-odkb-sdelali-zayavlenie-o-polozhenii-v-afganistane> [dostęp: 22 I 2026].

Организация Договора о коллективной безопасности (ОДКБ), Министерство иностранных дел Российской Федерации (*Organizacyja Dogowora o kollektiwnoj biezopasnosti (ODKB)*, Ministerstwo inostrannyh dzieł Rossijskoj Fiedieracyi), https://mid.ru/ru/foreign_policy/integracionnye-struktury-prostranstva-sng/odkb/ [dostęp: 22 I 2026].

Перечень организаций, признанных в соответствии с законодательством Российской Федерации экстремистскими, Министерство юстиции Российской Федерации (*Pierieczien' organizacyj, priznannyh w sootwietstwie s zakonodatielstwom Rossijskoj Fiedieracyi ekstremists*, Министерство юстиции Российской Федерации), <https://minjust.gov.ru/ru/documents/7822/> [dostęp: 20 IV 2026].

Rosyjskie akty prawne

Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 205. Террористический акт (*Ugołownyj Kodeks Rossijskoj Fiedieracyi ot 13.06.1996 No 63-FZ. Stat'ja 205. Tierroristiczeskij akt*), https://www.consultant.ru/document/cons_doc_LAW_10699/43942021d9206af7a0c78b6f65ba3665db940264/ [dostęp: 20 III 2026].

Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 282.2. Организация деятельности экстремистской организации и участие в деятельности такой организации (*Ugołownyj Kodeks Rossijskoj Fiedieracyi ot 13.06.1996 No 63-FZ. Stat'ja 282.2. Organizacyja diejatielnosti ekstremistskoj organizacyi i uczastije w diejatielnosti takoj organizacyi*).

Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 361. Акт международного терроризма (*Ugołownyj Kodeks Rossijskoj Fiedieracyi ot 13.06.1996. Stat'ja 361. Akt mieždunarodnogo tierrorizma*), https://www.consultant.ru/document/cons_doc_LAW_10699/0994b72ccab34fae773ced2c837691518a3e3dca/ [dostęp: 20 III 2026].

Федеральный закон Российской Федерации от 06.03.2006 No 35-ФЗ „О противодействии терроризму”. Статья 3. Основные понятия (*Fiedieralnyj zakon Rossijskoj Fiedieracyi ot 06.03.2006 No 35-FZ „O protiwodiejstwii tierrorizmu”*. Stat'ja 3. Osnownyje poniatija), https://www.consultant.ru/document/cons_doc_LAW_58840/4fdc493704d123d418c32ed33872ca5b3fb16936/ [dostęp: 20 III 2026].

Szef Działu Współpracy Międzynarodowej Defence24. Wykładowca na uczelniach polskich i zagranicznych, współpracownik NATO, analityk i publicysta. Były zastępca dyrektora Departamentu Afryki i Bliskiego Wschodu Ministerstwa Spraw Zagranicznych. Absolwent Europejskiej Akademii Dyplomacji oraz Akademii Sztuki Wojennej. Główne zainteresowania badawcze: relacje francusko-rosyjskie, wyzwania w Afryce i polityka bezpieczeństwa NATO.

Kontakt: a.olech@defence24.pl



Ochrona przestrzeni publicznych i wydarzeń publicznych przed atakami z użyciem pojazdu – znaczenie systemów HVM i barier pojazdowych VSB w kontekście rekomendacji dla Polski

Protecting public spaces and public events against vehicle-borne attacks – the importance of VSB and HVM systems in the context of recommendations for Poland

JAROSŁAW JAŻWIŃSKI

Autor niezależny



<https://orcid.org/0000-0001-7845-5492>

Abstrakt

Celem artykułu jest omówienie systemów HVM (od ang. *hostile vehicle mitigation*) i barier pojazdowych VSB (od ang. *vehicle security barriers*) jako elementu ochrony przestrzeni publicznych i wydarzeń publicznych przed atakami z użyciem pojazdu. Uporządkowano aparat pojęciowy związany z systemami HVM i barierami pojazdowymi VSB, przedstawiono aktualne standardy badawcze dotyczące urządzeń zabezpieczających. Omówiono charakter tego typu zagrożeń oraz podatność na nie przestrzeni publicznych, a następnie przedstawiono znaczenie analizy ryzyka, rozpoznania dróg dojazdowych, aktualnych standardów badawczych i praktycznej interpretacji wyników testów zderzeniowych. Wskazano najczęstsze błędy popełniane przy projektowaniu, instalacji i eksploatacji systemów ochrony. Osobną część tekstu poświęcono modelowi projektowania systemów HVM opartemu na analizie scenariusza zagrożenia, strefie buforowej,

ochronie warstwowej i odpowiedzialności organizacyjnej. W artykule podkreślono konieczność zwiększenia świadomości dotyczącej omawianego problemu w odniesieniu do polskich realiów oraz wskazano kierunki systemowego rozwoju zabezpieczeń dla przestrzeni publicznych i wydarzeń publicznych.

Słowa kluczowe

wydarzenie publiczne, impreza masowa, ochrona przestrzeni publicznych, atak z użyciem pojazdu, system HVM, bariera pojazdowa VSB, DoS SD-STD-02.01, ASTM F2656/F2656M, PAS 68, IWA 14-1, ISO 22343

Abstract

The aim of the article is to discuss HVM (hostile vehicle mitigation) systems and VSB (vehicle security barriers) devices as a means of protecting public spaces and mass events against the deliberate use of a vehicle as a weapon. The conceptual framework relating to HVM systems and VSBs was organised, and current research standards concerning security devices were presented. The nature of this type of threats and the vulnerability of public spaces to them were discussed, followed by a presentation on the importance of risk analysis, the assessment of access-routes, current testing standards and the practical interpretation of crash-test results. The most common errors made during the design, installation and operation of safety systems were highlighted. A separate section was devoted to a model for designing HVM systems based on threat-scenario analysis, buffer zones, layered protection and organisational responsibility. The article highlights the need to increase awareness of the issue in question in the Polish context and sets out directions for the systemic development of protective measures for public spaces and public events.

Keywords

public event, mass event, protection of public spaces, vehicle-as-a-weapon attack, HVM, VSB, DoS SD-STD-02.01, ASTM F2656/F2656M, PAS 68, IWA 14-1, ISO 22343

Wprowadzenie

Ochrona przestrzeni publicznych przed atakiem z użyciem pojazdu jest ważnym zagadnieniem z zakresu bezpieczeństwa publicznego. Nie chodzi przy tym wyłącznie o akty o charakterze terrorystycznym, lecz o szerszą kategorię zdarzeń, w których pojazd zostaje świadomie wykorzystany jako narzędzie oddziaływania na osoby przebywające w tych przestrzeniach.

Decydujące znaczenie ma sam mechanizm zagrożenia: gwałtowne wtargnięcie pojazdu w strefę ruchu pieszego, przy wykorzystaniu jego masy i energii kinetycznej jako podstawowych czynników rażenia.

Stan badań w tym obszarze ma charakter rozproszony i interdyscyplinarny¹. Obejmuje on:

- 1) opracowania poświęcone atakom typu *vehicle-ramming*, w których pojazd traktowany jest jako łatwo dostępne narzędzie zamachu na tzw. cele miękkie i zatłoczone miejsca;
- 2) dokumenty instytucjonalne dotyczące ochrony przestrzeni publicznych, miejsc zgromadzeń oraz imprez masowych, w tym wytyczne odnoszące się do planowania stref bezpieczeństwa, separacji ruchu kołowego od pieszego oraz stosowania systemów HVM (od ang. *hostile vehicle mitigation*);
- 3) normy i standardy techniczne określające sposób badania oraz klasyfikowania barier zabezpieczających przed uderzeniem pojazdu, w szczególności standardy odnoszące się do barier pojazdowych VSB (od ang. *vehicle security barriers*)².

¹ Por. C.R. Ludbey i in., *Classifying vehicle-as-a-weapon attacks: an inductive taxonomy and design implications*, „Crime Science” 2026, t. 15, art. 2. <https://doi.org/10.1186/s40163-025-00265-7>; V. Miller, K.J. Hayward, *‘I Did My Bit’: Terrorism, Tarde and the Vehicle Ramming Attack as an Imitative Event*, „The British Journal of Criminology” 2019, t. 59, nr 1, s. 1–23. <https://doi.org/10.1093/bjc/azy017>; J.P. Phillips, J.S. Young, W.J. Brady, *Preparation and response to a targeted automobile ramming mass casualty (TARMAC) attack: An analysis of the 2017 Charlottesville, Virginia TARMAC attack*, „American Journal of Disaster Medicine” 2019, t. 14, nr 3, s. 219–223. <https://doi.org/10.5055/ajdm.2019.0333>; P. Hess, S. Mandhan, *Ramming attacks, pedestrians, and the securitization of streets and urban public space: a case study of New York City*, „Urban Design International” 2022, t. 28, nr 1, s. 19–34. <https://doi.org/10.1057/s41289-022-00180-2>; A.M. Tsur i in., *Patterns in vehicle-ramming attacks*, „Israel Medical Association Journal” 2022, t. 24, nr 9, s. 579–583; M. Cichomski, *Jak samorządy mogą chronić przestrzeń publiczną przed atakami z użyciem pojazdów?*, „Terroryzm – studia, analizy, prewencja” 2025, nr 8, s. 203–233. <https://doi.org/10.4467/27204383TER.25.051.23038>; J. Jąźwiński, *Ochrona antyterrorystyczna obiektów użyteczności publicznej oraz infrastruktury krytycznej przed atakami z wykorzystaniem pojazdów mechanicznych*, „Terroryzm – studia, analizy, prewencja” 2023, nr 3, s. 120–171. <https://doi.org/10.4467/27204383TER.23.004.17444>.

² *Public Realm Design Guide for Hostile Vehicle Mitigation*, National Protective Security Authority, <https://www.npsa.gov.uk/specialised-guidance/hostile-vehicle-mitigation-hvm/public-realm-design-guide-hostile-vehicle-mitigation-0> [dostęp: 12 IV 2026]; *Vehicle Ramming Action Guide*, Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide> [dostęp: 20 VI 2026]; *Hostile Vehicle Guidelines for Crowded Places*, <https://www.nationalsecurity.gov.au/crowded-places-subsite/Files/hostile-vehicle-guidelines-crowded-places.pdf> [dostęp: 20 VI 2026];

W polskich realiach to zagadnienie pozostaje nierozpoznane w wystarczającym stopniu, zarówno na poziomie organizacyjnym, jak i projektowym. Mimo niewystąpienia na terytorium Polski zamachów terrorystycznych z użyciem pojazdu, nie należy marginalizować tego zagrożenia, zwłaszcza w odniesieniu do imprez masowych i innych wydarzeń organizowanych na otwartej przestrzeni.

Celem artykułu jest omówienie systemów HVM i barier pojazdowych VSB jako elementu ochrony przestrzeni publicznych i wydarzeń publicznych przed atakami z użyciem pojazdu. Uporządkowano podstawowe pojęcia związane z ochroną przed takim atakiem, przedstawiono aktualne standardy badawcze dotyczące urządzeń zabezpieczających oraz wskazano najczęstsze błędy popełniane przy projektowaniu, instalacji i eksploatacji systemów HVM. Problem badawczy sprowadza się do pytania, jakie warunki muszą zostać spełnione, aby ochrona przestrzeni publicznych i wydarzeń publicznych przed wtargnięciem pojazdu była realna i skuteczna, a nie pozorna.

W artykule postawiono trzy pytania badawcze: jakie znaczenie mają aktualne standardy badawcze i prawidłowa interpretacja wyników testów zderzeniowych dla doboru barier pojazdowych VSB? Jakie błędy najczęściej obniżają skuteczność systemu HVM? Jakie elementy powinien obejmować model projektowania systemu HVM dla przestrzeni publicznych i wydarzeń publicznych?

Artykuł ma charakter analityczno-praktyczny. Autor zastosował metody takie jak: analiza literatury przedmiotu, aktów prawnych, norm i dokumentów normalizacyjnych odnoszących się do barier pojazdowych VSB oraz materiałów instytucjonalnych i eksperckich pochodzących z różnych porządków krajowych i międzynarodowych, w tym Komisji Europejskiej, JRC, NPSA, CISA, materiałów francuskich, belgijskich i niemieckich, oraz analiza materiału empirycznego obejmującego obserwacje z zawodowej praktyki autora, przykłady wdrożeń oraz przypadki stosowania zabezpieczeń w przestrzeniach publicznych.

ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating, <https://www.iso.org/standard/50080.html> [dostęp: 20 VI 2026]; ASTM F2656/F2656M-20 Standard Test Method for Crash Testing of Vehicle Security Barriers, https://www.astm.org/f2656_f2656m-20.html [dostęp: 20 VI 2026].

Aparat pojęciowy

Jednym z podstawowych problemów występujących w polskiej debacie dotyczącej ochrony przestrzeni publicznych przed atakiem z użyciem pojazdu pozostaje niejednorodność terminologii. W obiegu funkcjonują określenia potoczne, uproszczenia w języku branżowym oraz kalki językowe, które nie oddają ani technicznego, ani organizacyjnego sensu poszczególnych rozwiązań. Brak precyzji pojęciowej prowadzi do błędów projektowych, błędnej oceny skuteczności urządzeń oraz mylenia środków ochronnych z elementami porządkowymi lub drogowymi. Z tego względu uporządkowanie terminologii stanowi warunek rozważań.

Podstawowym pojęciem stosowanym w artykule jest HVM. Oznacza system ochrony przed świadomym wykorzystaniem pojazdu jako narzędzia ataku. Obejmuje całość działań służących ograniczeniu możliwości wtargnięcia pojazdu do strefy chronionej albo zmniejszeniu skutków takiego wtargnięcia. W zakres HVM wchodzi zatem zarówno środki infrastrukturalne, jak i rozwiązania organizacyjne, proceduralne, urbanistyczne i operacyjne³.

Drugim pojęciem jest VSB, które oznacza konkretne urządzenia projektowane w celu zatrzymania, przechwycenia albo ograniczenia ruchu pojazdu w określonym scenariuszu zagrożenia i badane pod tym kątem. Do tej kategorii należą zarówno rozwiązania stałe, jak i tymczasowe oraz mobilne, pod warunkiem że ich funkcja ochronna została potwierdzona w odpowiednich testach zderzeniowych. Sam wygląd urządzenia, jego masa lub deklaracje marketingowe producenta nie wystarczają do uznania go za VSB w sensie technicznym⁴.

Dopuszczalne jest używanie określenia „bariery antyterrorystyczne” jako nazwy opisowej, o ile odnosi się ono do barier pojazdowych VSB stosowanych w ramach systemu HVM. Termin ten może być użyteczny w przekazie publicznym lub organizacyjnym, jednak nie zastępuje właściwej klasyfikacji technicznej. W dyskursie eksperckim pierwszeństwo powinny mieć pojęcia precyzyjne, pozwalające odróżnić system ochrony od jego elementów składowych a urządzenia przebadane od rozwiązań o wyłącznie pozornej funkcji ochronnej.

Należy unikać określenia „bariery antynajazdowe” jako głównego terminu z zakresu zabezpieczeń przed atakiem z użyciem pojazdu. Jest ono

³ Zob. J. Jaźwiński, *Ochrona antyterrorystyczna obiektów...*, s. 120–169.

⁴ Tamże, s. 121–123.

zbyt szerokie, nieostre i w praktyce prowadzi do mylnego utożsamiania barier pojazdowych VSB z elementami bezpieczeństwa ruchu drogowego, przeszkodami porządkowymi albo przypadkowymi obiektami małej architektury. Może ono sugerować równoważność rozwiązań, które z punktu widzenia bezpieczeństwa mają całkowicie odmienny status techniczny i operacyjny.

W artykule przyjęto zatem następujące rozróżnienie: HVM oznacza system ochrony przed świadomym wykorzystaniem pojazdu jako narzędzia ataku, VSB natomiast to fizyczne urządzenia wchodzące w skład tego systemu, o ile ich skuteczność została potwierdzona w badaniach właściwych dla tego rodzaju zagrożeń.

Charakter zagrożenia i podatność przestrzeni publicznych

Atak z użyciem pojazdu należy do tych zagrożeń, których skuteczność wynika z połączenia trzech czynników: prostoty wykonania, powszechnej dostępności narzędzia oraz możliwości oddziaływania – przy odpowiednio dobranym kierunku i momencie ataku – na dużą liczbę osób w krótkim czasie. Sprawca nie musi dysponować zaawansowanym zapleczem technicznym ani skomplikowaną logistyką. Z tego względu to zagrożenie ma szczególne znaczenie w kontekście ochrony wydarzeń publicznych oraz wszystkich przestrzeni o dużej koncentracji ruchu pieszego.

Ten rodzaj ataku polega na użyciu pojazdu jako nośnika energii kinetycznej, skierowanej bezpośrednio przeciwko osobom znajdującym się w przestrzeni publicznej. Oznacza to, że podstawowym mechanizmem rażenia nie jest sam pojazd rozumiany jako środek transportu, lecz jego masa, prędkość i zdolność do wtargnięcia w obszar, w którym nie powinien się znaleźć. Z perspektywy bezpieczeństwa publicznego ma to poważne konsekwencje: ocena zagrożenia nie może koncentrować się wyłącznie na intencji sprawcy, ale musi obejmować również warunki umożliwiające przeprowadzenie ataku.

Najbardziej narażone na tego typu ataki są wydarzenia organizowane na otwartej przestrzeni, zwłaszcza te o tymczasowym, sezonowym lub okazjonalnym charakterze, np. jarmarki, festyny, wydarzenia kulturalne czy religijne, które wymagają zamknięcia ulic. Ich podatność wynika z dostępności komunikacyjnej, dużego zagęszczenia osób, ograniczonej

możliwości pełnej kontroli wszystkich kierunków dojścia oraz częstego braku trwałych środków ochronnych⁵.

Z perspektywy potencjalnego sprawcy cele tego rodzaju są atrakcyjne również ze względu na efekt psychologiczny i medialny. Atak przeprowadzony w miejscu powszechnie postrzeganym jako bezpieczne i ogólnodostępne, przez które każdego dnia przewija się znaczna liczba osób, może wiązać się nie tylko z wieloma ofiarami, lecz także z silnym efektem destabilizującym.

Szczególne znaczenie mają w tym kontekście wydarzenia o charakterze symbolicznym i wysokiej wartości wspólnotowej, związane ze świętami, tradycjami lokalnymi, uroczystościami religijnymi itp.

Odmienny poziom podatności występuje natomiast w przypadku obiektów i przestrzeni projektowanych zgodnie z zasadą *security by design*. W takich lokalizacjach wymagania bezpieczeństwa są uwzględniane już na etapie planowania, projektowania i późniejszej eksploatacji infrastruktury. Dotyczy to zwłaszcza wybranych obiektów zamkniętych, stadionów, aren widowiskowych oraz tych przestrzeni miejskich, w których wdrożono trwałe środki kontroli dostępu, stałe elementy blokujące ruch pojazdów, czytelny podział przestrzeni na oznaczone strefy bezpieczeństwa oraz rozwiązania ograniczające możliwość bezpośredniego wjazdu w obszar koncentracji dużej liczby ludzi.

Nie oznacza to jednak, że obiekty projektowane z uwzględnieniem zasad bezpieczeństwa są całkowicie wolne od ryzyka. Ich podatność została jedynie ograniczona przez wcześniejsze rozpoznanie zagrożeń i wdrożenie rozwiązań infrastrukturalnych oraz organizacyjnych. Ta różnica wyznacza granicę między przestrzenią przygotowaną na zagrożenie a przestrzenią, która pozostaje na nie podatna, ponieważ w jej ramach bezpieczeństwo traktuje się dopiero jako reakcję na zdarzenie, a nie jako element planowania.

W praktyce oznacza to konieczność odejścia od myślenia, że atak z użyciem pojazdu to scenariusz skrajny albo możliwy wyłącznie w państwach o wyższym poziomie zagrożenia terrorystycznego. Z punktu widzenia ochrony przestrzeni publicznych istotne jest bowiem nie to, czy dane państwo doświadczyło już spektakularnego ataku, lecz to, czy jego przestrzenie pozostają podatne na tego rodzaju zdarzenie. To właśnie podatność powinna być podstawowym kryterium oceny potrzeby wdrażania systemów HVM.

⁵ Zob. M. Cichomski, *Jak samorządy mogą chronić przestrzenie publiczne...*, s. 207–215.

Szczególnie realistycznym elementem scenariuszy projektowych omawianego typu zagrożeń są pojazdy dostawcze i ciężarowe kategorii ok. 7,5 t. Wynika to z ich relatywnej dostępności, możliwości wykorzystania w ruchu miejskim oraz z parametrów energetycznych uderzenia, które przy prędkościach przyjmowanych w standardach badawczych pozwalają na wywołanie poważnych skutków w przestrzeni publicznej. Z tego względu projektowanie zabezpieczeń nie powinno koncentrować się na pojazdach osobowych, lecz na scenariuszach odpowiadających możliwościom sprawcy czy geometrii miejsca⁶.

Analiza miejsca i dróg dojazdowych jako podstawa oceny zagrożenia

Jednym z najważniejszych etapów oceny zagrożenia atakiem z użyciem pojazdu jest analiza konkretnego miejsca oraz identyfikacja wszystkich kierunków, z których pojazd mógłby wtargnąć do chronionej przestrzeni. Na tym etapie rozstrzyga się, czy projektowane zabezpieczenie będzie odpowiadało rzeczywistemu zagrożeniu, czy jedynie jego uproszczonemu wyobrażeniu. W tej części jako punkt odniesienia przyjęto ISO 22343-2:2023⁷ oraz uzupełniające wytyczne eksperckie dotyczące analizy ryzyka, geometrii dojazdu, scenariusza ataku z użyciem pojazdu i warunków lokalnych wpływających na skuteczność barier pojazdowych VSB.

Analiza miejsca powinna obejmować co najmniej pięć kroków:

- 1) identyfikację strefy chronionej i jej funkcji,
- 2) rozpoznanie wszystkich możliwych osi dojazdu,
- 3) ocenę parametrów geometrycznych i terenowych,
- 4) określenie realistycznego scenariusza ataku z użyciem pojazdu,
- 5) weryfikację ciągłości planowanej linii ochrony.

Należy zwrócić uwagę na główne i boczne drogi dojazdowe, ciągi techniczne i serwisowe, przejazdy awaryjne, parkingi, fragmenty infrastruktury

⁶ Por. ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirements...; ASTM F2656/F2656M-20 Standard Test Method for Crash Testing of Vehicle Security Barriers...; *Hostile Vehicle Mitigation ISO 22343-1:2023 NPSA Guidance Note*, <https://www.npsa.gov.uk/system/files/documents/npsa-hvm-guidance-note-iso-22343-1-feb-2024.pdf> [dostęp: 12 IV 2026].

⁷ ISO 22343-2:2023 Security and resilience – Vehicle security barriers – Part 2: Application, <https://www.iso.org/standard/81415.html> [dostęp: 12 IV 2026].

miejskiej umożliwiające ominięcie głównej linii zabezpieczenia oraz parametry ciągów pieszych, jeżeli ich geometria może zostać wykorzystana jako kierunek wtargnięcia pojazdu. Dopiero po tak przeprowadzonej analizie można przejść do odpowiedniego doboru barier pojazdowych VSB i organizacji stref buforowych.

Szczegółne znaczenie ma możliwość obejścia albo ominięcia zabezpieczenia. Nawet prawidłowo dobrane i ustawione bariery pojazdowe VSB nie spełnią swojej funkcji, jeżeli analiza ograniczy się do jednego kierunku wjazdu, pozostawiając po bokach przestrzeń umożliwiającą przejazd. Skuteczność systemu ochrony zależy zarówno od parametrów samego urządzenia, jak i od ciągłości geometrii zabezpieczenia w skali całej chronionej przestrzeni.

Błędem jest przyjmowanie, że administracyjne ograniczenia ruchu, takie jak zakaz wjazdu, oznakowanie tymczasowe, separacja organizacyjna czy ograniczenie tonażu, same w sobie obniżają poziom zagrożenia. Tego rodzaju środki mogą mieć znaczenie porządkowe i regulacyjne, ale nie stanowią fizycznej przeszkody dla sprawcy działającego świadomie i celowo. Z perspektywy HVM istotne jest więc to, czy przejazd został realnie zablokowany przed wtargnięciem pojazdu.

Analiza miejsca powinna obejmować zarówno sam przebieg możliwych dróg dojazdowych, jak i ich parametry przestrzenne i funkcjonalne. Znaczenie mają m.in. długość odcinka rozpędzania, szerokość przejazdu, promień skrętu, rodzaj nawierzchni, nachylenie terenu, obecność przeszkód pośrednich oraz możliwość wykorzystania infrastruktury towarzyszącej jako toru obejścia. Pozornie drugorzędne elementy geometrii terenu mogą w praktyce przesądzać o tym, czy dany kierunek powinien zostać uznany za możliwy scenariusz wtargnięcia.

Właściwa analiza miejsca polega na przyjęciu perspektywy pojazdu atakującego i rozpoznaniu wszystkich realnych możliwości dotarcia do obszaru chronionego. Dopiero takie podejście pozwala określić prawidłowe rozmieszczenie barier pojazdowych VSB, wyznaczyć linię ochrony, ocenić potrzebę zastosowania rozwiązań warstwowych oraz zidentyfikować punkty szczególnej podatności.

Z tego względu analiza miejsca i dróg dojazdowych powinna być fundamentem, a nie etapem pomocniczym procesu projektowania zabezpieczenia. Jeżeli zostanie przeprowadzona pobieżnie, błędnie albo fragmentarycznie, nawet najlepsze urządzenia ochronne nie zapewnią odpowiedniego poziomu bezpieczeństwa. W systemach HVM błędna diagnoza dotycząca przestrzeni niemal zawsze prowadzi do nieprawidłowego zabezpieczenia.

W kontekście etapu projektowania zasadne jest również rozróżnienie dwóch stref: strefy redukcji prędkości, w której wykorzystuje się szyszki, zwężenia i elementy porządkowe do ograniczania długości rozpędu, oraz docelowej strefy ochrony (strefy przechwycenia pojazdu), w której stosuje się urządzenia certyfikowane jako bariery pojazdowe. Elementy z pierwszej strefy mogą wspierać bezpieczeństwo, ale nie zastępują barier VSB w strefie przechwycenia pojazdu.

Modele stosowania barier pojazdowych VSB na przykładzie państw europejskich

Analiza rozwiązań stosowanych w praktyce pokazuje, że podejście do ochrony przestrzeni publicznych przed atakiem z użyciem pojazdu jest silnie zróżnicowane. Wynika to zarówno z poziomu rozpoznania zagrożenia, jak i z doświadczeń poszczególnych państw oraz miast w zakresie organizacji bezpieczeństwa, planowania przestrzeni i wdrażania rozwiązań infrastrukturalnych. W związku z tym nie istnieje jeden uniwersalny model ochrony, który można bezrefleksyjnie przenosić między różnymi realiami organizacyjnymi. Można jednak wskazać praktyki wyznaczające kierunki dojrzałego, bardziej systemowego podejścia.

W polskich realiach istotnym punktem odniesienia pozostaje Warszawa, gdzie zaczęto stosować certyfikowane bariery pojazdowe VSB podczas wybranych wydarzeń oraz w niektórych lokalizacjach miejskich, m.in. w obszarze Traktu Królewskiego, obejmującego Krakowskie Przedmieście i Nowy Świat⁸.

Jest to zjawisko istotne z dwóch powodów. Po pierwsze, pokazuje wzrost rozpoznania problemu ochrony przestrzeni publicznych przed wtargnięciem pojazdu. Po drugie, ujawnia, że rozwój tego obszaru nadal jest częściowy i nie prowadzi jeszcze do wdrożenia jednolitych, spójnych standardów systemowych. W praktyce oznacza to, że pojedyncze dobre realizacje nie są równoznaczne z dojrzałym modelem krajowym.

Inaczej jest przykładowo w Wielkiej Brytanii, gdzie problem ochrony przestrzeni publicznych przed atakiem z użyciem pojazdu został wcześniej

⁸ Zob. *Poprawiamy bezpieczeństwo w stolicy. Rozstawiamy bariery antyterrorystyczne i szkolimy z ich obsługi*, Zarząd Dróg Miejskich w Warszawie, 17 III 2026 r., <https://zdm.waw.pl/aktualnosci/poprawiamy-bezpieczenstwo-w-stolicy-rozstawiamy-bariery-antyterrorystyczne-i-szkolimy-z-ich-obslugi/> [dostęp: 12 IV 2026].

rozpoznany zarówno na poziomie praktycznym, jak i regulacyjnym. W brytyjskim podejściu szczególnie istotne jest łączenie rozwiązań infrastrukturalnych, organizacyjnych i prawnych. Ochrony nie sprowadza się tam wyłącznie do ustawienia urządzeń fizycznych. Stanowi ona element szerszego systemu zarządzania ryzykiem, odpowiedzialności organizacyjnej oraz obowiązków wynikających z konieczności zapewnienia bezpieczeństwa przestrzeni publicznych i wydarzeń publicznych. W Wielkiej Brytanii są ponadto rozwijane regulacje prawne związane z koncepcją Protect Duty, znanej jako Martyn's Law⁹. To rozwiązanie służy wzmocnieniu ochrony przed terroryzmem w odniesieniu do wybranych obiektów i wydarzeń publicznych przez nałożenie obowiązków dotyczących przygotowania, planowania reakcji i – w przypadku większych obiektów oraz wydarzeń – wdrażania proporcjonalnych środków ograniczających podatność na atak. Wymiar prawny nie zastępuje tu rozwiązań technicznych, lecz przypisuje odpowiedzialność za ich ocenę i wdrożenie¹⁰.

W Niemczech Berlin stał się jednym z ważniejszych punktów odniesienia dla praktyki zabezpieczania wydarzeń publicznych po ataku na jarmark bożonarodzeniowy w grudniu 2016 r. Po tym zdarzeniu nastąpiły wzrost znaczenia fizycznych środków ochrony w przestrzeni miejskiej oraz istotne przewartościowanie podejścia do bezpieczeństwa wydarzeń sezonowych.

Doświadczenie zamachu we francuskiej Nicei z 14 lipca 2016 r. unaczniło skalę zagrożenia związanego z użyciem pojazdu w przestrzeni publicznej o bardzo dużym zagęszczeniu ruchu pieszego. Przypadki Berlina i Nicei pokazują, że ochrona przestrzeni miejskich w Europie rozwijała się nie tylko na podstawie teorii bezpieczeństwa, lecz także pod wpływem doświadczeń.

W zakresie norm w Wielkiej Brytanii ważnym punktem odniesienia jest PAS 68¹¹ oraz powiązane z nią wytyczne. Od 2023 r. aktualnym międzynarodowym standardem w obszarze barier pojazdowych jest norma

⁹ Por. Terrorism (Protection of Premises) Act 2025, UK Public General Acts 2025 c. 10, <https://www.legislation.gov.uk/ukpga/2025/10/contents> [dostęp: 12 IV 2026]; *Martyn's Law: the SIA's New Regulatory Role*, Security Industry Authority, <https://www.gov.uk/government/publications/martyns-law-the-sias-new-regulatory-role/martyns-law-the-sias-new-regulatory-role> [dostęp: 12 IV 2026].

¹⁰ Zob. M. Cichomski, *Jak samorządy mogą chronić przestrzenie publiczne...*, s. 206–208, 214–224.

¹¹ British Standards Institution, PAS 68:2013 Impact test specifications for vehicle security barrier systems, <https://knowledge.bsigroup.com/products/impact-test-specifications-for-vehicle-security-barrier-systems> [dostęp: 12 IV 2026].

ISO 22343. Zwłaszcza ISO 22343-1:2023¹² określa wymagania badawcze, metodę testowania i klasyfikację wyników, ISO 22343-2:2023 natomiast odnosi się do zastosowania, doboru, instalacji i wykorzystania barier pojazdowych VSB w praktyce projektowej i operacyjnej. Jednocześnie analiza publicznie dostępnych materiałów francuskich, belgijskich i niemieckich wskazuje, że w praktyce istotne znaczenie mają przede wszystkim dokumenty operacyjne, rekomendacje oraz rozwiązania organizacyjne dotyczące zabezpieczania przestrzeni publicznych i wydarzeń publicznych przed atakiem z użyciem pojazdu. Nie oznacza to braku rozwiązań technicznych lub normatywnych, lecz pokazuje, że w publicznie dostępnych materiałach większy nacisk jest położony na organizację ochrony, analizę ryzyka i dobór środków zabezpieczających niż na eksponowanie odrębnych krajowych standardów testów zderzeniowych. Sekretariat Generalny Obrony i Bezpieczeństwa Narodowego Francji (Secrétariat général de la défense et de la sécurité nationale) publikuje kartę dobrych praktyk ochrony wydarzeń w przestrzeni publicznej przed atakami pojazdem taranującym, niemieckie Federalne Ministerstwo Spraw Wewnętrznych (Bundesministerium des Innern) informowało o wspieraniu standardu DIN dla barier pojazdowych, a niemiecka policja publikuje materiały o ochronie przestrzeni publicznych przed „Überfahrtaten”. Komisja Europejska w ramach JRC opublikowała natomiast wytyczne dotyczące projektowania, testowania i instalacji barier chroniących¹³.

Najważniejszy wniosek z analizy modeli miejskich jest następujący: dojrzałość systemu ochrony przed atakiem z użyciem pojazdu wynika z jakości całego procesu doboru barier w przestrzeni, ich rozmieszczenia, utrzymania i osadzenia w szerszym modelu odpowiedzialności organizacyjnej. Miasto wyposażone w pojedyncze urządzenia nie dysponuje jeszcze

¹² ISO 22343-1:2023, Security and resilience – Vehicle security barriers – Part 1: Performance requirement...

¹³ Por. *Se protéger contre les attaques au véhicule-bélier*, Secrétariat général de la défense et de la sécurité nationale, 11 VI 2018 r., <https://www.sgdns.gouv.fr/publications/se-protoger-contre-les-attaques-au-vehicule-belier> [dostęp: 12 IV 2026]; *Schutz öffentlicher Räume vor Überfahrtaten*, Polizeiliche Kriminalprävention der Länder und des Bundes, <https://www.polizei-beratung.de/themen-und-tipps/staedtebau/schutz-vor-ueberfahrtaten/> [dostęp: 12 IV 2026]; V. Karlos, M. Larcher, G. Solomos, *Review on vehicle barrier protection guidance*, Publications Office of the European Union, European Commission, Joint Research Centre, 2017. <https://doi.org/10.2760/845599>; *Protection of public spaces from terrorist attacks*, European Commission, Joint Research Centre, https://joint-research-centre.ec.europa.eu/projects-and-activities/protection-public-spaces-terrorist-attacks_en [dostęp: 12 IV 2026].

systemem HVM. O systemowym charakterze ochrony można mówić wtedy, gdy środki fizyczne są elementem wcześniej rozpoznanego, spójnego modelu zarządzania zagrożeniem.

Typologia wydarzeń a dobór barier pojazdowych VSB

W doborze barier pojazdowych VSB istotne jest rozróżnienie typów chronionych wydarzeń. Projekty ochrony dla wydarzenia cyklicznego i wielotygodniowego, wydarzenia z udziałem osób ochranianych, wydarzenia mobilnego lub wydarzenia organizowanego w przestrzeni nieprzystosowanej do gromadzenia tłumu różnią się od siebie. Typologia wydarzeń wpływa na przebieg osi dojazdu, organizację dostaw, możliwość utrzymania ciągłej linii ochrony oraz wymagania wobec rozwiązań tymczasowych.

Wydarzenia cykliczne i wielotygodniowe

Wydarzenia cykliczne i wielotygodniowe, takie jak jarmarki sezonowe, charakteryzują się długotrwałym zajęciem przestrzeni, powtarzalnymi dostawami oraz koniecznością utrzymania ochrony przez dłuższy czas. W takich przypadkach zasadne jest dążenie do stworzenia możliwie ciągłej linii ochrony z wykorzystaniem certyfikowanych barier pojazdowych, przy jednoczesnym zaplanowaniu kontrolowanych punktów wjazdu dla pojazdów uprawnionych.

Wydarzenia z udziałem osób ochranianych

Wydarzenia z udziałem osób ochranianych, w tym wizyty VIP-ów, wymagają elastycznego rozmieszczenia zabezpieczeń wzdłuż osi przejazdu oraz w punktach postoju. Taką realizację cechują krótki czas instalacji i demontażu, konieczność szybkiego przenoszenia sprzętu oraz potrzeba utrzymania rezerwy logistycznej i personelu gotowego do relokacji barier pomiędzy kolejnymi lokalizacjami. Zabezpieczenia tego typu mogą być stosowane czasowo, wyłącznie na potrzeby konkretnego wydarzenia lub okresu podwyższonego ryzyka.

Poniżej przedstawiono wybrane rozwiązania stosowane w państwach europejskich. Rozwiązania te różnią się konstrukcją, przeznaczeniem oraz odpornością na uderzenie pojazdu, a ich dobór powinien odpowiadać typowi wydarzenia, układowi linii ochrony i wymaganiom operacyjnym. Zdjęcie 1 pokazuje przykład czasowego zabezpieczenia z wykorzystaniem

barier RBM M30 przestrzeni publicznej w Warszawie podczas wydarzenia o podwyższonym znaczeniu ochronnym.



Zdjęcie 1. Bariery RBM M30 – czasowe zabezpieczenie przestrzeni publicznej podczas wydarzenia o podwyższonym znaczeniu ochronnym (Warszawa).

Źródło: materiały DFE Security sp. z o.o.

Na zdjęciu 2 przedstawiono fizyczne zabezpieczenie strefy wejściowej jarmarku bożonarodzeniowego w Ratyzbonie z wykorzystaniem tymczasowych mobilnych barier VSB, ograniczających możliwość wtargnięcia pojazdu do przestrzeni publicznej o wysokiej koncentracji ruchu pieszego.



Zdjęcie 2. Tymczasowe mobilne bariery VSB – zabezpieczenie strefy wejściowej jarmarku bożonarodzeniowego (Ratyzbona).

Źródło: materiały marketingowe firmy Hörmann Polska.

W tabeli 1 przedstawiono wybrane bariery pojazdowe VSB stosowane w Europie. Różnią się one konstrukcją, przeznaczeniem oraz odpornością na uderzenie pojazdu, a ich dobór powinien odpowiadać typowi wydarzenia, układowi linii ochrony i wymaganiom operacyjnym.

Tabela 1. Wybrane bariery pojazdowe VSB stosowane w ochronie wydarzeń publicznych w Europie.

			
RBM M30	SURFACE GUARD	OKTABLOCK	PITAGONE F18
imprezy cykliczne, długoterminowe zamknięcia ulic	imprezy cykliczne, długoterminowe zamknięcia ulic	jednorazowe, krótko- i długoterminowe wydarzenia	jednorazowe, krótkoterminowe wydarzenia
montaż w 20 minut (2 os.)	montaż 6 m w 40 minut (4 os.)	nie wymaga montażu, wystarczy samo ustawienie (1-2 os.)	szybki montaż i możliwość przestawiania (1-2 os.)
transport: ciężarówka z HDS	transport: samochód dostawczy	transport: ciężarówka z HDS lub z mobilnym dźwigiem montażowym	transport: samochód dostawczy
poziom bezpieczeństwa: pojazd o masie 7200 kg – prędkość 48 km/h	poziom bezpieczeństwa: pojazd o masie 7200 kg – prędkość 32 km/h i 2500 kg - prędkość 48 km/h	poziom bezpieczeństwa: pojazd o masie 7500 kg – prędkość 55 km/h i 3500 kg - prędkość 32 km/h	poziom bezpieczeństwa: pojazd o masie 7500 kg – prędkość 48 km/h

Źródło: opracowanie własne na podstawie materiałów udostępnionych przez DFE Security sp. z o.o.

Wydarzenia mobilne i przestrzenie nieprzystosowane do gromadzenia dużej liczby osób

Wydarzenia mobilne, takie jak przejazdy sportowe, oraz wydarzenia organizowane w przestrzeniach nieprzystosowanych do gromadzenia dużej

liczby osób wymagają identyfikacji punktów krytycznych, w których pojazd może osiągnąć relatywnie większą prędkość albo w których gromadzi się największa liczba uczestników. W takich sytuacjach szczególnego znaczenia nabiera wcześniejsze ustalenie możliwych kierunków dojazdu pojazdu do strefy chronionej, czyli potencjalnych dróg natarcia, oraz takie rozmieszczenie barier pojazdowych, aby uniemożliwić kontynuowanie przejazdu w kierunku obszaru koncentracji ludzi (zdjęcie 3).



Zdjęcie 3. Tymczasowa bariera mobilna – zabezpieczanie tras przejazdu oraz wydarzeń organizowanych na otwartej przestrzeni (Berlin).

Źródło: materiały marketingowe firmy Pitagone.

Normy, testy zderzeniowe i interpretacja parametrów barier pojazdowych VSB

Ocena barier pojazdowych VSB nie może się opierać na deklaracjach producenta, opisie handlowym ani samych obliczeniach inżynierskich. Kluczowe znaczenie mają normy i standardy badawcze, które porządkują sposób prowadzenia testów zderzeniowych, klasyfikacji wyników oraz porównywania różnych rozwiązań technicznych. Pozwalają ustalić, w jakim scenariuszu zagrożenia dane urządzenie zostało rzeczywiście przebadane i jakie parametry jego pracy potwierdzono empirycznie¹⁴.

Ocena skuteczności urządzenia powinna zatem być odpowiedzią na pytania: w jakim standardzie zostało przebadane, dla jakiej kategorii

¹⁴ Zob. *Impact Testing of Vehicle Security Barriers. An overview of vehicle impact test standards*, <https://www.npsa.gov.uk/system/files/documents/npsa-impact-testing-of-vehicle-security-barriers-18-august-2020.pdf> [dostęp: 29 III 2026].

pojazdu, przy jakiej masie, prędkości, kącie uderzenia i z jakim wynikiem penetracji. Przez penetrację należy rozumieć odległość, na jaką pojazd przemieszcza się poza linię bariery po uderzeniu. Parametr ten pozwala określić wymagany dystans między linią zabezpieczenia a obszarem chronionym. Bez takich danych ocena przydatności urządzenia jest wyłącznie deklaratorywna.

W sprzedaży często spotyka się tzw. rozwiązanie inżynierskie (ang. *engineering solution*). Tego rodzaju określenie może oznaczać konstrukcję zaprojektowaną na podstawie znajomości fizyki, mechaniki konstrukcji i mechaniki gruntu, lecz nie jest to tożsame z urządzeniem przebadanym w teście zderzeniowym. Rozwiązanie inżynierskie może być wartościowym etapem projektowania, ale nie zastępuje empirycznie potwierdzonego wyniku badania¹⁵.

Podstawowe standardy stosowane w ocenie barier pojazdowych VSB

Do najważniejszych dokumentów odnoszących się do badań urządzeń zabezpieczających przed atakiem z użyciem pojazdu należą zarówno starsze standardy krajowe i warsztatowe, jak i aktualna norma międzynarodowa ISO 22343. Historycznie istotne znaczenie miały amerykańskie klasyfikacje DoS SD-STD-02.01¹⁶, następnie brytyjski PAS 68 oraz dokument warsztatowy IWA 14-1:2013¹⁷, które porządkowały sposób badania barier pojazdowych i opisu wyników testów. W obrocie rynkowym nadal funkcjonują urządzenia klasyfikowane według starszych standardów, dlatego ich znajomość pozostaje niezbędna. Obecnie podstawowym punktem odniesienia jest wspomniana norma ISO 22343. Jej część pierwsza, ISO 22343-1:2023, określa wymagania badawcze, metodę testu i klasyfikację wyników, część druga, ISO 22343-2:2023, odnosi się do zastosowania, doboru, instalacji i wykorzystania barier pojazdowych VSB. Z praktycznego punktu widzenia oznacza to przejście od rozproszonych, częściowo krajowych podejść do

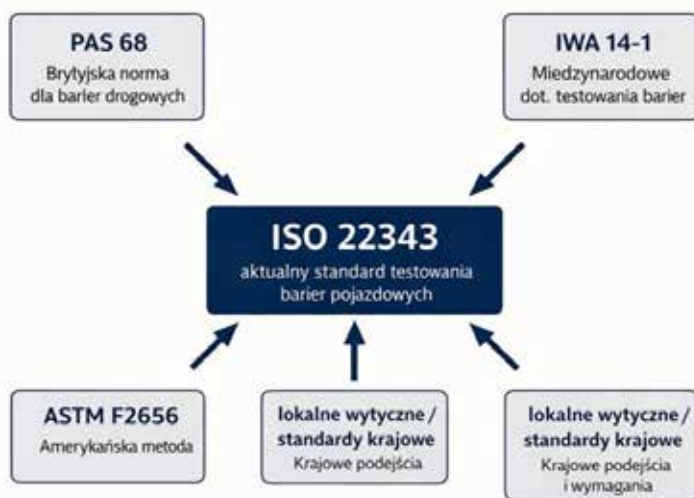
¹⁵ Zob. HVM – *Vehicle Impact Testing and FEA Computational Analysis Guidance Note*, <https://www.npsa.gov.uk/system/files/documents/npsa-guidance-note-hvm-vehicle-impact-testing-and-fea-computational-analysis-15-july-2021.pdf> [dostęp: 29 III 2026].

¹⁶ *Primer on Impact Protection for Critical Transportation Infrastructure*, FHWA-HIF-18-054, Federal Highway Administration, 2018 r., <https://www.fhwa.dot.gov/bridge/security/hif18054.pdf>, s. 17–20 [dostęp: 15 VI 2026].

¹⁷ IWA 14-1:2013 *Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating*.

bardziej zunifikowanego języka oceny, który pozwala porównywać rozwiązania badane w różnych porządkach normalizacyjnych.

DoS SD-STD-02.01 nie został ujęty na schemacie jako odrębny standard, ponieważ w artykule przyjęto syntetyczne ujęcie najważniejszych standardów funkcjonujących w praktyce rynkowej i dokumentacji technicznej. Jego aktualnym odpowiednikiem w klasyfikacji barier pojazdowych jest ASTM F2656/F2656M¹⁸ (rysunek 1).



Rysunek 1. Norma ISO 22343 jako aktualny punkt odniesienia w testowaniu barier pojazdowych.

Źródło: opracowanie własne.

Należy podkreślić, że norma PN-EN 1317¹⁹ nie jest właściwa dla barier pojazdowych VSB. Bywa w tym kontekście błędnie przywoływana, ponieważ dotyczy drogowych barier bezpieczeństwa. Została jednak opracowana z myślą o typowych zdarzeniach komunikacyjnych i ograniczaniu

¹⁸ ASTM F2656/F2656M-20 Standard...

¹⁹ PN-EN 1317 Systemy ograniczające drogę. Ta norma dotyczy drogowych systemów powstrzymujących pojazdy, np. barier stosowanych przy jezdniach lub między pasami ruchu na drogach i autostradach. Norma odnosi się do bezpieczeństwa ruchu drogowego i ograniczania skutków zdarzeń komunikacyjnych, a nie do barier pojazdowych VSB służących ochronie przed użyciem pojazdu jako narzędzia ataku.

skutków kolizji drogowych, a nie zagrożeniu świadomym użyciem pojazdu jako narzędzia ataku.

Istotne jest również odróżnienie rozwiązywania inżynierskiego od urządzenia przebadanego zgodnie z właściwym standardem. Sam opis konstrukcji lub obliczenia projektowe nie zastępują testu zderzeniowego, który potwierdza zachowanie urządzenia w warunkach dynamicznych. Z punktu widzenia projektanta znaczenie ma zarówno to, czy urządzenie zatrzymało pojazd, jak i to, w jakim scenariuszu badawczym zostało przebadane, ile wynosiły: masa pojazdu testowego, prędkość, kąt uderzenia, poziom penetracji oraz jakie były wtórne skutki zderzenia.

Analiza standardów powinna prowadzić od rozpoznania ich genezy i zakresu do odpowiedzi na pytanie, co wynik testu oznacza dla rzeczywistego projektu zabezpieczenia w konkretnym miejscu. W tym kontekście PAS 68, IWA 14-1 i DoS SD-STD-02.01 oraz ASTM F2656/F2656M zachowują znaczenie historyczne i porównawcze, a aktualnym standardem międzynarodowym pozostaje ISO 22343.

W artykule przyjęto syntetyczne ujęcie najważniejszych standardów nadal funkcjonujących w praktyce rynkowej i dokumentacji technicznej.

Dla właściwego doboru bariery pojazdowej VSB podstawowe znaczenie mają cztery parametry: masa pojazdu, prędkość uderzenia, kąt zderzenia oraz poziom penetracji pojazdu. Masa pojazdu wpływa na poziom obciążeń dynamicznych i energię oddziaływania. Prędkość determinuje energię kinetyczną, a więc jedną z najważniejszych wielkości decydujących o zachowaniu pojazdu, bariery oraz podłoża lub systemu mocowania podczas zderzenia. Istotnym parametrem uzupełniającym jest również dyspersja, rozumiana jako rozrzut odłamków lub elementów pojazdu po uderzeniu. Nie jest ona jednak podstawowym kryterium doboru bariery w takim samym stopniu jak wymienione wcześniej, lecz powinna być uwzględniana przy ocenie ryzyka dla osób oraz infrastruktury znajdujących się za linią zabezpieczenia.

Zależność między kątem uderzenia a torem ruchu pojazdu, linią bariery, strefą penetracji oraz strefą odłamków przedstawiono na rysunku 2.



Rysunek 2. Zderzenie pojazdu z barierą pojazdową z zaznaczeniem toru ruchu, linii bariery, strefy penetracji oraz strefy odłamków.

Źródło: opracowanie własne.

Kąt uderzenia wpływa na mechanizm przejęcia obciążenia oraz na to, czy urządzenie pracuje w warunkach zbliżonych do przebadanej konfiguracji. Penetracja określa natomiast, jak daleko pojazd lub jego elementy mogą wtargnąć za linię zabezpieczenia. Z punktu widzenia bezpieczeństwa uczestników wydarzenia ten parametr ma największe znaczenie, ponieważ decyduje o konieczności wyznaczenia strefy buforowej. Sam fakt zatrzymania pojazdu nie oznacza jeszcze pełnej skuteczności ochrony. Jeżeli penetracja jest znaczna, a za linią urządzenia znajdują się ludzie, skutki zdarzenia nadal mogą być poważne. Dlatego interpretacja wyników badań musi być zawsze powiązana z planowaniem bezpiecznej odległości między linią barier pojazdowych VSB a przestrzenią użytkowaną przez uczestników wydarzenia²⁰.

Znaczenie terminu „urządzenie przetestowane”

W praktyce rynkowej często używa się sformułowania „urządzenie przetestowane”, jednak bywa ono rozumiane zbyt szeroko. Nie oznacza ono każdej wersji handlowej urządzenia ani dowolnej konfiguracji jego montażu, lecz to, że określone urządzenie zostało przebadane w konkretnym układzie testowym.

Kluczowe znaczenie ma w tym kontekście pojęcie konfiguracji *as tested*. Parametry deklarowane dla urządzenia odnoszą się wyłącznie do takiego układu, w którym urządzenie zostało rzeczywiście przebadane. Każde odstępstwo od tej konfiguracji – zmiany w zakresie: kąta ustawienia,

²⁰ Zob. J. Jaźwiński, *Ochrona antyterrorystyczna obiektów...*, s. 127, 135–137.

liczby segmentów urządzenia, rodzaju podłoża, systemu połączeń, sposobu kotwienia lub warunków montażu – może prowadzić do zmiany mechanizmu pracy urządzenia i utraty parametrów potwierdzonych w teście²¹.

Zapis testu zderzeniowego – przykłady

Dla zrozumienia współczesnych norm badawczych istotne jest właściwe odczytywanie pełnego zapisu klasyfikacji bariery pojazdowej VSB. Taki zapis, oprócz tego, że jest kodem technicznym, stanowi także syntetyczny opis scenariusza, w którym urządzenie zostało przebadane.

Przykładowy zapis w starszym układzie klasyfikacyjnym:

IWA 14-1: V/7200[N3C]/48/90:29.1

Poszczególne elementy tego zapisu oznaczają: V – pojazd użyty w teście (vehicle), 7200 – masa pojazdu wyrażona w kilogramach, N3C – kategoria lub typ pojazdu według przyjętej klasyfikacji, 48 – prędkość uderzenia wyrażona w km/h, 90 – kąt uderzenia wyrażony w stopniach, 29.1 – parametr odnoszący się do przemieszczenia lub penetracji pojazdu poza linię odniesienia bariery.

Przykładowy zapis zgodny z aktualną normą:

ISO 22343-1: V/7,200(N2A)/48/90:2.6/5.0

W tym przypadku oznaczenia są następujące: V – pojazd testowy, 7,200 – masa pojazdu w kilogramach (7200), N2A – kategoria pojazdu zastosowanego w badaniu, 48 – prędkość uderzenia w km/h, 90 – kąt uderzenia w stopniach, 2.6 – wartość penetracji lub przemieszczenia pojazdu względem linii odniesienia, 5.0 – parametr odnoszony do wtórnych skutków zderzenia, w szczególności do dyspersji odłamków lub elementów pojazdu.

Pełny zapis klasyfikacyjny pozwala zatem odczytać, czy urządzenie zostało przebadane i w jakim dokładnie scenariuszu badawczym oceniano jego skuteczność. Ma to szczególne znaczenie przy doborze urządzenia do konkretnej przestrzeni publicznej, wydarzenia publicznego lub zabezpieczenia tymczasowego, ponieważ nawet pozornie podobne urządzenia mogą być testowane w odmiennych warunkach masy, prędkości i geometrii uderzenia.

²¹ Na temat znaczenia konfiguracji *as tested* oraz ograniczeń rozwiązań typu *engineered solutions* zob. J. Jaźwiński, *Ochrona antyterrorystyczna obiektów...*, s. 142–144. Zob. także: *Verifying solutions*, HVMhub, <https://hvmhub.com/products-advice/verifying-solutions/> [dostęp: 29 III 2026].

Z perspektywy projektowania to jakościowa zmiana podejścia. Ochrona nie może być oceniana wyłącznie przez pryzmat zatrzymania pojazdu. Równie ważne staje się pytanie, jakie wtórne efekty dynamiczne może wygenerować samo uderzenie i czy chroniona przestrzeń została zaprojektowana z uwzględnieniem tych skutków. ISO 22343-1 porządkuje sposób testowania i oceniania odporności bariery, a ISO 22343-2 pomaga przełożyć wynik testu na decyzję projektową i eksploatacyjną. Jednocześnie ani ISO, ani ASTM nie sugerują, że sam wynik testu automatycznie gwarantuje skuteczność w każdych warunkach terenowych – znaczenie nadal mają m.in. grunt, nawierzchnia, geometria dojazdu i konkretne warunki lokalne.

Test zderzeniowy a rozwiązanie inżynierskie

Na etapie projektowania jest możliwe opracowanie rozwiązania inżynierskiego na podstawie znanych zasad obliczeniowych, z uwzględnieniem wytrzymałości materiałów, momentów obrotowych, mechaniki gruntu i sposobu kotwienia. Takie podejście nie zastępuje jednak rzeczywistego testu zderzeniowego. Rozwiązanie inżynierskie może wskazywać prawdopodobny sposób działania urządzenia, jednak dopiero test potwierdza jego rzeczywiste działanie w dynamicznych warunkach.

Różnica ta ma fundamentalne znaczenie. Oddziaływanie pojazdu w zderzeniu nie ogranicza się do prostego statycznego obciążenia konstrukcji. Obejmuje złożone dynamiczne procesy, w których istotne są m.in. deformacja pojazdu, charakter kontaktu z urządzeniem, rozkład sił w czasie, zachowanie podłoża oraz wtórne przemieszczenia elementów.

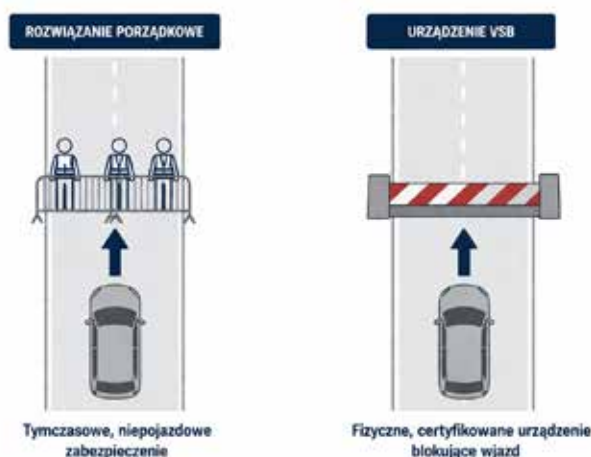
Znaczenie wyników badań dla projektowania systemów HVM

W odniesieniu do projektowania systemów HVM wyniki testów zderzeniowych nie mają charakteru wyłącznie technicznego ani laboratoryjnego. Stanowią bezpośrednią podstawę do wyznaczania strefy buforowej, oceny bezpiecznej odległości ruchu pieszych od barier pojazdowych VSB, doboru urządzenia do konkretnego scenariusza zagrożenia, oceny skutków wtórnych uderzenia oraz weryfikacji, czy dane rozwiązanie rzeczywiście odpowiada potrzebom ochrony przestrzeni publicznej. Innymi słowy, test zderzeniowy nie jest jedynie narzędziem certyfikacji produktu, lecz przede wszystkim źródłem danych niezbędnych do odpowiedzialnego projektowania zabezpieczenia. Bez prawidłowej interpretacji wyników badań cały proces doboru barier pojazdowych VSB staje się podatny na uproszczenia, błędne analogie oraz bezrefleksyjne przekładanie rozwiązań z jednego miejsca

lub scenariusza na drugi, bez uwzględnienia lokalnych warunków, takich jak możliwa prędkość uderzenia, kąt uderzenia, rodzaj nawierzchni, sposób montażu, dostępna przestrzeń buforowa i charakter chronionego obszaru.

Błędy projektowe, instalacyjne i operacyjne w stosowaniu barier pojazdowych VSB do zabezpieczania przestrzeni publicznych i wydarzeń publicznych

Skuteczność barier pojazdowych VSB zależy nie tylko od ich parametrów technicznych potwierdzonych w testach zderzeniowych, lecz także od czynników takich jak dobór urządzenia, warunki jego instalacji, organizacja przestrzeni oraz sposób użytkowania systemu w warunkach operacyjnych. Błędy, które mogą prowadzić do obniżenia skuteczności zabezpieczenia, mimo że samo urządzenie formalnie spełnia wymagania badawcze, pojawiają się właśnie na styku tych elementów. Dotyczy to zarówno zabezpieczeń stałych stosowanych w przestrzeniach publicznych, jak i zabezpieczeń tymczasowych wykorzystywanych podczas imprez masowych, wydarzeń cyklicznych, zgromadzeń oraz wydarzeń plenerowych. Różnicę między rozwiązaniem porządkowym a certyfikowaną barierą VSB blokującym wjazd przedstawiono na rysunku 3.

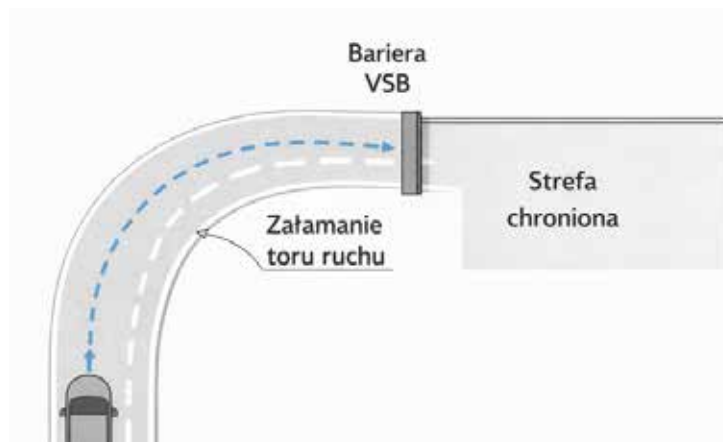


Rysunek 3. Schematy przedstawiające zastosowanie rozwiązania porządkowego oraz zastosowanie bariery pojazdowej VSB.

Źródło: opracowanie własne.

Błędne ustawienie urządzenia względem drogi dojazdowej

Jednym z istotnych błędów projektowych i instalacyjnych jest ustawienie urządzenia w geometrii nieodpowiadającej rzeczywistej drodze dojazdowej pojazdu. Ustawienie pod niewłaściwym kątem albo w osi nieodpowiadającej przewidywanemu torowi ruchu pojazdu może spowodować zmianę mechanizmu jego pracy i obniżenie skuteczności systemu. Nawet urządzenie o bardzo dobrych parametrach może nie zadziałać zgodnie z oczekiwaniem, jeżeli zostanie wprowadzone w układ przestrzenny odmienny od tego, dla którego projektowano scenariusz ochrony. Szczególnie korzystne z punktu widzenia ograniczania energii oddziaływania są te układy dróg dojazdowych, w których tor pojazdu zostaje załamany, np. pod kątem ok. 90° , a urządzenie jest zlokalizowane za skretem. Taka geometria automatycznie ogranicza możliwą prędkość pojazdu i czyni zabezpieczenie bardziej skutecznym (rysunek 4).



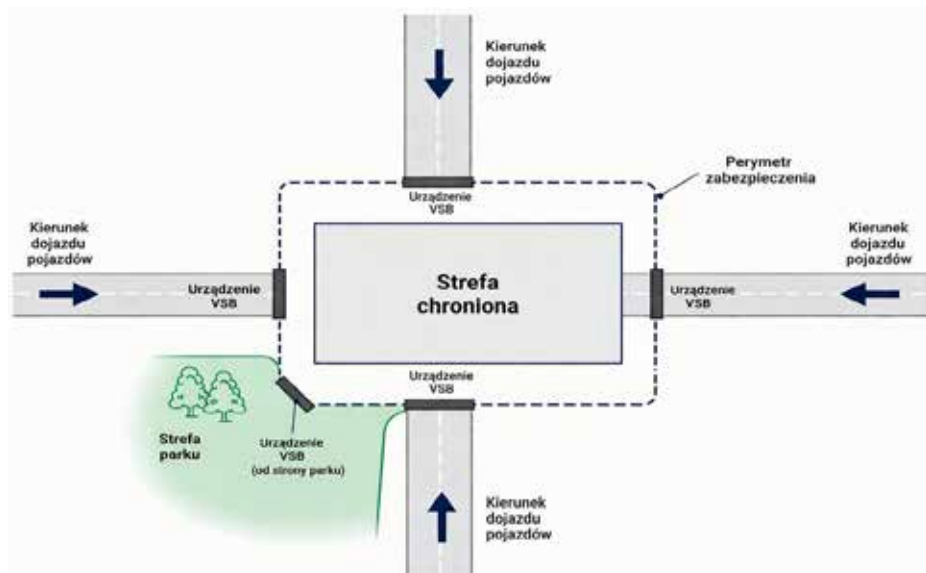
Rysunek 4. Schemat ustawienia bariery pojazdowej VSB za załamaniem toru ruchu pojazdu ograniczającym możliwość prostego najazdu w kierunku strefy chronionej.

Źródło: opracowanie własne.

Projektowanie ochrony tylko w osi głównych dróg dojazdowych

Jednym z najpoważniejszych błędów systemowych jest projektowanie ochrony wyłącznie w osi głównych dróg dojazdowych, przy jednoczesnym niezabezpieczeniu bocznych ciągów komunikacyjnych, chodników, przejść pieszych lub innych fragmentów przestrzeni. Skuteczne zabezpieczenie wydarzenia publicznego wymaga wyznaczenia pełnego perymetru

ochrony, czyli zewnętrznej linii ochrony wyznaczającej granicę strefy chronionej, oraz identyfikacji wszystkich potencjalnych osi dojazdu i dojazdu, także tych mniej oczywistych, wynikających z układu terenu, sąsiedztwa otwartych przestrzeni oraz możliwości przejazdu przez przyległe strefy zielone. Rysunek 5 przedstawia schemat perymetru ochrony terenu wydarzenia z zaznaczeniem kierunków dojazdu oraz lokalizacji barier pojazdowych VSB, w tym bariery usytuowanej na styku ze strefą parku.



Rysunek 5. Schemat perymetru ochrony terenu wydarzenia z zaznaczeniem kierunków dojazdu oraz lokalizacji barier pojazdowych VSB, w tym bariery na styku ze strefą parku.

Źródło: opracowanie własne.

W systemach HVM skuteczność zabezpieczenia zależy od jego ciągłości i spójności. Pojedyncze urządzenia ustawione w miejscach najbardziej oczywistych nie tworzą jeszcze systemu ochrony, jeżeli przestrzeń jako całość pozostaje możliwa do sforsowania z innego kierunku. Ochrona musi być oceniana w skali całego perymetru, a nie tylko przez pryzmat wybranych punktów.

Montaż na nieodpowiednim podłożu

Częstym błędem jest instalacja urządzenia na podłożu, które nie odpowiada warunkom przewidzianym dla jego prawidłowej pracy. W przypadku

rozwiązań tymczasowych lub mobilnych rodzaj nawierzchni ma bezpośredni wpływ na stabilność systemu, warunki tarcia oraz sposób przenoszenia obciążeń dynamicznych podczas uderzenia.

Różnica między nawierzchnią przewidzianą przez producenta a nawierzchnią faktycznie występującą w miejscu instalacji może prowadzić do istotnej zmiany działania urządzenia, co bywa bagatelizowane.

Błędy połączeń w układach modułowych

W systemach modułowych skuteczność zabezpieczenia wynika z pracy całego układu jako spójnego systemu. Jednym z poważnych błędów instalacyjnych jest brak właściwego połączenia segmentów albo zastosowanie niepełnego układu montażowego przewidzianego przez producenta. W takich przypadkach może dojść do utraty ciągłości pracy systemu, przemieszczenia sąsiednich elementów albo wystąpienia efektu domina. Awaria jednego segmentu może się przenieść na cały układ i prowadzić do obniżenia skuteczności zabezpieczenia w stopniu znacznie większym, niż wynikałoby to z oceny pojedynczego elementu.

W przypadku wydarzeń publicznych problem ten jest szczególnie wyraźny, ponieważ punkty dostaw, bramy techniczne, zaplecze sceniczne, strefy cateringu, przejazdu dla obsługi, montaż przed rozpoczęciem wydarzenia oraz demontaż po jego zakończeniu tworzą okresy podwyższonej podatności. Konieczne jest wówczas stosowanie ścisłych procedur kontroli wjazdu, czasowego zamykania przejazdów, nadzoru służb porządkowych oraz jednoznacznego przypisania odpowiedzialności za przywrócenie ciągłości zabezpieczenia po każdym czasowym otwarciu perymetru.

Brak właściwej strefy buforowej i nieuwzględnienie penetracji

Zlokalizowanie przestrzeni przeznaczonej dla uczestników wydarzenia zbyt blisko linii barier pojazdowych VSB jest istotnym błędem projektowym. Za linią zabezpieczenia konieczne jest wyznaczenie strefy buforowej. Pomijanie penetracji prowadzi do błędnego przekonania, że sama obecność urządzenia rozwiązuje problem bezpieczeństwa. Tymczasem pojazd może wtargnąć częściowo za linię ochrony, a skutki zdarzenia mogą obejmować przemieszczenie fragmentów konstrukcji lub elementów pojazdu. Z tego względu strefa buforowa jest jednym z podstawowych warunków skutecznej ochrony.

Brak ciągłości zabezpieczenia w punktach dostaw, serwisowych i ewakuacyjnych

Jednym z najczęstszych błędów operacyjnych jest niezapewnienie ciągłości systemu ochrony w miejscach takich jak wjazdy techniczne, punkty dostaw, przejazdy serwisowe, drogi służb ratunkowych oraz przejazdy awaryjne. Każde czasowe otwarcie przejazdu oznacza okres podwyższonej podatności, który musi zostać odpowiednio rozpoznany i zarządzony.

Te miejsca stanowią często najsłabsze ogniwo całego systemu. Jeżeli ochrona koncentruje się wyłącznie na głównym perymetrze, a punkty operacyjne pozostają słabo kontrolowane, dochodzi do sytuacji, w której zabezpieczenie jest nieszczelne.

Czynnik ludzki, nieodpowiednie kompetencje zespołów montażowych i niewłaściwy nadzór operacyjny

Źródłem ryzyka, na które trzeba zwrócić szczególną uwagę, jest czynnik ludzki. Żaden system nie będzie działał właściwie, jeśli jego montaż zostanie wykonany nieprawidłowo, bez odpowiedniego nadzoru i bez znajomości wymagań technicznych. Dotyczy to zarówno błędów stricte instalacyjnych, jak i niewłaściwej eksploatacji urządzeń w trakcie wydarzenia. Z tego względu ochrona oparta na barierach pojazdowych VSB wymaga zaangażowania kompetentnych zespołów montażowych, jasnego podziału odpowiedzialności oraz realnego nadzoru operacyjnego. W przeciwnym razie nawet dobrze zaprojektowany system pozostaje podatny na błędy wykonawcze i organizacyjne.

Mała architektura i urządzenia porządkowe jako pozorne zabezpieczenia

W wielu miastach można zauważyć wykorzystywanie elementów małej architektury, takich jak betonowe donice, słupki, dekoracyjne bloki czy inne przeszkody urbanistyczne, jako środków mających ograniczać wjazd pojazdów do stref pieszych. Rozwiązania tego typu mogą pełnić funkcję organizacyjną lub porządkową, ale w większości przypadków nie stanowią barier pojazdowych VSB (zdjęcie 4).



Zdjęcie 4. Barierki – zabezpieczenie porządkowe niebędące barierą pojazdową VSB (Berlin).

Źródło: archiwum autora.

Obecność fizycznej przeszkody, samochodu osobowego albo autobusu, zbiorników typu IBC, lekkich donic itp. bywa błędnie utożsamiana z istnieniem realnego zabezpieczenia (zdjęcie 5). Takie rozwiązania mogą czasowo ograniczać dostęp organizacyjny, porządkować przestrzeń albo wymuszać redukcję prędkości, lecz nie stanowią certyfikowanej bariery pojazdowej VSB i nie zapewniają przewidywalnych parametrów przejścia energii uderzenia pojazdu o większej masie. Tymczasem bez potwierdzonych parametrów badawczych, bez właściwej konfiguracji oraz bez odniesienia do konkretnego scenariusza zagrożenia takie elementy stwarzają jedynie iluzję bezpieczeństwa²².



Zdjęcie 5. Pojemnik typu IBC – element porządkowy niebędący barierą pojazdową VSB (Polska).

Źródło: archiwum autora.

²² Por. J. Jaźwiński, *Ochrona antyterrorystyczna obiektów...*, s. 127–129; M. Cichomski, *Jak samorządy mogą chronić przestrzeń publiczną...*, s. 216–224.

Ciężkie bloki betonowe (bariery) lub certyfikowane donice o znacznej masie własnej mogą stanowić element systemu tymczasowego, ale tylko wtedy, gdy ich działanie i sposób instalacji odpowiadają przyjętemu scenariuszowi zagrożenia. Nie powinny być jednak utożsamiane z certyfikowanymi barierami pojazdowymi VSB (zdjęcia 6, 7).



Zdjęcie 6. Donice – elementy małej architektury o funkcji porządkowej lub potencjalnie ochronnej. Ich kwalifikacja jako barier pojazdowych VSB zależy od certyfikacji i scenariusza zastosowania (Rzym).

Źródło: archiwum autora.



Zdjęcie 7. Bariery betonowe – rozwiązanie o funkcji porządkowej lub potencjalnie ochronnej. Ich kwalifikacja jako barier pojazdowych VSB zależy od certyfikacji i scenariusza zastosowania (Paryż).

Źródło: archiwum autora.

Wnioski z analizy błędów w stosowaniu barier pojazdowych VSB

Analiza błędów projektowych, instalacyjnych i operacyjnych prowadzi do jednoznacznego wniosku, że skuteczność systemów HVM zależy nie tylko od parametrów samych barier pojazdowych VSB, lecz przede wszystkim od jakości całego procesu projektowania, montażu i użytkowania systemu. Oznacza to, że nawet certyfikowane i poprawnie przebadane urządzenie nie gwarantuje właściwego poziomu ochrony, jeżeli zostanie źle dobrane, niewłaściwie ustawione, błędnie zainstalowane albo użyte w przestrzeni zaprojektowanej bez uwzględnienia rzeczywistego scenariusza zagrożenia.

Projektowanie systemów HVM w przestrzeniach publicznych

Projektowanie systemów HVM w przestrzeniach publicznych nie może polegać na ustawieniu pojedynczych barier pojazdowych VSB w miejscach intuicyjnie uznanych za niewrażliwe. Skuteczny system ochrony wymaga podejścia sekwencyjnego, w którym decyzje dotyczące doboru urządzeń, geometrii ich ustawienia, organizacji przestrzeni oraz sposobu użytkowania wynikają z wcześniej przeprowadzonych analiz ryzyka i miejsca. Zachowanie tej kolejności przesądza o różnicy między ochroną realną a pozorną.

Analiza ryzyka

Podstawowym etapem projektowania systemu zabezpieczenia przestrzeni publicznej przed atakiem z użyciem pojazdu powinna być analiza ryzyka, która stanowi punkt wyjścia do określenia rodzaju oraz parametrów barier pojazdowych VSB stosowanych w danej lokalizacji. Bez niej dobór urządzeń staje się działaniem intuicyjnym, nieodpowiadającym rzeczywistemu zagrożeniu.

Analiza ta powinna obejmować co najmniej: charakter chronionej przestrzeni, profil wydarzenia, przewidywaną liczbę uczestników, znaczenie symboliczne miejsca, możliwe scenariusze działania sprawcy, lokalne uwarunkowania komunikacyjne oraz potencjalne skutki wtargnięcia pojazdu. Dopiero zestawienie tych czynników pozwala przejść od ogólnego rozpoznania problemu do sformułowania konkretnych wymagań ochronnych²³.

²³ Por. J. Jaźwiński, *Ochrona antyterrorystyczna obiektów...*, s. 129-133; M. Cichomski, *Jak samorządy mogą chronić przestrzeń publiczną...*, s. 210-215.

Analiza drogi dojazdowej i scenariusza ataku z użyciem pojazdu

Infrastruktura drogowa umożliwia potencjalnemu sprawcy wykorzystanie pojazdu jako narzędzia ataku. Dlatego analiza dróg dojazdowych prowadzących do chronionej przestrzeni ma fundamentalne znaczenie dla projektowania barier pojazdowych VSB.

Na tym etapie należy określić, jakie pojazdy mogą zostać użyte w danej lokalizacji, z jaką prędkością mogą dotrzeć do strefy chronionej, z których kierunków mogą wtargnąć oraz jakie warunki terenowe wpływają na przebieg potencjalnego ataku. Projektowanie skutecznego systemu HVM wymaga bowiem nie abstrakcyjnego myślenia o „pojeździe”, lecz możliwie precyzyjnego określenia scenariusza ataku z jego wykorzystaniem.

Wyznaczenie strefy ochronnej i perymetru ochrony

Po analizie ryzyka i rozpoznaniu dróg dojazdowych jest konieczne wyznaczenie strefy ochronnej oraz określenie perymetru ochrony. Proces ten obejmuje rozmieszczenie barier pojazdowych VSB i organizację przestrzeni za linią zabezpieczenia. Z perspektywy bezpieczeństwa równie ważne jak ustawienie urządzeń jest to, co znajduje się za nimi i w jakiej odległości od przewidywanej strefy oddziaływania.

Wyznaczenie perymetru powinno być całościowe. Ochrona musi obejmować wszystkie realne kierunki wtargnięcia, z uwzględnieniem punktów technicznych, przejazdów awaryjnych, bocznych ciągów komunikacyjnych oraz wszelkich miejsc, które mogłyby zostać wykorzystane do obejścia głównej linii ochrony.

Dobór barier pojazdowych VSB do scenariusza zagrożenia

Dobór urządzeń służących do ochrony przed atakiem z użyciem pojazdu powinien wynikać bezpośrednio z przeprowadzonej analizy ryzyka oraz scenariusza zagrożenia. Nie istnieje uniwersalna bariera pojazdowa VSB odpowiednia dla wszystkich możliwych sytuacji. W praktyce projektowej jednym z częściej analizowanych scenariuszy pozostaje atak z użyciem pojazdu o masie ok. 7,5 t, poruszającym się z prędkością ok. 50 km/h i 64 km/h, w zależności od przyjętego standardu badawczego, klasyfikacji urządzenia oraz założeń projektowych. Jednak przywoływany model nie może być stosowany automatycznie we wszystkich lokalizacjach.

Dobór urządzenia musi uwzględniać parametry badawcze, rodzaj podłoża, charakter przestrzeni (np. rynek miejski, plac przed stadionem, strefa koncertowa, droga dojazdowa, zaplecze techniczne itp.), ograniczenia logistyczne, wymogi montażowe, potrzebę zachowania przejść

i dostępu dla służb oraz możliwość utrzymania ciągłości ochrony w czasie trwania wydarzenia.

Nadzór nad instalacją i odpowiedzialność organizacyjna

Przed dopuszczeniem tymczasowej instalacji barier VSB do użytkowania można ją sprawdzić według checklisty. Została ona opracowana na podstawie analizy problemów projektowych, instalacyjnych i operacyjnych omówionych w artykule, a także doświadczeń autora związanych z doborem i stosowaniem urządzeń zabezpieczających przed wtargnięciem pojazdu. Składają się na nią:

- zgodność zastosowanego urządzenia z przyjętym scenariuszem zagrożenia, zwłaszcza w zakresie rodzaju pojazdu, kierunku najazdu oraz przewidywanej prędkości;
- zgodność instalacji z konfiguracją *as tested*, jeżeli deklarowane parametry urządzenia odnoszą się do określonego układu montażowego, sposobu łączenia lub rodzaju podłoża;
- ocena stanu technicznego urządzeń oraz kompletności elementów systemu, w tym połączeń modułowych i elementów stabilizujących;
- weryfikacja rodzaju i nośności podłoża pod kątem warunków wymaganych dla prawidłowej pracy urządzenia;
- prawidłowość geometrii ustawienia urządzeń względem drogi dojazdowej, z uwzględnieniem osi najazdu, promieni skrętu oraz możliwości obejścia zabezpieczenia;
- sprawdzenie ciągłości linii ochrony, tak aby pomiędzy urządzeniami nie zostawiono prześwitów ani bocznych luk umożliwiających wtargnięcie pojazdu do strefy chronionej;
- wyznaczenie strefy buforowej za linią urządzeń, z uwzględnieniem przewidywanej penetracji pojazdu oraz możliwych wtórnych skutków zderzenia;
- ustalenie zasad funkcjonowania punktów dostaw, przejazdów technicznych i wjazdów awaryjnych, wraz z procedurą przywracania ciągłości zabezpieczenia po ich czasowym otwarciu;
- określenie procedur dla pojazdów uprawnionych oraz zapewnienie drożności tras dla służb ratowniczych i porządkowych przy jednoczesnym zachowaniu szczelności systemu ochrony;
- odbiór instalacji przez kompetentną osobę, połączony z potwierdzeniem gotowości operacyjnej systemu przed rozpoczęciem wydarzenia.

W realizacjach powtarzalnych checklista powinna być uzupełniana o obowiązek krótkiego instruktażu dla ekip technicznych oraz o potwierdzenie odbioru przez kompetentną osobę po stronie organizatora lub właściciela przestrzeni. Taki zabieg ogranicza ryzyko błędu ludzkiego i pomaga utrzymać zgodność instalacji z założeniami projektowymi.

Przykład przygotowania i szkoleniowego rozstawienia barier tymczasowych przed wydarzeniem publicznym przedstawiono na zdjęciu 8.



Zdjęcie 8. Rozstawianie barier tymczasowych podczas przygotowania zabezpieczenia wydarzenia publicznego oraz próbne rozstawienie barier (Warszawa).

Źródło: materiały DFE Security sp. z o.o.

Nawet najlepiej dobrane urządzenie nie zapewni właściwego poziomu ochrony, jeżeli zostanie nieprawidłowo zainstalowane. Z tego względu projektowanie systemu HVM powinno obejmować dobór urządzeń oraz organizację procesu ich montażu, odbioru oraz nadzoru operacyjnego.

W Europie spotyka się model, w którym wyspecjalizowane podmioty zajmują się zarówno doбором, jak i instalacją systemów ochrony przestrzeni publicznych przed atakiem z użyciem pojazdu. Takie rozwiązania przyjęto w Wielkiej Brytanii, gdzie systemowe podejście do ochrony przestrzeni publicznych jest wspierane przez rozwój regulacji prawnych związanych z Martyn's Law. Wniosek jest jednoznaczny – skuteczny system wymaga nie tylko urządzeń, lecz także kompetentnego procesu ich wdrożenia.

Ochrona strefowa i warstwowa

Odpowiednią efektywność systemu HVM zapewnia podejście określane jako ochrona strefowa lub warstwowa (ang. *layered security*). Oznacza ono projektowanie bezpieczeństwa w taki sposób, aby ewentualne przełamanie jednego poziomu ochrony nie prowadziło automatycznie do pełnego otwarcia dostępu do strefy chronionej.

Ochrona warstwowa może obejmować m.in. połączenie barier pojazdowych VSB, rozwiązań urbanistycznych, kontroli dostępu, organizacji ruchu, nadzoru operacyjnego oraz odpowiedniego kształtowania stref buforowych. Przewaga tego systemu polega na tym, że rozkłada bezpieczeństwo z jednej linii obrony na sekwencję uzupełniających się środków.

Śluzы ewakuacyjne i kontrolowane przejazdy w układach stałym i tymczasowym

Jednym z bardziej dojrzałych modeli ochrony przestrzeni publicznych podczas wydarzeń publicznych jest rozwiązanie systemowe, w którym zabezpieczenia stałe i tymczasowe wzajemnie się uzupełniają. Taki model może być stosowany zwłaszcza w centrach miast, na głównych ulicach i placach, gdzie na co dzień odbywa się zwykły ruch pojazdów, w okresie wydarzenia konieczne natomiast staje się czasowe przejęcie kontroli nad dostępem do strefy chronionej.

To rozwiązanie polega na tym, że główne osie dojazdowe do strefy wydarzenia są wyposażone w stałe i automatyczne bariery pojazdowe, które poza czasem wydarzenia mogą być opuszczone i umożliwiać normalny ruch drogowy. W momencie uruchomienia procedur związanych z wydarzeniem bariery są podnoszone i przejmują funkcję zasadniczej ochrony głównego ciągu komunikacyjnego. Jednocześnie boczne ulice, przejścia techniczne i inne potencjalne kierunki obejścia zabezpiecza się dodatkowymi rozwiązaniami tymczasowymi, tak aby zachować ciągłość ochrony całej strefy.

Szczególne znaczenie ma tu rozwiązanie w formie śluzы, rozumianej jako kontrolowany punkt przejazdowy dla pojazdów uprawnionych (zdjęcie 9). W takim układzie pojazd wjeżdża najpierw do wydzielonej strefy pomiędzy kolejnymi liniami zabezpieczenia. Po zamknięciu pierwszego odcinka bariery może zostać zatrzymany, zweryfikowany i poddany kontroli zgodnej z planem ochrony. Dopiero po potwierdzeniu uprawnień jest otwierany kolejny odcinek przejazdu. To rozwiązanie pozwala na jednocześnie utrzymanie szczelności perymetru, bezpieczne prowadzenie ewakuacji, przejazd służb porządkowych i ratowniczych, a także realizację procedur kontroli pojazdów wjeżdżających do strefy wydarzenia. Zaletą takiego modelu jest elastyczność i komplementarność. To samo miejsce

może funkcjonować w dwóch trybach: codziennego użytkowania oraz czasowej ochrony wydarzenia.



Zdjęcie 9. Rozwiązanie w formie służby w układzie miejskim – kontrolowany punkt przejazdu i separacji ruchu (Berlin).

Źródło: archiwum autora.

Z punktu widzenia projektowania bezpieczeństwa model służbowy jest szczególnie wartościowy, ponieważ łączy wymóg odporności infrastrukturalnej z potrzebą zachowania drożności ewakuacyjnej, możliwości przejazdu służb i kontroli dostępu. Takie rozwiązania uwiadcniają, że skuteczny system HVM nie polega wyłącznie na ustawieniu pojedynczej bariery, lecz na świadomym zaprojektowaniu całego modelu działania przestrzeni w warunkach wydarzenia (zdjęcie 10).



Zdjęcie 10. Bariery pojazdowe VSB – rozwiązanie stałe współgrające z organizacją ruchu i ochroną przestrzeni publicznej (Frankfurt).

Źródło: archiwum autora.

Security by design w planowaniu przestrzeni publicznych

Coraz większe znaczenie w projektowaniu ochrony przestrzeni publicznych ma podejście *security by design*, zakładające uwzględnianie aspektów bezpieczeństwa już na etapie planowania urbanistycznego lub organizacji przestrzeni wydarzeń. W takim modelu, rozwijanym na poziomie europejskim, ochrona nie jest dodatkiem wprowadzanym po fakcie, lecz elementem projektu przestrzeni²⁴. Im wcześniej wymagania bezpieczeństwa zostaną uwzględnione, tym większa jest możliwość ich harmonijnego połączenia z funkcjonalnością przestrzeni, estetyką miejsca oraz potrzebami użytkowników. W kontekście systemu HVM oznacza to możliwość takiego kształtowania układu przestrzennego, aby ograniczać podatność na wtargnięcie pojazdu, zanim zajdzie taka doraźna potrzeba. Przykłady barier pojazdowych VSB zintegrowanych z przestrzenią publiczną przedstawiono na zdjęciach 11 i 12.



Zdjęcie 11. Bariery pojazdowe VSB uruchamiane manualnie – rozwiązanie zintegrowane z przestrzenią publiczną.

Źródło: Unafor. *Certified Hostile Vehicle Mitigation with Design in Mind*, Crowdguard, <https://www.crowdguard.co.uk/products/unafor/> [dostęp: 29 III 2026].

²⁴ Por. *Protection of public spaces...*; *Protection*, European Commission, 23 IX 2024 r., https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection_en [dostęp: 12 IV 2026]; *EU Protective Security Advisors (EU PSA)*, European Commission, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [dostęp: 12 IV 2026].



Zdjęcie 12. Tymczasowe mobilne bariery pojazdowe VSB – rozwiązanie zintegrowane z przestrzenią publiczną.

Źródło: *ATG Surface Guard*, Crowdguard, <https://www.crowdguard.co.uk/products/atg-surface-guard/> [dostęp: 29 III 2026].

Rekomendacje końcowe dla projektowania systemów HVM

Przy projektowaniu systemów HVM wskazane jest zastosowanie się do kilku zasad. Po pierwsze, punktem wyjścia zawsze powinna być analiza ryzyka, a nie wybór urządzenia. Ochrona projektowana od strony produktu, bez uprzedniego rozpoznania scenariusza zagrożenia niemal zawsze prowadzi do niedopasowania środków do rzeczywistej podatności miejsca. Decyzje zakupowe lub dotyczące wynajmu powinny być wtórne wobec wniosków z analizy.

Po drugie, niezbędna jest szczegółowa analiza wszystkich dróg dojazdowych i realnych kierunków wtargnięcia pojazdu. Projektowanie ochrony jedynie dla głównego wjazdu tworzy zabezpieczenie częściowe, a przez to podatne na obejście. W odniesieniu do każdego wydarzenia perymetr powinien być oceniany jako całość, wraz z drogami serwisowymi, pieszymi i technicznymi.

Po trzecie, dobór barier pojazdowych VSB powinien wynikać z konkretnego scenariusza zagrożenia, a nie z deklaracji marketingowych. Kluczowe znaczenie mają parametry badawcze, konfiguracja *as tested*, warunki montażu oraz zgodność urządzenia z rzeczywistym układem przestrzennym. Produkt nieprzystający do miejsca i scenariusza nie tworzy skutecznego zabezpieczenia, nawet jeżeli sam w sobie ma wysoką klasę badawczą.

Po czwarte, projektowanie ochrony musi uwzględniać penetrację pojazdu i tym samym konieczność wyznaczenia strefy buforowej. Bezpieczna przestrzeń nie zaczyna się w osi urządzenia, lecz dopiero za obszarem możliwego oddziaływania pojazdu, jego fragmentów i odłamków. Pominiecie tego aspektu prowadzi do mylnego przeświadczenia o poziomie bezpieczeństwa.

Po piąte, skuteczny system powinien być warstwowy, przestrzennie spójny i objęty nadzorem operacyjnym. Ochrona nie może opierać się na jednym środku ani na jednym punkcie decyzyjnym. Wysoki poziom bezpieczeństwa osiąga się przez połączenie infrastruktury, procedur, kompetencji ludzi i właściwej organizacji przestrzeni²⁵.

Po szóste, większe znaczenie powinno mieć uwzględnianie zasad *security by design* w planowaniu przestrzeni publicznych i wydarzeń. Im wcześniej wymagania bezpieczeństwa zostaną wpisane w projekt miejsca lub organizację wydarzenia, tym mniejsza będzie potrzeba stosowania rozwiązań tymczasowych. Długofalowo jest to kierunek bardziej skuteczny, ekonomiczny i spójny z nowoczesnym podejściem do zarządzania ryzykiem.

Odpowiedzialność samorządów za bezpieczeństwo przestrzeni publicznych w Polsce

W polskich warunkach szczególna odpowiedzialność za rozwój systemowych mechanizmów ochrony przestrzeni publicznych spoczywa na samorządach terytorialnych. To one odpowiadają za organizację wielu wydarzeń, zarządzanie przestrzenią oraz planowanie wydatków związanych z bezpieczeństwem. Z tego względu samorzady nie powinny ograniczać się do reagowania na bieżące potrzeby organizacyjne, lecz tworzyć trwałe standardy HVM/VSB dla wydarzeń powtarzalnych, planować budżety z wyprzedzeniem oraz korzystać z wiedzy wyspecjalizowanych konsultantów²⁶. Na poziomie samorządowym może nastąpić instytucjonalizacja tych zagadnień.

Bez zaangażowania samorządów ochrona przestrzeni publicznych będzie nadal rozwijać się w sposób rozproszony, reaktywny i zależny

²⁵ Zob. *HVM specifying – some things to consider*, HVMhub, <https://hvmhub.com/products-advice/spec-writing-guidance/> [dostęp: 29 III 2026].

²⁶ Zob. M. Cichomski, *Jak samorzady mogą chronić przestrzenie publiczne...*, s. 206–208, 223–224.

od incydentalnych decyzji organizacyjnych. Z punktu widzenia bezpieczeństwa publicznego jest to model niewystarczający.

Istotne znaczenie ma również dobór podmiotów uczestniczących w projektowaniu, dostawie, instalacji i obsłudze systemów HVM i barier pojazdowych VSB. W odniesieniu do infrastruktury związanej z bezpieczeństwem publicznym zasadne jest korzystanie z podmiotów ze stosownymi uprawnieniami, w tym koncesją Ministerstwa Spraw Wewnętrznych i Administracji, a w przypadkach obejmujących dostęp do informacji wrażliwych dotyczących organizacji ochrony, konfiguracji systemu, procedur działania lub identyfikacji podatności – także odpowiednie gwarancje w zakresie ochrony informacji niejawnych²⁷. W szczególnych sytuacjach może to oznaczać konieczność posiadania świadectwa bezpieczeństwa przemysłowego, wydawanego przez Agencję Bezpieczeństwa Wewnętrznego. Ujawnienie danych dotyczących sposobu działania systemu, jego organizacji lub błędów instalacyjnych osobom nieuprawnionym może bowiem obniżać skuteczność ochrony i zwiększać podatność przestrzeni publicznej na obejście zabezpieczeń.

Podsumowanie

Najważniejszym wnioskiem płynącym z artykułu jest to, że ochrona przestrzeni publicznych przed atakiem z użyciem pojazdu wymaga podejścia systemowego. Nie może ona opierać się na incydentalnym ustawieniu pojedynczych urządzeń ani na stosowaniu rozwiązań o charakterze wyłącznie porządkowym. Skuteczność systemu zależy bowiem od połączenia analizy ryzyka, prawidłowego rozpoznania dróg dojazdowych, właściwego doboru barier pojazdowych VSB, poprawnej instalacji, zachowania ciągłości ochrony w całej przestrzeni objętej zabezpieczeniem oraz od realnego nadzoru operacyjnego.

Problem ochrony przestrzeni publicznych przed atakiem z użyciem pojazdu wymaga w Polsce dalszego uporządkowania zarówno na poziomie rozpoznania zagrożenia, jak i zasad doboru, instalacji oraz użytkowania

²⁷ Zob. *Ochrona informacji niejawnych*, Agencja Bezpieczeństwa Wewnętrznego, <https://www.abw.gov.pl/pl/o-abw/zadania/7,Ochrona-informacji-niejawnych.html> [dostęp: 4 V 2026]; *Bezpieczeństwo przemysłowe*, <https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-przemys/148%20CBEZPIECZENSTWO-PRZEMYSLOWE.pdf> [dostęp: 4 V 2026].

barier pojazdowych VSB w ramach systemów HVM. Dotyczy to w szczególności potrzeby szerszego stosowania zabezpieczeń opartych na parametrach badawczych, standardach technicznych i realistycznych scenariuszach zagrożenia. Do najistotniejszych problemów należy zaliczyć niedostateczne planowanie środków finansowych przeznaczanych na ochronę przestrzeni publicznych, stosowanie zabezpieczeń porządkowych zamiast certyfikowanych urządzeń ochronnych oraz dobór rozwiązań bez odniesienia do parametrów pojazdu, energii uderzenia i rzeczywistej funkcji barier pojazdowych VSB.

Za najpoważniejsze błędy techniczne można uznać pozostawianie bocznych dróg dojazdowych, stosowanie urządzeń porządkowych zamiast barier pojazdowych VSB, nieuwzględnienie penetracji oraz koniecznej strefy buforowej, a także brak ciągłości systemu w punktach technicznych i serwisowych. Błędy te mają charakter strukturalny, ponieważ wynikają nie tylko z niedostatku sprzętu, lecz przede wszystkim z niewłaściwego rozpoznania zagrożenia i powierzchownego podejścia do ochrony.

W tym kontekście należy przywołać zdarzenie w Sopocie z lipca 2014 r., kiedy kierowca wjechał samochodem na ul. Bohaterów Monte Casino, a następnie na molo, i spowodował obrażenia u wielu osób. Akt ten nie miał charakteru terrorystycznego, jednak potwierdza on, że zagrożenie związane z użyciem pojazdu w przestrzeni publicznej powinno być traktowane poważnie także w polskich realiach²⁸.

W wymiarze organizacyjnym zasadne jest wdrożenie stałych standardów HVM/VSB dla wydarzeń cyklicznych, korzystanie z wiedzy wyspecjalizowanych konsultantów lub podmiotów mających kompetencje w zakresie projektowania i instalacji barier pojazdowych VSB oraz planowanie budżetu na zabezpieczenia z odpowiednim wyprzedzeniem. Bez takich działań ochrona będzie nadal pozostawać zależna od doraźnych decyzji, a nie od spójnej polityki bezpieczeństwa²⁹.

W ujęciu porównawczym można stwierdzić, że Polska znajduje się obecnie na etapie przejściowym. Ochrona przestrzeni publicznych przed atakiem z użyciem pojazdu jest coraz lepiej rozpoznawana, jednak nadal nie rozwija się w sposób systemowy. Z tego względu zasadne pozostaje

²⁸ Por. *Szałeńczy rajd w Sopocie. Kierowca wjechał w grupę ludzi*, RMF24, 20 VII 2014 r., <https://www.rmfm24.pl/news-szalenczy-rajd-w-sopocie-kierowca-wjechał-w-grupe-ludzi,-nId,1471791> [dostęp: 12 IV 2026].

²⁹ Por. M. Cichomski, *Jak samorządy mogą chronić przestrzenie publiczne...*, s. 203–208; J. Jaźwiński, *Ochrona antyterrorystyczna obiektów...*, s. 168–169.

korzystanie z doświadczeń państw, które wcześniej zetknęły się z tego rodzaju zagrożeniami i wypracowały bardziej dojrzałe rozwiązania prawne, organizacyjne i techniczne, zwłaszcza Wielkiej Brytanii, Niemiec oraz Francji.

Szczególna waga tego zagadnienia wynika z tego, że dotyczy ono nie infrastruktury zamkniętej ani wyłącznie obiektów o znaczeniu strategicznym, lecz przestrzeni publicznych, z których korzystają uczestnicy życia społecznego. Każda osoba biorąca udział w koncercie, jarmarku, wydarzeniu sportowym, uroczystości religijnej czy zgromadzeniu na otwartej przestrzeni może znaleźć się w obszarze potencjalnego oddziaływania tego rodzaju zagrożenia.

Bibliografia

Cichomski M., *Jak samorządy mogą chronić przestrzenie publiczne przed atakami z użyciem pojazdów?*, „Terroryzm – studia, analizy, prewencja” 2025, nr 8, s. 203–233. <https://doi.org/10.4467/27204383TER.25.051.23038>.

