Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 263–287

https://doi.org/10.4467/27204383TER.25.010.21513

Artykuł

Wyniki badania ankietowego dotyczącego percepcji zagrożeń terrorystycznych i sabotażowych wśród ekspertów EU Protective Security Advisors

Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors

KAROLINA WOJTASIK https://orcid.org/0000-0002-1215-5005

Stałe Przedstawicielstwo RP przy Unii Europejskiej
Rządowe Centrum Bezpieczeństwa

DAMIAN SZLACHTER https://orcid.org/0000-0003-2763-9325

Agencja Bezpieczeństwa Wewnętrznego

Abstrakt

Artykuł przedstawia wyniki badań ankietowych dotyczących postrzegania zagrożeń terrorystycznych i sabotażowych przez ekspertów uczestniczących w inicjatywie DG Home Komisji Europejskiej – EU Protective Security Advisors (EU PSA). Ankieta została przeprowadzona w lutym 2025 r. na próbie 50 osób reprezentujących EU PSA, instytucje UE i partnerów strategicznych projektu. Kwestionariusz obejmował kilka ważnych aspektów zagrożeń terrorystycznych i sabotażowych, w tym rodzaje potencjalnych celów, metody ataków i przewidywany rozwój zagrożeń hybrydowych. Respondenci mieli również ocenić, które systemy infrastruktury krytycznej wymagają przyznania im najwyższego priorytetu w działaniach na rzecz

budowania odporności, a także to, jakie środki zwalczania terroryzmu powinny być traktowane priorytetowo na szczeblu UE. Ponadto za pomocą ankiety zbadano czynniki, które mogłyby poprawić bezpieczeństwo chronionych obiektów, i zidentyfikowano najbardziej prawdopodobnych sprawców ataków na infrastrukturę krytyczną UE. Wyniki ankiety dostarczają cennych spostrzeżeń dla kształtowania polityki antyterrorystycznej i antysabotażowej na poziomie UE. Autorzy podkreślają konieczność standaryzacji środków bezpieczeństwa fizycznego i rozwijania inicjatyw edukacyjnych w celu budowania kultury bezpieczeństwa.

Słowa kluczowe

infrastruktura krytyczna, przestrzeń publiczna, terroryzm, sabotaż, odporność, cele miękkie, cele twarde, Komisja Europejska, DG HOME, EU PSA, ochrona infrastruktury krytycznej, zagrożenia hybrydowe, wojna hybrydowa

Abstract

This article presents the results of a survey on the perception of terrorist and sabotage threats by experts participating in the European Commission's EU Protective Security Advisors (EU PSA) initiative. The survey was conducted in February 2025 on a sample of 50 individuals representing EU PSA, EU institutions, and strategic project partners. The questionnaire covered several key aspects of terrorist and sabotage threats, including the types of potential targets, attack methods, and expected developments in hybrid threats. Respondents were also asked to assess which critical infrastructure systems require the highest priority in resilience-building efforts, as well as which counter-terrorism measures should be prioritised at the EU level. Additionally, the survey explored factors that could improve the security of protected facilities and identified the most likely perpetrators of attacks on EU critical infrastructure. The survey results provide valuable insights for shaping counter-terrorism and counter-sabotage policies at the EU level. The authors emphasise the necessity of standardising physical security measures and developing educational initiatives to build a security culture.

Keywords

critical infrastructure, public space, terrorism, sabotage, resilience, soft targets, hard targets, European Commission, DG HOME, EU PSA, critical infrastructure protection, hybrid threats, hybrid warfare

Wprowadzenie

Ochrona przestrzeni publicznej i infrastruktury krytycznej (IK) jest podstawowym obowiązkiem państw członkowskich Unii Europejskiej. W odpowiedzi na rosnące zagrożenia terrorystyczne UE podejmuje inicjatywy wspierające państwa członkowskie w wysiłkach na rzecz ochrony obywateli i IK. Jedną z takich inicjatyw jest unijny program doradców ds. budowania odporności na zagrożenia – EU Protective Security Advisors (EU PSA)[1], stworzony przez Directorate-General for Migration and Home Affairs (DG HOME) Komisji Europejskiej.

Inicjatywa EU PSA ma swoje źródło w pracach UE nad ochroną przestrzeni publicznej, które rozpoczęły się w 2012 r. Impulsem do tych działań było wsparcie eksperckie udzielone Polsce podczas Mistrzostw Europy w Piłce Nożnej UEFA Euro 2012. Pozytywne doświadczenia z tego wydarzenia zaowocowały zaproszeniami z innych krajów UE do współpracy przy wzmacnianiu bezpieczeństwa podczas wydarzeń politycznych wysokiego szczebla i dużych zgromadzeń publicznych. Ważnym momentem w rozwoju unijnej polityki ochrony przestrzeni publicznej było przyjęcie w październiku 2017 r. planu działania poświęconego tym zagadnieniom. W jego ramach UE opracowała narzędzie do oceny podatności na zagrożenia. Finalnie doprowadziło to do stworzenia grupy specjalistów i ustanowienia unijnego programu PSA. Grupa EU PSA składa się z ok. 130 specjalistów z Komisji Europejskiej i państw członkowskich UE. Mają oni doświadczenie zawodowe w zakresie ochrony przestrzeni publicznej oraz wiedzę specjalistyczną na temat różnych obszarów bezpieczeństwa. Wdrożenie inicjatywy EU PSA do oficjalnego dorobku prawnego UE w dziedzinie walki z terroryzmem nastąpiło w grudniu 2020 r., wraz z publikacją agendy antyterrorystycznej UE.

Program EU PSA ma na celu udzielenie wsparcia państwom członkowskim UE na ich wniosek. Działania prowadzone w ramach tej inicjatywy obejmują:

- podnoszenie świadomości na temat słabych punktów bezpieczeństwa w przestrzeni publicznej i IK przez zapewnienie wspólnego systemu jego oceny,

[1] *EU Protective Security Advisors (EU PSA)*, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [dostęp: 26.02.2025].

- dzielenie się najlepszymi praktykami i zachęcanie do wymiany wiedzy w celu wyeliminowania zidentyfikowanych słabych punktów bezpieczeństwa,
- dostarczanie państwom członkowskim wskazówek dotyczących zapewniania bezpieczeństwa podczas imprez masowych i ochrony miejsc wysokiego ryzyka,
- budowanie sieci ekspertów przez organizowanie międzynarodowych sesji szkoleniowych i wspieranie inicjatyw przyczyniających się do rozwoju wspólnej kultury bezpieczeństwa w UE.

