Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 333–358

https://doi.org/10.4467/27204383TER.25.012.21515

Materiał ekspercki

Wartość unijnych projektów badawczych w ochronie infrastruktury krytycznej

The value of EU research projects in critical infrastructure protection

Małgorzata Wolbach
Polska Platforma Bezpieczeństwa Wewnętrznego
https://orcid.org/0009-0005-1837-0389

Rashel Talukder
Polska Platforma Bezpieczeństwa Wewnętrznego
https://orcid.org/0000-0003-4743-9355

Ochrona infrastruktury krytycznej (IK) i zapewnianie jej ciągłej odporności, zwłaszcza na zagrożenia hybrydowe, mają fundamentalne znaczenie dla stabilnego funkcjonowania współczesnych społeczeństw. Nieograniczony dostęp do energii, wody, żywności, opieki zdrowotnej i transportu stanowi podstawę bezpiecznego życia.

Instytucje Unii Europejskiej w ostatnich latach położyły nacisk na wzmocnienie ochrony i odporności IK. Wpływ na to miała trwająca wojna w Ukrainie, która spotęgowała obawy o bezpieczeństwo IK w całej Europie.

Do kluczowych obszarów działań UE należą:

- wprowadzenie dyrektywy CER[1] (*The Critical Entities Resilience Directive*) w sprawie odporności podmiotów krytycznych;

[1] *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.*

- wprowadzenie dyrektywy NIS 2[2] (*Network and Information Systems Directive 2*) w sprawie bezpieczeństwa sieci i informacji;
- ustalenie planu UE dotyczącego IK (zalecenia przyjęte przez Radę UE m.in. koordynują reakcje na zakłócenia funkcjonowania IK mające istotne znaczenie transgraniczne)[3];
- współpraca z NATO[4];
- wymiana informacji i dobrych praktyk m.in. przy zaangażowaniu Grupy ds. Odporności Podmiotów Krytycznych (ang. Critical Entities Resilience Group, CERG), która ułatwia współpracę i wymianę informacji między państwami członkowskimi w celu zapewnienia skutecznego wdrożenia dyrektywy CER[5].

Ponadto UE zapewnia znaczne wsparcie finansowe i strategiczne dla badań i innowacji w ochronie IK za pośrednictwem różnych programów finansowania. Pomagają one w rozwoju nowych technologii i wprowadzaniu rozwiązań w celu przeciwdziałania pojawiającym się zagrożeniom i poprawy odporności infrastruktury[6]. Unia Europejska ustanowiła kilka takich programów. Dzięki temu nie tylko wzmacnia ona ochronę swojej IK, lecz także promuje wzrost gospodarczy i zrównoważony rozwój. Jak podkreślono w rocznym sprawozdaniu z postępów we wdrażaniu wspólnych rozwiązań dotyczących przeciwdziałania zagrożeniom hybrydowym[7], finansowane przez UE projekty badawcze w zakresie bezpieczeństwa

[2] *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*.

[3] *Zalecenie Rady z dnia 25 czerwca 2024 r. w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne*.

[4] *NATO and European Union release final assessment report on resilience of critical infrastructure*, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [dostęp: 6.01.2025].

[5] *Critical infrastructure resilience at EU-level*, European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [dostęp: 6.01.2025].

[6] Tamże.

[7] *Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats*, https://defence-industry-space.ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [dostęp: 2.01.2025].

odgrywają kluczową rolę w identyfikowaniu istniejących luk oraz zwiększaniu bezpieczeństwa i odporności IK w całej UE.

W artykule przedstawiono wybrane projekty finansowane przez UE w ramach programów Horyzont 2020 i Horyzont Europa, takie jak: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, NBSINFRA, ENDURANCE i TRANSCEND. Ponadto omówiono wyzwania związane z realizacją tych projektów, w tym niespójności regulacji (odmienne krajowe regulacje prawne i niespójne interpretacje dyrektyw UE), ograniczenia finansowe i potrzebę współpracy transgranicznej. Przedstawiono zalecenia dotyczące przyszłych kierunków badań oraz podkreślono znaczenie cyberbezpieczeństwa, technologii kwantowej i wymiany w czasie rzeczywistym informacji o zagrożeniach w zwiększeniu zdolności UE do reagowania na zmieniające się zagrożenia bezpieczeństwa.

Finansowanie badań i innowacji w ochronie infrastruktury krytycznej na przykładzie programu Horyzont Europa

Jednym z unijnych programów finansowania, który wyróżnia się istotnym wkładem w badania i rozwój (mającymi na celu wzmocnienie odporności IK), jest Horyzont Europa. To flagowy program UE na lata 2021–2027 poświęcony badaniom naukowym i innowacjom, z przewidzianym budżetem w wysokości 93,5 mld euro. Wspieranie postępów w nauce i technologii staje się coraz pilniejsze, zwłaszcza w kontekście rosnącej niestabilności geopolitycznej. Wydarzenia takie jak pełnoskalowa inwazja Rosji na Ukrainę uwypukliły zagrożenia bezpieczeństwa, demokracji i globalnych łańcuchów dostaw, co uczyniło cele programu w drugiej połowie jego realizacji jeszcze bardziej istotnymi. Program Horyzont Europa wspiera międzynarodową współpracę i zwiększa wpływ badań naukowych i innowacji na kształtowanie polityki UE. Jednocześnie odgrywa ważną rolę w podejmowaniu działań związanych z pilnymi globalnymi wyzwaniami. Zapewnia zróżnicowany zestaw instrumentów – od badań podstawowych, przez przełomowe innowacje, do opracowywania i wdrażania najnowocześniejszych rozwiązań – dla rozwiązań opartych na badaniach naukowych[8].

[8] *Horizon Europe*, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [dostęp: 7.01.2025].

Plan strategiczny programu Horyzont Europa na lata 2025–2027[9] wyszczególnia najważniejsze cele strategiczne, działania priorytetowe i obszary tematyczne na ostatnich etapach jego realizacji. Ma na celu dostosowanie końcowej fazy tego programu do pojawiających się wyzwań, ewoluujących polityk UE i zmieniających się potrzeb państw członkowskich. Jest to jak dotąd najbardziej ambitny program UE w zakresie badań naukowych i innowacji, ponieważ odpowiada na globalne uwarunkowania, wspiera przełomowe rozwiązania i ułatwia dostęp do funduszy różnym grupom badawczym i firmom nie tylko z UE, a także ma rekordowy budżet. Plan ten łączy nadrzędne cele polityki UE z działaniami badawczo-rozwojowymi prowadzonymi w ramach programu Horyzont Europa. Oferuje stabilność planowania, która wykracza poza standardowy dwuletni cykl programu prac. Zapewnia społeczności badawczej przewidywalność, przy jednoczesnym zachowaniu elastyczności w celu sprostania nieoczekiwanym zmianom i wyzwaniom[10].

Projekty finansowane w ramach programu Horyzont Europa służą pozyskiwaniu nowej wiedzy, technologii i rozwiązań, spełniających określone wymagania. Są to projekty, w ramach których do współpracy są angażowani użytkownicy końcowi, naukowcy i partnerzy przemysłowi. Ten inkluzywny model zapewnia, że wyniki badań i innowacji są ściśle dostosowane do praktycznych potrzeb tych, którzy ostatecznie je wdrożą, dzięki czemu zwiększa się użyteczność projektów.