Hess P., Mandhan S., *Ramming attacks, pedestrians, and the securitization of streets and urban public space: a case study of New York City*, „Urban Design International” 2022, t. 28, nr 1, s. 19–34. <https://doi.org/10.1057/s41289-022-00180-2>.

Jażwiński J., *Ochrona antyterrorystyczna obiektów użyteczności publicznej oraz infrastruktury krytycznej przed atakami z wykorzystaniem pojazdów mechanicznych*, „Terroryzm – studia, analizy, prewencja” 2023, nr 3, s. 120–171. <https://doi.org/10.4467/27204383TER.23.004.17444>.

Karlos V., Larcher M., Solomos G., *Review on vehicle barrier protection guidance*, Publications Office of the European Union, European Commission, Joint Research Centre, 2017. <https://doi.org/10.2760/845599>.

Ludbey C.R., Versaci D., Bharthur S., Prabhakaran S., *Classifying vehicle-as-a-weapon attacks: an inductive taxonomy and design implications*, „Crime Science” 2026, t. 15, art. 2. <https://doi.org/10.1186/s40163-025-00265-7>.

Miller V., Hayward K.J., *‘I Did My Bit’: Terrorism, Tarde and the Vehicle Ramming Attack as an Imitative Event*, „The British Journal of Criminology” 2019, t. 59, nr 1, s. 1–23. <https://doi.org/10.1093/bjc/azy017>.

Phillips J.P., Young J.S., Brady W.J., *Preparation and response to a targeted automobile ramming mass casualty (TARMAC) attack: An analysis of the 2017 Charlottesville, Virginia TARMAC attack*, „American Journal of Disaster Medicine” 2019, t. 14, nr 3, s. 219–223. <https://doi.org/10.5055/ajdm.2019.0333>.

Tsur A.M., Nadler R., Sorkin A., Lipkin I., Gelikas S., Chen J., Benov A., *Patterns in vehicle-ramming attacks*, „Israel Medical Association Journal” 2022, t. 24, nr 9, s. 579–583.

Źródła internetowe

ATG Surface Guard, Crowdguard, <https://www.crowdguard.co.uk/products/atg-surface-guard/> [dostęp: 29 III 2026].

Bezpieczeństwo przemysłowe, <https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-przemys/148%2CBEZPIECZENSTWO-PRZEMYSLOWE.pdf> [dostęp: 4 V 2026].

EU Protective Security Advisors (EU PSA), European Commission, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [dostęp: 12 IV 2026].

Hostile Vehicle Guidelines for Crowded Places, <https://www.nationalsecurity.gov.au/crowded-places-subsite/Files/hostile-vehicle-guidelines-crowded-places.pdf> [dostęp: 20 VI 2026].

Hostile Vehicle Mitigation ISO 22343-1:2023 NPSA Guidance Note, <https://www.npsa.gov.uk/system/files/documents/npsa-hvm-guidance-note-iso-22343-1-feb-2024.pdf> [dostęp: 12 IV 2026].

HVM – Vehicle Impact Testing and FEA Computational Analysis Guidance Note, <https://www.npsa.gov.uk/system/files/documents/npsa-guidance-note-hvm-vehicle-impact-testing-and-fea-computational-analysis-15-july-2021.pdf> [dostęp: 29 III 2026].

HVM specifying – some things to consider, HVMhub, <https://hvmhub.com/products-advice/spec-writing-guidance/> [dostęp: 29 III 2026].

Impact Testing of Vehicle Security Barriers. An overview of vehicle impact test standards, <https://www.npsa.gov.uk/system/files/documents/npsa-impact-testing-of-vehicle-security-barriers-18-august-2020.pdf> [dostęp: 29 III 2026].

Martyn's Law: the SIA's New Regulatory Role, Security Industry Authority, <https://www.gov.uk/government/publications/martyns-law-the-sias-new-regulatory-role/martyns-law-the-sias-new-regulatory-role> [dostęp: 12 IV 2026].

Ochrona informacji niejawnych, Agencja Bezpieczeństwa Wewnętrznego, <https://www.abw.gov.pl/pl/o-abw/zadania/7,Ochrona-informacji-niejawnych.html> [dostęp: 4 V 2026].

Poprawiamy bezpieczeństwo w stolicy. Rozstawiamy bariery antyterrorystyczne i szkolimy z ich obsługi, Zarząd Dróg Miejskich w Warszawie, 17 III 2026 r., <https://zdm.waw.pl/aktualnosci/poprawiamy-bezpieczenstwo-w-stolicy-rozstawiamy-bariery-antyterrorystyczne-i-szkolimy-z-ich-obslugi/> [dostęp: 12 IV 2026].

Primer on Impact Protection for Critical Transportation Infrastructure, FHWA-HIF-18-054, Federal Highway Administration, 2018 r., <https://www.fhwa.dot.gov/bridge/security/hif18054.pdf> [dostęp: 15 VI 2026].

Protection of public spaces from terrorist attacks, European Commission, Joint Research Centre, https://joint-research-centre.ec.europa.eu/projects-and-activities/protection-public-spaces-terrorist-attacks_en [dostęp: 12 IV 2026].

Protection, European Commission, 23 IX 2024 r., https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection_en [dostęp: 12 IV 2026].

Public Realm Design Guide for Hostile Vehicle Mitigation, National Protective Security Authority, <https://www.npsa.gov.uk/specialised-guidance/hostile-vehicle-mitigation-hvm/public-realm-design-guide-hostile-vehicle-mitigation-0> [dostęp: 12 IV 2026].

Schutz öffentlicher Räume vor Überfahrtaten, Polizeiliche Kriminalprävention der Länder und des Bundes, <https://www.polizei-beratung.de/themen-und-tipps/staedtebau/schutz-vor-ueberfahrtaten/> [dostęp: 12 IV 2026].

Se protéger contre les attaques au véhicule-bélier, Secrétariat général de la défense et de la sécurité nationale, 11 VI 2018 r. <https://www.sgdsn.gouv.fr/publications/se-proteger-contre-les-attaques-au-vehicule-belier> [dostęp: 12 IV 2026].

Szaleńczy rajd w Sopocie. Kierowca wjechał w grupę ludzi, RMF24, 20 VII 2014 r., <https://www.rmfm24.pl/news-szalenczy-rajd-w-sopocie-kierowca-wjechał-w-grupe-ludzi,nId,1471791> [dostęp: 12 IV 2026].

Unafor. Certified Hostile Vehicle Mitigation with Design in Mind, Crowdguard, <https://www.crowdguard.co.uk/products/unafor/> [dostęp: 29 III 2026].

Vehicle Ramming Action Guide, Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide> [dostęp: 20 VI 2026].

Verifying solutions, HVMhub, <https://hvmhub.com/products-advice/verifying-solutions/> [dostęp: 29 III 2026].

Akty prawne

Terrorism (Protection of Premises) Act 2025, UK Public General Acts 2025 c. 10, <https://www.legislation.gov.uk/ukpga/2025/10/contents> [dostęp: 12 IV 2026].

Normy i standardy

ASTM F2656/F2656M-20 Standard Test Method for Crash Testing of Vehicle Security Barriers, https://store.astm.org/f2656_f2656m-20.html [dostęp: 20 VI 2026].

British Standards Institution, PAS 68:2013 Impact test specifications for vehicle security barrier systems, <https://knowledge.bsigroup.com/products/impact-test-specifications-for-vehicle-security-barrier-systems> [dostęp: 12 IV 2026].

ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating, <https://www.iso.org/standard/50080.html> [dostęp: 12 IV 2026].

ISO 22343-2:2023 Security and resilience – Vehicle security barriers – Part 2: Application, <https://www.iso.org/standard/81415.html> [dostęp: 20 VI 2026].

IWA 14-1:2013 Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating.

PN-EN 1317 Systemy ograniczające drogę.

Jarosław Jaźwiński

Specjalista w obszarze zabezpieczeń technicznych i antyterrorystycznych, szczególnie ochrony przestrzeni publicznych, imprez masowych oraz infrastruktury przed atakami z użyciem pojazdu. Rzecznik Polskiej Izby Ochrony i Polskiego Związku Pracodawców Ochrona, prelegent konferencji branżowych i naukowych. Autor publikacji poświęconych ochronie antyterrorystycznej obiektów użyteczności publicznej.

Kontakt: jarek.j@dfes.pl



VARIA



System ochrony lotnictwa cywilnego jako przykład wzmocnienia odporności infrastruktury krytycznej

Karol Dymek

Autor niezależny

 <https://orcid.org/0009-0004-3946-8695>

Wprowadzenie

Po kilkunastu latach pracy w obszarze ochrony lotnictwa cywilnego na różnych szczeblach podmiotu prowadzącego lub nadzorującego działalność lotniczą, w tym jako audytor kontroli jakości na poziomie europejskim i krajowym, przekonałem się, że nie istnieją rozwiązania zapewniające stuprocentową ochronę. Dynamika zmian we współczesnym świecie sprzyja kształtowaniu się nowych zagrożeń i kierunków, z których one przychodzą. W mediach coraz częściej pojawiają się informacje o zagrożeniach dla bankowości elektronicznej, o włamaniach do kont w mediach społecznościowych w celu szerzenia dezinformacji w związku z wojną w Ukrainie, o pożarach, np. w centrach handlowych¹, czy zapalających się

¹ 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: 15 III 2026].

przesyłkach kurierskich². Branża lotnicza, która uchodzi za jedną z najbezpieczniejszych gałęzi transportu, mimo wysokiego poziomu regulacji i wielu procedur ochrony, nie jest wolna od zagrażających jej incydentów. Należy przy tym pamiętać, że przewoźnicy lotniczy i lotniska są częścią infrastruktury krytycznej (IK). W lotnictwie funkcjonuje wiele wyspecjalizowanych grup zawodowych, których zadaniem jest zapewnienie sprawnego i bezpiecznego działania całego systemu. Aby to było możliwe, działalność lotnicza podlega ścisłym regulacjom prawnym, licznym zasadom i procedurom.

W środowisku mówi się, że przepisy lotnicze w większości są krwią pisane. Wydarzeniem, które zmieniło współczesny świat i w dużej mierze wpłynęło na podejście do ochrony lotnictwa cywilnego, był zamach na World Trade Center przeprowadzony 11 września 2001 r.³

W lotnictwie cywilnym względy bezpieczeństwa i ochrony są niezwykle ważne. Katastrofy – jeśli występują – często mają międzynarodowy zasięg z uwagi na obywateli wielu krajów znajdujących się na pokładzie statku powietrznego. O tym, że nawet drobne ustępstwa wobec zasad bezpieczeństwa bywają zgubne, przekonał się przewoźnik lotniczy Pan Am. Firma upadła m.in. w wyniku katastrofy samolotu nad szkocką miejscowością Lockerbie, kiedy to w bagażu rejestrowanym umieszczonym w luku bagażowym wybuchła bomba⁴.

Ochrona lotnictwa cywilnego nie ogranicza się do elementów widocznych dla podróżnych na pierwszy rzut oka, takich jak obecność pracowników ochrony w terminalu czy kontrola bezpieczeństwa pasażerów i ich bagażu. Ochrona lotnictwa stanowi rozbudowany ekosystem, obejmujący dostawców zaopatrzenia lotniska (np. sklepów wolnocłowych, paliwa)

² Akt oskarżenia w sprawie aktów sabotażu na rzecz rosyjskiego wywiadu, Prokuratura Krajowa, 16 I 2026 r., <https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-w-sprawie-aktow-sabotazu-na-rzecz-rosyjskiego-wywiadu> [dostęp: 15 III 2026].

³ K. Izak, *Dwadzieścia lat od ataku z 11 września 2001 r. Przygotowania do ataku terrorystycznego na USA oraz jego przebieg i skutki*, „Przegląd Bezpieczeństwa Wewnętrznego” 2021, nr 25, s. 219–250. <https://doi.org/10.4467/20801335PBW.21.027.14304>.

⁴ B. Makowski, I. Mazurek, *Zamach w Lockerbie. Kto stał za śmiercią 270 ofiar?*, Polskie Radio 24, 21 XII 2025 r., <https://polskieradio24.pl/artukul/2236228,zamach-w-lockerbie-kto-stal-za-smiercia-270-ofiar> [dostęp: 15 III 2026]; M. Walków, *30 lat od jednego z największych zamachów w lotnictwie cywilnym*, Business Insider Polska, 21 XII 2018 r., <https://businessinsider.com.pl/wiadomosci/30-lat-od-jednego-z-najwiekszych-zamachow-w-lotnictwie-cywilnym/2p7f04t> [dostęp: 15 III 2026]; D. Cowan, *Lockerbie bombing suspect appears in court*, BBC, 16 XII 2023 r., <https://www.bbc.com/news/uk-scotland-67659046> [dostęp: 15 III 2026].

i pokładu samolotu (np. catering), firmy logistyczne zajmujące się obsługą towarów przewożonych drogą lotniczą (cargo) i wiele innych. To wszystko tworzy powiązane ze sobą łańcuchy dostaw, które często wykraczają poza obszar lotniska, sięgając nawet do producentów poszczególnych dóbr.

Moje doświadczenie zawodowe pokazuje, że wyżej wymienione podmioty mają różne podejście do ochrony dóbr i obiektów. Poszczególne branże funkcjonują w odmiennych realiach prawnych i finansowych, co sprawia, że mają inne priorytety w zakresie ochrony. W praktyce zdarza się, że spełnienie nawet podstawowych wymagań wynikających z przepisów dotyczących ochrony⁵ bywa dla nich trudne. Te wymagania dotyczą m.in. opracowania odpowiednich procedur, określenia momentu identyfikowalności zaopatrzenia pokładowego czy cargo, od którego należy zapewnić reżim ograniczonego dostępu, przeprowadzenia analiz dotyczących grup osób mogących mieć nienadzorowany dostęp do towarów i stref objętych reżimem ochronnym, a także realizacji sprawdzeń przeszłości personelu, o czym będzie w dalszej części artykułu. Konieczne jest także uzyskanie certyfikatów lub innych zezwoleń wydawanych przez krajową władzę lotniczą, tj. Prezesa Urzędu Lotnictwa Cywilnego. Posiadanie takich zaświadczeń umożliwia m.in. wysyłanie towarów bez konieczności każdorazowej kontroli bezpieczeństwa, co znacznie skraca czas oczekiwania, zwłaszcza w warunkach dużego natężenia ruchu.

Ochrona a bezpieczeństwo

Na wstępie warto wyjaśnić znaczenia terminów „bezpieczeństwo” i „ochrona” w kontekście lotniczym. Słowa te często funkcjonują jako synonimy, co w środowisku bywa źródłem nieporozumień, ponieważ odnoszą się one do odmiennych obszarów.

Termin „bezpieczeństwo” odnosi się do bezpieczeństwa operacyjnego, czyli bezpiecznego wykonywania operacji lotniczych zarówno na ziemi, jak i w powietrzu. Rozumiane jako angielskie *safety* dotyczy zapobiegania

⁵ Chodzi o przepisy zarówno międzynarodowe, np. *Rozporządzenie wykonawcze Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego* (Dz. Urz. UE L 299/1 z 14 XI 2015 r.), jak i krajowe, np. *Rozporządzenie Ministra Infrastruktury z dnia 2 grudnia 2020 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego* (t.j. DzU z 2023 r. poz. 774).

wypadkom i incydentom w szerokim ich znaczeniu. W uproszczeniu jest to lotniczy odpowiednik bezpieczeństwa i higieny pracy, obejmujący ochronę przed zagrożeniami wynikającymi z czynników zarówno żywych, jak i nieżywych, tj. zagrożenia niezależne od woli człowieka, spowodowane czynnikiem ludzkim (ang. *human factor*), a także błędy w zarządzaniu organizacją itp.

Termin „ochrona” natomiast odpowiada angielskiemu terminowi *security* i oznacza zespół środków podejmowanych w celu przeciwdziałania zamierzonym i bezprawnym działaniom o celowym charakterze. Pracownicy realizujący zadania z zakresu ochrony lotnictwa to m.in. osoby wykonujące kontrolę bezpieczeństwa, a także funkcjonariusze Policji oraz Straży Granicznej. Działania w obszarze ochrony nie ograniczają się do czynności wykonywanych wyłącznie przez wyspecjalizowane służby, lecz obejmują również stosowanie przez pracowników środków w zakresie ochrony, np. fizyczne zabezpieczanie towarów zwolnionych z kontroli bezpieczeństwa podczas ich transportu.

W codziennej praktyce bezpieczeństwo i ochrona na lotnisku się przenikają. Każdy członek załogi statku powietrznego, pracownik lotniska oraz osoba wykonująca obowiązki w jego obrębie są zobowiązani do przestrzegania wymagań zarówno z zakresu bezpieczeństwa operacyjnego, jak i ochrony lotnictwa.

Przykładem trudności w zakresie precyzyjnego stosowania terminologii mogą być treści publikowane na stronie Międzynarodowej Organizacji Lotnictwa Cywilnego (International Civil Aviation Organization, ICAO). Ich często nieprawidłowe tłumaczenie, np. przez tłumaczy w przeglądarkach, z języka angielskiego na polski prowadzi do zatarcia różnic terminologicznych między pojęciami. Przykładowo w przypadku dokumentów dotyczących kultury ochrony, o której szerzej wspomnę dalej, automatyczne narzędzia błędnie tłumaczą *security* jako bezpieczeństwo zamiast ochrona. A zatem wspomniana przeze mnie kontrola bezpieczeństwa powinna być przetłumaczona jako kontrola ochrony, jednak w języku polskim takie sformułowanie w przywołanym kontekście nie jest używane i brzmiałoby absurdalnie.

Z tego względu szczególnie istotne staje się krytyczne podejście do źródeł informacji, ostrożne korzystanie z narzędzi opartych na sztucznej inteligencji oraz tłumaczy, a także właściwe rozumienie i rozróżnianie przepisów z zakresu ochrony i bezpieczeństwa. Fakt, że niektóre polityki, procedury i mechanizmy mogą być skutecznie stosowane zarówno

w obszarze ochrony, jak i bezpieczeństwa może być dodatkowym utrudnieniem, ale też dużą zaletą.

W konsekwencji podobieństwa w znaczeniu obu słów w języku polskim mogą powodować konsternację wśród osób próbujących zgłębić te dwa zagadnienia.

Kilka słów o podstawach prawnych ochrony

Prawo dotyczące lotnictwa i jego ochrony ma międzynarodowy zasięg. Wspólne normy wynikają z przepisów uchwalanych przez ICAO. Ich trzonem jest Konwencja o międzynarodowym lotnictwie cywilnym⁶ z 1944 r., zwana także konwencją chicagowską, regulująca zasady lotnictwa cywilnego na świecie. Powołała ona do życia ICAO, która jest organizacją uprawnioną do tworzenia międzynarodowego prawa lotniczego. Konwencja chicagowska ma aż 19 załączników, które dotyczą wielu obszarów, m.in. ochrony lotnictwa cywilnego (załącznik 17)⁷. Dodatkowo ICAO wydaje dla państw i organizacji implementujących przepisy dotyczące ochrony lotnictwa cywilnego podręcznik⁸, który jest dokumentem o ograniczonym dostępie.

W Polsce obowiązują przepisy regulowane przez konwencję chicagowską, ale z uwagi na członkostwo w Unii Europejskiej na terytorium RP stosuje się przepisy Komisji Europejskiej oraz Rady Europy w zakresie ochrony lotnictwa cywilnego. Podstawą prawną systemu ochrony lotnictwa cywilnego jest *Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002*⁹. W tym rozporządzeniu została ustanowiona wykładnia stosowania załącznika 17 konwencji chicagowskiej, co ujednoliciła wymogi dotyczące kluczowych

⁶ Konwencja o międzynarodowym lotnictwie cywilnym, podpisana w Chicago dnia 7 grudnia 1944 r. (DzU z 1959 r. nr 35 poz. 212, ze zm.).

⁷ Załącznik 17 do Konwencji o międzynarodowym lotnictwie cywilnym. Ochrona lotnictwa. Ochrona międzynarodowego lotnictwa cywilnego przed aktami bezprawnej ingerencji, Urząd Lotnictwa Cywilnego, https://ulc.gov.pl/_download/prawo/prawo_miedzynarodowe/konwencje/Zalacznik_17_Ochrona_lotnictwa_wydanie_12_zm_18.pdf [dostęp: 15 III 2026].

⁸ *Aviation Security Manual* (Doc 8973 – Restricted), 2022, ICAO, <https://www.icao.int/aviation-security-policy-section/SecurityManual> [dostęp: 15 III 2026].

⁹ Dz. Urz. UE L 97/72 z 9 IV 2008 r.

elementów systemu ochrony lotnictwa cywilnego w całej UE. Akt ten, oprócz określenia ogólnego zakresu odpowiedzialności państw członkowskich, wskazuje również obowiązek przyjęcia na poziomie krajowym uszczegóławiających aktów wykonawczych. W załączniku I do tego rozporządzenia¹⁰ zostało wymienionych 12 aspektów ochrony lotnictwa cywilnego, a wśród nich: ochrona portu lotniczego, ochrona statków powietrznych oraz zabezpieczenie ładunku i poczty.

Rozporządzenie Parlamentu i Rady Europy w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego z 2008 r. można uznać za swoistą konstytucję ochrony lotnictwa cywilnego w UE, do której było konieczne wydanie aktów wykonawczych. Najważniejszym z nich jest *Rozporządzenie wykonawcze Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r., ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego*.

Z kolei to rozporządzenie zostało uzupełnione o *Decyzję wykonawczą Komisji C (2015) 8005 z dnia 16 listopada 2015 r. ustanawiającą szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego, zawierającą informacje, o których mowa w art. 18 lit. a) rozporządzenia (WE) 300/2008*¹¹. Nie została ona opublikowana w Dzienniku Urzędowym UE ze względu na charakter wrażliwy zawartych w niej regulacji. Ujęte w niej przepisy mają charakter techniczny i są skierowane na zasadzie ograniczonego dostępu do określonych podmiotów oraz osób pełniących funkcje w systemie ochrony lotnictwa cywilnego.

Na poziomie prawa krajowego najważniejszym aktem dotyczącym ochrony lotnictwa cywilnego jest *Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze*¹². W dziale IX *Ochrona lotnictwa cywilnego* określono wymogi z zakresu ochrony lotnictwa cywilnego w krajowym porządku prawnym, przy czym zasadniczą część tych regulacji stanowią delegacje ustawowe do wydania

¹⁰ Załącznik I *Wspólne podstawowe normy ochrony lotnictwa cywilnego przed aktami bezprawnej ingerencji (artykuł 4) do Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad...*

¹¹ Urząd Lotnictwa Cywilnego, <https://ulc.gov.pl/prawo/prawo-uni-europejskiej/prawo-ue-akty-prawne/ochrona-lotnictwa/3-decyzja-wykonawcza-komisji-c-2015-8005-z-dnia-listopada-2015-r-ustanawiajaca-szczegolowe-srodk-i-w-celu-wprowadzenia-w-zycie-wspolnych-podstawowych-norm-ochrony-lotnictwa-cywilnego-zawierajaca-informacje-o-ktorych-mowa-w-art-18-lit-a-rozporzadzenia-we> [dostęp: 15 III 2026].

¹² Tekst jednolity: DzU z 2025 r. poz. 1431, ze zm.

aktów wykonawczych doprecyzowujących szczegółowe wymagania. Należą do nich:

- *Rozporządzenie Ministra Infrastruktury z dnia 2 grudnia 2020 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego,*
- *Rozporządzenie Ministra Infrastruktury z dnia 5 listopada 2020 r. w sprawie Krajowego Programu Kontroli Jakości w zakresie ochrony lotnictwa cywilnego*¹³,
- *Rozporządzenie Ministra Infrastruktury z dnia 26 lipca 2021 r. w sprawie Krajowego Programu Szkolenia w zakresie ochrony lotnictwa cywilnego*¹⁴.

Właśnie te rozporządzenia są uzupełnieniem do wspomnianych wcześniej wymogów przepisów europejskich. Na tych trzech fundamentach opiera się krajowy system ochrony lotnictwa cywilnego.

Akt bezprawnej ingerencji

W prawie międzynarodowym akty terroru przeciwko lotnictwu cywilnemu nazywa się aktami bezprawnej ingerencji (ABI)¹⁵. W art. 2 pkt 20 ustawy Prawo lotnicze są one enumeratywnie wymienione i rozumiane jako bezprawne i celowe akty polegające na:

- a) użyciu w czasie lotu statku powietrznego przemocy wobec osoby znajdującej się na jego pokładzie, jeżeli akt ten może zagrozić bezpieczeństwu tego statku,
- b) zniszczeniu statku powietrznego albo spowodowaniu jego uszkodzeń, które uniemożliwiają lot lub mogą stanowić zagrożenie bezpieczeństwa tego statku,
- c) umieszczeniu na pokładzie statku powietrznego przedmiotu, urządzenia lub substancji, które mogą zagrozić zdrowiu lub życiu pasażerów lub załogi lub zniszczyć statek powietrzny albo spowodować jego uszkodzenia, mogące uniemożliwić jego lot lub stanowić zagrożenie bezpieczeństwa tego statku w czasie lotu,
- d) porwaniu statku powietrznego z załogą i pasażerami na pokładzie lub bez nich, również w celu użycia statku powietrznego jako narzędzia ataku terrorystycznego z powietrza,

¹³ Tekst jednolity: DzU z 2023 r. poz. 1204.

¹⁴ DzU z 2013 r. poz. 1147.

¹⁵ *Załącznik 17 do konwencji o międzynarodowym lotnictwie cywilnym...*, s. 15.

- e) zniszczeniu albo uszkodzeniu lotniczych urządzeń naziemnych lub pokładowych, zakłóceniu ich działania lub użyciu przemocy wobec osoby obsługującej te urządzenia, w przypadku gdy powoduje to znaczne zakłócenie ruchu lotniczego lub zagrożenie bezpieczeństwa lotnictwa cywilnego,
- f) przekazaniu nieprawdziwej informacji, która powoduje zagrożenie osób i mienia w komunikacji lotniczej,
- g) zniszczeniu albo poważnym uszkodzeniu urządzeń na lotnisku, zakłóceniu ich działania lub użyciu przemocy wobec osoby obsługującej te urządzenia, w przypadku gdy powoduje to znaczne zakłócenie ruchu lotniczego lub funkcjonowania lotniska lub zagrożenie bezpieczeństwa lotnictwa cywilnego.

Siedem wymienionych kategorii ABI stanowi podstawę definiowania zagrożeń, przed którymi jest chronione lotnictwo cywilne. Uzgodnienie katalogu tych czynów na poziomie międzynarodowym oraz jego implementacja do krajowych porządków prawnych ułatwiają skuteczne przeciwdziałanie takim zagrożeniom, a także penalizowanie zachowań osób dopuszczających się zarówno realizacji, jak i planowania ABI. Odpowiedzialność karna za tego rodzaju czyny jest przewidziana na podstawie m.in. art. 212 ustawy Prawo lotnicze oraz art. 115, art. 166, art. 173 i art. 174 Kodeksu karnego¹⁶.

Security Management System

W organizacjach rośnie znaczenie systemów zarządzania, których celem jest wspieranie efektywności organizacji. Bez zintegrowanego systemu kierowania organizacją, w tym jej ochroną, traci się możliwości skutecznego i proaktywnego reagowania na zagrożenia pojawiające się w otoczeniu. W tym celu jest wymagane wdrożenie strukturalnego podejścia opartego na ocenie posiadanych zasobów, identyfikowaniu słabości w systemie ochrony, zarządzaniu ryzykiem (a w zasadzie ryzykami), promowaniu kultury ochrony, trosce o wysoki poziom zaangażowanych w system zasobów ludzkich (szkolenia, właściwy dobór kadry). Niemniej ważny jest skuteczny przepływ informacji wewnętrznej, jak również współpraca z organami i służbami zewnętrznymi.

W strukturze i wymaganiach przepisów, tworzonych ponad 80 lat, można dostrzec zarys mocnego systemu ochrony lotnictwa. Jednak dopiero

¹⁶ Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2025 r. poz. 383, ze zm.).

pełne wdrożenie wskazanych pryncypiów i zapewnienie im solidnych ram prawnych jest kluczowym elementem budowy silnego systemu w jego szerokim kontekście. Podstawą skutecznego systemu zarządzania ochroną (ang. *security management system*, SeMS)¹⁷, podobnie jak każdego nowoczesnego systemu zarządzania, jest opracowanie odpowiednich polityk ochrony, zaakceptowanych i wdrożonych przez kierownictwo podmiotu, w którym funkcjonuje SeMS. Polityki te powinny określać cele oraz priorytety w zakresie ochrony.

Istotny element tych polityk to ustanowienie wymagań dotyczących procedur reagowania na zagrożenia i incydenty z zakresu ochrony, w tym zasad komunikacji zarówno z właściwymi służbami wewnętrznymi, jak i z organami administracji publicznej odpowiedzialnymi za reagowanie kryzysowe. Równocześnie niezbędne jest zapewnienie odpowiednich zasobów ludzkich, infrastrukturalnych oraz technicznych.

Kolejny filar SeMS to zarządzanie ryzykiem oparte na identyfikacji zagrożeń oraz wdrażaniu środków służących ich kontroli i minimalizacji. Uzupełnieniem tych działań są mechanizmy monitorowania skuteczności ochrony, kontroli jakości oraz ciągłego doskonalenia systemu.

Jednym z nowszych elementów wprowadzonych do regulacji z zakresu ochrony lotnictwa cywilnego jest koncepcja kultury ochrony, rozumianej jako budowanie zaufania wśród pracowników, promowanie właściwych postaw i zachowań oraz zachęcanie do zgłaszania incydentów i nieprawidłowości.

Między innymi na tych zasadach zostały opracowane polskie przepisy wykonawcze, tj. wspomniane wcześniej:

- *Krajowy Program Ochrony Lotnictwa Cywilnego* regulujący obszary polityk i uszczegóławiający wymagania dotyczące działań opartych na zarządzaniu ryzykiem i działań typowo ochronnych,
- *Krajowy Program Szkolenia* regulujący obszar wymagań co do kompetencji osób zaangażowanych w system ochrony,
- *Krajowy Program Kontroli Jakości* regulujący obszar monitorowania zgodności z wymaganiami prawnymi, a co za tym idzie – jego jakości.

Z praktycznego punktu widzenia zasadne jest wyróżnienie kluczowych komponentów, które – w mojej ocenie – są niezbędne do zbudowania skutecznego SeMS. Jeden z nich to stworzenie stanowiska security managera, czyli osoby odpowiedzialnej nie tylko za wdrożenie systemu, lecz

¹⁷ *Aviation Security Manual* (Doc 8973 – Restricted)...

także za jego funkcjonowanie i rozwój. Osoba pełniąca tę funkcję powinna mieć realną, a nie wyłącznie formalną możliwość wpływania na zmiany oraz podejmowania kluczowych decyzji w obszarze ochrony. Zdarzają się przypadki powoływania w organizacji security managera, jednak osoba na tym stanowisku nie dysponuje faktycznym umocowaniem w strukturze organizacyjnej. W takich sytuacjach, mimo zaangażowania, poczucia odpowiedzialności i chęci do działania, security manager nie ma narzędzi umożliwiających realne zarządzanie ochroną. Dlatego przy tworzeniu stanowiska security managera jest niezbędne zapewnienie mu formalnych i rzeczywistych kompetencji w zakresie zarządzania zasobami finansowymi oraz ludzkimi w obszarze ochrony. Tylko takie umocowanie pozwala na skuteczne funkcjonowanie systemu ochrony.

W organizacji powinny zostać wdrożone spójne polityki, standardy i procedury ochrony, zaakceptowane i faktycznie wspierane przez najwyższe kierownictwo. Dokumenty te powinny jasno określać cele ochrony, identyfikować kluczowe zagrożenia oraz uwzględniać kontekst funkcjonowania organizacji.

Współcześnie coraz większy nacisk kładzie się na nowoczesne podejście do ochrony oparte na zarządzaniu ryzykiem. Wynika to z dynamicznie zmieniającego się i szerokiego spektrum zagrożeń, które wymagają regularnej identyfikacji, oceny oraz ponownej analizy. Zarządzanie ryzykiem polega na ocenie wpływu zagrożeń na organizację oraz świadomym wdrażaniu adekwatnych środków ochrony w celu osiągnięcia akceptowalnego poziomu ryzyka.

Nie istnieje jedno uniwersalne narzędzie oceny ryzyka – jego dobór powinien być dostosowany do charakteru organizacji, przy zachowaniu zasady prostoty i użyteczności. Należy również podkreślić, że całkowite wyeliminowanie ryzyka nie jest możliwe, a koncepcja „zero zagrożeń” pozostaje nierealna, dlatego wymagana jest świadoma akceptacja jego określonego poziomu.

W praktyce tworzenia polityk i procedur często pojawia się problem bezrefleksyjnego kopiowania rozwiązań, które nie zawsze są adekwatne do specyfiki danego podmiotu. Problemem nie jest korzystanie z gotowych wzorców, lecz brak umiejętności ich adaptacji do własnych celów, ryzyk i dostępnych zasobów.

Skuteczne zarządzanie ochroną wymaga również innowacyjności oraz kreatywności. To właściciel procesu lub ryzyka, najlepiej znający realia organizacji, powinien inicjować lub co najmniej uzgadniać identyfikowane

ryzyka oraz sposoby ich ograniczania. Jednocześnie warto podkreślić, że proste narzędzia, przy odpowiedniej i przemyślanej implementacji, mogą przynosić bardzo dobre efekty.

Na etapie tworzenia procedur oraz projektowania SeMS konieczne jest uwzględnienie sposobów reagowania na zidentyfikowane zagrożenia, incydenty i naruszenia, które mogą wystąpić w codziennej działalności. Działania ochronne powinny pełnić funkcję prewencyjną i odstraszającą, jednak równie istotne jest przygotowanie personelu do właściwego postępowania w przypadku wystąpienia zdarzenia. Pracownicy powinni wiedzieć, w jaki sposób uruchomić system reagowania oraz jakie służby, w tym Policję czy inne organy państwowe, należy zaangażować.

Zilustrowaniu, jakie znaczenie dla bezpieczeństwa ma odpowiednie przygotowanie infrastruktury i personelu, niech posłuży zdarzenie sprzed kilku lat. Przypadek dotyczył operatorów kontroli bezpieczeństwa i uruchomienia procedury neutralizacji potencjalnego zagrożenia w postaci improwizowanego urządzenia wybuchowego (ang. *improvised explosive device*, IED) znajdującego się w przesyłce w trakcie kontroli bezpieczeństwa. Formalnie działania były prowadzone zgodnie z obowiązującymi procedurami zarejestrowanego agenta¹⁸. Okazało się jednak, że ich realizacja była znacznie utrudniona z powodu lokalizacji urządzenia RTG, w którym prześwietlano przesyłkę. Paczkę zatrzymano w środku maszyny usytuowanej na znacznej wysokości, co uniemożliwiało użycie robota pirotechnicznego i powodowało komplikacje przy prowadzeniu dalszych czynności pirotechnicznych.

Unaocznilo to niedostosowanie procedur awaryjnych do rzeczywistych warunków infrastrukturalnych i technicznych, a także do potrzeb zapewnienia ciągłości działania. Schematyczne podejście polegające na zatrzymaniu operacji, ewakuacji personelu i oczekiwaniu na przybycie właściwych służb może prowadzić do poważnych konsekwencji organizacyjnych, operacyjnych i finansowych wynikających z zakłócenia realizacji usług.

¹⁸ Zarejestrowany agent oznacza przewoźnika lotniczego, agenta, spedytora lub inny podmiot zapewniający stosowanie środków kontroli w zakresie ochrony w odniesieniu do ładunku lub poczty. Zob. art. 3 ppkt 26 *Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad...*

Zasoby ludzkie

Filarem systemu ochrony, ale jednocześnie jego najbardziej wrażliwym i podatnym na zagrożenia ogniwem jest człowiek. Z tego względu w przepisach dotyczących ochrony lotnictwa cywilnego dużo uwagi poświęca się weryfikacji personelu, zwłaszcza osób zaangażowanych w stosowanie środków ochrony, takich jak kontrola bezpieczeństwa, kontrola dostępu, nadzór czy patrole, a także pracowników posiadających nienadzorowany dostęp do stref i obiektów chronionych¹⁹.

Obowiązujące regulacje przewidują dwa poziomy **sprawdzenia przeszłości personelu** lotniczego i lotniska, kandydatów oraz innych osób, które mają m.in. dostęp do stref zastrzeżonych. Sprawdzenie standardowe obejmuje weryfikację tożsamości, historii zatrudnienia i kształcenia z co najmniej ostatnich pięciu lat, a także potwierdzenie niekaralności również z państw, w których dana osoba przebywała w tym okresie. Sprawdzenie rozszerzone jest realizowane przy udziale właściwych służb, w szczególności Straży Granicznej, i polega na ustaleniu – także na podstawie informacji operacyjnych czy wywiadowczych – występowania negatywnych przesłanek.

Sprawdzenia są przeprowadzane cyklicznie, nierzadziej niż co pięć lat, przy czym aktualność poszczególnych elementów jest weryfikowana częściej – w przypadku sprawdzenia standardowego co trzy lata, a rozszerzonego – corocznie. Proces ten angażuje znaczne zasoby organizacyjne, zwłaszcza w przypadku portów lotniczych, gdzie obejmuje personel wielu podmiotów działających na ich terenie – może to być nawet od kilku do kilkunastu tysięcy osób. Warto podkreślić, że obowiązek sprawdzenia przeszłości dotyczy również osób mających nieograniczony dostęp do krytycznych lotniczych systemów teleinformatycznych i danych, co stanowi element ochrony przed cyberzagrożeniami. Personel ten jest traktowany analogicznie do osób mających dostęp bez eskorty do szczególnie chronionych stref lotniska.

Doświadczenia wskazują, że nawet najbardziej zaawansowane rozwiązania proceduralne i techniczne nie zastąpią odpowiednio zweryfikowanej i świadomej kadry odpowiadającej za funkcjonowanie kluczowych

¹⁹ Zob. np. rozdział 11 *Rozporządzenia wykonawczego Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki...*; dział IX *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze...*; *Rozporządzenie Ministra Infrastruktury z dnia 2 grudnia 2020 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego* (t.j. DzU z 2023 r. poz. 774).

elementów infrastruktury. Choć proces sprawdzeń wiąże się z nakładami czasu i środków, to pozwala on nie tylko na ograniczenie ryzyka, lecz także na szybkie pozyskanie informacji o ewentualnych negatywnych przesłankach dotyczących personelu.

Mechanizm ten, wypracowany na poziomie międzynarodowego środowiska lotniczego, aby mógł być skutecznie implementowany w innych sektorach IK, wymagałby odpowiedniego dostosowania do krajowych realiów i porządku prawnego. W porównaniu z postępowaniami sprawdzającymi prowadzonymi na potrzeby dostępu do informacji niejawnych, sprawdzenia przeszłości osób w branży lotniczej są realizowane w dość krótkim czasie, co jest ich istotną zaletą, ale przy dużej rotacji personelu nawet ten okres bywa postrzegany jako wyzwanie organizacyjne.

Drugim elementem skutecznego systemu ochrony są **kwalifikacje oraz kompetencje personelu**. W obszarze ochrony lotnictwa cywilnego funkcjonuje rozbudowany system szkoleń, dostosowany do zakresu obowiązków poszczególnych grup pracowników – od kadry kierowniczej i menedżerów średniego szczebla po osoby bezpośrednio zaangażowane w stosowanie środków ochrony. Istotne są również szkolenia podnoszące poziom świadomości ochrony wśród pracowników, którzy nie wykonują bezpośrednich zadań ochronnych, lecz funkcjonują w środowisku wymagającym podwyższonej czujności.

Kultura ochrony²⁰ stanowi zbiór norm, wartości, postaw i założeń związanych z ochroną, które są podstawą codziennego funkcjonowania organizacji i znajdują odzwierciedlenie w działaniach oraz zachowaniach wszystkich jej członków. Ochrona nie powinna być postrzegana wyłącznie jako zadanie wyspecjalizowanych służb, lecz jako wspólna odpowiedzialność, obejmująca wszystkie szczeble struktury organizacyjnej – od stanowisk operacyjnych po najwyższe kierownictwo.

W praktyce kultura ochrony łączy poszczególne elementy systemu ochrony. Bez jej ukształtowania nawet najlepiej zaprojektowane procedury, systemy i środki techniczne mogą się okazać nieskuteczne. Brak zrozumienia celu ochrony prowadzi bowiem do postrzegania jej wyłącznie jako zbioru nakazów i zakazów, które w związku z tym nie są akceptowane i właściwie realizowane. W tym sensie kultura ochrony stanowi czynnik napędowy systemu ochrony.

²⁰ *Security Culture*, International Civil Aviation Organization, <https://www.icao.int/security-culture> [dostęp: 15 III 2026].

W ostatnich latach w lotnictwie cywilnym coraz większą uwagę poświęca się zagrożeniom wewnętrznym (ang. *insider threats*)²¹. Pojęcie to odnosi się do celowych i umyślnych działań podejmowanych przez osoby mające uprawniony dostęp do organizacji, które mogą prowadzić do aktów sabotażu, dywersji lub bezprawnej ingerencji.

Przeciwdziałanie zagrożeniom wewnętrznym może opierać się na połączeniu kilku komplementarnych mechanizmów, takich jak sprawdzenia przeszłości, szkolenia z zakresu świadomości ochrony, budowanie kultury ochrony, kampanie informacyjne oraz wdrożone systemy zgłaszania i raportowania nieprawidłowości. Elementy te stosowane łącznie znacząco wzmacniają odporność organizacji na zagrożenia ze strony np. radykalizujących się, w szerokim znaczeniu tego słowa, pracowników.

Kontrola jakości

SeMS opiera się na koncepcji Plan-Do-Check-Act (PDCA)²², znanej również jako cykl Deminga, która traktuje ochronę jako proces ciągły. Podejście to zakłada planowanie działań ochronnych, ich wdrażanie, weryfikację skuteczności oraz wprowadzanie działań korygujących i doskonalących. Po przeprowadzeniu analizy ryzyka, wyznaczeniu celów oraz wdrożeniu odpowiednich środków ochrony konieczne jest sprawdzenie, czy system funkcjonuje zgodnie z założeniami.

W literaturze pojęcia monitorowanie zgodności oraz kontrola jakości są używane zamiennie, co wynika przede wszystkim z rozbieżności terminologicznych występujących w tłumaczeniach aktów prawnych. W krajowym porządku prawnym w odniesieniu do ochrony lotnictwa cywilnego utrwaliło się określenie kontrola jakości²³, które będzie stosowane w dalszej części opracowania.

W ciągu lat lotnictwo cywilne wykształciło rozbudowany system kontroli jakości w obszarze ochrony. Choć opiera się on na powszechnie stosowanych metodach kontroli i audytu, to jego charakter jest zbliżony do

²¹ Tamże.

²² Zob. szerzej: *PDCA – Klucz do ciągłego doskonalenia i skutecznego zarządzania procesami*, Instytut Doskonalenia Produkcji, <https://www.doskonalenieprodukcji.pl/blog/pdca-klucz-do-ciaglego-doskonalenia-i-skutecznego-zarzadzania-procesami> [dostęp: 15 III 2026].

²³ *Rozporządzenie Ministra Infrastruktury z dnia 5 listopada 2020 r. w sprawie Krajowego Programu Kontroli Jakości w zakresie ochrony lotnictwa cywilnego*.

podejścia znanego z obszaru cyberbezpieczeństwa. Szczególny nacisk kładzie się bowiem na ciągłe monitorowanie, identyfikację luk oraz szybkie reagowanie na zmieniające się zagrożenia, a nie jedynie na okresową ocenę zgodności z przyjętymi wymaganiami.

Kontrola jakości w lotnictwie cywilnym stanowi wielopoziomowy system weryfikacji spełniania co najmniej podstawowych wymagań ochrony przez państwa członkowskie, porty lotnicze, przewoźników lotniczych oraz pozostałych uczestników systemu. Uprawnienia kontrolne są realizowane na różnych szczeblach: na poziomie międzynarodowym przez ICAO, na poziomie Unii Europejskiej przez Komisję Europejską, w Polsce przez Prezesa Urzędu Lotnictwa Cywilnego, z kolei na poziomie poszczególnych podmiotów lotniczych – przez audytorów wewnętrznych.

Wielopoziomowy charakter tego systemu, a także możliwość udziału audytorów z różnych państw członkowskich we wspólnych kontrolach prowadzonych wraz z inspektorami Komisji Europejskiej sprzyjają wymianie wiedzy i dobrych praktyk. Dodatkowo przepisy unijne przewidują mechanizmy umożliwiające Komisji Europejskiej udostępnianie przez jej inspektorów ogólnych wyników i rezultatów przeprowadzonych kontroli.

Na tle innych państw członkowskich Polska wykształciła rozbudowany system certyfikowanych audytorów wewnętrznych, podejmując jednocześnie próbę przeniesienia mechanizmów oraz praktyk kontrolnych na poziom podmiotów prowadzących działalność lotniczą. Rozwiązanie to wzmacnia spójność systemu ochrony oraz zwiększa jego odporność dzięki systematycznym kontrolom i wdrażaniu działań naprawczych.

Do podstawowych metod kontroli w zakresie ochrony lotnictwa cywilnego zalicza się audyt, inspekcję, testy ochrony oraz przegląd ochrony.

Audyt jest czynnością zapowiadzianą i obejmuje całość stosowanych środków ochrony w danym podmiocie.

Inspekcja polega na weryfikacji wybranych elementów systemu ochrony, szczególnie tzw. bezpośrednio powiązanych środków ochrony, których prawidłowe stosowanie może zostać potwierdzone wyłącznie przez ich łączną ocenę.

Testy ochrony to niezapowiedziane i niejawne działania sprawdzające, takie jak próby wniesienia przez kontrolę bezpieczeństwa przedmiotów zabronionych, uzyskanie nieuprawnionego dostępu do stref zastrzeżonych lub nieuprawnionego wejścia na pokład statku powietrznego. Można to porównać do testów penetracyjnych znanych z cyberbezpieczeństwa.

Uzupełnieniem powyższych form jest przegląd ochrony, który polega na ocenie konkretnego środka ochrony i jest przeprowadzany przez właściwą władzę lotniczą w ramach sprawowania nadzoru.

W praktyce szczególnie wysoką wartość w ewaluacji systemu ochrony lotnictwa cywilnego mają niezapowiedziane metody kontroli, takie jak inspekcje oraz testy ochrony. Dzięki nim zyskuje się informacje o funkcjonowaniu systemu ochrony w codziennych warunkach, przez wykorzystanie nagrań z monitoringu, wywiady z pracownikami wykonującymi swoje czynności bez uprzedzania ich o tym.

Audyty, choć istotne z punktu widzenia całościowej oceny działalności oraz zgodności systemowej, w większym stopniu sprawdzają się przy analizie szerokich obszarów funkcjonowania organizacji. Jednocześnie zarówno audyty, jak i inspekcje z zakresu ochrony lotnictwa cywilnego często wymagają znacznych nakładów organizacyjnych i czasu – angażują wieloosobowe zespoły przez wiele dni roboczych w celu uzyskania pełnego obrazu funkcjonowania systemu ochrony.

Należy podkreślić, że w przypadku stwierdzenia niezgodności lub odstępstw od obowiązujących przepisów i procedur konieczne jest wdrożenie adekwatnych środków zaradczych oraz uruchomienie programu działań naprawczych. Takie działania mają na celu możliwie szybkie usunięcie zidentyfikowanych podatności systemu ochrony.

Realizacja programu naprawczego wymaga pełnego wsparcia ze strony osoby odpowiedzialnej za ochronę, zrozumienia całego procesu oraz przyjęcia odpowiedzialności za skuteczne usunięcie zidentyfikowanych nieprawidłowości. Równocześnie niezbędne jest uwzględnienie zasad kultury ochrony, tak aby w jasny sposób zakomunikować cele działań naprawczych i uzyskać realne wsparcie ze strony pracowników oraz współpracujących komórek organizacyjnych.

Na zakończenie należy zwrócić uwagę na jeszcze jeden element ujęty w *Krajowym Programie Kontroli Jakości*²⁴, który można uznać za innowacyjny, niewystępujący wprost w przepisach międzynarodowych dotyczących ochrony lotnictwa cywilnego. Mowa o ćwiczeniach ochrony, które w istotnym stopniu nawiązują do zagadnień związanych z zarządzaniem kryzysowym oraz wdrażaniem planów utrzymania ciągłości działania. Zgodnie z przywołanym programem każde lotnisko jest zobowiązane do corocznego przeprowadzania ćwiczeń, które polegają najczęściej na symulacji

²⁴ Tamże.

próby dokonania ABI i uruchomieniu sztabów kryzysowych oraz sprawdzeniu procedur reagowania obowiązujących w danym porcie lotniczym. Te ćwiczenia są realizowane, w zależności od uzgodnionego zakresu, we współpracy z przewoźnikami lotniczymi, innymi podmiotami prowadzącymi działalność lotniczą, służbą ochrony lotniska, a także państwowymi służbami funkcjonującymi na terenie portu lotniczego, szczególnie Strażą Graniczną, Policją oraz Agencją Bezpieczeństwa Wewnętrznego.

Ochrona lotnictwa cywilnego a ochrona infrastruktury krytycznej

Analiza *Narodowego Programu Ochrony Infrastruktury Krytycznej 2023*²⁵ oraz jego załącznika pt. *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*²⁶ wskazuje, że wiele zaproponowanych w nim rozwiązań jest zbieżnych z mechanizmami stosowanymi w systemie ochrony lotnictwa cywilnego. To istotne, gdyż system ochrony lotnictwa cywilnego należy do najbardziej rozwiniętych i sformalizowanych systemów bezpieczeństwa infrastruktury i opiera się na wielopoziomowym podejściu do zarządzania ryzykiem oraz ciągłym doskonaleniu procedur ochronnych.

Jednocześnie część rekomendacji zawartych w przywołanym narodowym programie ochrony IK ma charakter wyłącznie dobrych praktyk, co może ograniczać stopień ich wdrażania przez operatorów IK. Wydaje się zasadne wprowadzenie wybranych rozwiązań w drodze aktów normatywnych wyższego rzędu, co pozwoliłoby na ich bardziej jednolite i konsekwentne stosowanie. Dotyczy to szczególnie zagadnień związanych z zarządzaniem zasobami ludzkimi w systemach bezpieczeństwa i ochrony, takich jak rozwój kompetencji personelu czy wzmocnienie mechanizmów weryfikacji pracowników, zwłaszcza tych mających dostęp do krytycznych elementów infrastruktury. Doświadczenia sektora lotnictwa cywilnego wskazują, że odpowiednia selekcja, szkolenie oraz stałe doskonalenie kompetencji personelu stanowią jeden z filarów skutecznego systemu ochrony.

²⁵ *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, <https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej> [dostęp: 15 III 2026].

²⁶ Tamże.

Równie istotne jest rozwijanie kultury ochrony, która polega na budowaniu świadomości zagrożeń oraz odpowiedzialności za bezpieczeństwo i ochronę wśród wszystkich uczestników systemu. Oznacza to konieczność prowadzenia systematycznych działań szkoleniowych, informacyjnych oraz organizacyjnych, których celem jest wzmacnianie postaw sprzyjających identyfikowaniu i zgłaszaniu potencjalnych zagrożeń.

Należy również podkreślić, że choć w dokumentach programowych dotyczących ochrony IK jest rekomendowane prowadzenie audytów bezpieczeństwa, to w praktyce te działania często koncentrują się na ocenie zgodności formalnej oraz analizie dokumentacji. Tymczasem skuteczność systemu ochrony zależy od jego funkcjonowania w warunkach operacyjnych. Z tego względu szczególnego znaczenia nabierają praktyczne działania, takie jak ćwiczenia, testy ochrony z wykorzystaniem symulacji ABI, które pozwalają weryfikować rzeczywistą zdolność organizacji do reagowania na sytuacje kryzysowe.

Podsumowanie

Ze względu na swoje usytuowanie w sektorze transportu lotniska cywilne są jednym z ważniejszych obszarów IK. Wieloletnie doświadczenia lotnictwa cywilnego dotyczące funkcjonowania w silnie regulowanym środowisku ze szczególnie rozwiniętym SeMS mogą zostać wykorzystane do wzmocnienia odporności innych elementów IK.

Większość obowiązujących regulacji w obszarze ochrony koncentruje się na działaniach realizowanych w strefach operacyjnych, zastrzeżonych oraz w ich częściach krytycznych. Dotyczy to nie tylko lotnictwa cywilnego i portów lotniczych, lecz także innych zatłoczonych przestrzeni publicznych. Wobec współczesnych zagrożeń ochrona infrastruktury, z której korzystają duże skupiska ludności i do której dostęp jest prawie nieograniczony, takiej jak dworce, stacje metra, miejsca masowych imprez itp., powinna być priorytetem i wymaga ciągłego doskonalenia. W tym kontekście warto przypomnieć zamach na lotnisku Bruksela w Zaventem w 2016 r.²⁷, który – podobnie jak wiele innych ataków terrorystycznych – został przeprowadzony w strefie ogólnodostępnej hali odlotowej lotniska.

²⁷ M. Zieliński, *Zamachy terrorystyczne w Brukseli*, Polska Zbrojna, 22 III 2016 r., <https://polska-zbrojna.pl/Mobile/ArticleShow/18869> [dostęp: 28 III 2026].

Zasadne wydaje się prowadzenie dla służb ochrony częstych specjalistycznych szkoleń, obejmujących m.in. techniki interwencji czy posługiwanie się bronią. Jednocześnie wskazane jest rozszerzenie tematyki kursów o np. profilowanie behawioralne, które uczy identyfikacji zachowań potencjalnie niebezpiecznych oraz podejmowania adekwatnych działań na jak najwcześniejszym etapie rozwoju zagrożenia, skierowanych do szerokiej grupy pracowników, takich jak konduktorzy czy kierowcy komunikacji miejskiej.

Coraz częstsza obecność uzbrojonych strażników i funkcjonariuszy różnych służb w przestrzeni publicznej, w tym na ulicach oraz w rejonach węzłów komunikacyjnych, jest ważnym elementem działań prewencyjnych. Przy tej okazji warto rozważyć większe wykorzystanie psów służbowych przeszkolonych zarówno do działań patrolowych, jak i do wykrywania materiałów wybuchowych. Wiąże się to z wyzwaniem organizacyjnymi i formalnoprawnymi, jednak potencjał operacyjny oraz prewencyjny takiego rozwiązania jest duży, zwłaszcza w kontekście zagrożeń związanych z bagażami pozostawionymi bez nadzoru. Obecność w patrolu przewodników z wyszkolonymi psami może nie tylko przyczynić się do szybkiej weryfikacji ewentualnego zagrożenia, lecz także odstraszać potencjalnych sprawców aktów terroru lub sabotażu. W konsekwencji może to ograniczyć ryzyko eskalacji incydentu oraz skrócić czas reakcji służb, w tym czas ewentualnej ewakuacji zagrożonego obszaru.

Kolejny aspekt to ocena skuteczności wdrożonych środków ochrony w odniesieniu do najczęściej identyfikowanych scenariuszy zagrożeń terrorystycznych. Niezbędne jest podjęcie działań mających na celu identyfikację potencjalnych słabych punktów oraz przetestowanie istniejących rozwiązań. Rekomendowane jest także cykliczne powtarzanie takich kontroli.

W mojej ocenie do podniesienia poziomu ochrony IK w istotny sposób może przyczynić się:

- aktywne podejmowanie działań ukierunkowanych na wymianę doświadczeń,
- rozwijanie współpracy między podmiotami funkcjonującymi w różnych sektorach,
- budowanie świadomości konieczności zmian i ewolucji systemów ochrony,
- stworzenie i wykorzystywanie skutecznych narzędzi nadzoru i przeglądu systemu ochrony, opartych na solidnych podstawach prawnych.

Działania te sprzyjałyby transferowi dobrych praktyk obecnych w lotnictwie cywilnym do innych obszarów mających wpływ na prawidłowe funkcjonowanie państwa i społeczeństwa. Wpisują się one także w koncepcję ciągłego doskonalenia systemów bezpieczeństwa i ochrony oraz zwiększania odporności IK na współczesne zagrożenia.

Karol Dymek

Specjalista z ponaddwudziestoletnim doświadczeniem w branży ochrony. Przez ponad 18 lat związany z ochroną lotnictwa cywilnego, w tym jako krajowy audytor w Urzędzie Lotnictwa Cywilnego. Obecnie pracuje jako audytor wewnętrzny na jednym z największych lotnisk w Polsce.

Kontakt: dymek.karol@gmail.com

Bezpieczeństwo lotnictwa cywilnego w praktyce – systemy ochrony, kontrola i odporność operacyjna

Bohdan Paszukow

Securitas Services

Bezpieczeństwo lotnictwa cywilnego stanowi jeden z filarów funkcjonowania globalnego transportu. Wpływ na jego poprawę mają spójne procedury, nowoczesne narzędzia oraz odpowiednio zaprojektowane systemy ochrony. W ramach programów AVSEC (od ang. *aviation security*) są rozwijane standardy i praktyki mające na celu zapobieganie aktom nieprawnej ingerencji, wzmacnianie odporności infrastruktury oraz zapewnienie wysokiego poziomu kontroli ryzyka. Poszczególne państwa i organizacje międzynarodowe przyjmują różne modele organizacji systemów bezpieczeństwa – od centralnie zarządzanych po bardziej zdecentralizowane i oparte na odpowiedzialności operatorów. Ta różnorodność podejść jest szczególnie widoczna, gdy porówna się rozwiązania stosowane w Unii Europejskiej i Stanach Zjednoczonych.

Ocena jakości bezpieczeństwa lotnictwa cywilnego w Stanach Zjednoczonych i Unii Europejskiej

Podczas przeprowadzania oceny jakości bezpieczeństwa lotnictwa cywilnego, szczególnie w przypadku międzynarodowej korporacji zajmującej się ochroną osób i mienia w różnych obszarach, niezbędne jest zrozumienie, w jaki sposób poszczególne regiony organizują swoje systemy bezpieczeństwa lotniczego. Stany Zjednoczone i Unia Europejska dążą do tych samych celów, jakimi są zapobieganie incydentom o charakterze terrorystycznym i zapewnienie bezpieczeństwa pasażerów, personelu i infrastruktury. Jednak ich realizacja różni się sposobem zarządzania systemem bezpieczeństwa, stylem tworzenia i egzekwowania regulacji, a także mechanizmami nadzoru nad operatorami. Unia Europejska opiera się na szczegółowych, jednolitych normach technicznych i procedurach. Stany Zjednoczone preferują model bardziej scentralizowany, z silną rolą Administracji Ochrony Transportu (Transportation Security Administration, TSA) i większym naciskiem kładzionym na rozwiązania oparte na wynikach i skuteczności, a nie sztywnych wymaganiach proceduralnych. Unia Europejska stosuje zatem podejście normatywne, a USA – efektywnościowe, co wiąże się z odmiennymi sposobami organizacji i kontroli systemów AVSEC.

TSA, która przejęła bezpośrednią odpowiedzialność za bezpieczeństwo lotnicze w Stanach Zjednoczonych, została utworzona w ramach Departamentu Bezpieczeństwa Krajowego (Department of Homeland Security) po wydarzeniach z 11 września 2001 r. Ustanawia ona jednolite wymagania dotyczące kontroli bezpieczeństwa, wydaje dyrektywy federalne związane z bezpieczeństwem oraz zarządza działaniami punktów kontroli w większości portów lotniczych. Taka centralizacja pozwala na szybkie dostosowanie się do pojawiających się zagrożeń przez zmiany dyrektyw. Nadzór jest sprawowany w ramach federalnych inspekcji, ukrytego testowania oraz aktualizacji procedur, np. po incydentach. System amerykański jest zatem nakazowy i zawiera szczegółowe wymagania dotyczące kontroli pasażerów i bagażu, weryfikacji personelu oraz kontroli dostępu. Kładzie nacisk na ujednolicenie i szybkość reakcji, a za zgodność z przepisami odpowiadają bezpośrednio agencje federalne.

Model UE opiera się na harmonizacji systemów bezpieczeństwa wielu suwerennych państw, które muszą wdrażać wspólne standardy AVSEC przy zachowaniu własnych struktur administracyjnych i odpowiedzialności krajowej.

Podstawowym unijnym aktem w zakresie bezpieczeństwa lotniczego jest rozporządzenie 300/2008¹, ustanawiające wspólne zasady kontroli bezpieczeństwa, kontroli dostępu i bezpieczeństwa ładunków. Uzupełnieniem tych zasad są akty wykonawcze określające standardy wydajności. Egzekwowanie przepisów leży w gestii organów krajowych w każdym państwie członkowskim, ale to Komisja Europejska nadzoruje ten proces. Przeprowadza ona kontrole, wymaga corocznych sprawozdań dotyczących zgodności i potwierdza stosowanie przez państwa członkowskie wspólnych przepisów. Tym, co wyróżnia system UE, jest ocena w ramach Common Evaluation Process (CEP), czyli opracowanego przez European Civil Aviation Conference (ECAC) programu testów, który zapewnia znormalizowane badania laboratoryjne urządzeń zabezpieczających pod kątem kryteriów wydajności. Gwarantuje to porównywalność zatwierdzeń urządzeń w poszczególnych państwach członkowskich i pozwala uniknąć fragmentarycznych ocen krajowych. Model UE umożliwia zatem państwom członkowskim spełnienie podstawowych wymagań przy jednoczesnym zachowaniu spójności transgranicznej dzięki zunifikowanym normom i nadzorowi Komisji Europejskiej.

Dużą zaletą unijnego systemu regulacji bezpieczeństwa lotniczego jest standaryzacja środków ochrony. Prawodawstwo UE pozwala koncentrować zasoby i wysiłki na obszarach najbardziej narażonych na ryzyko, a jednocześnie tworzy ramy do współpracy między państwami członkowskimi, organami regulacyjnymi, branżą lotniczą i innymi podmiotami zaangażowanymi w AVSEC. Ważną rolę w tym procesie odgrywają wspólne platformy i mechanizmy koordynacji, takie jak SAGAS (Security Advisory Group for Aviation Security), działający przy Komisji Europejskiej, czy branżowe organizacje reprezentujące sektor prywatny, np. ASSA-i (Aviation Security Services Association – International).

Ponadto system regulacyjny UE wspiera mechanizmy kontroli jakości i monitorowania zgodności w celu zapewnienia spójnego nadzoru operacyjnego i regulacyjnego.

Choć podejścia unijne i amerykańskie różnią się strukturą zarządzania, stylem regulacji i mechanizmami nadzoru, to w praktyce zbliżają się do siebie w ramach współpracy transatlantyckiej. W celu uniknięcia powielania certyfikacji i ujednolicenia procedur technicznych Federalna

¹ Rozporządzenie Parlamentu Europejskiego i Rady (WE) NR 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz. Urz. UE L 97/72 z 9 IV 2008 r.).

Administracja Lotnictwa Stanów Zjednoczonych (U.S. Federal Aviation Administration) oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (European Union Aviation Safety Agency, EASA) mają podpisane umowy dwustronne. Współpraca ta obejmuje również kwestie bezpieczeństwa – wzajemne uznawanie niektórych kontroli i certyfikatów ułatwia działanie globalnych operatorów zgodnie z literą prawa.

Ocena środków bezpieczeństwa fizycznego w lotnictwie cywilnym UE

Oceny zgodności stanowią podstawę bezpieczeństwa lotniczego. Zapewniają ustrukturyzowany sposób weryfikacji tego, czy lotniska, linie lotnicze i powiązani dostawcy usług przestrzegają przepisów międzynarodowych i krajowych, a także wytycznych innych krajowych organów lotnictwa cywilnego.

Metody oceniania, ich zakres i kryteria zmieniają się wraz z pojawianiem się nowych zagrożeń, rozwojem technologii oraz doświadczeniami wynikającymi z incydentów i audytów. Ewolucja ta dotyczy zarówno sposobów identyfikowania ryzyka, jak i narzędzi wykorzystywanych do jego analizy. Proces ten odbywa się również w ramach międzynarodowej sieci współpracy AVSEC, obejmującej instytucje takie jak International Civil Aviation Organization (ICAO), Komisja Europejska, TSA, EASA oraz organizacje i stowarzyszenia branżowe. To właśnie ta sieć umożliwia wymianę informacji, aktualizację standardów i dostosowywanie metod oceny ryzyka do globalnie zmieniającego się środowiska zagrożeń.

Jednym z najważniejszych elementów oceny zgodności jest monitoring systemów kontroli dostępu. Lotniska to złożone środowiska z dużą liczbą stref o ograniczonym dostępie. W ramach kontroli jakości ochrony lotnictwa cywilnego weryfikuje się, czy dostęp do obszarów wrażliwych ma tylko upoważniony personel, czy systemy identyfikacji, kontrole biometryczne i technologie nadzoru działają prawidłowo oraz czy procedury wydawania i zarządzania uprawnieniami dostępu są skuteczne. Wyklucza to sytuacje, w których dostęp uzyskałyby nieupoważnione osoby, co mogłoby narazić na niebezpieczeństwo samolot, pasażerów albo ładunek.

Równie ważna jest ocena procedur kontroli pasażerów i bagażu. W ramach oceny zgodności sprawdza się, czy technologie wykorzystywane do kontroli, takie jak urządzenia rentgenowskie, systemy wykrywania materiałów wybuchowych i skanery ciała, są odpowiednio skalibrowane

i konserwowane. Kontrola jakości obejmuje również obserwację, czy personel podczas pracy konsekwentnie przestrzega protokołów oraz zachowuje czujność.

Kolejny istotny obszar oceny to bezpieczeństwo ładunków i łańcucha dostaw, który obejmuje kontrolę sposobu sprawdzania, przechowywania i transportu ładunków. W ramach oceny weryfikuje się, czy dostawcy i kontrahenci przestrzegają zatwierdzonych praktyk bezpieczeństwa oraz czy istnieje przejrzysty łańcuch nadzoru nad wszystkimi towarami wprowadzanymi do samolotu.

Siła systemu bezpieczeństwa zależy od ludzi, którzy go wdrażają, dlatego procesy kontroli jakości kładą nacisk na ciągłą edukację, ćwiczenia i oceny personelu. Musi być on przygotowany do właściwego reagowania na podejrzane zachowania, sytuacje awaryjne lub próby naruszenia bezpieczeństwa. Oceny zgodności często obejmują symulowane scenariusze, na podstawie których sprawdza się gotowość i odporność na zagrożenia.

Ważną rolę odgrywają systemy zarządzania ryzykiem i zgłaszania incydentów. Oceny zgodności zapewniają efektywne funkcjonowanie mechanizmów identyfikacji słabych punktów, szybkiego zgłaszania naruszeń i wdrażania działań naprawczych. Dzięki kontroli jakości można śledzić szybkość i skuteczność reakcji organizacji na zidentyfikowane ryzyka, czyli wprowadzenie zmian w procedurach, technologii czy szkoleniach. Tworzy to tzw. pętlę informacji zwrotnej. Zdobyte w ten sposób doświadczenia wzmacniają bezpieczeństwo fizyczne w lotnictwie.

Kolejny ważny element to integracja technologii. W ramach oceny zgodności sprawdza się, czy systemy nadzoru, identyfikacja biometryczna i automatyczne kontrole dostępu są zainstalowane oraz aktywnie monitorowane i konserwowane. Kontrola jakości zapewnia, że dane z tych systemów wykorzystuje się do skutecznego wykrywania anomalii i zapobiegania naruszeniom.

Jednym z najbardziej bezpośrednich i praktycznych narzędzi w procesie oceny zgodności są obserwacje przeprowadzane przez audytorów i inspektorów wdrażania procedur bezpieczeństwa w czasie rzeczywistym. Dotyczy to np. zarządzania punktami kontroli dostępu czy konsekwentnego stosowania kontroli identyfikacji lub sposobu przeprowadzania kontroli bagażu. Obserwacje mogą ujawnić ewentualne rozbieżności między procedurami a praktyką.

Obserwację uzupełnia weryfikacja dokumentów, w ramach której jest sprawdzana zgodność polityk, instrukcji operacyjnych i dokumentów

organizacji z wymogami regulacyjnymi. Obejmuje to przegląd dokumentacji szkoleń mający potwierdzić, że personel otrzymał wymagane instrukcje, sprawdzanie rejestrów incydentów w celu weryfikacji, czy naruszenia są zgłaszane i badane, oraz potwierdzanie zgodności sprzętu z normami. Bez dokładnej i aktualnej dokumentacji nawet najlepsze praktyki operacyjne są niezgodne z przepisami. Ponadto przegląd dokumentów dostarcza dowodów na to, że organizacja nie tylko przestrzega przepisów obowiązujących w danym momencie, lecz także posiada systemy umożliwiające aktualizację przepisów w przyszłości.

Wywiad z personelem pomaga ocenić jego poziom zrozumienia ryzyka, nastawienie do pracy oraz gotowość do działania. Te rozmowy, zwłaszcza z funkcjonariuszami ochrony, mogą ujawnić, czy szkolenia były skuteczne oraz czy pracownicy, stosując obowiązujące procedury, czują się pewnie. Wywiad z kadrą zarządzającą może natomiast pokazać, na ile poważnie kierownictwo traktuje kwestie bezpieczeństwa oraz czy w organizacji istnieje kultura odpowiedzialności. Co istotne, takie spotkania odsłaniają obszary, których nie da się wychwycić jedynie na podstawie dokumentów i obserwacji – np. czy personel czuje się komfortowo podczas wykonywania swoich obowiązków, szczególnie w godzinach największego natężenia ruchu, czy procedury służące do zgłaszania podejrzanych aktywności są jasne i czy kanały komunikacji budzą zaufanie.

Testowanie procedur można podzielić na metody jawne i ukryte. Testy jawne obejmują zaplanowane ćwiczenia, takie jak próbne ewakuacje czy kontrolowane próby dostępu, podczas których personel jest świadomy, że podlega ocenie. Tego typu testy mierzą poziom zgodności w obserwowanych warunkach i pomagają organizacjom doskonalić swoje procedury. Testy ukryte, określane jako red teaming, polegają na symulowaniu zagrożeń bez wcześniejszego uprzedzenia – np. przez próbę uzyskania nieautoryzowanego dostępu lub wprowadzenia przez punkty kontroli przedmiotów zabronionych. Jest to niezwykle cenne, ponieważ pokazuje funkcjonowanie systemów w warunkach rzeczywistej presji, bez sztuczności typowej dla zainscenizowanych ćwiczeń. Przeprowadzanie testów jawnych i ukrytych pokazuje, czy środki bezpieczeństwa fizycznego są zgodne z wymaganymi normami oraz skuteczne w obliczu prawdziwych zagrożeń.

Docelowo ocena zgodności i kontrola jakości bezpieczeństwa w lotnictwie cywilnym służy stworzeniu wieloaspektowego systemu ochrony. Przestrzeganie przepisów, kontrola dostępu, kontrola bezpieczeństwa, bezpieczeństwo ładunku, szkolenie personelu, zarządzanie ryzykiem i integracja

technologii razem tworzą kompleksową ochronę przed zagrożeniami. Takie podejście pozwala na utrzymanie na akceptowalnym poziomie bezpieczeństwa fizycznego w lotnictwie cywilnym. Chroni pasażerów, personel i mienie, a jednocześnie utrzymuje zaufanie publiczne do podróży lotniczych.

Wykorzystanie sztucznej inteligencji do zapewnienia bezpieczeństwa lotnictwa cywilnego

W celu zwiększenia efektywności, dokładności oraz zdolności adaptacji systemów bezpieczeństwa lotnictwa do zmieniających się zagrożeń i warunków operacyjnych coraz częściej jest z nimi integrowana sztuczna inteligencja (ang. *artificial intelligence*, AI).

Technologie kontroli pasażerów i bagażu wykorzystują obecnie algorytmy uczenia maszynowego do skuteczniejszego wykrywania przedmiotów zabronionych niż tradycyjne systemy rentgenowskie. Narzędzia oparte na AI mogą analizować ogromne ilości danych obrazowych, rozpoznawać wzorce i charakterystykę zagrożeń oraz z większą precyzją wykrywać anomalie, co zmniejsza ryzyko błędu. Podobnie systemy identyfikacji biometrycznej stosowane na lotniskach, takie jak rozpoznawanie twarzy czy skanowanie odcisków palców, wykorzystują AI do szybkiego i bezpiecznego dopasowywania tożsamości, usprawniając w ten sposób przepływ pasażerów przy jednoczesnym utrzymaniu ścisłej kontroli dostępu.

AI jest stosowana w systemach nadzoru i monitoringu. Nowoczesne sieci monitoringu wizyjnego CCTV (od ang. *closed circuit television*) są wzbogacane o analitykę opartą na AI, która w czasie rzeczywistym potrafi wykrywać podejrzanе zachowania, bagaż pozostawiony bez nadzoru czy nieautoryzowany dostęp. Ta proaktywna zdolność pozwala personelowi bezpieczeństwa szybciej i skuteczniej reagować na potencjalne zagrożenia. W bezpieczeństwie ładunków oraz w ochronie łańcucha dostaw narzędzia AI są wykorzystywane do śledzenia przesyłek, weryfikowania ich autentyczności oraz identyfikowania nieprawidłowości w procesie ich transportu.

W praktyce AI nie zastępuje tradycyjnych środków bezpieczeństwa, lecz je wspiera. Nadzór człowieka pozostaje niezbędny, ponieważ systemy AI muszą być nieustannie testowane, weryfikowane i monitorowane, aby działały w różnych warunkach. Połączenie eksperckiej wiedzy personelu z narzędziami opartymi na AI tworzy wielowarstwowy system obronny,

który wzmacnia bezpieczeństwo lotnictwa bez naruszania przy tym obowiązujących standardów.

Elementy programu bezpieczeństwa lotnictwa korporacyjnego

Lotnictwo ma wymiar globalny, dlatego programy AVSEC w lotnictwie korporacyjnym muszą być zgodne z międzynarodowymi standardami, przepisami regionalnymi oraz wymaganiami krajowych organów lotnictwa cywilnego. Uregulowane środowisko kształtuje każdy aspekt programu – od opracowywania polityk, przez realizację operacyjną, aż po kontrolę jakości przeprowadzaną przez zewnętrzne organy nadzorcze. Organizacje tworzą też wewnętrzne mechanizmy kontroli jakości, które obejmują weryfikację dokumentacji, obserwacje operacyjne, ustrukturyzowane wywiady z personelem oraz zarówno jawne, jak i ukryte testy procedur. Włączając te procesy do codziennej działalności, organizacje mogą wcześniej identyfikować luki, korygować nieprawidłowości oraz wykazywać przed organami regulacyjnymi, że spełniają wymagane standardy lub nawet je przewyższają. Taka proaktywna kultura zgodności jest charakterystyczną cechą bezpieczeństwa lotnictwa i rzadziej występuje w innych sektorach bezpieczeństwa prywatnego, gdzie nadzór bywa mniej rygorystyczny.

Zagrożenia dla bezpieczeństwa lotnictwa ewoluują, dlatego organizacje w ramach programu bezpieczeństwa muszą inwestować w szkolenia, budowanie świadomości oraz rozwój umiejętności pracowników na wszystkich poziomach organizacji. Personel pierwszej linii (ang. *frontline workers*) potrzebuje regularnych szkoleń dotyczących procedur kontroli, a kadra zarządzająca – w zakresie reagowania kryzysowego oraz aktualizacji przepisów. Budowanie zdolności obejmuje również adaptację technologiczną – zapewnia, że personel potrafi obsługiwać zaawansowany sprzęt do kontroli bezpieczeństwa oraz reagować na pojawiające się zagrożenia w cyberprzestrzeni. Nacisk na ciągłe kształcenie się sprawia, że organizacja pozostaje odporna na nowe wyzwania, a jednocześnie odzwierciedla on dynamiczny charakter bezpieczeństwa lotnictwa korporacyjnego w porównaniu z bardziej statycznymi środowiskami bezpieczeństwa prywatnego. Większość programów bezpieczeństwa prywatnego ogranicza się do kontekstu lokalnego lub krajowego i nie wymaga tak wysokiego poziomu koordynacji międzynarodowej.

Równie ważna jest rola globalnej wymiany informacji i współpracy sieciowej między organizacjami działającymi w sektorze lotnictwa. Korporacyjne programy AVSEC korzystają z globalnych sieci, które umożliwiają dzielenie się informacjami, najlepszymi praktykami oraz wnioskami wyciągniętymi z doświadczeń. Taka komunikacja, niezależnie od tego, czy odbywa się między stowarzyszeniami branżowymi, grupami roboczymi organów regulacyjnych czy w ramach partnerstw bilateralnych, pomaga organizacjom lepiej przewidywać zagrożenia, wdrażać sprawdzone strategie oraz dostosowywać swoje działania do światowych standardów.

Audyty bezpieczeństwa i cyberbezpieczeństwa obiektów infrastruktury krytycznej – potencjalne błędy

Dnia 3 kwietnia 2026 r. weszła w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa². Jej celem było dostosowanie krajowych regulacji do unijnej dyrektywy NIS 2³ przez zwiększenie zakresu obowiązków operatorów infrastruktury krytycznej (IK). Nowe przepisy obejmują znaczną liczbę podmiotów, w tym operatorów w sektorach takich jak energetyka, transport, ochrona zdrowia oraz usługi cyfrowe.

Jednym ze wspomnianych obowiązków jest przeprowadzanie zewnętrznych audytów bezpieczeństwa systemu informacyjnego. Skuteczność audytu w zakresie wzmocnienia odporności IK zależy od podejścia organizacji do takiej kontroli.

Przed wszystkim nie należy traktować audytów jedynie jako formalnego dostosowania do wymagań. Dyrektywa NIS 2 kładzie nacisk na ciągłe zarządzanie ryzykiem, a nie tylko okresowe kontrole. Organizacje powinny włączać wnioski z audytów do swojej strategii cyberbezpieczeństwa, tak aby wprowadzane usprawnienia były trwałe, a nie tymczasowe.

Kolejnym poważnym błędem jest ignorowanie ryzyk związanych z łańcuchem dostaw oraz podmiotami trzecimi. Dyrektywa NIS 2 wymaga od operatorów oceny ryzyk wynikających ze współpracy z dostawcami

² Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU z 2026 r. poz. 20, ze zm.).

³ Dyrektywa 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1772 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333/80 z 27 XII 2022 r.).

i usługodawcami. Wiele systemów IK opiera się na zewnętrznych wykonawcach odpowiedzialnych za oprogramowanie, sprzęt lub utrzymanie systemów. Jeśli audyty nie oceniają tych zależności, atakujący mogą wykorzystać słabe ogniwa znajdujące się poza bezpośrednią kontrolą organizacji.

Bardzo ważne jest dopilnowanie obowiązków związanych z raportowaniem incydentów oraz reagowaniem na nie. Dyrektywa NIS 2 wymaga terminowego zgłaszania incydentów cyberbezpieczeństwa do właściwych organów krajowych. Jeśli audyty nie testują zdolności reagowania na incydenty – takich jak ścieżki eskalacji, protokoły komunikacji czy współpraca z organami regulacyjnymi – organizacje mogą nie sprostać wymaganiom w sytuacji rzeczywistego kryzysu. Audyty powinny obejmować również symulacje, które pozwolą zweryfikować poziom gotowości. Wreszcie organizacje powinny łączyć audyt z planowaniem odporności.

Uzupełnieniem dyrektywy NIS 2 jest dyrektywa CER⁴, która koncentruje się na odporności fizycznej i operacyjnej podmiotów krytycznych. Jeśli audyty obejmują wyłącznie techniczne aspekty cyberbezpieczeństwa, a pomijają szersze działania zwiększające odporność – takie jak redundancja systemów, plany odtwarzania awaryjnego (ang. *disaster recovery*) czy koordynacja międzysektorowa – to IK może być narażona na ryzyka systemowe.

Podsumowując, obowiązkowe zewnętrzne audyty bezpieczeństwa IK w Polsce, gdy podejdziesz się do nich strategicznie, mogą być bardzo skutecznym narzędziem. Najważniejsze kroki to rzetelne podejście do zgodności z przepisami, uwzględnianie ryzyk w łańcuchu dostaw, zapewnienie odpowiedzialności w ramach systemu zarządzania, testowanie zdolności reagowania na incydenty oraz wprowadzenie planowania odporności.

Budowanie odporności na zagrożenia w lotnictwie cywilnym w UE – rekomendacje

Budowanie w krajach UE odporności lotnictwa cywilnego na zagrożenia wymaga kompleksowego i wielowarstwowego podejścia, które łączy nadzór regulacyjny, innowacje technologiczne oraz przygotowanie personelu. Fundament systemu stanowi przestrzeganie międzynarodowych i europejskich przepisów dotyczących bezpieczeństwa lotnictwa. Jednak odporność

⁴ 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.).

wykracza poza samą zgodność z przepisami – konieczne są proaktywne zarządzanie ryzykiem oraz zdolność do szybkiego dostosowywania się do zmieniających się zagrożeń.

Jednym z najważniejszych elementów jest wspomniana integracja zaawansowanych technologii. Systemy nadzoru wspierane przez AI, identyfikacja biometryczna przy obsłudze pasażerów czy zautomatyzowane narzędzia do kontroli ładunków przyczyniają się do skuteczniejszego wykrywania i minimalizowania ryzyka. Nieodzowne pozostaje ciągłe szkolenie oraz ocena kompetencji personelu.

Zagrożenia bezpieczeństwa często mają charakter transgraniczny, a odporność systemu zależy od terminowej wymiany informacji między organami krajowymi, liniami lotniczymi i lotniskami. Ponadto niemal każdy aspekt funkcjonowania lotnictwa wspierają systemy cyfrowe, dlatego tak istotne jest cyberbezpieczeństwo, w tym ochrona sieci przed cyberatakami oraz zapewnienie ciągłości operacji w przypadku ich zaistnienia.

Odporność na zagrożenia buduje się przez kulturę ciągłego doskonalenia. Raportowanie incydentów, audyty oraz pętla informacji zwrotnej pozwalają szybko identyfikować i eliminować słabości. Skuteczne jest podejście, w którym regulacje, technologie, wiedza i doświadczenie personelu oraz współpraca sektorowa się uzupełniają. Zaniedbanie któregośkolwiek z tych filarów osłabiłoby system, ale razem tworzą one solidną tarczę, która zapewnia, że lotnictwo w krajach UE pozostaje bezpieczne, elastyczne i cieszy się zaufaniem społeczeństwa.

Jednym z największych wyzwań w ochronie lotnisk przed terroryzmem i sabotażem jest wykrywanie insiderów. Tego typu osoby zwykle działają z powodów ideologicznych, pod przymusem lub są motywowane finansowo, a ich działania mogą być trudne do wykrycia. W tym zakresie obowiązują obecnie minimalne standardy określone w rozporządzeniu 300/2008. Obejmują one m.in. rygorystyczne sprawdzanie przeszłości pracowników, ciągłe monitorowanie personelu mającego dostęp do obszarów ograniczonego dostępu oraz obowiązkowe szkolenia z zakresu bezpieczeństwa. Lotniska są zobowiązane do wdrażania systemów kontroli dostępu, przeprowadzania wrywkowych kontroli personelu oraz egzekwowania zgłoszeń podejrzanych zachowań. Dla budowania odporności niezbędne jest wzmacnianie tych wytycznych.

Ekspertki podkreślają, że w organizacjach lotniczych powinien być kładziony większy nacisk na kulturę bezpieczeństwa, która zachęca pracowników do zachowania czujności, zgłaszania niepokojących sytuacji, a także

pozwała zrozumieć ryzyko związane z nadużywaniem uprawnień ze strony współpracowników. Organizacje powinny tworzyć środowisko, w którym pracownicy czują się odpowiedzialni za bezpieczeństwo i mają pełną świadomość zagrożeń.

Wykorzystanie rozwiązań stosowanych w lotnictwie cywilnym UE do budowania odporności na zagrożenia hybrydowe w transporcie morskim i kolejowym

Coraz większe wyzwanie dla transportowej IK stanowią zagrożenia hybrydowe, które łączą taktyki fizyczne, w cyberprzestrzeni, informacyjne, a nawet instrumenty prawne. Porty morskie i sieci kolejowe, podobnie jak lotniska, są powiązanymi systemami, których funkcjonowanie może zostać zakłócone przez sabotaż, w tym cyberataki, kampanie dezinformacyjne lub działania insiderów. Choć każdy sektor funkcjonuje we własnych realiach operacyjnych, to dorobek bezpieczeństwa lotnictwa cywilnego UE oferuje praktyki zwiększające odporność, które można zastosować w transporcie morskim i kolejowym w celu wzmocnienia ich bezpieczeństwa.

Jedną z najcenniejszych lekcji, jakie można czerpać z rozwiązań stosowanych w lotnictwie, jest przyjęcie wieloaspektowego podejścia do bezpieczeństwa opartego na ryzyku. Ochrona lotnictwa łączy wiele elementów – od kontroli pasażerów i sprawdzania ładunków po kontrolę dostępu i monitoring. To samo podejście można zastosować w transporcie morskim i kolejowym, dostosowując środki kontroli do kluczowych węzłów, takich jak terminale portowe, centra sterowania ruchem czy magazyny i terminale towarowe. Operatorzy powinni wdrażać elastyczne działania oparte na analizie wywiadowczej, które uwzględniają otwarty charakter portów i sieci kolejowych.

Warta wprowadzenia jest także dyscyplina w zakresie kontroli dostępu i systemów identyfikacyjnych. W lotnictwie wymaga się rygorystycznych sprawdzeń przeszłości pracowników, ciągłego monitorowania stref zastrzeżonych oraz wrywkowych kontroli personelu mającego do nich dostęp. W transporcie morskim i kolejowym podobne środki mogą chronić pomieszczenia sterowania, zaplecza utrzymaniowe oraz obiekty przeładunku towarów. Zarządzanie ryzykiem wewnętrznym nie powinno ograniczać się do jednorazowej weryfikacji pracownika, lecz obejmować także monitorowanie jego zachowań oraz przeprowadzanie oceny okresowej

w celu wykrycia zmian w jego sytuacji życiowej, które mogą budzić niepokój w kontekście bezpieczeństwa organizacji.

W lotnictwie ważna jest też kultura bezpieczeństwa. Ciągłe szkolenia, ćwiczenia oparte na scenariuszach oraz obowiązek zgłaszania podejrzanych zachowań pomagają tworzyć kadrę czujną i przygotowaną na zagrożenia. Operatorzy transportu morskiego i kolejowego mogą skorzystać na przyjęciu takiej kultury, aby mieć pewność, że pracownicy rozumieją zagrożenia hybrydowe i czują się upoważnieni do reagowania na nieprawidłowości. Wspólne ćwiczenia międzysektorowe z udziałem operatorów, organów regulacyjnych i służb ratunkowych wykorzystujące symulacje zagrożeń hybrydowych wzmacniają gotowość do reagowania.

Warto jednak podkreślić, że nie wszystkie praktyki, które skutecznie działają w lotnictwie, sprawdzają się w środowiskach transportu morskiego i kolejowego. Dotyczy to np. lotniskowych punktów kontroli. Przełożenie tych rozwiązań do otwartych środowisk transportu morskiego i kolejowego prowadziłoby do powstawania wąskich gardeł i nie rozwiązałoby problemów wynikających ze specyficznych podatności tych sektorów. Podobnie nadmierne poleganie na technologii bez odpowiedniego zarządzania i nadzoru człowieka może uczynić systemy podatnymi na manipulacje ze strony przeciwnika. Rozdzielone obowiązki należy zastąpić wspólnymi strukturami dowodzenia oraz współdziałającymi protokołami współpracy między agencjami.

Łącząc sprawdzone ramy wypracowane w lotnictwie z dostosowaniami specyficznymi dla danego sektora, UE może zbudować solidną tarczę chroniącą przed kampaniami hybrydowymi wymierzonymi w jej kluczowe systemy transportowe.

Bohdan Paszukow

Specjalista w zakresie lotnictwa cywilnego, autor publikacji naukowych dotyczących bezpieczeństwa lotnisk i kontroli w lotnictwie cywilnym.

Kontakt: bohdan.paszukow@gmail.com

Bezpieczniejsza Europa w lepszym świecie. European High Risk Security Network w latach 2024–2025

Pedro Nogueira
Guarda Nacional Republicana

W latach 2024–2025 European High Risk Security Network (EU-HRSN), czyli unijna sieć mundurowych formacji specjalnych ds. działań wysokiego ryzyka¹, działała pod przewodnictwem portugalskiej Guarda Nacional Republicana (GNR). W czasie tej prezydencji stopniowo przesuwano punkt ciężkości sieci z działań skupiających się na ochronie przestrzeni publicznych i szybkim reagowaniu w kierunku szerszego podejścia opartego na budowaniu odporności. Koncentrowano się na budowaniu potencjału oraz aktualnych i przyszłych zagrożeniach. Sieć umożliwia zarówno praktykom, jak i naukowcom regularne spotkania z osobami z instytucji zajmujących się zwalczaniem zagrożeń i tym samym zapoznawanie się z bieżącymi działaniami i formami współpracy na rzecz ochrony przestrzeni publicznej w okresie niestabilności geopolitycznej, konfliktów zbrojnych oraz rosnących wyzwań związanych z bezpieczeństwem i ochroną na szczeblach międzynarodowym, regionalnym i lokalnym.

¹ Więcej na temat EU-HRSN zob. G. Salazar, *Hiszpańska prezydencja w EU High Risk Security Network sprawowana przez Guardia Civil za pośrednictwem Grupo de Acción Rápida*, „Terroryzm – studia, analizy, prewencja” 2023, nr 4, s. 255–265. <https://doi.org/10.4467/27204383TER.23.026.18328>.

Powstanie i cele EU-HRSN

W odpowiedzi na wzrost liczby ataków terrorystycznych Parlament Europejski oraz Rada Unii Europejskiej przyjęły w 2017 r. dyrektywę 2017/541 w sprawie zwalczania terroryzmu². Był to kamień milowy w systemie zwalczania tego zjawiska w UE, wzmacniający podstawy prawne i operacyjne służące zapobieganiu zagrożeniom terrorystycznym i reagowaniu na nie. Na tej podstawie przyjęto unijny *Plan działania na rzecz wspierania ochrony przestrzeni publicznej*³, aby zwiększyć bezpieczeństwo i odporność obszarów ogólnodostępnych. Były to instytucjonalne i strategiczne podstawy do utworzenia sieci EU-HRSN, do czego doszło 1 listopada 2018 r. Powstała ona w celu zacieśnienia współpracy, wymiany wiedzy oraz koordynacji działań między państwami członkowskimi w dziedzinie ochrony przestrzeni publicznej, przy uwzględnianiu ograniczeń tradycyjnych środków w kontekście zmieniających się zagrożeń terrorystycznych i przestępczych. Cel ten odzwierciedla rosnącą świadomość na temat podatności tzw. celów miękkich (ang. *soft targets*), wynikającej z ich publicznego charakteru, a także z koncentracji dużej liczby osób narażonych na potencjalne zagrożenie. W tym kontekście sieć dąży do zachowania otwartości, dostępności i integracyjności przestrzeni publicznych w całej UE oraz niewprowadzania nadmiernie restrykcyjnych lub bardzo widocznych środków ochrony zbrojnej, które mogłyby osłabić funkcję społeczną tych przestrzeni. W związku z tym EU-HRSN promuje wdrażanie proporcjonalnych i skutecznych strategii ochronnych mających na celu ograniczanie podatności na zagrożenia oraz łagodzenie skutków potencjalnych ataków.

EU-HRSN działa w ramach sieci organów ścigania (ang. *law enforcement networks*) i podlega jednostce D2 ds. terroryzmu Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych (The Directorate-General for Migration and Home Affairs, DG HOME). Od czasu powstania EU-HRSN przewodniczyły jej: holenderska Royal Netherlands Marechaussee (2018–2021), hiszpańska Guardia Civil (2021–2023) oraz, jak wspomniano, portugalska Guarda Nacional Republicana (2024–2025).

² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88/6 z 31 III 2017 r.).

³ Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. *Plan działania na rzecz wspierania ochrony przestrzeni publicznej*, COM(2017) 612 final.

Struktura EU-HRSN

Ciągłość funkcjonowania sieci zależy nie tylko od zmieniającego się kierownictwa, lecz także od pamięci instytucjonalnej, czyli tego, jak jest wykorzystywane doświadczenie nabyte przy sytuacjach kryzysowych. Z tego powodu struktura EU-HRSN opiera się na stałym wsparciu ze strony biura programowego pełniącego funkcję sekretariatu, który ściśle współpracuje z poprzednią i przyszłą prezydencją (w przypadku Portugalii jest to odpowiednio hiszpańska Guardia Civil oraz francuska Gendarmerie Nationale), zapewniając spójność strategiczną w dłuższej perspektywie czasowej (okres sześciu lat).

Na poziomie taktycznym i operacyjnym sieć opiera się na trzech filarach: grupy robocze, współpraca i koordynacja oraz projekty i inicjatywy. Centrum sieci stanowią grupy robocze opracowujące kluczowe tematy, które zostały formalnie zatwierdzone przez Komisję Europejską (KE): Risk Assessment, UAS & C-UAS⁴, Tactical Rescue Response, Human Factor oraz Protective Security Advise & Coordination for Major Events (rysunek 1). Filar współpracy i koordynacji zapewnia stały kontakt z zainteresowanymi stronami, filar projektów i inicjatyw zapewnia natomiast doraźne wsparcie przy konkretnych wydarzeniach, takich jak szkolenia, konferencje czy webinary⁵.



Rysunek 1. Struktura i grupy robocze sieci EU-HRSN.

Źródło: materiały własne EU-HRSN.

⁴ UAS (ang. *unmanned aerial system*) – bezzałogowy system powietrzny; C-UAS (ang. *counter-unmanned aerial system*) – system zwalczania bezzałogowych systemów powietrznych (przyp. red.).

⁵ Zob. <https://hrsnu.eu/sample-page/>.

Odpowiedzialność za zarządzanie siecią spoczywa na grupie sterującej, zgodnie z decyzją podjętą większością głosów podczas pierwszej konferencji ogólnej prezydencji (zdjęcie 1). W skład grupy sterującej wchodzi: poprzedni przewodniczący, wiceprzewodniczący (który obejmie funkcję przewodniczącego), koordynatorzy grup roboczych, obserwator z KE oraz zaproszeni eksperci.



Zdjęcie 1. Konferencja ogólna EU-HRSN, 22 lutego 2024 r.

Źródło: materiały własne EU-HRSN.

Podejście koncepcyjne i osiągnięcia portugalskiej prezydencji

Zgodnie z *Planem działania na rzecz ochrony przestrzeni publicznej* EU-HRSN skupia przedstawicieli 41 wyspecjalizowanych jednostek organów ścigania z 30 krajów⁶, w tym partnerów spoza UE, m.in. amerykańskiego Federalnego Biura Śledczego (Federal Bureau of Investigation, FBI) czy policję nowojorską (New York Police Department, NYPD), jak również siły interwencyjne z Kenii, Ghany czy Senegalu. EU-HRSN korzysta ponadto ze wsparcia DG HOME oraz Protective Security Advisors (PSA), czyli programu grupy unijnych doradców ds. budowania odporności na zagrożenia, który zapewnia kontakt z ekspertami ds. bezpieczeństwa i oceny ryzyka. EU-HRSN ściśle współpracuje ze Wspólnym Centrum Badawczym Komisji Europejskiej (Joint Research Centre, JRC), projektami PRESERVE, ESIWA+

⁶ Zob. <https://hrsn.eu>.

i Public Spaces+ oraz z innymi sieciami organów ścigania (AIRPOL, AQUA-POL, ATLAS, EIFS, ENLETS, ESG i RAILPOL) pod koordynacją DG HOME D2 Komisji Europejskiej.

Sieć przyjęła podejście oparte na studiach przypadków (rysunek 2), polegające na dogłębnej analizie ataków terrorystycznych, do których doszło w Europie w ciągu ostatnich dwóch dekad, oraz innych zdarzeń (rysunek 3). To ciągle doksztalcanie się, jak uniknąć ataków i zapobiec im w przyszłości. EU-HRSN wspiera komisje UE i kraje członkowskie w określaniu priorytetów, strategii i mechanizmów mających na celu powstrzymanie zagrożeń, zapobieganie im, łagodzenie ich skutków, przy jednoczesnym badaniu obecnych i przyszłych wyzwań, rozpoznawaniu słabych punktów systemu oraz pracy nad potrzebami w zakresie budowania potencjału. Podstawą podejścia opartego na studiach przypadków jest teoria „Pathway to violence” (pol. droga do przemocy), która wywodzi się z badań behawioralnych przeprowadzonych przez Fredericka Calhouna i Steve’a Westona w 2016 r.⁷ Teoria ta przedstawia ogólny model wyjaśniający, w jaki sposób i dlaczego dochodzi do aktów przemocy o ukierunkowanym charakterze. Określa ona również ramy służące do rozpoznawania zagrożeń, zapobiegania im i radzenia sobie z nimi, co może pozwolić przerwać łańcuch przemocy i zapobiec takim aktom.