Program EU PSA obejmuje ochronę przestrzeni publicznej i IK, w tym:

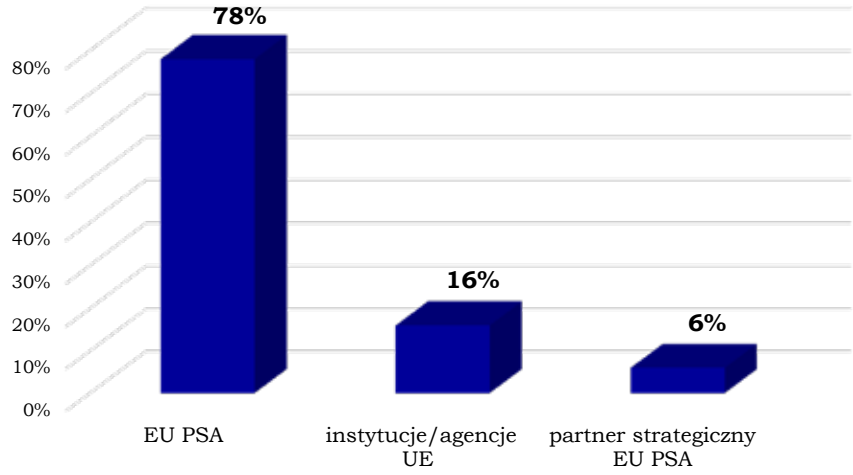
- miejsc kultu i instytucji religijnych,
- wydarzeń kulturalnych, takich jak np. duże festiwale muzyczne,
- wydarzeń z udziałem VIP-ów, takich jak np. szczyty UE,
- dużych obiektów przemysłowych niezaliczanych do IK,
- lotnisk, portów morskich, obiektów z sektora energetycznego oraz innych obiektów zaliczanych do IK.

Ze względu na rosnące uznanie dla programu EU PSA wśród władz państw członkowskich oraz niestabilną sytuację geopolityczną oczekuje się, że zainteresowanie działaniami tej grupy wzrośnie. Państwa członkowskie wyraziły zamiar zaproszenia ekspertów EU PSA do oceny krajowych obiektów IK, szczególnie w kontekście dyrektywy UE w sprawie odporności podmiotów krytycznych. Program EU PSA jest kluczową inicjatywą UE wspierającą państwa członkowskie w ochronie przestrzeni publicznej i IK przed zagrożeniami terrorystycznymi. Podnosząc świadomość, dzieląc się najlepszymi praktykami i zapewniając wsparcie ekspertów, EU PSA przyczynia się do poprawy bezpieczeństwa obywateli i infrastruktury w całej UE. To była przesłanka, dla której autorzy artykułu zdecydowali, że badanie ankietowe dotyczące postrzegania zagrożeń terrorystycznych i sabotażowych zostanie przeprowadzone wśród wspólnoty EU PSA. Składają się na nią członkowie EU PSA, przedstawiciele instytucji i agencji UE współpracujących z EU PSA oraz partnera strategicznego tej inicjatywy.

Wyniki badania ankietowego

Badanie przeprowadzono w lutym 2025 r., z wykorzystaniem standaryzowanego kwestionariusza składającego z 8 pytań[2]. Miało ono charakter anonimowy. W ankiecie wzięło udział 50 osób[3]. Respondenci reprezentowali: EU PSA (78%), instytucje i agencje UE wspierające tę inicjatywę (16%) oraz partnera strategicznego projektu EU PSA (6%). Podział respondentów obrazuje wykres 1.

Wykres 1. Podział respondentów ze względu na reprezentowane przez nich środowisko.



Pytanie nr 1 kwestionariusza brzmiało: *Jakimi obiektami interesują się terroryści/sabotażyści planujący swoje działania w Unii Europejskiej?*

Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 10 miejsca, przy czym 1 miejsce oznaczało obiekt, którym terroryści/sabotażyści interesują sią najbardziej, 10 – najmniej[4]. Respondenci mieli

[2] Załącznik: wzór kwestionariusza ankiety.

[3] Stanowi to ok. 40% liczby członków EU PSA.

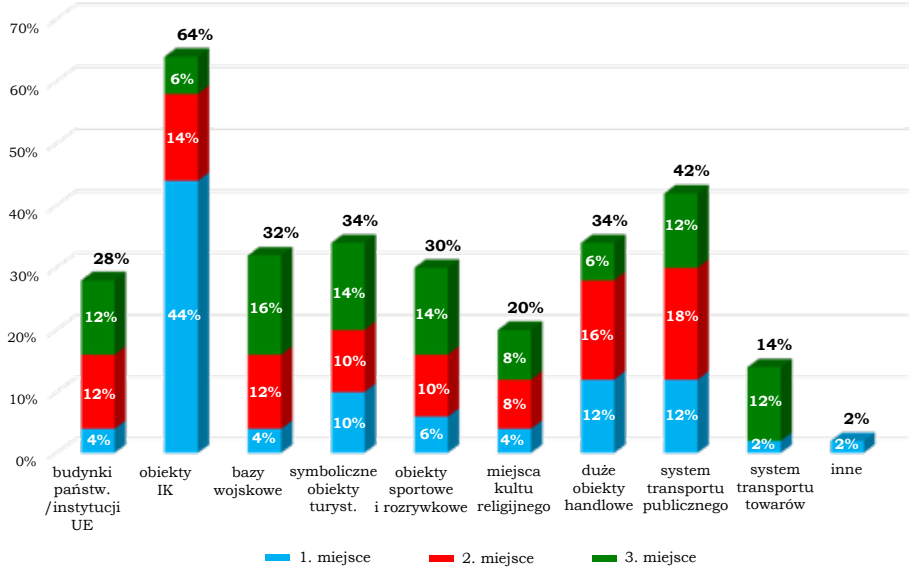
[4] Przy pytaniach, w których zadaniem respondentów było uszeregowanie odpowiedzi, przedstawiono wyniki tylko dla miejsc od 1 do 3. Z tego względu dane na wykresach prezentujących te wyniki nie sumują się do 100%.

podane następujące obiekty: budynki urzędów państwowych i instytucji UE, obiekty IK, bazy wojskowe, symboliczne obiekty turystyczne, obiekty sportowe i rozrywkowe, miejsca kultu religijnego, wielkopowierzchniowe obiekty handlowe, system transportu publicznego, system transportu towarów handlowych, inne.