Projekty te odgrywają kluczową rolę w działaniach służących rozwiązywaniu aktualnych globalnych problemów, w tym w zwiększaniu odporności IK[11]. Wojna w Ukrainie podkreśliła znaczenie badań i innowacji w takich kwestiach, jak: dostarczanie czystej energii, zrównoważonej żywności, leków, zapewnianie zdolności obronnych i bezpieczeństwa społeczno-gospodarczego. Wysiłki te są niezbędne nie tylko do minimalizowania bezpośrednich zagrożeń, lecz także do zapewnienia długoterminowej odporności i stabilności. Projekty realizowane w ramach programu Horyzont Europa już teraz

[9] *Horizon Europe. Strategic Plan 2025–2027*, European Commission, 2024, https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1 [dostęp: 7.01.2025].

[10] *Strategic plan*, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [dostęp: 3.01.2025].

[11] *Horizon Europe. Strategic Plan 2025–2027. Analysis*, European Commission, 2023, https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en [dostęp: 9.01.2025].

przyczyniają się do pokonywania szybko zmieniających się wyzwań związanych z IK o znaczeniu transgranicznym. W przyszłości będzie to wymagało jeszcze większej innowacyjności i bardziej skoordynowanych wysiłków.

Odporność IK, w tym energetycznej, transportowej i telekomunikacyjnej, jest priorytetem dla UE, szczególnie w obliczu istnienia zagrożeń hybrydowych. Podejmowane działania, np. wdrożenie dyrektywy CER, mają na celu zapewnienie zarówno fizycznej, jak i cybernetycznej odporności IK. Badania nad bezpieczeństwem prowadzone w ramach programu Horyzont Europa wspierają te wysiłki, zapewniają nowatorskie metody planowania scenariuszy służących jako środowisko testowe dla rozwiązań powstających w ramach projektów, testów w warunkach skrajnych (ang. *stress-test*) i minimalizowania zagrożeń. Rada UE zachęciła państwa członkowskie do pełnego wykorzystania wyników badań naukowych i innowacji finansowanych przez UE. Podkreśliła tym samym ich znaczenie dla zwiększenia odporności infrastruktury. W tym kontekście projekty badawczo-rozwojowe stanowią ważny pomost między polityką a praktyką, umożliwiają UE i jej państwom członkowskim skuteczne reagowanie na wyzwania. Przez współpracę, wspieranie innowacji i odporności na zagrożenia projekty te są integralną częścią ochrony infrastruktury, bezpieczeństwa i konkurencyjności UE w coraz bardziej złożonym świecie[12].

Program Horyzont Europa wspiera badania naukowe i innowacje za pomocą programów prac, które określają możliwości finansowania różnych działań. Struktura programu opiera się na 3 zasadniczych filarach. Filar II – Globalne wyzwania i europejska konkurencyjność przemysłowa jest podzielony na 6 klastrów działań badawczo-rozwojowych. Klastry zostały zaprojektowane tak, aby zwiększyć integralność i komplementarność między obszarami tematycznymi, przy jednoczesnym zapewnieniu, że UE osiągnie znaczący i trwały wpływ na wyzwania zidentyfikowane w poszczególnych klastrach programu Horyzont Europa w stosunku do zainwestowanych środków.

Klaster 3 – Bezpieczeństwo cywilne na rzecz społeczeństwa dotyczy zwiększania bezpieczeństwa przez wspieranie wysiłków na rzecz zapobiegania zagrożeniom bezpieczeństwa: wewnętrznego, indywidualnego i społeczeństwa jako całości oraz budowania odporności na nie[13]. Obejmuje również walkę z ewoluującymi zagrożeniami, w tym terroryzmem, korupcją, przestępczością zorganizowaną i atakami hybrydowymi na IK. Celem

[12] Tamże.

[13] *Horizon Europe. Strategic Plan 2025–2027*, European Commission, 2024...

Klastra 3 jest zwiększenie zrozumienia tych zagrożeń i ich społecznych uwarunkowań oraz opracowanie zaawansowanych narzędzi do zapobiegania im, wykrywania ich i badania, a także zwiększenie zdolności UE w zakresie bezpieczeństwa. Działania dotyczące badań i innowacji są skoncentrowane również na zapewnieniu odporności IK, takiej jak systemy energetyczne, wodne, zaopatrzenia w żywność i opieki zdrowotnej, na ataki fizyczne lub cybernetyczne. Na Klaster 3 przeznaczono budżet w wysokości 1,596 mld euro.

Klaster 3 jest podzielony na 6 głównych celów, z których każdy koncentruje się na określonych priorytetach w ramach nadrzędnego tematu bezpieczeństwa cywilnego. Cel 3 – Odporna infrastruktura – jest poświęcony zwiększaniu odporności i autonomii infrastruktury zarówno krytycznej, jak i cyfrowej. Oczekiwane rezultaty opisano w następujący sposób: *Odporność i autonomia infrastruktury fizycznej i cyfrowej są zwiększone, a kluczowe funkcje społeczne są zapewnione dzięki skuteczniejszemu zapobieganiu, gotowości i reagowaniu, głębszemu zrozumieniu powiązanych aspektów ludzkich, społecznych i technologicznych oraz rozwojowi najnowocześniejszych możliwości dla operatorów infrastruktury*[14].

Cel ten jest ściśle powiązany z Celem 6 – Wzmocnione badania i innowacje w zakresie bezpieczeństwa – który zapewnia badania, postęp technologiczny i nowatorskie rozwiązania, stanowiące podstawę i wsparcie Celu 3. Razem tworzą one uzupełniające się ramy dla realizacji priorytetów bezpieczeństwa UE, zwiększają ochronę IK przy jednoczesnym wzmacnianiu odporności społecznej i gospodarczej. Mają one praktyczne zastosowania w związku z wyposażaniem operatorów infrastruktury w zaawansowane narzędzia i możliwości skutecznego reagowania na wyzwania.

Przykładem realizacji założeń Celu 3 było zaproszenie do składania wniosków w ramach programu Odporna infrastruktura (HORIZON-CL3-2024) o finansowanie w 2024 r.[15] badań naukowych i innowacji mających na celu wzmocnienie odporności infrastruktury. Tematy finansowane w ramach HORIZON-CL3-2024 to:

- **INFRA01**: *Lepsza gotowość i reagowanie na zakłócenia na dużą skalę w europejskiej infrastrukturze*;

[14] *Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024)*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, s. 8 [dostęp: 10.01.2025]. Tłumaczenia w artykule pochodzą od redakcji (dop. red.).

[15] Tamże.

• **INFRA02:** *Odporne i bezpieczne obszary miejskie i inteligentne miasta*.

Szczegóły dotyczące tych tematów, w tym rodzaj działań i oczekiwane wyniki, podsumowano w tabeli 1.

Tabela 1. Podtematy programu Odporna infrastruktura (HORIZON-CL3-2024).