Rysunek 2. Podejście oparte na studiach przypadków.

Źródło: materiały własne EU-HRSN.

⁷ *Pathway to Violence*, CISA, 24 II 2023 r., <https://www.cisa.gov/resources-tools/resources/pathway-violence> [dostęp: 17 VI 2026].



Rysunek 3. Wybrane zdarzenia z 2025 r. analizowane przez EU-HRSN.

Źródło: materiały własne EU-HRSN.

Unidade de Intervenção (GNR Intervention Unit)⁸, jednostka GNR, która reprezentuje portugalską prezydencję, dysponuje wysoce wyspecjalizowanymi siłami w takich obszarach jak: kontrola tłumu i zamieszek (ang. *crowd and riot control*), działania typu SWAT i operacje specjalne, neutralizacja materiałów wybuchowych i bezpieczeństwo obiektów podziemnych (ang. *explosives and underground security*), działania z wykorzystaniem psów służbowych (K9). Ma także zdolności w zakresie szkolenia przedoperacyjnego. Szeroki zakres działań jednostki pozwolił na łatwe powiązanie jej z szeregiem międzynarodowych sieci specjalistycznych funkcjonujących w ramach europejskich struktur – takich jak m.in. ATLAS, ENLETS, PSA, EOD, RAILPOL, FRONTEX czy CEPOL. Umożliwiło to sieci HRSN skuteczną współpracę z innymi podmiotami zaangażowanymi w ochronę przestrzeni publicznych, opartą na wielopoziomowym i zintegrowanym podejściu.

Podczas portugalskiej prezydencji sieć wspierała opracowywanie i ujednolicanie taktyk, technik i procedur, przygotowywanie wytycznych oraz treści technicznych i taktycznych, gromadzenie i rozpowszechnianie wyciągniętych wniosków, a także rozwój zdolności w zakresie ochrony przestrzeni publicznych. Dzięki dynamicznej działalności pięciu istniejących grup sterujących oraz stałej współpracy z innymi sieciami, projektami

⁸ GNR – Unidade de Intervenção, profil na Facebooku, <https://www.facebook.com/gnr.ui.intervencao> [dostęp: 17 VI 2026].

i europejskimi forami zajmującymi się tym zagadnieniem udało się wnieść cenny wkład we wzmocnienie wymienionych najważniejszych obszarów bezpieczeństwa, co jest w pełni zgodne z celami zatwierdzonymi wcześniej przez KE.

Spośród 104 aktywności podjętych przez sieć oraz inicjatyw z jej udziałem⁹ (brało w nich udział 1097 ekspertów EU-HRSN), warto wymienić przede wszystkim następujące przykłady szkoleń i ćwiczeń:

- szkolenie Advanced Operators Counter-Unmanned Aircraft Systems Training Course, realizowane we współpracy z laboratorium JRC C-UAS w Belgii, mające na celu wzmocnienie technicznych i taktycznych zdolności w zakresie przeciwdziałania bezzałogowym statkom powietrznym;
- szkolenie Search, Detect and React Training Course, wdrażane we współpracy z policją litewską (1. edycja) oraz grecką (2. edycja), mające na celu poprawę wykrywalności podejrzanych zachowań w miejscach publicznych;
- treningi i ćwiczenia Tactical Rescue Response przeprowadzone w Irlandii (1. edycja) i Hiszpanii (2. edycja), mające poprawić interoperacyjność służb ratowniczych w sytuacjach ataku zbrojnego. Odbłyły się one z udziałem specjalistów z wielu krajów, którzy mają doświadczenie w pracy w policji, służbach ratowniczych i siłach zbrojnych;
- warsztaty i ćwiczenia symulacyjne Workshop and Table Top Exercise on Protective Security Advice and Coordination, zorganizowane w Portugalii, mające na celu wzmocnienie koordynacji działań podejmowanych przez różne podmioty i organizacje w sytuacjach kryzysowych;
- organizacja kilku telekonferencji, w których wzięło udział szerokie grono partnerów zajmujących się ochroną przestrzeni publicznej. Miały one na celu dzielenie się wiedzą i doświadczeniami na temat takich zagadnień jak handel bronią, druk 3D, studia przypadków dotyczące aktywnych strzelców i zagrożeń wewnętrznych, szacowanie ryzyka i zarządzanie nim, wnioski wyciągnięte z działań związanych z zapewnieniem bezpieczeństwa podczas XXXIII Letnich Igrzysk Olimpijskich w Paryżu oraz wizyty papieża Franciszka

⁹ Tamże.

w Fatimie, systemy barier drogowych, wykrywanie podejrzanego zachowania czy narzędzia wsparcia technologicznego JRC.

Za jedno z najważniejszych osiągnięć sieci w czasie portugalskiej prezydencji uważa się wdrożenie mechanizmu Pool & Sharing (P&S). To innowacyjne rozwiązanie, które umożliwia sprawne mobilizowanie wyspecjalizowanych zasobów oraz ekspertów w celu wzmocnienia bezpieczeństwa podczas międzynarodowych wydarzeń o podwyższonym ryzyku. Mechanizm polega na wysyłaniu w miejsce takich wydarzeń zespołów wsparcia technicznego o charakterze niewykonawczym (ang. *non-executive technical support teams*). Dzięki temu są wzmacniane zdolności państw członkowskich do przygotowywania i przeprowadzania złożonych działań związanych z bezpieczeństwem w sytuacji ograniczonych zasobów i wysokich wymagań operacyjnych.

Jednym z przykładów wykorzystania tego mechanizmu była operacja „Dawid”, polegająca na celu zapewnieniu bezpieczeństwa podczas wizyty prezydenta Ukrainy Wołodymyra Zełenskiego w Irlandii. Od czasu operacji mechanizm P&S był uruchamiany 10 razy, co dało łącznie 58 dni operacyjnych (470 godzin) oraz bezpośrednie zaangażowanie 47 ekspertów policyjnych z krajów członkowskich. To wyraźnie pokazuje, jakim zaufaniem obdarzono EU-HRSN, oraz uwydatnia zdolność sieci do przekształcania współpracy międzynarodowej w szersze działania operacyjne.

Wyzwania

W przyszłości wyzwania dla EU-HRSN związane z bezpieczeństwem wymagają przejścia od wąskiego skupienia się na ochronie, prewencji i szybkim reagowaniu do szerszego, przekrojowego podejścia. Cele to: utrzymanie funkcjonalnego środowiska operacyjnego w dobie kryzysów, wzmocnienie odporności na zagrożenia i podwyższenie poziomu gotowości w ramach rozwoju kultury bezpieczeństwa i ochrony, a także inwestowanie w bezpieczeństwo już na etapie projektowania. Zgodnie z tym podejściem do wspólnie organizowanych działań powinno się angażować służby bezpieczeństwa, służby ratownicze oraz jednostki specjalistyczne, społeczeństwo, a także polityków w ramach stałego uczenia się budowy potencjału.

Odpowiadając na to wyzwanie, należy udostępnić partnerom i zainteresowanym podmiotom z sektora przestrzeni publicznej sprawdzone praktyki i innowacyjne rozwiązania, które pomogą wypełnić lukę między

badaniami nad bezpieczeństwem a potrzebami operacyjnymi. Trzeba skupić się na nowych i pojawiających się zagrożeniach bezpieczeństwa oraz zapewnić niezbędną synergię operacyjną między komponentami: cywilnym, policyjnym i wojskowym.

Mechanizmy P&S, które w *Planie działania na rzecz ochrony przed dronami i zwalczania dronów* (*Action Plan on Drone and Counter-Drone Security*)¹⁰ zostały określone jako „zespoły szybkiego reagowania kryzysowego przy użyciu dronów”, muszą być w stanie zapewnić działania transgraniczne oraz wysyłać wyspecjalizowane jednostki mobilne w przypadku wydarzeń wysokiego ryzyka i o dużym znaczeniu, przy jednoczesnym zachowaniu interoperacyjności. Taki mechanizm jest uruchamiany na wniosek organu państwa członkowskiego w ramach europejskiej pomocy wzajemnej.

Podejście *security by design* (bezpieczeństwo na etapie projektowania) powinno być podstawową zasadą stosowaną przy kształtowaniu przestrzeni publicznej. Na przykład koncepcje projektowe wejść do budynków i otwartych przestrzeni (m.in. strefy kontroli dostępu i szlabany dla pojazdów) mogą ograniczać ryzyko i zapobiegać wtargnięciom osób niepożądanych. Władze lokalne powinny nadać priorytet we włączaniu podmiotów zajmujących się bezpieczeństwem i ochroną w proces aktualizacji planów urbanistycznych. Takie połączenie wiedzy m.in. architektów, urbanistów i policji pozwoli wdrażać optymalne, ekonomiczne, wielofunkcyjne i akceptowalne społecznie rozwiązania¹¹.

Ponadto ujednolicenie unijnej metodologii procesu oceny ryzyka to ważny krok w kierunku stworzenia wspólnego modelu oceny zagrożeń związanych z terroryzmem oraz pierwszy krok w stronę wypracowania wspólnego podejścia do etapu przygotowania i planowania. EU-HRSN oraz PSA już podjęły wysiłek w tej dziedzinie – zaproponowały trzystopniowy model skupiający się na planach i możliwościach, zagrożeniach i słabych punktach. Pozwoli to na ujednolicenie procedur i ułatwi rozpowszechnianie dobrych praktyk wśród wszystkich państw członkowskich. Zastosowana metodologia opierała się na następujących założeniach: jasne określenie podmiotu odpowiedzialnego za ryzyko; poziom i charakter zagrożenia na podstawie modus

¹⁰ *Plan działania na rzecz ochrony przed dronami i zwalczania dronów*, Komisja Europejska, <https://digital-strategy.ec.europa.eu/en/policies/drone-security> [dostęp: 17 VI 2026].

¹¹ M. Larcher, V. Karlos, R. Schumacher, D. Strezova, A. Caverzan, J. Coaffee, B. Moritz, A.V. Neves, S. Ilum, N. Gebbeken, A. Schröder, M. Schlüter, P. Warnstedt, M. Stewart, *Security by Design: Protection of public spaces from terrorist attacks*, JRC131172. Tekst jest dostępny na stronie: <https://publications.jrc.ec.europa.eu/repository/handle/JRC131172>.

operandi (scenariusza), wrogie zamiary, możliwości i szanse; najgorsze możliwe konsekwencje; poziom podatności na zagrożenia oraz ryzyko rezydualne; zalecenia dotyczące środków ograniczających ryzyko.

Przyjęcie unijnego programu działań w zakresie zapobiegania i przeciwdziałania terroryzmowi i brutalnemu ekstremizmowi¹² podkreśla potrzebę inwestowania w rozwiązania służące wczesnemu wykrywaniu zagrożeń oraz w innowacje mające na celu ochronę obywateli i przestrzeni publicznej przed zagrożeniami związanymi z materiałami wybuchowymi, dronami, bronią drukowaną w technologii 3D, atakami z użyciem pojazdów oraz bronią białą. Ponadto unijny program za kluczowe uznaje wsparcie dla testowania i wdrażania finansowanych przez UE rozwiązań służących doposażeniu organów ścigania. Są to obszary, w których sieć aktywnie angażuje się za pośrednictwem swoich grup roboczych w prace rozwojowe.

Zgodnie z dyrektywą w sprawie odporności podmiotów krytycznych¹³ nacisk w zakresie ochrony przestrzeni publicznej, zapobiegania zagrożeniom i natychmiastowej reakcji na nie jest przenoszony na większe wyzwania. Uwzględniana jest przy tym odporność jako coraz ważniejszy element struktury całego systemu walki z terroryzmem i zagrożeniami hybrydowymi. Podmioty prywatne i publiczne muszą być bardziej niż kiedykolwiek przygotowane do przeciwdziałania zdarzeniom, które mogą zakłócić funkcjonowanie podstawowych usług, łagodzenia ich skutków oraz podejmowania działań naprawczych.

Podsumowanie

W latach 2024–2025 EU-HRSN rozwinęło się pod względem liczby partnerów i możliwości. Umocniło swoją pozycję znaczącego europejskiego i międzynarodowego podmiotu działającego na rzecz ochrony przestrzeni publicznej przez organizację konferencji, spotkań ekspertów, warsztatów, programów szkoleniowych oraz międzynarodowych ćwiczeń. W ramach

¹² Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. *ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska*, COM(2026) 101 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52026DC0101> [dostęp: 17 VI 2026].

¹³ 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.).

tych działań dzielono się sprawdzonymi rozwiązaniami oraz opracowywano procedury na poziomie technicznym, taktycznym i operacyjnym.

EU-HRSN to coś więcej niż forum współpracy – wykracza ono bowiem poza swoje pierwotne zadania i staje się aktywną platformą bezpieczeństwa służącą poszerzaniu wiedzy i budowaniu specjalistycznych zdolności w zakresie ochrony wydarzeń wysokiego ryzyka oraz przestrzeni publicznych. Przekształca współpracę w ustrukturyzowane narzędzie zapewniające realny i skuteczny wpływ na codzienne potrzeby w zakresie bezpieczeństwa.

12 lutego 2026 r. portugalskie przewodnictwo nad siecią zostało symbolicznie przekazane francuskiemu odpowiednikowi GNR – Gendarmerie Nationale, która faktycznie objęła je od 1 marca. Przejęcie obowiązków nie powinno być postrzegane jako zakończenie działań poprzedników, lecz jako okazja do nabrania nowej energii, wykorzystania dynamiki wypracowanej w ramach poprzedniej prezydencji, pamięci instytucjonalnej oraz wiarygodności sieci operacyjnej w celu wdrożenia i konsolidacji planów działania oraz programu prac KE.

Zaangażowanie portugalskiej GNR w krajową i międzynarodową współpracę dotyczącą interwencji specjalistycznych oraz ochrony przestrzeni publicznej będzie w pełni kontynuowane w ramach EU-HRSN oraz na różnych platformach. GNR uczestniczy w nich jako proaktywny, dynamiczny i kompetentny partner, w pełni świadomy tego, że dzięki wspólnej pracy i koordynacji wysiłków będziemy lepiej przygotowani do stawiania czoła wyzwaniom związanym z bezpieczeństwem.

Płk Pedro Nogueira

Przewodniczący High Risk Security Network (HRSN) w latach 2024–2025.

Kontakt: presidency@hrs.eu

Młodzież a bezpieczeństwo państwa. Społeczne uwarunkowania podatności na radykalizację w świetle raportu „Diagnoza Młodzieży 2026”

Paweł Rabiej

Uczelnia Korczaka

 <https://orcid.org/0009-0008-4531-8684>

Konrad Ciesiołkiewicz

Uczelnia Korczaka

 <https://orcid.org/0000-0001-6926-3448>

Wzrastająca podatność młodych ludzi na radykalizację, dezinformację i wpływy społeczne prowadzące do destabilizacji, wzmacniana kryzysami psychicznymi tych osób, osłabieniem relacji społecznych, poczuciem wykluczenia oraz funkcjonowaniem w środowisku cyfrowym stanowi wyzwanie dla bezpieczeństwa państwa. Analizy zagrożeń w tym zakresie stosunkowo rzadko uwzględniają specyfikę wyzwań społecznych dotyczących młodego pokolenia. Opublikowany wiosną raport *Diagnoza Młodzieży 2026*¹ wskazuje na szereg czynników sprzyjających radykalizacji i prowadzących do zachowań szkodliwych z perspektywy bezpieczeństwa państwa, na które

¹ *Diagnoza Młodzieży 2026*, P. Rabiej (red.), Warszawa 2026.

wpływ ma również odporność psychospołeczna i informacyjna młodych ludzi – ich zdolność do radzenia sobie z kryzysami, dezinformacją, polaryzacją i presją środowiska cyfrowego. Takie opracowania powinny być jednym z elementów analizy ryzyk związanych z zagrożeniami o charakterze terrorystycznym. Dzięki ich wnikliwej analizie można skuteczniej przewidywać właściwą w danym czasie trajektorię procesów radykalizacji, prowadzących do przemocy, w tym działań skierowanych przeciwko państwu. Holistyczne diagnozy tego typu stanowią również cenny wkład Polski w przeprowadzane w innych krajach badania nad społeczno-ekonomicznymi kontekstami radykalizacji.

Obraz młodzieży i młodych dorosłych

Autorzy *Diagnozy Młodzieży 2026* w swoich badaniach skoncentrowali się na pokoleniu Z, czyli osobach urodzonych w latach 1996–2012. Na potrzeby badania przyjęli podział na dwie podstawowe grupy: młodzież w wieku 15–18 lat oraz młodych dorosłych w wieku 19–29 lat. Taki zakres definicyjny jest zgodny z rozwiązaniami stosowanymi w większości europejskich strategii młodzieżowych oraz dokumentów polityk publicznych dotyczących młodego pokolenia.

W publikacji zanalizowano ponad 220 raportów, badań i opracowań eksperckich opublikowanych głównie w latach 2020–2025 na temat różnych aspektów życia młodego pokolenia w Polsce i Europie. Uwzględniono w niej źródła zarówno krajowe, jak i międzynarodowe, w tym raporty instytucji publicznych, organizacji międzynarodowych, ośrodków badawczych oraz strategie młodzieżowe obowiązujące w państwach Unii Europejskiej.

Na potrzeby publikacji przeprowadzono reprezentatywne badania ilościowe młodzieży i młodych dorosłych, a także badania pracowników instytucji sektora edukacji, pomocy społecznej, ochrony zdrowia, kultury oraz organizacji pracujących z młodzieżą. Analizę uzupełniono badaniami jakościowymi dotyczącymi zarówno środowiska rodzinnego i relacji społecznych młodych ludzi, jak i kwestii związanych z ich tożsamością, dobrotanem psychicznym czy kapitałem psychologicznym. Uwzględniono zagadnienia z obszaru funkcjonowania młodzieży w środowisku cyfrowym, m.in. wpływ mediów społecznościowych, dezinformację, przemoc online i algorytmizację przekazu. Zanalizowano również środowisko edukacyjne, zaangażowanie obywatelskie młodych ludzi, ich sytuację na rynku pracy,

poziom stabilności zatrudnienia oraz strategię usamodzielniania, w tym bariery mieszkaniowe i ekonomiczne związane z wejściem w dorosłość.

Istotną wartością *Diagnozy Młodzieży 2026* jest przyjęcie interdyscyplinarnej perspektywy, łączącej dorobek polityki społecznej, socjologii, psychologii, pedagogiki, badań nad mediami cyfrowymi oraz analiz polityk publicznych. Pozwoliło to na wielowymiarowe ujęcie sytuacji młodych ludzi, uwzględniające zarówno ich doświadczenia indywidualne i relacje społeczne, jak i szersze uwarunkowania instytucjonalne, kulturowe czy strukturalne. W analizie zastosowano perspektywę trajektorii życia (ang. *life course approach*), rozwijaną przede wszystkim przez Glena H. Eldera Jr. U jej podstaw leży założenie, że przebieg życia jednostki jest kształtowany przez sekwencję wzajemnie powiązanych doświadczeń, punktów przejścia i kumulujących się czynników ryzyka oraz zasobów społecznych. Pozwoliło to m.in. na uchwycenie kumulacji ryzyk i punktów krytycznych pojawiających się na kolejnych etapach dorastania i wchodzenia w dorosłość².

Sytuację młodego pokolenia ujęto w raporcie zarówno w perspektywie bieżących wyzwań społecznych, jak i w kontekście długotrwałych przemian kulturowych, technologicznych i cywilizacyjnych z ostatnich 2–3 dekad. Trendy te mają charakter kumulatywny i wzajemnie się wzmacniają. Wpływają na dobrostan młodych ludzi, poziom spójności społecznej i bezpieczeństwa państwa. Współcześnie funkcjonują oni w warunkach silnej indywidualizacji życia, coraz wyraźniej widocznym skupianiu się na autonomii, własnych potrzebach i dobrostanie psychicznym. Rosnąca koncentracja na „ja”, przy jednoczesnym osłabieniu relacji i wspólnotowości, zwiększa podatność jednostek na wpływ środowisk oferujących silną tożsamość grupową i uproszczone narracje rzeczywistości. Zmiany te zachodzą równocześnie z cyfryzacją codziennego życia. Aż 71% młodych deklaruje, że ich pokolenie jest uzależnione od telefonów. Ponad 80% dzieci zakłada konta w mediach społecznościowych przed ukończeniem 13. roku życia, a średni czas online sięga niemal pięciu godzin dziennie³. Tendencje

² Zob. szerzej: G.H. Elder Jr., M.K. Johnson, R. Crosnoe, *The Emergence and Development of Life Course Theory*, w: *Handbook of the Life Course*, J.T. Mortimer, M.J. Shanahan (red.), New York 2003, s. 3–19; D. Woodman, J. Wyn, *Youth and Generation: Rethinking Change and Inequality in the Lives of Young People*, London 2015.

³ Zob. szerzej: A. Ładna, K. Kamiński, K. Rosłaniec, A. Wrońska, M. Błażej, A. Jankiewicz, F. Konopczyński, M. Nawrot, *Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców*, Warszawa 2025.

wzmacnia funkcjonowanie młodego pokolenia w warunkach chronicznego napięcia i poczucia niepewności. Niemal połowa nastolatków ma skrajnie niską samoocenę, a prawie co piąty uczeń w wieku 13–17 lat w ciągu ostatniego roku dokonał samookaleczeń⁴.

Pięć przyczyn podatności młodzieży na zachowania ryzykowne

Jak wynika z raportu, nadmierne korzystanie przez młodzież ze środowiska cyfrowego, pogarszający się dobrostan psychiczny, osłabienie relacji społecznych, kryzys więzi i samotność, problemy w szkole, na rynku pracy i w usamodzielnianiu się nie mają tylko charakteru odrębnych „wyzwań sektorowych”. Tworzą one układ czynników ryzyka, który może prowadzić do wykluczenia i osłabienia integracji społecznej, a także zwiększać podatność młodych ludzi na radykalizację, polaryzację oraz zachowania stanowiące zagrożenie dla bezpieczeństwa własnego i publicznego. Szczegółne znaczenie ma nagromadzenie różnych napięć psychospołecznych i środowiskowych.

Wnioski te są zgodne ze współczesnymi interpretacjami rozwijanymi w literaturze naukowej oraz raportach instytucji europejskich zajmujących się bezpieczeństwem i zapobieganiem ekstremizmowi. W raporcie *The Root Causes of Violent Extremism* przygotowanym przez Radicalisation Awareness Network opisano radykalizację jako kalejdoskop czynników obejmujący doświadczenia jednostkowe, społeczne, ekonomiczne, polityczne i cyfrowe⁵. W tym ujęciu omówiono wzajemnie wzmacniające się konfiguracje ryzyka, nakładające się doświadczenia marginalizacji, osłabienia więzi społecznych, kryzysów tożsamościowych, przeciążenia psychicznego, depriwacji politycznej oraz funkcjonowania w spolaryzowanym środowisku cyfrowym. Na tej podstawie można wskazać pięć kluczowych przyczyn zwiększających podatność młodego pokolenia w Polsce na narracje ekstremistyczne, przemoc symboliczną, wycofanie obywatelskie, radykalizację, skrajne postawy i zachowania destabilizujące bezpieczeństwo społeczne.

⁴ Zob. szerzej: M. Dębski, J. Pyżalski, J. Borchet, H. Witkowska, *Dobre i złe wiadomości – życie online i offline a zdrowie psychiczne polskich nastolatków. Raport z badań*, Gdańsk 2025.

⁵ M. Ranstorp, M. Meines, *The Root Causes of Violent Extremism*, Luxembourg 2024; Europol, *European Union Terrorism Situation and Trend Report 2025*, Luxembourg 2025.

Subiektywne poczucie niesprawiedliwości, marginalizacji i krzywdy

Jednym z kluczowych mechanizmów zwiększających podatność na radykalizację młodych ludzi w Polsce jest subiektywne poczucie niesprawiedliwości, marginalizacji oraz braku uznania społecznego. Ma on charakter emocjonalny i interpretatywny – istotne znaczenie ma nie tyle obiektywna sytuacja społeczna jednostki, ile sposób postrzegania własnego miejsca w społeczeństwie, relacji z instytucjami oraz możliwości wpływu na rzeczywistość społeczną. W literaturze dotyczącej radykalizacji poczucie krzywdy (ang. *grievance*) jest uznawane za jeden z najsilniejszych predyktorów podatności na narracje ekstremistyczne, szczególnie w sytuacjach kumulacji frustracji, deprywacji i osłabienia więzi społecznych⁶.

Znaczna część młodego pokolenia doświadcza poczucia „niewidzialności” i „nieważności” społecznej. Znajduje to potwierdzenie w wielu wskaźnikach opisujących relacje młodych ludzi z państwem, instytucjami i społeczeństwem. Jedynie 22% młodych osób uważa, że ich głos jest uwzględniany w procesach podejmowania decyzji publicznych, co należy do najniższych wyników w krajach OECD (ang. Organisation for Economic Co-operation and Development). Równocześnie tylko 35% młodych Polaków pozytywnie ocenia jakość usług publicznych, a w badaniach uczestnicy wielokrotnie wskazywali, że polityki publiczne są projektowane przede wszystkim z myślą o starszych grupach wiekowych. W efekcie młodzi często postrzegają siebie jako grupę pozbawioną realnego wpływu na decyzje dotyczące ich przyszłości. Takie osoby są przekonane, że ich potrzeby, styl życia i wartości nie są traktowane podmiotowo. W badaniach jakościowych młodzi dorośli używali takich określeń, jak „obywatele troszkę drugiej kategorii” czy „nikt nas nie słucha – w domu, w szkole, w państwie”. Poczucie marginalizacji jest wzmacniane paternalistycznym i niepodmiotowym traktowaniem młodzieży m.in. przez system edukacji, rynek pracy, partie polityczne, co wywołuje poczucie ograniczonego wpływu na życie społeczne. W takich warunkach radykalizacja może być postrzegana jako forma odzyskania wpływu, sprawczości i satysfakcji z działania.

Chroniczne napięcie i lęk, poczucie niepewności

Młodzi ludzie funkcjonują w silnym napięciu i lęku, permanentnej niepewności społecznej, ekonomicznej i geopolitycznej, co obniża ich poczucie

⁶ Por. A.W. Kruglanski, J.J. Bélanger, R. Gunaratna, *The Three Pillars of Radicalization: Needs, Narratives, and Networks*, Oxford 2019.

bezpieczeństwa. Silnym źródłem napięć są obawy ekonomiczne oraz lęki związane z sytuacją globalną – 69% młodych dorosłych obawia się wybuchu wojny⁷, 57% odczuwa niepewność w związku z rosnącymi kosztami utrzymania, ponad połowa lęka się konsekwencji zmian klimatycznych czy demograficznych⁸. Źródłem napięcia są też obawy o miejsca pracy – dotyczą one już nastolatków w wieku 14–15 lat i są efektem „transferu lęków” rodziców, którzy doświadczyli trudności na rynku pracy. Większość nastolatków (78%) boi się, że nie znajdzie odpowiedniego zatrudnienia, a 58% młodych dorosłych wskazuje brak stabilności zatrudnienia jako kluczowy problem utrudniający wejście w dorosłość. Wzmacnia to nastroje antyimigranckie młodzieży – aż 68% osób w wieku 18–24 lata niepokoi perspektywa masowych migracji zarobkowych do Europy. Jest to, obok wojny, jedno z najczęściej wskazywanych zagrożeń przyszłości. Jednocześnie 55% uczestników badania uważa, że migranci zaniżają płace, 66% – zwiększają przestępczość, a 69% – obciążają system świadczeń społecznych⁹.

Wysoki poziom frustracji pokolenia Z wywołuje sytuacja mieszkaniowa. Luka czynszowa oraz niski dostęp do instrumentów wsparcia powodują, że odsetek młodych dorosłych pozostających w domu rodzinnym systematycznie rośnie. Według badań CBOS niemal 39% osób stanu wolnego w wieku od 25 do 34 lat mieszka z rodzicami. Dla porównania w 2005 r. wskaźnik ten wynosił 29%¹⁰. Czynniki składające się na „zablokowaną dorosłość” są przyczyną głębokiej frustracji ponad połowy populacji młodych dorosłych, którzy reagują na ten stan rzeczy gniewem, lękiem i poczuciem zagrożenia. Sprzyja temu infodemia w środowisku cyfrowym, czyli nadmiar informacji, w których trudno odróżnić prawdę od kłamstw i manipulacji, a także trybalizacja dyskursu, bańki informacyjne i niski poziom edukacji medialnej. Wojna, migracje, niepewność ekonomiczna, rosnące koszty życia, konkurencja o miejsca pracy i pozycję społeczną wzmacniają potrzebę prostych odpowiedzi oraz podziałów typu my – oni.

⁷ *Młodzi Polacy o wyzwaniach stojących przed ich pokoleniem*, „Komunikat z badań CBOS” 2025, nr 56, oprac. J. Scovil, Warszawa 2025.

⁸ Zob. szerzej: European Parliament, *Eurobarometer Youth Survey 2024*, Brussels 2025.

⁹ *Młodzi Polacy o wyzwaniach...*

¹⁰ *Młodzi dorośli w domu rodzinnym*, „Komunikat z badań CBOS” 2025, nr 108, oprac. D. Litwin, Warszawa 2025.

Doświadczenie wykluczenia, marginalizacji, przemocy i upokorzenia

Jako trzeci mechanizm skłaniający młodzież i młodych dorosłych do zachowań radykalnych i zagrażających bezpieczeństwu wskazano w raporcie poczucie deprywacji. W 2023 r. skrajne ubóstwo dotyczyło 7,6% osób w wieku 0–17 lat (ok. 521 000 dzieci), co było najwyższym poziomem od 2015 r. oraz oznaczało wzrost o ok. 125 000 osób względem roku poprzedniego¹¹. Pomimo relatywnie korzystnej sytuacji gospodarczej Polski oraz bardzo dobrej kondycji rynku pracy na tle państw UE, ok. 10% młodych osób w wieku 15–29 lat pozostaje poza edukacją, zatrudnieniem i systemem szkoleń (ang. *not in education, employment or training*, NEET). Wiąże się to z ryzykiem trwałego wykluczenia społecznego i niestabilnych trajektorii wejścia w dorosłość. Co najmniej jednej z form zaniedbania doświadczyło ok. 23% osób w wieku 11–17 lat, przy czym najczęściej było to zaniedbanie emocjonalne¹².

Czynnikiem ryzyka jest wzrost przemocy wobec dzieci i młodzieży. Zgodnie z raportem Fundacji Dajemy Dzieciom Siłę (FDDS) aż 1/3 osób do 18. roku życia doświadczyła różnych form agresji ze strony najbliższych, a nawet 1/4 nastolatków w wieku 11–17 lat mogła doznać wykorzystywania seksualnego¹³. Na nasilenie zjawiska przemocy zwróciło uwagę 67% pracowników instytucji pracujących z młodzieżą, którzy wzięli udział w badaniach przeprowadzonych na potrzeby raportu. Wykluczenie i marginalizacja występują też w środowisku rodzinnym. Co czwarta osoba w wieku 15–19 lat nie odczuwa wsparcia i akceptacji ze strony rodziny. Z kolei w środowisku szkolnym 62% uczniów doświadczyło różnych form przemocy rówieśniczej¹⁴. Najnowsze badania FDDS wskazują, że przemoc rówieśnicza stała się doświadczeniem powszechnym. Według raportu *Rówieśnicy. Raport o przemocy rówieśniczej 2026* aż 87% dzieci i młodzieży w wieku 10–17 lat doświadczyło co najmniej jednej formy przemocy ze strony rówieśników, 75% zetknęło się z cyberprzemocą, a 63% z przemocą fizyczną. Szczególnie niepokojące jest to, że niemal co trzeci młody człowiek (31%)

¹¹ R. Szarfenberg, *Poverty Watch 2025*, Warszawa 2025.

¹² K. Makaruk, K. Drabarek, A. Popyk, S. Wójcik, *Diagnoza przemocy wobec dzieci w Polsce 2023*, Warszawa 2023, s. 6.

¹³ Tamże.

¹⁴ Zob. szerzej: R. Kaczan, P. Rycielski, M. Wójcik, *Obraz bullyingu w szkołach ponadpodstawowych*, https://swps.pl/images/DOKUMENTY/Raporty/Obraz-bullyingu-w-szkolach-ponadpodstawowych-raport-2025.pdf?utm_source=mautic&utm_medium=mailing [dostęp: 24 VI 2026].

doświadczał powtarzalnego dręczenia (z ang. *bullying*), które zgodnie z literaturą przedmiotu należy do najbardziej szkodliwych form przemocy rówieśniczej¹⁵.

Badania nad bullyingiem wskazują, że długotrwała przemoc, odrzucenie i marginalizacja zwiększają skłonność młodych ludzi do poszukiwania alternatywnych wspólnot zapewniających poczucie przynależności, znaczenia i sprawczości. Doświadczenie wykluczenia oraz „społecznej niewidzialności” może osłabiać zaufanie do instytucji, podczas gdy środowiska radykalne oferują emocjonalną wspólnotę, poczucie siły, a także symboliczną kompensację wcześniejszych doświadczeń poniżenia i porażki.

Przeciążenie, niska odporność psychiczna i kryzys tożsamości

Znaczna część młodego pokolenia funkcjonuje w warunkach permanentnego stresu, presji oraz obniżonej odporności psychicznej. Niemal 2/3 osób w wieku 15–18 lat, które wzięły udział w badaniu przeprowadzonym na potrzeby raportu, zadeklarowało odczuwanie wypalenia lub depresji, z czego 36% w znacznym lub bardzo dużym stopniu. Podczas moderowanych dyskusji młodzi ludzie powtarzali: „jeszcze nie zaczęliśmy żyć, a już jesteśmy śmiertelnie zmęczeni”. Szkołę jako jedno z głównych źródeł codziennego stresu oraz przeciążenia psychicznego wskazuje 70% młodych¹⁶.

Niemal połowa nastolatków w wieku 10–19 lat ma niską samoocenę, a objawy depresyjne dotyczą ok. 40% uczniów szkół ponadpodstawowych¹⁷. Co czwarty uczeń doświadcza poczucia smutku i pustki¹⁸. Szczególnie alarmujący jest wzrost liczby prób samobójczych wśród młodzieży – w latach 2013–2024 ok. sześciokrotny. Zdecydowana większość pracowników instytucji pracujących z młodzieżą (87%) obserwuje narastanie problemów emocjonalnych i psychicznych wśród pokolenia Z. Stan chronicznego przeciążenia, obniżonej odporności psychicznej i kryzysu tożsamości

¹⁵ J. Kopycka, S. Wójcik, P. Raczyński, *Rówieśnicy. Raport o przemocy rówieśniczej 2026*, Warszawa 2026, s. 8–9.

¹⁶ Zob. szerzej: *Prawa dziecka w Polsce 2024. Wyniki badania porównawczego prezentującego perspektywę dzieci, rodziców i nauczycieli oraz rekomendacje koniecznych zmian*, UNICEF, <https://unicef.pl/prawa-dziecka/analizy-i-rzeczniactwo/analizy-i-rekomendacje/prawa-dziecka-w-polsce-2024>, s. 12 [dostęp: 24 VI 2026].

¹⁷ Zob. szerzej: J. Flis, M. Dębski, *Młode głowy. Otwarcie o zdrowiu psychicznym. Raport z badania dotyczącego zdrowia psychicznego, poczucia własnej wartości i sprawczości wśród młodych ludzi w Polsce*, Warszawa 2023.

¹⁸ Zob. M. Dębski, J. Pyżalski, J. Borchet, H. Witkowska, *Dobre i złe wiadomości...*

może zwiększać podatność młodych ludzi na narracje radykalne oferujące proste wyjaśnienia rzeczywistości, silną identyfikację grupową, poczucie sprawczości i emocjonalną kompensację, a tym samym sprzyjać otwartości na zachowania destabilizujące bezpieczeństwo społeczne i publiczne.

Oslabione relacje, samotność, alienacja, brak poczucia przynależności

Ostatni zidentyfikowany w raporcie czynnik zwiększający podatność młodzieży na zachowania radykalne i zagrażające bezpieczeństwu publicznemu to osłabienie relacji społecznych oraz narastające doświadczenie samotności i alienacji. Indywidualizacja życia społecznego, koncentracja na autonomii jednostki, selektywność relacji i malejąca rola instytucji wspólnotowych prowadzą do zawężania sieci wsparcia młodych ludzi. Relacje młodzieży i młodych dorosłych często obejmują najczęściej jedynie 2–3 osoby, ponad 80% młodzieży utrzymuje najważniejsze więzi w bardzo wąskiej grupie przyjaciół¹⁹. Oslabiły się również więzi międzypokoleniowe oraz relacje budowane wcześniej przez szkołę, organizacje społeczne, grupy zainteresowań czy środowiska lokalne.

Okolo 1/4 uczniów doświadcza wykluczenia ze środowiska rówieśniczego i samotności w szkole, a poczucie przynależności do wspólnoty szkolnej deklaruje w Polsce 64% uczniów przy średniej OECD wynoszącej 75%²⁰. Poczucie samotności deklaruje 38% nastolatków, a 16% doświadcza samotności o wysokim nasileniu. W grupie młodych dorosłych poczucie osamotnienia dotyczy już ponad 42% osób. Jednocześnie 44% młodych dorosłych nie jest w żadnym związku, nie ma bliskiej osoby²¹. Niemal 2/3 młodych dorosłych uważa, że trudno dziś znaleźć odpowiedniego partnera lub partnerkę, połowa deklaruje brak zaufania do innych osób²². Często łączą się z tym niski poziom zaufania społecznego oraz trudności w budowaniu trwałych relacji emocjonalnych. Wskazane czynniki sprzyjają poszukiwaniu grup lub osób o sprecyzowanej tożsamości, oferujących wsparcie i poczucie przynależności, w tym ze środowisk radykalnych, które proponują łatwe uznanie i odzyskanie poczucia sprawczości.

¹⁹ Zob. szerzej: *Diagnoza Młodzieży 2026...*, s. 63.

²⁰ Zob. szerzej: *PISA 2022 Results. Learning During – and From – Disruption*, t. 2, Paris 2023.

²¹ Zob. szerzej: *Młodzi Polacy o męskości, kobiecości i różnicach między płciami*, „Komunikat z badań CBOS”, 2025, nr 52, oprac. J. Scovil, Warszawa 2025.

²² Zob. K. Gagateg, U. Karaś, J. Kelsz, *Stan młodych 2025*, Warszawa 2025.

Środowisko informacyjno-cyfrowe jako „multiplikator ryzyk”

Środowisko informacyjno-cyfrowe stało się kluczowym „multiplikatorem ryzyk” (ang. *risk multiplier*), czyli czynnikiem wzmacniającym ryzyko podatności młodzieży na radykalizację i zachowania destabilizujące bezpieczeństwo społeczne. Szczególnie niepokojąca jest specyfika życia młodych ludzi, kształtowanego przez algorytmy rekomendacyjne platform społecznościowych, serwisów streamingowych, gier online i komunikatorów. Cechą współczesnego środowiska cyfrowego jest asymetria pomiędzy tempem rozwoju platform internetowych a zdolnością instytucji publicznych do ich regulowania i nadzorowania. W efekcie młodzi użytkownicy pozostają narażeni na oddziaływanie algorytmicznych mechanizmów selekcji treści, które mogą wzmacniać polaryzację poznawczą, tworzyć zamknięte bańki informacyjne oraz zwiększać ekspozycję na narracje ekstremistyczne i antysystemowe.

Z dostępnych badań dotyczących tego obszaru można wyciągnąć kilka wniosków. Po pierwsze, zdecydowana większość młodych ludzi użytkujących platformy społecznościowe styka się w tym środowisku z różnego rodzaju teoriami konspiracyjnymi. Im więcej czasu tam spędzają, tym bardziej stają się podatni na ich działanie. Najmniej odporne na wpływ teorii spiskowych są osoby w wieku 14–16 lat, a wśród dorosłych – do 35. roku życia²³.

Po drugie, algorytmy rekomendacyjne umożliwiają łatwy dostęp do brutalnych treści – premiują treści radykalne, wyraziste, zamykające młodych ludzi w bańkach informacyjnych. Widoczny jest też wyraźny trend ekspozycji chłopców na przekazy mizoginistyczne, propagujące nienawiść wobec dziewcząt i kobiet, sprowadzające je do podrzędnej roli wobec mężczyzn. Tworzona – przez algorytmiczną radykalizację – tzw. manosfera jest konglomeratem treści ekstremistycznych²⁴.

Po trzecie, mamy do czynienia z ogromnym wzrostem liczby materiałów o charakterze seksualnym, w tym pornograficznych (ich dystrybutorami są głównie platformy społecznościowe), oraz treści prezentujące seksualne wykorzystanie dzieci, tzw. CSAM (ang. *child sexual abuse materials*).

²³ A. Byrne, D. Martin, C. Jones, N. Galbraith, T. Mercer, *Conspiracy theory beliefs in the adolescent population: A systematic review*, „Journal of Adolescence” 2024, t. 96, nr 5, s. 925–939. <https://doi.org/10.1002/jad.12316>.

²⁴ K. Regehr, C. Shaughnessy, M. Zhao, N. Shaughnessy, *Safer scrolling. How algorithms popularise and gamify online hate and misogyny for young people*, Canterbury 2024.

Analizy dotyczące działań grupy 764²⁵, uznanej przez niektóre kraje za terrorystyczną, wskazują, że tego rodzaju aktywności nie są związane wyłącznie z motywacjami seksualnymi, ale wykorzystują naturalną ciekawość i zagubienie młodych ludzi do tworzenia materiałów służących manipulacji, zastraszaniu, wymuszaniu działań przestępczych²⁶.

Jednocześnie widoczny jest wzrost użytkowania szyfrowanych komunikatorów, które poza tym, że dały poczucie prywatności, to stały się narzędziami działań przestępczych. Z licznych analiz instytucji odpowiedzialnych za bezpieczeństwo wynika, że jest to nowa dynamika rozwoju zjawisk zagrażających bezpieczeństwu publicznemu, które są związane z wykorzystywaniem popularnych aplikacji w celu weaponizacji (ang. *weaponization*) małoletnich, czyli wykorzystywania dzieci i młodzieży jako swojej broni, narzędzie wywierania wpływu, destabilizacji lub wyrządzania szkody. Szczególną uwagę należy zwrócić na dwa zjawiska: nihilistyczny ekstremizm²⁷ oraz zlecanie zadań osobom małoletnim za pośrednictwem popularnych komunikatorów. Pierwsze z nich jest związane z działaniem rozproszonych sieci nazywanych Com (od ang. *communities* – wspólnoty). Są to nieformalne grupy, ruchy i pojedyncze osoby komunikujące się ze sobą w cyberprzestrzeni, które mają własny system budowania statusu w grupie przez podejmowanie działań przestępczych²⁸. Opisana wcześniej grupa 764 jest kwintesencją tego typu nihilistycznej formy radykalizacji.

Na rosnącą skalę wykorzystywania komunikatorów do zlecania działań przestępczych wskazuje Europol. Określa je akronimem VaaS

²⁵ Grupa 764 (ang. 764 Network) to luźna, międzynarodowa sieć internetowa skupiająca głównie bardzo młode osoby, która jest kojarzona z ekstremalnymi formami przemocy psychicznej online, szantażu, samookaleczeń, wymuszeń seksualnych i radykalizacji nieletnich. Nazwa pochodzi od numeru używanego przez jednego z pierwszych administratorów tej społeczności. Zob. szerzej: K. Ciesiołkiewicz, *Weaponizacja osób małoletnich i młodych dorosłych. Nowe zagrożenia dla bezpieczeństwa wewnętrznego*, https://uczelniakorczaka.pl/wp-content/uploads/2026/06/WEAPONIZACJA_MATERIAL.pdf, s. 17 [dostęp: 24 VI 2026].

²⁶ *OSINT Report 764*, 12 September 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Public%20Version%20of%2020240910_nr02_OSINT_Report_764%20.pdf [dostęp: 12 V 2026].

²⁷ *Terror without ideology? The rise of nihilistic violence*, Institute for Strategic Dialogue, 8 V 2025 r., <https://www.isdglobal.org/digital-dispatch/terror-without-ideology-the-rise-of-nihilistic-violence-an-isd-investigation/> [dostęp: 12 V 2026].

²⁸ K. Ciesiołkiewicz, *Nowe zagrożenia. Nihilistycznie zorientowana przemoc małoletnich oraz „przemoc jako usługa” – wyzwania dla bezpieczeństwa wewnętrznego i społecznego*, https://uczelniakorczaka.pl/wp-content/uploads/2026/02/NOWE-ZAGROZENIA_Konrad-Ciesiolkiewicz_Uczelnia-Korczaka.pdf, s. 6 [dostęp: 12 V 2026].

(ang. *violence-as-a-service*)²⁹. Dane pokazują, że środowisko cyfrowe nie tylko zwiększa ekspozycję na skrajne treści, lecz także osłabia zdolność krytycznej oceny informacji i wzmacnia polaryzację społeczną. Dane wskazują na niski poziom kompetencji związanych z oceną wiarygodności treści cyfrowych. Ponad 40% młodych ludzi uważa, że w internecie trudno odróżnić informacje prawdziwe od fałszywych, a mniej niż połowa deklaruje zainteresowanie wiarygodnością obserwowanych profili i źródeł informacji³⁰. Z badań prowadzonych przez Centrum Analiz Społeczeństwa Informacyjnego Uczelni Korczaka wynika, że wśród nastolatków jest wyraźna silna relatywizacja prawdy i kierowanie się społecznym dowodem słuszności – im więcej komentarzy znajduje się pod danym postem i jest on popularniejszy, tym bardziej wiarygodny się staje. Wydaje się też, że przebadzcowanie informacyjne powoduje coraz większą bierność poznawczą³¹.

Rekomendacje

Diagnoza Młodzieży 2026 wskazuje, że ograniczanie podatności młodego pokolenia na radykalizację wymaga podejścia systemowego, wykraczającego poza działania instytucji bezpieczeństwa, i reagowania na pojedyncze incydenty. Wnioski zawarte w omawianym raporcie pozwalają sformułować najważniejsze kierunki przyszłych działań.

Należy stworzyć spójną strategię państwa na rzecz młodzieży, opartą na analizie trajektorii życia, łączącą działania edukacyjne, społeczne, zdrowotne i cyfrowe oraz wzmacniającą odporność psychospołeczną młodych ludzi. Jednym z elementów krajowej strategii na rzecz młodzieży powinny być instrumenty polityki publicznej związane z przeciwdziałaniem radykalizacji prowadzącej do przemocy.

Niezbędne są również międzysektorowe przedsięwzięcia podejmowane w celu przeciwdziałania radykalizacji młodzieży, w tym zaangażowanie

²⁹ *Operational Taskforce GRIMM*, Europol, 1 IV 2025 r., <https://www.europol.europa.eu/how-we-work/operations/operational-taskforce-grimm> [dostęp: 12 V 2026].

³⁰ R. Lange, A. Wrońska, A. Ładna, K. Kamiński, M. Błazej, A. Jankiewicz, K. Rosłaniec, *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*, R. Lange (red.), Warszawa 2023, s. 7.

³¹ K. Ciesiołkiewicz, A. Buchner, K. Fereniec-Błońska, M. Wierzbicka-Tarkowska, *Między faktem a feedem. Podatność młodzieży na dezinformację i teorie spiskowe w środowisku mediów cyfrowych*, Rzeszów 2025, s. 55–61.

sektora pomocy społecznej. W państwach europejskich rośnie znaczenie modelu prewencji społecznej (ang. *preventive social approach*) opartego na założeniu, że radykalizacja młodych ludzi jest często efektem kumulacji problemów relacyjnych, psychicznych, edukacyjnych i społecznych. W tym podejściu kluczową rolę odgrywają szkoły, służby społeczne, praca z rodziną, organizacje lokalne oraz instytucje zdrowia psychicznego. Szczególne znaczenie przypisuje się szkołom jako instytucjom wczesnego wykrywania kryzysów oraz budowania odporności psychospołecznej, kompetencji emocjonalnych i poczucia przynależności. W wielu krajach UE nauczyciele, pedagodzy i psychologowie są szkoleni w zakresie rozpoznawania sygnałów izolacji społecznej, gwałtownych zmian zachowania, fascynacji przemocą, radykalnych narracji czy kryzysów psychicznych. Istotne jest również przeciwdziałanie przemocy rówieśniczej, w tym bullyingowi, a także wzmacnianie relacji i integracji grupowej.

Coraz większe znaczenie przypisuje się środowiskowej pracy z młodzieżą (ang. *youth work*). Idea ta opiera się na tworzeniu bezpiecznych i łatwo dostępnych miejsc spotkań, aktywności i budowania relacji, z których młodzi ludzie mogą korzystać dobrowolnie, bez formalnych wymogów uczestnictwa czy instytucjonalnych barier. Takie „niskoprogowe przestrzenie relacyjne” funkcjonują poza szkołą i rodziną, umożliwiają młodzieży nawiązywanie kontaktów z rówieśnikami oraz zaufanymi dorosłymi. Kluby młodzieżowe, mentoring, streetworking czy działania sportowo-kulturalne wzmacniają więzi społeczne, sprawczość i integrację lokalną oraz umożliwiają wczesne rozpoznawanie marginalizacji, kryzysów psychicznych i procesów radykalizacji. Uzupełnieniem tych działań staje się edukacja obywatelska, medialna i cyfrowa rozwijająca odporność na dezinformację, manipulację i narracje ekstremistyczne. Prewencja w zakresie radykalizacji w coraz większym stopniu opiera się na rozwijaniu kompetencji społeczno-emocjonalnych i wzmacnianiu tzw. odporności wspólnotowej (ang. *community resilience*), ponieważ kluczową ochronę przed ekstremizmem stanowią silne relacje społeczne, poczucie przynależności, sprawczości oraz obecność dostępnych i wspierających instytucji.

Autorzy *Diagnozy Młodzieży 2026* proponują, by wysiłki sektora publicznego skupić na osłabianiu czynników społecznych sprzyjających radykalizacji i niebezpiecznym zachowaniom, profilaktyce oraz budowaniu odporności. Na podstawie wniosków z badań wskazują też dwa wektory działania: pierwszy skoncentrowany w większym stopniu na młodzieży, drugi – na młodych dorosłych. Zgodnie z triadą odporności postuluje się

wzmacnianie kompetencji i zasobów chroniących młodych ludzi przed wpływem dezinformacji, przemocy, manipulacji oraz środowisk radykalnych. Podstawą jest wzmacnianie odporności psychicznej i emocjonalnej młodzieży, co obejmuje rozwój kompetencji społeczno-emocjonalnych, zdolności radzenia sobie ze stresem, budowania relacji oraz regulacji emocji. Drugim filarem tego podejścia jest wzmacnianie odporności relacyjnej i wspólnotowej, odbudowa więzi społecznych, wzmacnianie poczucia przynależności, wspieranie relacji rówieśniczych, rodzinnych i lokalnych wspólnot. Trzeci element stanowi odporność informacyjna i cyfrowa – rozwój kompetencji medialnych, krytycznego myślenia, umiejętności rozpoznawania manipulacji, dezinformacji i treści ekstremistycznych w środowisku cyfrowym. Pilnie potrzebne są również regulacje środowiska cyfrowego, m.in. skuteczne regulacje platform cyfrowych, ograniczanie ekspozycji na przemoc, pornografię, patotreści i treści ekstremistyczne, większa odpowiedzialność platform za algorytmy rekomendacyjne oraz rozwój szybkich systemów reagowania i pomocy.

Drugi kierunek działań dotyczy młodych dorosłych, a celem jest w tym przypadku wzmacnianie stabilności życiowej jako elementu prewencji radykalizacji. Autorzy raportu wskazują, że niestabilność zatrudnienia, prekaryzacja pracy oraz bariery mieszkaniowe zwiększają frustrację i poczucie braku perspektyw. Dlatego kluczowe znaczenie ma wdrażanie polityk publicznych opisanych jako triada odporności. Obejmuje ona zwiększanie bezpieczeństwa zatrudnienia, dostępności mieszkań i wsparcia usamodzielniania oraz wzmacnianie mobilności społecznej przez ograniczanie wykluczenia transportowego.

W raporcie *Diagnoza Młodzieży 2026* przedstawiono jeden z najbardziej kompleksowych obrazów obecnej sytuacji młodego pokolenia w Polsce. Pokazano, że radykalizacja młodzieży nie jest wyłącznie problemem bezpieczeństwa czy wpływu ideologii, lecz zjawiskiem głęboko zakorzenionym w procesach społecznych. Autorzy opracowania wskazali, że skuteczna prewencja musi opierać się przede wszystkim na politykach wzmacniających społeczne funkcjonowanie młodego pokolenia – rozwijaniu odporności psychicznej, relacyjnej i informacyjnej oraz zapewnianiu młodym stabilnego wejścia w dorosłość przez bezpieczeństwo zatrudnienia, dostęp do mieszkań i zwiększanie mobilności społecznej. Ograniczanie radykalizacji wymaga więc działań u źródeł – odbudowy więzi społecznych, poczucia sprawczości i bezpieczeństwa życiowego młodych ludzi. W dłuższej perspektywie może to stać się jednym z kluczowych warunków wzmacniania odporności społecznej i bezpieczeństwa państwa.

Paweł Rabiej

Koordynator prac nad raportem *Diagnoza Młodzieży 2026*.

Kontakt: p.rabiej@uczelniakorczaka.pl

Dr Konrad Ciesiołkiewicz

Kierownik Centrum Analiz Społeczeństwa Informacyjnego Uczelni
Korczaka, współautor raportu *Diagnoza Młodzieży 2026*.

Kontakt: konrad.ciesiolkiewicz@gmail.com

Sprawozdanie z konferencji „Nowe uwarunkowania procesu radykalizacji młodych ludzi z perspektywy bezpieczeństwa państwa”

Warszawa, 23 kwietnia 2026 r.

Aleksandra Komar

Autorka niezależna

 <https://orcid.org/0000-0002-9717-5258>

Konferencja „Nowe uwarunkowania procesu radykalizacji młodych ludzi z perspektywy bezpieczeństwa państwa” poświęcona problemowi radykalizacji nieletnich odbyła się 23 kwietnia 2026 r. w siedzibie Agencji Bezpieczeństwa Wewnętrznego w Warszawie. Wzięli w niej udział przedstawiciele środowisk akademickich, eksperci ds. bezpieczeństwa oraz praktycy z Centralnego Biura Zwalczania Cyberprzestępczości, Państwowej Komisji ds. przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, Instytutu Bezpieczeństwa Społecznego, Uczelni Korczaka, Uniwersytetu Civitas, NASK-u, Wojskowej Akademii Technicznej oraz ABW. Przyjęta formuła organizacyjna pozwoliła połączyć różne perspektywy, co przełożyło się na główną oś problemową konferencji: napięcie między rozwojem technologicznym a bezpieczeństwem psychospołecznym młodych ludzi, ze szczególnym uwzględnieniem mechanizmów radykalizacji, mogącej prowadzić do działań terrorystycznych.

Problem radykalizacji młodzieży i młodych dorosłych to zjawisko wielowymiarowe, które rezonuje niemal w każdej sferze życia publicznego. Można je uznać za jedno z najważniejszych współczesnych zagrożeń bezpieczeństwa, które ma wpływ na: bezpieczeństwo wewnętrzne państwa, pracę służb specjalnych i policji, stabilność międzynarodową, cyberbezpieczeństwo i politykę społeczną.

Jak celnie zauważył dr Konrad Ciesiołkiewicz, wiceprzewodniczący Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15: (...) *wiek osób ulegających radykalizacji obecnie mocno się obniżył. Kryteria radykalizacji spełniają 10-, 11-letnie osoby. Powinniśmy więc potraktować je jako grupę krytycznie ważną, jako miękkie podbrzusze systemu bezpieczeństwa społecznego.*

Konferencja stanowiła odpowiedź na dynamicznie rozwijającą się radykalizację, która wymyka się istniejącym schematom analitycznym. W zakresie skali oddziaływania zjawiska należy wskazać kilka kluczowych obszarów i wymiarów. Warto podkreślić aspekty społeczny i naukowy – radykalizacja podważa dotychczasowe paradygmaty socjologiczne i pedagogiczne, wymaga interdyscyplinarnego podejścia badawczego. Wpływa na kondycję i rozwój społeczeństwa przez bezpośrednie uderzanie w jego struktury, co osłabia więzi międzyludzkie i hamuje potencjał rozwojowy młodego pokolenia. Warto zaznaczyć, że radykalne postawy młodzieży to fundament przyszłej polaryzacji politycznej, która może destabilizować struktury demokratyczne i instytucje publiczne. W skrajnej formie to zjawisko staje się realnym zagrożeniem dla porządku publicznego, co generuje potrzebę wzmożonej czujności ze strony systemów bezpieczeństwa. Uczestnicy konferencji omówili takie zagadnienia, jak: przyczyny, mechanizmy, skutki radykalizacji młodzieży i metody prewencji.

Przyczyny radykalizacji młodzieży

Paweł Rabiej, ekspert Polskiego Towarzystwa Polityki Społecznej (PTPS), przedstawił podatność młodych osób na radykalizację w świetle badań własnych, analiz danych zastanych oraz ustaleń raportu *Diagnoza Młodzieży 2026*¹.

¹ Pierwszy na tak dużą skalę holistyczny raport naukowy opisujący kondycję i potrzeby młodych Polaków (pokolenie Z) opracowany przez ekspertów PTPS na zlecenie Ministerstwa Edukacji Narodowej. Stanowi fundament dla nowej Krajowej Strategii Młodzieżowej.

Prelegent omówił tło radykalizacji młodzieży i podał jej przyczyny. Wskazał sześć kluczowych mechanizmów radykalizacji:

- 1) subiektywne poczucie niesprawiedliwości i krzywdy,
- 2) kryzysy i napięcia tworzące środowisko presji,
- 3) nierówności, wykluczenie społeczne, przemoc, negatywne trajektorie,
- 4) kryzys tożsamości i potrzeba poczucia przynależności,
- 5) deprywacja polityczna – poczucie braku wpływu i sprawczości,
- 6) środowisko cyfrowe i informacyjne – wzmacniacz procesu radykalizacji.

Z zaprezentowanych przez niego badań wynika, że aż 60% osób w wieku 15–18 lat funkcjonuje w stanie permanentnego napięcia, skarży się na silny stres, chroniczne zmęczenie i dotkliwy brak energii do życia. Cierpienie młodych ludzi dotyczy wielu sfer ich życia – odczuwają stres domowy (dom i rodzina nie są bezpieczną przystanią) oraz stres szkolny (szkoła jawi się jako system nastawiony na wynik, a nie na człowieka). Prelegent wskazał na dramatyczną skalę przemocy w świecie wirtualnym. Dla wielu młodych ludzi internet jest przestrzenią traumy, doświadczania przemocy, a nie rozwoju. Z przedstawionych badań wynika, że aż co czwarty nastolatek padł ofiarą cyberstalkingu i uporczywego nękania. Jeszcze bardziej alarmujący jest fakt, że 20% badanych doświadczyło molestowania seksualnego online. Wniosek płynący z tych danych brzmiał: doświadczenie przemocy i molestowania w sieci stanowi źródło radykalizacji. Ofiara mająca poczucie opuszczenia przez instytucje i dorosłych staje się podatna na narracje grup oferujących „siłę”, „odwet” lub radykalną zmianę systemu, który ich nie ochronił.

Uzupełniając powyższe ustalenia, jako istotne czynniki socjalizacji pierwotnej i wtórnej należy wskazać kryzys funkcji wychowawczej rodziny oraz osłabienie autorytetu szkoły i instytucji edukacyjnych. Deficyty w zakresie wsparcia emocjonalnego, stabilności relacji oraz przekazu norm i wartości mogą sprzyjać poszukiwaniu alternatywnych, często radykalnych wzorców identyfikacyjnych.

Istotną rolę odgrywają także czynniki polityczne i geopolityczne, w tym globalne kryzysy, konflikty zbrojne czy napięcia międzynarodowe,

Zob. szerzej: P. Rabiej, K. Ciesiołkiewicz, *Młodzież a bezpieczeństwo państwa. Społeczne uwarunkowania podatności na radykalizację w świetle raportu „Diagnoza Młodzieży 2026”*, „Terroryzm – studia, analizy, prewencja” 2026, nr 9, s. 175–189. <https://doi.org/10.4467/27204383TER.26.007.23790> (przyj. red.).

które – przez środowisko informacyjne – oddziałują na percepcję rzeczywistości przez młodych ludzi i mogą wzmacniać narracje radykalne oraz poczucie zagrożenia i polaryzacji. Nie bez znaczenia pozostają również czynniki psychologiczne i indywidualne, np. zaburzenia neurorozwojowe (m.in. zaburzenia ze spektrum autyzmu), trudności adaptacyjne, zaburzenia emocjonalne oraz deficyty kompetencji społecznych. Czynniki te mogą zwiększać podatność na wpływ uproszczonych, binarnych narracji, a także na oddziaływanie grup oferujących silną tożsamość, poczucie przynależności i jasno zdefiniowany system wartości.

Mechanizmy radykalizacji młodzieży

W trakcie konferencji wielokrotnie zwracano uwagę na fakt, że współczesny terroryzm coraz częściej wykorzystuje zdecentralizowane kanały komunikacji, co znacznie utrudnia jego kontrolę. Doktor Paulina Piasecka z Uniwersytetu Civitas wskazała, że radykalizacja to nie tylko zbiór pojedynczych stron czy postów, lecz także samonapędzająca się struktura kształtująca postawy młodzieży. Na podstawie aktualnych diagnoz i analiz bezpieczeństwa można ją opisać jako zamknięty obieg informacji, w którym technologia spotyka się z psychologią. Autorka trafnie zidentyfikowała cztery filary współczesnej rekrutacji cyfrowej:

- 1) targetowanie algorytmiczne (szybkie rozprzestrzenianie się informacji – wymuszane przez mechanizmy platform społecznościowych – wywołujące silne emocje),
- 2) inżynieria nostalgii (budowanie „wspólnot wyobrażonych” przez wykorzystywanie sentymentu np. do ery socjalizmu),
- 3) rekrutacja cyfrowa (wykorzystanie dla operacji wpływu m.in. Tik-Toka i Telegrama jako niskokosztowych kanałów),
- 4) nowe granice (wykorzystanie sztucznej inteligencji i technologii deepfake jako zaawansowanych narzędzi manipulacji).

Istotne są również środowiska powiązane z grami komputerowymi. Platformy komunikacyjne wykorzystywane przez graczy, takie jak Discord, a także fora i społeczności skupione wokół gier online mogą stanowić przestrzeń społeczną podatną na oddziaływanie treści radykalnych. Ze względu na wysoki poziom anonimowości, łatwość budowania zamkniętych grup oraz intensywność interakcji społecznych takie środowiska sprzyjają stopniowej socjalizacji użytkowników z określonymi narracjami

ideologicznymi. W praktyce mogą być wykorzystywane do rekrutacji, testowania lojalności uczestników oraz dystrybucji treści o charakterze ekstremistycznym, szczególnie wśród młodszych użytkowników.

Prelegenci zwracali uwagę, że współczesne mechanizmy radykalizacji obejmują również aktywną instrumentalizację dzieci i młodzieży przez organizacje ekstremistyczne, które stopniowo wciągają nieletnich w swoją działalność. Zlecają im do wykonania pozornie proste zadania operacyjne, np. rozpowszechnianie treści dezinformacyjnych, udział w zamkniętych grupach, realizację działań o charakterze propagandowym. Ten proces ma charakter etapowy i prowadzi do stopniowej internalizacji radykalnych narracji oraz budowania lojalności wobec grupy. Prelegenci wskazywali również, że czas, w jakim dochodzi do radykalizacji za pośrednictwem mediów społecznościowych, znacznie się skrócił. W sprzyjających warunkach może przebiegać bardzo dynamicznie i trwać nawet poniżej miesiąca. To zjawisko jest wzmacniane przez mechanizmy algorytmiczne oraz zamknięte środowiska komunikacyjne, które przyspieszają proces identyfikacji z narracją ekstremistyczną i ograniczają ekspozycję na alternatywne punkty widzenia.

W analizie społeczno-psychologicznych fundamentów podatności na radykalizację Paulina Piasecka trafnie zidentyfikowała jej kluczowe katalizatory, do których zaliczyła resentyment lokalny, czyli radykalizację zakorzenioną w poczuciu niesprawiedliwości, nierównościach ekonomicznych i marginalizacji społecznej. Regiony przygraniczne charakteryzują się większą podatnością na inicjowanie konfliktów przez aktorów zewnętrznych oraz silną potrzebą uznania i przynależności, co skutecznie przyciąga nieletnich do agresywnych narracji radykalnych. Te regiony mogą również stanowić przestrzeń oddziaływania różnych ideologii ekstremistycznych, w tym nurtów związanych z radykalnym islamizmem, wykorzystujących mechanizmy marginalizacji, poczucia niesprawiedliwości oraz deficytu tożsamości do rekrutacji i wzmacniania skrajnych postaw wśród podatnych grup młodzieży.

Według Konrada Ciesiołkiewicza cyfrowy ekosystem stał się głównym środowiskiem radykalizacji dzieci i młodzieży, która przyjmuje dziś formę sfragmentaryzowanych, trudnych do wykrycia sieci nazywanych Com (od ang. *communities* – wspólnoty). Klasyczna radykalizacja młodego pokolenia łączy się w tej przestrzeni z cyberzagrożeniami – od cyberprzemocy po zorganizowaną cyberprzestępczość – i buduje własne, autonomiczne struktury statusu. W tym kontekście należy również zwrócić uwagę na zjawisko „przemocy jako usługi”, związane z działalnością wyspecjalizowanych,

zdecentralizowanych grup przestępczych (np. grupa 764). Wykorzystują one nieletnich jako podatne cele oddziaływania, stosując mechanizmy presji psychologicznej, manipulacji i szantażu cyfrowego. Proces ten często rozpoczyna się od ekspozycji na treści o charakterze przemocowym lub szokowym, która prowadzi do stopniowego uzależnienia informacyjnego i obniżenia progu reakcji emocjonalnej. Następnie siła oddziaływania wzrasta i obejmuje wymuszanie określonych zachowań lub aktywności w środowisku cyfrowym, w tym działań wspierających rozwój struktur przestępczych lub ekstremistycznych. To zjawisko wpisuje się w szerszy trend instrumentalizacji dzieci i młodzieży w ramach operacji przestępczych i destabilizacyjnych. Stanowi to istotne wyzwanie dla systemów bezpieczeństwa państwa oraz mechanizmów ochrony nieletnich.

Powyższy temat ściśle wiąże się z zagadnieniem nihilistycznego podłoża agresji wśród najmłodszych oraz komercjalizacją agresji w formie „przemocy jako usługi” w kontekście bezpieczeństwa państwa. Prelegent zaznaczył, że skoncentrowanie się na czynnikach środowiskowych dowodzi niewydolności obecnych rozwiązań instytucjonalnych, które nie zapewniają optymalnej ochrony młodzieży przed zagrożeniami informacyjnymi. Naprawa tego stanu wymaga, jego zdaniem, holistycznego podejścia z zakresu ekologii mediów, oceniającego cały ekosystem cyfrowy. Przywołując tezę Neila Postmana, że nowa technologia wszystko zmienia, wskazał, że sfery cyfrowej nie można postrzegać jedynie instrumentalnie, ponieważ stała się ona nowym środowiskiem życia i sferą publiczną.

Należy również zwrócić uwagę na rosnące ryzyko instrumentalizacji dzieci i młodzieży przez podmioty zewnętrzne, w tym potencjalne działania obcych służb wywiadowczych oraz aktorów prowadzących operacje wpływu. Środowisko cyfrowe, charakteryzujące się wysokim poziomem anonimowości oraz ograniczoną kontrolą instytucjonalną, może sprzyjać wykorzystywaniu nieletnich jako narzędzi do prowadzenia działań destabilizacyjnych, w tym do rozpowszechniania treści propagandowych, wzmacniania narracji polaryzujących czy uczestnictwa w operacjach dezinformacyjnych. To zjawisko wpisuje się w szerszy kontekst zagrożeń hybrydowych, w których podatność młodego pokolenia na manipulację informacyjną stanowi istotny wektor oddziaływania na stabilność państwa i jego systemów bezpieczeństwa.

Skutki radykalizacji młodzieży

Skutki radykalizacji młodzieży mają charakter kaskadowy – zaczynają się od jednostki, a w skrajnych przypadkach mogą prowadzić do destabilizacji struktur państwowych. Należy podkreślić, że nie każde zachowanie ma podłoże ideologiczne. Część aktów przemocy może mieć charakter autoteliczny – stanowić przemoc dla samej przemocy. Na podstawie prelekcji i dyskusji uczestników wykazano cztery zasadnicze obszary skutków:

- 1) dla jednostki (destrukcja osobista),
- 2) dla społeczeństwa (głęboka polaryzacja, normalizacja przemocy, erozja zaufania publicznego),
- 3) dla państwa (destabilizacja systemowa),
- 4) cyfrowe (dominacja narracji nienawiści, rozwój technologii manipulacji).

Najpoważniejszym z nich jest utrata potencjału rozwojowego państwa. Młode pokolenie – zamiast budować przyszłość – angażuje energię w procesy destrukcyjne i konfrontacyjne.

Paulina Piasecka podkreśliła znaczenie mechanizmów tożsamościowych (skutki o charakterze systemowym i społecznym). Wskazała zjawiska będące przejawem polaryzacji afektywnej polegającej na wzmacnianiu dychotomii my – oni, co prowadzi do głębokich podziałów społecznych. Nasyćanie fałszywych narracji silnymi emocjami w celu manipulacji opinią publiczną służy pogłębianiu nieufności obywateli wobec służb państwowych i późniejszemu celowemu wykorzystywaniu takich postaw.

W debatach mocno wybrzmiewał temat tego, jak w dłuższej perspektywie radykalizacja może uderzyć w stabilność państwa i ładu międzynarodowego. Prelegenci podkreślali, że może ona osłabiać stabilność państwa, zwiększać wydatki na bezpieczeństwo, ograniczać wolności obywatelskie, pogarszać relacje międzynarodowe oraz wzmacniać konflikty ideologiczne. Z perspektywy zagrożeń wewnętrznych wskazywano, że radykalizacja może prowadzić do aktów terrorystycznych, przemocy politycznej, zamieszek i destabilizacji społecznej, ataków na instytucje państwowe oraz wzrostu przestępczości motywowanej ideologicznie. Może również osłabiać zaufanie obywateli do państwa, nasilać konflikty społeczne, utrudniać dialog polityczny oraz sprzyjać dezinformacji i rozpowszechnianiu teorii spiskowych. Ostatecznie może prowadzić do kryzysów politycznych czy osłabienia demokracji.

W analizach prelegentów kluczowe miejsce zajęły tematy związane z zagrożeniami w cyberprzestrzeni, na których w szczególności skupiła się

dr Katarzyna Maniszewska z Uniwersytetu Civitas oraz Uniwersytetu w Białymstoku. Omówiła wybrane zagrożenia spowodowane rozwojem sztucznej inteligencji, wskazując, że AI jest obecnie jednym z głównych narzędzi wykorzystywanych do prowadzenia operacji informacyjnych. Zautomatyzowane generowanie i miksowanie danych ułatwia wrogim podmiotom manipulację na niespotykaną dotąd skalę, począwszy od propagandy, a skończywszy na cyberatakach i weryfikacji luk w systemach bezpieczeństwa.

W trakcie konferencji podkreślano, że grupy radykalne coraz częściej działają online – rekrutują członków przez media społecznościowe, prowadzą propagandę, organizują cyberataki, rozpowszechniają materiały ekstremistyczne. Radykalizacja w internecie, zwłaszcza młodzieży, może prowadzić do wielu negatywnych skutków, takich jak: wzrost cyberprzestępczości, udział w atakach hakerskich, szerzenie propagandy czy stosowanie mowy nienawiści. Młodzi ludzie stają się coraz bardziej podatni na manipulację, dezinformację i wpływ grup ekstremistycznych.

Metody prewencji

Metody przeciwdziałania radykalizacji były nie tylko przedmiotem analizy teoretycznej, lecz także ożywionych dyskusji podczas paneli dyskusyjnych. W trakcie konferencji wybrzmiało, że metody przeciwdziałania radykalizacji dzielą się na trzy poziomy: od profilaktyki ogólnej, przez działania skierowane do grup ryzyka, aż po interwencje wobec osób już zradykalizowanych. Do kluczowych strategii opartych na współczesnych standardach bezpieczeństwa i edukacji zaliczono: budowanie odporności (poziom profilaktyczny), działania systemowe i instytucjonalne oraz interwencję i deradykalizację (poziom specjalistyczny).

Do najskuteczniejszych narzędzi zalicza się przedstawioną przez Pawła Rabieję triadę odporności (odporność i rozwój kapitału psychologicznego, rozwój umiejętności relacyjnych i społecznych oraz cyfrowa tarcza – bezpieczne środowisko dorastania), a także triadę samodzielności (zwiększenie stabilności i elastyczności zatrudnienia, wsparcie w zakresie samodzielności mieszkaniowej oraz zmniejszenie lokalnych barier transportowych). Prelegent wskazał również na istotę działań międzyresortowych we wdrożeniu zmian w celu zmniejszania zdiagnozowanych w raporcie problemów nastolatków. Synergia międzyinstytucjonalna powinna być oparta na: wspieraniu potencjału młodzieży na obszarach wiejskich, zdrowiu

i dobrostanie reprodukcyjnym młodzieży, propagowaniu zdrowych nawyków (odżywianie i aktywność fizyczna), równości szans i bezpieczeństwu rozwoju młodych kobiet, relacji i odporności młodych mężczyzn, łatwiejszym dostępie do kultury, sportu i czasu wolnego, przedsiębiorczości i potencjale innowacji osób młodych, trosce o klimat, środowisko oraz zrównoważony rozwój.

W trakcie debaty prelegenci zaznaczyli szczególną rolę służb prowadzących działania wywiadowcze i kontrwywiadowcze w sieci, monitorujących zagrożenia cyfrowe oraz współpracujących z platformami internetowymi w zakresie usuwania niebezpiecznych treści. Zaakcentowano znaczenie rozwoju mediów społecznościowych, które stworzyły nowe możliwości dla organizacji ekstremistycznych. Platformy internetowe umożliwiają szybkie rozpowszechnianie propagandy, tworzenie zamkniętych grup ideologicznych oraz anonimowy kontakt z potencjalnymi rekrutami. Z perspektywy służb specjalnych cyberprzestrzeń stała się jednym z kluczowych obszarów operacyjnych. Podkreślono, że współcześnie radykalizacja młodzieży może być wykorzystywana jako element wojny hybrydowej. Państwa wrogie lub organizacje ekstremistyczne mogą celowo pogłębiać podziały społeczne, wspierać skrajne ruchy polityczne oraz destabilizować sytuację wewnętrzną innych państw. Zgodnie stwierdzono, że jest to zjawisko zmuszające do modernizacji systemów bezpieczeństwa i rozwoju koordynacji operacyjnej na szczeblu krajowym oraz w ramach struktur transgranicznych. W szczególności istotna jest współpraca w ramach NATO, Unii Europejskiej czy Organizacji Narodów Zjednoczonych, która obejmuje wymianę informacji wywiadowczych, wspólne operacje antyterrorystyczne, sankcje wobec organizacji ekstremistycznych, a także programy przeciwdziałania radykalizacji.

Podsumowanie

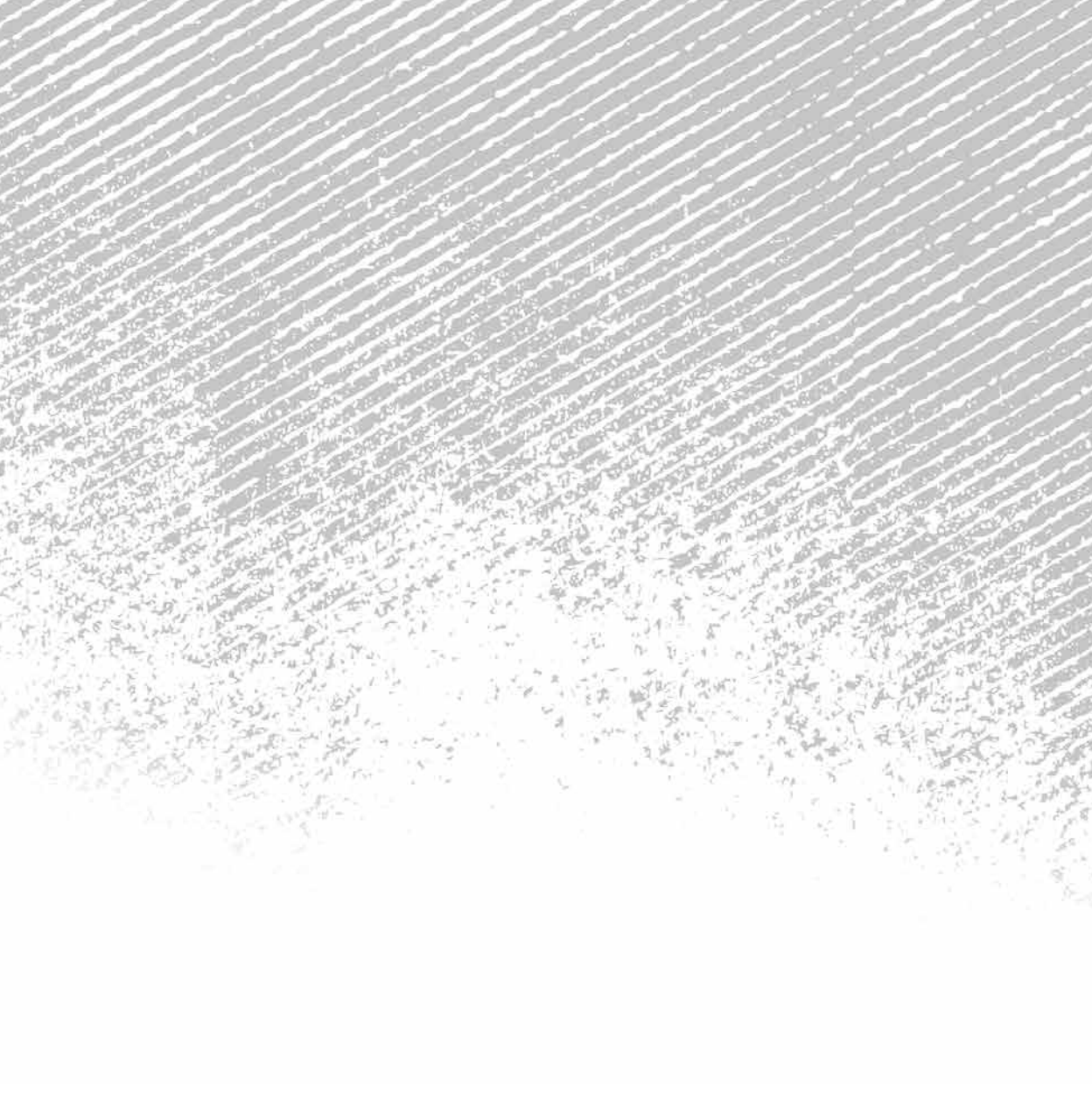
Konferencja „Nowe uwarunkowania procesu radykalizacji młodych ludzi z perspektywy bezpieczeństwa państwa” stanowiła wartościowe forum wymiany poglądów. Uwidoczniono złożoność problemu radykalizacji nieletnich. Radykalne postawy młodzieży to fundament przyszłej polaryzacji politycznej, która może destabilizować struktury demokratyczne i instytucje publiczne. Skuteczne przeciwdziałanie temu zjawisku wymaga podejścia interdyscyplinarnego, łączącego działania prewencyjne, edukacyjne

i systemowe. Dużym walorem konferencji była obecność przedstawicieli służb mundurowych i osób pracujących z młodzieżą. Ich udział pozwolił spojrzeć na poruszane zagadnienia z perspektywy operacyjnej i wysoce pragmatycznej. Dzięki temu metody takie jak triada odporności zostały przeanalizowane pod kątem ich realnej skuteczności w codziennej pracy organów ścigania i instytucji wychowawczych. Kwestią otwartą pozostaje to, czy zaprezentowane koncepcje znajdą realne odzwierciedlenie w praktyce oraz w jakim czasie nastąpi zmiana przepisów prawa zorientowanych na realizację zgłoszonych postulatów.

Dr Aleksandra Komar

Zastępca redaktora naczelnego czasopisma naukowego ABW „Terro-
ryzm – studia, analizy, prewencja”.

Kontakt: a.komar@abw.gov.pl



PRACE KONKURSOWE





Polityki bezpieczeństwa Francji i Belgii w odpowiedzi na zagrożenia terrorystyczne na przykładzie zamachów w Paryżu (2015 r.) i Brukseli (2016 r.)¹

The security policies of France and Belgium
in response to terrorist threats: a case study
of the Paris (2015) and Brussels (2016) attacks

Nicole Szostak

Autorka niezależna



<https://orcid.org/0009-0001-9307-4951>

Abstrakt

Celem artykułu jest analiza polityki bezpieczeństwa Francji i Belgii w odpowiedzi na zagrożenia terrorystyczne na przykładzie zamachów w Paryżu (2015 r.) i Brukseli (2016 r.). Autorka przyjmuje tezę, że doświadczenia związane z atakami terrorystycznymi znacząco wpłynęły na ewolucję strategii bezpieczeństwa Francji oraz Belgii i doprowadziły do wzmocnienia działań prewencyjnych i współpracy międzynarodowej. Artykuł opiera się na analizie literatury

¹ Artykuł powstał na podstawie pracy licencjackiej pt. *Polityka bezpieczeństwa krajów frankońskich w odpowiedzi na zagrożenia terrorystyczne na przykładzie zamachów w Paryżu (2015 r.) i Brukseli (2016 r.)* obronionej na Akademii Sztuki Wojennej. Praca została wyróżniona w XV edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

przedmiotu, strategii bezpieczeństwa oraz studiach przypadków zamachów. Pytania badawcze dotyczą przyczyn i skutków zamachów, znaczenia procesów radykalizacji oraz roli współpracy transnarodowej w zakresie przeciwdziałania terroryzmowi. Analiza wykazała, że dla rozwoju terroryzmu w tych państwach mają znaczenie uwarunkowania historyczne i specyfika działalności organizacji terrorystycznych, a dla prowadzenia skutecznej polityki bezpieczeństwa – skoordynowane działania na poziomie międzynarodowym.

Słowa kluczowe

terroryzm, polityka bezpieczeństwa, Francja, Belgia, radykalizacja, współpraca międzynarodowa

Abstract

The aim of the article is to analyse the security policies of France and Belgium in response to terrorist threats, using the examples of the attacks in Paris (2015) and Brussels (2016). The author adopts the thesis that experiences related to terrorist attacks have significantly influenced the evolution of the security strategies of France and Belgium, led to the strengthening of preventive measures and international cooperation. The article is based on an analysis of the relevant literature, security strategy and case studies of the attacks. Research questions are focused on the causes and consequences of the attacks, the importance of radicalisation processes and the role of transnational cooperation in counterterrorism efforts. The analysis shows that historical conditions and the specific nature of terrorist organisations' activities are significant for the development of terrorism in these countries, while coordinated actions at international level are essential for the implementation of an effective security policy.

Keywords

terrorism, security policy, France, Belgium, radicalization, international cooperation

Wprowadzenie

Terroryzm jako jedno z największych zagrożeń XXI w. wpływa nie tylko na sytuację polityczną w państwie i jego stabilność, lecz także na ład międzynarodowy. Komisja Europejska definiuje terroryzm jako (...) *zagrożenie, które nie uznaje granic i dotyczy krajów i ludzi niezależnie od ich położenia*

geograficznego². Uważa, że zagrożenia terrorystyczne utrzymują się na wysokim poziomie, a ich zwalczanie traktuje jako wspólny europejski obowiązek. Ciągły rozwój zagrożeń terrorystycznych to czynnik, za sprawą którego upowszechniła się potrzeba wprowadzenia zmian w polityce oraz strategii bezpieczeństwa przez państwa i organizacje międzynarodowe. Przełomowym momentem w tej kwestii były lata 2015–2016. Francja oraz Belgia doświadczyły wtedy ataków terrorystycznych, które wpłynęły na postrzeganie skuteczności polityki bezpieczeństwa zarówno tych państw, jak i całej Europy. Świadczą o tym reakcje i działania np. Europolu, który w styczniu 2016 r. powołał Europejskie Centrum do spraw Zwalczania Terroryzmu (European Counter Terrorism Centre, ECTC) czy Komisji Unii Europejskiej, która 24 lipca 2020 r. stworzyła strategię w zakresie bezpieczeństwa obejmującą lata 2020–2025 z (...) *ochroną Europejczyków przed terroryzmem i przestępczością zorganizowaną*³ jako jednym z filarów.

Przedmiotem badań jest charakterystyka zagrożeń terrorystycznych i polityki bezpieczeństwa Francji i Belgii. W artykule zostaną wskazane kluczowe założenia polityki bezpieczeństwa Francji i Belgii na tle ewolucji działań i strategii prewencyjnych wynikających z regionalnych oraz międzynarodowych uwarunkowań, w tym członkostwa obydwu krajów w Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego (NATO), oraz doświadczeń z zamachów terrorystycznych. Autorka uwzględnia przy tym przyczyny, przebieg i skutki ataków terrorystycznych.

Najważniejsze pytanie badawcze brzmi: jakie są główne determinanty polityki bezpieczeństwa Francji i Belgii wobec zagrożeń terrorystycznych? W celu udzielenia odpowiedzi na to pytanie sformułowano następujące problemy szczegółowe:

1. Jakie czynniki i wydarzenia miały wpływ na rozwój zagrożeń terrorystycznych dla Francji i Belgii?
2. Jakie były konsekwencje zamachów terrorystycznych w kwestii polityki bezpieczeństwa Francji i Belgii?

² *Zwalczanie terroryzmu i radykalizacji postaw*, Komisja Europejska, 26 II 2026 r., https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation_en?prefLang=pl&etrans=pl [dostęp: 30 III 2026].

³ *Strategia UE w zakresie unii bezpieczeństwa: wszystkie elementy układanki we właściwym miejscu – nowy ekosystem bezpieczeństwa*, Komisja Europejska – Komunikat prasowy, Bruksela, 24 VII 2020 r., https://ec.europa.eu/commission/presscorner/api/files/document/print/pl/ip_20_1379/IP_20_1379_PL.pdf, s. 2 [dostęp: 12 VI 2026].

3. Jakie są najważniejsze działania prewencyjne i strategie bezpieczeństwa Francji i Belgii?
4. Jak wygląda współpraca regionalna oraz międzynarodowa w związku z zagrożeniami terrorystycznymi?

W artykule przyjęto hipotezę, że najważniejszymi determinantami polityki bezpieczeństwa Francji i Belgii wobec zagrożeń terrorystycznych są:

- uwarunkowania historyczne wraz z doświadczeniami związanymi z terroryzmem w obydwu państwach,
- islamistyczny charakter organizacji terrorystycznych z uwzględnieniem ich motywacji i celów,
- wpływ radykalizacji i migracji na rozwój terroryzmu,
- współpraca międzynarodowa dotycząca działań prewencyjnych.

Analiza została przeprowadzona za pomocą metod badawczych charakterystycznych dla nauk o bezpieczeństwie, takich jak analiza i synteza literatury przedmiotu, metoda porównawcza oraz studium przypadku wybranych zamachów terrorystycznych. Wykorzystane metody pozwoliły na identyfikację zależności między doświadczeniami związanymi z terroryzmem a kształtowaniem polityki bezpieczeństwa w danych krajach.

W artykule przedstawiono historyczne uwarunkowania terroryzmu we Francji i w Belgii, analizę zamachów w Paryżu i Brukseli oraz charakterystykę działań prewencyjnych i współpracy międzynarodowej w zakresie zwalczania terroryzmu.

Historyczne uwarunkowania terroryzmu we Francji i Belgii

Terroryzm jest wieloaspektowym zjawiskiem, które może przybierać różne formy. Mogą na nie wpływać cel, ideologia i wartości uznawane przez dany podmiot. Warto zaznaczyć, że współczesne zagrożenia terrorystyczne są ściśle powiązane z procesem radykalizacji, który skupia się na przyjmowaniu skrajnych poglądów i postaw, mogących prowadzić do akceptacji przemocy jako środka realizacji celów ideologicznych.

Analiza współczesnych aktów terrorystycznych to nie tylko spojrzenie na wydarzenia, lecz także ukazanie środowiska, w jakim ukształtowały się mechanizmy bezpieczeństwa. Autorka przeanalizowała dwa przełomowe pod względem terroryzmu wydarzenia we Francji i w Belgii. Są to odpowiednio seria zamachów w Paryżu w listopadzie 2015 r. oraz w porcie lotniczym Bruksela w Zaventem i w metrze w Brukseli w marcu 2016 r.

Jednocześnie ukazała chronologię i ewolucję terroryzmu w obydwu państwach.

We Francji początki terroryzmu sięgają czasów rewolucji francuskiej i rządu jakobinów w XVIII w.⁴ Pierwsze ataki terrorystyczne były związane z ruchami anarchistycznymi. W XIX w. do tak motywowanego aktu przemocy doszło w Paryżu w 1893 r. W Izbie Deputowanych wybuchła bomba. Sprawcą był Auguste Vaillant, który wspierał ruch anarchistyczny, ponieważ uznawał system polityczno-społeczny rządu francuskiego za niesprawiedliwy. Jak napisano w ówczesnej prasie, (...) *bomba została zrzucona z jednej z trybun na drugim piętrze, (...) eksplodowała, zanim uderzyła o ziemię, rozsiewając (...) ogromne gwoździe, kawałki cynku i ołowiu*⁵. Ten zamach zapoczątkował falę podobnych ataków we Francji.

W XX w. terroryzm we Francji był ściśle związany z konfliktami kolonialnymi. Podczas wojny algierskiej powstał Front Wyzwolenia Narodowego (fr. Front de Libération Nationale, FLN), (...) *czyli partia, która była kontynuacją rewolucyjnego organu, który kierował algierską wojną o niepodległość przeciwko Francji (1954–62)*⁶ oraz jego militarna część – Armia Wyzwolenia Narodowego (fr. Armée de Libération Nationale, ALN). Podczas bitwy o Algier żołnierze ALN atakowali przeważnie budynki użytku publicznego, zakłady przemysłowe czy miejsca odpoczynku i rozrywki⁷.

W kontekście tej wojny trzeba też wspomnieć o francuskiej Organisation de l'Armée Secrète (OAS), grupie terrorystycznej o skrajnie prawicowym charakterze, której działania były skierowane przeciwko tymczasowemu prezydentowi Charles'owi de Gaulle'owi. Celem OAS było powstrzymanie procesu dekolonizacji ze szczególnym uwzględnieniem kwestii algierskiej. Kiedy prezydent de Gaulle zgodził się na niepodległość Algierii, generał francuskiej armii Raoul Salan uznał prezydenta za zdrajcę narodu. Kierowana

⁴ Rząd jakobinów realizował swoją politykę metodami zastraszania i represji, które uznano za terror.

⁵ Za: M. Nadaux, *La Troisième République. La «propagande par le fait»: les attentats anarchistes (1892–1894). Explosion d'une bombe à la Chambre des députés déposée par l'anarchiste Auguste Vaillant le 9 décembre 1893, Le XIX^e siècle*, <https://web.archive.org/web/20061125095024/http://www.19e.org/documents/troisiemerepublique/anarattentats/vaillant.htm> [dostęp: 21 I 2025]. Wszystkie tłumaczenia w tekście pochodzą od autorki (dop. red.).

⁶ *National Liberation Front*, Britannica, <https://www.britannica.com/topic/National-Liberation-Front-political-party-Algeria> [dostęp: 22 I 2025].

⁷ Ł. Macuga, *Wojna algierska, 1954–1962*, praca magisterska, Uniwersytet Mikołaja Kopernika, Toruń 2004, https://www.researchgate.net/publication/303636471_Wojna_algierska_1954_-1962, s. 156 [dostęp: 22 II 2025].

przez Salana OAS przeprowadziła serię zamachów, w tym na Charles'a de Gaulle'a. Skutkiem tych ataków było ok. 12 000 zabitych i rannych⁸.

Kolejną organizacją terrorystyczną we Francji była Action Directe (AD), która kierowała się ideologiami takimi jak komunizm, anarchizm czy też maoizm oraz sympatią do krajów Globalnego Południa. Organizacja była najbardziej aktywna w latach 1979–1986, kiedy przeprowadziła 80 ataków na terenie Francji, głównie na ważne osobistości oraz instytucje państwowe, np. ministerstwa⁹. Terroryści z AD atakowali także w Belgii i w Niemczech.

Początki terroryzmu islamskiego we Francji sięgają lat 90. XX w. Jego przykładem jest Zbrojna Grupa Islamska (fr. Groupe Islamique Armé, GIA), która w 1995 r. dokonała zamachu w paryskim metrze. W wyniku wybuchu bomby zginęło 8 osób, 25 zostało poważnie, a 150 lekko rannych¹⁰.

Nowa fala terroryzmu islamskiego we Francji zaczęła się na początku XXI w. serią ataków organizowanych przez Al-Kaidę oraz Państwo Islamskie (Islamic State of Iraq and Syria, ISIS). Od 11 do 19 marca 2012 r. w Tuluzie i jej okolicach doszło do trzech ataków terrorystycznych. Dokonał ich 23-letni Mohamed Merah, który był związany z Al-Kaidą i wspierał fundamentalizm islamski. Te wydarzenia zainicjowały debatę na temat radykalizacji w Europie oraz zwróciły uwagę na kwestie bezpieczeństwa i integracji społecznej.

Historia terroryzmu w Belgii zaczyna się później niż we Francji. W 1983 r. w Belgii powstała lewicowa organizacja Cellules Communistes Combattantes (CCC), pod względem ideologicznym podobna do AD. *Od 3 października 1984 r. do 16 grudnia 1985 r. CCC przyznało się do 21 ataków; przeprowadzono je w ramach trzech kampanii polityczno-wojskowych*¹¹. Za wiele aktów terroru przeprowadzonych w tym samym czasie w Belgii

⁸ A. Kerherve, O.A.S, Gaullisme.fr, 30 VII 2011 r., <http://www.gaullisme.fr/2011/07/30/o-a-s/> [dostęp: 11 VI 2026].

⁹ M. Kijewska, *Lewicowy terroryzm w Europie Zachodniej w drugiej połowie XX i na początku XXI wieku. Podstawowe informacje i kierunki rozwoju*, „Radzyński Rocznik Humanistyczny” 2018, t. 16, nr 1, s. 206.

¹⁰ *27 lat temu doszło do zamachu bombowego w paryskim metrze*, iFrancja, 25 VII 2024 r., <https://www.ifrancja.fr/27-lat-temu-doszlo-do-zamachu-bombowego-w-paryskim-metrze/> [dostęp: 23 I 2025].

¹¹ B. Francq, *Les Cellules communistes combattantes: les deux figures d'une inversion*, „Sociologie du Travail” 1986, t. 28, nr 4, https://www.jstor.org/stable/43149431?casa_token=uvu0DUMH-hm8AAAAA%3AyTH00xhPSaWldOexG8URrz6nNtuZbUTI7TZ9D-cgAn0hvmw0Z43g9lB-tlOxUD2Fd2EggWffEMzdOeaYrtRtkSWMZS4nP0ao3SNdYXUPwB9a-zDSQ&seq=1, s. 459 [dostęp: 24 I 2025].

odpowiadała organizacja przestępcza Les tueurs fous du Brabant wallon, która współpracowała z CCC. W latach 80. XX w. CCC i AD nawiązały ze sobą bliskie kontakty. W 1984 r. belgijska organizacja napadła na kamieniołom w okolicach Brukseli. Skradzione stamtąd materiały wybuchowe przekazała AD, a ta z kolei (...) użyła [ich] do wybudowania bomby, którą podłożono w siedzibie Unii Zachodnioeuropejskiej¹².

W Belgii, podobnie jak we Francji, terroryzm w XXI w. jest kojarzony z powiązaniami islamistycznymi. Al-Kaida przez ponad dekadę skutecznie rekrutowała nowych członków na terenie zarówno Belgii, jak i Francji. Osoby odpowiadające za rekrutację zostały zidentyfikowane i w 2010 r. skazane na kary od 3 do 8 lat więzienia¹³. To jednak nie powstrzymało organizacji od przeprowadzenia zamachów, np. o podłożu antysemickim w 2014 r., kiedy w wyniku strzelaniny w Muzeum Żydowskim w Brukseli zginęły trzy osoby.

Terroryzm we Francji ma zatem dłuższą historię niż w Belgii. To wieloletnie doświadczenie Francja wykorzystuje w działaniach prewencyjnych i strategiach związanych z bezpieczeństwem czy antyterroryzmem. Autorka artykułu uważa, że z powodu historii oraz statystyk, które plasują Francję w czołówce państw z największą liczbą ataków terrorystycznych¹⁴, terroryzm stał się integralną częścią tego kraju. Belgia w swojej historii doświadczyła mniej działań terrorystycznych, ale również wykazuje się skutecznością w wykrywaniu terrorystów i prowadzeniu działań prewencyjnych.