W grupie obiektów, które respondenci wytypowali na 1 miejscu, najczęściej były wskazywane: obiekty IK (44%), wielkopowierzchniowe obiekty handlowe i system transportu publicznego (oba po 12%) oraz symboliczne obiekty turystyczne (10%). Widoczna jest zatem zdecydowana różnica w częstości wskazań dla IK i kolejnych obiektów. Wśród obiektów, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: system transportu publicznego (18%), wielkopowierzchniowe obiekty handlowe (16%) oraz obiekty infrastruktury krytycznej (14%). Wśród obiektów, które respondenci wskazali na 3 miejscu, najczęstszą odpowiedzią były bazy wojskowe (16%). Wyniki dla kolejnych obiektów były takie same – symboliczne obiekty turystyczne oraz obiekty sportowe i rozrywkowe wskazało 14% ankietowanych. W przypadku obiektów, które respondenci wskazali na 2 i 3 miejscu, nie można zatem stwierdzić wyraźnej przewagi jednego z nich.

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które obiekty były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: obiekty IK (64%), system transportu publicznego (42%) oraz ex aequo symboliczne obiekty turystyczne i wielkopowierzchniowe obiekty handlowe (po 34%). Szczegółowe wyniki zostały przedstawione na wykresie 2.

Wykres 2. Obiekty, którymi interesują się terroryści/sabotażyści planujący działania w UE.

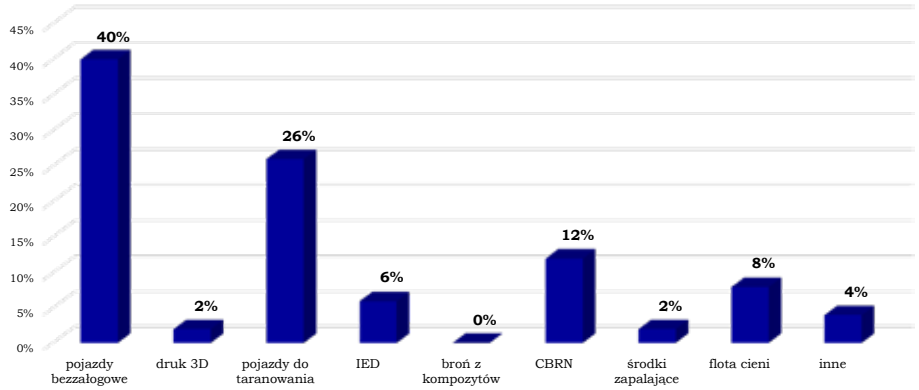


Pytanie nr 2 kwestionariusza brzmiało: *Jakie metody ataku i sabotażu mogą być największym wyzwaniem dla organów ścigania i instytucji zapewniających bezpieczeństwo ludzi i obiektów?*

Respondenci mogli wybrać jedną odpowiedź spośród następujących kategorii: pojazdy bezzałogowe (powietrzne, lądowe, wodne), druk 3D, pojazdy używane do taranowania, improwizowane ładunki wybuchowe (IED), broń wykonana z kompozytów, CBRN, środki zapalające, tzw. flota cieni/ciemna flota (ang. *shadow fleet/dark fleet*), inne.

Najwięcej respondentów (40%) wskazało pojazdy bezzałogowe (powietrzne, lądowe, wodne). W drugiej kolejności ankietowani wskazali pojazdy używane do taranowania (26%), następnie CBRN (12%). Wszystkie wyniki zostały przedstawione na wykresie 3.

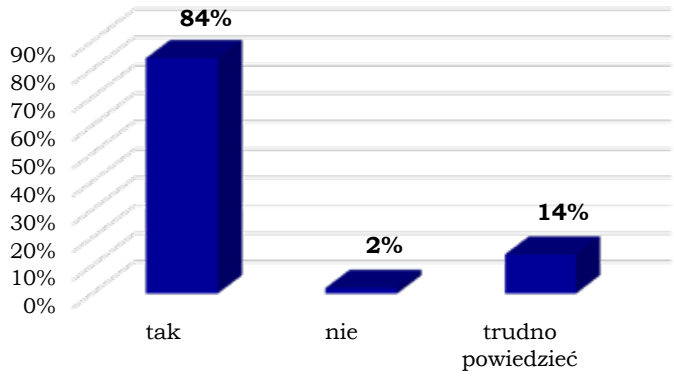
Wykres 3. Metody ataku i sabotażu, które mogą być największym wyzwaniem dla organów ścigania i instytucji zapewniających bezpieczeństwo ludzi i obiektów.



Pytanie nr 3 kwestionariusza brzmiało: *Czy w perspektywie 3 lat należy spodziewać się wykorzystania działań terrorystycznych/sabotażowych w ramach zagrożeń hybrydowych podejmowanych na terytorium UE przez obce państwo?*

Respondenci mogli wybrać jedną odpowiedź spośród: tak, nie, trudno powiedzieć. Twierdząco odpowiedziało 84% respondentów, 14% nie zajęło konkretnego stanowiska, a tylko 2% udzieliło odpowiedzi przeczącej. Wyniki przedstawiono na wykresie 4.

Wykres 4. Czy w perspektywie 3 lat działania terrorystyczne/sabotażowe mogą zostać wykorzystane jako narzędzie operacji hybrydowych w UE?



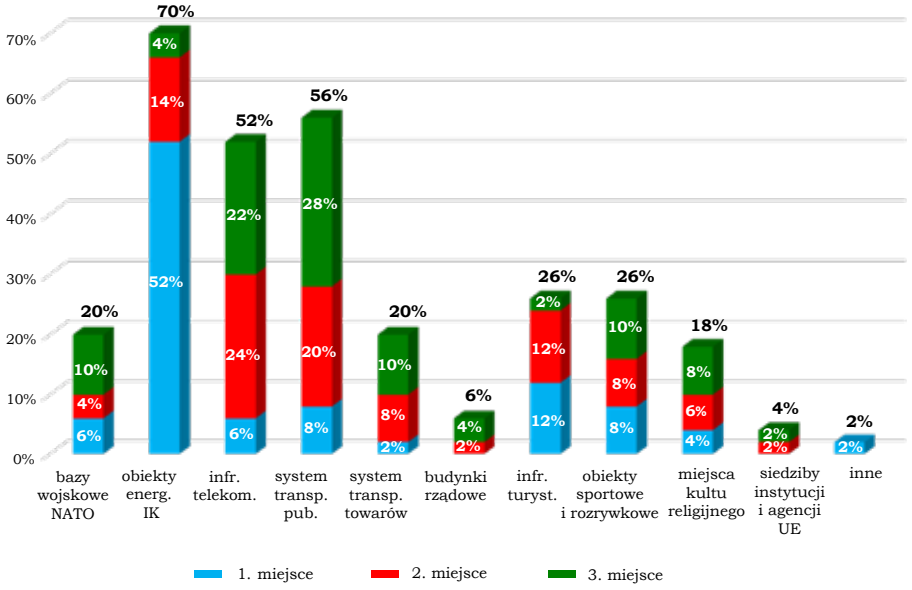
Pytanie nr 4 kwestionariusza brzmiało: *Które obiekty w perspektywie 3 lat będą charakteryzowały się najwyższym poziomem zagrożenia atakami terrorystycznymi/sabotażowymi w UE?*

Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 11 miejsca, przy czym 1 miejsce oznaczało obiekt charakteryzujący się najwyższym poziomem zagrożenia terrorystycznego/sabotażowego, a 11 – najniższym. Respondenci mieli podane następujące obiekty: bazy wojskowe NATO, obiekty energetycznej IK, infrastruktura telekomunikacyjna, system transportu publicznego, system transportu towarów handlowych, budynki rządowe, infrastruktura turystyczna, obiekty sportowe i rozrywkowe, miejsca kultu religijnego, siedziby instytucji i agencji UE, inne.