Podtemat INFRA01	**HORIZON-CL3-2024-INFRA-01-01: Temat otwarty**
Rodzaj działania	Działania w zakresie innowacji
Oczekiwane wyniki	Oczekuje się, że wyniki projektów przyczynią się do osiągnięcia wszystkich poniższych rezultatów: • zwiększona odporność operatorów IK na zagrożenia naturalne i spowodowane przez człowieka; • ulepszone techniki monitorowania, oceny ryzyka, jego prognozowania, ograniczania i modelowania mające na celu zwiększenie odporności IK, walidację scenariuszy obejmujących wiele zagrożeń, tworzenie interaktywnych map zagrożeń na podstawie obserwacji Ziemi i innych źródeł danych
Podtemat INFRA02	**HORIZON-CL3-2024-INFRA-01-02: Odporne i bezpieczne planowanie urbanistyczne oraz nowe narzędzia dla jednostek terytorialnych UE**
Rodzaj działania	Działania w zakresie innowacji
Oczekiwane wyniki	Oczekuje się, że wyniki projektów przyczynią się do osiągnięcia wszystkich poniższych rezultatów: • ocena odporności środowiska miejskiego i podmiejskiego, identyfikacja słabych punktów i zalecenia dotyczące zmian w procesach organizacyjnych; • tworzenie nowych narzędzi i efektywnych kosztowo ulepszeń bezpieczeństwa infrastruktury miejskiej z możliwością łączenia i współdzielenia złożonych systemów bezpieczeństwa, z uwzględnieniem ograniczonych budżetów władz lokalnych; • większa skuteczność sił bezpieczeństwa i służb ratunkowych (policji, straży pożarnej, ratowników medycznych itp.) z korzyścią dla obywateli i mieszkańców Europy; • promowanie najlepszych praktyk, stworzenie unijnego narzędzia/rozwiązania wspierającego podejmowanie decyzji oraz rozpowszechnianie skutecznych narzędzi i możliwości wśród podmiotów na różnych terytoriach UE, niezależnie od ich wielkości i lokalizacji

Podtemat INFRA02	**HORIZON-CL3-2024-INFRA-01-03: Zaawansowana analiza danych w czasie rzeczywistym wykorzystywana do zapewnienia odporności infrastruktury**
Rodzaj działania	Działania w zakresie badań i innowacji
Oczekiwane wyniki	Oczekuje się, że wyniki projektów przyczynią się do osiągnięcia wszystkich poniższych rezultatów: • ulepszone możliwości identyfikacji ryzyka i zdarzeń awaryjnych w sieciach infrastruktury i inteligentnych miastach przez analizę w czasie rzeczywistym (w tym dużych zbiorów danych) przez podmioty publiczne i prywatne za pośrednictwem zabezpieczonych i zaufanych platform oraz wzajemnie połączonych systemów, w których współpraca opiera się na jasnych ramach prawnych i politycznych; • narzędzia i procesy ułatwiające interesariuszom identyfikację, analizę, ocenę i ciągłe monitorowanie ryzyka oraz zwiększanie zdolności adaptacyjnych do nieoczekiwanych zdarzeń z wyprzedzeniem przez umożliwienie analizy różnych źródeł danych (np. audio, wideo, mediów społecznościowych, treści internetowych, informacji przestrzennych, danych generowanych przez czujniki lub maszyny); • szybka i ciągła identyfikacja, klasyfikacja i śledzenie w czasie rzeczywistym niebezpiecznych czynników, zanieczyszczeń lub anomalii w sieciach infrastruktury i łańcuchach dostaw; • interoperacyjne interfejsy i lepsza współpraca między systemami wykrywania i reagowania na operacje infrastrukturalne, krajowymi/unijnymi centrami zarządzania ryzykiem/koordynacji i sprzętem pierwszej pomocy w celu umożliwienia zdalnych operacji na miejscu zdarzenia z uwzględnieniem wiedzy obywateli; • zwiększona cyberodporność przemysłowych sieci xG i danych w chmurze obejmujących określone domeny infrastruktury; • ulepszona zdolność do mapowania w czasie rzeczywistym źródeł ryzyka, które mogłyby zagrozić infrastrukturze sieciowej wspieranej przez obserwację Ziemi i dane geolokalizacyjne. Jeśli analiza obejmuje przetwarzanie danych osobowych, należy rozważyć uwzględnienie oceny związanego z nim ryzyka lub wpływu na prywatność osób fizycznych i społeczeństwa.

Źródło: *Horizon Europe. Work Programme 2023–2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024)*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, s. 91–97 [dostęp: 10.01.2025].

Na program Odporna infrastruktura przydzielono w 2024 r. orientacyjny budżet w wysokości 16 mln euro[16]. Termin składania wniosków upłynął 20 listopada 2024 r. Z 79 wniosków, które złożono, tylko 3 zostaną rozpatrzone pozytywnie, a ich realizacja rozpocznie się we wrześniu 2025 r. To pokazuje nie tylko konkurencyjność konkursu, lecz także ograniczenie ogólnego budżetu przeznaczonego na badania i innowacje w dziedzinie ochrony IK.

Przegląd wybranych inicjatyw w zakresie badań naukowych i innowacji finansowanych w ramach programów Horyzont 2020 i Horyzont Europa

W ramach inicjatyw finansowanych przez UE w dziedzinie ochrony IK są rozwijane zarówno rozwiązania technologiczne, jak i nietechnologiczne. Inicjatywy te wzmacniają jednocześnie współpracę europejską. Celem przedstawienia wybranych przez autorów inicjatyw jest pokazanie możliwości, jakie projekty oferują interesariuszom, w tym instytucjom badawczym napędzającym innowacje, przedsiębiorstwom opracowującym najnowocześniejsze rozwiązania w zakresie bezpieczeństwa, organizacjom publicznym wdrażającym polityki oraz właścicielom i operatorom IK odpowiedzialnym za zapewnienie ciągłości usług.

EU-HYBNET

(Empowering a Pan-European Network to Counter Hybrid Threats, pol. Wzmocnienie Ogólnoeuropejskiej Sieci Przeciwdziałania Zagrożeniom Hybrydowym)[17]

Projekt finansowany z unijnego programu badań i innowacji Horyzont 2020 (poprzednika programu Horyzont Europa). Jest to pierwsza inicjatywa UE, która łączy praktyków bezpieczeństwa, naukowców, podmioty branżowe oraz organizacje biznesowe i pozarządowe w celu współpracy oraz identyfikacji i analizy wspólnych wyzwań i wymagań w zakresie przeciwdziałania zagrożeniom hybrydowym.

[16] *Resilient Infrastructures*, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [dostęp: 10.01.2025].

[17] *Empowering a Pan-European Network to Counter Hybrid Threats*, European Commission, https://cordis.europa.eu/project/id/883054 [dostęp: 13.01.2025].

Głównymi celami projektu EU-HYBNET są:

1. Stworzenie i rozwój sieci europejskich organizacji przeciwdziałających zagrożeniom hybrydowym oraz zapewnienie długoterminowej stabilności sieci.
2. Określenie wspólnych wymagań w celu wypełnienia luk w wiedzy, zaspokojenia potrzeb w zakresie wydajności i zwiększenia możliwości badań, innowacji i szkoleń dotyczących zagrożeń hybrydowych.
3. Monitorowanie rozwoju działalności badawczej i innowacyjnej w odniesieniu do zagrożeń hybrydowych.
4. Określenie priorytetów w zakresie wdrażania innowacji i uprzemysłowienia oraz w celu zwiększenia roli europejskiej sieci w skutecznym przeciwdziałaniu zagrożeniom hybrydowym.
5. Ustanowienie warunków dla zwiększonej interakcji między praktykami bezpieczeństwa, przedstawicielami sektora przemysłu i środowiskiem akademickim w celu wspierania rzeczowego dialogu i zwiększenia liczby członków sieci.
6. Wspieranie budowania potencjału i wymiany wiedzy na temat przeciwdziałania zagrożeniom hybrydowym.
7. Stworzenie podstaw do skutecznego współdziałania istniejących europejskich, krajowych i regionalnych sieci praktyków i innych podmiotów przeciwdziałających zagrożeniom hybrydowym.