Znaczenie Paryża i Brukseli w polityce międzynarodowej

Paryż oraz Bruksela odgrywają szczególną rolę w stosunkach międzynarodowych oraz w europejskiej polityce i kulturze.

Stolica Francji jest kojarzona z wartościami republikańskimi jak wolność, równość i braterstwo. Odzwierciedleniem tego są rewolucja francuska i związane z nią Deklaracja Praw Człowieka i Obywatela oraz traktat wersalski. W Paryżu znajdują się siedziby instytucji międzynarodowych takich jak: Interpol (International Criminal Police Organization), Organizacja Współpracy Gospodarczej i Rozwoju (Organisation for Economic Co-operation

¹² M. Kijewska, *Lewicowy terroryzm...*, s. 206.

¹³ *Koledzy z Al-Kaidy skazani w Belgii*, TVN24, 10 V 2010 r., <https://tvn24.pl/swiat/koledzy-z-al-kaidy-skazani-w-belgii-ra133541-ls3584645> [dostęp: 25 I 2025].

¹⁴ Zob. np. *Terroryzm w UE: fakty i liczby*, Rada Europejska i Rada Unii Europejskiej, <https://www.consilium.europa.eu/pl/infographics/terrorism-eu-facts-figures/> [dostęp: 25 I 2025].

and Development, OECD) czy Organizacja Narodów Zjednoczonych do spraw Edukacji, Nauki i Kultury (United Nations Educational, Scientific and Cultural Organization, UNESCO). Z kolei Bruksela pełni funkcję jednego z najważniejszych ośrodków decyzyjnych ze względu na siedziby UE i NATO. Różnorodność językowa oraz usytuowanie wielu organizacji międzynarodowych w belgijskiej stolicy sprawia, że wpisuje się ona w motto UE – *Zjednoczona w różnorodności*¹⁵.

Obydwa miasta od lat stanowią dla organizacji terrorystycznych cele o szczególnym znaczeniu strategicznym i symbolicznym. Zamachy terrorystyczne przeprowadzone w tych lokalizacjach nie tylko miały zadać straty materialne i ludzkie oraz wywołać poczucie braku bezpieczeństwa w społeczeństwie, lecz także były znakiem odrzucenia europejskich wartości przez organizacje terrorystyczne. Dodatkowo ataki w Paryżu i Brukseli miały na celu zmaksymalizowanie rozgłosu medialnego oraz wywarcie wpływu na opinię publiczną w Europie i na całym świecie.

Przebieg i przyczyny zamachów

Państwo Islamskie to organizacja, która zgodnie ze swoją religią uznaje państwa Zachodu za niewierne i niemoralne. Jednym z celów ISIS jest globalna ekspansja religijna. W przypadku ataków na Paryż ich przyczyną była także chęć zemsty za operację „Chammal”¹⁶, która rozpoczęła się 19 września 2014 r. Państwo Islamskie uznało ją za ingerencję w swoje terytorium i działalność, co przyczyniło się do wrogiego nastawienia wobec Francji. Ponadto organizacja uznała za słuszne zaatakowanie lokalizacji symbolicznej dla wolności osobistej oraz zachodniego stylu życia, interpretowanego przez islam jako konsumpcjonistyczny¹⁷.

¹⁵ *Motto UE*, Unia Europejska, 23 XII 2025 r., https://european-union.europa.eu/principles-countries-history/symbols/eu-motto_pl [dostęp: 18 III 2026].

¹⁶ Operacja „Chammal” – francuska część międzynarodowej operacji „Inherent Resolve”, skupiającej 80 krajów i 5 organizacji międzynarodowych, której celem było umożliwienie irackim władzom samodzielnego zapewnienia bezpieczeństwa swojego kraju. W ramach „Chammal” Francja zapewniała wsparcie militarne irackim siłom biorącym udział w walce z ISIS. Zob. *Opération CHAMMAL*, Ministère des Armées, <https://www.defense.gouv.fr/operations/monde/grand-levant/operation-chammal> [dostęp: 10 IV 2025].

¹⁷ V. Romania, S. Tozzo, *Terrorism as ritual process and cultural trauma: A performative analysis of ISIS's attacks in Europe*, „Italian Sociological Review” 2017, t. 7, nr 2, s. 243. <https://doi.org/10.13136/isr.v7i2.177>.

Paryż (2015)

Pierwszy atak terrorystyczny w Paryżu w 2015 r. został przeprowadzony 7 stycznia w siedzibie redakcji magazynu „Charlie Hebdo”. Ten satyryczny tygodnik jest znany z publikowania karykatur o kontekście politycznym, kulturowym oraz religijnym. Ostatni z nich okazał się kluczowy w odniesieniu do zamachu, ponieważ redakcja „Charlie Hebdo” wiele razy drukowała karykatury Mahometa i przywódcy ISIS Abu Bakra al-Bagdadi, czym narażała się wyznawcom islamu. Uznaje się to za przyczynę ataku¹⁸. W związku z wieloma prowokacjami ze strony redakcji budynek siedziby „Charlie Hebdo” został podpalony w listopadzie 2011 r.

Atak rozpoczął się od zaskoczenia i zastraszenia rysowniczek redakcji, która wpuściła terrorystów do budynku, a ci otworzyli ogień w kierunku pracowników. Podczas strzelaniny schowała się pod biurkiem. Według jej zeznań ostrzał trwał 5 minut, a od zamachowców słyszała okrzyki „Pomściliśmy proroka” i „Allah Akbar”¹⁹. W wyniku ataku zginęło 12 osób, w tym redaktor naczelny gazety Stephane Charbonnier „Charb”, od 2013 r. figurujący na czarnej liście Al-Kaidy. Po zamachu sprawcy podjęli próbę ucieczki, w czasie której ostrzelali samochód policyjny. Jeden z policjantów został zabity, co zwiększyło chaos i skalę zagrożenia. Po stłuczce terroryści porzucili swój samochód, w którym policjanci odnaleźli dokumenty umożliwiające odkrycie tożsamości oprawców. Byli to bracia szkoleni w Jemenie przez ISIS. Zatrzymano siedmiu członków ich rodziny. W następnych dniach nastąpiły kolejne ataki. W czasie jednego z nich kontrterroryści zabili zamachowców.

Do kolejnej serii skoordynowanych zamachów przeprowadzonych przez ISIS na terenie Paryża doszło w listopadzie 2015 r. Kluczowy atak nastąpił 13 listopada w Teatrze Bataclan, gdzie odbywał się koncert zespołu rockowego Eagles of Death Metal. Uczestnicy koncertu nie wiedzieli, że na stadionie Stade de France, gdzie w tym samym czasie rozgrywał się mecz reprezentacji Francji i Niemiec, doszło do eksplozji. O godzinie 21.49 mężczyźni uzbrojeni w karabiny maszynowe podeszli do drzwi teatru, zastrzelili portiera oraz ludzi stojących przed wejściem i weszli do budynku. Stanęli w tylnej części sali koncertowej, skąd otworzyli ogień w stronę tłumu. Funkcjonariusz, który pierwszy wszedł do budynku, strzelił do jednego

¹⁸ Abu Bakr al-Bagdadi – założyciel i przywódca sunnickiej organizacji terrorystycznej, od 2014 r. do śmierci w 2019 r. samowwłaściwy kalif Państwa Islamskiego.

¹⁹ *Najpierw zabijali w redakcji, potem zastrzelili policjanta. Tak przebiegał zamach*, TVN24, 8 I 2015 r., <https://tvn24.pl/swiat/zamach-na-charlie-hebdo-tak-przebiegal-atak-ra504096-1s3289349> [dostęp: 8 IV 2025].

z napastników uzbrojonego w granaty, co spowodowało wybuch i doprowadziło do śmierci terrorysty. Dwóch pozostałych terrorystów wzięło ok. 20 zakładników, których uratowano dzięki szturmowi policyjnemu. W teatrze zginęło 90 osób, przede wszystkim młodzi ludzie. Łącznie w wyniku ataków przeprowadzonych tego dnia śmierć poniosło 130 osób²⁰.

Policjanci odnaleźli w koszu na śmieci telefon jednego z oprawców. Doprowadziło to do pokoju hotelowego, w którym terroryści przebywali przez tydzień i gdzie znajdowały się sprzęty i materiały służące do zbudowania bomb.

Bruksela (2016)

Za głównego koordynatora zamachów we Francji uznawano Salaha Abdeslama, który ukrył się w brukselskiej dzielnicy Molenbeek. W gazetach tłumaczono, że (...) *„Molenbeek to miejsce, w którym bardzo łatwo można zniknąć”. To tu mieści się najwięcej brukselskich czarnych dziur, do których policja rzadko się zapuszcza, a rządzą gangi narkotykowe i handlarze broni. (...) Molenbeek nie bez powodu stał się centrum europejskiego dżihadu*²¹. Po atakach z 13 listopada 2015 r. terroryści niejednokrotnie otrzymywali schronienie w tej dzielnicy zamieszkałej w większości przez osoby pochodzące z Afryki Północnej oraz wyznania muzułmańskiego. Tak było też z Abdeslamem, którego pobyt przyczynił się do rozwoju radykalizmu w tej okolicy. Po aresztowaniu podczas przesłuchań Abdeslam przyznał, że były planowane kolejne ataki terrorystyczne, tym razem w Belgii. Miały one na celu demonstrację zdolności ISIS do przeprowadzenia zamachów, mimo poniesionych strat, oraz potwierdzenie gotowości do dalszych działań na terenie Francji i Belgii i całej Europy.

Cztery dni po aresztowaniu Abdeslama, 22 marca 2016 r., doszło do dwóch samobójczych ataków terrorystycznych. Pierwszy nastąpił w porcie lotniczym Zaventem, gdzie ok. godziny 7.45 trzej mężczyźni przyjechali taksówką z dzielnicy Molenbeek. Kilkanaście minut później w hali odlotów międzynarodowych (...) *jeden z terrorystów zdetonował pierwszą bombę znajdującą się w jego walizce, w kolejce do odprawy bagażowej przy stanowisku*

²⁰ K. Stańko, *Największy proces karny w historii Francji. Dziś wyrok w sprawie ataków terrorystycznych z 2015 roku*, Polska Agencja Prasowa, 29 VI 2022 r., <https://www.pap.pl/aktualnosci/news%2C1270741%2Cfrancja-byl-najwiekszy-proces-karny-w-historii-dzis-wyrok-w-sprawie-atakow#:~:text=13%20listopada%202015> [dostęp: 10 VI 2026].

²¹ „Mózg” krwawych zamachów w Paryżu zatrzymany, *Newsweek Polska*, 18 III 2016 r., <https://web.archive.org/web/20160322133717/http://swiat.newsweek.pl/sprawca-krwawych-zamachow-w-paryzu-salah-abdeslam-zatrzymany,artykuly,382261,1.html> [dostęp: 10 IV 2025].

nr 11. Kilka sekund później nastąpiła druga eksplozja przy stanowisku nr 2, drugi terrorysta zdetonował bombę ukrytą w swoim bagażu²². Trzeci mężczyzna, prawdopodobnie ze względu na rozpoczętą ewakuację lotniska, nie zdetonował bomby i uciekł. Służby bezpieczeństwa zlokalizowały jego torbę z ładunkiem. W wyniku wybuchów zginęło 20 osób. Po ataku udało się zidentyfikować tożsamości terrorystów. Zginęli Najim Laachraoui i Ibrahim El Bakraoui. Trzeci napastnik, Mohamed Abrini, który był powiązany również z atakami z 2015 r. w Paryżu, został aresztowany 8 kwietnia 2016 r.

Tego samego dnia ok. godziny 9.11 doszło do dwóch eksplozji w metrze. Według belgijskich władz sprawca wsiadł do pociągu na stacji metra Molenbeek. Wybuch, wywołany prawdopodobnie przy pomocy drugiego zamachowca, nastąpił w pobliżu unijnych budynków w godzinach porannego szczytu²³. Zginęło 12 osób.

W wyniku obu zamachów 22 marca 2016 r. śmierć poniosły łącznie 32 osoby, a ok. 320 zostało rannych. Następnego dnia ISIS przyznało się do dokonania ataków terrorystycznych w porcie lotniczym oraz na stacji metra. Śledztwo wykazało, że za zamachami we Francji i w Belgii stała ta sama francusko-belgijska komórka dżihadystów²⁴.

Najważniejsze skutki społeczne zamachów w Paryżu i Brukseli

Badania dotyczące wpływu ataków terrorystycznych na społeczeństwo²⁵ wyraźnie wskazują na negatywne skutki dla zdrowia psychicznego oraz

²² *Belgique – attentats à l’aéroport et dans le métro de Bruxelles*, Association française des Victimes du Terrorisme, <https://www.afvt.org/belgique-attentats-a-laeroport-et-dans-le-metro-de-bruxelles/> [dostęp: 10 IV 2025].

²³ *Tactics, Techniques and Procedures Used in the 22 March 2016 Brussels Attacks*, „Joint Intelligence Bulletin”, 12 IV 2016 r., <https://info.publicintelligence.net/DHS-FBI-NCTC-BrusselsAttacks.pdf>, s. 2 [dostęp: 11 IV 2025].

²⁴ Ch. Gracieux, *Les attentats du 22 mars 2016 à Bruxelles*, Lumni Enseignement, 23 III 2016 r., <https://enseignants.lumni.fr/fiche-media/00000001857/les-attentats-du-22-mars-2016-a-bruxelles.html> [dostęp: 11 IV 2025].

²⁵ P. Pirard i in., *Use of mental health supports by civilians exposed to the November 2015 terrorist attacks in Paris*, „BMC Health Services Research” 2020, t. 20. <https://doi.org/10.1186/s12913-020-05785-3>; R. Deschepper i in., *Association between feeling threatened by a terrorist attack and subjective health: a web survey a week after the attacks of 22 March 2016 in Belgium*, „European Journal of Psychotraumatology” 2018, t. 9, nr 1. <https://doi.org/10.1080/20008198.2018.1500821>.

fizycznego obywateli. Na tej podstawie można domniemywać, że zamachy terrorystyczne w 2015 r. oraz 2016 r. dotknęły mieszkańców Francji i Belgii i zwiększyły zapotrzebowanie na pomoc psychologiczną. Naukowcy podkreślają, że państwa zagrożone atakami terrorystycznymi powinny tworzyć oraz rozwijać programy wsparcia psychologicznego zarówno w trybie interwencji kryzysowej, jak i długofalowych terapii po zdarzeniach.

Zarówno francuskie władze, społeczeństwo, jak i media odebrały atak terrorystyczny na „Charlie Hebdo” nie tylko jako atak na redakcję i pracujące w niej osoby, lecz także jako zamach na wartości takie jak demokracja, wolność słowa czy pokój. Krótco po zamachu powstało logo z hasłem *Je suis Charlie* (pol. Jestem Charlie)²⁶, które szybko rozpowszechniło się w internecie i stało się symbolem wsparcia oraz solidarności z ofiarami. W wielu miastach odbywały się manifestacje i marsze, a wśród nich Marsz Republiki (fr. Marche Républicaine) w Paryżu, który miał na celu upamiętnienie ofiar ataku oraz wyrażał sprzeciw wobec agresji i samego terroryzmu. W marszu wzięli udział (...) *niemal wszyscy przywódcy polityczni, związkowi i religijni, a także głowy państw i rządów zagranicznych*²⁷.

Zauważono również wzrost postaw rasistowskich oraz islamofobicznych w społeczeństwie, co odnotowały nie tylko francuskie czy belgijskie media²⁸. Na popularności zyskały partie popierające politykę zamkniętych granic dla imigrantów²⁹.

Negatywnie oceniono służby specjalne i policyjne zarówno we Francji, jak i w Belgii. W Belgii zarzucano im długi czas reakcji, brak kontroli i inicjatyw policji w dzielnicach takich jak Schaerbeek oraz Molenbeek, uważanych za centrum rozwoju terroryzmu oraz radykalnych wpływów

²⁶ Autorem tej wizualizacji jest Joachim Roncin, który w tamtym czasie był dyrektorem artystycznym magazynu „Stylist”.

²⁷ J.-B. Garat, *L'impressionnante liste des politiques présents à la marche à Paris*, Le Figaro, 10 I 2015 r., <https://www.lefigaro.fr/politique/2015/01/10/01002-20150110ARTFIG00160-l-impressionnante-liste-des-politiques-presentes-a-la-marche-republicaine-a-paris.php> [dostęp: 9 IV 2025].

²⁸ C. Lafon, *Attentats de Paris: ces deux semaines qui ont changé la France*, Sud Ouest, 22 I 2015 r., <https://www.sudouest.fr/redaction/attentats-de-paris-ces-deux-semaines-qui-ont-change-la-france-8022926.php> [dostęp: 12 IV 2025]; B. Jastrzębski, *Jastrzębski: Zamachy w Brukseli – to nie koniec świata*, Respublica, 22 III 2016 r., <https://respublica.pl/teksty/jastrzebski-zamachy-w-brukseli-to-nie-koniec-swiata-56188.html> [dostęp: 12 IV 2025].

²⁹ A. Chrisafis, *Marine Le Pen's Front National makes political gains after Paris attacks*, The Guardian, 1 XII 2015 r., <https://www.theguardian.com/world/2015/dec/01/marine-le-pen-front-national-political-gains-paris-attacks> [dostęp: 12 VI 2026].

w tym kraju, takich jak Schaerbeek oraz Molenbeek³⁰. We Francji parlamentarna komisja śledcza, która zajmowała się analizą ataków z 2015 r., wydała raport dotyczący służb wywiadowczych. Oceniała zamachy jako porażkę wywiadu spowodowaną przez m.in. brak komunikacji między służbami wywiadowczymi³¹. Komisja zaleciła reorganizację na wzór amerykańskiego National Counterterrorism Center (NCTC) utworzonego w USA po zamachach z 11 września 2001 r.

Charakterystyka głównych instytucji i służb bezpieczeństwa zwalczających terroryzm we Francji i w Belgii

Doświadczenia z 2015 r. oraz 2016 r. wpłynęły na reorganizację i dążenie do wzmocnienia krajowych zdolności antyterrorystycznych we Francji i w Belgii.

We Francji kluczowe instytucje odpowiedzialne za zwalczanie terroryzmu to:

- 1) Generalna Dyrekcja Bezpieczeństwa Wewnętrznego (fr. Direction Générale de la Sécurité Intérieure, DGSI) – posiada m.in. wydział tematyczny zajmujący się rodzajami terroryzmu, wydział analiz ukierunkowany na regiony i państwa oraz wydział ds. sił zbrojnych i kontrwywiadu. Od 2018 r. DGSI jest najważniejszą instytucją w zakresie prewencji terrorystycznej we Francji;
- 2) Generalna Dyrekcja Bezpieczeństwa Zewnętrznego (fr. Direction Générale de la Sécurité Extérieure, DGSE) – francuski wywiad, który w kontekście terroryzmu koncentruje się na identyfikowaniu grup terrorystycznych, ich struktury organizacyjnej i kanałów rekrutacyjnych, a także udaremnianiu ataków planowanych za granicą³²;

³⁰ Tamże; M. Hallam, *Belgian shortcomings in focus*, DW, 30 III 2016 r., <https://www.dw.com/en/the-shortcomings-of-belgiums-brussels-terror-investigations/a-19151338> [dostęp: 12 VI 2026].

³¹ A. Kacprzak, *Komisja śledcza francuskiego parlamentu: Wywiad poniósł porażkę, nie zapobiegł atakom. Należy utworzyć agencję do walki z terroryzmem*, wPolityce, 5 VII 2016 r., <https://wpolityce.pl/swiat/299492-komisja-sledcza-francuskiego-parlamentu-wywiad-poniosl-porazke-nie-zapobieg-l-atak-om-nalezy-utworzyc-agencje-do-walki-z-terroryzmem?strona=1> [dostęp: 12 IV 2025].

³² *Nos missions*, Direction Générale de la Sécurité Extérieure, <https://www.dgse.gouv.fr/fr/nous-connaître/nos-missions> [dostęp: 30 IV 2025].

- 3) Generalna Dyrekcja Policji Krajowej (fr. Direction générale de la police nationale, DGPN) – realizuje podstawowe zadania w celu utrzymania porządku i bezpieczeństwa na terenie kraju. Dzięki swoim uprawnieniom może zapobiegać zamachom terrorystycznym;
- 4) Krajowa Prokuratura Antyterrorystyczna (fr. Le parquet national anti-terroriste, PNAT) – nie jest służbą specjalną, ale od 2019 r. odgrywa ważną rolę w zwalczaniu terroryzmu. Została powołana w celu zwiększenia zdolności reagowania na akty terrorystyczne.

W Belgii za przeciwdziałanie terroryzmowi są odpowiedzialne:

- 1) Służba Bezpieczeństwa Państwa (niderl. Veiligheid van de Staat, VSSE) – belgijski wywiad cywilny i służba bezpieczeństwa. Powołana w 1830 r., jest najstarszą służbą wywiadowczą na świecie³³. Zajmuje się wywiadem, śledztwem oraz kontrolą bezpieczeństwa. VSSE można porównać do francuskiego DGSi;
- 2) Organ Koordynacyjny ds. Analizy Zagrożeń (niderl. Orgaan voor de Coördinatie en de Analyse van de Dreiging, OCAD; fr. Organe de Coordination pour l'Analyse de la Menace, OCAM) – do jego zadań należy m.in. tworzenie bazy danych, z której korzystają służby policyjne, wywiadowcze oraz sądowe, wdrażanie *Strategii walki z ekstremizmem i terroryzmem* (fr. *La Stratégie Extrémisme et Terrorisme*, T.E.R.)³⁴, międzynarodowa współpraca w kwestii walki z terroryzmem;
- 3) Policja Federalna – zwalcza przestępczość, utrzymuje porządek publiczny i dba o bezpieczeństwo na poziomie krajowym;
- 4) Główna Służba Wywiadu i Bezpieczeństwa (niderl. Algemene Dienst Inlichting en Veiligheid, ADIV; fr. Service Général du Renseignement et de la Sécurité, SGRS) – monitoruje informacje i działania pochodzące z zagranicy, które mogą stanowić zagrożenie dla bezpieczeństwa Belgii³⁵.

W kontekście omawianej problematyki obydwa państwa mają strukturę, która łączy działania wywiadowcze, policyjne, sądowe oraz analityczne. Dzięki tak rozwiniętej organizacji jest możliwa szybka identyfikacja zagrożeń i reakcja na nie. Widoczne podobieństwa pomagają w utrzymaniu

³³ *Qui sommes-nous?*, Veiligheid van de Staat, <https://www.vsse.be/fr/qui-sommes-nous/historique> [dostęp: 1 V 2025].

³⁴ *La Stratégie Extrémisme et Terrorisme (Stratégie T.E.R.)*, OCAM, <https://ocam.belgium.be/la-strategie-extremisme-et-terrorisme-strategie-t-e-r/> [dostęp: 12 IV 2025].

³⁵ *Nos missions*, SGRS, <https://www.sgrs.be/nous-connaitre/nos-missions/> [dostęp: 1 V 2025].

bezpieczeństwa międzynarodowego. Stosunki między Francją i Belgią dotyczące działań prewencyjnych opierają się na strukturalnej integracji służb i współpracy w kwestiach informacji.

Strategie prewencyjne dotyczące radykalizacji

Rozwój i wzmocnienie ruchów radykalnych zwiększają prawdopodobieństwo wystąpienia aktów terroru. Aby przeciwdziałać tym procesom, Francja i Belgia skupiły się na prewencji społecznej, edukacyjnej i cyfrowej.

We Francji po atakach z 2015 r. i 2016 r. rozszerzono działania w ramach planu Vigipirate³⁶ oraz rozpoczęto wojskową operację „Sentinelle”, polegającą na rozmieszczeniu żołnierzy w przestrzeni publicznej w celu ochrony kluczowych obiektów i wsparcia działań policyjnych. Francuskie władze zwiększyły również uprawnienia służb antyterrorystycznych, rozszerzyły monitorowanie osób podejrzanych o ekstremizm oraz podjęły działania mające przeciwdziałać radykalizacji, m.in. w szkołach, więzieniach i internecie. Francuski rząd wprowadził 30 października 2017 r. ustawę o wzmocnieniu bezpieczeństwa wewnętrznego i walce z terroryzmem³⁷. Jednocześnie pracowano nad planem działania przeciwko postawom radykalnym i terroryzmowi (w skrócie PART), który ogłoszono w 2018 r. PART wskazuje pięć głównych osi, wokół których koncentruje się 60 środków do zmiany polityki prewencyjnej:

- 1) wzmacnianie odporności społeczeństwa na radykalizację,
- 2) uzupełnianie sieci wykrywania i zapobiegania radykalizacji,
- 3) lepsze zrozumienie i przewidywanie ewolucji radykalizacji,
- 4) profesjonalizacja lokalnych podmiotów i ocena stosowanych praktyk,
- 5) dostosowanie działań w zakresie wycofywania z radykalizacji³⁸.

³⁶ Plan Vigipirate to francuski rządowy system zapobiegania terroryzmowi, ochrony i reagowania. Zob. *The Plan Vigipirate*, Republique Francaise, <https://www.campusfrance.org/en/security> [dostęp: 26 V 2026].

³⁷ *LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035932811> [dostęp: 10 VI 2026].

³⁸ «Prévenir Pour Protéger». *Plan national de prévention de la radicalisation*, <https://www.cipdr.gouv.fr/wp-content/uploads/2018/11/DP2018-02-23-CIPDR-Radicalisation-V5.pdf>, s. 5 [dostęp: 10 VI 2026].

W 2026 r. została opublikowana nowa francuska strategia na lata 2026–2030 dotycząca zapobiegania przestępczości (*Stratégie nationale de prévention de la délinquance 2026–2030: Prévenir pour protéger*, SNPD), w której wskazano trzy główne osie działania:

- 1) dostosowywanie reakcji na nowe formy przestępczości, czyli wzmacnianie inicjatyw w zakresie podnoszenia świadomości, szkoleń i wsparcia, z jednoczesną konsolidacją proaktywnych zdolności interesariuszy;
- 2) zapewnienie ciągłości działań profilaktycznych od dzieciństwa do dorosłości, czyli wspieranie rodzicielstwa, rozwijanie umiejętności psychospołecznych, lepsze identyfikowanie sytuacji zagrożenia i promowanie zaangażowania młodzieży w celu zapobiegania przestępczości;
- 3) lepsza koordynacja i wyposażenie interesariuszy przez wzmacnianie zarządzania terytorialnego i tworzenie akademii prewencji cyfrowej, która będzie gromadzić zasoby, upowszechniać najlepsze praktyki i szkolić specjalistów³⁹.

Francja ma również program terytorialnego zapobiegania gwałtownej radykalizacji⁴⁰, polegający na udzielaniu pomocy osobom, które uległy radykalizacji lub są na nią narażone, i zapobieganiu ryzyku, że takie osoby staną się agresywne. Program został opracowany w 2014 r., a zaktualizowany w 2018 r. przez Les groupes d'évaluation départementaux, które są odpowiedzialne za analizę zagrożeń związanych z radykalizacją i koordynację programu.

W Belgii najważniejszym przedsięwzięciem przeciwko radykalizacji był tzw. plan R⁴¹, który został zastąpiony 8 września 2021 r. przez strategię T.E.R.⁴² W walkę z radykalizacją zaangażowały się też instytucje edukacyjne takie jak GO! – Edukacja Wspólnoty Flamandzkiej (GO! – onderwijs van de Vlaamse Gemeenschap) oraz Royal Athenaeum Antwerp. Te organizacje wspólnie opracowały piramidę prewencji Johana Declercka (rysunek 1).

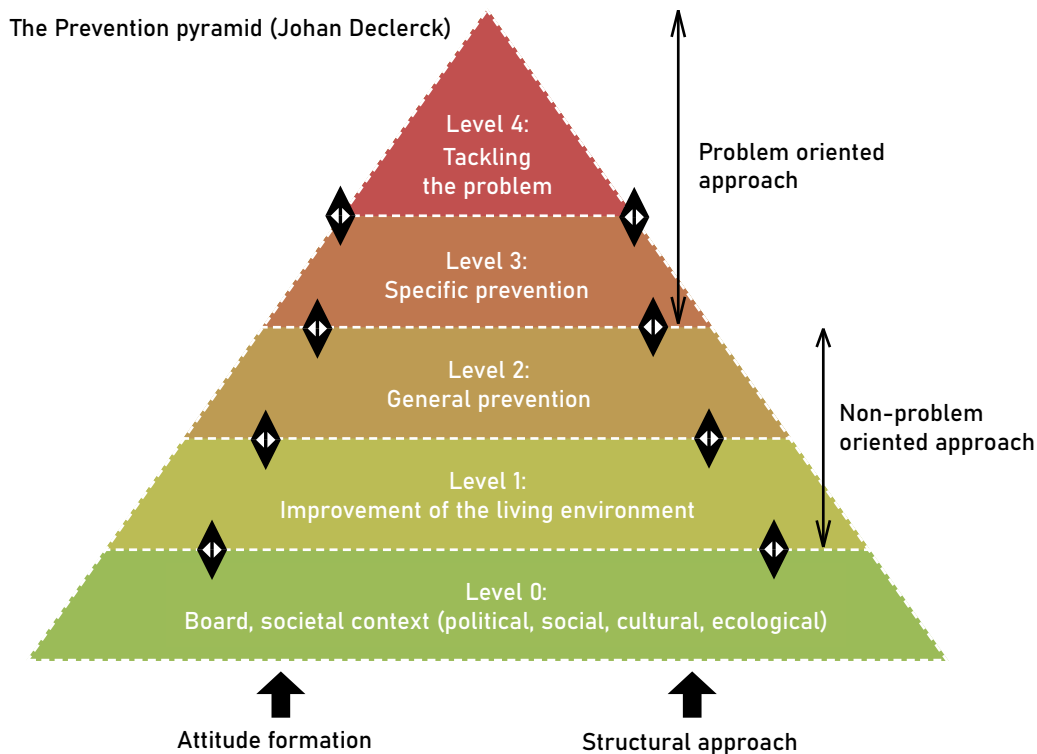
³⁹ *Stratégie nationale de prévention de la délinquance 2026–2030: Prévenir pour protéger*, CIPDR, 24 IV 2026 r., <https://www.cipdr.gouv.fr/strategie-nationale-de-prevention-de-la-delinquance-2026-2030-prevenir-pour-protoger/> [dostęp: 12 V 2026].

⁴⁰ *Dispositif territorial de prévention de la radicalisation violente*, Direction Générale de la Sécurité Intérieure, 14 VI 2021 r., <https://www.dgsi.interieur.gouv.fr/dispositif-territorial-de-prevention-de-radicalisation-violente> [dostęp: 11 VI 2026].

⁴¹ Zob. *Le Plan R. Le Plan d'Action Radicalisme*, https://ocam.belgium.be/wp-content/uploads/2020/11/brochure_radicalisme_fr.pdf [dostęp: 10 VI 2026].

⁴² *La Stratégie Extrémisme et Terrorisme (Stratégie T.E.R.)...*

Jest to projekt szkoleń dla różnych instytucji, który został przyjęty nie tylko przez belgijski rząd, lecz także przez Komisję Europejską.



Rysunek 1. Piramida prewencji Johana Declercka.

Źródło: opracowanie własne na podstawie: *The Prevention Pyramid*, European Commission, 2 VII 2024 r., https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/prevention-pyramid_en [dostęp: 4 V 2025]. Dokonano zmian w oprawie graficznej (dop. red.).

Piramida (...) jest narzędziem, które można wykorzystać do orientacji i uzyskania wglądu w sposób optymalizacji polityki zapobiegania radykalizacji⁴³. Została podzielona na pięć poziomów, z których pierwsze trzy są określone jako nieorientowane na problem:

⁴³ *The Prevention Pyramid*, European Commission, 2 VII 2024 r., https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/prevention-pyramid_en [dostęp: 4 V 2025].

- poziom 0 – środowisko społeczne,
- poziom 1 – warunki życia i możliwości ich poprawy,
- poziom 2 – ogólne zapobieganie,
- poziom 3 – prewencja szczególna,
- poziom 4 – rozwiązanie problemu.

Piramida Declercka powstała w 2001 r., ale po atakach z 2015 r. oraz 2016 r. została zaktualizowana. Wówczas niektóre środowiska uznały, że należy skupić się na poziomie 4 (podejście zorientowane na problem)⁴⁴. Projekt jest realizowany w całej Europie.

Na podstawie strategii T.E.R. w Belgii zaczęto także tworzyć Lokalne Grupy Zadaniowe (fr. Les Taskforces locales, TFL) oraz Lokalne Komórki Bezpieczeństwa Integralnego zajmujące się problemami radykalizmu, ekstremizmu i terroryzmu⁴⁵. TFL łączą ze sobą służby policyjne, bezpieczeństwa i wywiadu, urząd migracyjny oraz prokuraturę. Ich praca koncentruje się na poziomie operacyjnym (zbieranie informacji, monitorowanie i ocenianie ryzyka) oraz poziomie strategicznym (pilnowanie zgodności strategicznej między członkami TFL).

Współpraca międzynarodowa w walce z terroryzmem

Po doświadczeniach z atakami terrorystycznymi Francja i Belgia uznały, że skuteczna walka z tym zagrożeniem polega nie tylko na zabezpieczeniu kraju, lecz także wykracza poza jego granicę. Dlatego zacieśniły współpracę wywiadowczą oraz w zakresie działań operacyjnych, a także rozszerzyły ją na szczebel globalny.

Premier Belgii Charles Michel oraz premier Francji Manuel Valls spotkali się w Brukseli 1 lutego 2016 r.⁴⁶ Dzięki współpracy belgijskich władz i ich partnerów w Niemczech, Francji i Luksemburgu udaremniono m.in. atak terrorystyczny we Francji zaplanowany na 1 lipca 2018 r.⁴⁷

⁴⁴ Tamże, s. 1.

⁴⁵ *La Stratégie Extrémisme et Terrorisme (Stratégie T.E.R.)...*

⁴⁶ *France, Belgium to step up counter-terrorism cooperation in wake of Paris attacks*, France 24, 2 II 2016 r., <https://www.france24.com/en/20160202-france-belgium-step-counter-terrorism-cooperation-paris-attacks> [dostęp: 10 V 2025].

⁴⁷ EUROJUST, *The ARGO Case – Diplomatic immunity in a cross-border terrorism case*, <https://www.eurojust.europa.eu/sites/default/files/assets/argo-case-28-06-2024-pdf-v2.pdf>, s. 3 [dostęp: 10 V 2025].

Unia Europejska utworzyła instytucje, które skupiają się na bezpieczeństwie państw europejskich. Powołane przez Europol ECTC⁴⁸ zajmuje się wymianą informacji, danych oraz dostosowaniem wsparcia operacyjnego służb policyjnych, wywiadowczych czy specjalnych państw członkowskich, analizuje także szeroki kontekst zagrożeń terrorystycznych w celu identyfikacji nowych kierunków dochodzeń. Kooperacja ta pozwala na szybkie reagowanie oraz działanie przeciwko terroryzmowi.

Europol od 2006 r. publikuje coroczne sprawozdania dotyczące sytuacji i tendencji w obszarze terroryzmu w UE⁴⁹.

Unia Europejska wprowadziła też systemy wspomagające przeciwdziałanie terroryzmowi oraz kontrolę granic zewnętrznych i wewnętrznych:

- 1) System Informacyjny Schengen (Schengen Information System, SIS) – pomaga służbom granicznym oraz migracyjnym w ochronie i kontroli granic wewnętrznych UE⁵⁰;
- 2) Europejski system przekazywania informacji z rejestrów karnych (European Criminal Records Information System, ECRIS) – to zdecentralizowany system informatyczny oparty na bazach danych krajowych rejestrów karnych⁵¹;
- 3) Passenger Name Record (PNR) – to system, który przechowuje dane osobowe osób podróżujących liniami lotniczymi⁵²;

⁴⁸ *European Counter Terrorism Centre – ECTC*, Europol, <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> [dostęp: 10 V 2025].

⁴⁹ Zob. np. *EU Terrorism Situation & Trend Report (EU TE-SAT)*, Europol, <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> [dostęp: 11 VI 2026].

⁵⁰ *System Informacyjny Schengen*, Komisja Europejska, https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_pl [dostęp: 10 V 2025].

⁵¹ *Decyzja Rady 2009/316/WSiSW z dnia 6 kwietnia 2009 r. w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS)*, zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW; *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/884 z dnia 17 kwietnia 2019 r. zmieniająca decyzję ramową Rady 2009/315/WSiSW w odniesieniu do wymiany informacji dotyczących obywateli państw trzecich oraz w odniesieniu do europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS) i zastępująca decyzję Rady 2009/316/WSiSW*.

⁵² *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania*.

- 4) Entry-Exit System (EES) – system wdrożony 10 kwietnia 2026 r. umożliwia rejestrowanie każdorazowego przekroczenia zewnętrznych granic 29 krajów europejskich przez obywateli państw spoza UE przybywających na krótki pobyt do UE⁵³.

ONZ zapoczątkowała swoje działania w zakresie walki z terroryzmem w latach 90. XX w. Wówczas Rada Bezpieczeństwa ogłosiła sankcje dla państw posądzanych o wspieranie i powiązanie z terroryzmem, np. Libii (1992 r.) oraz Sudanu (1996 r.). W 1999 r. Rada przyjęła Rezolucję 1269, w której wyraziła zaniepokojenie (...) *wzrostem liczby aktów międzynarodowego terroryzmu, które zagrażają życiu i dobrobytowi osób na całym świecie, a także pokojowi i bezpieczeństwu wszystkich państw*⁵⁴. Aktualny dokument ONZ dotyczący terroryzmu to *Globalna Strategia Zwalczania Terroryzmu*, która weszła w życie 8 września 2006 r. z załączonym do niej Planem działania⁵⁵.

W ramach ONZ działa Biuro ds. Zwalczania Terroryzmu⁵⁶, którego zadaniem jest pomoc państwom członkowskim we wdrażaniu strategii. Biuro prowadzi łącznie 17 programów i projektów dotyczących różnych zagadnień związanych z terroryzmem, np. terroryzm CBRN czy ofiary terroryzmu. Organizuje wydarzenia i konferencje o tematyce walki z aktami przemocy, np. Tydzień Zwalczania Terroryzmu, który odbywa się co dwa lata⁵⁷.

NATO, która jest organizacją skupioną na aspektach wojskowych i militarnych, ma również programy przeciwdziałania terroryzmowi. NATO jedyny raz powołała się na art. 5 Traktatu Północnoatlantyckiego⁵⁸ dotyczący obrony zbiorowej państw członkowskich, kiedy Stany Zjednoczone doświadczyły ataku terrorystycznego ze strony Al-Kaidy 11 września 2001 r.

⁵³ *Entry-Exit System*, Straż Graniczna, 9 IV 2026 r., <https://www.strazgraniczna.pl/pl/ees/entry-exit-system-pl/13677,System-wjazdwyjazd-EES.html> [dostęp: 12 V 2026].

⁵⁴ *Resolution 1269 (1999) / adopted by the Security Council at its 4053rd meeting, on 19 October 1999, S/RES/1269(1999)*, <https://digitallibrary.un.org/record/287509?v=pdf#files>, s. 1 [dostęp: 10 VI 2026].

⁵⁵ *Globalna Strategia Zwalczania Terroryzmu*, UN Action Counterterrorism, <https://www.unic.un.org/pl/terroryzm/strategia.php> [dostęp: 10 V 2025].

⁵⁶ United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en> [dostęp: 10 V 2025].

⁵⁷ W dniach 26 czerwca – 2 lipca 2026 r. odbyła się kolejna edycja tego wydarzenia. Zob. *2026 Counter-Terrorism Week*, United Nations, <https://www.un.org/counterterrorism/en/2026-counter-terrorism-week> [dostęp: 12 VI 2026].

⁵⁸ *Traktat Północnoatlantycki*, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty?selectedLocale=pl> [dostęp: 12 VI 2026].

Polityka przeciwdziałania terroryzmowi NATO opiera się na trzech zasadach⁵⁹:

- 1) świadomości (ang. *awerness*) – polega na konsultacjach, wymianie informacji wywiadowczych, analizach strategicznych i ocenach sytuacji. W 2023 r. utworzono stanowisko Specjalnego Koordynatora ds. Zwalczania Terroryzmu,
- 2) możliwości i gotowości (ang. *capabilities and preparedness*) – czyli rozwoju zdolności i pracy nad innowacyjnymi technologiami, które będą odpowiedzią na zagrożenia terrorystyczne w każdej postaci,
- 3) zaangażowania i współpracy (ang. *engagement and cooperation*) między państwami członkowskimi i partnerami międzynarodowymi NATO – ma na celu wzmocnienie globalnego bezpieczeństwa, z naciskiem na działania antyterrorystyczne.

NATO organizowała też operacje wojskowe, np. „Active Endeavour” na Morzu Śródziemnym, która była odpowiedzią na atak terrorystyczny z 11 września 2001 r. na World Trade Center⁶⁰, czy „Sea Guardian”, która w 2016 r. zastąpiła „Active Endeavour” i dotyczyła bezpieczeństwa morskigo⁶¹.

NATO współpracuje z ONZ, UE, Global-Counter Terrorism Forum, Interpolem i OBWE, (...) *aby zapewnić wymianę poglądów i informacji oraz skuteczniejsze podejmowanie odpowiednich działań w walce z terroryzmem*⁶². Partnerstwa służą wymianie informacji, koordynacji wspólnych lub osobnych operacji, dostosowywaniu i harmonizowaniu norm prawnych dotyczących bezpieczeństwa.

Podsumowanie

Historia terroryzmu we Francji jest dłuższa niż w Belgii. W XXI w. Al-Ka-ida i Państwo Islamskie wpłynęły na zmianę charakteru współczesnego

⁵⁹ *Countering terrorism*, NATO, 31 III 2026 r., <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism> [dostęp: 12 V 2026].

⁶⁰ *Operation Active Endeavour (2001–2016)*, NATO, <https://www.nato.int/en/what-we-do/operations-and-missions/operation-active-endeavour-2001-2016?selectedLocale=> [dostęp: 10 VI 2026].

⁶¹ *Operation Sea Guardian*, NATO, 26 V 2023 r., https://www.nato.int/cps/en/natohq/topics_136233.htm? [dostęp: 10 V 2025].

⁶² *Countering terrorism...*

terroryzmu, który można określić jak zglobalizowany, bardziej radykalny pod względem religii oraz trudniejszy do przewidzenia.

Autorka skupiła się na analizie ataków na dwie stolice europejskie. Paryż, jako miasto symbolizujące wartości demokratyczne, oraz Bruksela, jako centrum UE, zostały uznane przez terrorystów za najodpowiedniejsze miejsca do przeprowadzenia ataku ze względu na możliwość zademonstrowania negacji poglądów świata zachodniego. Ataki we Francji i Belgii wykazały słabość w systemach bezpieczeństwa, szczególnie w zakresie koordynacji i komunikacji między służbami, oraz skalę problemu związanego z radykalizacją postaw w krajach UE. Społeczno-polityczne konsekwencje tych ataków miały daleko idące skutki. Jednym z nich było wzmocnienie współpracy międzynarodowej w kontekście przeciwdziałania terroryzmowi i walki z tym zjawiskiem. Ponadto państwa europejskie skupiły się na bezpieczeństwie, w tym na potrzebie zaostrzenia prawa antyterrorystycznego, działaniach prewencyjnych oraz koordynacji działań i zwiększeniu uprawnień wyspecjalizowanych służb. Rozpoczęła się też międzynarodowa debata na temat granicy między bezpieczeństwem a wolnością. Z drugiej strony zamachy wywarły wpływ na społeczeństwo związany m.in. z poglądami politycznymi, przyczyniły się do zwiększenia poparcia dla prawicowych partii politycznych w obydwu państwach.

W artykule potwierdzono, że współczesny terroryzm jest silnie powiązany z procesami radykalizacji oraz problemami integracji społecznej. Zarówno Francja, jak i Belgia, ze względu na swoje położenie, historię kolonialną oraz znaczenie polityczne w Europie, stały się szczególnie narażone na działalność ugrupowań islamistycznych powiązanych z Al-Kaidą oraz ISIS. Doświadczenia tych państw pokazują, że skuteczna walka z terroryzmem nie może się opierać wyłącznie na działaniach militarnych i represyjnych, lecz wymaga także długofalowych działań społecznych, edukacyjnych i politycznych mających na celu przeciwdziałanie radykalizacji oraz wzmacnianie spójności społecznej.

Na podstawie przeprowadzonej analizy autorka wskazała główne determinanty polityki bezpieczeństwa Francji i Belgii, którymi zgodnie z hipotezą są:

- 1) organizacje terrorystyczne, takie jak Al-Kaida oraz ISIS, które odrzucają wartości reprezentowane przez stolice europejskie i swoją uwagę kierują na Francję i Belgię także ze względu na ich tradycje kolonialne,

- 2) radykalizacja islamistyczna w społeczeństwach Francji i Belgii,
- 3) ścisła współpraca międzynarodowa jako konieczność do utrzymania bezpieczeństwa narodowego państwa.

Konsekwencje zamachów wymuszają szybkie reakcje polityczne i legislacyjne, a także w zakresie struktury, komunikacji i skuteczności działania służb odpowiedzialnych za bezpieczeństwo.

Przedstawione w artykule ataki terrorystyczne doprowadziły do głębokich zmian dotyczących bezpieczeństwa Francji i Belgii. Ponadto zmobilizowały środowisko międzynarodowe do wspólnego podejmowania działań prewencyjnych w walce z terroryzmem.

Należy podkreślić, że światowy terroryzm dostosowuje się do realiów i ewoluuje zgodnie z wyzwaniem, takimi jak rozwijające się technologie, problemy społeczno-polityczne, migracje itp. Polityka bezpieczeństwa Francji i Belgii (i nie tylko) powinna być elastyczna, integralna i skupiać się wokół wspólnych wartości. Te cechy będą zależeć od podejścia państw do walki z terroryzmem, która polega nie tylko na skuteczności służb antyterrorystycznych, lecz także na współpracy między instytucjami państwowymi, budowaniu zaufania społecznego, mobilizacji instytucji społecznych, edukacyjnych, przeciwdziałaniu radykalizacji oraz budowaniu odporności państw demokratycznych.

Bibliografia

Deschepper R., Six S., Gidron Y., Depoorter A.-M., Vandekerckhove M., Gheysens N., Overmeire R.V., Bilsen J., *Association between feeling threatened by a terrorist attack and subjective health: a web survey a week after the attacks of 22 March 2016 in Belgium*, „European Journal of Psychotraumatology” 2018, t. 9, nr 1. <https://doi.org/10.1080/20008198.2018.1500821>.

Kijewska M., *Lewicowy terroryzm w Europie Zachodniej w drugiej połowie XX i na początku XXI wieku. Podstawowe informacje i kierunki rozwoju*, „Radzyński Rocznik Humanistyczny” 2018 r., t. 16, nr 1.

Pirard P., Baubet T., Motreff Y., Rabet G., Marillier M., Vandentorren S., Vuillermoz C., Stene L.E., Messiah A., *Use of mental health supports by civilians exposed to the November 2015 terrorist attacks in Paris*, „BMC Health Services Research” 2020, t. 20. <https://doi.org/10.1186/s12913-020-05785-3>.

Romania V., Tozzo S., *Terrorism as ritual process and cultural trauma: A performative analysis of ISIS's attacks in Europe*, „Italian Sociological Review” 2017, t. 7, nr 2, s. 239–261. <https://doi.org/10.13136/isr.v7i2.177>.

Źródła internetowe

2026 Counter-Terrorism Week, United Nations, <https://www.un.org/counterterrorism/en/2026-counter-terrorism-week> [dostęp: 12 VI 2026].

27 lat temu doszło do zamachu bombowego w paryskim metrze, iFrancja, 25 VII 2025 r., <https://www.ifrancja.fr/27-lat-temu-doszlo-do-zamachu-bombowego-w-paryskim-metrze/> [dostęp: 23 I 2025].

Belgique – attentats à l’aéroport et dans le métro de Bruxelles, Association française des Victimes du Terrorisme, <https://www.afvt.org/belgique-attentats-a-laeroport-et-dans-le-metro-de-bruxelles/> [dostęp: 10 IV 2025].

Chrisafis A., *Marine Le Pen’s Front National makes political gains after Paris attacks*, The Guardian, 1 XII 2015 r., <https://www.theguardian.com/world/2015/dec/01/marine-le-pen-front-national-political-gains-paris-attacks> [dostęp: 12 VI 2026].

Countering terrorism, NATO, 31 III 2026 r., <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism> [dostęp: 12 V 2026].

Dispositif territorial de prévention de la radicalisation violente, Direction Générale de la Sécurité Intérieure, 14 VI 2021 r., <https://www.dgsi.interieur.gouv.fr/dispositif-territorial-de-prevention-de-radicalisation-violente> [dostęp: 11 VI 2026].

Entry-Exit System, Straż Graniczna, 9 IV 2026 r., <https://www.strazgraniczna.pl/pl/ees/entry-exit-system-pl/13677,System-wjazduwyjazdu-EES.html> [dostęp: 12 V 2026].

EU Terrorism Situation & Trend Report (EU TE-SAT), Europol, <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> [dostęp: 11 VI 2026].

EUROJUST, *The ARGO Case, Diplomatic immunity in a cross-border terrorism case*, <https://www.eurojust.europa.eu/sites/default/files/assets/argo-case-28-06-2024-pdf-v2.pdf> [dostęp: 10 V 2025].

European Counter Terrorism Centre – ECTC, Europol, <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> [dostęp: 10 V 2025].

France, *Belgium to step up counter-terrorism cooperation in wake of Paris attacks*, France 24, 2 II 2016 r., <https://www.france24.com/en/20160202-france-belgium-step-counter-terrorism-cooperation-paris-attacks> [dostęp: 10 V 2025].

Francq B., *Les Cellules communistes combattantes: les deux figures d'une inversion*, „Sociologie du Travail” 1986, t. 28, nr 4, https://www.jstor.org/stable/43149431?casa_token=uvu0DUMHhm8AAAAA%3AyTH0OxhPSaWldOexG8URrz6nNtuZbU-TI7TZ9D-cgAn0hvmw0Z43g9lBtlOxUD2Fd2EggWffEMzdOeaYrtRtkSWMZS4nP0a-o3SNdYXUPwB9a-zDSQ&seq=1 [dostęp: 24 I 2025].

Garat J-B., *L'impressionnante liste des politiques présents à la marche à Paris*, Le Figaro, 10 I 2015 r., <https://www.lefigaro.fr/politique/2015/01/10/01002-20150110ARTFIG-00160-l-impressionnante-liste-des-politiques-presents-a-la-marche-republicaine-a-paris.php> [dostęp: 9 IV 2025].

Globalna Strategia Zwalczania Terroryzmu, UN Action Counterterrorism, <https://www.unic.un.org.pl/terroryzm/strategia.php> [dostęp: 10 V 2025].

Gracieux Ch., *Les attentats du 22 mars 2016 à Bruxelles*, Lumni Enseignement, 23 III 2016 r., <https://enseignants.lumni.fr/fiche-media/00000001857/les-attentats-du-22-mars-2016-a-bruxelles.html> [dostęp: 11 IV 2025].

Hallam M., *Belgian shortcomings in focus*, DW, 30 III 2016 r., <https://www.dw.com/en/the-shortcomings-of-belgiums-brussels-terror-investigations/a-19151338> [dostęp: 12 VI 2026].

Jastrzębski B., *Jastrzębski: Zamachy w Brukseli – to nie koniec świata*, Respublica, 22 III 2016 r., <https://respublica.pl/teksty/jastrzebski-zamachy-w-brukseli-to-nie-koniec-swiata-56188.html> [dostęp: 12 IV 2025].

Kacprzak A., *Komisja śledcza francuskiego parlamentu: Wywiad poniósł porażkę, nie zapobiegł atakom. Należy utworzyć agencję do walki z terroryzmem*, wPolityce, 5 VII 2016 r., <https://wpolityce.pl/swiat/299492-komisja-sledcza-francuskiego-parlamentu-wywiad-poniosl-porazke-nie-zapobiegl-atak-om-nalezy-utworzyc-agencje-do-walki-z-terroryzmem?strona=1> [dostęp: 12 IV 2025].

Kerherve A., *O.A.S.*, Gaullisme.fr, 30 VII 2011 r., <http://www.gaullisme.fr/2011/07/30/o-a-s/> [dostęp: 11 VI 2026].

Koledzy z Al-Kaidy skazani w Belgii, TVN24, 10 V 2010 r., <https://tvn24.pl/swiat/koledzy-z-al-kaidy-skazani-w-belgii-ra133541-ls3584645> [dostęp: 25 I 2025].

La Stratégie Extrémisme et Terrorisme (Stratégie T.E.R.), OCAM, <https://ocam.belgium.be/la-strategie-extremisme-et-terrorisme-strategie-t-e-r/> [dostęp: 12 IV 2025].

Lafon C., *Attentats de Paris: ces deux semaines qui ont changé la France*, Sud Ouest, 22 I 2015 r., <https://www.sudouest.fr/redaction/attentats-de-paris-ces-deux-semaines-qui-ont-change-la-france-8022926.php> [dostęp: 12 IV 2025].

Le Plan R. Le Plan d'Action Radicalisme, https://ocam.belgium.be/wp-content/uploads/2020/11/brochure_radicalisme_fr.pdf [dostęp: 12 VI 2026].

Macuga Ł., *Wojna algierska, 1954–1962*, praca magisterska, Uniwersytet Mikołaja Kopernika, Toruń 2004, https://www.researchgate.net/publication/303636471_Wojna_algierska_1954_-_1962 [dostęp: 22 II 2025].

Motto UE, Unia Europejska, 23 XII 2025 r., https://european-union.europa.eu/principles-countries-history/symbols/eu-motto_pl [dostęp: 18 III 2026].

„Mózg” krwawych zamachów w Paryżu zatrzymany, *Newsweek Polska*, 18 III 2016 r., <https://web.archive.org/web/20160322133717/http://swiat.newsweek.pl/sprawca-krwawych-zamachow-w-paryzu-salah-abdeslam-zatrzymany,artykuly,382261,1.html> [dostęp: 10 IV 2025].

Nadaux M., *La Troisième République. La «propagande par le fait»: les attentats anarchistes (1892–1894). Explosion d’une bombe à la Chambre des députés déposée par l’anarchiste Auguste Vaillant le 9 décembre 1893*, *Le XIX^e siècle*, <https://web.archive.org/web/20061125095024/http://www.19e.org/documents/troisiemerepublique/anarattentats/vaillant.htm> [dostęp: 21 I 2025].

Najpierw zabijali w redakcji, potem zastrzelili policjanta. Tak przebiegał zamach, *TVN24*, 8 I 2015 r., <https://tvn24.pl/swiat/zamach-na-charlie-hebdo-tak-przebiegal-atak-ra504096-ls3289349> [dostęp: 8 IV 2025].

National Liberation Front, *Britannica*, <https://www.britannica.com/topic/National-Liberation-Front-political-party-Algeria> [dostęp: 22 I 2025].

Nos missions, *Direction Générale de la Sécurité Extérieure*, <https://www.dgse.gouv.fr/fr/nous-connaître/nos-missions> [dostęp: 30 IV 2025].

Nos missions, *SGRS*, <https://www.sgrs.be/nous-connaître/nos-missions/> [dostęp: 1 VI 2025].

Operation Active Endeavour (2001–2016), *NATO*, <https://www.nato.int/en/what-we-do/operations-and-missions/operation-active-endeavour-2001-2016?selectedLocale=> [dostęp: 12 VI 2026].

Opération CHAMMAL, *Ministère des Armées*, <https://www.defense.gouv.fr/operations/proche-moyen-orient/operations-militaires-au-proche-moyen-orient/operation-chammal> [dostęp: 10 IV 2025].

Operation Sea Guardian, *NATO*, 26 V 2023 r., https://www.nato.int/cps/en/natohq/topics_136233.htm? [dostęp: 10 V 2025].

«Prévenir Pour Protéger». *Plan national de prévention de la radicalisation*, <https://www.cipdr.gouv.fr/wp-content/uploads/2018/11/DP2018-02-23-CIPDR-Radicalisation-V5.pdf> [dostęp: 11 VI 2026].

Qui sommes-nous?, Veiligheid van de Staat, <https://www.vsse.be/fr/qui-sommes-nous/historique> [dostęp: 1 V 2025].

Stańko K., *Największy proces karny w historii Francji. Dziś wyrok w sprawie ataków terrorystycznych z 2015 roku*, Polska Agencja Prasowa, 29 VI 2022 r., <https://www.pap.pl/aktualnosci/news%2C1270741%2Cfrancja-byl-najwiekszy-proces-karny-w-historii-dzis-wyrok-w-sprawie-atakow#:~:text=13%20listopada%202015> [dostęp: 10 VI 2026].

Strategia UE w zakresie unii bezpieczeństwa: wszystkie elementy układanki we właściwym miejscu – nowy ekosystem bezpieczeństwa, Komisja Europejska – Komunikat prasowy, Bruksela, 24 VII 2020 r., https://ec.europa.eu/commission/presscorner/api/files/document/print/pl/ip_20_1379/IP_20_1379_PL.pdf [dostęp: 12 VI 2026].

Stratégie nationale de prévention de la délinquance 2026–2030: Prévenir pour protéger, CIPDR, 24 IV 2026 r., <https://www.cipdr.gouv.fr/strategie-nationale-de-prevention-de-la-delinquance-2026-2030-prevenir-pour-proteger/> [dostęp: 12 V 2026].

System Informacyjny Schengen, Komisja Europejska, https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_pl [dostęp: 10 V 2025].

Tactics, Techniques, and Procedures Used in the 22 March 2016 Brussels Attacks, „Joint Intelligence Bulletin”, 12 IV 2016 r., <https://info.publicintelligence.net/DHS-FBI-NCTC-BrusselsAttacks.pdf> [dostęp: 11 IV 2025].

Terroryzm w UE: fakty i liczby, Rada Europejska i Rada Unii Europejskiej, <https://www.consilium.europa.eu/pl/infographics/terrorism-eu-facts-figures/> [dostęp: 25 I 2025].

The Plan Vigipirate, Republique Francaise, <https://www.campusfrance.org/en/security> [dostęp: 26 V 2026].

The Prevention Pyramid, European Commission, 2 VII 2024 r., https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/prevention-pyramid_en [dostęp: 4 V 2025].

United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en> [dostęp: 10 V 2025].

Zwalczanie terroryzmu i radykalizacji postaw, Komisja Europejska, 26 II 2026 r., https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation_en?prefLang=pl&etrans=pl [dostęp: 30 III 2026].

Akty prawne

Resolution 1269 (1999) / adopted by the Security Council at its 4053rd meeting, on 19 October 1999, S/RES/1269(1999), <https://digitallibrary.un.org/record/287509?v=pdf#files> [dostęp: 11 VI 2026].

Traktat Północnoatlantycki, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty?selectedLocale=pl> [dostęp: 12 VI 2026].

Decyzja Rady 2009/316/WSiSW z dnia 6 kwietnia 2009 r. w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW (Dz. Urz. UE L 93/33 z 7 IV 2009 r.).

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

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/884 z dnia 17 kwietnia 2019 r. zmieniająca decyzję ramową Rady 2009/315/WSiSW w odniesieniu do wymiany informacji dotyczących obywateli państw trzecich oraz w odniesieniu do europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS) i zastępująca decyzję Rady 2009/316/WSiSW (Dz. Urz. UE L 151/143 z 7 VI 2019 r.).

LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035932811> [dostęp: 13 VI 2026].

Nicole Szostak

Absolwentka Akademii Sztuki Wojennej na kierunku bezpieczeństwo międzynarodowe i dyplomacja oraz Sciences Po Rennes na kierunku nauki polityczne. Główne zainteresowania badawcze: działania antyterrorystyczne, wywiad i kontrwywiad oraz analiza geopolityczna.

Kontakt: nicoleszostak1@gmail.com

ARTYKUŁY RECENZYJNE /
RECENZJE

**Tomasz Wróblewski,
Rola sztucznej inteligencji
w zapobieganiu atakom terrorystycznym¹**

Tomasz Michalak

Instytut Badawczy IDEAS
Wydział Matematyki, Informatyki i Mechaniki,
Uniwersytet Warszawski

 <https://orcid.org/0000-0002-5288-0324>



W trzeciej dekadzie XXI w. procesy rozwojowe w obszarze sztucznej inteligencji (ang. *artificial intelligence*, AI) uległy bezprecedensowej akceleracji, co jest określane mianem rewolucji AI. W kontekście gospodarczym ta technologia stanowi fundament czwartej rewolucji przemysłowej w związku z optymalizacją procesów wytwórczych. Niemniej potencjalny wpływ AI na społeczeństwa jest wielowymiarowy i wykracza daleko poza sferę czysto przemysłową. Obejmuje on zarówno fundamentalne zmiany w sposobie, w jaki wchodzimy w interakcje z informacją oraz sobą nawzajem,

¹ T. Wróblewski, *Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym*, Warszawa 2025, Difin, 178 s.

jak i głęboką transformację rynku pracy, na którym automatyzacja rutynowych zadań wymusza redefinicję ludzkich kompetencji. Wszystko to powoduje, że AI wiąże się nie tylko z korzyściami, lecz także wieloma wyzwaniami. Na przykład implementacja systemów inteligentnych w medycynie, edukacji czy administracji publicznej daje szansę na znaczne zwiększenie efektywności i personalizacji usług, ale jednocześnie generuje krytyczne pytania o prywatność, etykę algorytmiczną oraz odpowiedzialność za decyzje autonomicznie podejmowane przez systemy komputerowe.

Wielowymiarowość wpływu AI na rzeczywistość znajduje odbicie w dziedzinie bezpieczeństwa państwa, jesteśmy bowiem świadkami rewolucji w wojskowości. Trwająca wojna w Ukrainie stała się siłą napędową i poligonem doświadczalnym dla wojny algorytmicznej, w której o przewadze decydują zarówno zasoby ludzkie oraz ciężki sprzęt, jak i zdolność do błyskawicznej fuzji i analizy danych z dronów, satelitów wojskowych oraz innych dostępnych źródeł, w tym otwartych. Analiza masowych zbiorów informacji jest jednym z najważniejszych zastosowań algorytmów AI, które mogą dokonać zaawansowanego wnioskowania oraz rozpoznania korelacji i powiązań o tak wysokim stopniu złożoności, że są one w praktyce niemożliwe do identyfikacji przez człowieka. Na polu walki skracanie pętli decyzyjnej niemal do czasu rzeczywistego sprawia, że AI staje się kluczowym multiplikatorem siły. Co więcej, należy podkreślić, że rozwój AI nie tylko dotyczy sfery oprogramowania, lecz także jest głównym katalizatorem rozwoju autonomii w systemach uzbrojenia i robotyki. Wszystkie te trendy definiują pole walki w Ukrainie, można zatem stwierdzić, że AI odgrywa bardzo istotną rolę w trwających procesach przebudowy globalnej architektury geopolitycznej.

Postęp technologiczny oparty na AI nie dotyczy tylko sfery wojskowości. Ma także wpływ na bezpieczeństwo wewnętrzne: od przeciwdziałania przestępczości, po działania kontrwywiadowcze, walkę z terroryzmem czy z zagrożeniami hybrydowymi. W tych wszystkich obszarach stosuje się algorytmy AI dotyczące fuzji i analizy masowych zbiorów danych oraz ekstrakcję wiedzy z szumu informacyjnego i wnioskowanie na tej podstawie. Również rozwój systemów autonomicznych i robotyki jest niezwykle istotny w kontekście bezpieczeństwa wewnętrznego, gdyż te technologie są w stanie zwielokrotnić możliwości służb bezpieczeństwa. Oczywiście należy zwrócić uwagę na drugą stronę medalu – technologie AI i powiązane z rozwojem AI mogą być niezwykle groźne w rękach terrorystów.

Potencjałowi sztucznej inteligencji w walce z terroryzmem została poświęcona publikacja Tomasza Wróblewskiego pt. *Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym*, która ukazała się w 2025 r. nakładem wydawnictwa Difin i liczy 178 stron. Przed przystąpieniem do analizy merytorycznej tej pozycji należy zarysować sylwetkę autora, aby uniknąć pomyłek, częstych w przestrzeni publicznej. Autora recenzowanej publikacji dr. Tomasza Wróblewskiego, badacza i akademika o ugruntowanych kompetencjach w obszarze obronności i bezpieczeństwa wewnętrznego, nie należy mylić z dziennikarzem i publicystą o tym samym imieniu i nazwisku. Absolwent Akademii Obrony Narodowej (obecnie Akademia Sztuki Wojennej), zajmował kierownicze stanowiska w Siłach Zbrojnych RP oraz przez wiele lat pełnił służbę w Centralnym Biurze Śledczym Policji.

Recenzowana książka została podzielona na wstęp oraz cztery rozdziały. Rozdział pierwszy, zatytułowany *Podstawy terroryzmu i technologii AI*, ma charakter wprowadzający i kontekstualny. Autor definiuje w nim terroryzm i przedstawia podstawowe trendy w ewolucji tego zjawiska oraz opisuje cele i metody współczesnych grup ekstremistycznych. Definiuje najważniejsze pojęcia z zakresu AI, ze szczególnym uwzględnieniem technologii głębokiego uczenia (ang. *deep learning*) oraz uczenia maszynowego (ang. *machine learning*).

Rozdział drugi – *Badania nad wykorzystaniem AI w zapobieganiu terroryzmowi* – autor rozpoczyna od zarysowania za pomocą kilku przykładów niektórych kierunków badań nad wykorzystaniem AI do zwalczania terroryzmu. W następnym podrozdziale są krótko opisane wybrane ośrodki i organizacje badające AI w kontekście bezpieczeństwa, przy czym Wróblewski koncentruje się bardziej na badaniu bezpieczeństwa AI niż wykorzystaniu tej technologii w przeciwdziałaniu terroryzmowi. Ciekawy jest kolejny podrozdział, który zawiera porównanie tradycyjnych metod zwalczania terroryzmu z nowoczesnymi rozwiązaniami bazującymi na AI. Znajdujemy tutaj szerokie spojrzenie na nowe możliwości, jakie AI daje służbom bezpieczeństwa, oraz na zagrożenia niesione przez tę technologię. W tym świetle poprzednie dwa podrozdziały pozostawiają pewien niedosyt, ponieważ wbrew tytułowi całego rozdziału koncentrują się jedynie na kilku aspektach tego wielowymiarowego zagadnienia. Dopełnieniem rozdziału są analiza i omówienie wyników badania opinii ekspertów na temat skuteczności narzędzi AI w zwalczaniu terroryzmu. Badania ankietowe, do których odwołał się autor, zostały przeprowadzone w 2022 r. w ramach czasopisma Agencji Bezpieczeństwa Wewnętrznego „Terroryzm – studia,

analizy, prewencja”. W ankiecie wzięło udział 94 ekspertów, przeważnie z administracji państwowej i ośrodków akademickich. Zarówno wyniki badania, jak i dyskusję oceniam jako wartościowe, gdyż pokazują żywe i głębokie zainteresowanie wyzwaniami, jakie niesie gwałtowny rozwój AI, ze strony środowiska eksperckiego zajmującego się bezpieczeństwem wewnętrznym w Polsce.

Trzeci rozdział – *Identyfikacja zagrożeń przy użyciu AI* – jest najobszerniejszy i moim zdaniem najciekawszy, gdyż omawia zdecydowanie najwięcej aspektów i przykładów zastosowania do zwalczania terroryzmu technologii opartych na AI. Pierwszy podrozdział dotyczy przetwarzania i analizy danych. W drugim podrozdziale zostało omówione wykorzystanie technik przetwarzania języka naturalnego do analizy komunikacji między terrorystami. W rzeczywistości znajdujemy tam dużo więcej, gdyż znaczna część tekstu traktuje o zagrożeniach stwarzanych przez rozwój dużych modeli językowych (ang. *large language models*, LLM), które mogą zostać wykorzystane przez terrorystów na różne sposoby. Analizę tę uważam za bardzo potrzebną i celną. Kolejny podrozdział koncentruje się na podstawowych zagadnieniach związanych z monitoringiem sieci społecznościowych przy wykorzystaniu technologii AI. Autor bardziej szczegółowo omawia w nim konstrukcje modeli predykcyjnych, które mogą być użyte do identyfikacji zamiarów grup terrorystycznych na wstępnym etapie. Podrozdział 3.4 opisuje kwestie użycia rozwiązań AI do analizy danych finansowych w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Wróblewski podkreśla przewagę algorytmów nad możliwościami człowieka w konfrontacji z ogromem danych i złożonością wzorców działań przestępczych, jakie można wyłonić z tych danych. W następnym podrozdziale autor wprowadził zagadnienia związane z systemami rozpoznawania obrazów, w szczególności twarzy. Przytacza ciekawy przykład wykorzystania tych technologii do ujęcia w 2024 r. w Berlinie niemieckiej terrorystki z Frakcji Czerwonej Armii. Zaskakujący jest ostatni podrozdział, ponieważ dotyczy wykorzystania AI do wsparcia działań w sytuacjach kryzysowych, które mogą być efektem działań terrorystycznych. Same badania nad wykorzystaniem AI w sytuacjach kryzysowych są niezwykle istotne, a zwrócenie uwagi na to zagadnienie również pod kątem terroryzmu uważam za bardzo potrzebne.

W rozdziale czwartym autor koncentruje się na etycznych i społecznych konsekwencjach stosowania AI w kontekście bezpieczeństwa. Analizuje również dopiero powstający system regulacji prawnych na poziomie krajowym i międzynarodowym.

Należy podkreślić, że Tomasz Wróblewski podjął się wyjątkowo trudnego tematu. Sztuczna inteligencja to bowiem technologia o niemal bezprecedensowej dynamice rozwoju, która przenika wiele sfer życia jednostek i społeczeństw. W takiej sytuacji próba syntetycznego ujęcia nawet części dostępnych możliwości czy kierunków rozwoju AI z perspektywy działań antyterrorystycznych jest ogromnym wyzwaniem. Okazuje się ono jeszcze większe, gdy weźmiemy pod uwagę samą naturę terroryzmu – zjawiska niezwykle skomplikowanego, wielowymiarowego i podlegającego ciągłym przeobrażeniom. Każda próba połączenia obu tych złożoności i naukowo usystematyzowania tego obszaru badań jest godna pochwały. Niezwykle cenna w tym kontekście okazała się interdyscyplinarność zainteresowań naukowych autora.

Zaletą publikacji jest jej język. Wróblewski unika nadmiaru terminologii technicznej, co czyni tekst przystępnym dla osób niebędących informatykami. Uważam jednak, że pozycja jest bardzo wartościowa również dla tej grupy, gdyż pozwala uzmysłwić sobie złożoność zagadnień związanych zarówno z istnieniem technologii jako takiej, jak i jej wykorzystaniem w społeczeństwie. Inny atut książki to dwutorowe podejście do analizy roli AI w obszarze bezpieczeństwa. Z jednej strony autor omawia wykorzystanie tej technologii przez służby państwowe, z drugiej analizuje sposoby, w jakie te same technologie mogą zostać zaadaptowane przez grupy terrorystyczne do planowania zamachów, prowadzenia dezinformacji czy działań w cyberprzestrzeni. Przedstawienie AI jako narzędzia dostępnego dla obu stron konfliktu jest istotne, ponieważ pozwala czytelnikowi na lepszą ocenę ciągle zmieniających się zagrożeń.

Podsumowując, praca Tomasza Wróblewskiego to ważna pozycja dotycząca kwintesencji współczesnych zagrożeń związanych z terroryzmem, które na naszych oczach przybierają nowe formy. Autorowi udało się stworzyć ciekawą i wartościową kompilację wiedzy, będącą dobrym punktem wyjścia do głębszej analizy poszczególnych zagadnień.

Lider zespołu AI StrategyLab w Instytucie Badawczym IDEAS podlegającym Ministerstwu Cyfryzacji i Ministerstwu Obrony Narodowej oraz wykładowca na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Wcześniej lider samodzielnego zespołu badawczego „AI dla bezpieczeństwa” w IDEAS NCBR. Absolwent Uniwersytetu Warszawskiego. Stopień doktorski otrzymał na Uniwersytecie w Antwerpii, a habilitację na Akademii Górniczo-Hutniczej. W czasie kariery naukowej prowadził badania na Wydziale Informatyki Uniwersytetu Oksfordzkiego, w Szkole Inżynierii i Informatyki Uniwersytetu w Southampton oraz na Wydziale Informatyki Uniwersytetu w Liverpoolu. W latach 2024–2025 pełnił funkcję współdyrektora w projekcie „R-GRID: AI algorithms for Threat Prediction and Power Grid Protection” z grantem NATO oraz eksperta w projekcie europejskim EU-CIP dotyczącym ochrony infrastruktury krytycznej w Unii Europejskiej.

Kontakt: tomasz.michalak@ideas.edu.pl

Sprawozdanie z raportu „Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności”

Aleksandra Komar

Autorka niezależna

 <https://orcid.org/0000-0002-9717-5258>

Raport Agencji Bezpieczeństwa Wewnętrznego za lata 2024–2025¹ przedstawia najważniejsze działania podejmowane przez służbę w zakresie ochrony bezpieczeństwa wewnętrznego Rzeczypospolitej Polskiej. Opisuje aktywność ABW w obszarach kontrwywiadu, zwalczania terroryzmu, ochrony strategicznych interesów gospodarczych państwa, cyberbezpieczeństwa oraz ochrony informacji niejawnych. Podkreśla, że współczesne zagrożenia są wielowymiarowe i obejmują zarówno klasyczne działania wywiadowcze, jak i operacje hybrydowe, cyberataki, dezinformację czy inne próby destabilizacji życia społecznego i gospodarczego.

¹ Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności. Raport jest dostępny na stronie: <https://www.abw.gov.pl/pl/aktualnosci/2815,Agencja-Bezpieczenstwa-Wewnetrznego-2024-2025-Wybrane-aktywnosci.html>.

Najważniejsze kierunki działań ABW

Priorytetowymi zadaniami Agencji są ochrona stabilności państwa i porządku konstytucyjnego oraz ochrona bezpieczeństwa obywateli. W latach 2024–2025 mieliśmy do czynienia z rosnącą skalą zagrożeń ze strony służb Federacji Rosyjskiej, Republiki Białorusi oraz Chińskiej Republiki Ludowej.

Raport wskazuje, że Rosja prowadziła intensywne działania wywiadowcze i dywersyjne wymierzone w Polskę oraz państwa NATO i UE. Te działania miały na celu podważanie zaufania do instytucji państwowych, szerzenie dezinformacji, wzmacnianie nastrojów antyeuropejskich oraz destabilizację sytuacji społeczno-politycznej. Szczególnym zagrożeniem były próby przeprowadzenia aktów sabotażu wobec infrastruktury krytycznej, obiektów wojskowych oraz miejsc związanych z organizacją wsparcia dla Ukrainy.

Białoruś prowadziła głównie działania wymierzone w środowiska opozycyjne w Polsce oraz mające na celu rozpoznanie infrastruktury wojskowej i krytycznej. W raporcie podkreślono ścisłą współpracę białoruskich i rosyjskich służb specjalnych.

Istotnym wyzwaniem pozostaje również aktywność Chin. Chińskie służby wywiadowcze wykorzystują powiązania gospodarcze, naukowe i medialne do budowania wpływów politycznych i ekonomicznych. Ich szczególne zainteresowanie budzą polscy eksperci, naukowcy i urzędnicy mający dostęp do informacji strategicznych.

Raport – statystyki dotyczące działań ABW

Raport przedstawia dane liczbowe obrazujące skalę zagrożeń oraz efektywność działań ABW m.in. w takich obszarach jak kontrwywiad, ochrona strategicznych interesów gospodarczych Polski oraz zwalczanie terroryzmu.

Kontrwywiad

W tabeli 1 podano wskaźniki w obszarze działań kontrwywiadowczych.

Tabela 1. Wskaźniki w obszarze działań kontrwywiadowczych.

Wskaźnik	Wartość
Prowadzone postępowania dotyczące szpiegostwa	ponad 60 (w tym 48 wszczętych w 2025 r.)
Osoby objęte statusem podejrzanego od początku pełnoskalowej agresji Rosji na Ukrainę	91
Osoby, którym postawiono zarzuty szpiegostwa	82
Osoby zatrzymane za działanie na rzecz obcych służb	62
Analizy i informacje przygotowane dla najwyższych władz państwowych	ponad 430

Źródło: opracowanie własne na podstawie: *Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności.*

W raporcie podkreślono, że w latach 2024–2025 wszczęto 69 śledztw dotyczących działalności wywiadowczej, czyli tyle samo, ile łącznie w latach 1991–2023. Pokazuje to bezprecedensowy wzrost zagrożenia bezpieczeństwa państwa.

Ochrona strategicznych interesów gospodarczych Polski

W obszarze ochrony strategicznych interesów gospodarczych Polski działania ABW obejmowały:

- ochronę inwestycji energetycznych, w tym budowy pierwszej polskiej elektrowni jądrowej,
- monitorowanie projektów infrastrukturalnych oraz inwestycji realizowanych przez spółki Skarbu Państwa,
- przeciwdziałanie nadużyciom finansowym i korupcji,
- analizę zagrożeń związanych z kryptowalutami wykorzystywanymi do finansowania działalności przestępczej i terrorystycznej.

Istotnym elementem działalności była również osłona antykorupcyjna. Pod koniec 2024 r. ochroną objęto 23 strategiczne przedsięwzięcia, rok później ta liczba wzrosła do 36.

Terroryzm – studia, analizy, prewencja
2026, nr 9: 239–245

Zwalczanie terroryzmu

Bardzo ważnym obszarem działalności ABW jest przeciwdziałanie terroryzmowi. Raport wskazuje, że poziom zagrożenia terrorystycznego w Polsce pozostaje niższy niż w wielu państwach Europy Zachodniej, jednak nie oznacza to braku realnych niebezpieczeństw.

Największą uwagę zwrócono w raporcie na terroryzm islamski. Funkcjonariusze ABW identyfikowali przypadki radykalizacji zarówno wśród obywateli polskich, jak i cudzoziemców przebywających na terenie kraju. Szczególne zagrożenie stanowi nielegalna migracja przez granicę polsko-białoruską, która umożliwia przedostawanie się osób pochodzących z państw wysokiego ryzyka terrorystycznego.

W raporcie podkreślono także niepokojące zjawisko radykalizacji młodzieży i młodych dorosłych. Coraz częściej młodzi interesują się propagandą organizacji terrorystycznych, np. tzw. Państwa Islamskiego (Islamic State of Iraq and Syria, ISIS). Odbywa się to głównie za pośrednictwem internetu, w tym mediów społecznościowych oraz komunikatorów internetowych. W skrajnych przypadkach może prowadzić to do przygotowań zamachów terrorystycznych.

Dzięki działaniom prowadzonym przez ABW zatrzymano np.:

- 17-letniego mieszkańca województwa podkarpackiego przygotowującego zamach inspirowany ideologią ISIS,
- trzech 19-letnich mieszkańców Olsztyna planujących przeprowadzenie ataku terrorystycznego,
- 19-letniego obywatela Polski podejrzanego o przygotowywanie zamachu na terenie naszego kraju,
- obywatela Tadżykistanu będącego członkiem ISIS, który został deportowany z Polski.

W opracowaniu zaznaczono niezwykle istotną w działaniach antyterrorystycznych rolę całodobowej wymiany informacji pomiędzy służbami odpowiedzialnymi za bezpieczeństwo państwa. W ramach ABW odpowiada za to Centrum Antyterrorystyczne.

W tabeli 2 przedstawiono najważniejsze dane statystyczne dotyczące zwalczania terroryzmu.

Tabela 2. Wskaźniki w obszarze zwalczania terroryzmu.

Wskaźnik	Wartość
Prowadzone postępowania karne dotyczące terroryzmu	19 (w tym 7 wszczętych w 2025 r.)
Analizy dotyczące zagrożeń terrorystycznych	178
Raporty operacyjne dot. potencjalnych zagrożeń	blisko 700
Opinie związane z procedurami koncesyjnymi dotyczącymi broni, materiałów wybuchowych i technologii strategicznych	ponad 880
Liczba wniosków dot. wydania zezwoleń na międzynarodowy obrót towarami i technologiami strategicznymi	ok. 5500

Źródło: opracowanie własne na podstawie: *Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności.*

Szczególne znaczenie w zwalczaniu zagrożeń terrorystycznych mają działania profilaktyczne, monitorowanie procesów radykalizacji oraz szybka wymiana informacji między służbami krajowymi i zagranicznymi.

Komentarz do raportu

Szef ABW płk Rafał Syrysko udzielił wywiadu, w którym omówił raport ABW za lata 2024–2025². Zwrócił uwagę, że działalność rosyjskich służb specjalnych wobec Polski wyraźnie się zmieniła. Obecnie nie ogranicza się do klasycznego pozyskiwania informacji wywiadowczych, lecz coraz częściej obejmuje działania o charakterze dywersyjnym i sabotażowym, które mogą prowadzić do zniszczeń infrastruktury oraz zagrażać życiu ludzi. Według Szefa ABW Rosja „przesuwa granice” swoich operacji, a służby obserwują rosnącą skłonność przeciwnika do działań kinetycznych.

Szczególnie niepokojącym zjawiskiem jest wykorzystywanie przez rosyjskie służby osób ze środowisk przestępczych. Płk Rafał Syrysko uważa, że osoby z doświadczeniami kryminalnymi łatwiej zaangażować

² Zob. szerzej: Płk Rafał Syrysko, szef ABW o nowej taktyce rosyjskich służb w Polsce i największych ryzykach, Rzeczpospolita, 6 V 2026 r., <https://www.rp.pl/sluzby/art44311581-plk-rafal-syrysko-szef-abw-o-nowej-taktyce-rosyjskich-sluzb-w-polsce-i-najwiekszych-ryzykach> [dostęp: 14 VI 2026].

w działania dywersyjne, ponieważ potrafią ukrywać swoją aktywność i funkcjonować poza prawem. Oznacza to zacieranie granicy pomiędzy działalnością wywiadowczą a przestępczością zorganizowaną.

W wywiadzie Szef ABW omówił również zawarte w raporcie tezy dotyczące szczególnej roli Białorusi w działaniach przeciwko Polsce. Określił Białoruś jako najważniejsze państwowe zaplecze Rosji w regionie. Białoruskie służby uczestniczą w operacjach wpływu, działaniach migracyjnych, prowokacjach granicznych oraz wspierają rosyjskie przedsięwzięcia wymierzone w bezpieczeństwo Polski i państw NATO.

W rozmowie poruszono także problem aktywności chińskiego wywiadu. Według Szefa ABW działania Chin mają charakter długofalowy i koncentrują się na budowaniu wpływów gospodarczych, politycznych oraz społecznych. Chińskie służby wykorzystują relacje ekonomiczne i środowiska eksperckie do tworzenia zaplecza wpływu, a także prowadzą działania informacyjne mające poprawiać wizerunek chińskiego modelu państwa.

Rozmowa dotyczyła również zagrożeń terrorystycznych. Płk Rafał Syrysko ocenia, że zagrożenie terroryzmem islamskim w Polsce pozostaje stosunkowo niskie. ABW stale monitoruje przypadki radykalizacji zarówno wśród cudzoziemców, jak i polskich obywateli. Szczególne znaczenie ma współpraca międzynarodowa i szybka wymiana informacji między służbami, co umożliwi identyfikację osób mogących stanowić zagrożenie.

Szef ABW podkreśla, że terroryści coraz częściej wykorzystują internet, komunikatory i media społecznościowe do rekrutacji oraz radykalizacji młodych ludzi. Z tego względu działania prewencyjne służb specjalnych i monitorowanie przestrzeni cyfrowej stają się równie ważne jak tradycyjne działania operacyjne.

Podsumowanie

Raport ABW oraz wywiad z Szefem ABW pokazują, że Polska znajduje się obecnie w środowisku bezpieczeństwa charakteryzującym się wysoką dynamiką zagrożeń. Oprócz klasycznego szpiegostwa coraz większe znaczenie mają działania hybrydowe, sabotaż, dezinformacja, cyberataki oraz radykalizacja młodzieży. Szczególnym wyzwaniem pozostają operacje prowadzone przez Rosję i wspierającą ją Białoruś.

Dane przedstawione w raporcie wskazują na wysoką aktywność i skuteczność ABW w wykrywaniu oraz neutralizowaniu zagrożeń bezpieczeństwa państwa. Bezpieczeństwo Polski znajduje się obecnie pod silną

presją wynikającą z sytuacji międzynarodowej, szczególnie wojny w Ukrainie oraz agresywnej polityki Rosji. Wzrasta liczba działań wywiadowczych, sabotażowych i dezinformacyjnych wymierzonych w RP. Równocześnie ABW zwiększa skuteczność swoich działań, czego dowodem są liczne zatrzymania, postawione zarzuty oraz rosnąca liczba prowadzonych śledztw. W dokumencie podkreśla się również znaczenie współpracy międzynarodowej, zwłaszcza w ramach NATO i UE. Wspólne działania służb państw sojuszników są niezbędne do skutecznego przeciwdziałania współczesnym zagrożeniom.

Dr Aleksandra Komar

Zastępca redaktora naczelnego czasopisma naukowego ABW „Terro-
ryzm – studia, analizy, prewencja”.

Kontakt: a.komar@abw.gov.pl



MISJA:

BEZPIECZNE PAŃSTWO

- wykrywamy i zwalczamy wrogie działania obcych państw i organizacji
- strzeżemy porządku konstytucyjnego, tajemnic państwowych oraz strategicznych interesów gospodarczych
- działamy w świecie realnym i cyfrowym, w kraju i w ramach współpracy międzynarodowej

ABW to wyjątkowe miejsce dla osób, które chcą realnie wpływać na bezpieczeństwo kraju i jego obywateli!

Dołącz do nas! **abw.gov.pl**



TERRORISM

studies
analyses
prevention

Editorial team

Damian Szlachter, PhD (editor-in-chief)
Aleksandra Komar, PhD (deputy editor-in-chief)
Agnieszka Dębska (editorial secretary, layout editor)

Translation, proofreading of the English version

Sylwia Kłobuszewska

Cover design

Aleksandra Bednarczyk

© Copyright by Agencja Bezpieczeństwa Wewnętrznego 2026

ISSN 2720-4383
e-ISSN 2720-6351

The issue was published in July 2026

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:
<https://ejournals.eu/en/journal/terroryzm>

**Language versions**

Polish (print and electronic versions)
English translation (electronic version)

Texts submission

Articles for the journal should be submitted through the editorial panel available at: <https://ojs.ejournals.eu/Terroryzm/about/submissions>

Contact

phone (+48) 22 58 58 695
e-mail: wydawnictwo@abw.gov.pl

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

Academic Editor Board

Sebastian Wojciechowski, Professor
Adam Mickiewicz University,
Institute for Western Affairs in Poznań

Waldemar Zubrzycki, Professor
Police Academy in Szczytno

Aleksandra Gasztold, Associate Professor
(PhD with habilitation)
University of Warsaw

Ryszard Machnikowski, Associate Professor
(PhD with habilitation)
University of Łódź

Agata Tyburska, Associate Professor
(PhD with habilitation)
Police Academy in Szczytno

Barbara Wiśniewska-Paź, Associate Professor
(PhD with habilitation)
University of Wrocław

Piotr Burczaniuk, PhD
Internal Security Agency

Emilijus Čižas, Lt. Col.
The NATO Counter Intelligence Centre of Excellence
(CI COE)

Jarosław Jabłoński, PhD
Armed Forces of the Republic of Poland

Anna Matczak, PhD
The Hague University of Applied Sciences

Paulina Piasecka, PhD
Civitas University in Warsaw

Viktorija Rusinaitė, PhD
The European Centre of Excellence
for Countering Hybrid Threats (Hybrid COE)

Reviewers issue 9

Magdalena Adamczuk, PhD

Tomasz Białek, PhD

Łukasz Foryś, PhD

Tomasz Kijewski, PhD

Marcin Lipka, PhD

Katarzyna Maniszewska, PhD

Michał Piekarski, PhD

Karolina Wojtasik, PhD

TABLE OF CONTENTS

255 Foreword

ARTICLES

263 Digital revolution of the EU's counter-terrorism policy
under the new EU Agenda for Combating Terrorism of 2026
Piotr Burczaniuk

285 Terrorism in Russia at national, regional and international level
Aleksander Olech

329 Protecting public spaces and public events against
vehicle-borne attacks – the importance of VSB and HVM systems
in the context of recommendations for Poland
Jarosław Jaźwiński

VARIA

375 The civil aviation security system as an example
of strengthening critical infrastructure resilience
Karol Dymek

395 Civil aviation security in practice – security systems,
control and operational resilience
Bohdan Paszukow

407 For a safer and more secure Europe in a better world.
European High Risk Security Network | cycle 2024-2025
Pedro Nogueira

- 419** **Young people and state security.
Social factors contributing to radicalisation
in the Youth Diagnosis 2026 report**
Paweł Rabiej, Konrad Ciesiołkiewicz
- 435** **Report on the conference
'New factors influencing the radicalisation
of young people from a national security perspective'**
Aleksandra Komar

AWARDED THESES

- 447** **The security policies of France and Belgium
in response to terrorist threats: a case study
of the Paris (2015) and Brussels (2016) attacks**
Nicole Szostak

REVIEW ARTICLES / REVIEWS

- 477** **Tomasz Wróblewski,
*Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym***
Tomasz Michalak
- 483** **Summary of the report
'Internal Security Agency 2024–2025. Selected activities'**
Aleksandra Komar

Ladies and Gentlemen!

We are pleased to present to you the 9th issue of the magazine 'Terrorism – Studies, Analyses, Prevention' (T-SAP), which, within a few years of this project's launch, has gained recognition beyond Poland, particularly in NATO and European Union countries. We are proud that T-SAP is featured in presentations by European law enforcement agencies as expert material worthy of regular reading. At the same time, we are working intensively with the entire Editorial Team to meet all the requirements for highly ranked scientific journals. You can see these changes both on the Publishing House's subpage (www.abw.gov/wyd) and in the membership of the Academic Editor Board, which has recently welcomed representatives from the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the NATO Counter Intelligence Centre of Excellence (CI COE) and the NATO Centre of Excellence – Defence Against Terrorism (COE-DAT).

In this issue of T-SAP, the dominant theme is violent extremism and radicalisation, which lead to terrorist activities. That is why it opens with an article devoted to the new EU Agenda for Preventing and Combating Terrorism. This is a strategic document, adopted in February 2026, which will shape the approach to terrorist threats and violent extremism within the EU and its Member States for the next few years. It reflects what we also see in Poland – a gradual shift away from traditional, physical terrorist threats toward threats that take on a hybrid form or occur exclusively in digital environment. This translates into priorities in the fight against terrorism in the EU, including threat forecasting, preventing radicalisation, protecting citizens online, protecting citizens

from physical attacks, and responding directly to threats and attacks, as well as cooperation with international partners. In this issue of T-SAP, we describe a practical aspect of the cooperation, highlighting the achievements of the two-year Portuguese Presidency in one of the EU's counterterrorism initiatives – the European High Risk Security Network (EU-HRSN). The Internal Security Agency is a founding member of this network, which brings together special uniformed units and high-risk intervention units.

In the pages of T-SAP, we have repeatedly addressed difficult topics where the lack of access to reliable data poses a major obstacle to subjecting them to critical analysis and describing them in a scientific article. This time, you will read about a terrorism in Russia, treated as a political tool used by the Kremlin at the national, regional and international level.

The article shows how Moscow 'constructs' a narrative of the fight against terrorism in order to justify its military actions, strengthen social control and build influence beyond the state's borders – in Central Asia, Middle East and Africa.

In the previous issue of T-SAP, we discussed the protection of public spaces in Poland against vehicle-borne attacks and presented the recommendations for local authorities issued by the Ministry of the Interior and Administration (these were drawn up by police experts in collaboration with the Ministry of the Interior and Administration and the Internal Security Agency, taking into account the experiences of other countries). These recommendations have been implemented in Poland when designing security measures for selected Christmas markets organised in December 2025. In this issue, at the request of our readers, we explore the practical aspects of building resilience to such attacks. We discuss the vulnerability of open public spaces to them, as well as the importance of risk analysis, the assessment of access routes, research standards relating to counter-terrorism security measures, and the interpretation of crash-tests results. Importantly, we highlight the most common mistakes made during the design, installation and operation of VSBs (vehicle security barriers).

We will return to this subject once again, following the adoption of the *Draft Regulation of the Council of Ministers on minimum requirements for the security of critical infrastructure in terms of physical, technical, personal, cybersecurity, legal and business continuity aspects*. It addresses issues relating to the technical aspects of securing facilities against vehicle-borne attacks (the draft is part of a fundamental amendment to the Act on crisis management signed on 19 June 2026).

Our readers encourage us to publish the research papers prepared by the domestic and foreign practitioners. They rarely feature in the public debate on improving counter-terrorism measures or counter-terrorism tactics. In this issue, we present experiences in building airports' resilience to contemporary threats, including those of a terrorist nature, from two perspectives: national and international. We hope you will find inspiration here to develop your skills or pursue your professional passions.

In any debate on the effectiveness of national counter-terrorism systems in the Euro-Atlantic community, the question arises as to which country has the most effective measures in place to deal with the terrorist threats it faces. We will not be able to answer this question unless we apply the appropriate methods for assessing the effectiveness of the counter-terrorism objectives adopted in a given country or region. We are therefore publishing an excerpt from the bachelor's thesis that was recognised in this year's contest of the Head of the Internal Security Agency for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats. This thesis examines the security policies of France and Belgium in response to terrorist threats between 2015 and 2016, a period during which Paris and Brussels experienced the most tragic terrorist attacks in European history. It represents an important contribution by a young author to the debate on the effectiveness of European counter-terrorism systems.

In Europe, the main driving force behind violent extremism is the phenomenon of the radicalisation of views and attitudes among young people, which has also been observed

and studied in ever greater detail in Poland. We encourage you to read the conclusions drawn from both the *Youth Diagnosis 2026* report and the conference ‘New factors influencing the radicalisation of young people from a national security perspective’, which was organised at the Internal Security Agency in April 2026. According to the researchers studying this phenomenon in Poland, the central issue underlying the development of violent extremism is the tension between technological development and the psychosocial safety of young people, with particular emphasis on the mechanisms leading to radicalisation, which may result in acts of a terrorist nature.

Today, the uniformed services are exploring ways to utilise artificial intelligence to maintain public order, internal security, protection the country’s land, sea and air borders. We encourage you to read a review of one of the latest publications on the Polish publishing market, which addresses the role of AI in preventing terrorist threats. All the more so as this review was written by an expert who is an international authority in this field.