W grupie obiektów, które respondenci wytypowali na 1 miejscu, najczęściej były wskazywane: obiekty energetycznej IK (52%), infrastruktura turystyczna (12%) oraz obiekty sportowe i rozrywkowe (8%). Należy podkreślić zdecydowaną przewagę IK – następne w kolejności obiekty miały znacznie mniejszą liczbę wskazań. Wśród obiektów, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: infrastruktura telekomunikacyjna (24%), system transportu publicznego (20%) oraz obiekty energetycznej IK (14%). Wśród obiektów, które respondenci wskazali na 3 miejscu, najczęstszymi odpowiedziami były: system transportu publicznego (28%), infrastruktura telekomunikacyjna (22%) oraz bazy wojskowe NATO, system transportu towarów handlowych i obiekty sportowe i rozrywkowe (wszystkie po 10%). Zatem w przypadku 2 i 3 miejsca zjawisko przewagi jednego typu obiektu nie wystąpiło.

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które obiekty były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: obiekty energetycznej IK (70%), system transportu publicznego (56%) oraz infrastruktura telekomunikacyjna (52%). Szczegółowe wyniki zostały przedstawione na wykresie 5.

Wykres 5. Obiekty, które będą charakteryzowały się najwyższym poziomem zagrożenia atakami terrorystycznymi/sabotażowymi.



Pytanie nr 5 kwestionariusza brzmiało: *Które systemy infrastruktury krytycznej w perspektywie 3 lat powinny być traktowane priorytetowo w zakresie budowania ich odporności na zagrożenia hybrydowe?*

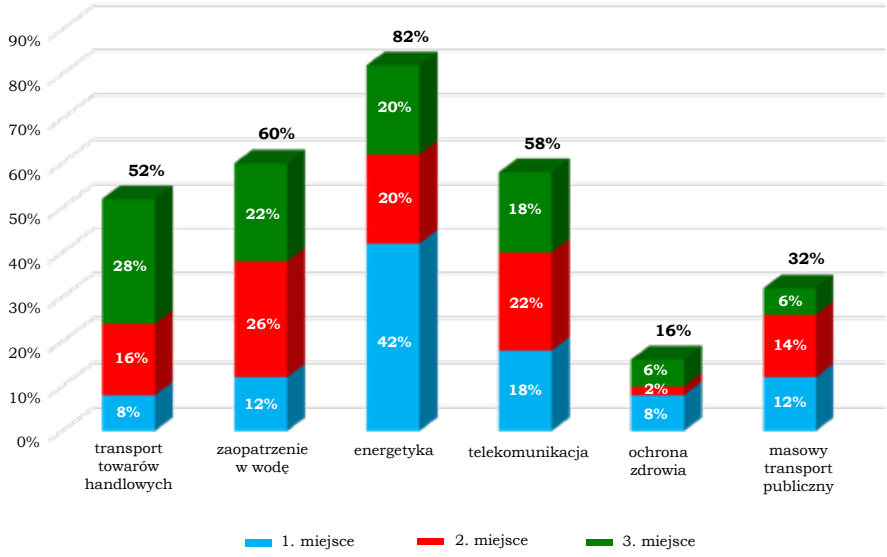
Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 7 miejsca, przy czym 1 miejsce oznaczało system IK o najwyższym priorytecie, a 7 – o najniższym. Respondenci mieli podane następujące systemy: transport towarów handlowych (szlaki komunikacyjne i węzły przeładunkowe), zaopatrzenie w wodę, energetyka, telekomunikacja, ochrona zdrowia, masowy transport publiczny, inne.

W grupie systemów IK, które respondenci wytypowali na 1 miejscu, zdecydowanie najwięcej badanych wskazało system energetyczny (42%), następne w kolejności były system telekomunikacyjny (18%) oraz system zaopatrzenia w wodę i system masowego transportu publicznego (oba po 12%). W przypadku 2 i 3 miejsca odpowiedzi respondentów rozkładają się bardziej równomiernie. Wśród systemów, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: system zaopatrzenia w wodę (26%), system telekomunikacyjny (22%) i system energetyczny (20%). Wśród systemów, które respondenci wskazali na 3 miejscu,

najczęstszymi odpowiedziami były: transport towarów handlowych (28%), system zaopatrzenia w wodę (22%) i system energetyczny (20%).

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które systemy IK były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: system energetyczny (82%), system zaopatrzenia w wodę (60%) oraz system telekomunikacyjny (58%). Szczegółowe wyniki zostały przedstawione na wykresie 6 (odpowiedź „inne" nie padła).

Wykres 6. Priorytetowe systemy IK w budowaniu odporności na zagrożenia hybrydowe.



Pytanie nr 6 kwestionariusza brzmiało: *Który z obszarów przeciwdziałania działalności terrorystycznej wymaga obecnie priorytetowego traktowania na poziomie UE?*

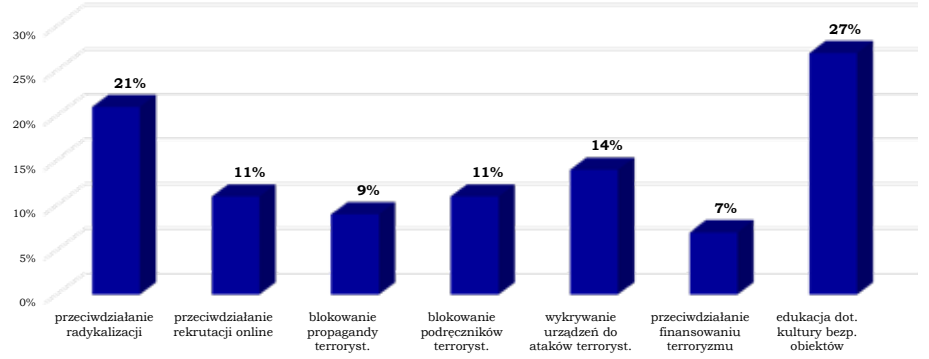
Respondenci mogli wybrać jedną odpowiedź spośród: przeciwdziałanie radykalizacji prowadzącej do działań terrorystycznych, przeciwdziałanie rekrutacji online do działań terrorystycznych/sabotażowych, wykrywanie i blokowanie propagandy terrorystycznej, wykrywanie i blokowanie podręczników terrorystycznych/sabotażowych publikowanych w internecie, rozwijanie technologii wykrywania urządzeń wykorzystywanych

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

do przeprowadzania ataków terrorystycznych, przeciwdziałanie finansowaniu terroryzmu, inicjatywy edukacyjne dotyczące kultury bezpieczeństwa obiektów narażonych na ataki terrorystyczne/sabotażowe, inne.