Projekt obejmuje 4 podstawowe tematy, aby zapewnić spójność jego wyników i ułatwić skupienie się na wszystkich domenach zagrożeń hybrydowych (w tym IK). Są to:

1. Przyszłe trendy zagrożeń hybrydowych.
2. Cyberbezpieczeństwo i technologie przyszłości.
3. Odporna ludność cywilna, administracja lokalna i krajowa.
4. Informacja i komunikacja strategiczna.

W ramach tych tematów szczególny nacisk kładzie się na interfejsy między domenami, zidentyfikowane i zdefiniowane przez Komisję Europejską i Połączone Centrum Badawcze UE (ang. EU Joint Research Centre). Zapewnia to niezbędne wsparcie dla działań badawczych i innowacyjnych w domenach zagrożeń hybrydowych uznanych za kluczowe dla dostarczania rozwiązań w trakcie cykli projektowych.

Pomimo tego, że projekt skończył się w kwietniu 2025 r., sieć stale się rozrasta (obecnie składa się z ponad 150 organizacji z krajów UE, Ukrainy i Wielkiej Brytanii)[18].

EU-CIP

(European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection, pol. Europejskie Centrum Wiedzy i Testowania Polityk w Zakresie Ochrony Infrastruktury Krytycznej)[19]

To inicjatywa również networkingowa, ale skupiająca się wyłącznie na ochronie IK. Trwa od października 2022 r. do września 2025 r.

Głównym celem EU-CIP jest ustanowienie unikalnego ogólnoeuropejskiego centrum wiedzy na temat odpornej infrastruktury, które umożliwi decydentom kształtowanie i tworzenie polityk opartych na danych i dowodach, przy jednoczesnym zwiększaniu zdolności innowacyjnych i konkurencyjności operatorów IK, władz, naukowców i innowatorów. W tym kierunku projekt rozwija utworzony i obsługiwany przez partnerów projektu European Cluster for Securing Critical Infrastructures, ECSCI (pol. Europejski Klaster na rzecz Zabezpieczenia Infrastruktury Krytycznej) – najważniejsze europejskie centrum wiedzy w zakresie badań i innowacji na rzecz bezpieczeństwa i odporności IK. Klaster ECSCI skupia 22 projekty, które współpracują w zakresie zapewniania odporności IK. W celu stworzenia ogólnounijnego centrum wiedzy EU-CIP wykorzystuje potencjał, organizację, społeczność i osiągnięcia klastra ECSCI.

EU-CIP oferuje zaawansowane możliwości analizy informacji w celu kształtowania polityki opartej na dowodach i wsparcia innowacji, by ułatwić wykorzystanie i komercjalizację wyników badań. Aby zmaksymalizować wpływ swoich działań, EU-CIP tworzy i rozwija dynamiczny ekosystem zainteresowanych i zaangażowanych interesariuszy wokół analizy informacji i usług wsparcia innowacji.

Główne cele EU-CIP:

1. Analiza: zwiększenie zdolności analitycznych w Europie w zakresie badań, technologii i polityk – wspieranie rozwoju polityki i innowacji opartego na danych. EU-CIP przyjmuje metodologię gromadzenia danych, monitorowania i analizy informacji, polegającą

[18] *EU-HYBNET*, https://euhybnet.eu/ [dostęp: 13.01.2025].

[19] *European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection*, European Commission, https://cordis.europa.eu/project/id/101073878 [dostęp: 13.01.2025].

na nieustannym gromadzeniu, analizie, selekcji, wyodrębnianiu i prezentowaniu informacji i spostrzeżeń na temat odporności infrastruktury. W ramach tego celu EU-CIP prezentuje prognozy i spostrzeżenia na temat luk w wiedzy, rozwiązań i technologii, a także wyników badań i praktyk.

2. Wzmocnienie: maksymalizacja wpływu działań badawczo-rozwojowych w zakresie ochrony IK (ang. c*ritical infrastructure protection*, CIP) i odporności IK (ang. *critical infrastructure resilience*, CIR) w Europie. Projekt zapewnia usługi wsparcia innowacji i walidacji rozwiązań dla wyników badań w obszarach odpornej infrastruktury (CIP/CIR). Wykorzystuje wyniki analityczne filaru EU-CIP-ANALYSIS w celu zidentyfikowania luk w istniejących rozwiązaniach i obszarach IK o znacznym potencjale innowacyjnym. W związku z tym oferowane przez EU-CIP usługi będą wspierać innowatorów CIP/CIR (w tym małe i średnie przedsiębiorstwa) w ich działaniach związanych z wykorzystywaniem i komercjalizacją wyników badań. Ponadto projekt oferuje zwirtualizowane środowisko testowe do eksperymentowania z opartymi na standardach rozwiązaniami CIP/CIR i systemami certyfikacji, wraz z odpowiednimi procesami walidacji i oceny obejmującymi zaangażowanie zainteresowanych stron.
3. Stworzenie ekosystemu: ustanowienie centrum wiedzy (ang. Knowledge Hub) i stworzenie wokół wyników projektu dynamicznego ekosystemu zainteresowanych i zaangażowanych interesariuszy. EU-CIP ustanawia i rozwija ogólnounijny ekosystem interesariuszy CIP/CIR, obejmujący 27 państw UE i inne kraje Europejskiego Obszaru Gospodarczego. Ekosystem ułatwia dostęp do wiedzy, wyników, usług i infrastruktury opracowanych w poprzednich celach, a także zaangażowanie zainteresowanych stron w rozwój innowacji i kształtowanie polityki w ramach inicjatyw UE (np. projektów badawczych, inicjatyw technologicznych, inicjatyw politycznych). Centrum wiedzy zapewnia dostęp (przez właściwą infrastrukturę cyfrową) do zasobów wiedzy projektu, w tym infrastruktury i wyników opracowanych w poprzednich celach. Pozwala na współpracę między różnymi zainteresowanymi stronami.

Oczekiwane rezultaty EU-CIP są następujące:

- zwiększona odporność IK – projekt przez kompleksową analizę umożliwia identyfikowanie i eliminowanie luk;

- rozwój polityki oparty na dowodach – projekt przez agregację i analizę wielu różnych danych wspiera tworzenie bardziej skutecznych polityk dla CIP/CIR;
- zwiększanie innowacyjności i konkurencyjności – projekt przez zaawansowane możliwości analizy informacji i usług wsparcia innowacji zwiększa możliwości innowatorów, zwłaszcza w zakresie wykorzystywania i komercjalizacji wyników badań;
- wspieranie ekosystemu współpracy – ustanowienie dynamicznego ekosystemu interesariuszy ułatwia dzielenie się wiedzą, współpracę i współtworzenie rozwiązań, co zwiększa zbiorową zdolność do sprostania wyzwaniom CIP/CIR[20].

VIGIMARE

(Vigilant Maritime Surveillance of Critical Submarine Infrastructure, pol. Uważny nadzór morski nad podwodną infrastrukturą krytyczną)[21]

To projekt typu działania innowacyjnego – koncentruje się na opracowywaniu rozwiązań podwyższających poziom gotowości technologicznej (ang. Technology Readiness Level, TRL).