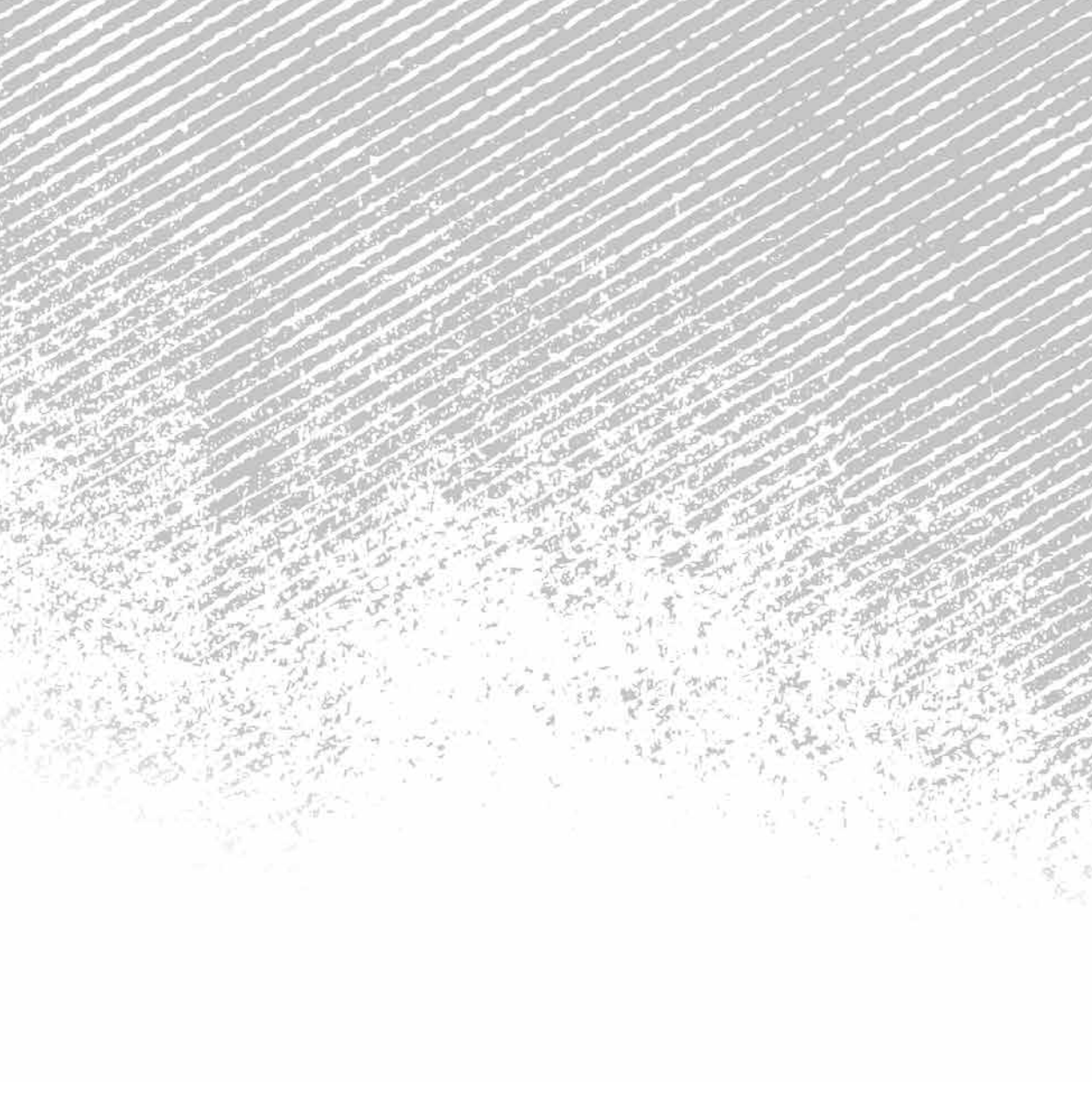
We also discuss a publication that has been the most frequently cited material from the Internal Security Agency worldwide for years. This refers to a report, published after a long break, setting out the key measures taken by the Agency in the field of Polish internal security. The current edition covers the years 2024–2025 and also describes the counter-terrorism activities of this service, including the identification of violent extremism and radicalisation processes that could lead to terrorist offences, the protection of critical infrastructure against sabotage and subversion, countering the crossing of the Polish-Belarusian border by individuals from countries posing a high terrorist risk, and conducting criminal investigations into terrorist activities targeting the citizens and the interests of the Republic of Poland at home and abroad.

We encourage you to read the articles that illustrate how contemporary threats are changing and how our thinking about security is evolving. Terrorism, violent extremism,

radicalisation, hybrid operations and sabotage are increasingly occurring side by side or intermingling with one another. That is precisely why we need reliable analyses, careful conclusions and ongoing discussion on how to effectively identify and mitigate the threats facing Poland and its allies today.

Editor-in-Chief
Damian Szlachter, PhD

Deputy Editor-in-Chief
dr Aleksandra Komar, PhD



ARTICLES

Digital revolution of the EU's counter-terrorism policy under the new EU Agenda for Combating Terrorism of 2026

PIOTR BURCZANIUK

Institute of Legal Sciences,
Cardinal Stefan Wyszyński University

 <https://orcid.org/0000-0002-6685-8769>

Abstract

On 26 February 2026, the European Commission published a new European Union Agenda for Preventing and Combating Terrorism in the form of communication, replacing a similar document that had been in force since 9 December 2020. The need to implement the new European Internal Security Strategy ‘Protect EU’ adopted on 1 April 2025 was cited as the main reason for the changes. The primary objective of the study is to outline the content of the new Agenda, with particular attention to the new approach presented therein regarding terrorist threats and violent extremism. The approach is gradually shifting away from traditional, physical terrorist threats in favour of threats that take a hybrid form or occur exclusively in the digital environment. The analysis of the document focuses on presenting the new map of terrorist threats outlined therein, based on six pillars encompassing: anticipating threats, preventing radicalisation, protecting citizens online, protecting citizens in the physical environment, responding to threats and attacks, as well as cooperation with international partners. The article pays particular attention

to the issue of the Agenda's place within the system of European legal sources and the normative effect that arises from it. The most significant differences in the approach to combating terrorism and violent extremism in the old and new agendas were also outlined.

Keywords

terrorism, violent extremism, EU security policy, EU Agenda 2026, ProtectEU, digitalisation of security, new technologies in the fight against terrorism

Agenda to combat terrorism as part of the ProtectEU strategy

On 26 February 2026, the European Commission (hereinafter: Commission or EC) published the new European Union agenda entitled *ProtectEU: Agenda to prevent and counter terrorism* (hereinafter: Agenda)¹ in the form of the communication addressed to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. It replaced the previous agenda entitled *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, published by the EC on 9 December 2020².

The main aim of the article is to provide a critical analysis of the assumptions underlying the Agenda and to demonstrate how it redefines EU's internal security policy by shifting the focus from the traditional (physical) countering of terrorism to addressing hybrid and digital threats. The main research problem of the article can be formulated as the following question: how have digitalisation, the development of new technologies, and changes in the geopolitical environment influenced

¹ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ProtectEU: Agenda to prevent and counter terrorism*, COM(2026) 101 final of 26 February 2026, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0101> [accessed: 28 IV 2026].

² *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, COM(2020) 795 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0795> [accessed: 28 IV 2026].

the evolution of EU's counterterrorism policy, and do the solutions adopted in the Agenda signify a lasting transition of the EU from a reactive-operational model to a technology-driven preventive model?

The article combines several research approaches. The study draws primarily on: the dogmatic-legal method, which was used for exegesis of the primary and secondary legislation of the EU and the case law of the Court of Justice of the European Union; the comparative method, used in the conclusion of the article, and the systemic-institutional method, applied to describe the EU's security architecture.

Work on the Agenda was initiated by the EC as part of the implementation of the ProtectEU: a European Internal Security Strategy, published on 1 April 2025 (hereinafter: Strategy)³. It constitutes a comprehensive update of the EU's approach to internal security and is based on the premise that protecting citizens and ensuring the stability of the EU's internal environment require integrated and multi-level action by all stakeholders, including EU institutions, Member States, national security and intelligence services, the private sector, and civil society.

The key element of the Strategy is to strengthen the EU's capacity to anticipate threats through the development of risk analyses, better exchange of information and the use of data provided by the EU agencies, particularly Europol. The Strategy emphasises prevention and combating of threats, particularly terrorism, organised crime and cybercrime, by dismantling criminal networks, preventing radicalisation, particularly online and restricting the sources of funding for criminal activities. Critical infrastructure security is also a significant pillar of the Strategy, which is intended to make the EU more resilient to sabotage, hybrid attacks and technological disruptions. Considerable importance is attached to strengthening the cybersecurity and resilience of digital systems, which are increasingly becoming a target of criminal and destabilising activities. The Strategy emphasises that:

(...) the terrorist threat level in Europe continues to loom. Regional crises outside the EU create a ripple effect, providing new motivation for terrorist actors across the entire ideological spectrum to recruit,

³ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy*, COM(2025) 148 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52025DC0148> [accessed: 28 IV 2026].

mobilise or build up their capacities. They target their radicalisation and recruitment efforts specifically towards the most vulnerable sections of our societies and in particular certain young people. They inspire lone actor attacks and a surge in anti-system extremism whose goal is to disrupt the democratic legal order⁴.

The fight against terrorism and violent extremism is becoming one of the pillars of the Strategy. The whole of section 6 is devoted to this issue. It is envisaged that a comprehensive counter-terrorism plan will be introduced to prevent radicalisation, secure the online and public spaces, curb funding channels, and respond to attacks should they occur.

The Strategy, similarly to the Agenda, does not define the term terrorism. Instead, it refers to the definition of 'terrorist offence' within the meaning of Article 3 of the *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*. According to that definition, these are (...) offences, which, given their nature or context, may seriously damage a country or an international organisation, if they are committed intentionally and for so-called terrorist purposes. Such damage includes:

- a) seriously intimidating a population,
- b) unduly compelling a government or an international organisation to perform or abstain from performing any act,
- c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a state or an international organisation.

At the same time, it should be noted that no legal definition of violent extremism has been adopted in the EU legislation. The Agenda merely states in a footnote that (...) *violent extremist acts do not meet the threshold set by the definition of terrorist offences; however, they pose a serious threat to security*⁵.

In the Strategy, the EC identified the following as the four key elements of the fight against terrorism:

⁴ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy...*, point 1.

⁵ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ProtectEU: Agenda to prevent and counter terrorism...*

- 1) prevention of radicalisation and protection of people online – the Commission recognises the need to tackle the root causes and, above all, highlights the way in which terrorists and violent extremists use online platforms to disseminate (particularly among minors) terrorist and other harmful content, to raise funds and to recruit. A key role in combating the spread of terrorist content online plays the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*, as it enables the rapid removal of the most repulsive and dangerous materials;
- 2) counter terrorism financing – the Commission points out that terrorists raise funds for their operations through crowdfunding campaigns, crypto-assets, neobanks or online payment platforms. Law enforcement authorities must detect and investigate these financial flows, which requires appropriate resources, tools and specialist knowledge;
- 3) protection from attacks – in addition to investing in preventing radicalisation, an important element of protecting citizens is limiting the means by which terrorists and criminals can carry out attacks. Action is needed both in relation to the tools used by terrorists and the protection of targets at risk of attack, with particular attention paid to public spaces. The Commission also points to the increasing security threats caused by the use of unmanned aerial vehicles for espionage and attacks;
- 4) foreign terrorist fighters – the Commission, together with Europol, has set out to strengthen cooperation with key third countries in order to obtain biographic and biometric data on individuals that might pose a terrorist threat, including foreign terrorist fighters. This data is to be entered into the Schengen Information System (SIS). The Commission emphasises how important it is for Member States to make use of all existing tools, including the SIS, as well as to improve biometric checks and carry out mandatory and systematic checks on all persons at the EU's external borders.

One of the most important measures in combating terrorism and violent extremism envisaged in the Strategy was the adoption in 2025 of a new EU Agenda in order to prevent and counter terrorism and violent extremism. The Agenda was ultimately adopted on 26 February 2026.

The place of the Agenda in the EU legal framework

The legal basis for the EU's actions to prevent and combat terrorism is provided by the provisions of the Treaty on the Functioning of the European Union (hereinafter: TFEU). As part of the regulation of the area of freedom, security and justice (title V), Article 67(3) of the TFEU sets out the EU's obligation to make every (...) *endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws.*

Article 83 of the TFEU constitutes the principal means of achieving this objective. It empowers the European Parliament and the Council by means of directives to (...) *establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.* The TFEU classifies the following as areas of this crime: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

In addition, in accordance with Article 84 of the TFEU: *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures to promote and support the action of Member States in the field of crime prevention, excluding any harmonisation of the laws and regulations of the Member States.* It is on this basis that the European Parliament and the Council may adopt strategy and agenda documents which set policy directions but are not directly binding in nature. At the same time, Article 17 of the Treaty on European Union (hereinafter: TEU) assigns the EC the task of supporting the general interest of the EU and, to that end, taking appropriate initiatives.

In summary, the adoption of strategies such as Agenda is not based on a single specific legal basis, but rather on a set of Treaty provisions. These provisions:

- set out the objective of the EU aimed at ensuring security (Article 67 of the TFEU),
- grant the EU powers to combat terrorism (Article 83 of the TFEU),
- enable supportive and strategic actions (Article 84 of the TFEU),

- give the Commission the role of driving EU policies (Article 17 of the TEU).

It is also worth noting that, in accordance with Article 4(2), third sentence of the TEU: (...) *In particular, national security remains the sole responsibility of each Member State.* This means that the EU's actions – including anti-terrorist strategies – are purely of a coordinating and supportive nature and do not replace national policies.

On these legal ground, the EC may accept strategic documents in the form of, among others, COM documents. They include official positions, strategies, analyses and announcements of legislative actions of the Commission and play a role of the so-called soft law. The role and the importance of such a law results mainly from the case law of the Court of Justice of the EU (CJEU). It emphasises that such law has no binding force, but cannot be completely ignored when interpreting EU law⁶. It may be a point of reference for interpretation, especially when it clarifies EU policy⁷, and at the same time it binds the Commission in its own practice, although it is not formally binding on the Member States of the EU⁸.

Map of terrorist threats according to the Agenda

The Agenda begins with an introduction in which the EC analyses the most significant risks and emphasises that (...) *terrorism and violent extremism remain a persistent challenge for the EU and its Member States. The increasing links between terrorism and other crime areas, more fluid networks and less ideologically driven actors, as well as the blurred lines between online and physical operations, pose a particular challenge to defining and identifying terrorist offences*⁹.

⁶ Cf. Judgment of the Court (Second Chamber) of 13 XII 1989 Salvatore Grimaldi v Fonds des maladies professionnelles. ECLI: EU:C:1989:646.

⁷ Cf. Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

⁸ Cf. Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. Dansk Rørindustri and Others v Commission of the European Communities.

⁹ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ProtectEU: Agenda to prevent and counter terrorism...*, p. 1.

As the authors of this document point out, the number of coordinated and large-scale attacks in the EU has decreased in recent years, however the threat has not disappeared, but has evolved, both subjectively and ideologically. The number of perpetrators acting alone and in small groups of several people, whose core is often minors, is growing. In terms of ideological motivation, it is emphasised that (...) *while jihadist terrorism remains the most prominent and lethal terrorist threat, terrorists and violent extremists are driven by a growing range of motivations, not always attached to a specific ideology, including the rejection of European democratic values, anti-semitism, or anti-Muslim hatred*¹⁰.

Furthermore, the EC notes that security in the EU, including the terrorist threat level, is influenced by the changing geopolitical environment and external conflicts affecting the EU, primarily in the Gaza Strip, as well as – in the context of an increase in the number of acts of sabotage and hybrid operations – the ongoing Russian war of aggression against Ukraine. The European Union faced complex threats stemming from both terrorist groups as well as foreign state and non-state actors. These entities model their actions on those traditionally attributed to terrorist groups, e.g. they use improvised ignition devices in aerial munitions, they carry out cyber attacks or sabotage of critical infrastructure, but also use terrorists and violent extremists as supporters. Links are formed and maintained between terrorism, organised crime and cybercrime. They utilise criminal service models and shared resources, primarily in the areas of recruitment, criminal trading platforms and underground banking networks.

Significant part of contemporary terrorism is its strong connection to the digital environment. Internet, social media, online gaming platforms have become key tools used by extremist organisations and individuals holding such views to conduct propaganda, recruit new members, as well as to exchange information and plan activities. The Agenda states that:

Terrorist actors coordinate plans on end-to-end encrypted (E2EE) communication platforms and finance their networks and attacks with cryptocurrencies, non-fungible digital assets (NFTs) and ‘digital hawala’¹¹. Generative AI is abused to create instruction

¹⁰ Ibid.

¹¹ Digital hawala is informal system for transferring financial value through the use of digital tools, operating outside the traditional banking system and relying on a network of trusted intermediaries.

manuals for attacks. 3D-printing technology (e.g. to manufacture firearms) and the increased use of unmanned aircraft systems (UASs / drones) further exacerbate the threat¹².

The Commission indicates that described threats are cross-border in nature. This means that no Member State is able to counter them effectively on its own. Therefore, it is necessary to strengthen the cooperation at EU and international level. However, it should not be forgotten, as the Commission emphasises, that a balance must be struck between ensuring security and protecting fundamental rights. Antiterrorist actions must be taken in accordance with EU values, such as democracy, the rule of law and respect for human rights. It is important in terms of both the legality of the actions taken and for maintaining public confidence in them.

Six pillars of the fight against terrorism and violent extremism

In the second point of the Agenda, the Commission sets out a comprehensive approach to counter terrorism and violent extremism based on a system of six interlinked pillars of action. These are: 1) anticipating threats, 2) preventing radicalisation, 3) protecting people online, 4) protecting people in the physical environment, 5) responding to threats and attacks, 6) cooperating with international partners. This approach reflects the belief that an effective antiterrorist policy cannot be limited to reacting to events, but must encompass the full spectrum of measures – from identifying risks, to prevention, as well as response and recovery following any attacks. Contemporary threats are dynamic, multidimensional and often cross-border, which requires an integrated approach involving various levels of government – local, national, EU and international.

Anticipating threats

The Commission highlights that (...) *security starts with effective anticipation and foresight*¹³.

¹² *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ProtectEU: Agenda to prevent and counter terrorism...*, p. 3.

¹³ *Ibid*, p. 4.

Anticipating threats is intended to form the foundation of the entire strategy and be based on the gathering, analysis and exchange of information. Cooperation between Member States and EU agencies, including the Single Intelligence Analysis Capacity¹⁴, which provides timely risk assessments, and Europol, which draws up regular reports on trends based on information received from law enforcement authorities, plays a key role in this regard. Dynamic and unpredictable nature of emerging threats requires – according to the Commission – strengthening the ability of law enforcement agencies to anticipate, in order to better identify emerging threats and take appropriate actions to combat terrorism.

In turn, anticipating is crucial from the perspective of identifying threats and is to be based on two elements. The first of these is to use the potential of new technologies in law enforcement. Artificial intelligence (AI), machine learning or big data analysis is a tool-based potential that allows for the identification of behavioural patterns and the detection of warning signals that may indicate the preparation of attacks. The second element is to prepare to counter the use by terrorists of new technology, such as AI, online platforms, electronic financing methods, particularly crypto-assets, or the use of 3D-printed weapons. Forecasting activities are to be based on the work of the Joint Research Centre of the European Commission and their financing basis is to be the Horizon Europe programme.

Analysis of the principles underlying this pillar leads to the conclusion that there should be a shift from reactive model previously presented by the EU to a preventive model, in which action is taken before the threat materialises.

Preventing radicalisation

The Commission defines preventing radicalisation as (...) *tackling its drivers before they take root*¹⁵. The second pillar is based on four elements:

¹⁴ SIAC – a structure linking the civilian EU INTCEN (European Union Intelligence and Situation Centre), i.e. the EU civilian intelligence unit, which is part of the European External Action Service with Military Intelligence Directorate as part of the European Union Military Staff (EUMS).

¹⁵ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ProtectEU: Agenda to prevent and counter terrorism...*, p. 5.

- 1) developing a prevention toolbox for minors. These tools are intended to enable early detection, strengthen protective factors, build resilience through education and social integration, in particular of minors, as well as support families and communities in using the internet safely;
- 2) building resilient societies, with a view to protecting all religious communities from hatred, discrimination and violence. The work of the EC will focus on using AI to improve detection of extremist content, develop common threat indicators and streamline cooperation between platforms, law enforcements agencies and scientists in order to identify propaganda generated by AI and coordinated campaigns aimed at radicalisation;
- 3) addressing radicalisation in prisons, prison leavers and managing the return of Foreign Terrorist Fighters and their family members. The basis is to develop tools for risk assessment and management in the pre-release phase and guidelines supporting national approaches to radicalised prison leavers and returnees, combined with training in rehabilitation and reintegration, with particular emphasis on the protection of children;
- 4) supporting victims of terrorism by raising awareness of the EU Remembrance Day for victims of terrorism and supporting victims' associations by promoting their active role in prevention programmes.

Institutionally, activities within the second pillar are handled by the EU Knowledge Hub on Prevention of Radicalisation established in 2024. The Centre draws up guidelines, tools, training and support services for decision-makers and practitioners.

Protecting people online

The European Union adopted the world's most advanced regulatory framework for combating terrorist activity online, but the threat continues to evolve. The Agenda states that: *Extremist networks adapt quickly, exploit emerging technologies and shift from open platforms to exploiting closed chats and encrypted services. This can create serious challenges for detecting and preventing terrorist plans, for mapping terrorist networks and their supporters, and for investigating and prosecuting terrorist activities*¹⁶.

¹⁶ Ibid, p. 8.

According to the Commission's guidelines, activities in this pillar are to focus on three issues:

- 1) making full use of regulatory frameworks to tackle terrorist and extremist content online by, among others, development by Europol of European hash-sharing database, i.e. database of digital traces for terrorist and violent extremist content, which will enable Member States and hosting service providers to securely flag, match and remove content across various platforms;
- 2) working with industry, mainly with online service providers, which will be implemented through the EU Internet Forum (which brings together EU Member States' ministries, law enforcement authorities, civil society and online service providers, including social media platforms) and by activities together with the European Board for Digital Services to intensify the fight against the dissemination of terrorist and violent extremist content;
- 3) ensuring effective and coordinated crisis response online, assuming the transformation of the existing EU Crisis Protocol into an EU Online Crisis Response Framework (included in the Digital Services Act). Member States will be able to use it where an incident leads to heightened online activity related to an attack.

Protecting people in the physical environment

The fourth pillar is based on changed approach, according to which the foundation is action based on resilience. It replaced the action focused on security. This occurred with the adoption in 2022 of the *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* (hereinafter: CER Directive). At the same time, the EU provides practical support based on EU security advisors. Their task is to assist in assessing vulnerability to threats and suggesting specific improvements. According to the Agenda, EU activities in the pillar under review are to focus on five issues:

- 1) impeding terrorist travel, by ensuring a high level of protection of the EU external borders. This is primarily achieved through large-scale information systems: the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the Visa Information System (VIS) and the interoperability framework. The big challenges remain cooperation with third

countries to obtain biographic and biometric data on individuals that might pose a terrorist threat and entering this data into the SIS system, as well as developing the procedure to be followed in the event of a 'hit'. The so-called screening process is due to come into application in June 2026¹⁷. Thanks to it, the identification of third-country nationals who have crossed the external borders illegally or are staying illegally on Member States' territory without having undergone entry checks is set to become easier. The Commission emphasises that it will promote the efficient return of individuals posing a security risk;

- 2) restricting access to means used to carry out attacks by harmonisation regulations on the criminalisation of illegal firearms trafficking and other firearms-related offences, including the illicit creation, possession and dissemination of blueprints to manufacture 3-D printed firearms. The Agenda also assumes a review of the *Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013* and the presentation of a new action plan for preparedness and response to chemical, biological, radiological and nuclear (CBRN) risks in 2026;
- 3) addressing the threat posed by drones. The Commission emphasises the importance of the threat associated with the use of new and emerging technologies, particularly drones by terrorist actors. Counter-drone operations are to be based on the Drone Strategy 2.0¹⁸ and the EU Action Plan on Drone and Counter Drone Strategy presented on 11 February 2026¹⁹;
- 4) protecting public spaces in Europe, whereas it is necessary to take into account security requirements already at the design stage

¹⁷ *Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817.*

¹⁸ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', COM(2022) 652 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0652> [accessed: 28 IV 2026].*

¹⁹ *Action Plan on Drone and Counter Drone Strategy*, European Commission, <https://digital-strategy.ec.europa.eu/en/policies/drone-security> [accessed: 28 IV 2026].

of urban areas, public spaces and places of worship. This should be reflected in appropriate obligations for operators of public spaces to implement security measures based on risk assessments. In organisational terms, this task is entrusted to the reinforced EU Forum on the Protection of Public Spaces;

- 5) resilience of critical entities, transport and supply chain security. This is linked to growing concerns about possible incidents in the form of hybrid campaigns and acts of sabotage by hostile state actors and their proxies. In order to improve security, the EC recommends urgent implementation of the aforementioned CER Directive and the *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*.

Responding to threats and attacks

The fifth pillar is to be based on a rapid and coordinated response provided by the law enforcement and judicial authorities, which require reinforcement, with the support of Europol and Eurojust. The Commission also highlights the need to take further actions aimed at eliminating gaps in the system for preventing the financing of terrorism.

Activities within this pillar are to focus on three issues:

- 1) countering terrorism financing and financing of violent extremism. The Commission highlights that the global nature of financial services requires the active response of the whole of Europe to the issue of terrorist financing. This is also of significant importance because of new sources of financing, such as crypto assets, digital hawala (and online payment services). The Commission considers the full implementation of the EU package on *anti-money laundering and countering the financing of terrorism* (AML/CFT), adopted on 30 May 2024, as the legal foundation for combating the financing of terrorism. The package includes the *Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing* (it will come into force on 10 July 2027) and the *Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on*

the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849. The Commission also plans to begin work on developing a EU-wide system that will enable the retrieval of financial data in order to track funds belonging to terrorists and organised crime proceeds. The system is due to be established by 2030 and will include intra-EU and Single European Payment Area (SEPA) transactions, crypto asset transfers, online payments or electronic fund transfers;

- 2) strengthening the law enforcement authorities response through enhancing the Europol's mandate, mainly its European Counter Terrorism Centre (ECTC) as a leading centre for information, technology and innovation for the law enforcement;
- 3) strengthening judicial cooperation through full implementation of the *Roadmap for lawful and effective access to data for law enforcement*²⁰ adopted by the Communication from the Commission of 24 June 2025. The ability to secure and obtain evidence directly from service providers offering their services in the EU is of crucial importance, pursuant to the *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*, which has been in force since 18 August 2026. The Commission draws attention to the essence of the SIRIUS project, endorsed by the EU, which is an EU system designed to support law enforcement authorities in gathering evidence from the internet across national borders²¹.

²⁰ *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Roadmap for lawful and effective access to data for law enforcement*, COM(2025) 349 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0349> [accessed: 29 IV 2026].

²¹ *SIRIUS project*, Europol, 21 I 2026, <https://www.europol.europa.eu/how-we-work/sirius-project> [accessed: 29 IV 2026].

Cooperating with international partners

The last pillar implies the need to strengthen international cooperation, primarily through the activities of the High Representative and the EU Counter-Terrorism Coordinator.

Activities under this pillar are to focus on four issues:

- 1) restrictive measures to combat terrorism, with the EU Terrorist List serving as the main tool to disrupt terrorist networks²²;
- 2) advancing international agreements, where the biggest challenge remains new Protocol amending the definition of terrorist offences in the Council of Europe Convention on the prevention of terrorism²³. Once it comes into force, it is intended to provide a common pan-European definition of terrorist offences for more than 40 countries;
- 3) deepening bilateral and regional cooperation, in particular strengthening cooperation with partners involved in the EU enlargement process, as well as on measures targeting specific regions, with particular attention being paid to the Western Balkans, the Middle East, including Syria, as well as African countries;
- 4) reinforcing the EU's role by coordination and activities within the multilateral forums of the High Representative, the Commission and the EU Counter Terrorism Coordinator. Thematic cooperation with the Council of Europe, the Financial Action Task Force, Interpol and NATO is to be maintained.

The 2026 vs. 2020 Agenda

The 2026 Agenda, which was drafted with a view to implementing the new ProtectEU Internal Security Strategy published on 1 April 2025, makes the adoption of the EU's strategy for combating terrorism and violent

²² The official list of individuals, groups, and entities designated by the EU as involved in terrorist activities is formally maintained pursuant to the *Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP)*.

²³ Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), [https://search.coe.int/cm/g#{%22CoEIdentifier%22:\[%220912594880264105%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/g#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}) [accessed: 14 V 2026].

extremism to current threats a central theme. As the Commission points out, their nature has undergone a noticeable shift – from traditional, physical terrorist threats to threats that take on a hybrid form or exist only in digital environment. Reactive-operational approach is therefore replaced by an approach focused on proactive, systemic actions in the digital sphere.

The 2020 Agenda addressed terrorist threats in the traditional way, as activities carried out by organised groups that were ideologically motivated and conducted primarily 'offline'. Internet appeared in it only as one of the tools and did not constitute the central focus of interest. The new Agenda considers digital space to be the primary environment in which threats occur. Radicalisation, recruitment, propaganda and financing are increasingly taking place exclusively in a virtual environment, which means that threats are more scattered, harder to detect at an early stage, and strongly linked to disinformation and information manipulation. The Agenda implies the need to shift from the approach focused on combating a specific organisation to one centred on managing a dynamic, primarily digital ecosystem of threats.

The approach to carrying out preventive measures has also changed. The previous Agenda was focused on countering radicalisation, including through social programmes, monitoring of high-risk groups and cooperation of the services. In 2026 Agenda, prevention is largely shifting online, with a focus on the early detection of extremist content, countering its algorithmic amplification, its rapid removal and limiting its reach. In this way, prevention is becoming more technology-driven and automated, and relies less on social activities.

In the previous Agenda, digital technologies were the tool only supporting activities (e.g. data analyses, information exchange). In the new Agenda technologies are becoming a central element of the strategy, focused primarily on using AI to identify threats, analyse big data, automate security processes and develop predictive tools. The difference, therefore, lies in the shift from a level of technological support to a strategy based on technology.

Both documents emphasise the importance of cooperation, however, the previous Agenda focused exclusively on the cooperation between Member States and EU agencies, while the new one has expanded this to include private sector, technological entities and global cooperation. This cooperation is becoming networked and multi-layered. In the 2020 document, private sector (particularly online platforms) acted as a partner

supporting the activities of states. In the 2026 Agenda, the role of this sector is clearly expanded. Social platforms are becoming jointly responsible for security. The Commission expects them to actively detect and remove content as well as to put in place systemic cooperation and monitoring mechanisms. There is a shift from the model of voluntary cooperation towards the model of shared regulatory responsibility.

There is also a noticeable shift in the approach to building public resilience. In 2020 Strategy, this resilience was important but was treated more as a supplementary element. In the new Agenda, it has become one of the most important pillars, primarily in the fight against disinformation, building digital awareness, and reducing online vulnerability to radicalisation. Security no longer concerns just a specific institution, but society as a whole, as a system.

In summary, it is important to remember that the adopted Agenda is, in fact, a document of a purely programme-related nature. The implementation of its objectives is to be achieved through proposed or already implemented EU legislative acts and activities focused mainly on developing cooperation among the law enforcement authorities of EU Member States and third countries, under the coordination of organisationally strengthened Europol with actual executive functions.

Bibliography

Internet sources

Action Plan on Drone and Counter Drone Strategy, European Commission, <https://digital-strategy.ec.europa.eu/en/policies/drone-security> [accessed: 28 IV 2026].

SIRIUS project, Europol, 21 I 2026, <https://www.europol.europa.eu/how-we-work/sirius-project> [accessed: 29 IV 2026].

Legal acts

Treaty on the Functioning of the European Union (Journal of Laws of 2004, no. 90, item 864).

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Official Journal of the EU L 1624 of 19 VI 2024).

Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817 (Official Journal of the EU L 1356 of 22 V 2024).

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (Official Journal of the EU L 191/118 of 28 VII 2023).

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172/79 of 17 V 2021).

Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013 (Official Journal of the EU L 186/1 of 11 VII 2019).

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (Official Journal of the EU L 1640 of 19 VI 2024).

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).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – (Official Journal of the EU L 333/80 of 27 XII 2016).

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 88/6 of 31 III 2017).

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM(2020) 795 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0795> [accessed: 28 IV 2026].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Roadmap for lawful and effective access to data for law enforcement, COM(2025) 349 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0349> [accessed: 29 IV 2026].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ProtectEU: Agenda to prevent and counter terrorism, COM(2026) 101 final of 26 February 2026, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0101> [accessed: 28 IV 2026].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', COM(2022) 652 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0652> [accessed: 28 IV 2026].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM(2025) 148 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148> [accessed: 28 IV 2026].

Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP) – (Official Journal of the EU L 344/93 of 28 XII 2001).

Case law

Judgment of the Court (Second Chamber) of 13 XII 1989 *Salvatore Grimaldi v Fonds des maladies professionnelles*. ECLI: EU:C:1989:646.

Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

Joined Cases C-189/02 P C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. *Dansk Rørindustri and Others v Commission of the European Communities*. ECLI: EU:C:2005:408.

Other documents

Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), [https://search.coe.int/cm/eng#{%22CoEIdentifier%22:\[%220912594880264105%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/eng#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}) [accessed: 14 V 2026].

Piotr Burczaniuk, PhD

Doctor of Law, Assistant Professor at the Chair of the Theory and Philosophy of Law of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw; legal counsel, member of the Regional Chamber of Legal Advisers in Warsaw; legislator, member of the Polish Legislation Society; legislative expert. Author of publications on the theory and philosophy of law, constitutional law and economic law.

Contact: p.burczaniuk@uksw.edu.pl

Terrorism in Russia at national, regional and international level

ALEKSANDER OLECH

Defence24

 <https://orcid.org/0000-0002-3793-5913>

Abstract

Terrorism in Russia should be analysed not only as a threat to national security, but also as a political tool used by the Kremlin at the national, regional and international level. The evolution of threats in the Russian Federation, from the North Caucasus and the Caucasus Emirate, through the growing significance of the so-called Islamic State, to the activities of the Islamic State – Khorasan Province and the attack at the Crocus City Hall, illustrates the many challenges facing the security services. The author analyses Russian anti-terrorist legislation and selected regulations concerning extremism, which, in practice, are used by the Russian state as part of a broader system of control and threat assessment. The article also discusses cooperation in the fight against terrorism in the Collective Security Treaty Organisation. The author demonstrates that Moscow uses the narrative of the fight against terrorism to justify military action, strengthen social control and build influence beyond the country's borders, including in Central Asia, the Middle East and Africa. The Russian anti-terrorist model is based less and less on prevention and more and more on political definition of opponents, which leads to incorrect management of threat perception and, as a result, to further terrorist attacks.

Keywords

Russia, terrorism, extremism, ISIS, Asia, CSTO, anti-terrorism, the Kremlin

Introduction

Terrorism is a term that is widely used but is difficult to define unambiguously. The phenomenon of terrorism is, in fact, dynamic, dependent on the legal and political context, as well as on the entities that define it: the state, international organisation or researcher. There are hundreds of different perspectives in the literature, ranging from accounts that emphasise violence against civilians and the psychological impact, to approaches that treat terrorism as a method of struggle aimed at bringing about political or ideological change. Alex P. Schmid describes terrorism as a method involving repeated acts of violence carried out by partly covert individual, groups or state actors, motivated by political, criminal or idiosyncratic reasons. In his view, the direct victims of violence are not the main addressee of the action, but they serve as a tool for conveying a message to a selected group, authorities or society¹. Bruce Hoffman defines terrorism as a deliberated instilling fear through violence or the threat of violence and exploiting it in the pursuit of political change. He emphasises that terrorism is intended to have psychological effects extending beyond the direct victims of the attack, as its real target is the wider public: society, government, public opinion or particular political, ethnic or religious group².

From a Polish perspective, Krzysztof Liedel and Paulina Piasecka define terrorism as an unlawful use of force or violence against persons or property in order to intimidate or coerce the government or the civilian population. The main aim of such activities is to achieve political or social goals³.

The Global Terrorism Index does not present the author's definition of terrorism, but based on the 2026 report, it can be assumed that it is (...) *a threat or actual use of illegal force and violence by a non-state actor to achieve a political, economic, religious or social objective through intimidation, coercion*

¹ A.P. Schmid, *Defining Terrorism*, https://icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf [accessed: 20 III 2026]; See also: A.P. Schmid, A.J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Amsterdam 1988.

² *Database Scope*, RAND National Security Research Division, <https://www.rand.org/nsrd/projects/terrorism-incidents/about/definitions.html> [accessed: 20 III 2026].

³ K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej* (Eng. How to survive in an age of terrorist threats. Elements of counter-terrorism education), Warszawa 2008, pp. 46–47.

or *instilling*⁴. In addition, the source distinguishes between the concepts of ‘terror’ and ‘terrorism’, and also questions the distinction between terrorism and resistance or guerrilla warfare, because what is an attack for some is, for others, a narrative in the struggle for freedom⁵.

It should be emphasised that, in this article, the term ‘extremism’ is not treated as a synonym for terrorism. Extremism refers to a broader ideological, organisational and political category associated with extreme views, radicalisation, propaganda or the activities of groups regarded as a threat. It may lead to violence or terrorist activity, but it is not necessarily the same thing. Terrorism refers, however, primarily to the use of violence or the threat of violence for political, ideological, religious or social purposes. In the Russian legal system, extremism and terrorism are treated as related but distinct legal categories. This is evident in Article 282.2 of the Criminal Code of the Russian Federation, which concerns extremist organisations but explicitly excludes organisations designated as terrorist under Russian law. Terrorist organisations are covered by separate regulations, in particular Article 205.5 of the Criminal Code of the RF concerning the organisation of and participation in the activities of a terrorist organisation. At the same time, in the practice of the Russian security apparatus, the concepts of extremism and terrorism are sometimes used in parallel as instruments of social control and for the political definition of threats. Therefore, in the text, the term ‘terrorism’ refers primarily to acts of violence, attacks and the activities of terrorist organisations, while ‘extremism’ appears where the Russian legal regulations, radicalisation, propaganda and broader mechanisms of politically defining opponents are discussed.

For the Moscow authorities, achieving the goals is crucial, so they use their own, context-dependent definition of terrorism⁶. On the one hand, as Russian politicians point out, no country is resistant to terrorist attacks⁷.

⁴ *Global Terrorism Index 2026*, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf>, pp. 6–7 [accessed: 13 IV 2026].

⁵ A.P. Schmid, *Defining Terrorism...*; L. Weinberg, A. Pedahzur, S. Hirsch-Hoefler, *The Challenges of Conceptualizing Terrorism*, “Terrorism and Political Violence” 2004, vol. 16, no. 4, pp. 777–794. <https://doi.org/10.1080/095465590899768>.

⁶ The Russian legislation defines a terrorist act as the commission of an explosion, arson or other acts designed to instil fear among the population and to pose a threat to life, causing significant material damage or other serious consequences, undertaken with the aim of destabilising the activities of public authorities or international organisations. More in the sub-section: *Russian legislation on terrorism and extremism*.

⁷ G. Faulconbridge, *Russian security failure? Kremlin says no country is immune to terrorism*,

On the other hand, from a Russian perspective, terrorism is linked to state policy, not just to a threat to security. This means that Russia can use a broad definition of terrorism to characterise the actions of opponents, including external actors (organisations, states and groups), as terrorist in nature as part of protecting its interests, including abroad. Russian understanding of terrorism differs from the concepts adopted in Western countries, including in Poland, both at the legal and political levels⁸.

In the article, the author presented terrorist threats that the RF has been struggling with for years. He described also the most important terrorist groups and the activities they carry out within the Russian territory, primarily in North Caucasus. Furthermore, he emphasised the role of Moscow's international cooperation and its foreign operations, with particular emphasis on combating terrorism. He discussed counter-terrorist activities, the strategy of the Collective Security Treaty Organisation (hereinafter: CSTO)⁹ in the fight against terrorism, and the national legislation relating to terrorism and selected regulations concerning extremism.

The scope of this article and the research objective set do not allow for a detailed discussion of all the aspects of the Russian internal politics. It does not take into account politically motivated prison sentences, nor does it provide a comprehensive analysis of the institutions involved in both the anti-terrorist activities and the functioning of the apparatus of repression. These issues require a separate study.

Since the start of the RF's full-scale invasion of Ukraine, terrorism in Russia has ceased to be merely one of the threats to security and has become an element of domestic and international policy, a tool used to support political and military actions. Subsequent attacks in Russia after 2022 revealed significant gaps in the operation of the security apparatus and a lack of effective response. This did not change the paradigm of Moscow's

Reuters, 25 III 2024, <https://www.reuters.com/world/europe/russian-security-failure-kremlin-says-no-country-is-immune-terrorism-2024-03-25/> [accessed: 20 III 2026].

⁸ A. Olech, *Terroryzm – określenie definicji zjawiska w polskich i zagranicznych badaniach* (Eng. Terrorism – defining the phenomenon in Polish and foreign research), “Studia Bezpieczeństwa Narodowego” 2020, vol. 18, no. 2, pp. 121–138. <https://doi.org/10.37055/sbn/145302>.

⁹ The Collective Security Treaty Organisation consists of: The Russian Federation, Belarus, Armenia, Kazakhstan, Kyrgyzstan and Tajikistan, although Armenia remains a formal member of the organisation, it has not been involved in its work since February 2024.

policy towards terrorist threats. On the contrary – the narrative attributing responsibility for the attacks against the RF primarily to Ukraine and Western countries is being reinforced¹⁰. As a result, the Russian anti-terrorist model relies increasingly on managing public perception and politically defining opponents, rather than on prevention. Therefore, the country becomes vulnerable to further attacks from different groups¹¹.

Russia's current strategy in Europe is based on the systemic use of criminal networks as a tool of hybrid war. Russian services recruit people with a criminal record, who are often in difficult economic situation and come from Russian-speaking communities, to carry out acts of sabotage, such as damage to infrastructure and acts of vandalism¹². This mechanism allows Russia to operate below the threshold of open conflict, limit the risk of being unequivocally held responsible, and reduce operating costs.

Russian legislation on terrorism and extremism

Russian legislation, including Article 205 of the Criminal Code of the RF, defines a terrorist act as the causing of an explosion, arson or other acts designed to instil fear in the population and pose a threat to life, causing significant property damage or other grave consequences, undertaken with the aim of destabilising the activities of the public authorities or international organisations or influencing their decisions. The provision also covers the mere threat of carrying out such actions. In the case of offenses committed by an organised group or resulting in serious consequences, enhanced penalties are provided. Actions involving the use of nuclear materials, chemical or biological substances, or actions leading to the death of a person may, however, result in a sentence of life imprisonment. At the same time, the regulations allow for exemption

¹⁰ K. Hird et al., *Russian Offensive Campaign Assessment, March 25, 2024*, Critical Threats, 25 III 2024, <https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-march-25-2024> [accessed: 20 III 2026].

¹¹ E. Ferris, *How Russia's War in Ukraine is Creating Domestic Security Gaps*, Royal United Services Institute, 23 IX 2025, <https://www.rusi.org/explore-our-research/publications/insights-papers/how-russias-war-ukraine-creating-domestic-security-gaps> [accessed: 21 III 2026].

¹² K. Rekawek, J. Lanchès, M. Zotova, *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 VI 2026].

from criminal liability for individuals who have contributed to preventing the commission of the attack¹³.

Russian legislation, in particular the Federal Law ‘On Countering Terrorism’, defines terrorism as an ideology of violence and the practice of influencing the decisions of government authorities or international organisations by intimidating the population or other forms of unlawful actions involving the use of violence¹⁴. At the same time, the Act introduces broad understanding of terrorist activity, including carrying out attacks, planning them, financing them, inciting them, creating illegal armed structures, recruiting and training perpetrators, as well as information activities and propaganda. The scope of terrorist activity can be very broad, taking into account activities of an informational and political nature as well. Regulations related to counterterrorism encompass not only the prevention, detection, and suppression of threats, but also the mitigation of their consequences, the conduct of counterterrorism operations, and the protection of facilities and sites of particular importance¹⁵. The broadening of the definition of ‘public space’ gives the state considerable leeway in classifying certain activities as terrorist acts¹⁶.

The National Antiterrorism Committee serves as the central body coordinating the RF’s counterterrorism efforts, integrating the activities

¹³ Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 205. Террористический акт (Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 No 63-FZ. Stat’ya 205. Terroristicheskiy akt), https://www.consultant.ru/document/cons_doc_LAW_10699/43942021d9206af7a0c78b6f65ba3665db940264/ [accessed: 20 III 2026].

¹⁴ Федеральный закон Российской Федерации от 06.03.2006 No 35-ФЗ „О противодействии терроризму”. Статья 3. Основные понятия (Federal’nyy zakon Rossiyskoy Federatsii ot 06.03.2006 No 35-FZ „O protivodeystvii terrorizmu”. Stat’ya 3. Osnovnyye ponyatiya), https://www.consultant.ru/document/cons_doc_LAW_58840/4fdc493704d123d418c32ed33872ca5b3fb16936/ [accessed: 20 III 2026].

¹⁵ Counterterrorism operation – a set of special, operational-combat, military and other actions involving the use of combat equipment, weapons and special means, aimed at stopping a terrorist act, neutralising terrorists, ensuring the safety of individuals, organisation, and institutions, and minimising consequences of a terrorist act. Russian legislation distinguishes between broadly understood counterterrorism activities (systemic measures) and a counterterrorism operation (a specific use of force), with both concepts being formulated in a manner that allows for their flexible – including political – application. Counterterrorism activities are defined as activities carried out by state authorities, public authorities of federal territories, local self-government bodies and private individuals. Quoted after: Федеральный закон Российской Федерации от 06.03.2006 No 35-ФЗ...

¹⁶ Ibid.

of federal, regional, and local structures under the leadership of the Federal Security Service (FSB). It is responsible for planning counterterrorism operations, shaping state policy in this area and managing communications related to threats¹⁷. This demonstrates the centralisation of Russia's security system and the significant role of the Kremlin in defining threats and combating terrorism.

Russia defines the phenomenon of international terrorism in very broad terms and in a way that is directly linked to its own interests. Article 361 of the Criminal Code includes not only traditional acts of violence, such as terrorist attacks or arson, but also any activities considered to be directed against the interests of the RF or to interfere with the 'peaceful coexistence of states'. In practice, this means that the category of terrorism can be applied much more broadly than simply to domestic security threats. Importantly, individuals who finance, recruit, or train the perpetrators of such attacks may also be subject to a sentence of life imprisonment. The regulations provide for the harshest penalties in the event of fatal attacks¹⁸. All of this is part of a general trend within the Russian state apparatus towards maximising criminal liability, while leaving room for interpretation.

Russian regulations concerning extremist and terrorist activities indicate that the state treats this category very broadly and, above all, as a tool of control. Article 282.2 of the Criminal Code provides for severe penalties (up to 10–12 years of imprisonment in cases involving the abuse of an official position), both for organising structures and for mere participation or recruitment. This means that the line between a real threat and activity arbitrarily defined as extremist is blurred. Importantly, this provision concerns organisations recognised as extremist¹⁹, excluding organisations which, under the legislation of the RF, have been recognised

¹⁷ *National Antiterrorism Committee: goals and objectives*, National Antiterrorism Committee, <https://en.nac.gov.ru/home> [accessed: 21 III 2026].

¹⁸ *Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Статья 361. Акт международного терроризма (Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 № 63-FZ. Stat'ya 361. Akt mezhdunarodnogo terrorizma)*, https://www.consultant.ru/document/cons_doc_LAW_10699/0994b72ccab34fae773ced2c837691518a3e3dca/ [accessed: 20 III 2026].

¹⁹ *List of organisations designated as extremist under the legislation of the Russian Federation*, see: *Перечень организаций, признанных в соответствии с законодательством Российской Федерации экстремистскими (Pierieczen' organizacyj, priznannyh w sootwietstwiu s zakonodatelstwom Rossijskoj Fiedieracyi ekstriemists)*, <https://minjust.gov.ru/ru/documents/7822/> [accessed: 20 IV 2026].

as terrorist²⁰. In practice, this shows that extremism and terrorism function in Russian law as related but not identical categories. At the same time, it is possible to avoid liability by voluntarily ceasing activities, but in practice the final decision rests with the security services, which determine whether a person has in fact ceased their activities and whether they should face the consequences.

Terrorist threats to the Russian Federation

Among the member states of the CSTO, Russia is the main source of terrorist threats in the post-Soviet space, and is also a country accused of terrorist activities both domestically and abroad. The Kremlin, in order to achieve its own objectives, demonstratively resorts to measures in domestic policy that fall within the definition of terrorism. At the same time, the RF is developing anti-terrorist strategy which it uses to subjugate regions and communities and to justify its military actions. For decades, Russia has demonstrated that it very effectively uses the 'terrorism threat' to achieve its goals. This is the case in relation to the Caucasus region, activities on the African continent, and with regard to Ukraine²¹. At the same time,

²⁰ Unified federal list of organisations (including foreign and international organisations) designated as terrorist under the legislation of the Russian Federation, see: *Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими (на 4 апреля 2026 г.)*, Федеральная служба безопасности Российской Федерации (*Yedinyy federal'nyy spisok organizatsiy, v tom chisle inostrannykh i mezhdunarodnykh organizatsiy, priznannykh v sootvet-stvii s zakonodatel'stvom Rossiyskoy Federatsii terroristicheskimi (na 4 aprelya 2026 g.)*), Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii), <http://www.fsb.ru/fsb/npd/terror.htm> [accessed: 20 IV 2026].

²¹ A. Wilk, W. Konończuk, *Ukrainian-Russian war under the banner of anti-terrorist operation*, Ośrodek Studiów Wschodnich, 6 VIII 2014, <https://www.osw.waw.pl/en/publikacje/analyses/2014-08-06/ukrainian-russian-war-under-banner-anti-terrorist-operation> [accessed: 19 I 2026].

the RF repeatedly suffers the consequences of its anti-terrorist activities²², as it becomes a target of terrorist groups²³.

After the collapse of the Soviet Union, the highest concentration of terrorist attacks on the RF territory was recorded in the North Caucasus, especially in Chechnya, Dagestan and Ingushetia. These areas have long been major centres of activity for Islamist and separatist groups. Although North Ossetia was the site of one of the most tragic terrorist attacks in Russia's history, its significance in contemporary attack statistics is smaller than that of other Caucasian republics²⁴. As recently as 2012, before the series of attacks in Western Europe, including in France, Great Britain, Belgium and Germany, the terrorist conflict in the North Caucasus was regarded as the most brutal of its kind in Europe. During this period, around 700–800 people were killed each year in clashes between the RF forces and militants described by the Russian authorities as terrorists²⁵. Furthermore, between 1992 and 2011, 1415 terrorist attacks linked to groups operating in the North Caucasus were recorded in Russia. The highest number of incidents occurred in Chechnya, Dagestan and Ingushetia, which confirms that terrorist threat is concentrated in that region. Some of the attacks were also carried out in Moscow and Saint Petersburg, among other places.

²² J. Flanagan, *Bloodshed and retreat from Mozambique for Putin's private army the Wagner Group*, The Times, 25 XI 2019, <https://www.thetimes.com/uk/politics/article/bloodshed-and-retreat-from-mozambique-for-putin-s-private-army-the-wagner-group-696tnpzqh> [accessed: 19 I 2026].

²³ *The Deadliest Attacks In Russia*, Radio Free Europe/Radio Liberty, <https://www.rferl.org/a/russia-timeline-terror-attacks/28410225.html> [accessed: 19 I 2026].

²⁴ *IntelBrief: Radicalization and Extremism in Russia's North Caucasus Region*, The Soufan Center, 12 IV 2024, <https://thesoufancenter.org/intelbrief-2024-april-12/> [accessed: 26 X 2025]; M. Bartosiewicz, *Increasing radicalisation: terrorist attacks in Dagestan*, Ośrodek Studiów Wschodnich, 25 VI 2024, <https://www.osw.waw.pl/en/publikacje/analyses/2024-06-25/increasing-radicalisation-terrorist-attacks-dagestan> [accessed: 26 X 2025]; T. Grabowski, *Terroryzm północnokaukaski: przejawy zjawiska* (Eng. Terrorism in the North Caucasus: manifestations of the phenomenon), "Res Politicae" 2014, vol. VI, pp. 59–78. <http://dx.doi.org/10.16926/rp.2014.06.04>; M. Johns, *Terrorism and the North Caucasus: An Overview*, "START Background Report", National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, April 2013, pp. 1–5, https://www.academia.edu/8490735/Terrorism_and_the_North_Caucasus_An_Overview [accessed: 16 VI 2026].

²⁵ T.W. Grabowski, *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku* (Eng. Terrorism in the North Caucasus. Sources, manifestations and counter-terrorism measures), Kraków 2017, p. 7.

The RF's experience of Islamist terrorism is long-standing and systemic. Since the war in Afghanistan (1979–1989), through the Chechen conflicts, right up to its involvement in Syria, Moscow has remained one of the main opponents of jihadist groups. As a result, Russia has been the target of numerous attacks, culminating in incidents carried out at the theatre in Dubrovka (2002), at the school in Beslan (2004), as well as at the Crocus City Hall (2024). At the same time, it should be emphasised that, despite being aware of the threat, the Russian security apparatus has limited capacity to neutralise it effectively²⁶, particularly while stretched by the war against Ukraine.

Since the 1990s, Russian 'war on terrorism' in Chechnya has not been merely an internal affair, but part of its foreign policy strategy. Following the attacks on 11 September 2001, the RF sought to frame its actions in the Caucasus within the global narrative of the fight against terrorism, capitalising on a temporary convergence of interests with the United States, particularly in the context of the operations in Afghanistan and the US military presence in Central Asia²⁷. Russia's relations with Europe remained strained due to criticism of human rights abuses in Chechnya, refusals to extradite suspects and accusations of interference in the countries of the former Soviet Union, which gradually reduced the scope for cooperation. Russia instrumentalised the anti-terrorist narrative, subordinating it to political interests. It opposed the growth of the US influence in many regions of the world. At the same time, it pointed to the discrepancy between the need to consistently combat terrorism declared by Washington and the diverse approach of the US to individual countries and organisations, including in the context of Afghanistan, Iran, Syria, Hezbollah and Hamas. In Russian narrative, this was intended to support the argument that the US applied double standards, whereby whether a particular entity was classified as a terrorist organisation or as a political partner depended not only on its methods but also on the current interests of the US and its allies. This allowed Moscow to undermine the credibility of the US and weaken the real dimension of cooperation

²⁶ J. de Glinasty, *Moscow Attack: Russia Confronts Islamist Terrorism*, Institut de Relations Internationales et Stratégiques, 26 III 2024, <https://www.iris-france.org/en/184928-moscow-attack-russia-confronts-islamist-terrorism/> [accessed: 21 III 2026].

²⁷ M. McFaul, *U.S. Russia Relations After September 11, 2001*, Carnegie Endowment for International Peace, 24 X 2001, <https://carnegieendowment.org/posts/2001/10/us-russia-relations-after-september-11-2001?lang=en> [accessed: 21 III 2026].

with the West in the fight against terrorism. Between 2001 and 2022, Russia consistently combined criticism of Western 'double standards' in the fight against terrorism with attempts to legitimise its own security policy, including activities carrying out in the North Caucasus, Syria and in other regions recognised by Moscow as important to its interests²⁸. It is currently continuing to balance political efforts in the field of counterterrorism policy with military involvement in counterterrorism operations in Russia and worldwide.

For many years, Chechen separatists were portrayed by the Russian authorities as the most serious terrorist threat for the RF. In some of the English-language literature they were referred to, among other things, as Chechen Rebels or Chechen Separatist Movement²⁹. Between 1999 and 2013, structures originating from this movement were responsible for most terrorist attacks carried out on the RF's territory, however, their activity gradually decreased considerably over time. A new phase of North Caucasian terrorism began with the establishment, on 31 October 2007, of another terrorist organisation founded by Doku Umarov, one of the leaders of the North Caucasian insurgency. He renounced his position as the President of the Chechen Republic of Ichkeria, and proclaimed the creation of the Caucasus Emirate³⁰ – an Islamist, self-proclaimed organisational structure that for many years served as the principal terrorist base in the North Caucasus region.

The process of forming armed terrorist structures in the North Caucasus began as early as 1999. The local jamaats operating at that time in Dagestan, Ingushetia, Kabardino-Balkaria, Karachay-Cherkessia and North Ossetia became in the following years the organisational and personnel

²⁸ I. Oldberg, *The War on Terrorism in Russian Foreign Policy*, FOI – Swedish Defence Research Agency, Defence Analysis, Stockholm 2006.

²⁹ P. Bhattacharji, *Chechen Terrorism (Russia, Chechnya, Separatist)*, Council on Foreign Relations, 8 IV 2010, <https://www.cfr.org/backgrounders/chechen-terrorism-russia-chechnya-separatist> [accessed: 20 III 2026]; T. Grabowski, *Terroryzm północnokaukaski: przejawy zjawiska...*

³⁰ *The North Caucasus: The Challenges of Integration (II), Islam, the Insurgency and Counter-Insurgency*, Europe Report N°221, 19 X 2012; *Caucasus Emirate*, START – National Consortium for the Study of Terrorism and Responses to Terrorism, January 2015, <https://www.start.umd.edu/baad/narratives/caucasus-emirate.html> [accessed: 19 I 2026]; B. Roggio, *Doku Umarov declares Islamic Caucasus Emirate*, Long War Journal, 26 XI 2007, https://www.longwarjournal.org/archives/2007/11/doku_umarov_declares.php [accessed: 19 I 2026].

base for the Caucasus Emirate, formally announced in 2007³¹. In December 2009, the Supreme Court of the Russian Federation banned the Caucasus Emirate's activity, considering it to be a terrorist organisation. From that moment on, the Caucasus Emirate became one of the main sources of terrorist threat related to North Caucasus and one of the significant challenges for Russian anti-terrorist system³².

The growing influence of the so-called Islamic State (Islamic State of Iraq and Syria, ISIS) has had a direct impact on the security situation in Russian North Caucasus. In this context, ISIS should be regarded first and foremost as a terrorist organisation, even though its activities were based on an extremist ideology, radical propaganda and international recruitment networks. Hundreds of militants left the region to join the armed conflict in Syria and Iraq, and among the foreign fighters serving in the ranks of ISIS and other jihadist organisations, a significant proportion were citizens of the RF, many of whom originated from the North Caucasus. This process weakened the Caucasus Emirate and limited its recruiting opportunities. This led to the fragmentation of this organisation, as some commanders and militants pledged allegiance to ISIS, while others continued their activities in the region under its banner³³. As a result, in the North Caucasus, the remnants of the Caucasus Emirate and new groups linked to Islamic State began to coexist – often in a competitive environment – which meant that the nature of the threat shifted from a local, Caucasian perspective to a transnational one.

After 2014, the structures of the Caucasus Emirate began to break down. This was a consequence of both the intensified activities of Russian security services and deep internal divisions within the community of the Caucasian jihadist groups. An important factor weakening the group's position was

³¹ T.W. Grabowski, *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku...*, p. 159.

³² J. Sinai, *The Terrorist Threats Against Russia and its Counterterrorism Response Measures*, "Connections: The Quarterly Journal" 2015, vol. 14, no. 4, pp. 95–101, <http://dx.doi.org/10.11610/Connections.14.4.08>; M. Falkowski, *The Islamic State in the Caucasus – who benefits?*, Ośrodek Studiów Wschodnich, 14 I 2015, <https://www.osw.waw.pl/en/publikacje/analyses/2015-01-14/islamic-state-caucasus-who-benefits> [accessed: 12 III 2026]; M. Youngman, C. Moore, *Guide: The Caucasus Emirate*, Radicalisation Research, 9 XI 2017, <https://radicalisationresearch.org/research/youngman-guide-caucasus-emirate/> [accessed: 12 III 2026].

³³ M. Ter, *The Caucasus Emirate, the Other Russian Front*, https://www.cidob.org/sites/default/files/2024-07/NOTES%20129_TER_ANG.pdf [accessed: 16 VI 2026].

the disloyalty of some of its commanders and militants, who pledged allegiance to ISIS between 2014 and 2015. This led to the subordination of some Caucasian structures to the Islamic State. ISIS gradually assumed the role of the dominant ideological and organisational centre for radical circles originating from the North Caucasus³⁴. As a result, the Caucasus Emirate lost its ability to independently set the direction of its activities and coordinate operations on a large scale in Russia and the autonomous republics. It gave way to a stronger organisation linked to ISIS.

The Islamic State Caucasus Province (Wilayat al-Qawqaz), established in June 2015, emerged as a significant actor in Russia's terrorist threat landscape in the subsequent years, drawing on part of the former Caucasus Emirate's cadre base and organisational infrastructure. This was a consequence of the mass oaths of allegiance to the Islamic State by the leaders of local jamaats. This process led to the absorption by the structures of ISIS of a significant number of the existing supporters of the Caucasus Emirate, and at the same time to the internal fragmentation of the armed environment in the North Caucasus. The result was a temporary decline in the operational activity of jihadist groups and a fall in the number of attacks between 2014 and 2015 in republics such as Dagestan and Ingushetia. It is estimated that during the Syrian conflict, around 2800 fighters from the countries of the former Soviet Union joined the fighting in the ranks of ISIS³⁵, including people from the North Caucasus region and Central Asian countries. This led to the gradual disintegration of the Caucasus Emirate and the takeover of its personnel and infrastructure by the structures of ISIS, primarily the Islamic State Caucasus Province³⁶, which has become a main hub of jihadist activity in the North Caucasus since 2015.

Thus, the activity of ISIS has been one of the greatest challenges for the Russian security apparatus, primarily due to the vulnerability of some

³⁴ *The North Caucasus Insurgency and Syria: An Exported Jihad?*, International Crisis Group, 16 III 2016, <https://www.crisisgroup.org/europe-central-asia/russia-internal-syria/238-north-caucasus-insurgency-and-syria-exported-jihad> [accessed: 19 I 2026].

³⁵ F. Hanoush, *Fighters from the Caucasus Join ISIS to Fight Russia*, Atlantic Council, 14 IX 2016, <https://www.atlanticcouncil.org/blogs/syriasource/fighters-from-the-caucasus-join-isis-to-fight-russia/> [accessed: 21 III 2026].

³⁶ M. Vatchagaev, *Caucasus Emirate and Islamic State Split Slows Militant Activities in North Caucasus*, Jamestown, 14 II 2015, <https://jamestown.org/program/caucasus-emirate-and-islamic-state-split-slows-militant-activities-in-north-caucasus-2/> [accessed: 20 I 2026].

regions of the North Caucasus to the development of terrorism. The ideas of global jihad and the establishment of a caliphate found supporters there even before the formal emergence of ISIS structures. The turning point came in 2015, when the organisation openly declared jihad against the RF. This decision was directly linked to the involvement of Russian military forces in Syria on the side of Bashar al-Assad's regime, which led to Russia being designated as a priority target of ISIS. This was accompanied by numerous propaganda, recruitment and terrorist activities.

The Kremlin responded by strengthening the capacities of the security apparatus, which on the one hand increased state control, but on the other could exacerbate social and political tensions³⁷.

In 2015, the threat of terrorism in Russia increased significantly, not only from militants of Chechen, Dagestani and, more broadly, North Caucasian origin fighting for independence, but also from other terrorist organisations. When, in September 2015, Russia launched a military offensive against rebel groups in Syria, a splinter faction of Al-Qaeda – al-Nusra Front (Jabhat al-Nusra) organisation responded³⁸. The leader of terrorist group, Abu Muhammad al-Julani, subsequently called for retaliatory attacks against Russian citizens in Syria. The reaction from the terrorist organisation's supporters was almost immediate – on 13 October 2015, two missiles struck the Russian embassy in Damascus³⁹. Thus, the terrorist groups in Africa and the Middle East have intensified their activities against the RF⁴⁰.

It is worth noting that, according to estimates from December 2015, Russian citizens accounted for approx. 8% of all foreign fighters who,

³⁷ A.M. Dyner, *Terrorists Kill at least 137 at Moscow Concert Hall*, Polski Instytut Spraw Międzynarodowych, 25 III 2024, <https://pism.pl/publications/terrorists-kill-at-least-137-at-moscow-concert-hall> [accessed: 19 I 2026].

³⁸ J. Beslin, M. Ignjatijevic, *Balkan foreign fighters: from Syria to Ukraine*, "Brief" 2017, no. 20, pp. 1–4.

³⁹ *Al-Qaeda in Syria calls for revenge attacks on Russia*, The Washington Post, 13 X 2015, https://www.washingtonpost.com/world/middle_east/al-qaeda-in-syria-calls-for-revenge-attacks-on-russia/2015/10/13/b7f7dfdf-a0a4-451d-bd2e-180f2f4882f5_story.html [accessed: 16 V 2026]; *Syria crisis: Rockets hit Russian embassy compound in Damascus, reports say*, ABC News, 13 X 2015, <https://www.abc.net.au/news/2015-10-13/rockets-hit-russian-embassy-compound-in-damascus-reports/6851968> [accessed: 16 V 2026].

⁴⁰ A.K. Olech, *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku* (Eng. Terrorist attacks in the Russian Federation in the 21st century), "Nowa Polityka Wschodnia" 2019, no. 4, pp. 110–115. <https://doi.org/10.15804/NPW20192306>.

during the Syrian conflict, travelled to Syria and Iraq to join ISIS and other jihadist organisations. The number of Russian volunteers was estimated at around 2400 individuals (as of September 2015), while overall scale of the phenomenon was assessed at 27 000–31 000 departures from at least 86 countries⁴¹. This confirms the significant presence of Russian nationals among foreign fighters.

Another example of the escalation of terrorist activity directed against the RF after the start of its military intervention in Syria was the bombing of a Russian passenger aircraft flying from Sharm el-Sheikh to Saint Petersburg. On 31 October 2015, an explosive device detonated on board an aircraft operated by airline Metrojet, killing a total of 224 people (217 passengers and 7 crew members). The majority of the victims were Russians, except for three Ukrainian passengers and one from Belarus. ISIS structures claimed responsibility for the attack, describing it as a direct retaliation for the Russian military intervention in Syria⁴². This demonstrates that Russia's involvement in the Middle East led to an intensification of the terrorist threat beyond the North Caucasus region, with Russian citizens also being targeted outside the country.

The Islamic State Caucasus Province claimed responsibility for an attack on Russian military facility in southern Dagestan carried out on 2 September 2015. However, this information was not independently confirmed. In a recording published by a Russian-language ISIS media outlet, the leader of the Dagestani structures of the Caucasus Province, Furat Media Abu Mukhammad Kadarsky (Rustam Asilderov), called on the organization's supporters to carry out the fight in the Caucasus instead of traveling to Syria⁴³. He argued that taking action in the region would be more effective than travelling to the Middle East to support ISIS structures in Iraq and Syria. This was an example of propaganda aimed at mobilising

⁴¹ *Foreign Fighters. An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq*, December 2015, https://thesoufancenter.org/wp-content/uploads/2017/05/TSG_ForeignFightersUpdate_format-for-print-120915-REBRAND-031317.pdf [accessed: 21 I 2026].

⁴² Z. Gold, *Wilayat Sinai Risks Backlash After Metrojet Bombing*, <https://ctc westpoint.edu/wp-content/uploads/2015/12/CTCSentinel-Vol8Iss118.pdf>, pp. 19–22 [accessed: 19 I 2026]; D. Costa-Roberts, *Questions swirl over Russian plane crash in Egypt that killed 224*, PBS News, 1 XI 2015, <https://www.pbs.org/newshour/world/details-emerge-case-downed-russian-jet> [accessed: 20 I 2026].

⁴³ J. Paraszczuk, *IS's North Caucasus Affiliate Calls for Recruits to Join It in Daghestan*, Radio Free Europe/Radio Liberty, 3 X 2015, <https://www.rferl.org/a/islamic-state-north-caucasus-affiliate-call-for-recruits-daghestan/27285024.html> [accessed: 16 V 2026].

supporters to take action in their country of residence, without having to travel to areas of armed conflict.

Another group operating against the RF was the Imam Shamil Battalion (Katibat Imam Shamil), affiliated with Al-Qaeda, which referred to itself as the 'Knights of Islam'. The group claimed responsibility for a suicide bombing carried out on 3 April 2017, in the Saint Petersburg metro, between the Sennaya Ploshchad and Tekhnologichesky Institut stations. As a result of the attack, 15 people were killed and several dozen were injured. A second explosive device was discovered and defused at another metro station. In connection with the attack, Russian authorities detained 11 individuals originating from Central Asia⁴⁴. These events demonstrate the importance of transnational jihadist networks and their capacity to conduct and inspire terrorist actions within the territory of the RF.

Between 2015 and 2022, Russia faced the threat of terrorist attacks concentrated in the North Caucasus. These were mainly carried out by jihadist groups linked to the Islamic State Caucasus Province, which had taken over part of the personnel and structures of the former Caucasus Emirate. The attacks most often took the form of targeted strikes and, importantly, were directed against security service officers, local government representatives and religious institutions⁴⁵.

The Russian language has become the third most popular language of ISIS propaganda (after Arabic and English), and the Russian intervention in Syria was a factor that may have further strengthened the influence of radical groups in Russia – both ISIS itself and other radical and jihadist circles⁴⁶. It can be concluded from this that, due to the increased activity of terrorist organisations and radical circles within Russia and in neighbouring countries, the Russian language has begun to play a significant role in transnational propaganda and recruitment communications amongst jihadist circles.

⁴⁴ A.K. Olech, *Ataki terrorystyczne...*, pp. 109–129.

⁴⁵ M.S. Stempień, *The evolution of terrorism in Russia in the years 2015–2022. Quantitative analysis of the phenomenon*, "Przegląd Wschodnioeuropejski" 2023, no.14, pp. 185–199. <https://doi.org/10.31648/pw.9711>.

⁴⁶ A. Borshchevskaya, *Russian Officials Inadvertently Aid Radical Islamists in Russia*, The Washington Institute for Near East Policy, 31 XII 2015, <https://www.washingtoninstitute.org/policy-analysis/russian-officials-inadvertently-aid-radical-islamists-russia> [accessed: 22 I 2026].

Since 2020, the activities of the Islamic State Khorasan Province (ISIS-K) – a regional ISIS structure operating primarily in Afghanistan and Central Asia – have been gaining increasing prominence in Russia. The organisation gradually took the lead in planning and instigating attacks aimed at Russia. This group operates differently from previous North Caucasian groups. This applies both to its modus operandi and to its recruitment, which relies heavily on economic migrants from Tajikistan, Uzbekistan and Kyrgyzstan, functioning on the margins of Russian society. It was precisely these circles that became a recruitment base for the organisation. They are susceptible to radicalisation in situations of discrimination, repression and disinformation in Russia. There are also international structures, and even global terrorist organisations, operating in the RF⁴⁷. From this perspective, it is not possible to neutralise the threat solely through the use of brutal methods or the deployment of specialised counter-terrorism units – that is, the procedures employed to date by the Kremlin.

It should be noted that, across the wider region of Central Asia and Afghanistan, activities of ISIS-K have been gradually increasing since 2020, culminating in the attack in Russia on 22 March 2024, in which 144 people were killed and 551 were injured. It was not only one of the largest demonstrations of ISIS-K's capabilities in Russia⁴⁸, but also one of the largest terrorist attacks on a global scale. ISIS-K carried out the attack at the Crocus City Hall in the Krasnogorsk area in the Moscow Oblast. Just one day after the attack, the National Antiterrorism Committee announced that 11 suspects had been arrested⁴⁹. Among the key motives behind the perpetrators' actions, it should be noted that activities of ISIS-K were a response to Russia's closer cooperation with the Taliban⁵⁰, as well as to military operations in Syria and the Sahel against the Islamic State⁵¹.

⁴⁷ IntelBrief: *Radicalization and Extremism in Russia's...*

⁴⁸ K. Strachota, *Islamic State-Khorasan: global jihad's new front*, 29 III 2024, Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-03-29/islamic-state-khorasan-global-jihads-new-front> [accessed: 20 I 2026].

⁴⁹ *Global Terrorism Index 2025*, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf> [accessed: 22 I 2026]; A.M. Dwyer, *Terrorists Kill...*

⁵⁰ M.N. Katz, *No, Putin, the ISIS-K attack in Moscow wasn't about Ukraine*, Atlantic Council, 29 III 2024, <https://www.atlanticcouncil.org/blogs/menasource/isis-k-putin-moscow-al-qaeda/> [accessed: 20 I 2026].

⁵¹ A. Olech, *The Wagner Group in Africa. The sham battle of Russian mercenaries against terrorism*,

In the context of the attack at the Crocus City Hall, Russia was to have received information about planned attacks on concert halls in Moscow from the security services of other countries, friendly countries (Iran) and hostile countries (the US⁵²). The limited response from the Russian authorities may suggest that they either did not have sufficient knowledge of the threat or did not attach sufficient importance to the warning signs. Russian security services may therefore not have completely ruled out the possibility of a threat, but rather misjudged its likelihood, scale or urgency. It is also possible that their attention was focused on other priorities at the time, including operations being carried out abroad.

The Royal United Service Institute indicates that the state apparatus, led by the FSB, prioritised political and social challenges relating to the Russian operation against Ukraine. Terrorism was not a priority. Even immediately after the attack itself, it was assumed that Western intelligence services (led by American and British ones) and Ukraine were responsible for it. Another important aspect is radicalisation in Russia itself, also among migrants from Tajikistan and Uzbekistan. In 2024, there were five attacks in Russia, neither of which was previously detected⁵³. For a country that has been grappling with terrorism for decades, such serious shortcomings point to a lack of capacity to respond, a shortage of resources (including specialist officers), a failure to treat terrorism as a priority, and a significant focus on the war with Ukraine.

Also in 2024, a terrorist attack took place in Dagestan on Russian territory, where armed assailants carried out coordinated attacks on Orthodox churches, synagogues and police stations in the cities of Derbent and Makhachkala⁵⁴. As a result of these attacks, which the authorities have described as terrorist attacks, at least 20 people were killed, including officers of security services and clergy, and more than 40 were injured. Russian services did not confirm the identities of the perpetrators. Some information indicates that they cooperated with organisations associated with ISIS, including with the Islamic State Caucasus Province, but also ISIS-K

"Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 273–309. <https://doi.org/10.4467/27204383TER.24.010.19398>.

⁵² *On the Terrorist Attack at the Crocus City Hall in Moscow*, U.S. Mission to the Organization for Security and Cooperation in Europe, 11 IV 2024, <https://osce.usmission.gov/on-the-terrorist-attack-at-the-crocus-city-hall-in-moscow/> [accessed: 20 III 2026].

⁵³ E. Ferris, *How Russia's War in Ukraine...*

⁵⁴ M. Bartosiewicz, *Postępująca radykalizacja. Ataki terrorystyczne w Dagestanie...*

provided media support. Importantly, Russian authorities constructed a narrative alleging that Western or Ukrainian organisations were involved in instigating and supporting terrorist attacks.

The FSB is currently publishing 'Unified federal list of organizations, including foreign and international organizations, recognized as terrorist in accordance with the legislation of the Russian Federation'. It covers 70 entities, including foreign and international organisations, as well as local and regional structures⁵⁵ operating within the RF.

Although the Central Spiritual Administration of the Muslims of Russia, one of the nationwide Russian organisations representing Muslim communities in the RF, repeatedly and publicly condemned terrorism and extremist ideologies as actions contrary to the principles of Islam, acts of violence were nevertheless carried out within the territory of the Russian Federation by individuals claiming affiliation with this religion. In response to the 2010 Moscow Metro bombings, Russia's Supreme Mufti, Talgat Tadzhuddin, emphasised that Muslim communities in Russia unequivocally condemned the perpetrators of terrorist attacks. He stated that such acts have no religious justification and are contrary to the teachings of Islam⁵⁶. In the following years, official Muslim institutions in the RF continued to maintain a critical stance toward religiously motivated terrorism and violence, emphasising that terrorist acts should not be equated with Muslim communities⁵⁷.

Due to the international involvement of the RF, terrorist threats in Africa should also be taken into account. Russia declares that its counterterrorism efforts are focused primarily on the Sahel states, particularly in Mali, where the fight against terrorism serves as one of the main justifications for the presence of Russian military forces and mercenaries. In practice, however, this activity also serves broader political, economic and military objectives, including the maintenance of influence and access to natural resources.

⁵⁵ *Единый федеральный список организаций...*

⁵⁶ *Peaceful Muslims have no relation to extremists – supreme mufti of Russia*, Pravmir, 30 XII 2013, <https://www.pravmir.com/peaceful-muslims-have-no-relation-to-extremists-supreme-mufti-of-russia/> [accessed: 21 I 2026].

⁵⁷ B. Vitkine, *Russia faces wave of Islamophobia after Moscow attacks*, Le Monde, 30 III 2024, https://www.lemonde.fr/en/international/article/2024/03/30/russia-faces-wave-of-islamophobia-after-moscow-attacks_6666864_4.html [accessed: 20 I 2026].

Russia's antiterrorist policy in Africa is presented as a response to the activities of many jihadist groups operating on the continent. These include, among others: the Group for the Support of Islam and Muslims (Jama'at Nusrat al-Islam wal-Muslimin, JNIM), the Islamic State Sahel Province (IS Sahel, ISSP), the Islamic State West Africa Province (ISWAP), as well as Islamic State structures in Mozambique, also referred to as Ansar al-Sunna/Ahl al-Sunna. In the context of Central Africa, the Allied Democratic Forces (ADF) and Islamic State structures in the Democratic Republic of the Congo (ISIS-DRC), related to the Islamic State Central Africa Province (ISCAP) should also be mentioned. In the Russian narrative on security, they are portrayed as a threat that justifies Moscow's continued military and political presence in certain African countries⁵⁸.

It is therefore important to analyse with particular care the actions taken by terrorists against Russia, especially in Mali, Burkina Faso, Niger, Mozambique, Libya or the Central African Republic. If Russia were to decide to build its bases in any of these countries, continue expanding the presence of the Wagner Group⁵⁹ or the African Corps⁶⁰, attempt to maintain infrastructure in Syria, and begin constructing additional bases, it would certainly have to commit additional troops and resources to counterterrorism efforts both in Russia and the Caucasus, as well as in Africa and the Middle East. This will require additional, unforeseen and significant investments, along with a reallocation of resources, including funds currently allocated to the war in Ukraine.

The Kremlin will have to decide how important it is to establish new military bases on the African continent in the context of further fighting against terrorists and the difficulties associated with conducting

⁵⁸ A. Olech, *The Wagner Group in Africa...*

⁵⁹ A. Olech, *Rosyjscy najemnicy – raport z działalności w Afryce* (Eng. Russian mercenaries – report on activities in Africa), Defence24, 8 IV 2024, <https://defence24.pl/geopolityka/rosyjscy-najemnicy-raport-z-dzialalnosci-w-afryce> [accessed: 22 I 2026].

⁶⁰ After the death of Yevgeny Prigozhin in 2023, Russian paramilitary presence of mercenaries in Africa was gradually reorganised and brought under the control of state-run structures, primarily the Africa Corps, which is linked to the Russian Ministry of Defence. In practice, this meant the partial takeover or replacement of the functions previously carried out by the Wagner Group in countries such as Mali, Burkina Faso, Niger, Libya and the Central African Republic. See: F. Bryjka, J. Czerep, *Africa Corps – a New Iteration of Russia's Old Military Presence in Africa*, Polski Instytut Spraw Międzynarodowych, 29 V 2024, <https://www.pism.pl/publikacje/africa-corps-a-new-iteration-of-russias-old-military-presence-in-africa> [accessed: 22 I 2026].

operations and training. So far, Russian mercenaries in Africa – who are, after all, most often regular soldiers of the Russian army – have been losing this confrontation with terrorists and have proven unable to effectively oppose them. This scenario occurred in Mozambique, the Central African Republic, and now in Mali and Burkina Faso. Due to the difficulties involved in combating terrorist groups, Russia cannot afford to build military bases, as they would automatically become targets for terrorist groups, including jihadist organisations. Therefore, it must select locations for new investments with great caution and in close cooperation with the governments of African countries.

The Russian Federation, in the context of current security challenges, carried out attacks and the influence of terrorism on the functioning of the state, remains among the countries particularly exposed to terrorist threats. In the Global Terrorism Index 2025 report, Russia was ranked 17th in the world (moving up 20 places compared with the 2024 report), and in the Global Terrorism Index 2026 report – 16th. The rise in the country's ranking in 2025 and staying in the top twenty in 2026 are a consequence of increased terrorist activity within the country, including successful attacks with a significant impact on society. Russia, conducting a full-scale military operation against Ukraine and engaging militarily in Africa under the slogan of combating terrorism, is simultaneously increasing its vulnerability to such threats and becoming a target of retaliatory actions by terrorist groups⁶¹.

The data presented in Table 1 shows that the high level of terrorist impact in the years 2020–2025 in countries, such as Somalia, Syria, Mali, Burkina Faso, Niger, Mozambique, Libya, the Central African Republic and Sudan, persists despite the presence or involvement of the RF. At the same time, in countries cooperating with Moscow at political and military level, such as Egypt, Algeria, Serbia and Eritrea, there is no clear improvement in the security situation. In practice, this means that Russian activity – both in the Sahel countries and in Libya, the Central African Republic, Mozambique and Sudan – does not lead to the elimination of terrorism, but rather fits into a mechanism maintaining an environment of instability, that enables governments or juntas to become dependent on external support⁶². As a result, Russia functions as a beneficiary of prolonged

⁶¹ *Global Terrorism Index 2025...; Global Terrorism Index 2026...*

⁶² See: A. Arieff et al., *Russia's Security Operations in Africa*, Congressional Research Service,

chaos, in which terrorism remains an element of cooperation enabling and justifying its continued presence, rather than a problem that Moscow will resolve at systemic level.

Table 1. The ranking of the selected countries between 2021 and 2025 in terms of the impact of terrorist threats on their functioning according to the Global Terrorism Index (1 – the greatest impact, 100 – the least impact).

Country	Place in the world				
	2021	2022	2023	2024	2025
Egypt	15	16	20	29	32
Eritrea	93*	93*	89*	100*	100*
Mozambique	13	12	15	17	15
Central African Republic	93*	55	59	71	76
Somalia	3	3	7	7	7
Sudan	86	93*	89*	100* (engulfed in war)	100* (engulfed in war)
Syria	5	5	5	3	6
Mali	7	4	3	4	5
Burkina Faso	4	2	1	1	2
Niger	8	10	10	5	3
Libya	26	32	39	53	59
Algeria	39	37	44	42	47
Serbia	93	93	89	82	66

* Last place in the report

Source: own elaboration based on: *Global Terrorism Index 2022*, <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf>, pp. 8–9 [accessed: 22 I 2026]; *Global Terrorism Index 2023*, <https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf>, pp. 8–9 [accessed: 22 I 2026]; *Global Terrorism Index 2024*, <https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf>, pp. 6–7 [accessed: 22 I 2026]; *Global Terrorism Index 2025*, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>, pp. 6–7 [accessed: 22 I 2026]; *Global Terrorism Index 2026*, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/GTI-2026-web-04112026.pdf>, pp. 8–9 [accessed: 22 I 2026].

8 IV 2026, <https://www.congress.gov/crs-product/IF12389> [accessed: 12 IV 2026].

www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf, pp. 6–7 [accessed: 13 IV 2026].

Terrorist threats to the Member States of the Collective Security Treaty Organisation

There is a risk that terrorist organisations from the Caucasus will attempt to carry out terrorist attacks not only in Russia, but also in the CSTO member states. Operations of terrorist organisations also have a criminal character, as they continuously cooperate with criminal groups. In order to obtain funds to sustain their activities, these organisations are involved in, among others, international drug trafficking, kidnappings or arms sales. Consequently, the use of the territories of the CSTO member states to carry out illegal activities, such as by establishing a Europe–Asia trade route, poses a huge threat to security in the region. Furthermore, the ongoing operations in Syria, and the unstable situation in the southern part of the country, mean that the RF must monitor conflict regions while also ensuring that border security in the CSTO member states is not neglected.

Attention should be paid to the threat posed by Afghanistan. Tajikistan, the CSTO Member State bordering it, reported threats related to terrorism from its southern border. This was due to the unstable situation in Afghanistan, and the lack of security at border crossings. It should be added that, after 2022, the Central Asian countries significantly changed their policy towards Kabul. On the one hand, the risks are recognised, but on the other, the main factor influencing the development of Afghanistan's relations with Kazakhstan, Uzbekistan, Turkmenistan, Tajikistan and Kyrgyzstan is precisely Russia. In addition to the above, Moscow seeks to oversee cooperation and projects carried out by Central Asia countries, preventing them from strengthening their independence, and at the same time presents itself as a guarantor of security⁶³, even though it faces its greatest challenges in the fight against terrorism (Table 2).

⁶³ D. Zielińska, *Pragmatism beyond divides: Central Asia's engagement with Afghanistan*, Ośrodek Studiów Wschodnich, 7 XI 2025, <https://www.osw.waw.pl/en/publikacje/analyses/2025-11-07/pragmatism-beyond-divides-central-asias-engagement-afghanistan> [accessed: 12 I 2026].

Table 2. The ranking of the selected CSTO countries and Afghanistan between 2021 and 2025 in terms of the impact of terrorist threats on their functioning according to the Global Terrorism Index (1 – the greatest impact, 100 – the least impact).

Country	Place in the world				
	2021	2022	2023	2024	2025
Armenia	93*	93*	76	79	81
Belarus	93*	93*	89*	90	94
Kazakhstan	93*	93*	89*	100*	100*
Kyrgyzstan	93*	93*	89*	100*	100*
Russia	44	45	35	16	17
Tajikistan	47	50	69	70	41
Afghanistan	1	1	6	9	11

* Last place in the report

Source: own elaboration based on: *Global Terrorism Index 2022*, <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf>, pp. 8–9 [accessed: 22 I 2026]; *Global Terrorism Index 2023*, <https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf>, pp. 8–9 [accessed: 22 I 2026]; *Global Terrorism Index 2024*, <https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf>, pp. 6–7 [accessed: 22 I 2026]; *Global Terrorism Index 2025*, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>, pp. 6–7 [accessed: 22 I 2026]; *Global Terrorism Index 2026*, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf>, pp. 6–7 [accessed: 13 IV 2026].

The potential threat posed by lone actors or individuals who declare their affiliation with or loyalty to terrorist organisations⁶⁴ may currently constitute one of the most serious challenges to Russian government and CSTO countries. This is linked to the mass exodus of Russian citizens to the Middle East, their indoctrination, and subsequently their return to Russia and their engagement in terrorist activities. The exact number of such individuals is unknown, but the threat posed by returning fighters and those becoming radicalised on their own has been repeatedly highlighted as one of the problems facing Russian security system.

⁶⁴ B.M. Jenkins, *Stray Dogs and Virtual Armies. Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11*, RAND, 31 VIII 2011, https://www.rand.org/pubs/occasional_papers/OP343.html [accessed: 22 IV 2026].

The most important thing in this regard is to determine how (means, tools) and where an attack can be carried out. One of the main ways in which terrorists communicate and discuss specific targets is through social media and gaming platforms. They contain training materials, as well as resources designed to encourage and motivate people to attacks. This ensures that indoctrinated terrorists remain in constant contact with their superiors in Africa or in the Middle East. For this reason, verifying all the evidence and sources requires the ongoing involvement of Russian services. The Russian government takes into account similar threats arising from the ongoing migration and development of cyberterrorism.

For years, Russian security services have been carrying out preventative measures in the country's largest cities, aimed primarily at safeguarding public transport, areas with heavy traffic and mass events. This involves deploying police officers and soldiers to patrol the streets, as well as establishing zones of heightened checks, which will help to maintain security in critical areas of cities. Border controls and international cooperation are also important elements. Previous experiences of terrorist attacks on Russia's territory and repeated threats from terrorists are the basis for stepping up security measures. This is mainly due to the fact that terrorist organisations, e.g. Al-Qaeda and ISIS, continue to call, in their statements, for attacks to be carried out on the Russia's territory, and urge people to individual attacks⁶⁵. In view of the above, international engagement of the CSTO member states is essential to ensure that each member state implements similar methods and measures to combat terrorism. Common military initiatives and response to threats should consist of carrying out simultaneous actions and adopting a similar strategy in the implementation of counter-terrorism measures.

⁶⁵ A. Aji, B. Mroue, *Russian Embassy shelled in Syria as insurgents hit back*, Associated Press, 13 X 2015, <https://apnews.com/article/991656eab57d4aa79fbd5458af62b60e> [accessed: 21 III 2026]; T. Joscelyn, *Head of al Qaeda's Syrian branch threatens Russia in audio message*, Long War Journal, 13 X 2015, <https://www.longwarjournal.org/archives/2015/10/head-of-al-qaedas-syrian-branch-threatens-russia-in-audio-message.php> [accessed: 21 III 2026]; *ISIS video threatens attacks in Russia, Moscow*, Ahram Online, 12 XI 2015, <https://english.ahram.org.eg/News/165409.aspx> [accessed: 21 III 2026]; *Why is ISIS targeting Russia?*, Vision of Humanity, 25 III 2024, <https://www.visionofhumanity.org/why-is-isis-targeting-russia/> [accessed: 21 III 2026].

Working Group on the Fight against Terrorism and Extremism under the CSTO

A special organisational structure has been established within the CSTO – the Working Group on the Fight against Terrorism and Extremism (Russian: *Рабочая группа экспертов по вопросам борьбы с терроризмом и экстремизмом*), operating under the auspices of the Committee of Secretaries of Security Councils of the CSTO. Its main tasks include coordinating Member States' efforts to combat terrorism and extremism, identifying and analysing current and potential security threats, and formulating recommendations for joint preventive and operational measures. The Group performs an expert and advisory role, supporting the development of a common CSTO security policy, including by initiating the harmonisation of legal frameworks and institutional cooperation between member states in the field of countering terrorist and extremist threats⁶⁶.

As early as 2015, the CSTO countries were pointing to an increase in security threats linked to activities of the Islamic State and Al-Qaeda, particularly in the context of the unstable situation in Afghanistan⁶⁷. Particular importance was attached to the protection of the southern borders of the member states, above all the Tajik-Afghan border, which is regarded as one of the most vulnerable sections in terms of security terrorist, extremist and drug-related threats. The cooperation of the CSTO countries in this area was intended to strengthen border security, coordinate actions and develop the capabilities of the collective security system⁶⁸.

⁶⁶ *Меры по противодействию международному терроризму и экстремизму рассмотрены на заседании Комитета секретарей советов безопасности стран ОДКБ*, Национальный правовой Интернет-портал Республики Беларусь (*Mery po protivodeystviyu mezhdunarodnomuterrorizmu i ekstremizmu rassmotreny na zasedanii Komiteta sekretarey sovetov bezopasnosti stran ODKB*, Natsional'nyy pravovoy Internet-portal Respubliki Belarus'), 24 V 2018, <https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2018/may/28997/> [accessed: 22 I 2026].

⁶⁷ *Заявление глав государств-членов Организации Договора о Коллективной Безопасности о противодействии международному терроризму, 21 декабря 2015 года, г. Москва*, Организация Договора о коллективной безопасности (*Zayavleniye glav gosudarstv-chlenov Organizatsii Dogovora o Kollektivnoy Bezopasnosti o protivodeystvii mezhdunarodnomu terrorizmu, 21 dekabrya 2015 goda, g. Moskva*, Organizatsiya Dogovora o kolektivnoy bezopasnosti), 21 XII 2015, https://odkb-csto.org/documents/documents/zayavlenie_glav_gosudarstv_chlenov_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_o_protivodeystv/?sphrase_id=66457 [accessed: 10 III 2026].

⁶⁸ *В Астане состоялась сессия СКБ ОДКБ*, Организация Договора о коллективной безопасности (*V Astane sostoyalas' sessiya SKB ODKB*, Organizatsiya Dogovora okollektivnoy

According to representatives of the CSTO, it is precisely terrorism that significantly increases the likelihood of conflicts breaking out in various regions of the world, hinders the development of military activities – including those on the borders of CSTO's area of responsibility – and therefore requires a comprehensive and in-depth analysis, as well as joint efforts to counteract threats. The consolidation of efforts to promote global and regional security, including the exchange of information, joint exercises and shared priorities in the field of security, is one of the priorities of the CSTO⁶⁹.

During regular meetings, the Working Group on the Fight against Terrorism and Extremism draws up proposals to improve cooperation in organising joint operations to combat terrorism and extremism. It regularly updates the list of organisations recognised as terrorist and extremist in the CSTO member states. It also carries out activities aimed at improving the operational and combat training of the special forces units of the CSTO.

Between 2024 and 2025, under the CSTO, the existing priorities of the Working Group were maintained and developed, and adapted to the changing security environment. Particular emphasis was placed on countering terrorist and extremist activities involving the exploitation of disinformation and new technologies, including propaganda and recruitment carried out in cyberspace, combating transnational terrorist groups linked to cells in Afghanistan, and strengthening the protection of Member States' external borders (particularly along the Tajik-Afghan border), stepping up joint exercises and deepening of IT and legal cooperation between the CSTO states. At the same time, the importance of preventive measures – including educational programmes and efforts to counter radicalisation – was emphasised as an integral element of regionally strengthening collective security⁷⁰.

bezopasnosti), 28 XI 2024, https://odkb-csto.org/news/news_odkb/v-astane-sostoyalas-sessiya-skb-odkb/ [accessed: 22 I 2026].

⁶⁹ Генеральный секретарь ОДКБ Станислав Зась 4 сентября выступил на совместном заседании министров обороны СНГ, ШОС и ОДКБ, Организация Договора о коллективной безопасности (*General'nyy sekretar' ODKB Stanislav Zas' 4 sentyabryavystupil na sovmestnom zasedanii ministrov oborony SNG, SHOS IODKB, Organizatsiya Dogovora o kollektivnoy bezopasnosti*), https://odkb-csto.org/news/news_odkb/generalnyy-sekretar-odkb-stani-slav-zas-4-sentyabrya-vystupil-na-sovmestnom-zasedanii-ministrov-oboro/?sphrase_id=66458 [accessed: 11 III 2026].

⁷⁰ О. Keskin, *Лидеры стран ОДКБ выразили глубокую озабоченность эскалацией в зоне израильско-палестинского конфликта* (*Lidery stran ODKB vyrazili glubokuyu ozabochennost'eskalatsiyey v zone izrail'sko-palestinskogo konflik*), Anadolu Agency,

Russia's role remains a key issue in the fight against terrorism within the CSTO. Its counter-terrorism strategy is based on building cooperation both with the organisation's member states and with selected external partners. The Russian Federation was supported in its counter-terrorism efforts by, among others, the UN and China⁷¹. This means that Moscow will seek to develop counter-terrorism cooperation both within the CSTO and outside it. It may also turn out that, once the war in Ukraine is over, the narrative of the fight against terrorism will become one of the tools enabling Russia to make a partial return to the international stage.

At the same time, measures to protect the interests of the RF, which will be undertaken by the Kremlin as counter-terrorism measures, remain a priority, including within a broader jurisdiction, i.e. on the territory of all states belonging to the CSTO. This gives Russia the opportunity to maintain influence over CSTO Member States through cooperation between security services, the exchange of information, training and joint operations carried out under the banner of counter-terrorism. The fight against terrorism as

28 XI 2024, <https://www.aa.com.tr/ru/мир/лидеры-стран-одкб-выразили-глубокую-озабоченность-эскалацией-в-зоне-израильско-палестинского-конфликта/3407532> [accessed: 22 I 2026]; МИД стран-членов ОДКБ сделали заявление о положении в Афганистане (*MID stran-chlenov ODKB sdelali zayavleniye o polozhenii v Afganistane*), KazTAG, 28 XI 2024, <https://kaztag.kz/ru/news/mid-stran-chlenov-odkb-sdelali-zayavlenie-o-polozhenii-v-afganistane> [accessed: 22 I 2026]; Касым-Жомарт Токаев принял участие в сессии Совета коллективной безопасности ОДКБ в узком составе, Официальный сайт Президента Республики Казахстан (*Kasym-Zhomart Tokayev prinyal uchastie v sessii Sovetakov kolektivnoy bezopasnosti ODKB v uzkom sostave*, Ofitsial'nyy sayt Prezidenta Respubliki Kazakhstan), 28 XI 2024, <https://www.akorda.kz/ru/kasym-zhomart-tokayev-prinyal-uchastie-v-sessii-soveta-kollektivnoy-bezopasnosti-odkb-v-uzkom-sostave-2810955> [accessed: 22 I 2026]; Организация Договора о коллективной безопасности (ОДКБ), Министерство иностранных дел Российской Федерации (*Organizatsiya Dogovora o kolektivnoy bezopasnosti (ODKB)*, Ministerstvo inostrannykh del Rossiyskoy Federatsii), https://mid.ru/ru/foreign_policy/integracionnye-struktury-prostranstva-sng/odkb/ [accessed: 22 I 2026].

⁷¹ В Москве прошла Международная конференция «О роли и характере взаимодействия международных и региональных организаций в борьбе с международным терроризмом», организованная Секретариатом ОДКБ при участии ОБСЕ, Организация Договора о коллективной безопасности (*V Moskve proshla Mezhdunarodnaya konferentsiya «O roli i kharaktere vzaimodeystviya mezhdunarodnykh iregional'nykh organizatsiy v bor'be s mezhdunarodnym terrorizmom», organizovannaya Sekretariatom ODKB pri uchastii OBSE, Organizatsiya Dogovora o kolektivnoy bezopasnosti*), 30 X 2019, https://odkb-csto.org/news/news_odkb/v-moskve-proshla-mezhdunarodnaya-konferentsiya-o-rol-i-kharaktere-vzaimodeystviya-mezhdunarodnykh-i/?sphrase_id=66458 [accessed: 16 I 2026].

understood by the Kremlin – a point echoed in numerous statements⁷² – has a completely different dimension than it does from the perspective of the West.

There are many areas of cooperation between the CSTO and the UN regarding international fight against terrorism. The basis for joint activities is the agreements concluded between the CSTO Secretary General and selected UN organisational units, and, above all, the memorandum of understanding with the Counter-Terrorism Committee (CTC) of the UN Security Council and the cooperation agreement between the CSTO Secretary General and the United Nations Office of Counter-Terrorism (UNOCT). Cooperation with partners – the Commonwealth of Independent States and the Shanghai Cooperation Organisation – is also significant. It should be noted that, since the UNOCT was established in 2017, the Office has been led by the representatives of the RF⁷³, which from a political and institutional perspective, may have helped to maintain active relations between the UN and the CSTO in the field of combating terrorism.