W przypadku odpowiedzi na to pytanie zdania ankietowanych były podzielone. Najwięcej respondentów wskazało na działania edukacyjne i budowanie kultury bezpieczeństwa w obiektach, które mogłyby być celem działań terrorystycznych bądź sabotażowych (27%). W drugiej kolejności ankietowani wskazali przeciwdziałanie radykalizacji prowadzącej do działań terrorystycznych (21%), a następnie rozwijanie technologii wykrywania urządzeń wykorzystywanych do przeprowadzania ataków terrorystycznych (14%). Wszystkie wyniki zostały przedstawione na wykresie 7.

Wykres 7. Priorytety w przeciwdziałaniu terroryzmowi.



Pytanie nr 7 kwestionariusza brzmiało: *Co może zwiększyć poziom odporności chronionych obiektów na ataki terrorystyczne i działania sabotażowe?*

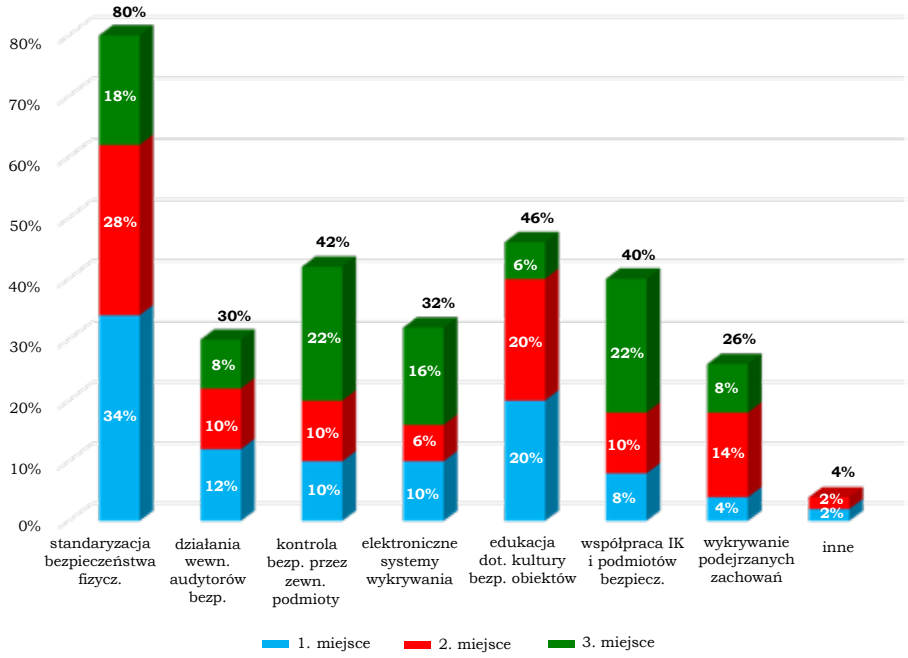
Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 8 miejsca, przy czym 1 miejsce oznaczało działania najważniejsze, a 8 – najmniej ważne. Respondenci mieli podane następujące odpowiedzi: standaryzacja bezpieczeństwa fizycznego (także procedur dotyczących pracowników ochrony), zadania wykonywane przez wewnętrznych audytorów bezpieczeństwa, testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty nadzorujące (takie jak: instytucje UE, państwowe organy kontrolne), rozwój inteligentnych elektronicznych systemów

wykrywania zdarzeń zagrażających bezpieczeństwu, rozwój inicjatyw związanych z prewencją terrorystyczną jako elementem kultury bezpieczeństwa obiektu (edukacja dla bezpieczeństwa), poprawa współpracy pomiędzy podmiotami IK a podmiotami odpowiedzialnymi za bezpieczeństwo, wykrywanie podejrzanych zachowań przez przeszkolonych pracowników ochrony, inne.

W grupie działań, które respondenci wytypowali na 1 miejscu, najczęściej były wskazywane: standaryzacja bezpieczeństwa fizycznego (34%), rozwój inicjatyw związanych z prewencją terrorystyczną (20%) oraz zadania wykonywane przez wewnętrznych audytorów bezpieczeństwa (12%). Przy czym różnica między kolejnymi wskazanymi działaniami – testami kontrolnymi bezpieczeństwa przeprowadzanymi przez zewnętrznych nadzorców (takich jak: instytucje UE, państwowe organy kontroli) oraz rozwojem inteligentnych elektronicznych systemów wykrywania zdarzeń zagrażających bezpieczeństwu była niewielka – obie opcje uzyskały po 10% wskazań. Wśród działań, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: standaryzacja bezpieczeństwa fizycznego (28%), rozwój inicjatyw związanych z prewencją terrorystyczną (20%) i wykrywanie podejrzanych zachowań przez przeszkolonych pracowników ochrony (14%). Wśród działań, które respondenci wskazali na 3 miejscu, najczęstszymi odpowiedziami były: testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty nadzorujące oraz poprawa współpracy pomiędzy podmiotami IK a podmiotami odpowiedzialnymi za bezpieczeństwo (oba po 22%). Kolejną odpowiedzią była standaryzacja bezpieczeństwa fizycznego (18%).

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które działania były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: standaryzacja bezpieczeństwa fizycznego (80%), rozwój inicjatyw związanych z prewencją terrorystyczną (46%), testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty (42%). Szczegółowe wyniki zostały przedstawione na wykresie 8.

Wykres 8. Działania mające na celu zwiększenie odporności obiektów na ataki terrorystyczne i działania sabotażowe.