W ramach projektu opracowano innowacyjne rozwiązanie umożliwiające poprawę bezpieczeństwa i ograniczenia ryzyka ataków fizycznych i cyberzagrożeń. Celem projektu jest identyfikacja wczesnych sygnałów ostrzegawczych i wsparcie analizy przez mapowanie systemów podwodnych, ocenę słabych punktów i tworzenie świadomości sytuacyjnej w czasie rzeczywistym, zarówno nawodnej, jak i podwodnej IK. Projekt przyjmuje systematyczne podejście do wzmocnienia europejskiego sektora IK podmorskich kabli telekomunikacyjnych, energetycznych i gazociągów. Analiza, a także system VIGIMARE będą wspierać operatorów IK sieci podwodnej przez zwiększenie jej odporności na ataki i uszkodzenia.

Cele VIGIMARE:

- zapewnienie operatorom IK środowiska wymiany informacji w celu przeciwdziałania zagrożeniom dla IK okrętów podwodnych UE;
- zwiększenie odporności operatorów IK na zagrożenia fizyczne, cybernetyczne i hybrydowe przez wdrożenie środków zapobiegających ryzyku i ograniczających je;

[20] *EU-CIP*, https://www.eucip.eu/ [dostęp: 13.01.2025].

[21] *Vigilant Maritime Surveillance of Critical Submarine Infrastructure*, European Commission, https://cordis.europa.eu/project/id/101168016 [dostęp: 14.01.2025].

- wzmocnienie świadomości sytuacyjnej operatorów IK i państw członkowskich UE w odniesieniu do europejskich obszarów morskich, zarówno wodnych, jak i lądowych, w celu rozpoznawania fizycznych (spowodowanych przez człowieka i naturalnych), cybernetycznych i hybrydowych ataków i incydentów, co umożliwi lepsze planowanie odpowiedzi na atak oraz działań naprawczych;
- wsparcie państw członkowskich UE w wypełnianiu wymogów dyrektyw CER i NIS 2. Wyniki tego projektu wprowadzą również wspólne środowisko wymiany informacji (ang. *common information sharing enviroment*, CISE) Europejskiej Agencji Bezpieczeństwa Morskiego (European Maritime Safety Agency, EMSA) do tego nowego obszaru zainteresowań. Rozwiązanie zaproponowane w ramach projektu VIGIMARE zostanie przetestowane w warunkach skrajnych, z wykorzystaniem danych z rzeczywistych incydentów i zatwierdzone na 3 różnych europejskich obszarach morskich – Morzu Śródziemnym, Morzu Irlandzkim i Morzu Bałtyckim – w celu promowania jego cennych wyników w społeczeństwie europejskim[22].

TESTUDO

(Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention, pol. Wykorzystanie rojów autonomicznych pojazdów bezzałogowych w celu przewidywania zagrożeń i zapobiegania im)[23]

Ten projekt ma na celu wzmocnienie nadzoru nad europejską IK i jej ochrony przy użyciu autonomicznych systemów i zaawansowanych technologii, aby zapewnić ich solidne działanie.

Cele TESTUDO:

- wykorzystanie zaawansowanych pojazdów bezzałogowych wraz z istniejącym sprzętem do ciągłego monitorowania nawet w trudnych warunkach i na odległych terytoriach;
- włączenie najnowocześniejszych technologii wykrywania niebezpiecznych zdarzeń, zapobiegania im i przewidywania ich, aby zwiększyć możliwości w tym zakresie;

[22] *VIGIMARE,* https://vigimare.eu/ [dostęp: 15.01.2025].

[23] *Autonomous Swarm of Heterogeneous resourcse in infrastructure protection via threat prediction and prevention,* European Commission, https://cordis.europa.eu/project/id/101121258 [dostęp: 15.01.2025].

- identyfikacja zasobów potrzebnych do realizacji działań operacyjnych za pomocą technik optymalizacji, przyczyniająca się do całkowitej autonomii systemu;
- zebranie multidyscyplinarnej grupy składającej się ze specjalistów w zakresie: modeli opartych na sztucznej inteligencji, zagrożeń chemicznych, biologicznych, radiacyjnych, nuklearnych (ang. *chemical, biological, radiological, nuclear*, CBRN), zagrożeń cyberbezpieczeństwa, cyfrowych bliźniaków (cyfrowej repliki fizycznych obiektów, procesów i systemów) oraz IK, w celu opracowania innowacyjnych rozwiązań służących ochronie różnych obiektów IK funkcjonujących w długiej perspektywie czasowej i całkowicie autonomicznie[24].

NBSINFRA

(Citynature-based Solutions Integration to Local Urban Infrastructure Protection for a Climate Resilient Society, pol. Integracja rozwiązań opartych na przyrodzie z lokalną infrastrukturą miejską w celu ochrony społeczeństwa odpornego na zmiany klimatu)[25]

To pionierska europejska inicjatywa, która wspiera wzmocnienie ochrony lokalnej miejskiej IK przed zagrożeniami naturalnymi i spowodowanymi przez człowieka. Polega na współprojektowaniu i współtworzeniu rozwiązań opartych na przyrodzie (ang. *Nature-based Solutions*, NbS) w celu zbudowania społeczeństwa odpornego na zmiany klimatu. NBSINFRA wykazuje, że NbS są: a) technicznie wykonalne w zakresie ochrony IK przed zagrożeniami, b) społecznie akceptowalne i opłacalne w skali lokalnej, c) zdolne do skutecznego wzmocnienia pozycji społeczności przez zwiększenie ich odporności ekologicznej, społecznej i gospodarczej.

NBSINFRA ustanawia 5 reprezentatywnych regionów europejskich z taką samą liczbą tzw. laboratoriów miejskich (ang. City Labs) w: Fingal (Irlandia), Kolonii (Niemcy), Ruse (Bułgaria), Aveiro (Portugalia), Pradze (Czechy). Laboratoria ocenią opłacalność rozwiązań NbS w ochronie lokalnej infrastruktury i zmaksymalizują ich wpływ na nią. Rozwiązania te będą własnością obywateli i będą współtworzone przez użytkowników końcowych i zarządców oraz społeczeństwo obywatelskie.

[24] *TESTUDO*, https://testudo-project.eu/ [dostęp: 15.01.2025].

[25] *Citynature-based Solutions integration to local urban infrastructure protection for a climate resilient society*, https://cordis.europa.eu/project/id/101121210 [dostęp: 17.01.2025].

NBSINFRA zapewnia zestaw narzędzi, które zainteresowane strony i społeczeństwo mogą wykorzystać do porównania i wyboru najbardziej skutecznych NbS dla ochrony lokalnej IK. Głównym celem jest zwiększenie jej ochrony przed zagrożeniami przez współprojektowanie, współmonitorowanie i współtworzenie NbS służących rozwojowi zrównoważonego i odpornego społeczeństwa[26].

ENDURANCE

(Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe, pol. Strategie i usługi na rzecz zwiększonej odporności na zakłócenia i współpracy w Europie)[27]

Projekt ENDURANCE ma na celu wzmocnienie w Europie sektorów takich jak energetyka, ochrona zdrowia, woda pitna. Zapewnia zgodność z europejskimi regulacjami, zwłaszcza z dyrektywami CER i NIS 2, daje operatorom i organom niezbędne narzędzia, strategie i wiedzę w celu minimalizowania ryzyka i skutecznego usuwania skutków zakłóceń.