Russia's war against Ukraine exposed the weakness of the CSTO as collective security mechanism. In other words, instead of consolidation and cooperation, there has been a distancing, and most members – apart from Belarus – are avoiding openly supporting Moscow. This combines two conflicting approaches from Russia's perspective. Most members do not want to legitimise aggression or risk losing profits in their relationships with the West. At the same time, the Kremlin continues to seek to develop its regional policy by drawing on the narrative of the ongoing need to combat terrorism and to maintain the special operation in Ukraine, which is intended to justify decisive action in the region and to build influence in forums such as the CSTO and the Shanghai Cooperation Organisation. The problem is that, without Russia's ability to intervene and impose resolutions on conflicts (e.g. Armenia – Azerbaijan or Kyrgyzstan – Tajikistan), the CSTO as an organisation becomes powerless, and the countries in the region are increasingly seeking alternative

⁷² *Putin Accuses Ukraine of Wanting Ceasefire to Rearm and Prepare 'Terrorist Attacks'*, The Moscow Times, 4 VI 2025, <https://www.themoscowtimes.com/2025/06/04/putin-saysukraine-wants-ceasefire-to-rearm-and-prepare-terrorist-attacks-a89340> [accessed: 22 I 2026].

⁷³ *Leadership*, United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en/leadership> [accessed: 14 III 2026].

cooperation projects with, among others, China and Turkey, as well as seeking cooperation with the European Union⁷⁴.

Summary

The authorities in Moscow portray Russia as a key actor in the international fight against terrorism, emphasising the need to avoid double standards and to build a broad coalition against terrorism and extremism. They treat counterterrorism as a tool of state policy. They promote a narrative that prioritises eliminating existing threats (rather than prevention). They completely control the information space and marginalise the importance of human rights. All this is intended to legitimise repressive methods within the country and increase influence abroad⁷⁵. At the same time, establishing cooperation with the Taliban government or using ‘counterterrorism’ operations instrumentally to support activities in Syria, the Sahel and Ukraine undermines the credibility of this narrative. This shows that the aim is to intensify rivalry with Western countries, not so much in terms of the fight against terrorism itself, but rather in the way threats are defined, security narratives are constructed, and their own actions are legitimised under the banner of counter-terrorism. Russia uses this category as a political instrument, presents its own approach as an alternative to the Western model and as a justification for actions taken both within the country and abroad.

The Russian Federation has been putting forward the view for years that the fight against terrorism should be conducted without double standards, and it often uses this issue to highlight the shortcomings of the West⁷⁶.

⁷⁴ P. Filkowska, *Pierwsze reakcje państw członkowskich Organizacji Układu o Bezpieczeństwie Zbiorowym na inwazję Federacji Rosyjskiej na Ukrainę* (Eng. First reactions of the member states of the Collective Security Treaty Organisation on the Russian Federation invasion in Ukraine), “Wschód Europy” 2024, vol. 10, no. 1. <https://doi.org/10.17951/we.2024.10.1.113-128>; A.M. Dyner, *CSTO Ambiguous on War in Ukraine and Faces Regional Challenges*, Polski Instytut Spraw Międzynarodowych, 27 III 2023, <https://pism.pl/publications/csto-ambiguous-on-war-in-ukraine-and-faces-regional-challenges> [accessed: 12 I 2026].

⁷⁵ See wider: J. Hedenskog, *Russia and International Cooperation on Counter-Terrorism. From the Chechen Wars to the Syria Campaign*, FOI, March 2020, <https://foi.se/rest-api/report/FOI-R--4916--SE> [accessed: 12 I 2026].

⁷⁶ *Russia accuses West of double standards regarding Daesh*, Middle East Monitor, 29 VIII 2019, <https://www.middleeastmonitor.com/20190829-russia-accuses-west-of-double-standards-regarding-daesh/> [accessed: 12 I 2026].

The authorities in Moscow accuse Western countries of adopting a selective approach to ISIS (including in the context of Afghanistan), suggesting that some states treat terrorist organisations instrumentally – as tools for pursuing their own political objectives – rather than combating them consistently. Furthermore, it can thus blame other actors for the attacks⁷⁷.

At the same time, experiences from the North Caucasus and the participation of the RF citizens in foreign conflicts show that the terrorist threat is long-term in nature and will continue to develop. It is estimated that at the peak of ISIS's activities, around 2300 Russian citizens and around 4700 fighters from the former Soviet republics took part in the fighting in Syria and Iraq. Some of them may have returned to Russia or neighbouring countries, strengthening local radical and terrorist networks⁷⁸. Returning terrorists possess combat experience, contacts and funding, which facilitates the recruitment of further people and the execution of operations, leading to a growing level of terrorist threat. Given Russian counterterrorism system, based mainly on special services and military operations, conditions conducive to further radicalisation and violence are emerging.

The 2022 Russian aggression against Ukraine exposed serious weaknesses in Russian special services, which for years had built an image of an effective security apparatus⁷⁹. Analytical units not only failed to correct the Kremlin's political assumptions, but may also have reinforced them by adapting their assessments to the expectations of decision-makers clustered around Vladimir Putin. As a result, Russian services, including the FSB, instead of performing functions that would ensure security, became part of a system confirming false assumptions, which had direct consequences for operational activities in Ukraine. A similar pattern

⁷⁷ A. Kozioł, *Russia Shifts Counter Terrorism into War Propaganda*, Polski Instytut Spraw Międzynarodowych, 18 X 2024, <https://www.pism.pl/publications/russia-shifts-counter-terrorism-into-war-propaganda> [accessed: 19 III 2026].

⁷⁸ D. Nicolson, *Foreign Terrorist Fighters from the North Caucasus: Understanding Islamic State Influence in the Region*, "Connections: The Quarterly Journal" 2017, vol. 16, no. 4. <https://doi.org/10.11610/Connections.16.4.04>.

⁷⁹ J.M. Raubo, *Ukraina 2022. Historyczna rysa na propagandowym obrazie rosyjskich służb specjalnych* (Eng. Ukraine 2022. Historic crack in the propaganda image of the Russian special services), InfoSecurity24, 12 III 2022, <https://infosecurity24.pl/sluzby-specjalne/ukraina-2022-historyczna-rysa-na-propagandowym-obrazie-rosyjskich-sluzb-specjalnych> [accessed: 19 I 2026].

of behaviour by the services also applies to the fight against terrorism in the RF.

The Russian security apparatus's focus on the war against Ukraine and its rivalry with the West has limited the state's ability to effectively detect and neutralise some terrorist threats. The events of 2024, including the attack in the Crocus City Hall or attacks in Dagestan, showed not only the scale of challenges in the domain of terrorism, but also gaps in the response system, despite earlier warnings from other states. At the same time, the Kremlin's response focused largely on controlling the narrative, crackdowns, expanding the powers of the security services, and attributing responsibility to selected terrorist groups and opponents, in particular Ukraine and Western countries⁸⁰. All of this is consistent with the premise of using terrorism as an element of domestic policy and a tool for mobilising public support in order to maintain control, although attacks continue to occur in Russia and the region.

It should be emphasised that it was the attack on the Crocus City Hall which demonstrated that, despite years of pacification efforts, Russia had not eliminated the sources of the terrorist threat, and that the root of the problem still lies in the North Caucasus. Although the scale of attacks within the country has been small in recent years, radicalisation in republics such as Chechnya, Dagestan and Ingushetia remains a persistent phenomenon, particularly among the younger generation. Jihadist structures – both those linked to the Islamic State and to the re-emerging Caucasus Emirate – focus on operations against security services and state institutions⁸¹. An increasingly important aspect is international dimension in which attacks may be carried out by individuals from Russia as well as from across the wider Caucasus region.

The conditions and threats discussed do not indicate an increase in the scale of terrorism in the RF, but they do indicate the existence of persistent factors that cannot be fully eliminated, even by the authoritarian Russian apparatus. The neglect of early signs of radicalisation, as well as the ongoing and escalating terror and the privileged position of Russian security services at both the local and regional levels, led to

⁸⁰ A. Koziol, *Walka z terroryzmem jako element propagandy wojennej Rosji...*; P. Sonne, E. Schmitt, M. Schwartz, *Why Russia's Vast Security Services Fell Short on Deadly Attack*, The New York Times, 28 III 2024, <https://www.nytimes.com/2024/03/28/world/europe/russia-concert-attack-security-failures.html> [accessed: 21 III 2026].

⁸¹ *IntelBrief: Radicalization and Extremism in Russia's...*

incorrect threat assessments and a delayed state response. The experience related to the underestimation of earlier attacks in Russia, including the influence of Chechen elements, the activities of Al-Qaeda and ISIS⁸², indicate that Russia is not capable, and will never be able, to fully eliminate terrorist threat, both domestically and abroad.

Bibliography

Beslin J., Ignjatijevic M., *Balkan foreign fighters: from Syria to Ukraine*, "Brief" 2017, no. 20, pp. 1–4.

Filkowska P., *Pierwsze reakcje państw członkowskich Organizacji Układu o Bezpieczeństwie Zbiorowym na inwazję Federacji Rosyjskiej na Ukrainę* (Eng. First reactions of the member states of the Collective Security Treaty Organisation on the Russian Federation invasion in Ukraine), "Wschód Europy" 2024, vol. 10, no. 1. <https://doi.org/10.17951/we.2024.10.1.113-128>.

Grabowski T., *Terroryzm północnokaukaski: przejawy zjawiska* (Eng. North Caucasus Terrorism: Manifestations of the Phenomenon), "Res Politicae" 2014, vol. VI, pp. 59–78. <http://dx.doi.org/10.16926/rp.2014.06.04>.

Grabowski T.W., *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku* (Eng. North Caucasus Terrorism: Sources, Manifestations and Counteracting the Phenomenon), Kraków 2017.

Liedel K., Piasecka P., *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej* (Eng. How to survive in an age of terrorist threats. Elements of counter-terrorism education), Warszawa 2008.

Nicolson D., *Foreign Terrorist Fighters from the North Caucasus: Understanding Islamic State Influence in the Region*, "Connections: The Quarterly Journal" 2017, vol. 16, no. 4. <https://doi.org/10.11610/Connections.16.4.04>.

Oldberg I., *The War on Terrorism in Russian Foreign Policy*, FOI – Swedish Defence Research Agency, Defence Analysis, Stockholm 2006.

⁸² L. Aron, *The Expansion of Russia's Radical Islamism Outside the North Caucasus*, American Enterprise Institute, 30 IX 2015, <https://www.aei.org/research-products/testimony/the-expansion-of-russias-radical-islamism-outside-the-north-caucasus/> [accessed: 22 I 2026].

Olech A., *The Wagner Group in Africa. The sham battle of Russian mercenaries against terrorism*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 273–309. <https://doi.org/10.4467/27204383TER.24.010.19398>.

Olech A., *Terroryzm – określenie definicji zjawiska w polskich i zagranicznych badaniach* (Eng. Terrorism – defining the phenomenon in Polish and foreign research), "Studia Bezpieczeństwa Narodowego" 2020, vol. 18, no. 2, pp. 121–138. <https://doi.org/10.37055/sbn/145302>.

Olech A.K., *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku* (Eng. Terrorist attacks in the Russian Federation in the 21st century), "Nowa Polityka Wschodnia" 2019, no. 4, pp. 110–115. <https://doi.org/10.15804/NPW20192306>.

Schmid A.P., Jongman A.J., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Amsterdam 1988.

Sinai J., *The Terrorist Threats Against Russia and its Counterterrorism Response Measures*, "Connections: The Quarterly Journal" 2015, vol. 14, no. 4, pp. 95–101. <http://dx.doi.org/10.11610/Connections.14.4.08>.

Stempień M.S., *The evolution of terrorism in Russia in the years 2015–2022. Quantitative analysis of the phenomenon*, "Przegląd Wschodnioeuropejski" 2023, no. 14, pp. 185–199. <https://doi.org/10.31648/pw.9711>.

The North Caucasus: The Challenges of Integration (II), Islam, the Insurgency and Counter-Insurgency, Europe Report N°221, 19 X 2012.

Weinberg L., Pedahzur A., Hirsch-Hoefler S., *The Challenges of Conceptualizing Terrorism*, "Terrorism and Political Violence" 2004, vol. 16, no. 4, pp. 777–794. <https://doi.org/10.1080/095465590899768>.

Internet sources

Aji A., Mroue B., *Russian Embassy shelled in Syria as insurgents hit back*, Associated Press, 13 X 2015, <https://apnews.com/article/991656eab57d4aa79fbd5458af62b60e> [accessed: 21 III 2026].

Al-Qaeda in Syria calls for revenge attacks on Russia, The Washington Post, 13 X 2015, https://www.washingtonpost.com/world/middle_east/al-qaeda-in-syria-calls-for-revenge-attacks-on-russia/2015/10/13/b7f7dfdf-a0a4-451d-bd2e-180f2f4882f5_story.html [accessed: 16 V 2026].

Arieff A., Blanchard L.P., Collins S.R., Husted T.F., *Russia's Security Operations in Africa*, Congressional Research Service, 8 IV 2026, <https://www.congress.gov/crs-product/IF12389> [accessed: 12 IV 2026].

Aron L., *The Expansion of Russia's Radical Islamism Outside the North Caucasus*, American Enterprise Institute, 30 IX 2015, <https://www.aei.org/research-products/testimony/the-expansion-of-russias-radical-islamism-outside-the-north-caucasus/> [accessed: 22 I 2026].

Bartosiewicz M., *Increasing radicalisation: terrorist attacks in Dagestan*, Ośrodek Studiów Wschodnich, 25 VI 2024, <https://www.osw.waw.pl/en/publikacje/analyses/2024-06-25/increasing-radicalisation-terrorist-attacks-dagestan> [accessed: 26 X 2025].

Bhattacharji P., *Chechen Terrorism (Russia, Chechnya, Separatist)*, Council on Foreign Relations, 8 IV 2010, <https://www.cfr.org/backgrounders/chechen-terrorism-russia-chechnya-separatist> [accessed: 20 III 2026].

Borshchevskaya A., *Russian Officials Inadvertently Aid Radical Islamists in Russia*, The Washington Institute for Near East Policy, 31 XII 2015, <https://www.washingtoninstitute.org/policy-analysis/russian-officials-inadvertently-aid-radical-islamists-russia> [accessed: 22 I 2026].

Bryjka F., Czerep J., *Africa Corps – a new iteration of Russia's old military presence in Africa*, Polski Instytut Spraw Międzynarodowych, 29 V 2024, <https://pism.pl/publications/africa-corps-a-new-iteration-of-russias-old-military-presence-in-africa> [accessed: 22 I 2026].

Caucasus Emirate, START – National Consortium for the Study of Terrorism and Responses to Terrorism, January 2015, <https://www.start.umd.edu/baad/narratives/caucasus-emirate.html> [accessed: 19 I 2026].

Costa-Roberts D., *Questions swirl over Russian plane crash in Egypt that killed 224*, PBS News, 1 XI 2015, <https://www.pbs.org/newshour/world/details-emerge-case-downed-russian-jet> [accessed: 20 I 2026].

Database Scope, RAND National Security Research Division, <https://www.rand.org/nsrd/projects/terrorism-incidents/about/definitions.html> [accessed: 20 III 2026].

Dyner A.M., *CSTO Ambiguous on War in Ukraine and Faces Regional Challenges*, Polski Instytut Spraw Międzynarodowych, 27 III 2023, <https://pism.pl/publications/csto-ambiguous-on-war-in-ukraine-and-faces-regional-challenges> [accessed: 12 I 2026].

Dyner A.M., *Terrorists Kill at least 137 at Moscow Concert Hall*, Polski Instytut Spraw Międzynarodowych, 25 III 2024, <https://pism.pl/publications/terrorists-kill-at-least-137-at-moscow-concert-hall> [accessed: 19 I 2026].

Falkowski M., *The Islamic State in the Caucasus – who benefits?*, Ośrodek Studiów Wschodnich, 14 I 2015, <https://www.osw.waw.pl/en/publikacje/analyses/2015-01-14/islamic-state-caucasus-who-benefits> [accessed: 12 III 2026].

Faulconbridge G., *Russian security failure? Kremlin says no country is immune to terrorism*, Reuters, 25 III 2024, <https://www.reuters.com/world/europe/russian-security-failure-kremlin-says-no-country-is-immune-terrorism-2024-03-25/> [accessed: 20 III 2026].

Ferris E., *How Russia's War in Ukraine is Creating Domestic Security Gaps*, Royal United Services Institute, 23 IX 2025, <https://www.rusi.org/explore-our-research/publications/insights-papers/how-russias-war-ukraine-creating-domestic-security-gaps> [accessed: 21 III 2026].

Flanagan J., *Bloodshed and retreat from Mozambique for Putin's private army the Wagner Group*, The Times, 25 XI 2019, <https://www.thetimes.com/uk/politics/article/bloodshed-and-retreat-from-mozambique-for-putin-s-private-army-the-wagner-group-696tnpzqh> [accessed: 19 I 2026].

Foreign Fighters. An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq, December 2015, https://thesoufancenter.org/wp-content/uploads/2017/05/TSG_ForeignFightersUpdate_format-for-print-120915-REBRAND-031317.pdf [accessed: 21 I 2026].

Gliniasty J. de, *Moscow Attack: Russia Confronts Islamist Terrorism*, Institut de Relations Internationales et Stratégiques, 26 III 2024, <https://www.iris-france.org/en/184928-moscow-attack-russia-confronts-islamist-terrorism/> [accessed: 21 III 2026].

Global Terrorism Index 2022, <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf> [accessed: 22 I 2026].

Global Terrorism Index 2023, <https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf> [accessed: 22 I 2026].

Global Terrorism Index 2024, <https://reliefweb.int/report/world/global-terrorism-index-2024> [accessed: 22 I 2026].

Global Terrorism Index 2025, <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf> [accessed: 22 I 2026].

Global Terrorism Index 2026, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf> [accessed: 13 IV 2026].

Gold Z., *Wilayat Sinai Risks Backlash After Metrojet Bombing*, <https://ctc.westpoint.edu/wp-content/uploads/2015/12/CTCSentinel-Vol8Iss118.pdf> [accessed: 19 I 2026].

Hanoush F., *Fighters from the Caucasus Join ISIS to Fight Russia*, Atlantic Council, 14 IX 2016, <https://www.atlanticcouncil.org/blogs/syriasource/fighters-from-the-caucasus-join-isis-to-fight-russia/> [accessed: 21 III 2026].

Hedenskog J., *Russia and International Cooperation on Counter-Terrorism. From the Chechen Wars to the Syria Campaign*, FOI, March 2020, <https://foi.se/rest-api/report/FOI-R--4916--SE> [accessed: 12 I 2026].

Hird K., Mappes G., Wolkov N., Harward Ch., Evans A., Kagan F.W., *Russian Offensive Campaign Assessment, March 25, 2024*, Critical Threats, 25 III 2024, <https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-march-25-2024> [accessed: 20 III 2026].

IntelBrief: Radicalization and Extremism in Russia's North Caucasus Region, The Soufan Center, 12 IV 2024, <https://thesoufancenter.org/intelbrief-2024-april-12/> [accessed: 26 X 2025].

ISIS video threatens attacks in Russia, Moscow, Ahram Online, 12 XI 2015, <https://english.ahram.org.eg/News/165409.aspx> [accessed: 21 III 2026].

Jenkins B.M., *Stray Dogs and Virtual Armies. Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11*, RAND, 31 VIII 2011, https://www.rand.org/pubs/occasional_papers/OP343.html [accessed: 22 IV 2026].

Johns M., *Terrorism and the North Caucasus: An Overview*, "START Background Report", National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, April 2013, https://www.academia.edu/8490735/Terrorism_and_the_North_Caucasus_An_Overview [accessed: 16 VI 2026].

Joscelyn T., *Head of al Qaeda's Syrian branch threatens Russia in audio message*, Long War Journal, 13 X 2015, <https://www.longwarjournal.org/archives/2015/10/head-of-al-qaedas-syrian-branch-threatens-russia-in-audio-message.php> [accessed: 21 III 2026].

Katz M.N., *No, Putin, the ISIS-K attack in Moscow wasn't about Ukraine*, Atlantic Council, 29 III 2024, <https://www.atlanticcouncil.org/blogs/menasource/isis-k-putin-moscow-al-qaeda/> [accessed: 20 I 2026].

Koziół A., *Russia Shifts Counter Terrorism into War Propaganda*, Polski Instytut Spraw Międzynarodowych, 18 X 2024, <https://www.pism.pl/publications/russia-shifts-counter-terrorism-into-war-propaganda> [accessed: 19 III 2026].

Leadership, United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en/leadership> [accessed: 14 III 2026].

McFaul M., *U.S. Russia Relations After September 11, 2001*, Carnegie Endowment for International Peace, 24 X 2001, <https://carnegieendowment.org/posts/2001/10/us-russia-relations-after-september-11-2001?lang=en> [accessed: 21 III 2026].

National Antiterrorism Committee: goals and objectives, National Antiterrorism Committee, <https://en.nac.gov.ru/home> [accessed: 21 III 2026].

Olech A., *Rosyjscy najemnicy – raport z działalności w Afryce* (Eng. Russian mercenaries – report on activities in Africa), Defence24, 8 IV 2024, <https://defence24.pl/geopolityka/rosyjscy-najemnicy-raport-z-dzialalnosci-w-afryce> [accessed: 22 I 2026].

On the Terrorist Attack at the Crocus City Hall in Moscow, U.S. Mission to the Organization for Security and Cooperation in Europe, 11 IV 2024, <https://osce.usmission.gov/on-the-terrorist-attack-at-the-crocus-city-hall-in-moscow/> [accessed: 20 III 2026].

Paraszczyk J., *IS's North Caucasus Affiliate Calls for Recruits to Join It in Dagestan*, Radio Free Europe/Radio Liberty, 3 X 2015, <https://www.rferl.org/a/islamic-state-north-caucasus-affiliate-call-for-recruits-dagestan/27285024.html> [accessed: 16 V 2026].

Peaceful Muslims have no relation to extremists – supreme mufti of Russia, Pravmir, 30 XII 2013, <https://www.pravmir.com/peaceful-muslims-have-no-relation-to-extremists-supreme-mufti-of-russia/> [accessed: 21 I 2026].

Putin Accuses Ukraine of Wanting Ceasefire to Rearm and Prepare 'Terrorist Attacks', The Moscow Times, 4 VI 2025, <https://www.themoscowtimes.com/2025/06/04/putin-says-ukraine-wants-ceasefire-to-rearm-and-prepare-terrorist-attacks-a89340> [accessed: 22 I 2026].

Raubo J.M., *Ukraina 2022. Historyczna rysa na propagandowym obrazie rosyjskich służb specjalnych* (Eng. Ukraine 2022. Historic crack in the propaganda image of the Russian special services), InfoSecurity24, 12 III 2022, <https://infosecurity24.pl/sluzby-specjalne/ukraina-2022-historyczna-rysa-na-propagandowym-obrazie-rosyjskich-sluzb-specjalnych> [accessed: 19 I 2026].

Rekawek K., Lanchès J., Zotova M., *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 VI 2026].

Roggio B., *Doku Umarov declares Islamic Caucasus Emirate*, Long War Journal, 26 XI 2007, https://www.longwarjournal.org/archives/2007/11/doku_umarov_declares.php [accessed: 19 I 2026].

Russia accuses West of double standards regarding Daesh, Middle East Monitor, 29 VIII 2019, <https://www.middleeastmonitor.com/20190829-russia-accuses-west-of-double-standards-regarding-daesh/> [accessed: 12 I 2026].

Schmid A.P., *Defining Terrorism*, https://icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf [accessed: 20 III 2026].

Sonne P., Schmitt E., Schwirtz M., *Why Russia's Vast Security Services Fell Short on Deadly Attack*, The New York Times, 28 III 2024, <https://www.nytimes.com/2024/03/28/world/europe/russia-concert-attack-security-failures.html> [accessed: 21 III 2026].

Strachota K., *Islamic State-Khorasan: global jihad's new front*, 29 III 2024, Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-03-29/islamic-state-khorasan-global-jihads-new-front> [accessed: 20 I 2026].

Syria crisis: Rockets hit Russian embassy compound in Damascus, reports say, ABC News, 13 X 2015, <https://www.abc.net.au/news/2015-10-13/rockets-hit-russian-embassy-compound-in-damascus-reports/6851968> [accessed: 16 V 2026].

Ter M., *The Caucasus Emirate, the Other Russian Front*, https://www.cidob.org/sites/default/files/2024-07/NOTES%20129_TER_ANG.pdf [accessed: 16 VI 2026].

The Deadliest Attacks In Russia, Radio Free Europe/Radio Liberty, <https://www.rferl.org/a/russia-timeline-terror-attacks/28410225.html> [accessed: 19 I 2026].

The North Caucasus Insurgency and Syria: An Exported Jihad?, International Crisis Group, 16 III 2016, <https://www.crisisgroup.org/europe-central-asia/russia-internal-syria/238-north-caucasus-insurgency-and-syria-exported-jihad> [accessed: 19 I 2026].

Vatchagaev M., *Caucasus Emirate and Islamic State Split Slows Militant Activities in North Caucasus*, Jamestown, 14 II 2015, <https://jamestown.org/program/caucasus-emirate-and-islamic-state-split-slows-militant-activities-in-north-caucasus-2/> [accessed: 20 I 2026].

Vitkine B., *Russia faces wave of Islamophobia after Moscow attacks*, Le Monde, 30 III 2024, https://www.lemonde.fr/en/international/article/2024/03/30/russia-faces-wave-of-islamophobia-after-moscow-attacks_6666864_4.html [accessed: 20 I 2026].

Why is ISIS targeting Russia?, Vision of Humanity, 25 III 2024, <https://www.visionofhumanity.org/why-is-isis-targeting-russia/> [accessed: 21 III 2026].

Wilk A., Konończuk W., *Ukrainian-Russian war under the banner of anti-terrorist operation*, Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/en/publikacje/analyses/2014-08-06/ukrainian-russian-war-under-banner-anti-terrorist-operation> 6 VIII 2014, [accessed: 19 I 2026].

Youngman M., Moore C., *Guide: The Caucasus Emirate*, Radicalisation Research, 9 XI 2017, <https://radicalisationresearch.org/research/youngman-guide-caucasus-emirate/> [accessed: 12 III 2026].

Zielińska D., *Pragmatism beyond divides: Central Asia's engagement with Afghanistan*, Ośrodek Studiów Wschodnich, 7 XI 2025, <https://www.osw.waw.pl/en/publikacje/analyses/2025-11-07/pragmatism-beyond-divides-central-asias-engagement-afghanistan> [accessed: 12 I 2026].

Russian and Belarusian internet sources

Keskin O., *Лидеры стран ОДКБ выразили глубокую озабоченность эскалацией в зоне израильско-палестинского конфликта* (*Lidery stran ODKB vyrazili glubokuyu ozabochennost'eskalatsiyey v zone izrail'sko-palestinskogo konflik*), Anadolu Agency, 28 XI 2024, <https://www.aa.com.tr/ru/мир/лидеры-стран-одкб-выразили-глубокую-озабоченность-эскалацией-в-зоне-израильско-палестинского-конфликта/3407532> [accessed: 22 I 2026].

В Астане состоялась сессия СКБ ОДКБ, Организация Договора о коллективной безопасности (*V Astane sostoyalas' sessiya SKB ODKB*, Organizatsiya Dogovora okollektivnoy bezopasnosti), 28 XI 2024, https://odkb-csto.org/news/news_odkb/v-astane-sostoyalas-sessiya-skb-odkb/ [accessed: 22 I 2026].

В Москве прошла Международная конференция «О роли и характере взаимодействия международных и региональных организаций в борьбе с международным терроризмом», организованная Секретариатом ОДКБ при участии ОБСЕ, Организация Договора о коллективной безопасности (*V Moskve proshla Mezhdunarodnaya konferentsiya «O roli i kharaktere vzaimodeystviya mezh-dunarodnykh iregional'nykh organizatsiy v bor'be s mezhdunarodnym terrorizmom»*, organizovannaya Sekretariatom ODKB pri uchastii OBSE, Organizatsiya Dogovora o kollektivnoy bezopasnosti), 30 X 2019, https://odkb-csto.org/news/news_odkb/v-moskve-proshla-mezhdunarodnaya-konferentsiya-o-rol-i-kharaktere-vzaimodeystviya-mezhdunarodnykh-i/?sphrase_id=66458 [accessed: 16 I 2026].

Генеральный секретарь ОДКБ Станислав Зась 4 сентября выступил на совместном заседании министров обороны СНГ, ШОС и ОДКБ, Организация Договора о коллективной безопасности (*General'nyy sekretar' ODKB Stanislav Zas' 4 sentyabryavystupil na sovmestnom zasedanii ministrov oborony SNG, SHOS IODKB, Organizatsiya Dogovora o kolektivnoy bezopasnosti*), https://odkb-csto.org/news/news_odkb/generalnyy-sekretar-odkb-stanislav-zas-4-sentyabrya-vystupil-na-sovmestnom-zasedanii-ministrov-oboro/?sphrase_id=66458 [accessed: 11 III 2026].

Заявление глав государств-членов Организации Договора о Коллективной Безопасности о противодействии международному терроризму, 21 декабря 2015 года, г. Москва, Организация Договора о коллективной безопасности (Zayavleniye glav gosudarstv-chlenov Organizatsii Dogovorao Kollektivnoy Bezopasnosti o protivodeystvii mezhdunarodnomu terrorizmu, 21 dekabrya 2015 goda, g. Moskva, Organizatsiya Dogovora o kolektivnoy bezopasnosti), 21 XII 2015, https://odkb-csto.org/documents/documents/zayavlenie_glav_gosudarstv_chlenov_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_o_protivodeystv/?sphrase_id=66457 [accessed: 10 III 2026].

Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими (на 4 апреля 2026 г.), Федеральная служба безопасности Российской Федерации (Yedinyy federal'nyy spisok organizatsiy, v tom chisle inostrannykh i mezhdunarodnykh organizatsiy, priznannykh v sootvetstviy s zakonodatel'stvom Rossiyskoy Federatsii terroristicheskimi (na 4 aprelya 2026 g.), Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii), <http://www.fsb.ru/fsb/npd/terror.htm> [accessed: 20 IV 2026].

Касым-Жомарт Токаев принял участие в сессии Совета коллективной безопасности ОДКБ в узком составе, Официальный сайт Президента Республики Казахстан (Kasym-Zhomart Tokayev prinyal uchastiye v sessii Sovetakollektivnoy bezopasnosti ODKB v uzkom sostave, Ofitsial'nyy sayt Prezidenta Respubliki Kazakhstan), 28 XI 2024, <https://www.akorda.kz/ru/kasym-zhomart-tokayev-prinyal-uchastie-v-sessii-soveta-kollektivnoy-bezopasnosti-odkb-v-uzkom-sostave-2810955> [accessed: 22 I 2026].

Меры по противодействию международному терроризму и экстремизму рассмотрены на заседании Комитета секретарей советов безопасности стран ОДКБ, Национальный правовой Интернет-портал Республики Беларусь (Mery po protivodeystviyu mezhdunarodnomu terrorizmu i ekstremizmu rassmotreny na zasedanii Komitetasekretarey sovetov bezopasnosti stran ODKB, Natsional'nyy pravovoy Internet-portal Respubliki Belarus'), 24 V 2018, <https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2018/may/28997/> [accessed: 22 I 2026].

МИД стран-членов ОДКБ сделали заявление о положении в Афганистане (*MID stran-chlenov ODKB sdelali zayavleniye o polozhenii v Afganistane*), KazTAG, 28 XI 2024, <https://kaztag.kz/ru/news/mid-stran-chlenov-odkb-sdelali-zayavlenie-o-polozhenii-v-afganistane> [accessed: 22 I 2026].

Организация Договора о коллективной безопасности (ОДКБ), Министерство иностранных дел Российской Федерации (*Organizatsiya Dogovora o kolektivnoy bezopasnosti (ODKB), Ministerstvo inostrannykh del Rossiyskoy Federatsii*), https://mid.ru/ru/foreign_policy/integracionnye-strukturnye-prostranstva-sng/odkb/ [accessed: 22 I 2026].

Перечень организаций, признанных в соответствии с законодательством Российской Федерации экстремистскими (*Perechen' organizatsiy, priznannykh v sootvetstvi s zakonodatel'stvom Rossiyskoy Federatsii ekstremist-skimi*), <https://minjust.gov.ru/ru/documents/7822/> [accessed: 20 IV 2026].

Russian legal acts

Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 205. Террористический акт (*Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 No 63-FZ. Stat'ya 205. Terroristicheskiy akt*), https://www.consultant.ru/document/cons_doc_LAW_10699/43942021d9206af7a0c78b6f65ba3665db940264/ [accessed: 20 III 2026].

Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 282.2. Организация деятельности экстремистской организации и участие в деятельности такой организации (*Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 No 63-FZ. Stat'ya 282.2. Organizatsiya deyatel'nosti ekstremist-skoy organizatsii i uchastiye v deyatel'nosti takoy organizatsii*).

Уголовный кодекс Российской Федерации от 13.06.1996 No 63-ФЗ. Статья 361. Акт международного терроризма (*Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 No 63-FZ. Stat'ya 361. Akt mezhdunarodnogo terrorizma*), https://www.consultant.ru/document/cons_doc_LAW_10699/0994b72ccab34fae773ced2c837691518a3e3dca/ [accessed: 20 III 2026].

Федеральный закон Российской Федерации от 06.03.2006 No 35-ФЗ „О противодействии терроризму“. Статья 3. Основные понятия (*Federal'nyy zakon Rossiyskoy Federatsii ot 06.03.2006 No 35-FZ „O protivodeystvii terrorizmu“. Stat'ya 3. Osnovnyye ponyatiya*), https://www.consultant.ru/document/cons_doc_LAW_58840/4fdc493704d123d418c32ed33872ca5b3fb16936/ [accessed: 20 III 2026].

Aleksander Olech, PhD

Head of International Cooperation at Defence24 and Editor-in-Chief of Defence24.com. Lecturer at both national and international universities, NATO associate, analyst and publicist. Former deputy director of the Department at the Ministry of Foreign Affairs. Graduate of the European Academy of Diplomacy and War Studies University. Recipient of scholarships from US Department of State, UNODA and NATO 2030. Main research interests: French-Russian relations, challenges in Africa and NATO security policy.

Contact: a.olech@defence24.pl

Protecting public spaces and public events against vehicle-borne attacks – the importance of VSB and HVM systems in the context of recommendations for Poland

JAROSŁAW JAŻWIŃSKI

Independent author



<https://orcid.org/0000-0001-7845-5492>

Abstract

The aim of the article is to discuss HVM (hostile vehicle mitigation) systems and VSB (vehicle security barriers) as a means of protecting public spaces and public events against the deliberate use of a vehicle as a weapon. The conceptual framework relating to HVM systems and VSBs was organised, and current research standards concerning security devices were presented. The nature of this type of threats and the vulnerability of public spaces to them were discussed, followed by a presentation on the importance of risk analysis, the assessment of access-routes, current testing standards and the practical interpretation of crash-test results. The most common errors made during the design, installation and operation of safety systems were highlighted. A separate section was devoted to a model for designing HVM systems based on threat-scenario analysis, buffer zones, layered protection and organisational responsibility. The article highlights the need to increase awareness of the issue in question in the Polish context and sets out directions for the systemic development of protective measures for public spaces and public events.

Keywords

public event, mass event, protection of public spaces, vehicle-as-a-weapon attack, HVM system, VSB, DoS SD-STD-02.01, ASTM F2656/F2656M, PAS 68, IWA 14-1, ISO 22343.

Introduction

Protecting public spaces from vehicle-borne attacks is an important public safety issue. This is not limited to terrorist acts, but encompasses a broader category of incidents in which a vehicle is deliberately used as a tool to target people in these spaces. The mechanism of the risk itself is of decisive importance: the violent intrusion of a vehicle into a pedestrian zone, utilising its mass and kinetic energy as the primary means of causing harm.

Research in this field is fragmented and interdisciplinary in nature¹. It includes:

- 1) studies on vehicle-ramming attacks, in which a vehicle is treated as an easily accessible tool for attacking so-called 'soft targets' and crowded places;
- 2) institutional documents concerning the protection of public spaces, places of assembly and mass events, including guidelines relating to the planning of safety zones, the separation of vehicular and pedestrian traffic, and the use of HVM (hostile vehicle mitigation) systems;
- 3) technical norms and standards specifying the methods for testing and classifying barriers designed to protect against vehicle impact, in particular standards relating to VSBs (vehicle security barriers)².

¹ Cf. C.R. Ludbey et al., *Classifying vehicle-as-a-weapon attacks: an inductive taxonomy and design implications*, "Crime Science" 2026, vol. 15, art. 2. <https://doi.org/10.1186/s40163-025-00265-7>; V. Miller, K.J. Hayward, 'I Did My Bit': *Terrorism, Tarde and the Vehicle Ramming Attack as an Imitative Event*, "The British Journal of Criminology" 2019, vol. 59, no. 1, pp. 1–23. <https://doi.org/10.1093/bjc/azy017>; J.P. Phillips, J.S. Young, W.J. Brady, *Preparation and response to a targeted automobile ramming mass casualty (TARMAC) attack: An analysis of the 2017 Charlottesville, Virginia TARMAC attack*, "American Journal of Disaster Medicine" 2019, vol. 14, no. 3, pp. 219–223. <https://doi.org/10.5055/ajdm.2019.0333>; P. Hess, S. Mandhan, B. Ganor, *Ramming attacks, pedestrians, and the securitization of streets and urban public space: a case study of New York City*, "Urban Design International" 2022, vol. 28, no. 1, pp. 1–14; A.M. Tsur et al., *Patterns in vehicle-ramming attacks*, "Israel Medical Association Journal" 2022, vol. 24, no. 9, pp. 586–591; M. Cichomski, *How can local governments protect public spaces from vehicle attacks?*, "Terrorism – Studies, Analyses, Prevention" 2025, no. 8, pp. 487–516. <https://doi.org/10.4467/27204383TER.25.062.23049>; J. Jaźwiński, *Anti-terrorist protection of public facilities and critical infrastructure against attacks with motor vehicles*, "Terrorism – Studies, Analyses, Prevention" 2023, no. 3, pp. 361–409. <https://doi.org/10.4467/27204383TER.23.011.17451>.

² *Public Realm Design Guide for Hostile Vehicle Mitigation*, National Protective Security Authority, <https://www.npsa.gov.uk/specialised-guidance/hostile-vehicle-mitigation-hvm/>

In the Polish context, this issue remains insufficiently recognised, both at the organisational and project levels. Despite the fact that there have been no terrorist attacks involving vehicles on Polish territory, this threat should not be downplayed, particularly with regard to mass gatherings and other events held in open spaces.

The aim of this article is to discuss HVM systems and VSBs as a means of protecting public spaces and public events against vehicle-borne attacks. The article clarifies the basic concepts relating to protection against such attacks, presents current research standards for security devices, and highlights the most common errors made during the design, installation and operation of HVM systems. The research problem comes down to the question of what conditions must be met for the protection of public spaces and public events against vehicle intrusion to be effective and practical, rather than superficial.

The article poses three research questions: what is the significance of current research standards and the correct interpretation of crash test results for the selection of VSBs? What errors most commonly reduce the effectiveness of HVM system? What elements should an HVM system design model for public spaces and public events include?

This article is both analytical and practical in nature. The author employed methods such as: analysis of the relevant literature, legal acts, standards and standardisation documents relating to VSBs, as well as institutional and expert materials from various national and international bodies, including the European Commission, the JRC, the NPSA, CISA, French, Belgian and German materials, as well as an analysis of empirical data comprising observations from the author's professional practice, examples of implementations and cases of security measures being applied in public spaces.

public-realm-design-guide-hostile-vehicle-mitigation-0 [accessed: 12 IV 2026]; *Vehicle Ramming Action Guide*, Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide> [accessed: 20 VI 2026]; *Hostile Vehicle Guidelines for Crowded Places*, <https://www.nationalsecurity.gov.au/crowded-places-subsite/Files/hostile-vehicle-guidelines-crowded-places.pdf> [accessed: 20 VI 2026]; ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating, <https://www.iso.org/standard/50080.html> [accessed: 20 VI 2026]; ASTM F2656/F2656M-20 Standard Test Method for Crash Testing of Vehicle Security Barriers, https://www.astm.org/f2656_f2656m-20.html [accessed: 20 VI 2026].

Conceptual framework

One of the fundamental problems in the Polish debate on protecting public spaces against vehicle-borne attacks is the lack of consistency in terminology. Colloquial terms, industry-specific simplifications and direct translations are all in use, yet none of them accurately convey either the technical or organisational significance of the various solutions. The lack of conceptual precision leads to design errors, misjudgements regarding the effectiveness of devices, and confusion between security measures and traffic or public order elements. For this reason, standardising the terminology is a prerequisite for further discussion.

The key concept used in this article is HVM. It refers to a system designed to protect against the deliberate use of a vehicle as a weapon. It encompasses all measures designed to limit the possibility of a vehicle intruding into a protected area or to minimise the consequences of such an intrusion. The scope of HVM therefore includes not only infrastructural measures but also organisational, procedural, urban planning and operational solutions³.

The second concept is the VSB, which denotes specific devices designed to stop, intercept or restrict the movement of a vehicle in a specific threat scenario and tested for this purpose. This category includes both permanent and temporary solutions, as well as mobile ones, provided that their protective function has been confirmed in appropriate crash tests. The appearance of the device, its weight or the manufacturer's marketing claims are not sufficient in themselves for it to be recognised as a VSB in a technical sense⁴.

It is acceptable to use the term 'anti-terrorism barriers' as a descriptive label, provided it refers to VSBs used as part of the HVM system. This term may be useful in public or organisational communications, but it does not replace the correct technical classification. In expert discourse, priority should be given to precise terms that allow a distinction to be made between a security system and its constituent parts, as well as between tested devices and solutions with only an apparent security function.

The term 'protective barriers' should be avoided as the primary term in the field of protection against vehicle-borne attacks. It is too broad, vague and, in practice, leads to the erroneous equating of VSBs with road

³ See: J. Jaźwiński, *Anti-terrorist protection of public facilities...*, pp. 361–407.

⁴ *Ibid.*, pp. 362–364.

safety features, traffic calming measures or random street furniture. It may suggest equivalence between solutions which, from a safety perspective, have entirely different technical and operational statuses.

The article therefore adopts the following distinction: HVM refers to a system designed to prevent the deliberate use of a vehicle as a weapon, whilst VSB refers to the physical devices that form part of this system, provided their effectiveness has been confirmed by tests specific to this type of threat.

The nature of the threat and the vulnerability of public spaces

A vehicle-borne attack is one of those threats whose effectiveness stems from a combination of three factors: simplicity of execution, widespread availability of the means, and the ability to affect – with the direction and timing of the attack chosen appropriately – a large number of people in a short time. The perpetrator does not need to have advanced technical resources or complex logistics at their disposal. For this reason, this threat is of particular significance in the context of securing public events and all areas with high concentrations of pedestrian traffic.

This type of attack involves using a vehicle as a carrier of kinetic energy, directed directly against people in a public space. This means that the primary mechanism of harm is not the vehicle itself, understood as a means of transport, but its mass, speed and ability to intrude into an area where it should not be. From a public safety perspective, this has serious implications: the threat assessment cannot focus solely on the perpetrator's intent, but must also take into account the conditions that enable the attack to be carried out.

Events held in open spaces are most vulnerable to this type of attack, particularly those of a temporary, seasonal or occasional nature, e.g. fairs, festivals, cultural or religious events that require roads to be closed. Their vulnerability stems from their accessibility by public transport, high crowd density, limited ability to fully control all access routes, and the frequent absence of permanent security measures⁵.

From the perspective of a potential perpetrator, targets of this kind are also attractive because of the psychological and media impact they have.

⁵ See: M. Cichomski, *How can local governments protect public spaces...*, pp. 490–499.

An attack carried out in a place widely perceived as safe and accessible to the public, through which a large number of people pass every day, may result not only in numerous casualties but also in a powerful destabilising effect.

Of particular significance in this context are events of a symbolic nature and of great community value, linked to public holidays, local traditions, religious celebrations, etc.

However, a different level of vulnerability applies to facilities and spaces designed in accordance with the 'security by design' principle. In such locations, security requirements are taken into account right from the planning and design stages, right through to the subsequent operation of the infrastructure. This applies in particular to certain enclosed facilities, stadiums, entertainment arenas and those urban spaces where permanent access control measures have been implemented, along with permanent barriers to vehicle traffic, a clear division of the space into designated security zones, and solutions limiting the possibility of direct vehicle access to areas where large numbers of people are gathered.

This does not, however, mean that facilities designed with safety principles in mind are entirely risk-free. Their vulnerability has merely been reduced through the early identification of threats and the implementation of infrastructural and organisational measures. This distinction marks the boundary between a space that is prepared for a threat and one that remains vulnerable to it, because within the latter, security is treated merely as a reaction to an incident rather than as an integral part of planning.

In practice, this means moving away from the mindset that a vehicle-borne attack is an extreme scenario or one that is possible only in countries with a higher level of terrorist threat. From the perspective of protecting public spaces, what matters is not whether a given country has already experienced a high-profile attack, but whether its public spaces remain vulnerable to such an incident. It is this vulnerability that should be the primary criterion for assessing the need to implement HVM systems.

Delivery vans and lorries in the approx. 7.5-tonne category are particularly realistic element in the design scenarios for this type of threats. This is due to their relative availability, their suitability for use in urban traffic, and their impact energy parameters, which – at the speeds specified in research standards – are capable of causing serious consequences in public spaces. For this reason, the design of safety measures should

not focus exclusively on passenger cars, but on scenarios that reflect the perpetrator's capabilities and the geometry of the location⁶.

Analysis of the site and access routes as a basis for risk assessment

One of the most important stages in assessing the threat of a vehicle-borne attack is the analysis of a specific site and the identification of all directions from which a vehicle could breach the protected area. At this stage, it is determined whether the proposed security measures will address the actual threat or merely a simplified version of it. In this section, ISO 22343-2:2023⁷ has been adopted as a reference, together with supplementary expert guidelines concerning risk analysis, approach geometry, vehicle-borne attack scenario and local conditions affecting the effectiveness of VSBs.

Site analysis should comprise at least five steps:

- 1) identifying the protected area and its functions,
- 2) identifying all possible access routes,
- 3) assessing the geometric and terrain parameters,
- 4) defining a realistic scenario for a vehicle-borne attack,
- 5) verifying the continuity of the planned line of defence.

Attention should be drawn to main and side access spaces, utility and service routes, emergency access points, parking areas, sections of urban infrastructure that could be used to bypass the main security line, and the characteristics of pedestrian routes, should their layout be exploitable as a vehicle intrusion route. Only after carrying out such an analysis can one proceed to the appropriate selection of VSBs and the organisation of buffer zones.

The ability to bypass or circumvent the security measure is of particular importance. Even correctly selected and configured VSBs will not fulfil their function if the analysis is limited to a single entry direction, leaving

⁶ Cf. ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirement...; ASTM F2656/F2656M-20 Standard Test Method for Crash Testing of Vehicle Security Barriers...; *Hostile Vehicle Mitigation ISO 22343-1:2023 NPSA Guidance Note*, <https://www.npsa.gov.uk/system/files/documents/npsa-hvm-guidance-note-iso-22343-1-feb-2024.pdf> [accessed: 12 IV 2026].

⁷ ISO 22343-2:2023 Security and resilience – Vehicle security barriers – Part 2: Application, <https://www.iso.org/standard/81415.html> [accessed: 12 IV 2026].

space at the sides through which vehicles can pass. The effectiveness of the security system depends both on the parameters of the device itself and on the continuity of the security geometry across the entire protected area.

It is a mistake to assume that administrative traffic restrictions, such as entry bans, temporary signage, organisational separation or weight limits, in themselves reduce the level of risk. Such measures may serve an organisational and regulatory purpose, but they do not constitute a physical barrier to a perpetrator acting knowingly and deliberately. From an HVM perspective, it is therefore crucial whether the passage was effectively blocked before the vehicle intruded.

The site analysis should cover both the route of potential access roads and their spatial and functional parameters. Factors of significance include, among others, the length of the acceleration section, the width of the carriageway, turning radius, type of road surface, gradient of the terrain, the presence of intermediate obstacles, and the possibility of using ancillary infrastructure as a bypass route. Elements of the terrain's geometry that may appear secondary can, in practice, determine whether a given direction should be considered a possible intrusion scenario.

A proper site analysis involves adopting the perspective of an attacking vehicle and identifying all realistic ways of reaching the protected area. Only such an approach allows for determining the correct deployment of VSBs, defining the line of defence, assessing the need for layered solutions, and identifying points of particular vulnerability.

For this reason, the analysis of the site and access routes should be the foundation, not a secondary stage of the entire safety design process. If it is carried out superficially, incorrectly or piecemeal, even the best safety devices will fail to ensure an adequate level of safety. In HVM systems, an incorrect assessment of the space almost always leads to incorrect safety measures.

In the context of the design stage, it is also appropriate to distinguish between two zones: the speed reduction zone, where chicanes, narrowings and traffic control elements are used to limit the stopping distance, and the target protection zone (vehicle interception zone), where devices certified as vehicle barriers are employed. Elements from the first zone may enhance safety, but they do not replace VSBs in the vehicle interception zone.

Models for the implementation of VSBs, using European countries as examples

An analysis of solutions applied in practice shows that approaches to protecting public spaces against vehicle-borne attacks is highly varied. This stems both from the level of threat assessment and from the experiences of individual countries and cities in terms of security organisation, spatial planning and the implementation of infrastructure solutions. Consequently, there is no single universal security model that can be uncritically transferred between different organisational contexts. However, it is possible to identify practices that point the way towards a more mature, systematic approach.

In the Polish context, Warsaw remains a key point of reference, where VSBs began to be used at selected events and in certain urban areas, including in the area of the Royal Route, which encompasses Krakowskie Przedmieście and Nowy Świat streets⁸.

This phenomenon is significant for two reasons. Firstly, it demonstrates a growing awareness of the problem of protecting public spaces from vehicle intrusion. Secondly, it reveals that progress in this area remains incomplete and has not yet led to the implementation of uniform, consistent systemic standards. In practice, this means that individual successful projects do not amount to a mature national model.

The situation is different, for example, in the United Kingdom, where the problem of protecting public spaces against vehicle-borne attacks was recognised at an early stage, both in practical and regulatory terms. A key feature of the British approach is the integration of infrastructural, organisational and legal measures. Security there is not limited solely to the installation of physical barriers. It forms part of a broader system of risk management, organisational accountability and responsibilities arising from the need to ensure safety of public spaces and public events. Furthermore, legal regulations relating to the concept of the 'Protect Duty', known as Martyn's Law, are being developed in the UK⁹. This measure is

⁸ See: *Poprawiamy bezpieczeństwo w stolicy. Rozstawiamy bariery antyterrorystyczne i szkolimy z ich obsługi* (Eng. We are improving security in the capital. We are installing anti-terrorist barriers and providing training on how to use them), Zarząd Dróg Miejskich w Warszawie, 17 III 2026, <https://zdm.waw.pl/aktualnosci/poprawiamy-bezpieczenstwo-w-stolicy-rozstawiamy-bariery-antyterrorystyczne-i-szkolimy-z-ich-obsługi> [accessed: 12 IV 2026].

⁹ Cf. Terrorism (Protection of Premises) Act 2025, UK Public General Acts 2025 c. 10, <https://www.legislation.gov.uk/ukpga/2025/10/contents>; *Martyn's Law: the SIA's New Regulatory*

designed to strengthen protection against terrorism in relation to selected venues and public events by imposing obligations relating to preparation, planning of responses and – in the case of larger venues and events – implementation of proportionate measures to reduce vulnerability to attack. The legal framework does not replace technical solutions here, but assigns responsibility for their assessment and implementation¹⁰.

In Germany, Berlin has become one of the key benchmarks for the security of public events following the attack on the Christmas market in December 2016. This incident led to an increased emphasis on physical security measures in urban spaces and a significant re-evaluation of the approach to the security of seasonal events.

The attack in Nice, France, on 14 July 2016 highlighted the scale of the threat posed by the use of a vehicle in public spaces with very high pedestrian traffic. The cases of Berlin and Nice show that protection of urban spaces in Europe has developed not only on the basis of security theory, but also under the influence of experiences.

In the UK, PAS 68¹¹ and its associated guidelines serve as an important point of reference. From 2023, the current international standard for vehicle barriers is ISO 22343. In particular, ISO 22343-1:2023¹² specifies test requirements, test methods and the classification of results, whilst ISO 22343-2:2023 relates to the application, selection, installation and use of VSBs in design and operational practice. At the same time, an analysis of publicly available French, Belgian and German materials indicates that, in practice, operational documents, recommendations and organisational solutions concerning the protection of public spaces and public events against vehicle-borne attacks are of primary importance. This does not imply a lack of technical or regulatory solutions, but demonstrates that publicly available materials place greater emphasis on the organisation of security, risk analysis and the selection of security measures than on

Role, Security Industry Authority, <https://www.gov.uk/government/publications/martyns-law-the-sias-new-regulatory-role/martyns-law-the-sias-new-regulatory-role> [accessed: 12 IV 2026].

¹⁰ See: M. Cichomski, *How can local governments protect public spaces...*, pp. 490–492, 497–499.

¹¹ British Standards Institution, PAS 68:2013 Impact test specifications for vehicle security barrier systems, <https://knowledge.bsigroup.com/products/impact-test-specifications-for-vehicle-security-barrier-systems> [accessed: 12 IV 2026].

¹² ISO 22343-1:2023, Security and resilience – Vehicle security barriers – Part 1: Performance requirement...

highlighting separate national crash-test standards. The French General Secretariat for Defence and National Security (Secrétariat général de la défense et de la sécurité nationale) has published a code of good practice on protecting public events against vehicle-ramming attacks; the German Federal Ministry of the Interior (Bundesministerium des Innern) has announced its support for the DIN standard for vehicle barriers, whilst the German police are publishing materials on protecting public spaces against 'Überfahrtaten'. The European Commission under the JRC framework, meanwhile, has published guidelines on the design, testing and installation of protective barriers¹³.

The most important conclusion drawn from the analysis of urban models is as follows: the maturity of a system for protection against vehicle-borne attacks stems from the quality of the entire process of selecting barriers within the urban space, their deployment, maintenance and integration into a broader model of organisational responsibility. A city equipped with individual devices is not yet a city with an HVM system. Protection can be described as systematic only when physical measures form part of a previously identified, coherent threat management model.

Event typology and the selection of VSBs

When selecting VSBs, it is important to distinguish between the different types of protected events. Security plans for a recurring or multi-week event, an event involving persons under protection, a mobile event or an event held in a venue unsuitable for large gatherings differ from one another. The type of event influences the route of access, the organisation

¹³ Cf. *Se protéger contre les attaques au véhicule-bélier*, Secrétariat général de la défense et de la sécurité nationale, 11 VI 2018, <https://www.sgdsn.gouv.fr/publications/se-proteger-contre-les-attaques-au-vehicule-belier> [accessed: 12 IV 2026]; *Schutz öffentlicher Räume vor Überfahrtaten*, Polizeiliche Kriminalprävention der Länder und des Bundes, <https://www.polizei-beratung.de/themen-und-tipps/staedtebau/schutz-vor-ueberfahrtaten/> [accessed: 12 IV 2026]; V. Karlos, M. Larcher, G. Solomos, *Review on vehicle barrier protection guidance*, Publications Office of the European Union, European Commission, Joint Research Centre, 2017. <https://doi.org/10.2760/845599>; *Protection of public spaces from terrorist attacks*, European Commission, Joint Research Centre, https://joint-research-centre.ec.europa.eu/projects-and-activities/protection-public-spaces-terrorist-attacks_en [accessed: 12 IV 2026].

of supplies, the ability to maintain a continuous security perimeter and the requirements for temporary solutions.

Recurring and multi-week events

Recurring events lasting several weeks, such as seasonal markets, are characterised by long-term occupation of the space, regular deliveries and the need to maintain security in the long term. In such cases, it is advisable to aim to create as continuous a security perimeter as possible using certified vehicle barriers, whilst at the same time planning controlled entry points for authorised vehicles.

Events involving persons under protection

Events involving protected individuals, including VIP visits require flexible deployment of security measures along the route and at stopping points. Such operations are characterised by short set-up and dismantling times, the need to move equipment quickly, and the requirement to maintain logistical reserves and personnel ready to relocate barriers between successive locations. Security measures of this type may be implemented on a temporary basis, solely for the purposes of a specific event or a period of heightened risk.

Selected solutions used in European countries are presented below. These solutions differ in terms of design, purpose and resistance to vehicle impact, and their selection should correspond to the type of event, the layout of the security perimeter and operational requirements. Image 1 shows an example of temporary security measures using RBM M30 barriers in a public space in Warsaw during an event requiring a high level of security.



Image 1. RBM M30 barriers – temporary security measures of public space during an event requiring a higher level of security (Warsaw).

Source: DFE Security Sp. z o.o. materials.

Image 2 shows the physical security measures in place at the entrance to the Christmas market in Regensburg, where temporary mobile VSBs have been installed to prevent vehicles from entering public spaces with high concentrations of pedestrian traffic.

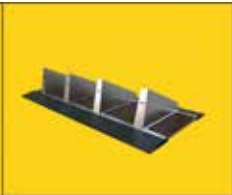


Image 2. Temporary mobile VSBs – security measures at the entrance to a Christmas market (Regensburg).

Source: Hörmann Polska marketing materials.

Table 1 sets out selected VSBs used in Europe. They differ in terms of design, purpose and resistance to vehicle impact, and their selection should be tailored to the type of incident, the layout of the security perimeter and operational requirements.

Table 1. Selected VSBs used in the security of public events in Europe.

			
RBM M30	SURFACE GUARD	OKTABLOCK	PITAGONE F18
recurring events, long term road closures	recurring events, long term road closures	one-off, short-term and long-term events	one-off, short-term-events
assembly in 20-minutes (2 people)	assembly: 6 m in 40 minutes (4 people)	no assembly required, setting it up is enough (1-2 people)	quick assembly and the ability to reposition (1-2 people)
transport: lorry with a crane	transport: van	transport: lorry with a crane or a mobile installation crane	transport: van
security level: vehicle weighing 7200 kg – speed 48 km/h	security level: vehicle weighing 7200 kg – speed 32 km/h and 2500 kg – speed 48 km/h	security level: vehicle weighing 7500 kg – speed 55 km/h and 3500 kg – speed 32 km/h	security level: vehicle weighing 7500 kg – speed 48 km/h

Source: own elaboration based on materials provided by DFE Security sp. z o.o.

**Mobile events and spaces unsuitable
for accommodating large numbers of people**

Mobile events, such as motor rallies, and events organised in venues not designed to accommodate large numbers of people require the identification of critical points where a vehicle may reach relatively higher speeds or where the largest number of participants gather. In such

situations, it is particularly important to determine in advance the possible routes by which a vehicle could reach the protected zone – that is, potential dredge routes – and to position vehicle barriers in such a way as to prevent the vehicle from continuing its journey towards the area where people are gathered (Image 3).



Image 3. Temporary mobile barrier – security for traffic routes and events held in open spaces (Berlin).

Source: Pitagone marketing materials.

Standards, crash tests and interpretation of the parameters of VSBs

The assessment of VSBs must not be based on the manufacturer's declarations, the product description or engineering calculations alone. Test standards and specifications are of key importance, as they set out the procedures for conducting impact tests, classifying results and comparing different technical solutions. They enable us to determine the specific hazard scenario in which a given device has actually been tested and which of its performance parameters have been empirically verified¹⁴.

¹⁴ See: *Impact Testing of Vehicle Security Barriers. An overview of vehicle impact test standards*, <https://www.npsa.gov.uk/system/files/documents/npsa-impact-testing-of-vehicle-security-barriers-18-august-2020.pdf> [accessed: 29 III 2026].

An assessment of the device's effectiveness should therefore address the following questions: to which standard has it been tested, for which vehicle category, at what mass, speed and angle of impact, and with what penetration result? Penetration should be understood as the distance the vehicle travels beyond the barrier line following an impact. This parameter allows the required distance between the safety barrier and the protected area to be determined. Without such data, an assessment of the device's suitability is purely declarative.

So called 'engineering solutions' are often found on the market. This term may refer to a structure designed on the basis of knowledge of physics, structural mechanics and soil mechanics, but it is not the same as a device that has been tested in a crash test. An engineering solution can be a valuable stage in the design process, but it does not replace an empirically verified test result¹⁵.

Basic standards used in the assessment of VSBs

The most important documents relating to the testing of devices designed to protect against vehicle-borne attacks include both older national and industry standards, as well as the current international standard ISO 22343. Of historical significance were the American DoS SD-STD-02.01 classifications¹⁶, followed by the British PAS 68 and the IWA 14-1:2013 industry document¹⁷, which standardised the method for testing vehicle barriers and reporting test results. Devices classified according to older standards are still in circulation on the market, which is why familiarity with them remains essential. Currently, the primary reference standard is the aforementioned ISO 22343. Its first part, ISO 22343-1:2023, specifies the test requirements, test method and classification of results, the second part, ISO 22343-2:2023, covers the application, selection, installation and use of VSBs. From a practical point of view, this marks a shift from fragmented, partly national approaches to a more unified assessment

¹⁵ See: *HVM – Vehicle Impact Testing and FEA Computational Analysis Guidance Note*, <https://www.npsa.gov.uk/system/files/documents/npsa-guidance-note-hvm-vehicle-impact-testing-and-fea-computational-analysis-15-july-2021.pdf> [accessed: 29 III 2026].

¹⁶ *Primer on Impact Protection for Critical Transportation Infrastructure*, FHWA-HIF-18-054, Federal Highway Administration, 2018., <https://www.fhwa.dot.gov/bridge/security/hif18054.pdf>, pp. 17–20 [accessed: 15 VI 2026].

¹⁷ IWA 14-1:2013 Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating.

framework, which allows for the comparison of solutions assessed under different standardisation systems.

DoS SD-STD-02.01 has not been included in the diagram as a separate standard, as the article adopts a summary approach to the most important standards used in market practice and technical documentation. Its current equivalent in the classification of vehicle barriers is ASTM F2656/F2656M¹⁸ (Figure 1).

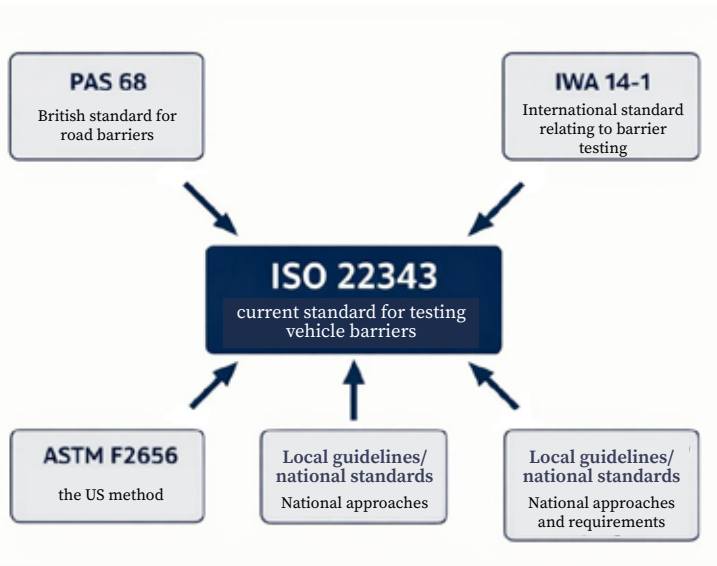


Figure 1. ISO 22343 as the current benchmark for vehicle barrier testing.

Source: own elaboration.

It should be emphasised that PN-EN 1317¹⁹ standard does not apply to VSBs. It is sometimes incorrectly cited in this context, as it relates to road safety barriers. However, it was developed with typical traffic incidents in mind and to mitigate the consequences of road collisions, rather than the threat posed by the deliberate use of a vehicle as a weapon.

¹⁸ ASTM F2656/F2656M Standard...

¹⁹ PN-EN 1317 Road restraint systems. This standard applies to road systems designed to stop vehicles, such as barriers installed alongside carriageways or between lanes on roads and motorways. The standard relates to road safety and mitigating the consequences of traffic incidents, rather than to VSBs intended to prevent vehicles from being used as weapons.

It is also important to distinguish between an engineering solution and a device that has been tested in accordance with the relevant standard. A mere description of the design or design calculations does not replace a crash test, which is the only way to confirm the device's behaviour under dynamic conditions. From the designer's point of view, it is important not only whether the device stopped the vehicle, but also the test scenario under which it was tested, the mass of the test vehicle, the speed, the angle of impact, the level of penetration, and the secondary effects of the collision.

An analysis of standards should proceed from identifying their origins and scope to answering the question of what the test result means for the actual safety design in a specific location. In this context, PAS 68, IWA 14-1, DoS SD-STD-02.01 and ASTM F2656/F2656M retain historical and comparative significance, while ISO 22343 remains the current international standard.

The article provides an overview of the most important standards still in use in market practice and technical documentation.

Four parameters are of fundamental importance for the correct selection of a VSBs: vehicle mass, impact speed, angle of impact and the level of vehicle penetration. Vehicle mass influences the level of dynamic loads and the impact energy. Speed determines the kinetic energy, and is therefore one of the most important factors determining the behaviour of the vehicle, the barrier and the ground or anchoring system during a collision. Another important supplementary parameter is dispersion, understood as the scattering of debris or vehicle components following an impact. However, it is not a fundamental criterion for barrier selection in the same extent as mentioned earlier, rather, it should be taken into account when assessing the risk to people and infrastructure located beyond the safety line.

The relationship between the angle of impact and the vehicle's trajectory, the barrier line, the penetration zone and the debris zone is shown in Figure 2.

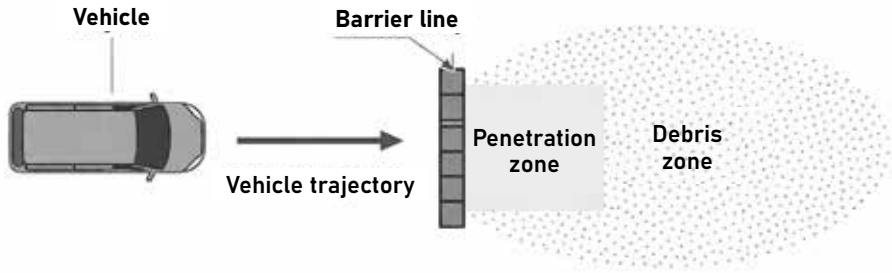


Figure 2. Vehicle collision with a crash barrier, showing the trajectory, the barrier line, the penetration zone and the debris zone.

Source: author's own elaboration.

The angle of impact affects the load-absorption mechanism and determines whether the device operates under conditions similar to those of the tested configuration. Penetration, on the other hand, determines how far a vehicle or its components can intrude beyond the safety line. From the point of view of the safety of those involved in the incident, this parameter is of the utmost importance, as it determines the need to establish a buffer zone. The mere fact that a vehicle has been stopped does not in itself guarantee that the protection is fully effective. If penetration is significant and there are people behind the barrier, the consequences of an incident may still be serious. Therefore, the interpretation of test results must always be linked to planning a safe distance between the VSB line and the space used by event participants²⁰.

The meaning of the term 'tested device'

In market practice, the term 'tested device' is frequently used, but it is sometimes interpreted too broadly. It does not refer to every commercial version of the device or any installation configuration, but rather that a specific device has been tested in a specific test setup.

The concept of configuration 'as tested' is of key importance in this context. The parameters declared for the device relate exclusively to the specific test setup in which the device was actually tested. Any deviation from this configuration – a change in the angle of installation, the number of device segments, the type of substrate, the connection

²⁰ See: J. Jaźwiński, *Anti-terrorist protection of public facilities...*, p. 367, 374–376.

system, the method of anchoring or the installation conditions – may lead to a change in the device's operating mechanism and a loss of the parameters confirmed in the test²¹.

Crash test records – examples

To understand current testing standards, it is essential to interpret the full VSB classification code correctly. This code is not only a technical code but also provides a concise description of the scenario under which the device was tested.

An example of a code under the older classification system:

IWA 14-1: V/7200[N3C]/48/90:29.1

The individual elements of this entry are as follows: V – vehicle used in the test, 7200 – the vehicle's mass expressed in kilograms, N3C – the vehicle category or type according to the adopted classification, 48 – the impact speed expressed in km/h, 90 – the impact angle expressed in degrees, 29.1 – a parameter relating to the displacement or penetration of the vehicle beyond the barrier's reference line.

An example of a notation compliant with the current standard:

ISO 22343-1: V/7,200(N2A)/48/90:2.6/5.0

In this case, the designations are as follows: V – test vehicle, 7,200 – vehicle mass in kilograms (7200), N2A – category of the vehicle used in the test, 48 – impact speed in km/h, 90 – impact angle in degrees, 2.6 – the value of penetration or displacement of the vehicle relative to the reference line, 5.0 – a parameter relating to the secondary effects of the collision, in particular the dispersion of debris or vehicle components.

The full classification record therefore allows one to determine whether the device has been tested and in exactly which test scenario its effectiveness was assessed. This is particularly important when selecting a device for a specific public space, public event or temporary security measure, as even seemingly similar devices may have been tested under different conditions of mass, speed and impact geometry.

²¹ For more on the significance of 'as tested' configurations and the limitations of engineered solutions, see: J. Jaźwiński, *Anti-terrorist protection of public facilities...*, pp. 381–383. See also: *Verifying solutions*, HVMhub, <https://hvmhub.com/products-advice/verifying-solutions/> [accessed: 29 III 2026].

From a design perspective, this is a qualitative shift in approach. Protection cannot be assessed solely in terms of 'stopping the vehicle'. Equally important is the question of what secondary dynamic effects the impact itself may generate, and whether the protected space has been designed with these effects in mind. ISO 22343-1 sets out the method for testing and assessing the resistance of a barrier, whilst ISO 22343-2 helps to translate the test result into design and operational decisions. At the same time, neither ISO nor ASTM suggest that the test result alone automatically guarantees effectiveness in all field conditions – factors such as the ground, road surface, approach geometry and specific local conditions remain significant.

Crash test versus an engineering solution

At the design stage, it is possible to develop an engineering solution based on established calculation principles, taking into account material strength, torques, soil mechanics and the method of anchoring. However, this approach does not replace an actual crash test. An engineering solution may indicate how a device is likely to behave, but only a test confirms its actual behaviour under dynamic conditions.

This difference is of fundamental importance. The impact of a vehicle in a collision is not limited to a simple static load on the structure. It involves complex dynamic processes in which factors such as vehicle deformation, the nature of contact with the structure, the distribution of forces over time, the behaviour of the ground, and secondary displacements of components all play a role.

The significance of the research findings for the design of HVM systems

With regard to the design of HVM systems, the results of crash tests are not purely technical or laboratory-based. They form the direct basis for determining the buffer zone, assessing the safe distance between pedestrians and VSBs, selecting the appropriate device for a specific hazard scenario, assessing the secondary effects of an impact, and verifying whether a given solution actually meets the needs of public space safety. In other words, a crash test is not merely a tool for product certification, but above all a source of data essential for the responsible design of safety measures. Without a correct interpretation of the test results, the entire process of selecting VSBs becomes prone to oversimplification, erroneous analogies and the thoughtless transfer of solutions from one location

or scenario to another, without taking into account local conditions such as the possible impact speed, impact angle, surface type, method of installation, available buffer space and the nature of the protected area.

Design, installation and operational errors in the use of VSBs for securing public spaces and public events

The effectiveness of VSBs depends not only on their technical specifications, as confirmed by crash tests but also on factors such as the choice of device, its installation conditions, the layout of the space and how the system is used in operational conditions. Errors which can lead to a reduction in the effectiveness of the safety measure, even though the device itself formally meets the test requirements, occur precisely at the interface between these elements. This applies to both permanent safety barriers used in public spaces and temporary barriers used during mass gatherings, recurring events, assemblies and outdoor events. The difference between a crowd control solution and a certified VSB is illustrated in Figure 3.

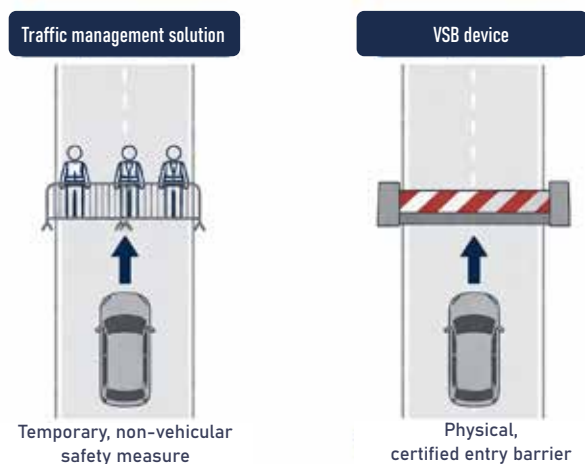


Figure 3. Diagrams illustrating the use of the traffic management solution and VSB.

Source: own elaboration.

Incorrect positioning of the equipment in relation to the access road

One of the key design and installation errors is positioning the device in a configuration that does not correspond to the vehicle's actual approach path. Positioning it at an incorrect angle or along an axis that does not correspond to the vehicle's anticipated trajectory may alter its operating mechanism and reduce the effectiveness of the system. Even a device with excellent performance parameters may not function as expected if it is installed in a spatial configuration different from that for which the security scenario was designed. Particularly advantageous from the point of view of limiting impact energy are those access route layouts in which the vehicle's path is deflected, e.g. at an angle of approx. 90°, and the device is located beyond the bend. Such geometry automatically limits the vehicle's possible speed and makes the safety measure more effective (Figure 4).

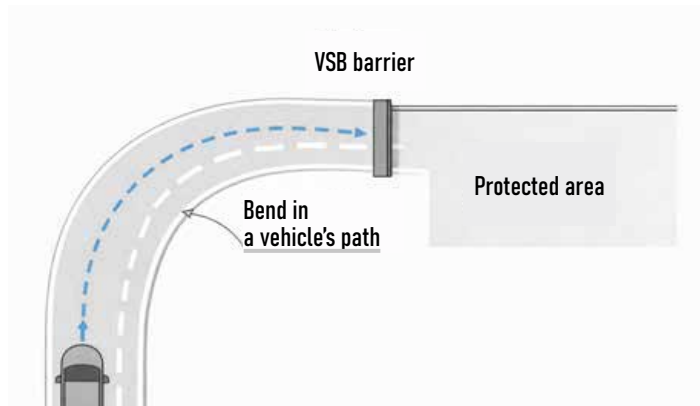


Figure 4. Diagram showing the positioning of the VSB behind a bend in the vehicle's path, restricting the possibility of a direct approach towards the protected area.

Source: own elaboration.

Designing security measures only along the main access routes

One of the more serious systemic errors is to design security measures solely along the main access routes, while leaving side roads, pavements, pedestrian crossings or other areas unsecured. Effective security for a public event requires the designation of a complete security perimeter, i.e. the outer line of the security perimeter marking the boundary of the protected zone, and the identification of all potential access routes, including those that are less obvious, arising from the topography, the proximity of open spaces,

and the possibility of access through adjacent green areas. Figure 5 shows a diagram of the security perimeter around the event site, highlighting access routes and the locations of VSBs, including a barrier situated at the boundary with the park area.

In HVM systems, the effectiveness of security measures depends on their continuity and coherence. Individual devices positioned in the most obvious locations do not, in themselves, constitute a security system if the area as a whole can still be breached from another direction. Security must be assessed across the entire perimeter, rather than solely in terms of selected points.

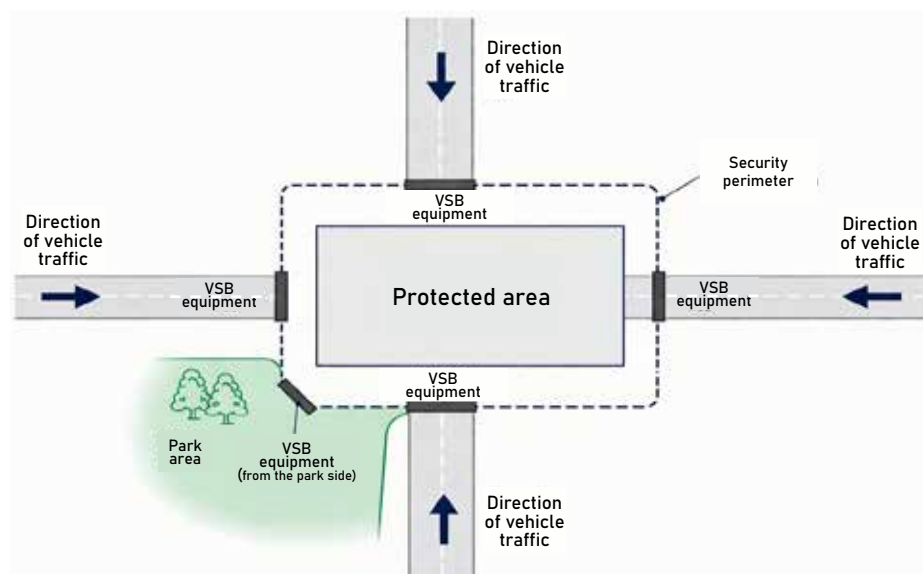


Figure 5. Diagram of the perimeter security zone for the event site, showing access routes and the locations of VSBs, including a barrier at the boundary with the park.

Source: own elaboration.

Installation on an unsuitable surface

A common mistake is to install the equipment on a surface that does not meet the conditions required for its proper operation. In the case of temporary or mobile solutions, the type of surface has a direct impact on the system's stability, friction conditions and the way dynamic loads are transferred during an impact.

The difference between the surface specified by the manufacturer and the surface actually present at the installation site can lead to a significant change in the device's performance, which is sometimes downplayed.

Connection faults in modular systems

In modular systems, the effectiveness of the protection stems from the operation of the entire assembly as a coherent system. One of the more serious installation errors is the failure to connect the segments correctly or the use of an incomplete assembly as specified by the manufacturer. In such cases, this may result in a loss of system continuity, the displacement of adjacent components, or a domino effect. A failure in a single segment can propagate throughout the entire system and lead to a reduction in the effectiveness of the safety measures to a far greater extent than would be indicated by an assessment of the individual component alone.

At public events, this problem is particularly pronounced, as delivery points, technical gates, backstage areas, catering zones, staff access routes, installation prior to the event, and dismantling once it has ended create periods of heightened vulnerability. It is then essential to implement strict access control procedures, temporarily close access points, ensure supervision by security personnel, and clearly assign responsibility for restoring security continuity following each temporary opening of the perimeter.

The lack of a proper buffer zone and failure to take penetration into account

Locating the area designated for event participants too close to the VSBs line is a significant design flaw. A buffer zone must be established behind the safety line. Failing to account for penetration leads to the mistaken belief that the mere presence of the equipment solves the safety issue. However, a vehicle may intrude partially beyond the safety line, and the consequences of an incident may include the displacement of structural components or vehicle parts. For this reason, the buffer zone is one of the fundamental prerequisites for effective protection.

Lack of continuity in security at delivery, service and evacuation points

One of the most common operational errors is failing to ensure the continuity of the security system at locations such as service entrances, delivery points, service access routes, emergency service routes and emergency access routes. Every temporary opening of an access point

represents a period of increased vulnerability, which must be properly identified and managed.

In practice, it is precisely these areas that often constitute the weakest link in the entire system. If security focuses exclusively on the main perimeter, whilst operational points remain poorly controlled, a situation arises in which security is porous.

The human factor, inadequate skills among installation teams and poor operational supervision

A source of risk that requires particular attention is the human factor. No system will function properly if it is installed incorrectly, without adequate supervision and without knowledge of the technical requirements. This applies both to purely installation-related errors and to the improper operation of equipment during an incident. For this reason, protection based on VSBs requires the involvement of competent installation teams, a clear division of responsibilities and effective operational supervision. Otherwise, even a well-designed system remains vulnerable to operational and organisational errors.

Street furniture and organisational equipment as makeshift security measures

In many towns and cities, it is common to see street furniture such as concrete planters, bollards, decorative blocks or other urban barriers being used as a means of restricting vehicle access to pedestrian zones. Solutions of this type may serve an organisational or regulatory function, but in most cases they do not constitute VSBs (Image 4).



Image 4. Barriers – security measure that is not a VSB (Berlin).

Source: author's archive.

The presence of a physical barrier, passenger car or a city bus, IBC container or lightweight planters is sometimes mistakenly equated with the existence of a genuine security measure (Image 5). Such solutions may temporarily restrict access for organisational purposes, organise the space or force drivers to reduce their speed, but they do not constitute a certified VSB and do not ensure predictable energy absorption parameters in the event of an impact by a heavier vehicle. However, without verified test parameters, without the correct configuration and without reference to a specific threat scenario, such elements merely create an illusion of security²².



Image 5. An IBC container – element of the traffic management solution that is not a VSB (Poland).

Source: author's archive.

Heavy concrete blocks (barriers) or certified planters with a significant dead weight may form part of a temporary system, but only if their function and method of installation correspond to the adopted hazard scenario. However, they should not be equated with certified VSBs (Images 6, 7).

²² Cf. J. Jaźwiński, *Anti-terrorist protection of public facilities...*, pp. 367–369; M. Cichomski, *How can local governments protect public spaces...*, pp. 499–507.



Image 6. Planters – elements of street furniture serving organisational or potentially protective function. Whether they are classified as VSBs depends on their certification and the scenario in which they are used (Rome).

Source: author's archive.



Image 7. Concrete barriers – a solution with organisational or potentially protective function. Whether they are classified as VSBs depends on their certification and the scenario in which they are used (Paris).

Source: author's archive.

Conclusions from the analysis of errors in the use of VSBs

An analysis of design, installation and operational errors leads to the unequivocal conclusion that the effectiveness of HVM systems depends not only on the parameters of the VSBs themselves, but above all on the quality of the entire process of designing, installing and operating the system. This means that even a certified and properly tested device does not guarantee an adequate level of protection if it is incorrectly selected,

improperly positioned, faulty installed or used in a space designed without taking the actual hazard scenario into account.

Designing HVM systems in public spaces

The design of HVM systems in public spaces cannot simply involve the placement of individual VSBs in locations intuitively deemed to be critical. An effective protection system requires a sequential approach, in which decisions regarding the selection of devices, the geometry of their placement, the organisation of the space and the manner of use are based on a prior risk and site analyses. Adhering to this sequence determines the difference between real and apparent security.

Risk analysis

Risk analysis should be the fundamental stage in designing a system to protect public spaces against vehicle-borne attacks, which serves as the starting point for determining the type and specifications of VSBs to be used at a given location. Without it, the selection of devices becomes an intuitive process that does not reflect the actual threat.

This analysis should cover at least the following: the nature of the protected area, the profile of the event, the anticipated number of participants, the symbolic significance of the location, possible scenarios for the perpetrator's actions, local traffic conditions, and the potential consequences of a vehicle intrusion. Only by taking all these factors into account is it possible to move from a general assessment of the problem to the formulation of specific security requirements²³.

Analysis of the access route and vehicle-borne attack scenario

The road infrastructure enables a potential attacker to use a vehicle as a weapon. Therefore, an analysis of the access routes leading to the protected area is of fundamental importance for the design of VSBs.

At this stage, it is necessary to determine which vehicles could be used at a given location, at what speed they could reach the protected area, from which directions they could intrude, and what terrain conditions might

²³ Cf. J. Jaźwiński, *Anti-terrorist protection of public facilities...*, pp. 369-372; M. Cichomski, *How can local governments protect public spaces...*, pp. 493-499.

influence the course of a potential attack. Designing an effective HVM system requires not abstract thinking about a 'vehicle', but the most precise possible definition of the attack scenario involving its use.

Establishment of a protection zone and a security perimeter

Following a risk analysis and an assessment of access routes, it is necessary to designate a protection zone and define the security perimeter. This process involves the deployment of VSBs and the organisation of the space behind the security line. From a security perspective, what lies behind the devices and at what distance from the anticipated impact zone is as important as the positioning of the devices themselves.

The perimeter should be defined comprehensively. Security measures must cover all realistic points of entry, taking into account technical access points, emergency access routes, side passageways and any locations that could be used to bypass the main security line.

Selection of VSBs for a hazard scenario

The selection of devices designed to protect against vehicle-borne attacks should be based directly on the risk analysis and threat scenario. There is no universal VSB suitable for all possible situations. In design practice, one of the most frequently analysed scenarios involves an attack using a vehicle weighing approx. 7.5 tonnes, travelling at a speed of around 50 km/h and 64 km/h, depending on the test standard adopted, the classification of the device and the design specifications. However, the cited model cannot be automatically applied in all locations.

The choice of equipment must take into account the test parameters, the type of surface, the nature of the space (e.g. a town square, a square in front of a stadium, a concert area, an access road, an event's technical facilities, etc.), logistical constraints, installation requirements, the need to maintain passageways and access for emergency services, and the ability to ensure continuous security throughout the event.

Supervision of the installation and organisational responsibility

Before the temporary VSB installation is authorised for use, it can be verified against a checklist. This checklist has been drawn up on the basis of an analysis of the design, installation and operational issues discussed in the article, as well as the author's practical experience relating to the selection and use of vehicle intrusion prevention devices. It consists of:

- compatibility of the device used with the adopted hazard scenario, particularly in terms of vehicle type, direction of impact and anticipated speed;
- compliance of the installation with the 'as tested' configuration, if the declared parameters of the device relate to a specific mounting arrangement, method of connection or type of substrate;
- assessment of the technical condition of the devices and the completeness of the system components, including modular connections and stabilising elements;
- verification of the type and load-bearing capacity of the substrate in relation to the conditions required for the device to function correctly;
- correctness of the alignment of the equipment relative to the access road, taking into account the approach axis, turning radii and the possibility of bypassing the safety barrier;
- continuity check of the safety line to ensure that no gaps or side openings are left between the equipment that would allow a vehicle to enter the protected zone;
- designation of a buffer zone behind the line of devices, taking into account the anticipated vehicle penetration and possible secondary effects of a collision;
- establishment of operating rules for delivery points, service access points and emergency entrances, together with a procedure for restoring the continuity of the safety system following their temporary opening;
- establishment of procedures for authorised vehicles and ensuring that routes remain clear for emergency and security services, whilst maintaining the integrity of the security system;
- acceptance of the installation by a competent person, together with confirmation of the system's operational readiness prior to the start of the event.

For recurring projects, the checklist should include a requirement for a brief training for the technical teams and confirmation of acceptance by a competent person on the part of the organiser or the venue owner. This measure reduces the risk of human error and helps to ensure that the installation complies with the design specifications.

An example of the preparation and training-based deployment of temporary barriers prior to a public event is shown in Image 8.

Even the best-suited device will not provide an adequate level of protection if it is installed incorrectly. For this reason, the design of an HVM system should include the selection of devices and the organisation of their installation, commissioning and operational supervision.

In European practice, a model is commonly found in which specialist organisations are responsible for both the selection and installation of systems designed to protect public spaces against vehicle-borne attacks. Such solutions have been adopted in the United Kingdom, where a systematic approach to the protection of public spaces is supported by the development of legislation relating to Martyn's Law. The conclusion is clear – an effective system requires not only equipment, but a competent implementation process.



Image 8. Installation of temporary barriers as part of the security preparations for a public event, and a trial placement of barriers (Warsaw).

Source: DFE Security Sp. z o.o. materials.

Zone-based and layered protection

An adequate effectiveness of an HVM system is ensured by an approach known as zonal or layered security. This involves designing security measures in such a way that a breach of one level of protection does not automatically result in full access to the protected zone.

The layered protection may include, among other things, a combination of VSBs, urban planning solutions, access control, traffic management, operational surveillance and the appropriate design of buffer zones.

The advantage of this system lies in the fact that it distributes security from a single line of defence across a sequence of complementary measures.

Evacuation airlocks and controlled access points in permanent and temporary set-ups

One of the more sophisticated models for safeguarding public spaces during public events is a systemic approach in which permanent and temporary security measures complement one another. Such a model can be applied particularly in city centres, on main streets and in squares, where normal traffic flows on a day-to-day basis, while during an event it becomes necessary to temporarily take control of access to the protected zone.

This solution involves equipping the main access routes to the event area with permanent, automatic vehicle barriers, which can be lowered outside event hours to allow normal traffic flow. When event-related procedures are activated, the barriers are raised and take on the role of providing primary protection for the main transport route. At the same time, side streets, underpasses and other potential bypass routes are secured with additional temporary measures to ensure the continuity of protection across the entire zone.

Of particular importance here is the 'airlock' solution, understood as a controlled access point for authorised vehicles (Image 9). In this arrangement, a vehicle first enters a designated zone between successive security lines. Once the first section of the barrier has closed, the vehicle may be stopped, verified and subjected to a security check in accordance with the security plan. Only once authorisation has been confirmed is the next section of the passage opened. This solution allows for the simultaneous maintenance of perimeter security, the safe conduct of evacuations, the passage of law enforcement and emergency services, as well as the implementation of vehicle inspection procedures for vehicles entering the event zone. The advantage of this model is its flexibility. The same location can operate in two modes: everyday use and temporary event security.



Image 9. An airlock solution in an urban setting – a controlled access point and traffic separation point (Berlin).

Source: author's archive.

From a safety design perspective, the airlock model is a particularly valuable, as it combines the requirement for infrastructure resilience with the need to maintain evacuation routes, access for emergency services and access control. Such solutions demonstrate that an effective HVM system does not rely solely on the installation of a single barrier, but on the deliberate design of the entire operational model of the space in the event of an incident (Image 10).



Image 10. VSB – a permanent solution that works in conjunction with traffic management and the protection of public spaces (Frankfurt).

Source: author's archive.

Security by design in the planning of public spaces

The ‘security by design’ approach is becoming increasingly important in the design of public spaces. This approach involves taking security aspects into account right from the urban planning stage or when organising event spaces. In such a model, developed at European level, security is not an afterthought but an integral part of the spatial design²⁴. The earlier security requirements are taken into account, the greater the possibility of harmoniously integrating them with the functionality of the space, the aesthetics of the location and the needs of users. In the context of HVM system, this means the possibility of shaping the spatial layout in such a way as to reduce vulnerability to vehicle intrusion, before such a pressing need arises. Examples of VSBs integrated into a public space is shown in Images 11 and 12.



Image 11. VSBs manually activated – a solution integrated with the public space.

Source: *Unafor. Certified Hostile Vehicle Mitigation with Design in Mind*, Crowdguard, <https://www.crowdguard.co.uk/products/unafor/> [accessed: 29 III 2026].

²⁴ Cf. *Protection of public spaces...*; *Protection*, European Commission, 23 IX 2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection_en [accessed: 12 IV 2026]; *EU Protective Security Advisors (EU PSA)*, European Commission, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [accessed: 12 IV 2026].



Image 12. Temporary mobile VSBs – a solution integrated with the public space.

Source: *ATG Surface Guard*, Crowdguard, <https://www.crowdguard.co.uk/products/atg-surface-guard/> [accessed: 29 III 2026].

Final recommendations for the design of HVM systems

When designing HVM systems, it is advisable to follow a few principles. Firstly, the starting point should always be a risk analysis, rather than the choice of equipment. Designing security measures from a product-centred perspective, without first identifying the threat scenario, almost always results in the measures being ill-suited to the site's actual vulnerabilities. In practice, this means that decisions regarding purchase or hire should be secondary to the conclusions drawn from the analysis.

Secondly, a detailed analysis of all access routes and realistic directions from which a vehicle might intrude is essential. Designing security measures solely for the main entrance provides partial protection and is therefore vulnerable to circumvention. For each event, the perimeter should be assessed as a whole, including service roads, footpaths and service routes.

Thirdly, the selection of VSBs should be based on a specific threat scenario, rather than on marketing claims. Test parameters, the 'as tested' configuration, installation conditions and the device's compatibility with the actual spatial layout are of key importance. A product that is unsuitable for the location and scenario does not provide effective protection, even if it has a high test rating in its own right.

Fourthly, the design of protective measures must take into account vehicle penetration and, consequently, the need to define a buffer zone. The safe zone does not begin at the centreline of the device, but only beyond the area of potential impact from the vehicle, its fragments and debris. Omitting this aspect leads to a misleading perception of the level of safety.

Fifthly, an effective system should be layered, spatially coherent and subject to operational oversight. Security cannot rely on a single measure or a single decision-making point. A high level of security is achieved through a combination of infrastructure, procedures, human expertise and the appropriate organisation of space²⁵.

Sixthly, greater emphasis should be placed on incorporating the principles of 'security by design' into the planning of public spaces and events. The earlier security requirements are integrated into the design of a venue or the organisation of an event, the less need there will be for temporary solutions. In the long term, this approach is more effective, cost-efficient and consistent with a modern approach to risk management.

Local authorities' responsibility for the safety of public spaces in Poland

In the Polish context, local authorities bear particular responsibility for developing systemic mechanisms to protect public spaces. They are responsible for organising many events, managing space and planning expenditure related to safety. For this reason, local authorities should not limit themselves to responding to day-to-day organisational needs, but should establish sustainable HVM/VSB standards for recurring events, plan budgets in advance and draw on the expertise of specialised consultants²⁶. It is at local government level that these issues may be institutionalised. Without the involvement of local authorities, the protection of public spaces will continue to develop in a fragmented, reactive manner, dependent on ad hoc organisational decisions. From the point of view of public safety, this model is inadequate.

²⁵ See: *HVM specifying – some things to consider*, HVMhub, <https://hvmhub.com/products-advice/spec-writing-guidance/> [accessed: 29 III 2026].

²⁶ See: M. Cichomski, *How can local governments protect public spaces ...*, pp. 490–492, 505–507.

The selection of entities involved in the design, supply, installation and maintenance of HVM systems and VSBs is also of significant importance. With regard to public safety infrastructure, it is advisable to use entities with the appropriate authorisations, including a licence from the Ministry of the Interior and Administration, and, in cases involving access to sensitive information concerning security arrangements, system configuration, operating procedures or the identification of vulnerabilities, appropriate safeguards regarding the protection of classified information must also be in place²⁷. In certain circumstances, this may mean that an industrial security certificate is required, issued by the Internal Security Agency. This is because the disclosure of information concerning the system's operation, its organisation or installation faults to unauthorised persons may reduce the effectiveness of security measures and increase the vulnerability of public spaces to security breaches.

Summary

The most important conclusion drawn from the article is that protecting public spaces against vehicle-borne attacks requires a systemic approach. It cannot rely on the ad hoc deployment of individual devices or on the use of solutions that are purely regulatory in nature. The effectiveness of the system depends on a combination of risk analysis, the correct identification of access routes, the appropriate selection of VSBs, correct installation, the maintenance of continuous protection throughout the entire secured area, and effective operational supervision.

The issue of protecting public spaces against vehicle-borne attacks in Poland requires further clarification, both in terms of threat assessment and the principles governing the selection, installation and use of VSBs within HVM systems. This applies in particular to the need for wider use of security measures based on research data, technical standards and realistic threat scenarios. Among the most significant problems are

²⁷ See: *Ochrona informacji niejawnych* (Eng. Protection of classified information), Agencja Bezpieczeństwa Wewnętrznego, <https://www.abw.gov.pl/pl/o-abw/zadania/7,Ochrona-informacji-niejawnych.html> [accessed: 4 V 2026]; *Bezpieczeństwo przemysłowe* (Eng. Facility security), <https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-przemys/148%2CBEZPIECZENSTWO-PRZEMYSLOWE.pdf> [accessed: 4 V 2026].

insufficient planning of financial resources allocated to the protection of public spaces, the use of standard security measures instead of certified protective devices, and the selection of solutions without reference to vehicle parameters, impact energy and the actual function of VSBs.

The most serious technical errors include leaving side access routes, using standard security devices instead of VSBs, failing to take into account penetrations and the necessary buffer zone, as well as a lack of system continuity at technical and service points. These errors are structural in nature, as they stem not only from a lack of equipment, but above all from an incorrect assessment of the threat and a superficial approach to security.

In this context, it is worth recalling the incident in Sopot in July 2014, when a driver drove a car onto Bohaterów Monte Cassino Street and then onto the pier, injuring many people. This incident was not of a terrorist nature, but it does confirm that the threat posed by the use of a vehicle in public spaces should be taken seriously in the Polish context as well²⁸.

From an organisational perspective, it is advisable to implement fixed HVM/VSB standards for recurring events, to draw on the expertise of specialist consultants or organisations with expertise in the design and installation of VSBs, and to plan the security budget well in advance. Without such measures, security will continue to depend on ad hoc decisions rather than on a coherent security policy²⁹.

By way of comparison, it can be said that Poland is currently in a transitional phase. The protection of public spaces against vehicle-borne attacks is increasingly recognised, but is still not being developed in a systemic manner. For this reason, it remains appropriate to draw on the experience of countries that have previously faced such threats and developed more mature legal, organisational and technical solutions, in particular the United Kingdom, Germany and France.

The particular importance of this issue stems from the fact that it concerns not closed infrastructure or solely facilities of strategic importance, but public spaces used by members of the community. Anyone attending a concert, a fair, a sporting event, a religious ceremony

²⁸ Cf. *Szaleńczy rajd w Sopocie. Kierowca wjechał w grupę ludzi* (Eng. A reckless drive in Sopot. A driver ploughed into a group of people), RMF24, 20 VII 2014, <https://www.rmf24.pl/news-szalenczy-rajd-w-sopocie-kierowca-wjechał-w-grupe-ludzi,nId,1471791> [accessed: 12 IV 2026].