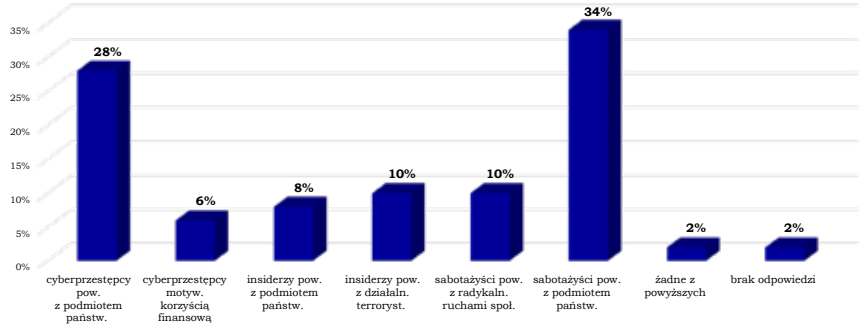


Pytanie nr 8 kwestionariusza dotyczyło sprawców ataków na IK.

Respondenci mogli wybrać jedną odpowiedź spośród: cyberprzestępcy powiązani z podmiotem państwowym, cyberprzestępcy kierujący się wyłącznie chęcią osiągnięcia korzyści finansowych, tzw. insiderzy powiązani z podmiotem państwowym, tzw. insiderzy powiązani z działalnością terrorystyczną, sabotażyści powiązani z działalnością radykalnych ruchów społecznych, sabotażyści powiązani z podmiotem państwowym, żadne z powyższych.

Najwięcej respondentów (34%) wskazało sabotażystów powiązanych z podmiotem państwowym. W drugiej kolejności badani wskazali cyberprzestępców powiązanych z podmiotem państwowym (28%), a następnie ex aequo insiderów powiązanych z działalnością terrorystyczną oraz sabotażystów powiązanych z działalnością radykalnych ruchów społecznych (po 10%). Wszystkie wyniki zostały przedstawione na wykresie 9.

Wykres 9. Potencjalni sprawcy ataków na obiekty IK.



Podsumowanie wyników badań ankietowych

Eksperci zaangażowani w EU PSA wskazali obiekty IK (64% wszystkich odpowiedzi), system transportu publicznego (42%) oraz symboliczne obiekty turystyczne i wielkopowierzchniowe obiekty handlowe (oba 34%) jako najbardziej prawdopodobne cele ataku terrorystycznego/sabotażowego w UE. Należy podkreślić, że przy konstruowaniu kwestionariusza ankiety autorzy artykułu skupili się przede wszystkim na celu ataku, a nie na metodzie. Wnioski wynikające z badań ankietowych nie odbiegają od innych danych. Najnowszy raport TE-SAT przedstawia informacje dotyczące ataków terrorystycznych, do których doszło w 2023 r. W 45 ze 120 przypadków podano bardziej szczegółowe dane, z których wynika, że w 1/3 tych ataków celem była IK[5].

Jeśli chodzi o metody ataku i sabotażu, które mogą być największym wyzwaniem dla organów ścigania, władz i instytucji odpowiedzialnych za zapewnienie bezpieczeństwa fizycznego, najczęstszym wskazaniem respondentów były pojazdy bezzałogowe (powietrzne, lądowe, wodne). Takiej odpowiedzi udzieliło 40% ankietowanych. Ostatnie lata to czas intensywnego rozwoju dronów. Coraz częściej są one wykorzystywane do popełniania przestępstw. Warto podkreślić, że podwodne drony mogą w przyszłości stanowić poważne zagrożenie dla morskiej IK. We wspomnianym raporcie TE-SAT podano również, że osoby z różnych środowisk ideologicznych mogące stanowić zagrożenie aktywnie poszukują materiałów szkoleniowych online i instrukcji obsługi zawierających informacje na temat taktyki

[5] *European Union Terrorism Situation and Trend Report* (EU TE-SAT) 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf, s. 12 [dostęp: 26.02.2025].

przeprowadzania ataków i tworzenia broni, w tym chemicznej, konstruowania dronów, bomb[6]. Na drugim miejscu uczestnicy badania ankietowego wskazali pojazdy używane do taranowania (26% respondentów), co prawdopodobnie ma związek z ostatnimi wydarzeniami (atak w Magdeburgu w grudniu 2024 r. i atak w Mannheim w marcu 2025 r.)[7].

84% respondentów uważa, że w perspektywie 3 lat działania terrorystyczne i sabotażowe zostaną wykorzystane w ramach działań hybrydowych podejmowanych na terytorium UE przez obce państwo.

Jeśli chodzi o rodzaje obiektów w UE, które w ciągu najbliższych 3 lat będą charakteryzować się najwyższym poziomem zagrożenia atakiem terrorystycznym/sabotażowym, to respondenci najczęściej wskazywali: obiekty energetycznej IK (70%), system transportu publicznego (56%) oraz infrastrukturę telekomunikacyjną (52%). Liczba ataków, głównie cybernetycznych, na infrastrukturę energetyczną i telekomunikacyjną stale rośnie[8] i staje się podstawą wojny hybrydowej. Ataki na transport publiczny są powszechną taktyką stosowaną przez grupy dżihadystów[9].

Większość respondentów wskazała, że systemem IK, który w perspektywie 3 lat powinien być traktowany priorytetowo przy budowaniu odporności na zagrożenia hybrydowe, jest system energetyczny (82%). Sprawne funkcjonowanie infrastruktury energetycznej jest warunkiem

---

[6] Tamże, s. 7.

[7] Atak w Magdeburgu – 20 grudnia 2024 r. kierowca wjechał w grupę ludzi na jarmarku bożonarodzeniowym. Zginęło 6 osób, ponad 100 zostało rannych. Sprawcą był 50-letni lekarz pochodzenia saudyjskiego, mieszkający w Niemczech od 2006 r. Atak w Mannheim – 3 marca 2025 r. 40-letni obywatel Niemiec wjechał samochodem w grupę ludzi na deptaku. Zabił 2 osoby i ranił kilka innych. Sprawca został zatrzymany przez policję wkrótce po zdarzeniu.

[8] B. Nieróbca, *Energetyka w sieci cyberzagrożeń*, EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [dostęp: 26.02.2025]; *Raport: cyberbezpieczeństwo w energetyce*, https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [dostęp: 26.02.2025]; K. Pohoska, *Cyberprzestępczość – prognozy na 2025 rok*, Stołeczny Magazyn Policyjny, 3.03.2025, https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html [dostęp: 20.03.2025].