Cele ENDURANCE:

- wzmocnienie na wszystkich poziomach strategicznej współpracy między interesariuszami IK z różnych sektorów i krajów;
- opracowanie zbiorów danych, rejestrów, metodologii, technologii i usług (na poziomie TRL 6-7) w celu bezpiecznego udostępniania i przetwarzania danych istotnych dla CER, wspólnej oceny istotnych zagrożeń i odporności oraz testowania gotowości w warunkach skrajnych na dużą skalę;
- zapewnienie zharmonizowanej i pragmatycznej strategii na rzecz ciągłości połączonych podstawowych usług[28].

[26] *NBSINFRA*, https://nbsinfra.eu/ [dostęp: 17.01.2025].

[27] *Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe*, European Commission, https://cordis.europa.eu/project/id/101168007 [dostęp: 17.01.2025].

[28] *ENDURANCE*, https://endurance-horizon.eu/ [dostęp: 17.01.2025].

TRANSCEND

(Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption, pol. Odporność transportu na zdarzenia cybernetyczne i niecybernetyczne w celu zapobiegania zakłóceniom sieci)[29]

Projekt TRANSCEND ma na celu:

- zapewnienie operatorom transportu towarowego zintegrowanego zestawu zaawansowanych narzędzi, wytycznych i rozwiązań technologicznych w celu zmniejszenia ryzyka dla sieci i usług transportowych, które może wynikać ze zdarzeń cybernetycznych i niecybernetycznych;
- zwiększenie ochrony i odporności systemów transportowych przed zagrożeniami fizycznymi, cybernetycznymi i hybrydowymi.

Aby zrealizować te cele, w ramach projektu zostanie zapewniona platforma cyfrowa do monitorowania zagrożeń i ryzyka, a także zostanie opracowanych 5 rzeczywistych projektów pilotażowych. Są one podzielone na 3 główne: pilotażowy port lotniczy w Luksemburgu, pilotażowy terminal kolejowo-drogowy w Bolonii we Włoszech i pilotażowe wdrożenie portu trimodalnego w Hiszpanii; oraz na 2 naśladowców: port rzeczny w Budapeszcie i autostrada Egnatia w Grecji.

Wyniki projektu zostaną zintegrowane w Wieżę Kontroli, czyli platformę cyfrową z wbudowaną inteligencją biznesową (ang. *Business Intelligence*), zapewniającą interesariuszom wspólny i ciągły wgląd w zagrożenia i ryzyko przez poprawę przepływu wiedzy w organizacjach i między nimi. Aby przetestować skuteczność tego podejścia, z rozwiązaniami metodologicznymi i technologicznymi będzie eksperymentować 5 różnych obiektów transportowej IK, 3 w roli liderów i 2 naśladowców[30].

Wyzwania i doświadczenia związane z realizacją projektów

Konkurencja o fundusze unijne jest duża, a pozyskanie takich środków stanowi cenną okazję do międzynarodowej współpracy. Wdrażanie kolejnych unijnych projektów badawczych i innowacyjnych cieszy się zatem dużym uznaniem w środowisku naukowym. W porównaniu z grantami krajowymi, które czasami zawierają komponent międzynarodowy, projekty unijne

[29] *Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption,* European Commission, https://cordis.europa.eu/project/id/101168023 [dostęp: 17.01.2025].

[30] *TRANSCEND*, https://www.transcend-logistics.eu/ [dostęp: 17.01.2025].

zakładają współpracę między uczestnikami z krajów europejskich, reprezentujących różne organizacje, w tym uniwersytety, instytucje badawcze, firmy prywatne, podmioty sektora publicznego i organizacje pozarządowe. Średni budżet projektu w wysokości 3–5 mln euro może wydawać się znaczny, ale w ciągu 3 lat realizacji projektu musi on zostać rozdzielony między konsorcja składające się z 10–15 lub nawet więcej partnerów. Biorąc pod uwagę wysokie – zdaniem autorów – oczekiwania co do wyników projektu, a także poziom inflacji w Europie w ostatnich latach, dostępny obecnie budżet może już nie być tak korzystny.

Po przeanalizowaniu tych wszystkich czynników wyciągnięto wnioski i zidentyfikowano kilka wyzwań. W koordynacji między państwami członkowskimi jednym z wyzwań są odmienne regulacje prawne i interpretacje dyrektyw UE. Mimo że UE zapewnia wspólne dyrektywy dotyczące CIP, cyberbezpieczeństwa i zarządzania danymi, to ich wdrażanie i interpretacja różnią się w poszczególnych państwach członkowskich. Niektóre kraje ściśle dostosowują przepisy krajowe do dyrektyw UE, podczas gdy inne pozostawiają sobie większy margines swobody lub mają opóźnienia w ich transpozycji do prawa krajowego. Na przykład dyrektywy CER i NIS 2 mają na celu stworzenie wspólnych ram bezpieczeństwa, ale ich praktyczne egzekwowanie różni się w poszczególnych krajach[31]. Te niespójności regulacji mogą prowadzić do opóźnień w realizacji projektów i komplikacji we wspólnych inicjatywach państw członkowskich.

Dodatkowym wyzwaniem może być odmienne postrzeganie przez nie zagrożeń i priorytetów krajowych, które również mają wpływ na projekty UE. Przekłada się to na zaangażowanie tych państw w ułatwianie wymiany doświadczeń i pogłębianie wiedzy na temat zagrożeń hybrydowych, a także w prowadzenie międzynarodowych ćwiczeń obejmujących scenariusze hybrydowe[32]. Ta rozbieżność jest szczególnie widoczna w przypadku Rosji i Chin, w odniesieniu do których państwa członkowskie UE zajmują odmienne stanowiska. Na przykład zarówno rządy, jak i społeczeństwa w Polsce i krajach bałtyckich uważają Chiny za zagrożenie cyberbezpieczeństwa, a Rosję za agresora po ataku na Ukrainę i ograniczają z nimi współpracę,

[31] *The Commission calls on 23 Member States to fully transpose the NIS2 Directive*, European Commission, 28.11.2024, https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive [dostęp: 29.01.2025].

[32] P. Szymański, *NATO i Unia Europejska wobec zagrożeń hybrydowych*, Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 7.02.2025].

podczas gdy niektóre rządy w państwach członkowskich (np. Węgry i Słowacja) prowadzą intensywną współpracę gospodarczą i infrastrukturalną z Chinami i Rosją, szczególnie w dziedzinie energetyki. Ten brak ujednoliconej oceny ryzyka utrudnia pełne wdrożenie wspólnych środków ochronnych i zapewnienie spójnych standardów bezpieczeństwa infrastruktury w całej UE.

Doświadczenia z realizacji projektów UE, potwierdzone obserwacjami autorów artykułu, wskazują, że kraje członkowskie mają różne możliwości skutecznego wdrażania projektów ochrony IK z powodu odmiennych zasobów finansowych, technologicznych i ludzkich. Na lepszej pozycji są kraje Europy Zachodniej i Północnej. Kraje Europy Wschodniej i Południowej z kolei borykają się z większymi ograniczeniami budżetowymi, co prowadzi do wolniejszego wdrażania nowych technologii bezpieczeństwa i modernizacji infrastruktury.