²⁹ Cf. M. Cichomski, *How can local governments protect public spaces...*, pp. 487–492; J. Jaźwiński, *Anti-terrorist protection of public facilities...*, pp. 406–407.

or a gathering in open space may find themselves within the potential impact zone of such a threat.

Bibliography

Cichomski M., *How can local governments protect public spaces from vehicle attacks?*, "Terrorism – Studies, Analyses, Prevention" 2025, no. 8, pp. 487–516. <https://doi.org/10.4467/27204383TER.25.062.23049>.

Hess P., Mandhan S., *Ramming attacks, pedestrians, and the securitization of streets and urban public space: a case study of New York City*, "Urban Design International" 2022, vol. 28, no. 1, pp. 19–34. <https://doi.org/10.1057/s41289-022-00180-2>.

Jaźwiński J., *Anti-terrorist protection of public facilities and critical infrastructure against attacks with motor vehicles*, "Terrorism – Studies, Analyses, Prevention" 2023, no. 3, pp. 361–409. <https://doi.org/10.4467/27204383TER.23.011.17451>.

Karlos V., Larcher M., Solomos G., *Review on vehicle barrier protection guidance*, Publications Office of the European Union, European Commission, Joint Research Centre, 2017. <https://doi.org/10.2760/845599>.

Ludbey C.R., Versaci D., Bharthur S., Prabhakaran S., *Classifying vehicle-as-a-weapon attacks: an inductive taxonomy and design implications*, "Crime Science" 2026, vol. 15, art. 2. <https://doi.org/10.1186/s40163-025-00265-7>.

Miller V., Hayward K.J., *'I Did My Bit': Terrorism, Tarde and the Vehicle Ramming Attack as an Imitative Event*, "The British Journal of Criminology" 2019, vol. 59, no. 1, pp. 1–23. <https://doi.org/10.1093/bjc/azy017>.

Phillips J.P., Young J.S., Brady W.J., *Preparation and response to a targeted automobile ramming mass casualty (TARMAC) attack: An analysis of the 2017 Charlottesville, Virginia TARMAC attack*, "American Journal of Disaster Medicine" 2019, vol. 14, no. 3, pp. 219–223. <https://doi.org/10.5055/ajdm.2019.0333>.

Tsur A.M., Nadler R., Sorkin A., Lipkin I., Gelikas S., Chen J., Benov A., *Patterns in vehicle-ramming attacks*, "Israel Medical Association Journal" 2022, vol. 24, no. 9, pp. 579–583.

Internet sources

ATG Surface Guard, Crowdguard, <https://www.crowdguard.co.uk/products/atg-surface-guard/> [accessed: 29 III 2026].

Bezpieczeństwo przemysłowe (Eng. Facility security), <https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-przemys/148%2C-BEZPIECZENSTWO-PRZEMYSLOWE.pdf> [accessed: 4 V 2026].

EU Protective Security Advisors (EU PSA), European Commission, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [accessed: 12 IV 2026].

Hostile Vehicle Guidelines for Crowded Places, <https://www.nationalsecurity.gov.au/crowded-places-subsite/Files/hostile-vehicle-guidelines-crowded-places.pdf> [accessed: 20 VI 2026].

Hostile Vehicle Mitigation ISO 22343-1:2023 NPSA Guidance Note, <https://www.npsa.gov.uk/system/files/documents/npsa-hvm-guidance-note-iso-22343-1-feb-2024.pdf> [accessed: 12 IV 2026].

HVM – Vehicle Impact Testing and FEA Computational Analysis Guidance Note, <https://www.npsa.gov.uk/system/files/documents/npsa-guidance-note-hvm-vehicle-impact-testing-and-fea-computational-analysis-15-july-2021.pdf> [accessed: 29 III 2026].

HVM specifying – some things to consider, HVMhub, <https://hvmhub.com/products-advice/spec-writing-guidance/> [accessed: 29 III 2026].

Impact Testing of Vehicle Security Barriers. An overview of vehicle impact test standards, <https://www.npsa.gov.uk/system/files/documents/npsa-impact-testing-of-vehicle-security-barriers-18-august-2020.pdf> [accessed: 29 III 2026].

Martyn's Law: the SIA's New Regulatory Role, Security Industry Authority, <https://www.gov.uk/government/publications/martyns-law-the-sias-new-regulatory-role/martyns-law-the-sias-new-regulatory-role> [accessed: 12 IV 2026].

Ochrona informacji niejawnych (Eng. Protection of classified information), Agencja Bezpieczeństwa Wewnętrznego, <https://www.abw.gov.pl/pl/o-abw/zadania/7,Ochrona-informacji-niejawnych.html> [accessed: 4 V 2026].

Poprawiamy bezpieczeństwo w stolicy. Rozstawiamy bariery antyterrorystyczne i szkolimy z ich obsługi (Eng. We are improving safety in the capital. We are installing anti-terrorist barriers and providing training on how to use them), Zarząd Dróg Miejskich w Warszawie, 17 III 2026, <https://zdm.waw.pl/aktualnosci/poprawi>

amy-bezpieczenstwo-w-stolicy-rozstawiamy-bariery-antyterrorystyczne-i-szkolimy-z-ich-obslugi/ [accessed: 12 IV 2026].

Primer on Impact Protection for Critical Transportation Infrastructure, FHWA-HIF-18-054, Federal Highway Administration, 2018, <https://www.fhwa.dot.gov/bridge/security/hif18054.pdf> [accessed: 15 VI 2026].

Protection of public spaces from terrorist attacks, European Commission, Joint Research Centre, https://joint-research-centre.ec.europa.eu/projects-and-activities/protection-public-spaces-terrorist-attacks_en [accessed: 12 IV 2026].

Protection, European Commission, 23 IX 2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection_en [accessed: 12 IV 2026].

Public Realm Design Guide for Hostile Vehicle Mitigation, National Protective Security Authority, <https://www.npsa.gov.uk/specialised-guidance/hostile-vehicle-mitigation-hvm/public-realm-design-guide-hostile-vehicle-mitigation-0> [accessed: 12 IV 2026].

Schutz öffentlicher Räume vor Überfahrtaten, Polizeiliche Kriminalprävention der Länder und des Bundes, <https://www.polizei-beratung.de/themen-und-tipps/staedtebau/schutz-vor-ueberfahrtaten/> [accessed: 12 IV 2026].

Se protéger contre les attaques au véhicule-bélier, Secrétariat général de la défense et de la sécurité nationale, 11 VI 2018, <https://www.sgdsn.gouv.fr/publications/se-proteger-contre-les-attaques-au-vehicule-belier> [accessed: 12 IV 2026].

Szaleńczy rajd w Sopocie. Kierowca wjechał w grupę ludzi (Eng. A reckless drive in Sopot. A driver ploughed into a group of people), RMF24, 20 VII 2014, <https://www.rmfm24.pl/news-szalenczy-rajd-w-sopocie-kierowca-wjechał-w-grupe-ludzi,nId,1471791> [accessed: 12 IV 2026].

Unafor. Certified Hostile Vehicle Mitigation with Design in Mind, Crowdguard, <https://www.crowdguard.co.uk/products/unafor/> [accessed: 29 III 2026].

Vehicle Ramming Action Guide, Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide> [accessed: 20 VI 2026].

Verifying solutions, HVMhub, <https://hvmhub.com/products-advice/verifying-solutions/> [accessed: 29 III 2026].

Legal acts

Terrorism (Protection of Premises) Act 2025, UK Public General Acts 2025 c. 10, <https://www.legislation.gov.uk/ukpga/2025/10/contents> [accessed: 12 IV 2026].

Norms and standards

ASTM F2656/F2656M-20 Standard Test Method for Crash Testing of Vehicle Security Barriers, https://store.astm.org/f2656_f2656m-20.html [accessed: 20 VI 2026].

British Standards Institution, PAS 68:2013 Impact test specifications for vehicle security barrier systems, <https://knowledge.bsigroup.com/products/impact-test-specifications-for-vehicle-security-barrier-systems> [accessed: 12 IV 2026].

ISO 22343-1:2023 Security and resilience – Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating, <https://www.iso.org/standard/50080.html> [accessed: 20 VI 2026].

ISO 22343-2:2023 Security and resilience – Vehicle security barriers – Part 2: Application, <https://www.iso.org/standard/81415.html> [accessed: 12 IV 2026].

IWA 14-1:2013 Vehicle security barriers – Part 1: Performance requirement, vehicle impact test method and performance rating.

PN-EN 1317 Road restraint systems.

Jarosław Jaźwiński

Specialist in the field of technical and anti-terrorist security, particularly the protection of public spaces, mass events and infrastructure against vehicle-borne attacks. Expert of the Polish Chamber of Persons and Property Security and the Polish Employers' Association Protection, speaker at industry and academic conferences. Author of publications on anti-terrorist protection of public facilities.

Contact: jarek.j@dfes.pl



VARIA



The civil aviation security system as an example of strengthening critical infrastructure resilience

Karol Dymek

Independent author

 <https://orcid.org/0009-0004-3946-8695>

Introduction

After more than a decade of working in the field of civil aviation security at various levels within organisations conducting or supervising aviation activities – including serving as a quality control auditor at both the European and national levels – I have become convinced that no solutions exist that can guarantee a one hundred percent security. The pace of change in today's world is giving rise to new threats and new sources from which they originate. The media are increasingly reporting on threats to online banking, on social media account hacks aimed at spreading disinformation in connection with the war in Ukraine, and on fire, for example in shopping centres¹ or in courier shipments that catch

¹ *Zarzuty w związku z pożarem hali przy ul. Marywilskiej 44* (Eng. Charges relating to the fire at the shopping centre on Marywilska Street 44), Prokuratura Krajowa, 12 V 2025, <https://www.gov.pl/web/prokuratura-krajowa/zarzuty-m44> [accessed: 15 III 2026].

fire². The aviation industry, which is regarded as one of the safest modes of transport, is not immune to incidents that pose a threat, despite its high level of regulation and numerous security procedures. It should be borne in mind that airlines and airports are part of critical infrastructure (CI). There are many specialist professional groups within the aviation industry whose role is to ensure the smooth and safe operation of the entire system. To make this possible, aviation activities are subject to strict legal regulations, numerous rules and procedures.

It is said in the industry that most aviation regulations are written in blood. The event that changed the modern world and had a major impact on the approach to civil aviation security was the attack on the World Trade Center carried out on 11 September 2001³.

In civil aviation, safety and security are of paramount importance. Air disasters – when they occur – often have international implications, given that the aircraft carries passengers from many different countries. The Pan Am airline has learnt the hard way that even minor breaches of safety regulations can have disastrous consequences. The company went bankrupt, partly as a result of the plane crash near the Scottish town of Lockerbie when a bomb exploded in checked-in luggage stored in the hold⁴.

Civil aviation security is not limited to the elements that are immediately visible to travellers, such as the presence of security staff in the terminal or security checks on passengers and their luggage. Aviation security constitutes a complex ecosystem, encompassing suppliers

² *Akt oskarżenia w sprawie aktów sabotażu na rzecz rosyjskiego wywiadu* (Eng. Indictment in the case of acts of sabotage on behalf of the Russian intelligence services), Prokuratura Krajowa, 16 I 2026, <https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-w-sprawie-aktow-sabotazu-na-rzecz-rosyjskiego-wywiadu> [accessed: 15 III 2026].

³ K. Izak, *Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA*, "Przegląd Bezpieczeństwa Wewnętrznego" 2021, no. 25, pp. 341–369. <https://doi.org/10.4467/20801335PBW.21.033.14310>.

⁴ B. Makowski, I. Mazurek, *Zamach w Lockerbie. Kto stał za śmiercią 270 ofiar?* (Eng. The attack in Lockerbie. Who was responsible for the deaths of 270 victims?), Polskie Radio 24, 21 XII 2025, <https://polskieradio24.pl/artykul/2236228,zamach-w-lockerbie-kto-stal-za-smiercia-270-ofiar> [accessed: 15 III 2026]; M. Walków, *30 lat od jednego z największych zamachów w lotnictwie cywilnym* (Eng. Thirty years on from one of the worst civil aviation disasters), Business Insider Polska, 21 XII 2018, <https://businessinsider.com.pl/wiadomosci/30-lat-od-jednego-z-najwiekszych-zamachow-w-lotnictwie-cywilnym/2p7f04t> [accessed: 15 III 2026]; D. Cowan, *Lockerbie bombing suspect appears in court*, BBC, 16 XII 2023, <https://www.bbc.com/news/uk-scotland-67659046> [accessed: 15 III 2026].

to airports (e.g. duty-free shops, fuel suppliers) and aircraft (e.g. catering), as well as logistics companies handling air cargo and many more. All of this forms interconnected supply chains that often extend beyond the airport grounds, reaching as far as the manufacturers of the goods in question.

My professional experience shows that the entities mentioned above have various approaches to security of goods and facilities. Particular sectors operate within different legal and financial frameworks, which means they have different priorities when it comes to security. In practice, it is sometimes the case that even meeting the basic requirements set out in the regulations concerning security⁵ can be difficult for them. These requirements concern, among other things, the development of appropriate procedures, the determination of the point at which in-flight supplies or cargo become traceable and from which a restricted-access regime must be ensured, the conduct of analyses regarding groups of people who may have unsupervised access to goods and security-restricted areas, as well as the carrying out of background checks on staff, which will be discussed later in the article.

Security and safety

To begin with, it is worth clarifying the meanings of the terms ‘security’ and ‘safety’ in the aviation context. These words are often used interchangeably, which can lead to misunderstandings within the industry, as they refer to different areas.

The term *safety* refers to operational safety, i.e. the safe conduct of aviation operations both on the ground and in the air. In this context, *safety* in English concerns the prevention of accidents and incidents in the broadest sense. In simple terms, it is the aviation equivalent of health and safety at work, covering protection against threats arising from both animate and inanimate factors, i.e. threats beyond human control caused by human factor, as well as errors in organisational management, etc.

⁵ This concerns the regulations regarding both international, e.g. *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security* (Official Journal of the EU L 299/1 of 14 XI 2015), and national regulations, e.g. *Regulation of the Minister of Infrastructure of 2 December 2020 on the National Civil Aviation Security Programme* (Journal of Laws of 2021, item 774).

Security in English, on the other hand, refers to a set of measures taken to counter deliberate and unlawful acts. Staff carrying out aviation security tasks include, among others, those conducting security checks, as well as Police and Border Guard officers. These operations in the field of security are not limited to activities carried out exclusively by specialist services, but also include the use of security measures by staff, such as physically securing goods exempt from screening during their transport.

In everyday practice, safety and security at the airport go hand in hand. Every aircraft crew member, airport employee and person carrying out duties within the airport is obliged to comply with the requirements relating to both operational safety and aviation security.

An example of the difficulties involved in using terminology accurately can be seen in the content published on the International Civil Aviation Organization (ICAO) website. Their often inaccurate translation from English into Polish, e.g. using browser-based translation tools, leads to a blurring of the terminological distinctions between concepts. For example, in the case of documents relating to security culture – which I will discuss in more detail later – automatic translation tools incorrectly translate ‘security’ as ‘bezpieczeństwo’ rather than ‘ochrona’. Therefore, the term ‘screening’ (kontrola bezpieczeństwa) that I have mentioned should be translated as ‘kontrola ochrony’, but in Polish such a phrase does not exist in the context in question and would sound absurd.

For this reason, it is particularly important to adopt a critical approach to information sources, to use AI-based tools and translation services with caution, as well as to properly understand and distinguish between security and safety regulations. The fact that certain policies, procedures and mechanisms can be effectively applied in both the security and safety domains may present an additional complication, but it can also be a significant advantage.

Consequently, the similarities in the meaning of both terms in Polish may cause confusion among those attempting to explore these two issues.

A few words on the legal basis for security

Law concerning aviation and its protection has an international scope. Common standards are derived from legislation adopted by the ICAO.

At its core is the Convention on International Civil Aviation⁶ of 1944, also known as Chicago Convention, regulating civil aviation worldwide. It has established the ICAO, an organisation authorised to draft international aviation legislation. The Chicago Convention comprises as many as 19 annexes covering a wide range of topics, including civil aviation security (Annex 17)⁷. In addition, the ICAO publishes a manual for states and organisations implementing civil aviation security regulations⁸, which is a restricted-access document.

In Poland, the regulations are governed by the Chicago Convention, however, due to Poland's membership in the European Union, regulations of the European Commission and the Council of Europe on civil aviation security apply within Polish territory. The legal basis for the civil aviation security system is the *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002*⁹. In this regulation, an interpretation for the application of Annex 17 to the Chicago Convention was established. It harmonises the requirements relating to key elements of the civil aviation security system across the entire EU. In addition to setting out the general scope of Member States' responsibilities, this act also stipulates the obligation to adopt detailed implementing acts at national level. Annex I to this regulation¹⁰ lists 12 aspects of civil aviation security, including airport security, aircraft security, as well as cargo and mail security.

The Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security of 2008 can be regarded as a kind of constitution for civil aviation security in the EU, for which implementing regulations had to be issued. The most important of them is

⁶ *Convention on International Civil Aviation, signed in Chicago on 7 December 1944* (Journal of Laws of 1959, no. 35, item 212, as amended).

⁷ *Annex 17 to the Convention on International Civil Aviation Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Civil Aviation Authority, https://ulc.gov.pl/_download/prawo/prawo_miedzynarodowe/konwencje/Zalacznik_17_Ochrona_lotnictwa_wydanie_12_zm_18.pdf [accessed: 15 III 2026].

⁸ *Aviation Security Manual* (Doc 8973 – Restricted), 2022, ICAO, <https://www.icao.int/aviation-security-policy-section/SecurityManual> [accessed: 15 III 2026].

⁹ Official Journal of the EU L 97/72 of 9 IV 2008.

¹⁰ *Annex I Basic standards for safeguarding civil aviation against acts of unlawful interference (article 4) to the Regulation of the European Parliament and of the Council of 11 March 2008 on common rules...*

the *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security*.

In turn, this regulation was supplemented by the *Commission Implementing Decision C(2015) 8005 final of 16 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security containing information, as referred to in point (a) of Article 18 of Regulation (EC) No 300/2008*¹¹. This decision has not been published in the Official Journal of the EU. The provisions contained therein are of a sensitive nature and are directed on a limited access basis to specific entities and persons holding positions in the civil aviation security system.

At the level of national law, the most important piece of legislation concerning the civil aviation security is the *Act of 3 July 2002 – Aviation Law*¹². Section IX, *Civil Aviation Security*, sets out the civil aviation security requirements within the national legal framework. However, the essential part of these regulations consists of statutory powers to issue implementing acts specifying the detailed requirements. These include:

- *Regulation of the Minister of Infrastructure of 2 December 2020 on the National Civil Aviation Security Programme,*
- *Regulation of the Minister of Infrastructure of 5 November 2020 on the National Quality Control Programme in the field of civil aviation security*¹³,
- *Regulation of the Minister of Infrastructure of 26 July 2021 on the National Civil Aviation Security Training Programme*¹⁴.

It is precisely these regulations that supplement the aforementioned requirements of the European regulations I mentioned earlier. They form three pillars on which the civil aviation security system is based.

¹¹ Civil Aviation Authority, <https://ulc.gov.pl/prawo/prawo-uni-europejskiej/prawo-ue-akty-prawne/ochrona-lotnictwa/3-decyzja-wykonawcza-komisji-c-2015-8005-z-dnia-16-listopada-2015-r-ustanawiajaca-szczegolowe-srodki-w-celu-wprowadzenia-w-zycie-wspolnych-podstawowych-norm-ochrony-lotnictwa-cywilnego-zawierajaca-informacje-o-ktorych-mowa-w-art-18-lit-a-rozporzadzenia-we> [accessed: 15 III 2026].

¹² Consolidated text, Journal of Laws of 2025, item 1431, as amended.

¹³ Consolidate text, Journal of Laws of 2023, item 1204.

¹⁴ Journal of Laws of 2013, item 1147.

Act of unlawful interference

In the international law, acts of terrorism against civil aviation are referred to as acts of unlawful interference (AUI)¹⁵. Article 2(20) of the Aviation Law sets them out in detail and defines them as unlawful and deliberate acts involving:

- a) use of violence against a person on board an aircraft during flight, where such an act may endanger the safety of that aircraft,
- b) destruction of an aircraft or causing damage to it that renders it unable to fly or may pose a threat to the safety of that aircraft,
- c) placement on board an aircraft of an object, device or substance that may endanger the health or lives of passengers or crew, or destroy the aircraft or cause damage to it that could prevent it from flying or pose a threat to the safety of the aircraft during flight,
- d) hijacking of an aircraft, with or without crew and passengers on board, including for the purpose of using the aircraft as a means of carrying out a terrorist attack from the air,
- e) destruction or damage of ground-based or on-board aviation equipment, the disruption of its operation, or the use of violence against a person operating such equipment, where this causes a significant disruption to air traffic or a threat to civil aviation safety,
- f) dissemination of false information that poses a threat to persons and property in the field of aviation,
- g) destruction or serious damage to airport facilities, the disruption of their operation, or the use of violence against a person operating such facilities, where this causes a significant disruption to air traffic or the operation of the airport, or poses a threat to the civil aviation security.

The seven AUI categories listed above form the basis for defining the threats against which the civil aviation is protected. Establishing an international framework for these acts and incorporating it into national legal systems facilitates effective countermeasures against such threats, as well as the criminalisation of behaviour by individuals who either carry out or plan AUI. Criminal liability for such acts is provided for under, among others, Art. 212 of the Aviation Law, as well as Art. 115, Art. 166, Art. 173 and Art. 174 of the Criminal Code¹⁶.

¹⁵ *Annex 17 to the Convention on International Civil Aviation...*, p. 15.

¹⁶ *Act of 6 June 1997 – Criminal Code* (consolidated text, Journal of Laws of 2025, item 383, as amended).

Security Management System

In today's world, management systems to boost an organisation's efficiency are becoming increasingly important. Without an integrated management system for the organisation, including its security, the ability to respond effectively and proactively to threats arising in the external environment is lost. To this end, it is necessary to adopt a structured approach based on assessing existing resources, identifying weaknesses in the security system, managing risk (or rather risks), promoting security culture, and ensuring a high standard of human resources involved in the system (training, appropriate staff selection). Equally important is the effective flow of internal information as well as cooperation with the authorities and external services.

In the structure and requirements of legislation developed over more than 80 years, one can discern the outline of a strong aviation protection system. However, the full implementation of these principles and providing them with robust legal framework is a key element in building a strong system within a broader context. The cornerstone of an effective security management system (SeMS)¹⁷, as with any modern management system, is the development of appropriate security policies approved and implemented by the management of the entity in which SeMS operates. These policies should set out objectives and priorities for security.

An important element of these policies is the establishment of requirements for procedures to respond to security threats and incidents, including guidelines for communication with both the relevant internal services and the public administration authorities responsible for crisis response. At the same time, it is essential to ensure that adequate human, infrastructural and technical resources are in place.

Another pillar of SeMS is risk management based on the identification of risks and the implementation of measures to control and minimise them. These activities are complemented by mechanisms for monitoring the effectiveness of security measures, quality control and the system's continuous improvement.

One of the more recent elements introduced into civil aviation security regulations is the concept of security culture, understood as building trust among employees, promoting appropriate attitudes and behaviours, and encouraging the reporting of incidents and irregularities.

¹⁷ *Aviation Security Manual* (Doc 8973 – Restricted)...

It was on these principles, among others, that the Polish implementing regulations were drawn up, namely the ones mentioned earlier:

- *National Civil Aviation Security Programme* governing policy areas and setting out detailed requirements relating to risk-based measures and purely protective measures,
- *National Training Programme* governing the scope of competence requirements for those involved in the security system,
- *National Quality Control Programme* governing the area of monitoring compliance with legal requirements, and consequently its quality.

From a practical point of view, it makes sense to identify the key components that, in my opinion, are essential for building an effective SeMS. One of them is to create the role of a security manager – someone responsible not only for implementing the system, but also for its operation and development. The person in this role should have a genuine, rather than merely formal, ability to influence change and make key decisions in the area of security. There are examples where a security manager is appointed within an organisation, yet the person in that role has no real authority within the organisational structure. In such situations, despite their commitment, sense of responsibility and willingness to act, security manager lacks the tools to effectively manage security. It is therefore essential, when establishing the role of security manager, to ensure that they are granted formal and practical powers to manage financial and human resources in the area of security. Only such a framework allows the security system to function effectively.

The organisation should implement consistent security policies, standards and procedures that are endorsed and actively supported by senior management. These documents should clearly define security objectives, identify key threats and take into account the context in which the organisation operates.

Nowadays, there is an increasing emphasis on a modern, risk-based approach to security. This is due to the rapidly changing and wide range of threats, which require regular identification, assessment and re-analysis. Risk management involves assessing the impact of risks on an organisation and consciously implementing appropriate safeguards to achieve an acceptable level of risk.

There is no single universal risk assessment tool – the choice of tool should be tailored to the nature of the organisation, while adhering to the principles of simplicity and usability. It should be also emphasised that it is impossible to eliminate risk entirely, and that the concept of zero

risk remains unrealistic. Therefore, informed acceptance of certain level is required.

In practice, when developing policies and procedures, there is often a problem of unreflective copying of solutions that are not always appropriate to the specific nature of a given entity. The problem is not the use of ready-made templates, but the inability to adapt them to one's own objectives, risks, and available resources.

Effective security management also requires innovation and creativity. The process or risk owner, being the person most familiar with the realities of the organisation, should initiate, or at least approve, the identified risks and the methods used to mitigate them. At the same time, it is worth emphasising that simple tools, when implemented properly and thoughtfully, can deliver very good results.

At the stage of developing procedures and designing SeMS, it is necessary to take into account the methods of responding to identified threats, incidents and breaches that may occur in day-to-day operations. Protective measures should serve a preventive and deterrent function. However, it is equally important to prepare personnel to respond appropriately in the event of an incident. Employees should know how to activate the response system and which services – including the Police or other public authorities – should be engaged.

To illustrate the importance of properly preparing infrastructure and personnel for safety purposes, the experience of aviation security screeners from several years ago may serve as an example. The case concerned the security screeners activation of a procedure for neutralising a potential threat involving an improvised explosive device (IED) found in a shipment during security check. Formally, the activities were carried out in accordance with the applicable procedures of the registered agent¹⁸. However, it turned out that carrying them out was significantly hindered due to the location of the X-ray machine in which the shipment was being scanned. The package became stuck inside the machine, which was positioned at a considerable height, making it impossible to use the bomb disposal robot and causing complications in conducting further pyrotechnic operations.

¹⁸ Regulated agent means an air carrier, agent, freight forwarder or any other entity who ensures security controls in respect of cargo or mail. See: Article 3(26) of the *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules...*

This highlighted the inadequacy of emergency procedures in relation to the actual infrastructural and technical conditions, as well as the need to ensure operational continuity. A schematic approach consisting of suspending operations, evacuating personnel and waiting for the appropriate services to arrive may lead to serious organisational, operational and financial consequences resulting from disruptions to service delivery.

Human resources

The key component of the security system, yet at the same time its most vulnerable and threat-susceptible element, is the human factor. For this reason, civil aviation security regulations place considerable emphasis on personnel vetting, particularly of individuals involved in implementing security measures such as screening, access control, surveillance and patrols, as well as employees with unescorted access to protected areas and facilities¹⁹.

Current regulations provide for two levels of **background checks** for aviation and airport personnel, candidates and other individuals who have access to among other things, the airport's restricted areas. The standard background check includes verification of identity, employment and education history covering at least the previous five years, as well as confirmation of a clean criminal record, including from countries where the person resided during that period. The enhanced background check is carried out with the involvement of the competent services, in particular the Border Guard, and consists of determining – including on the basis of operational or intelligence information – the existence of negative premises.

Background check procedures are carried out on a regular basis, at least every five years, although the validity of particular elements is verified more frequently – every three years for standard background check procedure and annually for enhanced background check. This process involves significant organisational resources, particularly in the case

¹⁹ See e.g. chapter 11 of the *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures...*; section IX of the *Act of 3 July 2002 – Aviation Law...*; *Regulation of the Minister of Infrastructure of 2 December 2020 on the National Civil Aviation Security Programme...*

of airports, where it encompasses staff from numerous entities operating within their area, numbering anywhere from several to over a dozen thousand people. It is worth emphasising that the obligation to conduct background checks also applies to individuals with unrestricted access to critical aviation ICT systems and data, as part of protection against cyber threats. Such personnel are treated analogously to persons who have unescorted access to specially protected areas of an airport.

Experience shows that even the most advanced procedural and technical solutions cannot replace properly background-checked and security-aware personnel responsible for the operation of key infrastructure components. Although the background check requires time and resources, it not only helps reduce risk but also enables the rapid identification of any potential adverse information concerning personnel.

This mechanism, developed within the international aviation sector, would require appropriate adaptation to national conditions and legal order to be effectively implemented in other CI sectors. Compared with vetting procedures conducted for access to classified information, background checks of personnel in the aviation industry are carried out within a relatively short timeframe, which is their significant advantage. However, in the context of high staff turnover, even this period is sometimes perceived as an organisational challenge.

The second key pillar of an effective security system is the **qualifications and competencies of personnel**. In the field of civil aviation security, there is a comprehensive training system tailored to the scope of responsibilities of particular groups of employees – from senior management and middle managers to individuals directly involved in the implementation of security measures. An important element is also the training aimed at raising security awareness among employees who do not perform direct security-related duties but operate in an environment requiring heightened vigilance.

Security culture²⁰ constitutes a set of standards, values, attitudes and principles relating to security, which are the foundation of the organisation's daily functioning and are reflected in the actions and behaviour of all its members. Security should not be viewed solely as the task of specialised services, but as a shared responsibility encompassing all

²⁰ *Security Culture*, International Civil Aviation Organization, <https://www.icao.int/security-culture> [accessed: 15 III 2026].

levels of the organisational structure – from operational staff to senior management.

In practice, security culture connects individual elements of the security system. Without developing it, even the best-designed procedures, systems and technical measures may prove ineffective. A lack of understanding of the purpose of security leads to it being viewed merely as a set of rules and prohibitions that are therefore not accepted or properly implemented. In this sense, the security culture is the driving force of the security system.

In recent years, insider threats²¹ have been receiving increasing attention within the civil aviation. This term refers to deliberate and intentional actions taken by individuals with authorised access to an organisation, which may lead to acts of sabotage, subversion or unlawful interference.

Countering internal threats can be based on a combination of several complementary mechanisms, such as background checks, security awareness training, fostering a security culture, information campaigns and the implementation of systems for reporting irregularities. When used in combination, these elements significantly strengthen the organisation's resilience to threats posed, for instance, by employees who are becoming radicalised, in the broadest sense of the word.

Quality control

SeMS is based on Plan–Do–Check–Act (PDCA) concept²², also known as the Deming cycle, which treats security as a continuous process. This approach involves planning security measures, implementing them, assessing their effectiveness, as well as introducing corrective and improvement measures. Once a risk analysis has been carried out, objectives have been set and appropriate protective measures have been implemented, it is necessary to check whether the system is functioning as intended.

²¹ Ibid.

²² See in more detail: *PDCA – Klucz do ciągłego doskonalenia i skutecznego zarządzania procesami* (Eng. PDCA – The key to continuous improvement and effective process management), Instytut Doskonalenia Produkcji, <https://www.doskonalenieprodukcji.pl/blog/pdca-klucz-do-ciaglego-doskonalenia-i-skutecznego-zarzadzania-procesami> [accessed: 15 III 2026].

In the literature, the terms ‘compliance monitoring’ and ‘quality control’ are used interchangeably, primarily due to terminological discrepancies in the translations of legal acts. In the national legal order, the term quality control²³ has become established in the context of civil aviation security, and this is the term that will be used in the remainder of this study.

Over the years, civil aviation has developed a comprehensive quality control system in the field of security. Although it is based on commonly used control and audit methods, its nature is similar to the approach familiar from the field of cybersecurity. Particular emphasis is placed on continuous monitoring, identifying vulnerabilities and responding swiftly to evolving threats, rather than merely on periodic assessments of compliance with established requirements.

Quality control in the civil aviation constitutes a multi-level system for verifying that Member States, airports, air carriers and other system participants meet at least the basic security requirements. Supervisory powers are exercised at various levels: at international level by the ICAO, at the European Union level by the European Commission, in Poland by the President of the Civil Aviation Authority, whereas at the level of individual aviation entities – by the internal auditors.

The multi-level nature of this system, as well as the possibility for auditors from different Member States to participate in joint audits carried out together with the European Commission inspectors, are conducive to exchange the knowledge and good practices. In addition, European Union regulations provide for mechanisms enabling the European Commission’s inspectors to share the results of the audits carried.

Compared to other Member States, Poland has developed an extensive system of certified internal auditors, while at the same time attempting to transfer control mechanisms and practices to the level of aviation operators. This solution strengthens the coherence of the security system and increases its resilience through systematic inspections and the implementation of corrective actions.

The basic control methods in the field of civil aviation security include audit, inspection, security testing and survey.

²³ *Regulation of the Minister of Infrastructure of 5 November 2020 on the National Quality Control Programme in the field of civil aviation security.*

An audit is an announced activity and covers all the security measures applied in a given entity.

The inspection consists in the verification of selected elements of the security system, especially the so-called directly linked security measures, the correct application of which can only be confirmed by their joint assessment.

Security testing constitute unannounced and covert verification activities, such as attempts to bring in prohibited articles by security, gain unauthorised access to restricted areas or unauthorised board an aircraft. This can be compared to the pentests known from cybersecurity.

The above forms are complemented by survey, which consists in the assessment of a specific security measure and is carried out by the competent aviation authority as part of the oversight exercise.

In practice, unannounced control methods, such as inspections and security testing, are of particular value in the evaluation of the civil aviation security system. Thanks to them, information about the functioning of the security system in everyday conditions are obtained, through the use of CCTV recordings, interviews with employees performing their activities without notifying them.

Although important from the point of view of the overall assessment of operations and system compliance, audits are more effective in the analysis of broad areas of the organisation's functioning. At the same time, both civil aviation security audits and inspections often require significant organisational effort and time, involving multi-person teams for many working days to get a complete picture of the functioning of the security system.

It should be emphasised that in the event of non-compliance or deviations from the applicable regulations and procedures, it is necessary to implement adequate remedial measures and launch a corrective action programme. The aim of these activities is to remove identified vulnerabilities of the security system as quickly as possible.

The implementation of a corrective programme requires full support from the person responsible for security, understanding of the entire process, and taking responsibility for effectively removing identified deficiencies. At the same time, it is necessary to take into account the principles of the security culture in order to clearly communicate the objectives of corrective actions and to obtain real support from employees and cooperating organisational units.

Finally, attention should be paid to one more element included in the *National Quality Control Programme*²⁴, which can be considered innovative, which does not appear directly in the international regulations on the civil aviation security. We are talking about security exercises, which significantly relate to crisis management issues and the implementation of business continuity plans. According to the mentioned programme, each airport is obliged to conduct annual exercises, which most often consist of simulating an attempt to carry out AUI and activating crisis management teams as well as checking the response procedures in force in a given airport. These exercises are carried out, depending on the agreed scope, in cooperation with air carriers, other entities conducting aviation activities, the airport security service, as well as state services operating at the airport, especially the Border Guard, the Police and the Internal Security Agency.

Security of civil aviation and security of critical infrastructure

The analysis of the *National Critical Infrastructure Protection Program 2023*²⁵ and its annex entitled *Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations*²⁶ indicates that many of the solutions proposed in it are consistent with the mechanisms used in the civil aviation security system. This is positive, as the civil aviation security system is one of the most developed and formalised infrastructure security systems, and it is based on a multi-level approach to risk management and the continuous improvement of security procedures.

At the same time, some recommendations contained in the aforementioned national CI Protection Program are merely good practices in nature, which may limit the extent of their implementation by CI operators. It seems justified to introduce selected solutions through higher-level normative acts, which would allow for their uniform and consistent application. This applies in particular to issues related to human resource management in safety and security systems, such as the development

²⁴ Ibid.

²⁵ *Narodowy Program Ochrony Infrastruktury Krytycznej* (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, <https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program> [accessed: 15 III 2026].

²⁶ Ibid.

of personnel competencies or the strengthening of employee verification mechanisms, especially for those having access to critical elements of infrastructure. Experience of the civil aviation sector indicates that appropriate selection, training and continuous improvement of personnel competencies constitute one of the pillars of an effective security system.

Equally important is the development of security culture, which involves building threat awareness and a sense of responsibility for safety and security among all system participants. This means the need to carry out systematic training, informational and organisational activities aimed at strengthening attitudes conducive to identifying and reporting potential threats.

It should also be emphasised that although conducting security audits is recommended in policy documents concerning the protection of CI, in practice these activities often focus on assessing formal compliance and analysing documentation. Meanwhile, the effectiveness of the security system depends on its functioning in operational conditions. For this reason, activities such as exercises and security testing using AUI simulation, become particularly important, as they make it possible to verify an organisation's actual ability to respond to crisis situations.

Summary

Due to their location in the transport sector, civil airports are one of the key areas of CI. Civil aviation experience of operating in a highly regulated environment with a particularly developed SeMS can be used to strengthen the resistance of other elements of CI.

Most of the regulations currently in force in security area focus on activities carried out in operational, restricted zones and in their critical parts. This applies not only to civil aviation and airports, but also to other crowded public spaces. In the face of modern threats, the protection of infrastructure that is used by large population centres and to which access is almost unrestricted, such as stations, metro stations, venues of mass events, etc. should be a priority and needs continuous improvement. In this context, it is worth recalling the attack on Brussels Airport in Zaventem

in 2016²⁷, which – like many other terrorist attacks – was carried out in the public area of the airport's departure hall.

It seems reasonable to conduct frequent specialist training for security services, including, among others, intervention techniques or the use of weapons. At the same time, it is advisable to expand the course content to include, for example, behavioural profiling, which teaches the identification of potentially dangerous behaviour and taking adequate actions at the earliest possible stage of threat development, addressed to a wide group of employees, such as conductors and transport drivers.

The increasingly frequent presence of armed guards and officers from various services in public spaces, including streets and transport hubs, is an important element of preventive measures. In this context, it is worth considering the greater use of service dogs trained both for patrol operations and for detecting explosives. This involves organisational, formal and legal challenges, but the operational and preventive potential of such a solution is large, especially in the context of threats related to unattended luggage. The presence of handlers with trained dogs on patrols can not only contribute to the rapid identification of potential threats but also deter potential perpetrators of acts of terrorism or sabotage. Consequently, this can reduce the risk of incident escalation and shorten the response time of the services, including the time required to evacuate the area at risk.

Another aspect is the assessment of effectiveness of the implemented protection measures in relation to the most frequently identified terrorist threat scenarios. It is essential to take actions to identify potential vulnerabilities and test existing solutions. It is also recommended to repeat such checks periodically.

In my opinion, the following can significantly contribute to increasing the level of CI protection:

- actively undertaking actions aimed at exchanging experiences,
- developing cooperation between entities operating in different sectors,
- building awareness of the need for changes and the evolution of security systems,
- creating and using effective tools for the supervision and review of the security system, based on solid legal foundations.

²⁷ M. Zieliński, *Zamachy terrorystyczne w Brukseli* (Eng. Terrorist attacks in Brussels), Polska Zbrojna, 22 III 2016, <https://polska-zbrojna.pl/Mobile/ArticleShow/18869> [accessed: 28 III 2026].

These actions would promote the transfer of good practices present in civil aviation to other areas affecting the proper functioning of the state and society, and they are also consistent with the concept of continuous improvement of safety and security systems, as well as increasing the resilience of CI to contemporary threats.

Karol Dymek

Specialist with over twenty years' experience in the security. For over 18 years, he has been involved in civil aviation security, also as a national auditor in the Civil Aviation Authority. He currently works as an internal auditor at one of the largest airports in Poland.

Contact: dymek.karol@gmail.com

Civil aviation security in practice – security systems, control and operational resilience

Bohdan Paszukow

Securitas Services

Civil aviation security is one of the cornerstones of the global transport system. Consistent procedures, modern tools and well-designed security systems contribute to its improvement. As part of the AVSEC (aviation security) programmes, standards and practices are being developed to prevent acts of unlawful interference, strengthen the resilience of infrastructure and ensure a high level of risk control. Particular states and international organisations adopt different models for organising their security systems – ranging from centrally managed to more decentralised models based on operator responsibility. This diversity of approaches is particularly evident when comparing the solutions used in the European Union and the United States.

Assessment of civil aviation security quality in the United States and the European Union

When conducting a quality assessment of the aviation security, particularly for a global corporation engaged in the protection of people and property

in various domains, it is essential to understand how particular regions structure their aviation security frameworks. The United States and the European Union both pursue the same overarching goals which are preventing terrorist incidents and ensuring the safety of passengers, staff, and infrastructure. However, their implementation differs in terms of how the security system is managed, the approach to drafting and enforcing regulations, and the mechanisms of supervising operators. The European Union is based on detailed, uniform technical standards and procedures. The United States prefer a more centralised model, with a strong role for the Transportation Security Administration (TSA) and a greater emphasis on outcomes- and effectiveness-based solutions rather than rigid procedural requirements. The EU therefore adopts a normative approach, while the US takes an efficiency-based approach, which involves different ways of organising and monitoring the AVSEC systems.

The TSA, which assumed direct responsibility for aviation security in the US, was established as part of the Department of Homeland Security following the events of 11 September 2001. It sets uniform screening requirements, issues federal security directives, and manages checkpoint operations at most airports. This centralised approach allows rapid adaptation to emerging threats through directive changes. Oversight is conducted through federal inspections, covert testing, and incident driven updates to procedures. The American regulatory system focuses on and includes detailed requirements for passenger and baggage screening, staff vetting, and access control. It emphasises uniformity and speed of response, with federal agencies directly accountable for compliance.

The EU model is built on harmonisation across multiple sovereign states, which must implement common AVSEC standards while retaining their own administrative structures and national responsibilities.

Regulation (EC) No 300/2008¹ provides the baseline framework for aviation security across the EU, setting common rules for screening, access control, and cargo security. These rules are supplemented by detailed implementing acts that specify performance standards. Enforcement is carried out by national authorities within each Member State, but the European Commission plays a central role in oversight. It conducts

¹ *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002* (Official Journal of the EU L 97/72 of 9 IV 2008).

inspections, requires annual compliance reporting, and ensures that Member States apply the common rulebook consistently. A distinctive feature of the EU system is the ECAC Common Evaluation Process (CEP), which provides standardised laboratory testing of security equipment against agreed performance criteria. This ensures comparability of equipment approvals across Member States and avoids fragmented national assessments. Therefore, the EU model allows Member States to meet the baseline requirements while maintaining crossborder consistency through harmonised standards and EU Commission oversight.

A key strength of the EU's aviation security regulatory regime is the standardisation of security measures. EU legislation allows resources and efforts to be focused on the areas of most risk, while providing a framework for close cooperation between Member States, regulatory authorities, aviation industry and other stakeholders involved in AVSEC. Common platforms and coordination mechanisms such as SAGAS (Security Advisory Group for Aviation Security), which operates within the European Commission, or industry organisations representing the private sector, such as ASSA-i (Aviation Security Services Association – International), play a key role in this process.

In addition, the EU regulatory system supports quality control and compliance monitoring mechanisms to ensure consistent operational and regulatory oversight.

Although the EU and US approaches differ in terms of governance structure, regulatory style and supervisory mechanisms, in practice they are converging through transatlantic cooperation. The US Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA) maintain bilateral agreements to avoid duplicative certifications and align technical procedures. This cooperation extends into security, where mutual recognition of certain controls and certifications helps streamline compliance for global operators.

Assessment of physical security measures in the EU civil aviation

Compliance assessments serve as the backbone of aviation security. They provide a structured way to verify that airports, airlines, and associated

service providers adhere to international and national regulations, as well as other national local civil aviation authorities.

Assessments methods, their scope and criteria evolve in response to emerging threats, technological advancements, and lessons learned from past incidents and audits. This evolution concerns both the methods used to identify risks and the tools employed to analyse them. This process also takes place within the framework of the AVSEC international cooperation network, which encompasses institutions such as International Civil Aviation Organization (ICAO), the European Commission, TSA, EASA, as well as industry organisations and associations. It is this network that facilitates the exchange of information, the updating of standards and the adaptation of risk assessment methods to a globally changing risk environment.

One of the most critical components of compliance assessment is the monitoring of access control systems. Airports are complex environments with multiple restricted zones. Processes of civil aviation security quality control verify that only authorised personnel have access to sensitive areas, identification systems, biometric checks, and surveillance technologies are functioning correctly and that procedures for issuing and managing access credentials are effective. This prevents unauthorised entry, which could compromise aircraft, passengers, or cargo.

Equally important is the evaluation of passenger and baggage screening procedures. Compliance assessments ensure that screening technologies such as X-ray machines, explosive detection systems, and body scanners are properly calibrated and maintained. Quality control also involves observing the performance of security personnel, checking whether they follow protocols consistently, and identifying gaps in training or vigilance.

Cargo and supply chain security is another significant area of assessment. It covers the procedures for screening, storing, and transporting cargo. It is checked whether the suppliers and contractors adhere to approved security practices and that there is a clear chain of custody for all goods entering the aircraft environment.

Security is only as strong as the people implementing it, and therefore, quality control processes emphasise continuous education, drills, and evaluations. Personnel must be prepared not only to respond effectively to suspicious behaviour, emergencies, or attempted breaches. Compliance

assessments often include simulated scenarios to test readiness and resilience.

Risk management and incident reporting systems play a crucial role. Compliance assessments ensure the effective operation of mechanisms for identifying vulnerabilities function effectively, promptly, reporting incidents, and implementing corrective actions. Quality control processes track how quickly and effectively organisations respond to identified risks, whether through procedural changes, technology upgrades, or enhanced training. This creates a feedback loop where lessons learned strengthen overall physical security in aviation.

Technology integration is another key component. As part of the compliance assessment, checks are carried out to ensure that surveillance systems, biometric identification, and automated access controls are installed and are actively monitored and maintained. Quality control ensures that data from these systems is used effectively to detect anomalies and prevent breaches.

Observations are one of the most immediate and practical tools in the compliance assessment process. By conducting onsite inspections, auditors and inspectors can directly observe how security procedures are implemented in real time. For example, they may watch how access control points are managed, whether identification checks are consistently applied, or how baggage screening is conducted. Observations might reveal eventual discrepancies between procedures and practice.

Document validation complements observations by ensuring that the organisation's policies, manuals, and records align with regulatory requirements. This involves reviewing training records to confirm that personnel have received the required instruction, checking incident logs to verify that breaches are reported and investigated, as well as validating certifications to ensure equipment meets standards. Without accurate and up-to-date documentation, even the best operational practices can drift into noncompliance. Moreover, document reviews provide evidence that the organisation is not only compliant today but has systems in place to remain compliant over time.

Interviews with personnel help gauge their level of understanding of risk, their attitudes to work, and readiness for action. Speaking with frontline staff such as security officers might reveal whether training has been effective and whether employees feel confident in applying protocols. Interviews with management can uncover how

seriously leadership prioritises security and whether there is a culture of accountability. Importantly, interviews often highlight areas that documents and observations cannot capture, for instance, whether staff feel comfortable to execute their activities especially during peak hours or whether the procedures for reporting suspicious activity are clear and the communication channels are trusted.

Testing protocols can be divided into overt and covert methods. Overt testing includes scheduled drills, such as evacuation exercises or controlled access challenges, where staff are aware they are being evaluated. These tests measure compliance under observed conditions and help organisations refine their procedures. Covert testing, often referred to as red teaming, involves simulating realworld threats without prior notice, for example, attempting unauthorised access or introducing prohibited items through checkpoints. Covert tests are invaluable because they reveal how systems perform under genuine stress, without the artificiality of a staged exercise. Together, overt and covert testing ensure that physical security measures are not only compliant on paper but effective against actual threats.

Ultimately, the assessment of compliance and security quality control in civil aviation serve to establish a layered security system. Regulatory adherence, access control, screening, cargo security, personnel training, risk management, and technology integration together form a comprehensive shield against threats. This approach ensures that physical security in civil aviation remains at an acceptable level. It protects passengers, staff, and assets maintaining public confidence in air travel at the same time.

The use of artificial intelligence to ensure civil aviation security

In order to enhance the efficiency, accuracy and adaptability of aviation security systems to changing threats and operational conditions, artificial intelligence (AI) is increasingly being integrated into them.

Passenger and baggage screening technologies now use machine learning algorithms to detect prohibited items more effectively than traditional X-ray systems. The AI-driven tools can analyse vast amounts of imaging data, recognise patterns and characteristics of risks, and flag anomalies with greater precision, reducing the likelihood of human error. Similarly, biometric identification systems at airports, such as facial

recognition and fingerprint scanning, rely on AI to match identities quickly and securely, streamlining passenger flow while maintaining strict access control.

AI is used in surveillance and monitoring systems. Modern CCTV (closed circuit television) networks are enhanced with AI-powered analytics that can detect suspicious behaviour, unattended baggage, or unauthorised access in real time. This proactive capability allows security personnel to respond faster and more effectively to potential threats. In cargo and supply chain security, AI tools are used to track shipments, verify authenticity, and identify irregularities during their transport.

In practice, AI is not replacing traditional security measures but augmenting them. Human oversight remains essential, as AI systems must be continuously tested, validated, and monitored to ensure they perform reliably under diverse conditions. The combination of human expertise and AI-driven tools creates a layered defence system that strengthens aviation security without compromising safety standards.

Components of a corporate aviation security programme

Aviation has a global dimension, and therefore corporate AVSEC programmes must align with international standards, regional directives, and national civil aviation authority requirements. This regulated environment shapes every aspect of the programme, from policy development, operational execution to quality control carried out by external authorities. Organisations also establish internal quality control mechanisms that include document validation, operational observations, structured interviews with staff, and both overt and covert testing protocols. By embedding these processes into daily operations, organisations can identify gaps early, correct deficiencies, and demonstrate to regulators that they are meeting or exceeding required standards. This proactive compliance culture is a hallmark of aviation security and is less common in other private security sectors, where oversight may be less stringent.

Aviation security threats evolve, and organisations within the security programme must invest in training, awareness, and skill development at all levels. Frontline staff need regular refresher courses on screening procedures, while management must be trained in crisis response and regulatory updates. Capacity building also extends to technological

adaptation, ensuring that staff can operate advanced screening equipment and respond to emerging cyber threats. This emphasis on continuous learning ensures that the organisation remains resilient in the face of new challenges, and at the same time it reflects the dynamic nature of corporate aviation security compared to more static private security environments. Most private security programmes are limited to the local or national context and do not require such a high level of international coordination.

Equally important is the role of global network sharing and collaboration between organisations operating in the aviation sector. Corporate AVSEC programmes benefit from participating in global networks that share intelligence, best practices, and lessons learned. Whether through industry associations, regulatory working groups, or bilateral partnerships, this exchange of information allows organisations to anticipate emerging threats, adopt proven strategies, and align their practices with global standards.

Security and cybersecurity audits for critical infrastructure facilities – potential errors

On 3 April 2026, the amendment to the Act on the National cybersecurity system² came into force. Its aim was to bring national regulations into line with the EU's NIS2 Directive³ by expanding obligations for critical infrastructure (CI) operators. The new law will affect significant number of entities, including operators across energy, transport, healthcare, and digital services.

One of these obligations is to carry out external information system security audits. The effectiveness of audits in strengthening the resilience of CI depends on the organisation's approach to such an audit.

Above all, audits should not be viewed merely as a box-ticking exercise. The NIS2 Directive emphasises continuous risk management, not just periodic checks. Organisations should embed audit findings into their

² *Act on the National cybersecurity system* (Journal of Laws of 2026, item 20, as amended).

³ *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)* – (Official Journal of the EU L 333/80 of 27 XII 2022).

cybersecurity strategy, ensuring improvements are sustained rather than temporary.

Another critical error is ignoring supply chain and third-party risks. The NIS2 Directive requires operators to assess risks from vendors and service providers. Many CI systems rely on external contractors responsible for software, hardware, or system maintenance. If audits fail to evaluate these dependencies, attackers may exploit weak links outside the organisation's direct control.

It is very important that obligations relating to incident reporting and response are met. The NIS2 Directive requires timely reporting of cybersecurity incidents to national authorities. If audits do not test incident response capabilities such as escalation paths, communication protocols, and coordination with regulators, organisations may fail during a real crisis. Audits should include simulations to verify readiness. Finally, organisations should align audits with resilience planning.

The Critical Entities Resilience (CER) Directive⁴ complements the NIS2 Directive by focusing on physical and operational resilience of critical entities. If audits only cover technical cybersecurity without considering broader resilience measures like system redundancy, disaster recovery, and crosssector coordination – CI may remain exposed to systemic risks.

In summary, Poland's mandatory external audits of CI security are a powerful tool, but only if approached strategically. Taking a rigorous approach to regulatory compliance, addressing supply chain risks, ensuring governance accountability within the management system, testing incident response, and integrating resilience planning are essential steps.

Building resilience to threats in civil aviation in the EU – recommendations

Building civil aviation resilience to threats within EU countries requires a comprehensive and layered approach that balances regulatory oversight, technological innovation, and human preparedness. At the core of the system, strict adherence to international and European aviation

⁴ 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).

security regulations provides the foundation. However, resilience goes beyond compliance, as it requires proactive risk management and the ability to adapt quickly to evolving threats.

One of the most important elements is the integration of advanced technology. Surveillance systems enhanced with AI, biometric identification for passenger processing, and automated cargo screening tools all contribute to detecting and mitigating risks more effectively. Continuous training and competency assessments of personnel remain indispensable.

Security threats are often transnational, and system resilience depends on timely intelligence exchange between national authorities, airlines, and airports. Furthermore, digital systems underpin nearly every aspect of aviation operation, which is why cybersecurity is so important, including the protecting networks from intrusion and ensuring continuity of operations in the face of cyberattacks.

Resilience to threats is built through a culture of continuous improvement. Incident reporting, auditing, and feedback loops allow vulnerabilities to be identified and corrected swiftly. What works is a layered defence where regulation, technology, human expertise, and cooperation reinforce one another. Neglecting any of these pillars would weaken the system, but when combined, they create a robust shield that ensures aviation in EU countries remains secure, adaptable, and trusted by the public.

One of the biggest challenges in protecting airports against terrorism and sabotage is detecting insiders. They may act out of ideology, coercion, or financial motivation, and their activities can be difficult to detect. Certain standards are currently in place in this regard, but it is essential to further strengthen them in order to build resilience. In this regard, the minimum standards set out in Regulation (EC) No 300/2008 currently apply. These include, among other things, strict background checks of employees, continuous monitoring of staff with access to restricted areas, and mandatory training in security awareness. Airports are required to implement access control systems, conduct random screening of staff, and enforce reporting mechanisms for suspicious behaviour. To build resilience, it is essential to reinforce these guidelines.

Experts argue that more emphasis should be placed on security culture encouraging employees to remain vigilant, report concerns, and understand the risks posed by colleagues who may misuse their privileges.

Organisations should create environment in which employees feel responsible for safety and are fully aware of risks.

Using solutions from the EU civil aviation sector to build resilience to hybrid threats in maritime and rail transport

Hybrid threats, those that blend physical, cyber, informational, and even legal-instrumental tactics, pose a growing challenge to transport CI. Maritime ports and rail networks, much like airports, are highly interconnected systems whose operation can be disrupted through sabotage, including cyberattacks, disinformation campaigns, or insider manipulation. While each sector has its own operational realities, the EU civil aviation acquis offers a mature framework of resilience practices that can be adapted to strengthen maritime and rail security.

One of the most valuable lessons from aviation is the risk-based, layered approach to security. Aviation combines multiple layers of defence from passenger screening and cargo checks to access control and surveillance. This principle can be applied to maritime and rail transport by tailoring controls to critical nodes such as port terminals, signalling centres, and freight depots. Operators should adopt flexible, intelligence-led measures that reflect the open nature of ports and rail networks.

Another transferable strength is access control and credentialing discipline. Aviation requires strict background checks, continuous monitoring of restricted areas, and random screening of staff with access to these areas. In maritime and rail, similar measures can safeguard control rooms, maintenance yards, and cargo handling facilities. Importantly, insider risk management must go beyond one-time vetting, incorporating behavioural monitoring and periodic re-assessment to detect changes in staff circumstances or vulnerabilities.

Equally critical is the security culture embedded in aviation. Continuous training, scenario-based exercises, and mandatory reporting of suspicious behaviour help to create a workforce that is alert and prepared for threats. Maritime and rail operators can benefit from adopting this culture, ensuring that employees understand hybrid threats and feel empowered to act when anomalies arise. Joint drills across sectors involving operators, regulators, and emergency services can simulate hybrid scenarios, strengthening the ability to response.

It is worth noting, however, that not all practices that work effectively in aviation will necessarily work in the maritime and rail transport sectors. This applies, for example, to airport checkpoints. Copy pasting these solutions into open maritime and rail environments would create bottlenecks without addressing the unique vulnerabilities of these sectors. Similarly, overreliance on technology without governance and human oversight can leave systems exposed to adversarial manipulation. The siloed responsibilities must be replaced with joint command structures and interoperable protocols across agencies.

By combining aviation's proven frameworks with sector-specific adaptations, the EU can build a robust shield against hybrid campaigns that target its critical transport lifelines.

Bohdan Paszukow

Specialist in civil aviation, author of scientific publications on airport security and control in civil aviation.

Contact: bohdan.paszukow@gmail.com

For a safer and more secure Europe in a better world. European High Risk Security Network | cycle 2024–2025

Pedro Nogueira

Guarda Nacional Republicana

In the years 2024–2025, the European High Risk Security Network (EU-HRSN) – an EU network of uniformed special forces for high-risk operations¹ – operated under the leadership of the Portuguese Guarda Nacional Republicana (GNR). During this presidency, the Network’s focus gradually shifted from activities centred on the protection of public spaces and immediate response towards a broader resilience-building approach. The focus was on capacity-building as well as current and future threats. The Network provides both practitioners and researchers with regular opportunities to meet representatives from organisations involved in combating threats, thereby enabling them to learn about current initiatives and forms of cooperation aimed at protecting public spaces during a period of geopolitical instability, armed conflict as well as growing security and safety challenges at international, regional and local levels.

¹ More on the EU-HRSN, see: G. Salazar, *Spanish Presidency of the EU High Risk Security Network held by the Guardia Civil through the Grupo de Acción Rápida*, “Terrorism – Studies, Analyses, Prevention” 2023, no. 4, pp. 525–535. <https://doi.org/10.4467/27204383TER.23.038.18340>.

The origins and aims of the EU-HRSN

In 2017, in response to an increase in terrorist attacks, the European Parliament and the Council of the European Union adopted Directive (EU) 2017/541 on combating terrorism². This was a key milestone in the EU's counterterrorism architecture, reinforcing the legal and operational basis for preventing and responding to terrorist threats. Building upon this foundation, the *EU Action Plan – Union for Security: Protection of Public Spaces*³ was introduced to enhance the security and resilience of public accessible areas. This initiative provided the institutional and strategic groundwork for the establishment of the EU-HRSN network, which took place on 1 November 2018. It was established to strengthen cooperation, exchange knowledge and coordinate activities between Member States, in the field of public space protection, while taking into account traditional protective measures limitations in the context of evolving terrorist and criminal threats. This objective reflects an increased awareness of the so-called soft targets vulnerabilities, which stem from their public and shared nature, along with the high concentration of people who could be exposed to potential harm. In this context, the Network aims to preserve the openness, accessibility and inclusive nature of public spaces across the EU while avoiding the implementation of overly restrictive or highly visible armed security measures that could undermine their social function. Accordingly, the EU-HRSN promotes the adoption of proportionate and effective protective strategies aimed at reducing vulnerabilities and mitigating the impact of potential attacks.

The EU-HRSN operates within the Law Enforcement Networks ecosystem under the Counter-Terrorism Unit (D2) of the European Commission's Directorate-General for Migration and Home Affairs (DG HOME). Since its establishment, the EU-HRSN has been chaired by: the Dutch *Royal Netherlands Marechaussee* (2018–2021), the Spanish *Guardia Civil* (2021–2023) and, as mentioned, the Portuguese *Guarda Nacional Republicana* (2024–2025).

² 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 88/6 of 31 III 2017).

³ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan to support the protection of public spaces, COM(2017) 612 final.

The structure of the EU-HRSN

The Network's continuity depends not only on rotating leadership, but also on institutional memory, in other words, how the experience gained in crisis situations is put to use. For that reason, the structure of the EU-HRSN rests on permanent programme office support, acting as a secretariat, in close cooperation with the previous and future chairmanship (in the case of Portugal, this is, respectively, Spanish – Guardia Civil, and French – Gendarmerie Nationale), thereby ensuring strategic alignment over a longer time horizon (6 years' window).

At the tactical and operational level, the Network is organised into three pillars: Working Groups, Cooperation and Coordination, as well as Projects and Initiatives. The Working Groups are the heart of the Network and develop key topics that have been formally approved by the European Commission (EC): Risk assessment, Tactical UAS & C-UAS⁴, Tactical Rescue Response, Human Factor, and Protective Security Advise & Coordination for Major Events (Figure 1). The Cooperation and Coordination pillar establishes a permanent link with ongoing stakeholders, while the Projects and Initiatives pillar provides ad-hoc support for specific events, such as training courses, conferences and webinars⁵.



Figure 1. Network structure and Working Groups.

Source: EU-HRSN's own materials.

⁴ UAS – unmanned aerial system; C-UAS – counter-unmanned aerial system (editor's note).

⁵ See: <https://hrsn.eu/sample-page/>.

Responsibility for network management lies with the Steering Group, as approved by a majority at the first General Conference of the current cycle (Image 1). The Steering Group comprises the previous chair, the vice-chair (who will become the next chair), the Working Group Coordinators, an observer from the European Commission and invited experts.



Image 1. EU-HRSN General Conference, 22 February 2024.

Source: EU-HRSN's own materials.

Conceptual approach and the achievements of the Portuguese Presidency

As outlined in the Public Spaces Protection Action Plan, the EU-HRSN brings together representatives from 41 specialised law enforcement units across 30 countries⁶, including non-EU partners such as the US Federal Bureau of Investigation (FBI) and the New York Police Department (NYPD), as well as intervention forces from Kenya, Ghana and Senegal. The EU-HRSN also benefits from the participation of the DG HOME and the Protective Security Advisors (PSA), namely the programme run by the EU group of advisers on building resilience to threats, which facilitates contact

⁶ See: <https://hrsn.eu>.

with experts in security and risk assessment. The EU-HRSN cooperates closely with the Joint Research Centre (JRC) and the PRESERVE, ESIWA+ and Public Spaces+ projects, alongside other Law Enforcement Networks (AIRPOL, AQUAPOL, ATLAS, EIFS, ENLETS, ESG and RAILPOL) under the coordination of the European Commission's DG HOME D2.

The Network has adopted a case-study approach (Figure 2), examining in depth the terror incidents that have occurred in Europe over the past two decades and other events (Figure 3). This approach is based on a permanent learning process to help us better understand how to avoid and prevent similar incidents in a near future. The EU-HRSN supports the EU commissions and Member States in setting priorities, strategies and mechanisms to deter, prevent, dissuade, protect and mitigate those threats, while studying current and future challenges, identifying vulnerabilities and working on capacity building development needs. The case-study approach is based on the *Pathway to violence* theory, which is rooted in the behavioural research conducted by Frederick Calhoun and Steve Weston in 2016⁷. This theory provides a general model that explains how and why incidents of targeted violence occur. It also defines a framework for identifying, preventing and managing threats, which may enable us to break the chain of violence and prevent future incidents.



Figure 2. Case-study approach.

Source: EU-HRSN's own materials.

⁷ *Pathway to Violence*, CISA, 24 II 2023, <https://www.cisa.gov/resources-tools/resources/pathway-violence> [accessed: 17 VI 2026].



Figure 3. Some of the selected events from 2025 analysed by the EU-HRSN.

Source: EU-HRSN's own materials.

The Portuguese chairmanship, represented by the GNR Intervention Unit (Unidade de Intervenção)⁸, integrates highly specialised forces in the areas of Crowd and Riot Control, SWAT and Special Operations, Explosives and Underground Security, and K9 (units with service dogs), as well as pre-deployment training capabilities. The unit's wide scope easily links it to several international specialised networks within the European framework, such as ATLAS, ENLETS, EU PSA, EOD, RAILPOL, FRONTEX and CEPOL, among others. This has enabled the EU-HRSN to easily collaborate with other stakeholders in the protection of public spaces, working in a multilayer integrated perspective.

Throughout the Portuguese presidency, the Network supported the production and harmonisation of tactics, techniques and procedures, the drafting of directives as well as technical and tactical content, the collection and dissemination of identified lessons, as well as the consolidation and development of capabilities in the field of public space protection. Thanks to a strong momentum across the five established Working Groups and ongoing cooperation with other networks, projects and European forums dedicated to this issue, valuable contributions were

⁸ GNR - Unidade de Intervenção, Facebook profile, <https://www.facebook.com/gnr.ui.intervencao> [accessed: 17 VI 2026].

made to reinforce the aforementioned critical security areas, fully in line with objectives previously approved by the EC.

Of the 104 activities organised or attended by the Network⁹ (involving 1097 EU-HRSN experts), particular emphasis should be given to the creation and delivery of several training and exercise initiatives:

- *Advanced Operators Counter-Unmanned Aircraft Systems Training Course*, delivered in cooperation with the JRC C-UAS laboratory in Belgium, strengthening technical and tactical CUAS capabilities;
- *Search, Detect and React Training Course*, implemented in cooperation with the Lithuanian Police (1st edition) and the Greek Police (2nd edition), enhancing the detection of suspicious behaviour in public spaces;
- *Tactical Rescue Response* training and exercises, held in Ireland (1st edition) and Spain (2nd edition), improving operational interoperability of first responders in active attacker scenarios, involving specialists from multiple countries with police, emergency services and armed forces background;
- *Workshop and table top exercise on Protective Security advice and coordination*, organised in Portugal, aiming to better coordinate the response to a crisis situations by different entities and organisations;
- Several online web conferences were held, involving a wide set of partners working on public spaces protection. These conferences aimed to share knowledge and identify lessons on key topics such as arms trafficking, 3D printing, case studies on active shooters and insider threats, threat assessment and risk management, lessons learned from security operations during the 33rd Olympic Games in Paris and His Holiness Pope Francis' visit to the Sanctuary of Fátima, vehicle barrier systems, detection of suspicious behaviour, and JRC technological support tools.

One of the Network most significant achievements during the Portuguese presidency is considered to be the operationalisation of a Pool & Sharing (P&S) mechanism. This is an innovative high-impact solution that enables the agile and reliable mobilisation of specialised

⁹ Ibid.

assets and experts to reinforce high-risk international events security. This is achieved through the deployment of non-executive technical support teams, thereby strengthening Member States capacity to prepare and conduct complex security events, in a context of limited resources and demanding operational requirements.

One example of the use of this mechanism was the deployment for *Operation David*, providing security for the visit of the Ukrainian president, Volodymyr Zelensky, to Ireland. Since the implementation, the P&S mechanism has been activated 10 times, resulting in 58 operational deployment days (a total of 470 hours) and the direct involvement of 47 police experts from member countries. This clearly reflects the credibility achieved by the EU-HRSN and emphasises its capacity to turn international cooperation into an effective operational response.

Challenges

Looking ahead, challenges for the EU-HRSN in the area of security require a shift from a narrow focus on protection, prevention and immediate response towards a broader crosscutting approach. This aims to maintain a functional operating environment in times of crises, strengthening resilience and preparedness levels, based in a security and safety community culture development and a clear investment on security by design principles. This approach should involve security forces first responders, emergency services as well as specialised units, people and politicians in a collective organised effort, as a permanent learning and capacity building process.

In response to this challenge, good practices and innovative solutions must be made available to public spaces partners and stakeholders, helping to bridge the gap between security research and operational needs. The focus should be on new and emerging security threats, as well as ensuring the necessary operational synergies between civilian, police and military components.

The P&S mechanisms referred to as *Rapid Counter-drone Emergency Response Teams* in the *Action Plan on Drone and Counter-Drone Security*¹⁰,

¹⁰ *Action Plan on Drone and Counter-Drone Security*, European Commission, <https://digital-strategy.ec.europa.eu/en/policies/drone-security> [accessed: 17 VI 2026].

must be able to provide cross-border coverage and deploy specialised mobile units in the context of high-risk and high-profile events, while maintaining interoperability. The mechanism is activated at the request of a Member State authority, as a mutual European assistance approach.

Security by design approach should be an essential principle applied when designing public spaces. For example, design concepts for building entrances and open public areas (e.g. access control zones and vehicles barriers) can mitigate risk and prevent hostile intrusions. Local authorities need to prioritise integrating security and safety partners in the renovation process of urban plans. This combination of the expertise from, among others, architects, planners and the police will enable the implementation of optimal, cost-effective, multi-functional and socially acceptable solutions¹¹.

Moreover, consolidating a European Union Risk Assessment Process Methodology is an important step towards a common model for assessing terror-related risks, and is the first step towards a collective approach to preparation and planning. The EU-HRSN and PSA have already made efforts in this area, proposing a three-step model that focuses on intent and capability, threat and vulnerabilities. This will allow procedures to be standardised and facilitate the dissemination of good practices among all EU members. The methodology applied was based on the following assumptions: clear identification of the risk owner; level and nature of threat, based on the *modus operandi* (scenario), hostile intent, capability and opportunity; worst-case consequences; level of vulnerability and residual risk; mitigation/counter measures recommendations.

The adoption of the new EU Agenda on Preventing and Countering Terrorism and Violent Extremism¹² highlights the need to invest in early detection capabilities and innovations to protect citizens and public spaces from threats posed by explosives, drones, 3D-printed weapons, vehicle ramming and bladed weapons. Furthermore, the EU programme identifies

¹¹ M. Larcher, V. Karlos, R. Schumacher, D. Strezova, A. Caverzan, J. Coaffee, B. Moritz, A.V. Neves, S. Ilum, N. Gebbeken, A. Schröder, M. Schlüter, P. Warnstedt, M. Stewart, *Security by Design: Protection of public spaces from terrorist attacks*, JRC131172. The text is available on a website: <https://publications.jrc.ec.europa.eu/repository/handle/JRC131172>.

¹² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ProtectEU: Agenda to prevent and counter terrorism, COM(2026) 101 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026DC0101> [accessed: 17 VI 2026].

as a key action the support to testing and deployment of EU-funded solutions to equip law enforcement. These are areas in which the Network is actively ongoing developments through its working groups.

In line with the Directive on the resilience of critical entities¹³, the focus of public space prevention, protection and immediate response is shifting towards a wider challenge. Resilience is recognised as an increasingly important element of the overall framework for combating terrorism and hybrid threats. Private and public stakeholders must be, more than ever, prepared to counter incidents that could disrupt the functioning of essential services, to mitigate their effects, and to take remedial action.

Summary

During the 2024-2025 cycle, the EU-HRSN has grown in terms of partners and capabilities. It has consolidated its role as a relevant European and international stakeholder in the protection of public spaces by organising conferences, expert meetings, workshops, training programmes and international exercises. These activities systematically aligned efforts, shared good practices and developed technical, tactical and operational-level procedures.

The EU-HRSN is more than a cooperation forum, it has been evolving beyond its initial responsibilities as a European cooperation forum, assuming itself as an active security platform for knowledge development and specialised capability building in support of high-risk events and public areas. It translates cooperation into a structured instrument for a real and effective impact into daily security needs.

On 12 February 2026, the Portuguese Chairmanship symbolically handed over the Network leadership to the French counterpart of the GNR, the Gendarmerie Nationale, which actually took over on 1 March. The takeover of responsibilities should not be seen as the, but as an opportunity for renovated energy, taking advantage of the momentum, institutional memory and operational network credibility to implement and consolidate the EC action plans and agenda.

¹³ 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).

The Portuguese GNR's commitment to national and international cooperation in the field of specialised intervention and public spaces protection will remain fully active within the EU-HRSN and across the various platforms, the GNR participates, as a proactive, dynamic and highly proficient partner, fully aware that, by working together and aligning efforts, we will be always better prepared to deal with (in)security challenges.

Col. Pedro Nogueira

Chaired the High Risk Security Network (HRSN) 2024–2025.

Contact: presidency@hrsn.eu

Young people and state security. Social factors contributing to radicalisation in the Youth Diagnosis 2026 report

Paweł Rabiej

Korczak University

 <https://orcid.org/0009-0008-4531-8684>

Konrad Ciesiołkiewicz

Korczak University

 <https://orcid.org/0000-0001-6926-3448>

The growing vulnerability of young people to radicalisation, disinformation and social influences leading to destabilisation – exacerbated by their mental health crises, the weakening of social ties, a sense of exclusion and functioning in digital environment – poses a challenge to national security. Risk analyses in this area rarely take into account the specific nature of the social challenges facing the young generation. The *Youth Diagnosis 2026 report*¹ published in the spring identifies a number of factors that foster radicalisation and lead to behaviours detrimental from the perspective of state security, which is also influenced by the psychosocial and informational resilience of young people – their ability to cope with crises,

¹ *Diagnoza Młodzieży 2026* (Eng. Youth Diagnosis 2026), P. Rabiej (ed.), Warszawa 2026.

disinformation, polarisation and pressure of digital environment. Such studies should form part of the risk analysis relating to threats of a terrorist nature. Their in-depth analysis enables a more accurate prediction of the trajectory of radicalisation processes at any given time, including those that result in violence or actions directed against the state. Holistic assessments of this kind also represent a valuable contribution by Poland to research conducted in other countries on the social and economic dimensions of the radicalisation.

A portrait of young people and young adults

In their research, the authors of the *Youth Diagnosis 2026* focused on Generation Z, i.e. individuals born between 1996 and 2012. For the purposes of the study, they adopted a division into two basic groups: young people aged 15–18 and young adults aged 19–29. This definitional scope is consistent with the solutions adopted in most European youth strategies and public policy documents concerning young generation.

The publication analyses more than 220 reports, studies and expert analyses published primarily between 2020 and 2025 on various aspects of the young generation's lives in Poland and Europe. It includes both national and international sources, including reports of public institutions, international organisations, research centres as well as youth strategies currently in force in the European Union states.

For the purposes of this publication, representative quantitative research was conducted on adolescents and young adults, as well as on staff working at institutions in the education, social services, healthcare and culture sectors, as well as organisations working with young people. The analysis was supplemented by qualitative research covering both the family environment and social relationships of young people, as well as issues relating to their identity, mental wellbeing and psychological capital. Issues concerning the functioning of youth in the digital environment were addressed, including the impact of social media, disinformation, online violence and the algorithmisation of content. The analysis covered also the educational environment, young people's civic engagement, their position in the labour market, the level of employment stability, and their strategies for achieving independence, including housing-related and economic barriers to entering adulthood.

A key value of the *Youth Diagnosis 2026* lies in its adoption of an interdisciplinary perspective combining the contributions of social policy, sociology, psychology, pedagogy, digital media studies and public policy analyses. This enabled a multidimensional approach to the situation of young people, encompassing both their individual experiences and social relations, as well as broader institutional, cultural and structural determinants. The analysis employs a life course approach, developed primarily by Glen H. Elder Jr. It is based on the assumption that an individual's life course is shaped by a sequence of interrelated experiences, transition points and accumulating risk factors as well as social resources. This made it possible, among other things, to capture the accumulation of risks and critical points emerging at successive stages of adolescence and the transition to adulthood².

The situation of the young generation was analysed both from the perspective of current social challenges, and in the context of long-term cultural, technological and civilisational transformations over the last 2–3 decades. These trends are cumulative in nature and reinforce each other. They affect young people's wellbeing, the level of social cohesion and national security. Nowadays, they live in a world characterised by a high degree of individualisation, with an increasingly evident focus on autonomy, personal needs and mental wellbeing. The growing focus on the 'self', accompanied by a weakening of relationships and communal bonds, increases individuals' susceptibility to environments that offer a strong group identity and simplified narratives of reality. These changes are taking place alongside the digitalisation of everyday life. As many as 71% of young people declare that their generation is addicted to mobile phones. More than 80% of children create social media accounts before the age of 13, and the average time spent online reaches nearly five hours per day³. These trends are reinforced by the functioning of the young generation under conditions of chronic stress and a sense of uncertainty.

² See in more detail: G.H. Elder Jr., M.K. Johnson, R. Crosnoe, *The Emergence and Development of Life Course Theory*, in: *Handbook of the Life Course*, J.T. Mortimer, M.J. Shanahan (eds.), New York 2003, pp. 3–19; D. Woodman, J. Wyn, *Youth and Generation: Rethinking Change and Inequality in the Lives of Young People*, London 2015.

³ See in more detail: A. Ładna, K. Kamiński, K. Rosłaniec, A. Wrońska, M. Błazej, A. Jankiewicz, F. Konopczyński, M. Nawrot, *Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców* (Eng. Teenagers. Report on a nationwide survey of students and parents), Warszawa 2025.

Nearly half of teenagers have extremely low self-esteem, and almost every fifth student aged 13–17 has engaged in self-harm over the past year⁴.

Five reasons of youth susceptibility to risky behaviours

As the report shows, excessive use of digital environment by young people, deteriorating mental wellbeing, weakening social relationships, a crisis of social bonds and loneliness, problems at school, in the labour market, and the process of becoming independent, are not merely separate ‘sector-specific challenges’. Together, they form a constellation of risk factors that can lead to exclusion and undermine social integration, as well as increase young people’s vulnerability to radicalisation, polarisation, and behaviour that poses a threat to their own safety and public safety. The accumulation of various psychosocial and environmental stressors is of particular significance.

These conclusions are consistent with contemporary interpretations identified in academic literature and in reports by European institutions dealing with safety and the prevention of extremism. *The Root Causes of Violent Extremism* report prepared by the Radicalisation Awareness Network describes radicalisation as a kaleidoscope of factors encompassing individual, social, economic, political and digital experiences⁵. In this context, the report discusses mutually reinforcing risk configurations, overlapping experiences of marginalisation, the weakening of social bonds, identity crises, psychological strain, political deprivation and functioning within polarised digital environment. On this basis, five key factors can be identified that increase the vulnerability of young generation in Poland to extremist narratives, symbolic violence, civic withdrawal, radicalisation, extremist attitudes and behaviours that destabilise social safety.

⁴ See in more detail: M. Dębski, J. Pyżalski, J. Borchet, H. Witkowska, *Dobre i złe wiadomości – życie online i offline a zdrowie psychiczne polskich nastolatków. Raport z badań* (Eng. Good and bad news – online and offline life and the mental health of Polish teenagers. Research report), Gdańsk 2025.

⁵ M. Ranstorp, M. Meines, *The Root Causes of Violent Extremism*, Luxembourg 2024; Europol, *European Union Terrorism Situation and Trend Report 2025*, Luxembourg 2025.

A subjective sense of injustice, marginalisation and grievance

One of the key mechanisms increasing young people's vulnerability to radicalisation in Poland is a subjective sense of injustice, marginalisation and lack of social recognition. It has emotional and interpretative character, what matters is not so much the individual's objective social situation, but rather the way they perceive their own position in the society, relations with institutions and their ability to influence social reality. In the literature on radicalisation, a sense of grievance is considered one of the strongest predictors of susceptibility to extremist narratives, particularly in situations of accumulated frustration and weakening of social bonds⁶.

A significant proportion of the young generation experiences a sense of social 'invisibility' and 'insignificance'. This is confirmed by many indicators describing young people's relations with the state, institutions and society. Only 22% of young people believe that their views are taken into account in public decision-making processes, which is one of the lowest figures among the OECD (Organisation for Economic Co-operation and Development) countries. At the same time, only 35% of young Poles view the quality of public services positively, and in surveys, participants have repeatedly pointed out that public policies are designed primarily with older age groups in mind. As a result, young people often perceive themselves as a group lacking real influence on decisions concerning their future. Such people are convinced that their needs, lifestyle and values are not treated as a matter of individual choice. In qualitative research, young adults used expressions such as 'somewhat second-class citizens' and 'no one listens to us – at home, at school or in the state'. The sense of marginalisation is reinforced by the paternalistic and disrespectful treatment of young persons, among others by the education system, the labour market, and political parties, which generates a sense of limited influence over one's social life. In such conditions, radicalisation may be perceived as a form of regaining influence, agency and a sense of satisfaction from action.

⁶ Cf. A.W. Kruglanski, J.J. Bélanger, R. Gunaratna, *The Three Pillars of Radicalization: Needs, Narratives, and Networks*, Oxford 2019.

Chronic stress and anxiety, a sense of uncertainty

Young people live under a great deal of stress and anxiety, constant social, economic and geopolitical uncertainty, which reduces their sense of security. Major sources of tensions include economic concerns and anxiety related to the global situation: 69% of young adults fear the outbreak of war⁷, 57% feel uncertainty due to rising living costs, and more than half are worried about the consequences of climate or demographic change⁸. Concerns about jobs are also a source of tension – these already affect teenagers aged 14–15 and are the result of the ‘transfer of fears’ from parents who have experienced difficulties in the labour market. Most teenagers (78%) are afraid that they will not find suitable employment, and 58% of young adults indicate a lack of job stability as a key problem that makes it difficult to enter adulthood. This reinforces anti-immigrant sentiment among the young people – as many as 68% of people aged 18–24 are concerned about the prospect of large-scale labour migration to Europe. Alongside war, this is one of the most frequently cited threats to the future. At the same time, 55% of study participants believe that migrants drive down wages, 66% – increase crime, and 69% – place a burden on the social welfare system⁹.

The housing situation is a major source of frustration for the Generation Z. The rent gap and limited access to support schemes mean that the proportion of young adults still living at home is steadily rising. According to CBOS research, almost 39% of single people aged between 25 and 34 live with their parents. By way of comparison, in 2005, this figure stood at 29%¹⁰. The factors contributing to ‘blocked adulthood’ are the cause of deep frustration among more than half of the young adults population, who respond to this situation with anger, fear and a sense of threat. This is exacerbated by an infodemic in a digital environment – that is, an overload of information in which it is difficult to distinguish truth from lies and manipulation – as well as the tribalisation of discourse, information bubbles and a low level of media literacy. War, migration, economic uncertainty,

⁷ *Młodzi Polacy o wyzwaniach stojących przed ich pokoleniem* (Eng. Young Poles on the challenges facing their generation), ‘CBOS Research report’ 2025, no. 56, comp. J. Scovil, Warszawa 2025.

⁸ See in more detail: European Parliament, *Eurobarometer Youth Survey 2024*, Brussels 2025.

⁹ *Młodzi Polacy o wyzwaniach...*

¹⁰ *Młodzi dorośli w domu rodzinnym* (Eng. Young adults living at home), ‘CBOS Research report’ 2025, no. 108, comp. D. Litwin, Warszawa 2025.

rising cost of living, competition for jobs and social status are fuelling the need for simple answers and 'us versus them' divisions.

The experience of exclusion, marginalisation, violence and humiliation

The report identifies a sense of deprivation as a third mechanism driving adolescents and young adults toward radical behaviours that threaten security. In 2023, extreme poverty affected 7.6% of people aged 0–17 (approx. 521 000 children), which was the highest level since 2015 and represented an increase of around 125 000 people compared with the previous year¹¹. Despite Poland's relatively favourable economic situation and the very strong state of its labour market compared with other EU countries, around 10% of young people aged 15–29 are not in education, employment or training (NEET). This involves the risk of long-term social exclusion and unstable pathways into adulthood. Approx. 23% of people aged 11–17 experienced at least one form of neglect, with emotional neglect being the most common type¹².

The increase in violence against children and youth is a risk factor. According to the report of the 'We Give Children Strength Foundation' (Polish: Fundacja Dajemy Dzieciom Siłę, FDDS), as many as one-third of people up to the age of 18 have experienced various forms of aggression from those closest to them, and up to one-fourth aged 11–17 may have been sexually abused¹³. 67% of staff at youth-oriented institutions, who participated in the study for the report, highlighted an increase in violence. Exclusion and marginalisation also occur within the family environment. One in four 15- to 19-year-olds does not feel supported or accepted by their families. In turn, in the school environment, 62% of students experienced various forms of peer violence¹⁴. The latest research by the FDDS indicates that peer

¹¹ R. Szarfenberg, *Poverty Watch 2025*, Warszawa 2025.

¹² K. Makaruk, K. Drabarek, A. Popyk, S. Wójcik, *Diagnoza przemocy wobec dzieci w Polsce 2023* (Eng. Diagnosis of violence against children in Poland 2023), Warszawa 2023, p. 6.

¹³ Ibid.

¹⁴ See in more detail: R. Kaczan, P. Rycielski, M. Wójcik, *Obraz bullingu w szkołach ponadpodstawowych* (Eng. Bullying in secondary schools), https://swps.pl/images/DOKUMENTY/Raporty/Obraz-bullingu-w-szkolach-ponadpodstawowych- raport-2025.pdf?utm_source=mautic&utm_medium=mailing [accessed: 24 VI 2026].

violence has become a widespread phenomenon. According to the *Peers. Report on Peer Violence 2026*, as many as 87% of children and young people aged 10–17 have experienced at least one form of peer violence, 75% have encountered cyberbullying, and 63% have experienced physical violence. It is particularly worrying that almost one in three young people (31%) has experienced repeated bullying, which, according to the relevant literature, is one of the most harmful forms of peer violence¹⁵.

Research on bullying indicates that prolonged violence, rejection and marginalisation increase young people's inclination to seek out alternative communities that provide a sense of belonging, significance and agency. The experience of exclusion and 'social invisibility' can undermine trust in the institutions, whereas radical circles offer emotional community, empowerment, as well as symbolic compensation for earlier experiences of humiliation and failure.

Mental overload, low mental resilience and an identity crisis

A significant proportion of the young generation lives under conditions of constant stress, pressure and reduced mental resilience. Almost two-thirds of people aged 15–18, who took part in the survey conducted for the report, said they felt burnt out or depressed, with 36% reporting this to a significant or very significant extent. During the moderated discussions, young people kept saying: 'We haven't even started living yet, and we are already utterly exhausted'. 70% of young people cite school as one of the main sources of everyday stress and mental overload¹⁶.

Almost half of teenagers aged 10–19 have low self-esteem, and around 40% of secondary school pupils show symptoms of depression¹⁷. One in

¹⁵ J. Kopycka, S. Wójcik, P. Raczyński, *Rówieśnicy. Raport o przemocy rówieśniczej 2026* (Eng. *Peers. Report on peer violence 2026*) Warszawa 2026, pp. 8–9.

¹⁶ See in more detail: *Prawa dziecka w Polsce 2024. Wyniki badania porównawczego prezentującego perspektywę dzieci, rodziców i nauczycieli oraz rekomendacje koniecznych zmian* (Eng. *Children's rights in Poland 2024. The results of a comparative study presenting the perspectives of children, parents and teachers, and recommendations for necessary changes*), UNICEF, <https://unicef.pl/prawa-dziecka/analizy-i-rzeczniactwo/analizy-i-rekomendacje/prawa-dziecka-w-polsce-2024>, p. 12 [accessed: 24 VI 2026].

¹⁷ See in more detail: J. Flis, M. Dębski, *Młode głowy. Otwarcie o zdrowiu psychicznym. Raport z badania dotyczącego zdrowia psychicznego, poczucia własnej wartości i sprawczości wśród młodych ludzi w Polsce* (Eng. *Young heads. Opening up about mental health. Report from*

four pupils experiences feelings of sadness and emptiness¹⁸. Particularly alarming is the rise in the number of suicide attempts among young people – between 2013 and 2024, the figure increased approx. sixfold. The vast majority of staff in institutions working with young people (87%) have observed a rise in emotional and mental health problems among the Generation Z. A state of chronic stress, reduced mental resilience and an identity crisis may increase young people's susceptibility to radical narratives that offer simple explanations of reality, a strong sense of group identity, a sense of agency and emotional compensation, and thus foster openness to behaviour that undermines social and public security.

Weakened relationships, loneliness, alienation, lack of sense of belonging

The final factor identified in the report as increasing young people's susceptibility to radical behaviour that threatens public safety is the weakening of social ties and a growing sense of loneliness and alienation. Individualisation of social life, focus on individual autonomy, the selective nature of relationships and the diminishing role of community institutions are leading to a narrowing of the support networks available to young people. Relationships between adolescents and young adults often involve only 2–3 people, more than 80% of young people maintain their most important bonds within a very narrow group of friends¹⁹. Intergenerational ties have also weakened, as have the relationships previously forged by school, social organisations, interest groups or local communities.

Around a quarter of pupils experience exclusion from their peer group and loneliness at school, while 64% of pupils in Poland say they feel part of the school community, compared with the OECD average of 75%²⁰. 38% of teenagers report feeling lonely, and 16% experience severe loneliness. Among young adults, the sense of loneliness affects more than 42% people. At the same time, 44% of young adults are not in any relationship and do

a study on mental health, self-esteem and agency among young people in Poland), Warszawa 2023.

¹⁸ See: M. Dębski, J. Pyżalski, J. Borchet, H. Witkowska, *Dobre i złe wiadomości...*

¹⁹ See in more detail: *Diagnoza Młodzieży 2026...*, p. 63.

²⁰ See in more detail: *PISA 2022 Results. Learning During – and From – Disruption*, vol. 2, Paris 2023.

not have anyone close to them²¹. Almost two-thirds of young adults believe that it is difficult to find a suitable partner these days, half say they do not trust other people²². This is often accompanied by low levels of social trust and difficulties in building lasting emotional relationships. The factors mentioned encourage the search for groups or individuals with a clearly defined identity who offer support and a sense of belonging, including those from radical circles, promising easy respect and a restoration of a sense of agency.

The digital and information environment as 'a risk multiplier'

The digital and information environment has become a key 'risk multiplier', that is, a factor that increases the risk of young people being susceptible to radicalisation and behaviour that undermines social security. Particularly worrying is the nature of young people's lives, which are shaped by the recommendation algorithms of social platforms, streaming services, online games and messaging apps. A characteristic of the modern digital environment is the asymmetry between the pace of development of online platforms and the ability of public institutions to regulate and oversee them. As a result, young users remain exposed to the influence of algorithmic content selection mechanisms that can reinforce cognitive polarisation, create closed information bubbles and increase exposure to extremist and anti-establishment narratives.

Several conclusions can be drawn from the available research in this field. Firstly, the vast majority of young people who use social platforms are exposed to various types of conspiracy theories in this environment. The more time they spend there, the more susceptible they become to their influence. Those least resistant to the influence of conspiracy theories are individuals aged 14–16, and among adults, those up to the age of 35²³.

²¹ See in more detail: *Młodzi Polacy o męskości, kobiecości i różnicach między płciami* (Eng. Young Poles on masculinity, femininity and gender differences), 'CBOS Research report', 2025, no. 52, comp. J. Scovil, Warszawa 2025.

²² See: K. Gagatęk, U. Karaś, J. Kelsz, *Stan młodych 2025* (Eng. State of youth 2025), Warszawa 2025.

²³ A. Byrne, D. Martin, C. Jones, N. Galbraith, T. Mercer, *Conspiracy theory beliefs in the adolescent population: A systematic review*, "Journal of Adolescence" 2024, vol. 96, no. 5, pp. 925–939. <https://doi.org/10.1002/jad.12316>.

Secondly, recommendation algorithms enable easy access to violent content – they promote radical, eye-catching content that isolates young people in information bubbles. There is also a clear trend in boys' exposure to misogynistic messages that promote hatred towards girls and women, reducing them to a subordinate role in relation to men. The so-called manosphere – created through algorithmic radicalisation is a conglomerate of extremist content²⁴.

Thirdly, we are seeing a huge increase in the amount of sexually explicit material, including pornography (distributed mainly by social platforms), and content depicting the sexual abuse of children, the so-called CSAM (child sexual abuse materials). Analyses concerning the activities of the 764 Network²⁵ – deemed terrorist by some countries – indicate that such actions are not driven solely by sexual motives, rather, they exploit the natural curiosity and confusion of young people to generate materials used for manipulation, intimidation and the coercion of criminal acts²⁶.

At the same time, there has been a noticeable increase in the use of encrypted messaging apps, which, while providing a sense of privacy, have also become tools for criminal activity. Numerous analyses carried out by institutions responsible for security indicate that this represents a new trend in the development of phenomena threatening public safety, which are linked to the use of popular applications for weaponisation of minors – that is, exploitation of children and young people as a form of weapon, a tool for exerting influence, destabilisation or causing harm. Particular attention should be paid to two phenomena: nihilistic violence²⁷ and assigning tasks

²⁴ K. Regehr, C. Shaughnessy, M. Zhao, N. Shaughnessy, *Safer scrolling. How algorithms popularise and gamify online hate and misogyny for young people*, Canterbury 2024.

²⁵ The 764 Network is a loose international online community comprising mainly very young people associated with extreme forms of online psychological abuse, blackmail, self-harm, sexual coercion and the radicalisation of minors. The name derives from the number used by one of the community's first administrators. See in more detail: K. Ciesiołkiewicz, *Weaponizacja osób małoletnich i młodych dorosłych. Nowe zagrożenia dla bezpieczeństwa wewnętrznego* (Eng. Weaponisation of minors and young adults. New threats to internal security), https://uczelniaokrczaka.pl/wp-content/uploads/2026/06/WEAPONIZACJA_MATERIAL.pdf, p. 17 [accessed: 24 VI 2026].

²⁶ *OSINT Report 764*, 12 September 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Public%20Version%20of%2020240910_nr02_OSINT_Report_764%20.pdf [accessed: 12 V 2026].

²⁷ *Terror without ideology? The rise of nihilistic violence*, Institute for Strategic Dialogue, 8 V 2025, <https://www.isdglobal.org/digital-dispatch/terror-without-ideology-the-rise-of-nihilistic-violence-an-isd-investigation/> [accessed: 12 V 2026].

to minors through popular messaging apps. The first of these relates to the operation of distributed networks known as Com (English: Communities). These are informal groups, movements and individuals who communicate with one another online and who have their own system for establishing their status within the group by engaging in criminal activities²⁸. The 764 Network, as described earlier, is the very epitome of this type of nihilist form of radicalisation.

Europol points to the growing scale of the use of instant messaging apps to commission criminal activities. It refers to them with the acronym VaaS (violence-as-a-service)²⁹. The data shows that digital environment not only increases exposure to extreme content but also weakens the ability to critically evaluate information and reinforces social polarisation. The data indicates a low level of competence regarding the assessment of digital content credibility. More than 40% young people believe it is difficult to distinguish between true and false information online, and less than half say they are interested in the credibility of the profiles they follow and sources of information³⁰. Research conducted by the Centre for Information Society Analysis at Korczak University shows that among teenagers there is a distinct, strong relativisation of truth and a reliance on the principle of fairness – the more comments there are under a particular post and the more popular it is, the more credible it becomes. It also seems that information overload is leading to ever-increasing cognitive passivity³¹.

²⁸ K. Ciesiołkiewicz, *Nowe zagrożenia. Nihilistycznie zorientowana przemoc małoletnich oraz „przemoc jako usługa” – wyzwania dla bezpieczeństwa wewnętrznego i społecznego* (Eng. New threats. Nihilistic juvenile violence and ‘violence as a service’ – challenges to internal and social security), https://uczelniakorczaka.pl/wp-content/uploads/2026/02/NOWE-ZAGROZENIA_Konrad-Ciesiolkiewicz-Uczelnia-Korczaka.pdf, p. 6 [accessed: 12 V 2026].

²⁹ *Operational Taskforce GRIMM*, Europol, 1 IV 2025, <https://www.europol.europa.eu/how-we-work/operations/operational-taskforce-grimm> [accessed: 12 V 2026].

³⁰ R. Lange, A. Wrońska, A. Ładna, K. Kamiński, M. Błażej, A. Jankiewicz, K. Rosłaniec, *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców* (Eng. Teenagers 3.0. Report on a nationwide survey of schoolchildren and parents), R. Lange (ed.), Warszawa 2023, p. 7.

³¹ K. Ciesiołkiewicz, A. Buchner, K. Ferenc-Błońska, M. Wierzbicka-Tarkowska, *Miedzy faktem a feedem. Podatność młodzieży na dezinformację w środowisku mediów cyfrowych* (Eng. Between fact and feed. Young people’s susceptibility to disinformation in the digital media environment), Rzeszów 2025, pp. 55–61.

Recommendations

The *Youth Diagnosis 2026* indicates that limiting the young generation's susceptibility to radicalisation requires a systemic approach that goes beyond the actions of security institutions, and responses to isolated incidents. The conclusions included in the discussed report make it possible to formulate the key directions for further actions.

A coherent national youth strategy should be developed, based on an analysis of life trajectories, combining educational, social, health and digital initiatives, as well as measures to strengthen psychosocial resilience of young people. One element of national youth strategy should be public policy measures aimed at countering radicalisation leading to violence.