[9] *The Tactics and Targets of Domestic Terrorists*, Center for Strategic and International Studies, 30.07.2020, https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists [dostęp: 26.02.2025]; B.M. Jenkins, B.R. Butterworth, K.S. Shrum, *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, https://transweb.sjsu.edu/research/Terrorist-Attacks-Public-Bus-Transportation-Preliminary-Empirical-Analysis [dostęp: 26.02.2025].

funkcjonowania nowoczesnego społeczeństwa. Skutki ataku na system energetyczny są wielopoziomowe. Z tego względu jest on uznawany za najbardziej narażony na ataki.

W przypadku pytania o obszar przeciwdziałania działalności terrorystycznej, który dziś wymaga priorytetowego potraktowania przez UE, zdania respondentów były podzielone. Najwięcej ankietowanych (27%) wskazało jednak na działania edukacyjne i budowanie kultury bezpieczeństwa w obiektach, które mogą stać się celem ataku. Będzie to istotne wyzwanie dla operatorów IK i instytucji sprawujących nad nimi nadzór.

Przedsięwzięciami, które w największym stopniu mogą zwiększyć poziom odporności na ataki terrorystyczne i działania sabotażowe w chronionych obiektach, są: standaryzacja ochrony fizycznej (80%), rozwój inicjatyw prewencji terrorystycznej w ramach kultury bezpieczeństwa obiektu (46%) oraz testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty (42%).

Najwięcej respondentów uważa, że sprawcami przeprowadzanych obecnie ataków na systemy IK są sabotażyści powiązani z podmiotem państwowym (34%) lub cyberprzestępcy powiązani z podmiotem państwowym (28%).

Wyniki przeprowadzonego badania jednoznacznie wskazują na zagrożenie atakami terrorystycznymi i sabotażowymi, wymierzonymi zwłaszcza w IK, system transportu publicznego oraz system telekomunikacyjny. Respondenci, reprezentujący środowisko ekspertów ds. bezpieczeństwa, podkreślili potrzebę priorytetowego traktowania działań mających na celu wzmacnianie odporności obiektów o kluczowym znaczeniu dla funkcjonowania państwa i społeczeństwa.

Na podstawie analizy wyników ankiety można zauważyć, że w najbliższych latach będzie konieczne dalsze rozwijanie środków służących zapobieganiu atakom, obejmujących: standaryzację ochrony fizycznej, wdrażanie nowoczesnych technologii wykrywania zagrożeń oraz inicjatywy edukacyjne w zakresie prewencji terrorystycznej. Ponadto istotne znaczenie będzie miała współpraca między operatorami IK a organami odpowiedzialnymi za bezpieczeństwo, co pozwoli na lepszą koordynację działań i skuteczniejsze reagowanie na incydenty.

Badanie potwierdza również, że zagrożenia terrorystyczne i sabotażowe coraz częściej stanowią element strategii działań hybrydowych podejmowanych przez podmioty państwowe i niepaństwowe. W obliczu dynamicznie zmieniającego się środowiska bezpieczeństwa państwa

członkowskie UE powinny dążyć do wdrażania kompleksowych strategii ochrony, uwzględniających zarówno aspekty fizyczne, jak i cyberbezpieczeństwo.

Bibliografia

EU Protective Security Advisors (EU PSA), https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [dostęp: 26.02.2025].

Jenkins B.M., Butterworth B.R., Shrum K.S., *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, https://transweb.sjsu.edu/research/Terrorist-Attacks-Public-Bus-Transportation-Preliminary-Empirical-Analysis [dostęp: 26.02.2025].

Nieróbca B., *Energetyka w sieci cyberzagrożeń*, EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [dostęp: 26.02.2025].

Pohoska K., *Cyberprzestępczość – prognozy na 2025 rok*, Stołeczny Magazyn Policyjny, 3.03.2025, https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html [dostęp: 20.03.2025].

The Tactics and Targets of Domestic Terrorists, Center for Strategic and International Studies, 30.07.2020, https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists [dostęp: 26.02.2025].

Inne dokumenty

European Union Terrorism Situation and Trend Report (EU TE-SAT) 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [dostęp: 26.02.2025].

Raport: cyberbezpieczeństwo w energetyce, https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [dostęp: 26.02.2025].

Załącznik

Wzór kwestionariusza ankiety wykorzystanego w lutym 2025 r.

BADANIE EU PSA 2025

Niniejsza ankieta jest przeprowadzana wśród przedstawicieli państw członkowskich UE i Komisji Europejskiej uczestniczących w projekcie budowania odporności na ataki terrorystyczne w przestrzeni publicznej – EU PSA (Protective Security Advisors) w DG HOME Komisji Europejskiej. Ankieta jest anonimowa, a jej wyniki zostaną zebrane w sposób uniemożliwiający identyfikację osoby ją wypełniającej.

Celem ankiety jest uzyskanie opinii respondentów na temat najbardziej prawdopodobnych sposobów rozwoju zagrożeń terrorystycznych/sabotażowych w UE.

Wyniki ankiety zostaną opublikowane w numerze specjalnym czasopisma naukowego „Terroryzm – studia, analizy, prewencja", który będzie poświęcony zagrożeniom terrorystycznym i hybrydowym dla infrastruktury krytycznej. Wydanie specjalne ukaże się w maju 2025 r. i będzie dystrybuowane na posiedzeniach grup roboczych Rady UE: WPT, PROCIV CER w ramach polskiej prezydencji w Radzie UE.

Naszym zdaniem wyniki tego badania mogą przyczynić się do dyskusji na temat rozwoju inicjatyw antyterrorystycznych i antysabotażowych, w tym do zapobiegania zagrożeniom i podnoszenia świadomości na ich temat na poziomie UE i w państwach członkowskich.

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

Początek kwestionariusza ankiety

1. Jakimi obiektami interesują się terroryści/sabotażyści planujący swoje działania w Unii Europejskiej?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   - budynki urzędów państwowych i instytucji UE,
   - obiekty infrastruktury krytycznej,
   - bazy wojskowe,
   - symboliczne obiekty turystyczne,
   - obiekty sportowe i rozrywkowe,
   - miejsca kultu religijnego,
   - wielkopowierzchniowe obiekty handlowe,
   - system transportu publicznego,
   - system transportu towarów handlowych,
   - inne.

2. Jakie metody ataku i sabotażu mogą być największym wyzwaniem dla organów ścigania i instytucji zapewniających bezpieczeństwo ludzi i obiektów?

   Wybierz jedną odpowiedź:

   - pojazdy bezzałogowe (powietrzne, lądowe, wodne),
   - druk 3D,
   - pojazdy używane do taranowania,
   - improwizowane ładunki wybuchowe,
   - broń wykonana z kompozytów,
   - CBRN,
   - środki zapalające,
   - tzw. flota cieni/ciemna flota,
   - inne.