Problemem w wielu projektach UE w zakresie bezpieczeństwa jest złożoność współpracy transgranicznej, w tym wymiana danych. Należy jednak podkreślić, że zarówno Komisja Europejska, jak i państwa członkowskie wdrażają specjalne mechanizmy i tworzą instytucje (powołują nowe struktury w ramach istniejących instytucji lub nowe instytucje) wspierające ten proces w obszarze ochrony IK. Są to m.in. dyrektywy CER i NIS 2, Europejski Program Ochrony Infrastruktury Krytycznej (European Programme for Critical Infrastructure Protection, EPCIP), Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (European Cybersecurity Competence Centre, ECCC), a także działania w zakresie cyberbezpieczeństwa prowadzone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity, ENISA). Wszystkie te mechanizmy i instytucje powinny wspierać zarówno realizację projektów, jak i wykorzystanie ich wyników.

Inna grupa wyzwań wiąże się z równoważeniem innowacyjności z praktycznością. Projekty finansowane przez UE koncentrujące się na ochronie IK (zwłaszcza w ramach Klastra 3 programu Horyzont Europa) mają na celu wprowadzenie rozwiązań innowacyjnych, aby zwiększyć bezpieczeństwo, odporność i wydajność. Wdrażanie najnowocześniejszych rozwiązań jest jednak trudne z powodu m.in. wykonalności technologicznej, ograniczeń regulacyjnych, zagrożeń bezpieczeństwa, braku opłacalności i możliwości zastosowania w praktyce.

Duża część projektów badawczych koncentruje się na opracowywaniu zaawansowanych technologicznie rozwiązań, takich jak wykrywanie zagrożeń oparte na sztucznej inteligencji, zaawansowane narzędzia cyberbezpieczeństwa, szyfrowanie kwantowe. Wiele innowacji jednak znajduje się w fazie eksperymentalnej i wymaga miesięcy, a nawet lat testów i kalibracji, zanim będzie można je bezpiecznie zintegrować z istniejącą infrastrukturą. Infrastruktura krytyczna działa przez wiele lat (tzw. długi cykl życia), co oznacza, że nowe technologie muszą być kompatybilne ze starszymi systemami, a to często jest trudne i kosztowne. Niektóre pojawiające się technologie (np. sztuczna inteligencja; blockchain; systemy bezpieczeństwa internetu rzeczy, ang. Internet of Things, IoT) mogą nie być jeszcze wystarczająco dojrzałe do rzeczywistego zastosowania w środowiskach wysokiego ryzyka. Zatem innowacje, chociaż niezbędne, muszą być praktyczne, skalowalne i sprawdzone w rzeczywistych warunkach, zanim zostaną wdrożone.

Nawet jeśli istnieją techniczne możliwości wprowadzenia innowacji, to mogą pojawić się przeszkody prawne i regulacyjne[33]. Unijne i krajowe przepisy dotyczące cyberbezpieczeństwa, ochrony danych i bezpieczeństwa IK mogą spowalniać lub ograniczać wykorzystanie nowych technologii. Różne interpretacje prawne w poszczególnych państwach członkowskich powodują niespójności, co utrudnia wdrożenie jednego innowacyjnego rozwiązania w wielu krajach. Rządy i operatorzy muszą się upewnić, że nowe technologie nie stworzą dodatkowego ryzyka, co w praktyce oznacza długie procesy zatwierdzania, testowania i oceny bezpieczeństwa. W rezultacie nawet najbardziej zaawansowane innowacje mogą potrzebować lat, aby organy regulacyjne wyraziły na nie zgodę.

Dodatkowym wyzwaniem jest to, że innowacje często wiążą się z wysokimi kosztami początkowymi na rozwój, testowanie i wdrażanie nowych technologii. Ponadto IK, taka jak sieci energetyczne, sieci transportowe, systemy wodne i systemy telekomunikacyjne, często opiera się na technologiach sprzed dziesięcioleci. W związku z tym wykonalność technologiczna nie zawsze przekłada się na szybkie praktyczne wdrożenie ze względu na brak kompatybilności i względy operacyjne.

Nowe technologie oprócz tego, że mogą zwiększyć bezpieczeństwo, powodują również luki w zabezpieczeniach. Zaawansowane technologie

[33] *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*, OECD Publishing, Paris 2021. https://doi.org/10.1787/8fa190b5-en.

(np. IoT, sztuczna inteligencja, przetwarzanie w chmurze) są celem cyberprzestępców i podmiotów państwowych i wymagają ciągłych aktualizacji i poprawek bezpieczeństwa[34]. Co więcej, niektóre innowacje mogą opierać się na sprzęcie lub oprogramowaniu pochodzącym z krajów spoza UE, co budzi obawy o bezpieczeństwo danych, backdoory i ingerencję z zagranicy.

Innowacje w zakresie ochrony IK wymagają współpracy między rządami, operatorami z sektora prywatnego i społeczeństwem. Często jednak pojawiają się opory i sceptycyzm wobec nowych technologii, związane z brakiem zaufania do automatyzacji i sztucznej inteligencji oraz obawy o prywatność. Technologie, takie jak zabezpieczenia biometryczne i inteligentny monitoring często spotykają się ze sprzeciwem opinii publicznej ze względu na obawy przed masową inwigilacją i niewłaściwym wykorzystaniem danych. W niektórych krajach, np. w Niemczech, Francji czy Polsce, społeczeństwo sprzeciwia się zaangażowaniu prywatnych firm technologicznych lub podmiotów zagranicznych w projekty IK. Jeśli interesariusze nie ufają technologii, nie będą wspierać jej wdrożenia. Głosy obywateli są istotne, ponieważ bierze się je pod uwagę przy kształtowaniu polityk dotyczących technologii, które mają znaczący wpływ na społeczeństwo[35].

Przyszłe kierunki badań UE nad ochroną infrastruktury krytycznej

Przyszłe kierunki badań UE nad ochroną IK zdecydowanie muszą uwzględniać wyzwania mogące się pojawić w przyszłości. Na podstawie badań i publikacji, w tym wyników projektu EU-HYBNET i raportów Europejskiego Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE), autorzy wskazują następujące obszary jako najbardziej istotne w perspektywie krótko- i średnioterminowej:

- cyberataki (w tym ataki oparte na sztucznej inteligencji i brak zabezpieczeń IoT);

[34] *The cybersecurity challenges of legacy OT and how to manage them*, Control Engineering, 21.03.2024, https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them [dostęp: 7.02.2025].

[35] K. Kieslich, M. Lünich, *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, https://arxiv.org/abs/2401.13605v3 [dostęp: 7.02.2025]. https://doi.org/10.48550/arXiv.2401.13605.

- technologia kwantowa (zwłaszcza przejście na kryptografię postkwantową i związane z nią luki w zabezpieczeniach);
- surowce krytyczne i bezpieczeństwo łańcucha dostaw (baterie, półprzewodniki, telekomunikacja);
- zagrożenia fizyczne (pożary, drony);
- satelity;
- szczególna dbałość o odporność energetyczną;
- bezpieczna telekomunikacja (5G, ale także 6G).