Cross-sectoral initiatives are also essential to counter the radicalisation of young people, including the involvement of the social services sector. In European countries, the importance of the preventive social approach is growing. It is based on the premise that young people's radicalisation is often the result of a combination of relational, mental health, educational and social problems. Schools, social services, working with families, local organisations and mental health institutions play a key role in this approach. Particular importance is attached to schools as institutions for the early detection of crises and the building of psychosocial resilience, emotional competences and a sense of belonging. In many EU countries, teachers, educators and psychologists are trained to recognise signs of social isolation, sudden changes in behaviour, fascination with violence, radical narratives and mental health crises. It is also important to combat peer violence, including bullying, as well as to strengthen relationships and group cohesion.

Increasing importance is being attached to environmental youth work. This idea is based on creating safe and easily accessible spaces for meeting, engaging in activities and building relationships, which young people can use voluntarily, without any formal requirements for participation and institutional barriers. Such 'low-threshold social spaces' operate outside school and family, enabling young people to form relationships with their peers and trusted adults. Youth clubs, mentoring, street working or sport and cultural activities strengthen social bonds, agency and local integration, as well as enable the early identification of marginalisation, mental health crises and radicalisation processes. These measures are complemented by civic, media and digital education, which helps to build resilience to disinformation, manipulation and

extremist narratives. Prevention of radicalisation is increasingly based on the development of social and emotional skills as well as strengthening the so-called community resilience, because strong social relationships, sense of belonging, agency as well as presence of accessible and supportive institutions are a key safeguard against extremism.

The authors of the *Youth Diagnosis 2026* propose focusing public sector efforts on weakening the social factors conducive to radicalisation and dangerous behaviours, as well as on prevention and building resilience. Based on the findings of the research, they also identify two areas of action: the first focuses more on youth, the second on young adults. In accordance with the triad of resilience, it is proposed that the competencies and resources that protect young people from the influence of disinformation, violence, manipulation and radical groups should be strengthened. The key is to reinforce young people's mental and emotional resilience, which involves developing social and emotional skills, the ability to cope with stress, build relationships and regulate emotions. The second pillar of this approach is strengthening relational and community resilience, rebuilding social ties, reinforcing the sense of belonging and supporting peer, family and local communities. The third element is information and digital resilience – the development of media literacy skills, critical thinking and the ability to recognise manipulation, disinformation and extremist content in the digital environment. Regulations of digital environment are also urgently needed, including, among other things, effective regulation of digital platforms, limiting exposure to violence, pornography, toxic content and extremist content, greater responsibility of platforms for their recommendation algorithms, and the development of rapid response and support systems.

The second line of action focuses on young adults, and the aim in this case is to strengthen life stability as a means of preventing radicalisation. The authors of the report indicate that job insecurity, the precarious nature of work and barriers to housing increase frustration and a sense of a lack of prospects. It is therefore crucial to implement the public policies described as the triad of resilience. This includes improving job security, access to housing and support for becoming independent, as well as enhancing social mobility by reducing transport exclusion.

The *Youth Diagnosis 2026* presents one of the most comprehensive pictures of the current situation of young generation in Poland. It shows that radicalisation of young people is not just a problem of security

or the influence of ideology, but a phenomenon deeply rooted in social processes. The authors of the study indicated that effective prevention must be based primarily on policies that strengthen social functioning of the young generation – developing psychological, relational and informational resilience, and ensuring a stable transition to adulthood for young people through job security, access to housing and increased social mobility. Curbing radicalisation therefore requires action at the source – rebuilding social ties, a sense of agency and a sense of security in young people's lives. In the long term, this may become one of the key factors in strengthening social resilience and state security.

Paweł Rąbiej

Coordinator of work on *The Youth Diagnosis 2026*.

Contact: p.rąbiej@uczelniakorcza.pl

Konrad Ciesiołkiewicz, PhD

Head of the Centre for Information Society Analysis at Korczak University, co-author of *The Youth Diagnosis 2026*.

Contact: konrad.ciesiolkiewicz@gmail.com

Report on the conference 'New factors influencing the radicalisation of young people from a national security perspective'

Warsaw, 23 April 2026

Aleksandra Komar

Independent author

 <https://orcid.org/0000-0002-9717-5258>

'New factors influencing the radicalisation of young people from a national security perspective' conference on the issue of the radicalisation of minors took place on 23 April 2026 at the Internal Security Agency headquarters in Warsaw. The event was attended by representatives from the academic community, security experts and practitioners from the Central Cybercrime Bureau, the State Commission for Investigation of Cases against Sexual Liberty and Decency against Minors under the Age of 15 years old, the Institute of Social Safety, the Korczak University, the Civitas University, NASK, the Military University of Technology and the Internal Security Agency. The organisational structure adopted made it possible to bring together different perspectives, which shaped the conference's central theme: the tension between technological development and the psychosocial safety of young people, with particular emphasis on the mechanisms of radicalisation that may lead to terrorist actions.

The problem of radicalisation of young people and young adults is a multifaceted phenomenon, which has repercussions in almost every sphere of public life. It can be regarded as one of the most significant contemporary security threats, affecting: the state's internal security, the work of the security services and the police, international stability, cybersecurity and social policy.

As Konrad Ciesiołkiewicz, PhD, a deputy chairman of the State Commission for Investigation of Cases against Sexual Liberty and Decency against Minors under the Age of 15 years old, rightly pointed out: (...) *the age of those becoming radicalised has now fallen significantly. Children as young as 10 or 11 meet the criteria for radicalisation. We should therefore regard them as a critically important group, as a soft underbelly of the social security system.*

The conference was a response to the rapidly developing radicalisation, which defies existing analytical frameworks. In terms of the scale of the phenomenon's impact, several key areas and dimensions should be highlighted. It is worth emphasising the social and scientific aspects – radicalisation challenges existing sociological and pedagogical paradigms and requires an interdisciplinary research approach. It affects the wellbeing and development of society by directly undermining its structures, which weakens social bonds and hampers the development potential of the young generation. It should be emphasised that radical attitudes among young people are the foundation of the future political polarisation, which could destabilise democratic structures and public institutions. In its most extreme form, this phenomenon becomes a real threat to public order, which gives rise to the need for heightened vigilance on the part of security systems. The participants of the conference discussed issues such as: causes, mechanisms, consequences of youth radicalisation and methods of prevention.

Causes of youth radicalisation

Paweł Rabiej, an expert of the Polish Society for Social Policy (PTPS), presented the susceptibility of young people to radicalisation, in the light of his own research, analyses of existing data and the findings of the *Youth Diagnosis 2026* report¹.

¹ The first large-scale, holistic scientific report describing the situation and needs of young Poles (Generation Z), compiled by the experts of the PTPS on behalf of the Ministry of National Education. It forms the basis for the new National Youth Strategy. See in more

The speaker discussed the background to the radicalisation of young people and outlined its causes. He pointed out six key mechanisms of radicalisation:

- 1) a subjective sense of injustice and grievance,
- 2) crises and tensions that create a climate of pressure,
- 3) inequalities, social exclusion, violence, negative trajectories,
- 4) identity crisis and the need for a sense of belonging,
- 5) political deprivation – a sense of lacking influence and agency,
- 6) digital and information environment – exacerbates the process of radicalisation.

The research he presented shows that as many as 60% of people aged 15–18 live in a state of constant tension, complaining of severe stress, chronic fatigue and a severe lack of energy for everyday life. The suffering of the young people affects many areas of their lives – they experience stress at home (their home and family are not a safe haven) and stress at school (school is seen as a system focused on results rather than on the individual). The speaker highlighted the dramatic scale of violence in the virtual world. For many young people, the internet is a space of trauma and violence, rather than one of personal development. The research presented shows that as many as one in four teenagers has been a victim of cyberstalking and persistent harassment. Even more alarming is the fact that 20% of respondents have experienced sexual harassment online. The conclusion drawn from these figures was that experiencing violence and harassment online is a source of radicalisation. A victim who feels abandoned by institutions and adults becomes susceptible to narratives put forward by groups offering ‘strength’, ‘retaliation’ or a radical change to the system that failed to protect them.

To supplement the above findings, the crisis in the family’s educational role and the erosion of authority within school and educational institutions should be identified as significant factors in primary and secondary socialisation. Shortcomings in terms of emotional support, relationship stability and the transmission of norms and values may encourage the search for alternative, often radical role models.

detail: P. Rabiej, K. Ciesiołkiewicz, *Young people and state security. Social factors contributing to radicalisation in the Youth Diagnosis 2026 report*, “Terrorism – Studies, Analyses, Prevention” 2026, no. 9, pp. 421–435. <https://doi.org/10.4467/27204383TER.26.018.23801> (editor’s note).

Political and geopolitical factors also play a significant role, including global crises, armed conflicts and international tensions, which – through the information environment – influence young people's perception of reality and may strengthen radical narratives as well as a sense of threat and polarisation. Psychological and individual factors are also significant, such as neurodevelopmental disorders (including autism spectrum disorders), adjustment difficulties, emotional disorders and deficits in social competence. These factors may increase susceptibility to the influence of simplistic, binary narratives, as well as to the influence of groups promoting a strong identity, a sense of belonging and clearly defined system of values.

Mechanisms of radicalisation among young people

During the conference, it was repeatedly pointed out that contemporary terrorism is increasingly using decentralised channels of communication, which makes it much more difficult to monitor. Paulina Piasecka, PhD, from the Civitas University pointed out that radicalisation is not merely a collection of individual pages or posts, but also a self-perpetuating structure that shapes young people's attitudes. Based on current assessments and analyses of security, it can be described as a closed information loop in which technology intersects with psychology. The author accurately identified four pillars of contemporary digital recruitment:

- 1) algorithmic targeting (rapid spread of information – driven by the mechanisms of social platforms – that trigger strong emotions),
- 2) engineering of nostalgia (building 'imagined communities' by drawing on nostalgia, for example, for the socialist era),
- 3) digital recruitment (the use of, among other things, Tik Tok and Telegram as low-cost channels for outreach activities),
- 4) new frontiers (the use of artificial intelligence and deepfake technology as advanced tools of manipulation).

Communities associated with computer games are also significant. Communication platforms used by gamers, such as Discord, as well as forums and communities centred around online games, can constitute a social space susceptible to the influence of radical content. Due to the high level of anonymity, the ease with which closed groups can be formed, and the intensity of social interaction, such environments foster

the gradual socialisation of users within specific ideological narratives. In practice, they can be used for recruitment, participants' loyalty testing and distribution of extremist content, especially among younger users.

The speakers pointed out that contemporary mechanisms of radicalisation also involve the active exploitation of children and young people by extremist organisations that gradually draw minors into their activities. They assign them seemingly simple operational tasks, such as spreading disinformation, participating in closed groups, and carrying out propaganda-related activities. This is a phased process and leads to the gradual internalisation of radical narratives as well as the development of loyalty to the group. The speakers also pointed out that the time it takes for radicalisation to occur via social media has been significantly reduced. Under favourable conditions, it can unfold very rapidly and last for less than a month. This phenomenon is exacerbated by algorithmic mechanisms and closed communication environments, which accelerate the process of identification with extremist narrative and limit exposure to alternative points of view.

In an analysis of socio-psychological foundations of susceptibility to radicalisation, Paulina Piasecka accurately identified its key catalysts, including local resentment – that is radicalisation rooted in a sense of injustice, economic inequalities and social marginalisation. Border regions are characterised by a greater susceptibility to the initiation of conflicts by external actors and a strong need for recognition and belonging, factors that effectively draw minors toward aggressive radical narratives. These regions can also serve as a space for the influence of various extremist ideologies, including movements linked to radical Islamism, that exploit mechanisms of marginalisation, sense of injustice and identity deficit to recruit and reinforce extremist attitudes among vulnerable groups of young people.

According to Konrad Ciesiolkiewicz, the digital ecosystem has become the main radicalisation environment of children and youth, which today takes the form of fragmented, hard-to-detect networks known as Com (English: communities). Traditional radicalisation of the young generation intertwines with cyber threats – ranging from cyberbullying to organised cybercrime – and builds its own autonomous status structures. In this context, attention should also be drawn to 'violence-as-a-service' (VaaS) phenomenon, associated with the activities of specialised, decentralised criminal groups (referred to in the literature as the 764 Network). They

exploit minors as vulnerable targets for influence, and use psychological pressure mechanisms, manipulation and digital blackmail. This process often begins with exposure to content of a violent or shocking nature, leading to gradual information addiction and a lowered threshold of emotional reaction. Subsequently, the force of influence increases and extends to compelling specific behaviours or activities within the digital environment, including actions that support the development of criminal or extremist structures. This phenomenon is part of a wider trend towards the exploitation of children and young people in the context of criminal and destabilisation operations. This poses a significant challenge for state security systems and mechanisms for the protection of minors.

The topic above is closely linked to the issue of the nihilistic underpinnings of aggression among the youngest and commercialisation of aggression in the form of 'violence-as-a-service' within the context of state security. The speaker pointed out that the focus on environmental factors demonstrates the inadequacy of current institutional solutions, which fail to provide optimal protection for young people against online threats. In his view, remedying this situation requires a holistic approach to media ecology, which assesses the entire digital ecosystem. Referring to the thesis of Neil Postman that new technology changes everything, he pointed out that the digital sphere cannot be viewed merely in instrumental terms, as it has become a new living environment and public sphere.

Attention should also be paid to the growing risk of children and young people being exploited by external actors, including potential actions by foreign intelligence services and actors carrying out influence operations. Digital environment, characterised by a high level of anonymity and limited institutional control, may encourage the exploitation of minors as tools for carrying out destabilising activities, including the dissemination of propaganda content, reinforcing polarising narratives or participation in disinformation operations. This phenomenon fits into a broader trend of hybrid threats, in which the susceptibility of young generation to information manipulation constitutes a significant vector of influence on state's stability and its security systems.

Consequences of youth radicalisation

Consequences of youth radicalisation are of a cascade nature – start with the individual, and in extreme cases may lead to destabilisation of state structures. It should be emphasised that not all behaviour has an ideological basis. Some acts of violence may be autotelic in nature – that is, to constitute violence for its own sake. Based on the presentation and discussion of participants, four key areas of impact were identified:

- 1) for an individual (personal destruction),
- 2) for a society (deep polarisation, normalisation of violence, erosion of public trust),
- 3) for a state (systemic destabilisation),
- 4) digital (prevalence of hate speech, development of manipulation technology).

The most serious of these is the loss of the state's development potential. Young generation – instead of building a future – channels its energy into destructive and confrontational processes.

Paulina Piasecka emphasised the importance of identity-related mechanisms (systemic and social consequences). She indicated phenomena that are manifestations of affective polarisation – specifically the reinforcement of an 'us vs. them' dichotomy – which leads to deep social divisions. The saturation of false narratives with strong emotions, with the aim of manipulating public opinion, serves to deepen citizens' distrust of the public services and to subsequently exploit such attitudes.

The debates were dominated by the issue of how, in the long term, radicalisation could undermine the stability of the state and the international order. The speakers highlighted that it may weaken the state's stability, increase security spending, restrict civil liberties, worsen international relations and exacerbate ideological conflicts. From the perspective of internal threats, it was pointed out that radicalisation could lead to terrorist acts, political violence, riots and social destabilisation, attacks on state institutions as well as a rise in ideologically motivated crime. It can also undermine citizen's trust in the state, exacerbate social conflicts, hinder political dialogue as well as encourage disinformation and the spread of conspiracy theories. Ultimately, it can lead to political crises and the weakening of democracy.

In the analyses of the speakers, topics relating to cyberspace threats – on which Katarzyna Maniszewska, PhD from Civitas University and the University of Białystok focused in particular – took centre stage.

She discussed selected threats caused by the development of artificial intelligence, pointing out that AI is currently one of the main tools used to conduct information operations. Automated generation and mixing of data makes it easier for hostile actors to manipulate information on an unprecedented scale, ranging from propaganda to cyber attacks and the verification of vulnerabilities in security systems.

During the conference, it was emphasised that radical groups are increasingly operating online – recruiting members via social media, spreading propaganda, organising cyber attacks, disseminating extremist materials. Online radicalisation, especially among young people, can lead to a number of negative consequences, such as: the rise in cybercrime, participation in hacker attacks, spread of propaganda and use of hate speech. Young people are becoming more and more susceptible to manipulation, disinformation and the influence of extremist groups.

Prevention methods

Methods for countering radicalisation were not only the subject of a theoretic analysis but also of lively discussions. During the conference, it was pointed out that methods for countering radicalisation can be divided into three levels: from general prevention, to measures aimed at risk groups, and interventions for people already radicalised. Key strategies based on contemporary standards of security and education included: building resilience (preventive level), systemic and institutional activities as well as and intervention and deradicalisation (specialist level).

Among the most effective tools are the triad of resilience presented by Paweł Rabiej (resilience and development of psychological capital, development of relational and social skills as well as digital shield – a safe upbringing environment), as well as the triad of independence (increasing employment stability and flexibility, support for independent living, and reducing local transport barriers). The speaker also highlighted the importance of inter-ministerial cooperation in implementing changes aimed at reducing problems of teenagers identified in the report. Interinstitutional synergy should be based on: supporting the potential of young people in rural areas, health and reproductive wellbeing of youth, promoting healthy habits (nutrition and physical activity), equal opportunities and safety of young women's development, relationships

and young men's resilience, easier access to culture, sport and leisure time, entrepreneurship and innovation potential of young people, concern for the climate, environment and sustainable development.

During the debate, the speakers emphasised the special role of services carrying out intelligence and counter-intelligence operations in cyberspace, monitoring digital threats and cooperating with online platforms on the removal of harmful content. The importance of social media development was emphasised, as it created new opportunities for extremist organisations. Online platforms enable the rapid dissemination of propaganda, creation of closed ideological groups and anonymous contact with potential recruits. From the perspective of special services, cyberspace has become one of the key operational areas. It was emphasised that, in the present day, the radicalisation of young people can be exploited as part of a hybrid war. Hostile states or extremist organisations can deliberately exacerbate social divisions, support extremist political movements and destabilise the internal situation in other countries. It was unanimously agreed that this is a phenomenon that necessitates the modernisation of security systems and the enhancement of operational coordination at the national level and within cross-border structures. Cooperation within NATO, the European Union and the United Nations is particularly important. It includes the exchange of intelligence, joint counter-terrorism operations, sanctions against extremist organisations, and programmes to counter radicalisation.

Summary

'New factors influencing the radicalisation of young people from a national security perspective' conference provided a valuable forum for the exchange of views. The complexity of the problem of the radicalisation of minors was highlighted. Radical attitudes among young people are the foundation of a future political polarisation, which can destabilise democratic structures and public institutions. Effectively tackling this phenomenon requires an interdisciplinary approach that combines preventive, educational and systemic measures. A major highlight of the conference was the presence of representatives from the uniformed services and people working with young people. Their participation made it possible to examine the issues raised from an operational and highly pragmatic perspective. As a result,

methods such as triad of resilience have been analysed in terms of their actual effectiveness in the day-to-day work of law enforcement agencies and educational institutions. It remains to be seen whether the concepts presented will be effectively implemented in practice, and when legislative changes aimed at fulfilling the proposals put forward will come into effect.

Aleksandra Komar, PhD

Deputy Editor-in-Chief of the “Terrorism – Studies, Analyses, Prevention” – the scientific journal of the Internal Security Agency.

Contact: a.komar@abw.gov.pl



AWARDED THESES

The security policies of France and Belgium in response to terrorist threats: a case study of the Paris (2015) and Brussels (2016) attacks¹

Nicole Szostak

Independent author

 <https://orcid.org/0009-0001-9307-4951>

Abstract

The aim of the article is to analyse the security policies of France and Belgium in response to terrorist threats, using the examples of the attacks in Paris (2015) and Brussels (2016). The author adopts the thesis that experiences related to terrorist attacks have significantly influenced the evolution of the security strategies of France and Belgium, led to the strengthening of preventive measures and international cooperation. The article is based on an analysis of the relevant literature, security strategy and case studies of the attacks. Research questions are focused on the causes and consequences of the attacks, the importance of radicalisation processes and the role of transnational cooperation in counterterrorism efforts. The analysis shows that historical conditions and the specific nature of terrorist organisations' activities

¹ The article is based on the bachelor's thesis entitled *The security policy of French-speaking countries in response to terrorist threats: A Case study of the Paris (2015) and Brussels (2016) attacks* defended at the War Studies Academy. The thesis was awarded in the 15th edition of the contest of the Head of the Internal Security Agency for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats.

are significant for the development of terrorism in these countries, while coordinated actions at international level are essential for the implementation of an effective security policy.

Keywords

terrorism, security policy, France, Belgium, radicalisation, international cooperation

Introduction

Terrorism as one of the greatest threats of the 21st century affects not only the political situation in a country and its stability, but also the international order. The European Commission defines terrorism as (...) *a menace that does not recognise borders and affects countries and people irrespective of their geographical location*². It considers that the terrorist threats remain high and regards combating them as a shared European responsibility. The constant evolution of terrorist threats is a factor that has led to a widespread recognition of the need for states and international organisations to make changes to their security policies and strategies. The years 2015–2016 marked a turning point in this regard. At that time, France and Belgium suffered terrorist attacks that affected perceptions of the effectiveness of security policies, both within those countries and across the whole of Europe. This is evidenced by the responses and actions of, for example, Europol, which in January 2016 established the European Counter Terrorism Centre (ECTC), and the European Commission, which on 24 July 2020 drew up a security strategy covering the years 2020–2025, with the (...) *protecting Europeans from terrorism and organised crime*³ as one of the pillars.

The research focuses on the nature of terrorist threats and the security policies of France and Belgium. The article will outline the key principles of security policies of France and Belgium against the backdrop

² *Counter-terrorism and radicalisation*, European Commission, 26 II 2026, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation_en [accessed: 30 III 2026].

³ *EU Security Union Strategy: connecting the dots in a new security ecosystem*, European Commission – Press release, Brussels, 24 VII 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379, p. 2 [accessed: 12 VI 2026]

of the evolution of preventive measures and strategies resulting from regional and international factors, including both countries' membership of the European Union and the North Atlantic Treaty Organization (NATO), and their experiences of terrorist attacks. In doing so, the author takes into account the course and consequences of terrorist attacks.

The most important research question is: what are the main factors shaping France's and Belgium's security policies in response to terrorist threats? In order to answer this question, the following specific problems have been formulated:

1. What factors and events have influenced the development of terrorist threats to France and Belgium?
2. What were the consequences of the terrorist attacks for the security policies of France and Belgium?
3. What are the key preventive measures and safety strategies of France and Belgium?
4. What does regional and international cooperation look like in relation to terrorist threats?

The article posits the hypothesis that the most important determinants of security policies of France and Belgium in the face of terrorist threats are:

- historical circumstances, together with experiences of terrorism in both countries,
- Islamist nature of terrorist organisations, taking into account their motivations and objectives,
- impact of radicalisation and migration on the development of terrorism,
- international cooperation on matters relating to preventive measures.

The analysis was carried out using research methods typical of the security sciences, such as the analysis and synthesis of the relevant literature, the comparative method, and case studies of selected terrorist attacks. The methods used enabled the identification of links between experiences related to terrorism and the shaping of security policies in those countries.

The article examines historical context of terrorism in France and Belgium, analyses the attacks in Paris and Brussels, as well as outlines preventive measures and international cooperation in the fight against terrorism.

The historical context of terrorism in France and Belgium

Terrorism is a multifaceted phenomenon that can take various forms. It can be influenced by the actor's purpose, ideology and values. It is worth noting that contemporary terrorist threats are closely linked to the process of radicalisation, which focuses on the adoption of extreme views and attitudes that may lead to the acceptance of violence as a means of achieving ideological goals.

The analysis of modern terrorist acts involves not only examining the events themselves, but also exploring the context in which security mechanisms have taken shape. The author analysed two events in France and Belgium that marked turning points in the history of terrorism. These were, respectively, a series of attacks in Paris in November 2015, as well as at Brussels Airport in Zaventem and on the underground in Brussels in March 2016. At the same time, she presented the chronology and evolution of terrorism in both countries.

In France, the origins of terrorism date back to the French Revolution and the Jacobin government in the 18th century⁴. First terrorist attacks were linked to the anarchist movements. In 19th century, an act of violence motivated in this way took place in Paris in 1893. A bomb went off in the Chamber of Deputies. The perpetrator was Auguste Vaillant, who supported the anarchist movement because he considered the French government's political and social system to be unjust. As reported in the press at the time, (...) *the bomb was thrown from one of the stands on the second floor (...) it exploded before it hit the ground, scattering (...) huge nails and pieces of zinc and lead*⁵. This attack triggered a wave of similar attacks in France.

In the 20th century, terrorism in France was closely linked to colonial conflicts. During the Algerian War, the National Liberation Front (French: Front de Libération Nationale, FLN) was established – the party which was *a continuation of the revolutionary body that directed the Algerian war*

⁴ The Jacobin government pursued its policy through intimidation and repression which were regarded as terror.

⁵ Quoted after: M. Nadaux, *La Troisième République. La «propagande par le fait»: les attentats anarchistes (1892-1894). Explosion d'une bombe à la Chambre des députés déposée par l'anarchiste Auguste Vaillant le 9 décembre 1893, Le XIX^e siècle*, <https://web.archive.org/web/20061125095024/http://www.19e.org/documents/troisiemerepublique/anarattentats/vaillant.htm> [accessed: 21 I 2025].

of *Independence against France (1954–62)*⁶. Its military wing – the National Liberation Army (French: Armée de Libération Nationale, ALN) – was also formed then. During the Battle of Algiers, ALN soldiers mainly targeted public buildings, industrial facilities, and places of leisure and entertainment⁷.

In the context of this war, it is also worth mentioning the French Organisation de l'Armée Secrète (OAS), a far-right terrorist group whose actions were directed against the interim president Charles de Gaulle. The aim of the OAS was to halt the process of decolonisation, with particular emphasis on the Algerian question. When the president de Gaulle agreed to Algerian independence, General Raoul Salan of the French army deemed the president a traitor to the nation. The OAS, led by Salan, carried out a series of assassinations, including that of Charles de Gaulle. The attacks left around 12 000 people dead or injured⁸.

The next terrorist organisation in France was Action Directe (AD), which was characterised by ideologies such as communism, anarchism and Maoism, as well as fondness for the countries of the Global South. The organisation was most active between 1979 and 1986, when it carried out 80 attacks in France, mainly targeting prominent figures and state institutions, e.g. ministries⁹. Terrorists from AD attacked also in Belgium and Germany.

The origins of the Islamic terrorism in France date back to the 1990s. One example is the Armed Islamic Group (French: Groupe Islamique Armé, GIA), which carried out an attack on the Paris metro in 1995. The bomb explosion killed 8 people, left 25 seriously injured and 150 with minor injuries¹⁰.

⁶ *National Liberation Front*, Britannica, <https://www.britannica.com/topic/National-Liberation-Front-political-party-Algeria> [accessed: 22 I 2025].

⁷ Ł. Macuga, *Wojna algierska, 1954–1962* (Eng. The Algerian war, 1954–1962), master's thesis, Uniwersytet Mikołaja Kopernika, Toruń 2004, https://www.researchgate.net/publication/303636471_Wojna_algierska_1954_-1962 [accessed: 22 II 2025].

⁸ A. Kerherve, O.A.S., Gaullisme.fr, 30 VII 2011, <http://www.gaullisme.fr/2011/07/30/o-a-s/> [accessed: 11 VI 2026].

⁹ M. Kijewska, *Lewicowy terroryzm w Europie Zachodniej w drugiej połowie XX i na początku XXI wieku. Podstawowe informacje i kierunki rozwoju* (Eng. Leftist terrorism in Western Europe in the second half of the 20th century and the beginning of the 21st century. Basic information and directions of development), "Radzyński Rocznik Humanistyczny" 2018, vol. 16, no. 1, p. 206.

¹⁰ 27 lat temu doszło do zamachu bombowego w paryskim metrze (Eng. There was a bomb attack on the Paris Metro 27 years ago), iFrancja, 25 VII 2024, <https://www.ifrancja.fr/27-lat-temu-doszlo-do-zamachu-bombowego-w-paryskim-metrze/> [accessed: 23 I 2025].

The new wave of Islamic terrorism in France began in the early 21st century with a series of attacks organised by Al-Qaeda and the Islamic State (Islamic State of Iraq and Syria, ISIS). Between 11 and 19 March 2012, three terrorist attacks took place in Toulouse and the surrounding area. They were carried out by the 23-year-old Mohamed Merah, who had links to Al-Qaeda and supported the Islamic fundamentalism. These events sparked a debate on radicalisation in Europe and drew attention to issues of security and social integration.

The history of terrorism in Belgium began later than in France. In 1983, a left-wing organisation known as Cellules Communistes Combattantes (CCC), ideologically similar to AD, was founded in Belgium. *Between 3 October 1984 and 16 December 1985, CCC claimed responsibility for 21 bomb attacks; these took place as part of three political and military campaigns*¹¹. A criminal organisation known as Les tueurs fous du Brabant wallon, which collaborated with CCC, was responsible for many acts of terror carried out at the same time in Belgium. In 1980s, CCC and AD established close ties with one another. In 1984, the Belgian organisation raided a quarry near Brussels. The explosives stolen from there were handed over to AD, who (...) *used them to build a bomb that was planted at the headquarters of the Western European Union*¹².

In Belgium, just as in France, terrorism in the 21st century is associated with Islamic connections. Al-Qaeda was successfully recruiting new members for over a decade, both in Belgium and in France. Those responsible for the recruitment were identified and sentenced in 2010 to prison in terms of between 3 to 8 years¹³. However, this did not stop the organisation from carrying out attacks, for example, with an anti-Semitic motive in 2014, when three people were killed in a shooting at the Jewish Museum in Brussels.

¹¹ B. Francq, *Les Cellules communistes combattantes: les deux figures d'une inversion*, "Sociologie du Travail" 1986, vol. 28, no. 4, https://www.jstor.org/stable/43149431?casa_token=uvu0DU MHhm8AAAAA%3AyTH0OxhPSaWldOexG8URrz6nNtuZbUTI7TZ9D-cgAn0hvmw0Z43g9lBtlOxUD2Fd2EggWffEMzdOeaYrtRtkSWMZS4nP0ao3SNdYXUPwB9a-zDSQ&seq=1, p. 459 [accessed: 24 I 2025].

¹² M. Kijewska, *Lewicowy terroryzm...*, p. 206.

¹³ *Koledzy z Al-Kaidy skazani w Belgii* (Eng. Colleagues from Al-Qaeda sentenced in Belgium), TVN24, 10 V 2010, <https://tvn24.pl/swiat/koledzy-z-al-kaidy-skazani-w-belgii-ra133541-ls3584645> [accessed: 25 I 2025]

Terrorism in France therefore has a longer history than in Belgium. France is drawing on this long-standing experience in its preventive measures and strategies relating to security and counter-terrorism. The author of the article believes that, due to the history and statistical data, which place France among the leading countries with the highest number of terrorist attacks¹⁴, terrorism has become an integral part of the country. Belgium has experienced fewer terrorist attacks in its history, but it has demonstrated effectiveness in detecting terrorists and carrying out preventive measures.

The significance of Paris and Brussels in the international politics

Paris and Brussels play a special role in the international arena as well as within European political and cultural system.

The capital of France is associated with republican values such as liberty, equality and fraternity. This is reflected in the French Revolution and the associated Declaration of the Rights of Man and of the Citizen and the Treaty of Versailles. Paris is home to the headquarters of international institutions such as: the International Criminal Police Organization (Interpol), the Organisation for Economic Co-operation and Development (OECD), and the United Nations Educational, Scientific and Cultural Organization (UNESCO). In turn, Brussels serves as one of the most important decision-making centres, given that it is home to the headquarters of the EU and NATO. The linguistic diversity and the presence of numerous international organisations make the Belgian capital a place that lives up to the EU's motto – *United in diversity*¹⁵.

For years, both cities have been targets of particular strategic and symbolic importance to terrorist organisations. Terrorist attacks carried out in these locations were intended not only to cause material and human losses and to instil a sense of insecurity in the public, but also served as a sign of the rejection of European values by terrorist organisations. In addition,

¹⁴ See, e.g.: *Terrorism in EU: facts and figures*, The European Council and the Council of the European Union, <https://www.consilium.europa.eu/en/infographics/terrorism-eu-facts-figures/> [accessed: 25 I 2025].

¹⁵ *EU motto*, European Union, 23 XII 2025, https://european-union.europa.eu/principles-countries-history/symbols/eu-motto_en [accessed: 18 III 2026].

the attacks in Paris and Brussels were intended to maximise media coverage and influence public opinion in Europe and around the world.

The course and causes of the attacks

The Islamic State is an organisation that regards Western countries as unfaithful and immoral in relation to its religion. One of ISIS's objectives is global religious expansion. In the case of attacks in Paris, they were also motivated by a desire for revenge for Operation Chammal¹⁶, which began on 19 September 2014. The Islamic State regarded this as an encroachment on its territory and activities, which contributed to a hostile attitude towards France. Furthermore, the organisation decided it was right to attack a site symbolic of personal freedom and the Western way of life, which is interpreted by Islam as consumerist¹⁷.

Paris (2015)

The first attack in Paris in 2015 was carried out on 7 January at the editorial offices of 'Charlie Hebdo' magazine. This satirical weekly magazine is known for publishing caricatures with political, cultural and religious themes. The last one turned out to be crucial to the case of the attack, as 'Charlie Hebdo' editorial team apublished many times caricatures of Muhammad and ISIS leader Abu Bakr al-Bagdadi, thereby antagonising followers of Islam. This is believed to be the reason for the attack¹⁸. Following numerous provocative actions by the editorial team, the 'Charlie Hebdo' headquarters was set on fire in November 2011.

The attack began with the surprise and intimidation of a female illustrator at the editorial office, who let the terrorists into the building,

¹⁶ Operation Chammal – the French contingent of international operation 'Inherent Resolve', involving 80 countries and 5 international organisations, the aim of which was to enable the Iraqi authorities to ensure their country's security independently. As part of the Chammal, France provided military support to Iraqi forces involved in the fight against ISIS. See: *Opération CHAMMAL*, Ministère des Armées, <https://www.defense.gouv.fr/operations/monde/grand-levant/operation-chammal> [accessed: 10 IV 2025].

¹⁷ V. Romania, S. Tozzo, *Terrorism as ritual process and cultural trauma: A performative analysis of ISIS's attacks in Europe*, "Italian Sociological Review" 2017, vol. 7, no. 2, p. 243. <https://doi.org/10.13136/isr.v7i2.177>.

¹⁸ Abu Bakr al-Bagdadi – founder and leader of a Sunni terrorist organisation, from 2014 until his death in 2019, the self-proclaimed caliph of Islamic State.

whereupon they opened the fire on the employees. During the shooting, she hid under her desk. According to her testimony, the gunfire lasted 5 minutes, and she heard the attackers say: 'We avenged the Prophet' and 'Allah Akbar'¹⁹. The attack left 12 people dead, including the newspaper's editor-in-chief, Stephane Charbonnier 'Charb', who had been blacklisted by Al-Qaeda since 2013. After the attack, the perpetrators attempted to flee, during which they fired at a police car. One of the police officers was killed, which added to the chaos and the scale of the threat. Following the collision, the terrorists abandoned their car, in which the police found documents that enabled them to identify the attackers. They were brothers who had been trained in Yemen by ISIS. Seven members of their family were arrested. Further attacks took place in the following days. During one of these, counter-terrorism officers killed the attackers.

Another series of coordinated attacks carried out by ISIS in Paris took place in November 2015. The key attack took place on 13 November at the Bataclan Theatre, where a concert by the rock band Eagles of Death Metal was being held. Those attending the concert were unaware of the explosion at the Stade de France stadium, where a match between French and German national teams was taking place. At 9.49 p.m., men armed with machine guns approached the theatre doors, shot the doorman and the people standing at the entrance, and entered the building. They took up positions at the back of the auditorium, from where they opened fire on the crowd. The officer who was the first to enter the building shot one of the attackers, who was armed with grenades, causing an explosion that killed a terrorist. The two remaining terrorists took around 20 hostages, who were rescued thanks to a police raid. As a result of the attack in the theatre, 90 people were killed, mostly young people. In total, 130 people were killed as a result of the attacks carried out that day²⁰.

The policemen found the phone of one of the perpetrators' in a rubbish bin. This led them to a hotel room where the men had been staying for

¹⁹ *Najpierw zabijali w redakcji, potem zastrzelili policjanta. Tak przebiegał zamach* (Eng. First they killed people in the newsroom, then they shot a police officer. That's how the attack unfolded), TVN24, 8 I 2015, <https://tvn24.pl/swiat/zamach-na-charlie-hebdo-tak-przebiegal-atak-ra504096-ls3289349> [accessed: 8 IV 2025].

²⁰ A. Chrisafis, 'It looked like a battlefield': the full story of what happened in the Bataclan, *The Guardian*, 20 XI 2015, <https://www.theguardian.com/world/2015/nov/20/bataclan-witnesses-recount-horror-paris-attacks> [accessed: 10 IV 2025].

a week and where they found equipment and medical supplies used to make bombs.

Brussels (2016)

Salah Abdeslam, who had gone into hiding in Molenbeek district of Brussels, was believed to be the main coordinator of the attacks in France. Newspapers reported that (...) *'Molenbeek is a place where it is very easy to disappear'. This is where most of Brussels' dark corners are found – places the police rarely venture into, and where drug gangs and arms dealers rule. (...) It is no coincidence that Molenbeek has become the centre of European jihad*²¹. Following the attacks on 13 November 2015, terrorists were often given shelter in a neighbourhood inhabited mainly by people of North African origin and the Muslim faith. This was also the case with Abdeslam, whose presence contributed to the rise of radicalism in that area. Following his arrest, Abdeslam admitted during questioning that further terrorist attacks had been planned, this time in Belgium. Their aim was to demonstrate the ability of ISIS to carry out attacks despite suffering losses, and to confirm its readiness to continue operations in France and Belgium and across Europe.

Four days after Abdeslam's arrest, on 22 March 2016, there were two suicide terrorist attacks. The first took place at Zaventem Airport, where at around 7.45 a.m., three men arrived by taxi from Molenbeek district. A dozen or so minutes later, in the international departures hall (...) *one of the terrorists detonated the first bomb, which was in his suitcase, while queuing at the check-in counter no. 11. A few seconds later, a second explosion occurred at counter no. 2, and a second terrorist detonated a bomb hidden in his luggage*²². The third man, presumably because the airport evacuation had begun, did not detonate the bomb and fled. Security services located the bag containing the explosive. As a result of the explosions, 20 people were killed. Following the attack, terrorists were identified. Najim Laachraoui and Ibrahim El Bakraoui were killed. The third attacker Mohamed Abrini,

²¹ „Mózg” krwawych zamachów w Paryżu zatrzymany (Eng. ‘The mastermind’ behind the bloody attacks in Paris arrested), Newsweek Polska, 18 III 2016, <https://web.archive.org/web/20160322133717/http://swiat.newsweek.pl/sprawca-krwawych-zamachow-w-paryzu-salah-abdeslam-zatrzymany,artykuly,382261,1.html> [accessed: 10 IV 2025].

²² Belgique – attentats à l'aéroport et dans le métro de Bruxelles, Association française des Victimes du Terrorisme, <https://www.afvt.org/belgique-attentats-a-laeroport-et-dans-le-metro-de-bruxelles/> [accessed: 10 IV 2025].

who was also linked to the attacks in 2015 in Paris, was arrested on 8 April 2016.

At around 9.11 a.m. on the same day, there were two explosions in the underground. According to the Belgian authorities, the perpetrator boarded a train at Molenbeek underground station. The explosion, which was probably triggered by a second bomber, occurred near the EU buildings during the morning rush hour²³. Twelve people died.

A total of 32 people were killed and around 320 were injured in the attacks on 22 March 2016. The following day, ISIS claimed responsibility for the terrorist attacks at the airport and the underground station. The investigation revealed that the same French-Belgian jihadist cell was behind the attacks in France and Belgium²⁴.

The most important social consequences of the attacks in Paris and Brussels

Research into the impact of terrorist attacks on society²⁵ clearly points to negative effects on the mental and physical health of citizens. On this basis, it can be assumed that terrorist attacks in 2015 and 2016 had impact on the people of France and Belgium and increased the demand for psychological support. Researchers emphasise that countries at risk of terrorist attacks should establish and develop psychological support programmes, both in the form of crisis intervention and long-term post-traumatic therapy.

The French authorities, the public and the media all viewed the terrorist attack on 'Charlie Hebdo' not only as an attack on the editorial

²³ *Tactics, Techniques, and Procedures Used in the 22 March 2016 Brussels Attacks*, "Joint Intelligence Bulletin", 12 IV 2016, <https://info.publicintelligence.net/DHS-FBI-NCTC-BrusselsAttacks.pdf>, p. 2 [accessed: 11 IV 2025].

²⁴ Ch. Gracieux, *Les attentats du 22 mars 2016 à Bruxelles*, Lumni Enseignement, 23 III 2016, <https://enseignants.lumni.fr/fiche-media/00000001857/les-attentats-du-22-mars-2016-a-bruxelles.html> [accessed: 11 IV 2025].

²⁵ P. Pirard et al., *Use of mental health supports by civilians exposed to the November 2015 terrorist attacks in Paris*, "BMC Health Services Research" 2020, vol. 20. <https://doi.org/10.1186/s12913-020-05785-3>; R. Deschepper et al., *Association between feeling threatened by a terrorist attack and subjective health: a web survey a week after the attacks of 22 March 2016 in Belgium*, "European Journal of Psychotraumatology" 2018, vol. 9, no. 1. <https://doi.org/10.1080/20008198.2018.1500821>.

team and the people working there, but also as an assault on values such as democracy, freedom of speech and peace. Shortly after the attack, a logo featuring the slogan *Je suis Charlie* (Eng. I am Charlie)²⁶ was created. It quickly went viral online and became a symbol of support and solidarity with the victims. Demonstrations and marches took place in many cities, including the March of the Republic (French: Marche Républicaine) in Paris, which was held to commemorate the victims of the attack and to express opposition to aggression and terrorism itself. *Almost all political, trade union and religious leaders, as well as heads of state and government from abroad*²⁷ (...) took part in the march.

There has also been a rise in racist and Islamophobic attitudes within society, a trend noted not only by the French and Belgian media²⁸. Parties that support a policy of closed borders for immigrants have gained popularity²⁹.

The security services and police forces in both France and Belgium received negative assessment. In Belgium, they were accused of slow response times, a lack of police control and initiative in neighbourhoods, such as Schaerbeek and Molenbeek, considered to be hotbeds of terrorism and radical influence in this country³⁰. In France, the parliamentary select committee tasked with investigating the attacks in 2015 published a report on the intelligence services. It described the attacks as an intelligence failure caused, among other things, by a lack of communication between

²⁶ The author of this visualisation is Joachim Roncin, who was the art director of the *Stylist* magazine at the time.

²⁷ J-B. Garat, *L'impressionnante liste des politiques présents à la marche à Paris*, Le Figaro, 10 I 2015, <https://www.lefigaro.fr/politique/2015/01/10/01002-20150110ARTFIG00160-l-impressionnante-liste-des-politiques-present-a-la-marche-republicaine-a-paris.php> [accessed: 9 IV 2025].

²⁸ C. Lafon, *Attentats de Paris: ces deux semaines qui ont changé la France*, Sud Ouest, 22 I 2015, <https://www.sudouest.fr/redaction/attentats-de-paris-ces-deux-semaines-qui-ont-change-la-france-8022926.php> [accessed: 12 IV 2025]; B. Jastrzębski, *Jastrzębski: Zamachy w Brukseli – to nie koniec świata* (Eng. The attacks in Brussels are not the end of the world), Respublica, 22 III 2016, <https://respublica.pl/teksty/jastrzebski-zamachy-w-brukseli-to-nie-koniec-swiata-56188.html>, [accessed: 12 IV 2025].

²⁹ A. Chrisafis, *Marine Le Pen's Front National makes political gains after Paris attacks*, The Guardian, 1 XII 2015, <https://www.theguardian.com/world/2015/dec/01/marine-le-pen-front-national-political-gains-paris-attacks> [accessed: 12 VI 2026].

³⁰ Ibid.; M. Hallam, *Belgian shortcomings in focus*, DW, 30 III 2016, <https://www.dw.com/en/the-shortcomings-of-belgiums-brussels-terror-investigations/a-19151338> [accessed: 12 VI 2026].

intelligence services³¹. The committee recommended a reorganisation modelled on the US National Counterterrorism Center (NCTC) established in the USA following the attacks of 11 September 2001.

An overview of the main security institutions and services combating terrorism in France and Belgium

The experiences of 2015 and 2016 led to a reorganisation and efforts to strengthen national counter-terrorism capabilities in France and Belgium.

In France, the key institutions responsible for combating terrorism are:

- 1) The General Directorate for Internal Security (French: Direction Générale de la Sécurité Intérieure, DGSI) – comprises, among other things, a thematic department dealing with various forms of terrorism, analysis department, targeted at regions and countries, as well as divisions focusing on the armed forces and counter-intelligence. Since 2018, the DGSI has served as the most important institution responsible for counter-terrorism prevention in France;
- 2) The Directorate General for External Security (French: Direction Générale de la Sécurité Extérieure, DGSE) – French intelligence, which, in the context of terrorism, focuses on identifying terrorist groups, their organisational structures and recruitment channels, as well as on thwarting attacks planned abroad³²;
- 3) The Directorate General of National Police (French: Direction Generale de la Police Nationale, DGPN) – carries out essential tasks to maintain order and security throughout the country. Thanks to its powers, it prevents terrorist attacks;

³¹ A. Kacprzak, *Komisja śledcza francuskiego parlamentu: Wywiad poniósł porażkę, nie zapobiegł atakom. Należy utworzyć agencję do walki z terroryzmem* (Eng. French parliamentary inquiry committee: The intelligence services failed – they did not prevent the attacks. An agency to combat terrorism should be established), wPolityce, 5 VII 2016, <https://wpolityce.pl/swiat/299492-komisja-sledcza-francuskiego-parlamentu-wywiad-poniosl-porazke-nie-zapobieg-l-atak-om-nalez-y-utworzyc-agencje-do-walki-z-terroryzmem?strona=1> [accessed: 12 IV 2025].

³² *Nos missions*, Direction Générale de la Sécurité Extérieure, <https://www.dgse.gouv.fr/fr/nous-connaître/nos-missions> [accessed: 30 IV 2025].

- 4) The National Anti-terror Prosecutor's Office (French: Le parquet national anti-terroriste, PNAT) – it is not a special service, but since 2019 it has played a key role in the fight against terrorism. It was established to improve response capacity to terrorist attacks.

In Belgium, the following bodies are responsible for counter-terrorism:

- 1) The State Security Service (Dutch: Veiligheid van de Staat, VSSE) – the Belgian civil intelligence and security service. It was established in 1830 and is the oldest intelligence service in the world³³. It is responsible for intelligence, investigation and security check. The VSSE can be compared to the French DGSi;
- 2) The Coordination Unit for Threat Analysis (Dutch: Orgaan voor de Coördinatie en de Analyse van de Dreiging, OCAD; French: Organe de Coordination pour l'Analyse de la Menace, OCAM), whose remit includes, among other things, creating a database used by the police, intelligence and judicial authorities, implementing the *Strategy for combating extremism and terrorism* (French: La Stratégie Extrémisme et Terrorisme, T.E.R.)³⁴ and international cooperation in the fight against terrorism;
- 3) The Federal Police – combat crime, maintain public order and ensure security at national level;
- 4) The General Intelligence and Security Service (Dutch: Algemene Dienst Inlichting en Veiligheid, ADIV; French: Service Général du Renseignement et de la Sécurité, SGRS) – monitors information and activities originating from abroad that may pose a threat to Belgium's security³⁵.

In the context of the issue under discussion, both countries have a structure that combines intelligence, police, judicial and analytical activities. Thanks to such a well-developed organisation, it is possible to identify and respond to threats quickly. The clear similarities help to maintain international security. Relations between France and Belgium regarding preventive measures are based on the structural integration of services and cooperation on intelligence matters.

³³ *Qui sommes-nous?*, Veiligheid van de Staat, <https://www.vsse.be/fr/qui-sommes-nous/historique> [accessed: 1 V 2025].

³⁴ *La Stratégie Extrémisme et Terrorisme (Stratégie T.E.R.)*, OCAM, <https://ocam.belgium.be/la-strategie-extremisme-et-terrorisme-strategie-t-e-r/> [accessed: 12 IV 2025].

³⁵ *Nos missions*, SGRS, <https://www.sgrs.be/nous-connaître/nos-missions/> [accessed: 1 V 2025].

Preventive strategies regarding radicalisation

The growth and strengthening of radical movements increase the likelihood of terrorist acts. To counter these trends, France and Belgium have focused on social, educational and digital prevention.

In France, following the attacks in 2015 and 2016, measures under the Plan Vigipirate³⁶ were expanded and the Sentinelle military operation was launched, involving the deployment of soldiers in public spaces to protect key facilities and support police operations. French authorities have also expanded the powers of counter-terrorism agencies, stepped up surveillance of individuals suspected of extremism, and introduced measures to counter radicalisation, including in schools, prisons and online. On 30 October 2017, French government introduced the Act on strengthening internal security and the fight against terrorism³⁷. At the same time, work was underway on an action plan to combat radicalism and terrorism (abbreviated to PART), which was announced in 2018. PART identifies five main themes around which 60 measures to refocus preventive policy are centred:

- 1) strengthening society's resilience to radicalisation,
- 2) expanding the network for detecting and preventing radicalisation,
- 3) better understanding and preparing for developments in radicalisation,
- 4) professionalising local stakeholders and assessing employed practices,
- 5) tailoring measures to counter radicalisation³⁸.

In 2026, a new crime prevention strategy for the period 2026–2030 was published (*Stratégie nationale de prévention de la délinquance 2026–2030: Prévenir pour protéger*, SNPD), which sets out three main areas of action:

- 1) adapting responses to new forms of crime, namely by strengthening initiatives in the areas of awareness-raising, training

³⁶ The Plan Vigipirate is the French government's system for the prevention of terrorism, security and response. See: *The Plan Vigipirate*, République Française, <https://www.campusfrance.org/en/security> [accessed: 26 V 2026].

³⁷ LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035932811> [accessed: 10 VI 2026].

³⁸ *Prévenir Pour Protéger». Plan national de prévention de la radicalisation*, <https://www.cipdr.gouv.fr/wp-content/uploads/2018/11/DP2018-02-23-CIPDR-Radicalisation-V5.pdf>, p. 5 [accessed: 10 VI 2026].

- and support, while consolidating the proactive capabilities of stakeholders;
- 2) ensuring the continuity of preventive measures from childhood to adulthood, namely by supporting parenting, developing psychosocial skills, better identifying situations of risk, and promoting youth engagement in order to prevent crime;
 - 3) better coordination and support for stakeholders by strengthening local governance and establishing a digital prevention academy to compile resources, disseminate best practices and train specialists³⁹.

France has also a regional programme for the prevention of violent radicalisation⁴⁰, which involves providing support to people who have been radicalised or are at risk of radicalisation, and preventing the risk of such people becoming violent. The programme was established in 2014, but in 2018 it was updated by Les groupes d'évaluation départementaux, which are responsible for analysing the risks associated with radicalisation and coordinating the programme.

In Belgium, the key strategy for combating radicalisation was the so-called Plan R⁴¹, which was replaced by the T.E.R. Strategy⁴² on 8 September 2021. Educational institutions such as GO! Education of Flemish Community (GO! – onderwijs van de Vlaamse Gemeenschap) and the Royal Athenaeum Antwerp have also become involved in the fight against radicalisation. These organisations worked out together the prevention pyramid of Johan Declerck (Figure 1). This is a training programme for various institutions, which has been adopted not only by the Belgian government, but also by the European Commission.

³⁹ *Stratégie nationale de prévention de la délinquance 2026–2030: Prévenir pour protéger*, CIPDR, 24 VI 2026, <https://www.cipdr.gouv.fr/strategie-nationale-de-prevention-de-la-delinquance-2026-2030-prevenir-pour-protger/> [accessed: 12 V 2026].

⁴⁰ *Dispositif territorial de prévention de la radicalisation violente*, Direction Générale de la Sécurité Intérieure, 14 VI 2021, <https://www.dgsi.interieur.gouv.fr/dispositif-territorial-de-prevention-de-radicalisation-violente> [accessed: 11 VI 2026].

⁴¹ See: *Le Plan R. Le Plan d'Action Radicalisme*, https://ocam.belgium.be/wp-content/uploads/2020/11/brochure_radicalisme_fr.pdf [accessed: 10 VI 2026].

⁴² *La Stratégie Extrémisme et Terrorisme (Stratégie T.E.R.)...*

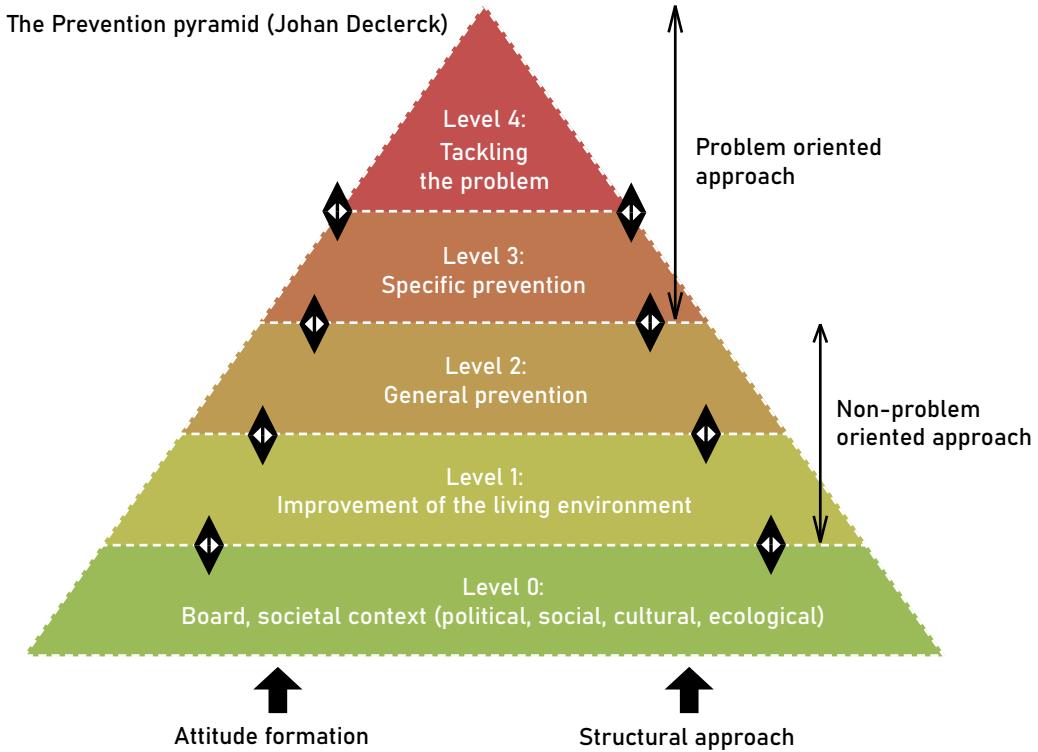


Figure 1. The Prevention pyramid of Johan Declerck.

Source: own elaboration based on: *The Prevention Pyramid*, European Commission, 2 VII 2024, https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/prevention-pyramid_en [accessed: 4 V 2025 r.]. Changes were made to the graphic design (editor's note).

The pyramid (...) is an instrument that can be used to orient and achieve insights into how to optimise one's policy for the prevention of radicalisation⁴³. It was divided into five levels, the first three of which are described as non-problem-oriented:

- level 0 – social environment,
- level 1 – living conditions and ways of improving them,
- level 2 – general prevention,
- level 3 – specific prevention,
- level 4 – tackling the problem.

⁴³ *The Prevention Pyramid*, European Commission, 2 VII 2024, https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/prevention-pyramid_en [accessed: 4 V 2025 r.].

The pyramid of Declerck was created in 2001, but following the attacks in 2015 and 2016, the authors updated it. At that time, some circles felt that the focus should be on level 4 (a problem-oriented approach)⁴⁴. The project is being implemented across Europe.

In line with the T.E.R. Strategy, the Local Task Forces (French: Les Taskforces locales, TFL) and the Local Integral Security Cells dealing with issues relating to radicalism, extremism and terrorism began to be formed in Belgium⁴⁵. TFL connect the police, security and intelligence services, the migration office and the prosecutor's office. Their work focuses on operational level (collecting information, monitoring and assessing risks) as well as strategic level (ensuring strategic consistency between TFL members).

International cooperation in the fight against terrorism

Following the experiences with attacks, France and Belgium have concluded that effectively combating this threat involves not only securing the country, but also extending efforts beyond its borders. They have therefore stepped up their cooperation on intelligence and operational matters, and have extended this to the global level.

The Prime Minister of Belgium, Charles Michel and the Prime Minister of France, Manuel Valls met in Brussels on 1 February 2016⁴⁶. Due to the cooperation between the Belgian authorities and their partners in Germany, France and Luxembourg, a terrorist attack in France planned for 1 July 2018 was foiled⁴⁷.

The European Union has created institutions that focus on the security of European countries. The ECTC⁴⁸, established by Europol, is responsible for exchanging information, data and adapting operational support

⁴⁴ Ibid, p. 1.

⁴⁵ *La Strategie Extremisme et Terrorisme (Strategie T.E.R.)...*

⁴⁶ *France, Belgium to step up counter-terrorism cooperation in wake of Paris attacks*, France 24, 2 II 2016, <https://www.france24.com/en/20160202-france-belgium-step-counter-terrorism-cooperation-paris-attacks> [accessed: 10 V 2025].

⁴⁷ EUROJUST, *The ARGO Case – Diplomatic immunity in a cross-border terrorism case*, <https://www.eurojust.europa.eu/sites/default/files/assets/argo-case-28-06-2024-pdf-v2.pdf>, p. 3. [accessed: 10 V 2025],

⁴⁸ *European Counter Terrorism Centre – ECTC*, Europol, <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> [accessed: 10 V 2025].

for police, intelligence and special services of Member States, and also analyses the broad context of terrorist threats in order to identify new directions of investigation. This cooperation allows for quick response and action against terrorism.

Since 2006, Europol has been publishing annual reports on the situation and trends in the field of terrorism in the EU⁴⁹.

The European Union introduced also the systems supporting counter-terrorism and the control of external and internal borders:

- 1) Schengen Information System (SIS) – assists border and migration services in protecting and controlling the EU's internal borders⁵⁰;
- 2) The European Criminal Records Information Exchange System (ECRIS) – a decentralised IT system based on national criminal records databases⁵¹;
- 3) Passenger Name Record (PNR) – a system that stores the personal data of air passengers⁵²;
- 4) Entry-Exit System (EES) – a system introduced on 10 April 2026, enabling the recording of every instance in which citizens of non-EU countries cross the external borders of the 29 European countries while entering the EU for a short stay⁵³.

The UN began its counter-terrorism activities in the 1990s. At that time, the Security Council imposed sanctions on countries accused of supporting and having links to terrorism, such as Libya (1992) and Sudan (1996). In 1999, the Council adopted the Resolution 1269 in which it expressed concern at (...) *the increase in acts of international terrorism*

⁴⁹ See, e.g.: *EU Terrorism Situation & Trend Report (EU TE-SAT)*, Europol, <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> [accessed: 11 VI 2026].

⁵⁰ Schengen Information System, European Commission, https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_en [accessed: 10 V 2025].

⁵¹ *Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA; Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA.*

⁵² *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.*

⁵³ *Entry-Exit System*, Straż Graniczna, 9 IV 2026, <https://www.strazgraniczna.pl/pl/ees/entry-exit-system-pl/13677,System-wjazduwyjazd-EES.html> [accessed: 12 V 2026].

which endangers the lives and well-being of individuals worldwide as well as the peace and security of all States⁵⁴. The current UN document on terrorism is the *United Nations Global Counter-Terrorism Strategy*, which came into force on 8 September 2006, together with the attached Action Plan⁵⁵.

Within the UN, there is the Office of Counter-Terrorism⁵⁶ tasked with assisting the Member States in implementing strategy. The Office manages a total of 17 programmes and projects addressing various issues concerning terrorism, such as CBRN terrorism or the victims of terrorism. It organises events and conferences on combating acts of violence, e.g. the Week to Combat Terrorism, which is held every two years⁵⁷.

NATO, an organisation focused on military matters, also runs counter-terrorism programmes. NATO invoked Article 5 of the North Atlantic Treaty⁵⁸ on collective defence of Member States only once, when the US suffered a terrorist attack by Al-Qaeda on 11 September 2001. NATO's counter-terrorism policy is based on three principles⁵⁹:

- 1) awareness – it involves consultations, the exchange of intelligence information, strategic analyses and situation assessments. In 2023, the position of Special Coordinator for Counter-Terrorism was created,
- 2) capabilities and preparedness – development and work on innovative technologies, which will be a response to terrorist threats in all forms,
- 3) engagement and cooperation between NATO Member States and international partners to strengthen global security, with an emphasis on counter-terrorism activities.

⁵⁴ *Resolution 1269 (1999) / adopted by the Security Council at its 4053rd meeting, on 19 October 1999, S/RES/1269(1999)*, https://digitallibrary.un.org/record/287509?v=pdf#files_p.1, [accessed: 10 VI 2026].

⁵⁵ *The United Nations Global Counter-Terrorism Strategy*, UN Action Counterterrorism, <https://www.unic.un.org.pl/terroryzm/strategia.php> [accessed: 10 V 2025].

⁵⁶ United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en> [accessed: 10 V 2025].

⁵⁷ The next edition of this event took place between 26 June and 2 July 2026. See: *2026 Counter-Terrorism Week*, United Nations, <https://www.un.org/counterterrorism/en/2026-counter-terrorism-week> [accessed: 12 VI 2026].

⁵⁸ *The North Atlantic Treaty*, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty> [accessed: 12 VI 2026].

⁵⁹ *Countering terrorism*, NATO, 31 III 2026, <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism> [accessed: 12 V 2026].

NATO also organised military operations, such as Active Endeavour in the Mediterranean Sea, which was a response to the attack of 11 September 2001 on the World Trade Center⁶⁰ or Sea Guardian, which replaced Active Endeavour in 2016 and focused on maritime security⁶¹.

NATO cooperates with the UN, the EU, the Global-Counter Terrorism Forum, Interpol and the OSCE (...) *to ensure that views and information are shared and that appropriate action can be taken more effectively in the fight against terrorism*⁶². Partnerships serve to facilitate the exchange of information, coordinate joint or separate operations, as well as align and harmonise legal standards relating to security.

Summary

The history of terrorism in France is longer than in Belgium. In the 21st century, Al-Qaeda and the Islamic State have influenced the nature of modern terrorism, which can be described as globalised, more radical in religious terms, and more difficult to predict.

The author focused on an analysis of the attacks on two European capital cities. Paris, as a city symbolising democratic values, and Brussels, as the centre of the EU, were deemed by terrorists to be the most suitable targets to launch an attack, given the opportunity they offered to demonstrate the negation of Western values. Attacks in France and Belgium have highlighted weaknesses in their security systems, with a particular focus on coordination and communication between services, as well as the scale of the problem of radicalisation in the EU countries. The socio-political consequences of these attacks had far-reaching effects. One of these was the strengthening of international cooperation in the context of countering terrorism and combating this phenomenon. Furthermore, European states focused on security, including the need to tighten anti-terrorism legislation, preventative measures, as well as the coordination of activities and expansion of the powers of specialist agencies. An

⁶⁰ *Operation Active Endeavour (2001–2016)*, NATO, [https://www.nato.int/en/what-we-do/operations-and-missions/operation-active-endeavour-2001-2016?selectedLocale=\[accessed: 12 V 2025\]](https://www.nato.int/en/what-we-do/operations-and-missions/operation-active-endeavour-2001-2016?selectedLocale=[accessed: 12 V 2025]).

⁶¹ *Operation Sea Guardian*, NATO, 26 V 2023, [https://www.nato.int/cps/en/natohq/topics_136233.htm? \[accessed: 10 V 2025\]](https://www.nato.int/cps/en/natohq/topics_136233.htm? [accessed: 10 V 2025]).

⁶² *Countering terrorism...*

international debate on the balance between security and freedom has also begun. On the other hand, the attacks have had an impact on society – in terms of e.g. political views – and have contributed to increased support for right-wing political parties in both countries.

The article confirms that the contemporary terrorism is strongly linked to processes of radicalisation and issues of social integration. Both France and Belgium, due to their location, colonial history and political significance in Europe, have become particularly vulnerable to the activities of Islamist groups linked to Al-Qaeda and ISIS. Experiences of these countries show that an effective fight against terrorism cannot rely solely on military and repressive measures, but also requires long-term social, educational and political initiatives aimed at countering radicalisation and strengthening social cohesion.

On the basis of the analysis carried out, the author identified the main determinants of the security policy of France and Belgium, which, according to the hypothesis, are:

- 1) terrorist organisations, such as Al-Qaeda and ISIS, which reject the values promoted by European capitals and focus their attention on France and Belgium partly because of colonial traditions,
- 2) Islamic radicalisation in France and Belgium,
- 3) close international cooperation as a necessity for maintaining national security.

The consequences of the attacks require swift political and legislative responses, as well as changes to the structure, communication and operational effectiveness of the services responsible for security.

Terrorist attacks described in the article have led to profound changes in the security of France and Belgium. Furthermore, they have mobilised the international community to take joint action on preventive measures in the fight against terrorism.

It should be emphasised that the global terrorism adapts to reality and evolves in response to challenges such as advancing technologies, socio-political issues, migration, etc. The security policies of France and Belgium (and others) should be flexible, cohesive and focused on shared values. These characteristics will depend on the approach taken by states to the fight against terrorism, which relies not only on the effectiveness of counter-terrorism services, but also on cooperation between state institutions, building public trust, mobilising social and educational institutions, countering radicalisation, and building the resilience of democratic states.

Bibliography

Deschepper R., Six S., Gidron Y., Depoorter A.-M., Vandekerckhove M., Gheysens N., Overmeire R.V., Bilsen J., *Association between feeling threatened by a terrorist attack and subjective health: a web survey a week after the attacks of 22 March 2016 in Belgium*, "European Journal of Psychotraumatology" 2018, vol. 9, no. 1. <https://doi.org/10.1080/20008198.2018.1500821>.

Kijewska M., *Lewicowy terroryzm w Europie Zachodniej w drugiej połowie XX i na początku XXI wieku. Podstawowe informacje i kierunki rozwoju* (Eng. Leftist terrorism in Western Europe in the second half of the 20th century and the beginning of the 21st century. Basic information and directions of development), "Radzyński Rocznik Humanistyczny" 2018, vol. 16, no. 1, [accessed: 23 I 2025].

Pirard P., Baubet T., Motreff Y., Rabet G., Marillier M., Vandentorren S., Vuillermoz C., Stene L.E., Messiah A., *Use of mental health supports by civilians exposed to the November 2015 terrorist attacks in Paris*, "BMC Health Services Research" 2020, vol. 20. <https://doi.org/10.1186/s12913-020-05785-3>.

Romania V., Tozzo S., *Terrorism as ritual process and cultural trauma: A performative analysis of ISIS's attacks in Europe*, "Italian Sociological Review" 2017, vol. 7, no. 2, pp. 239–261. <https://doi.org/10.13136/isr.v7i2.177>.

Internet sources

2026 Counter-Terrorism Week, United Nations, <https://www.un.org/counterterrorism/en/2026-counter-terrorism-week> [accessed: 12 VI 2026].

27 lat temu doszło do zamachu bombowego w paryskim metrze (Eng. There was a bomb attack on the Paris Metro 27 years ago), iFrancja, 25 VII 2025, <https://www.ifrancja.fr/27-lat-temu-doszlo-do-zamachu-bombowego-w-paryskim-metrze/> [accessed: 23 I 2025].

Belgique – attentats à l'aéroport et dans le métro de Bruxelles, Association française des Victimes du Terrorisme, <https://www.afvt.org/belgique-attentats-a-laeroport-et-dans-le-metro-de-bruxelles/> [accessed: 10 IV 2025].

Chrisafis A., *Marine Le Pen's Front National makes political gains after Paris attacks*, The Guardian, 1 XII 2015, <https://www.theguardian.com/world/2015/dec/01/marine-le-pen-front-national-political-gains-paris-attacks> [accessed: 12 VI 2026].

Countering terrorism, NATO, 31 III 2026, <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism> [accessed: 12 V 2026].

Counter-terrorism and radicalisation, European Commission, 26 II 2026, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation_en [accessed: 30 III 2026].

Dispositif territorial de prévention de la radicalisation violente, Direction Générale de la Sécurité Intérieure, 14 VI 2021, <https://www.dgsi.interieur.gouv.fr/dispositif-territorial-de-prevention-de-radicalisation-violente> [accessed: 11 VI 2026].

Entry-Exit System, Straż Graniczna, 9 IV 2026, <https://www.strazgraniczna.pl/pl/ees/entry-exit-system-pl/13677,System-wjazduwyjazd-EES.html> [accessed: 12 V 2026].

EU motto, European Union, 23 XII 2025, https://european-union.europa.eu/principles-countries-history/symbols/eu-motto_en [accessed: 18 III 2026].

EU Security Union Strategy: connecting the dots in a new security ecosystem, European Commission – Press release, Brussels, 24 VII 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379 [accessed: 12 VI 2026].

EU Terrorism Situation & Trend Report (EU TE-SAT), Europol, <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> [accessed: 11 VI 2026].

EUROJUST, The ARGO Case, Diplomatic immunity in a cross-border terrorism case, <https://www.eurojust.europa.eu/sites/default/files/assets/argo-case-28-06-2024-pdf-v2.pdf> [accessed: 10 V 2025].

European Counter Terrorism Centre – ECTC, Europol, <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> [accessed: 10 V 2025].

France, Belgium to step up counter-terrorism cooperation in wake of Paris attacks, France 24, 2 II 2016, <https://www.france24.com/en/20160202-france-belgium-step-counter-terrorism-cooperation-paris-attacks> [accessed: 10 V 2025].

Francq B., *Les Cellules communistes combattantes: les deux figures d'une inversion*, "Sociologie du Travail" 1986, vol. 28, no. 4, https://www.jstor.org/stable/43149431?casa_token=uvu0DUMHhm8AAAAA%3AyTH0OxhPSaWldOexG8URrz6nNtuZ-bUTI7TZ9D-cgAn0hvmw0Z43g9lBtlOxUD2Fd2EggWffEMzdOeaYrtRtkSWMZS4n-P0ao3SNdYXUPwB9a-zDSQ&seq=1 [accessed: 24 I 2025].

Garat J-B., *L'impressionnante liste des politiques présents à la marche à Paris*, Le Figaro, 10 I 2015, <https://www.lefigaro.fr/politique/2015/01/10/01002-20150110ARTFIG00160-l-impressionnante-liste-des-politiques-presents-a-la-marche-republicaine-a-paris.php> [accessed: 9 IV 2025].

Globalna Strategia Zwalczania Terroryzmu (Eng. Global counter-terrorism strategy), UN Action Counterterrorism, <https://www.unic.un.org.pl/terroryzm/strategia.php> [accessed: 10 V 2025].

Gracieux Ch., *Les attentats du 22 mars 2016 à Bruxelles*, Lumni Enseignement, 23 III 2016, <https://enseignants.lumni.fr/fiche-media/00000001857/les-attentats-du-22-mars-2016-a-bruxelles.html> [accessed: 11 IV 2025].

Hallam M., *Belgian shortcomings in focus*, DW, 30 III 2016, <https://www.dw.com/en/the-shortcomings-of-belgiums-brussels-terror-investigations/a-19151338> [accessed: 12 VI 2026].

Jastrzębski B., *Jastrzębski: Zamachy w Brukseli – to nie koniec świata* (Eng. The attacks in Brussels are not the end of the world), Respublica, 22 III 2016, <https://respublica.pl/teksty/jastrzebski-zamachy-w-brukseli-to-nie-koniec-swiata-56188.html> [accessed: 12 IV 2025].

Kacprzak A., *Komisja śledcza francuskiego parlamentu: Wywiad poniósł porażkę, nie zapobiegł atakom. Należy utworzyć agencję do walki z terroryzmem* (Eng. French parliamentary inquiry committee: The intelligence services failed – they did not prevent the attacks. An agency to combat terrorism should be established), wPolityce, 5 VII 2016, <https://wpolityce.pl/swiat/299492-komisja-sledcza-francuskiego-parlamentu-wywiad-poniosl-porazke-nie-zapobieg-l-atak-om-nalezy-utworzyc-agencje-do-walki-z-terroryzmem?strona=1> [accessed: 12 IV 2025].

Kerherve A., O.A.S, Gaullisme.fr, 30 VII 2011, <http://www.gaullisme.fr/2011/07/30/o-a-s/> [accessed: 11 VI 2026].

Koledzy z Al-Kaidy skazani w Belgii (Eng. Colleagues from Al-Qaeda sentenced in Belgium), TVN24, 10 V 2010, <https://tvn24.pl/swiat/koledzy-z-al-kaidy-skazani-w-belgii-ra133541-ls3584645> [accessed: 25 I 2025]

La Stratégie Extrémisme et Terrorisme (Stratégie T.E.R.), OCAM, <https://ocam.belgium.be/la-strategie-extremisme-et-terrorisme-strategie-t-e-r/> [accessed: 12 IV 2025].

Lafon C., *Attentats de Paris : ces deux semaines qui ont changé la France*, Sud Ouest, 22 I 2015, <https://www.sudouest.fr/redaction/attentats-de-paris-ces-deux-semaines-qui-ont-change-la-france-8022926.php> [accessed: 12 IV 2025].

Le Plan R. Le Plan d'Action Radicalisme, https://ocam.belgium.be/wp-content/uploads/2020/11/brochure_radicalisme_fr.pdf [accessed: 12 VI 2026]

Macuga Ł., *Wojna algierska, 1954–1962* (Eng. The Algerian war, 1954–1962), master's thesis, Uniwersytet Mikołaja Kopernika, Toruń 2004, https://www.researchgate.net/publication/303636471_Wojna_algierska_1954_-_1962 [accessed: 22 II 2025].

„Mózg” krwawych zamachów w Paryżu zatrzymany (Eng. ‘The mastermind’ behind the bloody attacks in Paris arrested), *Newsweek Polska*, 18 III 2016, <https://web.archive.org/web/20160322133717/http://swiat.newsweek.pl/sprawca-krwawych-zamachow-w-paryzu-salah-abdeslam-zatrzymany,artykuly,382261,1.html> [accessed: 10 IV 2025].

Nadaux M., *La Troisième République. La «propagande par le fait»: les attentats anarchistes (1892–1894). Explosion d’une bombe à la Chambre des députés déposée par l’anarchiste Auguste Vaillant le 9 décembre 1893, Le XIX^e siècle*, <https://web.archive.org/web/20061125095024/http://www.19e.org/documents/troisiemerepublique/anaratentats/vaillant.htm> [accessed: 21 I 2025].

Najpierw zabijali w redakcji, potem zastrzelili policjanta. Tak przebiegał zamach (Eng. First they killed people in the newsroom, then they shot a police officer. That's how the attack unfolded), *TVN24*, 8 I 2015, <https://tvn24.pl/swiat/zamach-na-charlie-hebdo-tak-przebiegal-atak-ra504096-ls3289349> [accessed: 8 IV 2025].

National Liberation Front, Britannica, <https://www.britannica.com/topic/National-Liberation-Front-political-party-Algeria> [accessed: 22 I 2025].

Nos missions, Direction Générale de la Sécurité Extérieure, <https://www.dgse.gouv.fr/fr/nous-connaître/nos-missions> [accessed: 30 IV 2025].

Nos missions, SGRS, <https://www.sgrs.be/nous-connaître/nos-missions/> [accessed: 1 VI 2025].

Operation Active Endeavour (2001–2016), NATO, <https://www.nato.int/en/what-we-do/operations-and-missions/operation-active-endeavour-2001-2016?selectedLocale=> [accessed: 12 VI 2026].

Opération CHAMMAL, Ministère des Armées, <https://www.defense.gouv.fr/operations/proche-moyen-orient/operations-militaires-au-proche-moyen-orient/operation-chammal> [accessed: 10 IV 2025].

Operation Sea Guardian, NATO, 26 V 2023, https://www.nato.int/cps/en/natohq/topics_136233.htm? [accessed: 10 V 2025].

«Prévenir Pour Protéger». *Plan national de prévention de la radicalisation*, 23 II 2018, <https://www.cipdr.gouv.fr/wp-content/uploads/2018/11/DP2018-02-23-CIPDR-Radicalisation-V5.pdf> [accessed: 11 VI 2026].

Qui sommes-nous?, Veiligheid van de Staat, <https://www.vsse.be/fr/qui-sommes-nous/historique> [accessed: 1 V 2025].

Schengen Information System, European Commission, https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_en [accessed: 10 V 2025].

Stańko K., *Największy proces karny w historii Francji. Dziś wyrok w sprawie ataków terrorystycznych z 2015 roku* (Eng. The largest criminal trial in the history of France. Today, the verdict in the case of the 2015 terrorist attacks), Polska Agencja Prasowa, 29 VI 2022, <https://www.pap.pl/aktualnosci/news%2C1270741%2Cfrancja-byl-najwiekszy-proces-karny-w-historii-dzis-wyrok-w-sprawie-atakow#:~:text=13%20listopada%202015> [accessed: 10 VI 2026].

Stratégie nationale de prévention de la délinquance 2026–2030: Prévenir pour protéger, CIPDR, 24 VI 2026, <https://www.cipdr.gouv.fr/strategie-nationale-de-prevention-de-la-delinquance-2026-2030-prevenir-pour-proteger/> [accessed: 12 V 2026].

Tactics, Techniques, and Procedures Used in the 22 March 2016 Brussels Attacks, “Joint Intelligence Bulletin”, 12 IV 2016, <https://info.publicintelligence.net/DHS-FBI-NCTC-BrusselsAttacks.pdf> [accessed: 11 IV 2025].

Terrorism in EU: facts and figures, The European Council and the Council of the European Union, <https://www.consilium.europa.eu/en/infographics/terrorism-eu-facts-figures/> [accessed: 25 I 2025].

The Plan Vigipirate, Republique Francaise, <https://www.campusfrance.org/en/security> [accessed: 26 V 2026].

The Prevention Pyramid, European Commission, 2 VII 2024, https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/prevention-pyramid_en [accessed: 4 V 2025].

United Nations Office of Counter-Terrorism, <https://www.un.org/counterterrorism/en> [accessed: 10 V 2025].

Legal acts

Resolution 1269 (1999) / adopted by the Security Council at its 4053rd meeting, on 19 October 1999, S/RES/1269(1999), <https://digitallibrary.un.org/record/287509?v=pdf#files> [accessed: 11 VI 2026].

The North Atlantic Treaty, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty> [accessed: 12 VI 2026].

Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (Official Journal of the EU L 93/33 of 7 IV 2009).

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (Official Journal of the EU L 119/132 z 4 V 2016).

Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA (Official Journal of the EU L 151/143 of 7 VI 2019).

LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035932811> [accessed: 13 VI 2026].

Nicole Szostak

Graduate of international security and diplomacy at the War Studies University and political studies at Sciences Po Rennes. Her main research interests include counter-terrorism operations, intelligence and counter-intelligence, as well as geopolitical analysis.

Contact: nicoleszostak1@gmail.com

REVIEW ARTICLES /
REVIEWS

Tomasz Wróblewski, Rola Sztucznej inteligencji w zapobieganiu atakom terrorystycznym¹

Tomasz Michalak

IDEAS Research Institute,
Faculty of Mathematics, Informatics and Mechanics,
University of Warsaw

 <https://orcid.org/0000-0002-5288-0324>



In the third decade of the 21st century, developments in the field of artificial intelligence (AI) have accelerated at an unprecedented rate, a phenomenon referred to as the AI revolution. In an economic context, this technology forms the foundation of the Fourth Industrial Revolution due to its ability to optimise manufacturing processes. Nevertheless, the potential impact of AI on society is multifaceted and goes far beyond the purely industrial sphere. It encompasses both fundamental changes in the way we interact with information and with one another, as well as

¹ T. Wróblewski, *Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym* (Eng. The role of artificial intelligence in preventing terrorist attacks), Warszawa 2025, Difin, 178 p. The book is available only in Polish.

a profound transformation of the labour market, where the automation of routine tasks is forcing a redefinition of human skills. All of this means that AI brings not only benefits but also many challenges. For example, the implementation of smart systems in medicine, education and public administration offers an opportunity to significantly increase the efficiency and personalisation of services, but at the same time raises critical questions about privacy, algorithmic ethics and accountability for decisions made autonomously by computer systems.

The multifaceted nature of AI's impact on reality is reflected in the realm of national security, as we are witnessing a revolution in the military. The ongoing war in Ukraine has become both a driving force and a testing ground for algorithmic warfare, in which superiority is determined not only by human resources and heavy equipment but also by the ability to rapidly fuse and analyse data from drones, military satellites and other available sources, including open-source ones. The analysis of massive datasets is one of the most important applications of AI algorithms, which are capable of performing advanced inference and identifying correlations and relationships of such high complexity that they are practically impossible for a human to identify. On the battlefield, shortening the decision-making cycle to near real time makes AI a key force multiplier. Furthermore, it should be emphasised that the development of AI not only pertains to the field of software but is also a main catalyst for the advancement of autonomy in weapons systems and robotics. All these trends define the battlefield in Ukraine, it can therefore be concluded that AI plays a very significant role in the ongoing processes of reshaping the global geopolitical architecture.

Technological progress based on AI extends beyond the military sphere. It also has an impact on internal security, ranging from crime prevention to counter-intelligence, counter-terrorism, and hybrid threat mitigation. In all these areas, AI algorithms are used for merging and analysing large datasets, as well as for extracting knowledge from information noise and drawing conclusions based on that knowledge. The development of autonomous systems and robotics is also extremely important in the context of internal security, as these technologies can greatly expand the capabilities of security services. Of course, we must also consider the other side of the coin – AI technologies and developments related to AI can be extremely dangerous in the hands of terrorists.

The potential of artificial intelligence in combating terrorism was highlighted in the publication of Tomasz Wróblewski entitled *Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym* (Eng. The role of artificial intelligence in preventing terrorist attacks), which was published in 2025 by Difin Publishing and runs 178 pages. Before proceeding with a substantive analysis of this publication, it is necessary to provide a brief overview of the author in order to avoid the misconceptions that are common in the public sphere. The author of the reviewed publication, Tomasz Wróblewski, PhD – a researcher and academic with extensive expertise in the field of defence and internal security – should not be confused with the journalist and publicist of the same name. He is a graduate of the National Defence Academy (currently the War Studies University). He has held leadership positions in the Polish Armed Forces and has many years of service at the Central Investigation Bureau of Police (CBŚP).

The book under review is divided into an introduction and four chapters. The first chapter, entitled *The basics of terrorism and AI technology*, is introductory and contextual. The author defines terrorism, presents the fundamental trends in the evolution of this phenomenon, and describes the goals and methods of contemporary extremist groups. He defines key concepts in the field of AI, with particular emphasis on deep learning and machine learning.

The second chapter – *Research on the use of AI in the prevention of terrorism* – begins with the author outlining, through a few examples, some areas of research into the use of AI to combat terrorism. The following subchapter briefly describes selected centres and organisations that examine AI from a security perspective, with Wróblewski focusing more on researching the security of AI than on the use of this technology for counter-terrorism purposes. The next subchapter is particularly interesting, as it compares traditional counter-terrorism methods with modern solutions based on AI. It offers a comprehensive overview of the new opportunities that AI offers the security services and the risks posed by this technology. In this light, the previous two subchapters leave something to be desired, as, contrary to the title of the entire chapter, they focus only on a few aspects of this multidimensional issue. The chapter is complemented by an analysis and discussion of the results of the expert opinion survey on the effectiveness of AI tools in combating terrorism. The survey research referred to by the author was conducted in 2022 as part of “Terrorism – Studies, Analyses, Prevention” – the journal of the Internal

Security Agency. Ninety four experts took part in the survey, mostly from the state administration and academic centres. I consider both the findings of the study and the discussion to be valuable, as they demonstrate an active and profound interest in the challenges – posed by the rapid development of AI – on the part of the internal security expert community in Poland.

The third chapter – *Identifying threats using AI* – is the most comprehensive and, in my opinion, the most interesting, as it covers by far the widest range of aspects and examples of how AI-based technologies are used to combat terrorism. The first subchapter relates to data processing and analysis. The second subchapter discusses the use of natural language processing techniques to analyse communication between terrorists. In fact, there is much more to it than that, as a significant portion of the text deals with the risks posed by the development of large language models (LLM), which can be exploited by terrorists in various ways. I consider this analysis to be both very necessary and accurate. The next subchapter focuses on the fundamental issues relating to social media monitoring using AI technology. In it, the author discusses in greater detail the design of predictive models that can be used to identify the intentions of terrorist groups at a relatively early stage. The subchapter 3.4 describes the use of AI solutions for analysing financial data in the context of anti-money laundering and counter-terrorist financing. Wróblewski emphasises the advantage of algorithms over human capabilities when dealing with the sheer volume of data and the complexity of criminal patterns that can be identified from that data. In the next subchapter, the author introduced issues related to image recognition systems, in particular faces. He cites an interesting example of how these technologies were used in 2024 in Berlin by a German female terrorist from the Red Army Faction. The last subchapter is surprising because it deals with the use of AI to support operations in crisis situations that may result from terrorist activities. Research into the use of AI in crisis situations is extremely important, and I believe it is essential to address this issue in the context of terrorism as well.

In the fourth chapter, the author focuses on ethical and social implications of using AI in the context of security. He also analyses the regulatory framework currently being developed at the national and international level.

It should be emphasised that Tomasz Wróblewski took on an exceptionally difficult topic. Artificial intelligence is, in fact, a technology

characterised by an almost unprecedented pace of development, one that permeates many aspects of the lives of individuals and societies. In such a situation, any attempt to provide a comprehensive overview of even a fraction of the available possibilities or directions for the development of AI from the perspective of counter-terrorism efforts is a huge challenge. This becomes even more apparent when we consider the very nature of terrorism – a phenomenon that is extremely complex, multifaceted and constantly evolving. Each attempt to combine these two areas of complexity and to systematically organise this field of research is praiseworthy. The author's interdisciplinary approach to academic interests proved to be extremely valuable in this context.

One of the publication's strengths is its language. Wróblewski avoids excessive use of technical jargon, making the text accessible to non-IT professionals. However, I believe that this book is also very valuable for this group, as it helps them grasp the complexity of issues related both to the existence of technology as such and to its use in society. Another strength of the book is its two-pronged approach to analysing the role of AI in the field of security. On the one hand, the author discusses the use of this technology by government agencies, on the other, he analyses the ways in which the same technologies can be adapted by terrorist groups to plan attacks, spread disinformation or carry out operations in cyberspace. Presenting AI as a tool available to both sides of the conflict is important because it allows the reader to better assess the ever-changing threats.

In summary, Tomasz Wróblewski's work is an important publication that addresses the essence of contemporary threats related to terrorism, which are taking on new forms right before our eyes. The author has succeeded in creating an interesting and valuable compilation of knowledge that serves as a good starting point for a deeper analysis of specific issues.

Assoc. Prof. Tomasz Michalak
Professor of the University of Warsaw

AI Strategy Lab leader at IDEAS Research Institute subordinate to the Ministry of Digital Affairs and the Ministry of National Defence as well as a lecturer at the Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw. Previously, the leader

of the independent 'AI for Security' research team at IDEAS NCBR. He is a graduate of the University of Warsaw. He obtained a PhD at the University of Antwerp and his postdoctoral degree at the AGH University. During his academic career, he conducted research at the Department of Computer Science at the University of Oxford, the School of Engineering and Computer Science at the University of Southampton as well as the Department of Computer Science at the University of Liverpool. From 2024 to 2025, he served as co-director of the 'R-GRID: AI algorithms for Threat Prediction and Power Grid Protection' project, funded by NATO grant, and as an expert on an EU-CIP project concerning the protection of critical infrastructure in the European Union.

Contact: tomasz.michalak@ideas.edu.pl

Summary of the report 'Internal Security Agency 2024–2025. Selected activities'

Aleksandra Komar

Independent author



<https://orcid.org/0000-0002-9717-5258>

The Internal Security Agency (ABW)'s report for 2024–2025¹ outlines the key measures taken by the Agency to safeguard the internal security of the Republic of Poland. It describes the ABW's activities in the areas of counter-intelligence, counter-terrorism, the protection of the strategic economic interests of the state, cyber security and the protection of classified information. It emphasises that contemporary threats are multifaceted and encompass both traditional intelligence activities and hybrid operations, cyber attacks, disinformation and attempts to destabilise social and economic life.

¹ *Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności* (Eng. Internal Security Agency 2024–2025. Selected activities). Website link: <https://www.abw.gov.pl/pl/aktualnosci/2815,Agencja-Bezpieczenstwa-Wewnetrznego-2024-2025-Wybrane-aktywnosci.html>.

The main focus areas for the ABW

The Agency’s priority tasks are to safeguard the stability of the state and the constitutional order and the security of citizens. In 2024–2025, we faced an increasing scale of threats from the intelligence services of the Russian Federation, the Republic of Belarus and the People’s Republic of China.

The report indicates that Russia carried out intensive intelligence and subversive activities targeting Poland, as well as NATO and European Union member states. These activities were aimed at undermining trust in state institutions, spreading disinformation, fuelling anti-European sentiment and destabilising the socio-political situation. Attempts to carry out acts of sabotage against critical infrastructure, military facilities and sites involved in organising support for Ukraine posed a particular threat.

Belarus mainly carried out operations against opposition groups in Poland and aimed at surveying military and critical infrastructure. The report also highlighted the close cooperation between the Belarusian and Russian secret services.

China’s activities remain a significant challenge. Chinese intelligence services exploit economic, scientific and media links to build political and economic influence. They are particularly interested in Polish experts, academics and civil servants who have access to strategic information.

Report – statistics on the ABW’s activities

The report presents figures illustrating the scale of the threats and the effectiveness of the ABW’s activities in areas such as counter-intelligence, the protection of Poland’s strategic economic interests and the fight against terrorism.

Counter-intelligence

Table 1 shows indicators in the field of counter-intelligence activities.

Table 1. Indicators in the field of counter-intelligence activities.

Indicator	Value
Ongoing investigations into espionage	over 60 (including 48 initiated in 2025)

Indicator	Value
Individuals who have been classified as suspects since the start of Russia's full-scale aggression against Ukraine	91
Individuals charged with espionage	82
Individuals detained for acting on behalf of foreign intelligence services	62
Analyses and information prepared for the highest levels of government	over 430

Source: own elaboration based on: *Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności*.

The report highlights that 69 investigations into intelligence activities were launched between 2024 and 2025, which is the same number as the total for the period 1991–2023. This demonstrates an unprecedented increase in the threat to national security.

Protection of Poland's strategic economic interests

In the area of protecting Poland's strategic economic interests, the ABW's activities included:

- protecting energy investments, including the construction of Poland's first nuclear power station,
- monitoring infrastructure projects and investments carried out by state-owned companies,
- combating financial fraud and corruption,
- analysing threats associated with cryptocurrencies used to finance criminal and terrorist activities.

Anti-corruption measures were also a key element of the organisation's activities. By the end of 2024, 23 strategic projects were covered by these measures, a year later, that number had risen to 36.

Counter-terrorism

Counter-terrorism is a very important area of the ABW's work. The report indicates that the level of terrorist threat in Poland remains lower than

in many Western European countries, however, this does not mean that there are no real dangers.

The report focused primarily on Islamic terrorism. ABW officers identified cases of radicalisation among both Polish citizens and foreign nationals residing in the country. Illegal migration across the Polish-Belarusian border poses a particular threat, as it may enable individuals from countries posing a high risk of terrorism to enter the country.

The report also highlights the worrying phenomenon of the radicalisation of teenagers and young adults. Young people are increasingly taking an interest in the propaganda of terrorist organisations, such as the so-called Islamic State of Iraq and Syria (ISIS). This mainly takes place via the internet, social media and instant messaging services. In extreme cases, this can lead to the planning of terrorist attacks.

Thanks to operations carried out by the ABW, the following individuals, for example, were arrested:

- a 17-year-old resident of the Podkarpackie Voivodeship who was preparing an attack inspired by ISIS ideology,
- three 19-year-old residents of Olsztyn who were planning to carry out a terrorist attack,
- a 19-year-old Polish citizen suspected of preparing an attack on Polish soil,
- a Tajik citizen who was a member of ISIS and who was deported from Poland.

The report highlights the extremely important role played in counter-terrorism operations by the 24-hour exchange of information between the services responsible for national security. Within the ABW, this responsibility lies with the Counter-Terrorism Centre (CAT ABW).

Table 2 shows the key statistics on counter-terrorism.

Table 2. Indicators in the field of counter-terrorism.

Indicator	Value
Ongoing criminal proceedings relating to terrorism	19 (including 7 initiated in 2025)
Analyses of terrorist threats	178
Operational reports on potential threats	almost 700

Indicator	Value
Opinions relating to licensing procedures for weapons, explosives and strategic technologies	over 880
Number of applications for licences for the international trade in strategic goods and technologies	ca. 5500

Source: own elaboration based on: *Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności.*

Preventive measures, monitoring of radicalisation processes and the rapid exchange of information between domestic and foreign intelligence services are of particular importance in combating terrorist threats.

Comments on the report

The Head of the ABW, Colonel Rafał Syrysko, gave an interview to the media in which he discussed the ABW's report for the years 2024–2025². He pointed out that the activities of the Russian secret services towards Poland have clearly changed. Currently, these activities are not limited to traditional intelligence-gathering, but increasingly involve acts of subversion and sabotage, which may lead to damage to infrastructure and endanger human lives. According to the Head of the ABW, Russia is 'pushing the boundaries' of its operations, and the services are observing a growing tendency on the part of the adversary towards kinetic actions.

A particularly worrying trend is the Russian security services' exploitation of individuals from criminal circles. Colonel Rafał Syrysko believes that individuals with a criminal background are easier to recruit for subversive activities, as they are able to conceal their activities and operate outside the law. This blurs the line between intelligence operations and organised crime.

In the interview, the Head of the ABW also discussed the report's findings regarding Belarus's specific role in activities directed against

² See in more detail: *Plk Rafał Syrysko, szef ABW o nowej taktyce rosyjskich służb w Polsce i największych Ryzykach* (Eng. Col. Rafał Syrysko, the Head of the ABW on the new tactics of the Russian security services in Poland and the greatest Risks), Rzeczpospolita, 6 V 2026, <https://www.rp.pl/sluzby/art44311581-plk-rafal-syrysko-szef-abw-o-nowej-taktyce-rosyjskich-sluzb-w-polsce-i-najwiekszych-ryzykach> [accessed: 14 VI 2026].

Poland. He described Belarus as Russia's most important state-backed base in the region. The Belarusian security services are involved in influence operations, migration activities and border provocations, and they support Russian initiatives aimed at undermining the security of Poland and NATO member states.

The discussion also touched upon the issue of Chinese intelligence activities. According to the Head of the ABW, China's activities are long-term in nature and focus on building economic, political and social influence. The Chinese intelligence services utilise economic ties and expert circles to establish a base of influence, and also carry out information campaigns aimed at improving the image of the Chinese model of state.

The interview also touched on terrorist threats. Colonel Rafał Syrysko believes that the threat of Islamic terrorism in Poland remains relatively low. The ABW constantly monitors cases of radicalisation among both foreign nationals and Polish citizens. International cooperation and the rapid exchange of information between security services are of particular importance, as they enable the identification of individuals who may pose a threat.

The Head of the ABW emphasises that terrorists are increasingly using the internet, instant messaging apps and social media to recruit and radicalise young people. For this reason, preventive measures by the security services and the monitoring of the digital space are becoming just as important as traditional operational activities.

Conclusions

The ABW report and the interview with the Head of the ABW show that Poland currently finds itself in a security environment characterised by rapidly evolving threats. In addition to traditional espionage, hybrid operations, sabotage, disinformation, cyber attacks and the radicalisation of young people are becoming increasingly significant. Operations carried out by Russia and its ally Belarus remain a particular challenge.

The data presented in the report point to the high level of activity and effectiveness of the ABW in detecting and neutralising threats to national security. Poland's security is currently under severe pressure due to the international situation, particularly the war in Ukraine and Russia's aggressive policy. The number of intelligence, sabotage and disinformation

operations targeting Poland is on the rise. At the same time, the ABW is increasing the effectiveness of its operations, as evidenced by numerous arrests, charges brought and the growing number of investigations being conducted. The document also emphasises the importance of international cooperation, particularly within NATO and the EU. Joint action by the security services of allied states is essential to effectively counter contemporary threats.

Aleksandra Komar, PhD

Deputy Editor-in-Chief of the “Terrorism – Studies, Analyses, Prevention” – the scientific journal of the Internal Security Agency.

Contact: a.komar@abw.gov.pl