3. Czy w perspektywie 3 lat należy spodziewać się wykorzystania działań terrorystycznych/sabotażowych w ramach zagrożeń hybrydowych podejmowanych na terytorium UE przez obce państwo?

   Wybierz jedną odpowiedź:

   - tak,
   - nie,
   - trudno powiedzieć.

4. Które obiekty w perspektywie 3 lat będą charakteryzowały się najwyższym poziomem zagrożenia atakami terrorystycznymi/sabotażowymi w UE?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   - bazy wojskowe NATO,
   - obiekty energetycznej infrastruktury krytycznej,
   - infrastruktura telekomunikacyjna,
   - system transportu publicznego,
   - system transportu towarów handlowych,
   - budynki rządowe,
   - infrastruktura turystyczna,
   - obiekty sportowe i rozrywkowe,
   - miejsca kultu religijnego,
   - siedziby instytucji i agencji UE,
   - inne.

5. Które systemy infrastruktury krytycznej w perspektywie 3 lat powinny być traktowane priorytetowo w zakresie budowania ich odporności na zagrożenia hybrydowe?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

- transport towarów handlowych (szlaki komunikacyjne i węzły przeładunkowe),
- zaopatrzenie w wodę,
- energetyka,
- telekomunikacja,
- ochrona zdrowia,
- masowy transport publiczny,
- inne.

6. Który z obszarów przeciwdziałania działalności terrorystycznej wymaga obecnie priorytetowego traktowania na poziomie UE?

   Wybierz jedną odpowiedź:

   - przeciwdziałanie radykalizacji prowadzącej do działań terrorystycznych,
   - przeciwdziałanie rekrutacji online do działań terrorystycznych/sabotażowych,
   - wykrywanie i blokowanie propagandy terrorystycznej,
   - wykrywanie i blokowanie podręczników terrorystycznych/sabotażowych publikowanych w internecie,
   - rozwijanie technologii wykrywania urządzeń wykorzystywanych do przeprowadzania ataków terrorystycznych,
   - przeciwdziałanie finansowaniu terroryzmu,
   - inicjatywy edukacyjne dotyczące kultury bezpieczeństwa obiektów narażonych na ataki terrorystyczne/sabotażowe,
   - inne.

7. Co może zwiększyć poziom odporności chronionych obiektów na ataki terrorystyczne i działania sabotażowe?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

- standaryzacja bezpieczeństwa fizycznego (także procedur dotyczących pracowników ochrony),
- zadania wykonywane przez wewnętrznych audytorów bezpieczeństwa,
- testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty nadzorujące (takie jak: instytucje UE, państwowe organy kontrolne),
- rozwój inteligentnych elektronicznych systemów wykrywania zdarzeń zagrażających bezpieczeństwu,
- rozwój inicjatyw związanych z prewencją terrorystyczną jako elementem kultury bezpieczeństwa obiektu (edukacja dla bezpieczeństwa),
- poprawa współpracy między podmiotami IK a podmiotami odpowiedzialnymi za bezpieczeństwo,
- wykrywanie podejrzanych zachowań przez przeszkolonych pracowników ochrony,
- inne.

8. Ataki na infrastrukturę krytyczną są obecnie przeprowadzane przez:

Wybierz jedną odpowiedź:

- cyberprzestępców powiązanych z podmiotem państwowym,
- cyberprzestępców kierujących się wyłącznie chęcią osiągnięcia korzyści finansowych,
- tzw. insiderów powiązanych z podmiotem państwowym,
- tzw. insiderów powiązanych z działalnością terrorystyczną,
- sabotażystów powiązanych z działalnością radykalnych ruchów społecznych,
- sabotażystów powiązanych z podmiotem państwowym,
- żadne z powyższych.

UZUPEŁNIJ INFORMACJE

Wybierz jedną odpowiedź:

- przedstawiciel państwa członkowskiego UE,
- przedstawiciel instytucji lub agencji UE,
- przedstawiciel kraju będącego partnerem strategicznym projektu EU PSA.

Koniec kwestionariusza ankiety

Dr Karolina Wojtasik, MBA

Specjalista ds. bezpieczeństwa, biegły sądowy, pracownik naukowy, wiceprezes ds. naukowych Polskiego Towarzystwa Bezpieczeństwa Narodowego, główny specjalista w Rządowym Centrum Bezpieczeństwa. Podczas polskiej prezydencji w Radzie Unii Europejskiej pełni funkcję przewodniczącej grupy roboczej PROCIV CER. Zajmuje się szeroko pojętym bezpieczeństwem infrastruktury krytycznej, szczególnie w kontekście zagrożeń bezpieczeństwa fizycznego i osobowego. Ponadto analizuje działalność salafickich organizacji terrorystycznych, modus operandi sprawców zamachów terrorystycznych w UE i USA, a także publikacje instruktażowe dotyczące metod przeprowadzania ataków na ludność cywilną i obiekty. Autorka książek: *Anatomia zamachu. O strategii i taktyce terrorystów*; *Ścieżki radykalizacji dżihadystycznej. Podręcznik dla studentów socjologii, politologii i bezpieczeństwa*. Współautorka publikacji *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* oraz wielu innych publikacji związanych z terroryzmem, a także bezpieczeństwem i budowaniem odporności infrastruktury krytycznej. Twórca kanału popularnonaukowego Anatomia zamachu na YouTube.

Kontakt: karolina.wojtasik@rcb.gov.pl

Dr Damian Szlachter

Redaktor naczelny czasopisma naukowego ABW „Terroryzm – studia, analizy, prewencja". Członek komitetu sterującego unijnej grupy doradców ds. budowania odporności na zagrożenia (EU Protective Security Advisors). Ekspert narodowy w Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej (Directorate-General for Migration and Home Affairs) w ramach grupy roboczej ds. ochrony antyterrorystycznej przestrzeni publicznych (Policy Group on Public Spaces Protection). Audytor krajowy kontroli jakości w zakresie ochrony lotnictwa cywilnego (Urzędu Lotnictwa Cywilnego). Uczestnik prac kilkunastu zespołów międzyresortowych oraz grup roboczych administracji państwowej, których zadaniem było budowanie odporności na zagrożenia terrorystyczne i hybrydowe obiektów strategicznych dla bezpieczeństwa państwa oraz infrastruktury krytycznej. Członek zespołu do spraw badania wyzwań inżynierii bezpieczeństwa obiektów budowlanych infrastruktury krytycznej przy Głównym Urzędzie Nadzoru Budowlanego. Autor blisko 40 artykułów naukowych oraz współautor kilku książek i raportów specjalistycznych na temat bezpieczeństwa wewnętrznego.

Kontakt: d.szlachter@abw.gov.pl