Ze względu na szybki rozwój technologii, niestabilność geopolityczną i zmieniającą się percepcję społeczną trudno jest dokładnie przewidzieć wszystkie zagrożenia. W przyszłych projektach i innowacyjnych działaniach powinny zostać dodatkowo uwzględnione następujące obszary:

- wzmocnienie wspólnego monitorowania zagrożeń cybernetycznych i fizycznych w czasie rzeczywistym oraz wymiana informacji o nich;
- wspólne ćwiczenia w całej UE;
- współpraca z globalnymi organizacjami normalizacyjnymi w celu zapewnienia, że priorytety UE w zakresie bezpiecznej infrastruktury już na etapie projektowania, etycznej sztucznej inteligencji i cyberbezpieczeństwa opartego na prywatności są odzwierciedlone w globalnych standardach;
- zwiększenie partnerstw publiczno-prywatnych z dostawcami technologii;
- współpraca z zaufanymi partnerami UE, w tym z Wielką Brytanią, USA, Kanadą, Japonią, Koreą Południową i Australią.

Wnioski

Ochrona IK pozostaje fundamentem europejskiej polityki bezpieczeństwa, zwłaszcza w obliczu ewoluujących zagrożeń hybrydowych. Unia Europejska podejmuje istotne działania w zakresie finansowania inicjatyw mających na celu wzmocnienie odporności IK. Projekty takie jak: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, TRANSCEND, NBSINFRA i ENDURANCE pokazują zakres wysiłków na rzecz zwiększenia bezpieczeństwa obejmujących rozwój technologii, koordynację polityki i współpracę transgraniczną.

Jednym z wniosków płynących z tej analizy jest rosnąca złożoność zagrożeń stojących przed operatorami IK. Konwergencja cybernetycznych

i fizycznych zagrożeń bezpieczeństwa, trudności wynikające z odmiennych krajowych regulacji prawnych i niespójnych interpretacji dyrektyw UE w państwach członkowskich UE oraz wyzwania dotyczące równoważenia innowacyjnych projektów z ich wdrażaniem wzmacniają potrzebę ciągłych wysiłków badawczo-rozwojowych. Pomimo że program Horyzont Europa i inne mechanizmy finansowania zapewniły duże wsparcie, konieczne są dodatkowe zasoby finansowe i strategiczne, aby utrzymać wiodącą pozycję UE w zakresie odporności infrastruktury.

Kolejnym istotnym spostrzeżeniem jest konieczność wspierania silniejszej współpracy między zainteresowanymi stronami. Omówione projekty pokazują znaczenie integracji perspektyw przemysłu, środowiska akademickiego, władz publicznych i społeczeństwa obywatelskiego. Wzmacnianie bardziej elastycznych i adaptacyjnych partnerstw będzie miało zasadnicze znaczenie w zmieniającym się krajobrazie zagrożeń. Ponadto zapewnienie, że wyniki badań zostaną przełożone na praktyczne zastosowania, będzie wymagało ściślejszej współpracy między decydentami, twórcami technologii i operatorami infrastruktury.

Kolejna faza badań i rozwoju polityki powinna koncentrować się na zwiększaniu odporności przez prognozowanie strategiczne, innowacje technologiczne i współpracę międzysektorową. Dzięki temu unijna IK pozostanie odporna na przyszłe zagrożenia i tym samym będzie chronić bezpieczeństwo i stabilność społeczeństw na kontynencie.

Zdaniem autorów warto monitorować i analizować, czy i w jaki sposób wyniki projektów opisanych w artykule zostały wdrożone w praktyce.

Bibliografia

Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses, OECD Publishing, Paris 2021. https://doi.org/10.1787/8fa190b5-en.

Źródła internetowe

Autonomous Swarm of Heterogeneous resourcse in infrastructure protection via threat prediction and prevention, European Commission, https://cordis.europa.eu/project/id/101121258 [dostęp: 15.01.2025].

Citynature-based Solutions integration to local urban infrastructure protection for a climate resilient society, https://cordis.europa.eu/project/id/101121210 [dostęp: 17.01.2025].

Critical infrastructure resilience at EU-level, European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [dostęp: 6.01.2025].

Empowering a Pan-European Network to Counter Hybrid Threats, European Commission, https://cordis.europa.eu/project/id/883054 [dostęp: 13.01.2025].

ENDURANCE, https://endurance-horizon.eu/ [dostęp: 17.01.2025].

EU-CIP, https://www.eucip.eu/ [dostęp: 13.01.2025].

EU-HYBNET, https://euhybnet.eu/ [dostęp: 13.01.2025].

European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection, European Commission, https://cordis.europa.eu/project/id/101073878 [dostęp: 13.01.2025].

Horizon Europe, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [dostęp: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027, European Commission, 2024, https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1 [dostęp: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027. Analysis, European Commission, 2023, https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en [dostęp: 9.01.2025].

Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024), https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf [dostęp: 10.01.2025].

Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats, https://defence-industry-space.ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [dostęp: 2.01.2025].

Kieslich K., Lünich M., *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, https://arxiv.org/abs/2401.13605v3 [dostęp: 7.02.2025]. https://doi.org/10.48550/arXiv.2401.13605.

NATO and European Union release final assessment report on resilience of critical infrastructure, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [dostęp: 6.01.2025].

NBSINFRA, https://nbsinfra.eu/ [dostęp: 17.01.2025].

Resilient Infrastructures, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [dostęp: 10.01.2025].

Strategic plan, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [dostęp: 3.01.2025].

Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe, European Commission, https://cordis.europa.eu/project/id/101168007 [dostęp: 17.01.2025].

Szymański P., *NATO i Unia Europejska wobec zagrożeń hybrydowych,* Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 7.02.2025].

TESTUDO, https://testudo-project.eu/ [dostęp: 15.01.2025].

The Commission calls on 23 Member States to fully transpose the NIS2 Directive, European Commission, 28.11.2024, https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive [dostęp: 29.01.2025].

The cybersecurity challenges of legacy OT and how to manage them, Control Engineering, 21.03.2024, https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them [dostęp: 7.02.2025].

TRANSCEND, https://www.transcend-logistics.eu/ [dostęp: 17.01.2025].

Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption, European Commission, https://cordis.europa.eu/project/id/101168023 [dostęp: 17.01.2025].

Vigilant Maritime Surveillance of Critical Submarine Infrastructure, European Commission, https://cordis.europa.eu/project/id/101168016 [dostęp: 14.01.2025].

VIGIMARE, https://vigimare.eu/ [dostęp: 15.01.2025].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. L 333/164 z 27.12.2022).

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. L 333/80 z 27.12.2022).

Zalecenie Rady z dnia 25 czerwca 2024 r. w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne (Dz. Urz. UE C 2024/4371 z 5.07.2024).

Małgorzata Wolbach

Starsza specjalistka ds. realizacji projektów w Polskiej Platformie Bezpieczeństwa Wewnętrznego (PPBW). Absolwentka studiów magisterskich na kierunku bezpieczeństwo wewnętrzne oraz licencjackich na kierunku kryminologia w Wyższej Szkole Policji w Szczytnie. W PPBW odpowiada za wdrażanie i realizację projektów finansowanych z programów Unii Europejskiej, ze szczególnym uwzględnieniem projektów dotyczących zagrożeń hybrydowych oraz bezpieczeństwa przestrzeni publicznych.

Kontakt: malgorzata.wolbach@ppbw.pl

Rashel Talukder

Prezes zarządu Polskiej Platformy Bezpieczeństwa Wewnętrznego. Od 2009 r. aktywnie uczestniczy w pracach badawczo-rozwojowych w obszarze bezpieczeństwa w Polsce i Europie, w tym jako koordynator projektów europejskich. Angażował się także w sprawy społeczności lokalnej jako radny gminy Stęszew (2018–2024).

Kontakt: rashel.talukder@ppbw.pl